e-Sveučilišta

Priručnik

o mrežnoj opremi, vatrozidu i sustavu za upravljanje i nadzor mreže (Cisco)

PROSINAC 2025.

CARNET

Sadržaj

Popis kratica

ACL (engl. *Access Control List*) – popis s pravima pristupa

ADOM (engl. *Administrative Domains*) – administrativna domena

AP (engl. *Access Point*) – bežična pristupna točka

BD (engl. *Building Distributor*) – razdjelnik zgrade

EBD (engl. *Existing Building Distributor*) – postojeći razdjelnik zgrade

CD (engl. *Campus Distributor*) – razdjelnik kampusa

ECD (engl. *Existing Campus Distributor*) – postojeći razdjelnik kampusa

FD (engl. *Floor Distributor*) – etažni razdjelnik

EFD (engl. *Existing Floor Distributor*) – postojeći etažni razdjelnik

EANE (engl. *Existing Active Network Equipment*) – postojeća aktivna oprema koja nije smještena u EFD

CCD (engl. *Computer Classroom Distributor*) – razdjelnik računalne učionice

ECCD (engl. *Existing Computer Classroom Distributor*) – postojeći razdjelnik računalne učionice

CPE (engl. *Customer Premises Equipment*) – oprema smještena na lokaciji korisnika

CSV (engl. *Comma-separated Values*) – format datoteke u kojoj su vrijednosti odvojene zarezom

DHCP (engl. *Dynamic Host Configuration Protocol*) – mrežni protokol kojim se koriste mrežna računala za dodjeljivanje IP adresa

DIS – dokumentacija izvedenog stanja

DNS (engl. *Domain Name System*) – domenski sustav imena

EFD (engl. *Existing Floor Distributor*) – postojeći etažni razdjelnik

EKM – elektronička komunikacijska mreža

FD (engl. *Floor Distributor*) – etažni razdjelnik

FORTILINK – protokol proizvođača Fortinet za komunikaciju između usmjerivača i preklopnika

GE (engl. *Gigabit Ethernet*) – prijenos okvira Ethernet brzinom od gigabita u sekundi

HTML (engl. *HyperText Markup Language*) – prezentacijski jezik za izradu mrežnih stranica

HTTPS (engl. *Hypertext Transfer Protocol Secure*) – skup pravila za siguran prijenos hipertekstualnih dokumenata između dvaju računala

ICMP (engl. *Internet Control Message Protocol*) – komunikacijski protokol koji je ugrađen u svaki IP modul da bi omogućio usmjerivačima i računalima slanje kontrolnih poruka o greškama

IP (engl. *Internet Protocol*) – mrežni protokol za prijenos podataka

LAN (engl. *Local Area Network*) – lokalna računalna mreža

MU-MIMO (engl. *Multi-user MIMO*) – skup tehnologija s više ulaza i više izlaza za višestruku bežičnu komunikaciju

NAT (engl. *Network Address Translation*) – prijevod IP adrese iz jedne mreže u drugu IP adresu u drugoj mreži

OSI (engl. *Open Systems Interconnection*) – model ili referentni model za otvoreno povezivanje sustava najkorišteniji je apstraktni opis arhitekture mreže

PDF (engl. *Portable Document Format*) – format zapisa dokumenata društva Adobe Systems

PoE (engl. *Power Over Ethernet*) – napajanje preko pasivne mrežne infrastrukture
PSK (engl. *Pre-shared key*) – unaprijed podijeljeni ključ

PP – prespojni panel

QoS (engl. *Quality of Service*) – kvaliteta usluge u mreži

RF (engl. *Radio Frequency*) – radijska frekvencija

SSID (engl. *Service Set Identifier*) – naziv (identifikator) bežične mreže

STP (engl. *Spanning Tree Protocol*) – mrežni protokol koji gradi logičku topologiju mreže bez petlji

TCP/IP (engl. *Transmission Control Protocol / Internet Protocol)* – referentni model, tehnički otvoreni standard interneta

TO (engl. *Telecommunications Outlet*) – priključna točka na pasivnu mrežnu infrastrukturu

UTP (engl. *Unshielded Twisted Pair*) – neoklopljena upletena parica

VLAN (engl. *Virtual Local Area Network*) – virtualna lokalna mreža

WAN (engl. *Wide Area Network*) – mreža širokog područja

WPA2 (engl. *Wi-Fi Protected Access 2*) – algoritam za sigurnu komunikaciju s pomoću bežičnih mreža IEEE 802.11

XML (engl. *Extensible Markup Language*) – jezik za označivanje podataka

1. Uvodne informacije

Ovaj priručnik o mrežnoj opremi i sustavu za upravljanje i nadzor mreže opisuje aktivnu i pasivnu mrežnu infrastrukturu implementiranu na sveučilištima u sklopu projekta „e-Sveučilišta“.

Obradit ćemo teme koje stručnom osoblju pokazuju najčešće probleme pri radu s novom opremom te načine rješavanja problema uočenih tijekom implementacije rješenja u sklopu projekta e-Sveučilišta. Također ćemo predstaviti dizajn sustava kako bi stručno osoblje bilo upoznato s novoimplementiranim uređajima i kako bi se olakšala administracija sustava u cjelini.

U priručniku se ujedno nalaze upute o postupanju u slučajevima poteškoća u radu sustava i o načinu prijave takvih poteškoća CARNET-ovu *helpdesku*.

Priručnik je namijenjen osobama koje pružaju tehničku podršku sveučilištima, odnosno stručno-tehničkom osoblju na ustanovama visokog obrazovanja, i svim drugim osobama koje jesu ili će biti angažirane na održavanju funkcionalnoga mrežnog sustava na sveučilištima radi što boljeg upoznavanja s implementiranim sustavom na operativnoj razini.

Budući da se u sklopu projekta koristi oprema više proizvođača, pojedina poglavlja usmjerena su na opis rada različitih ekosustava kako bi se razjasnili najčešći izazovi s kojima se stručno osoblje može susresti.

Također su objašnjene fizičke oznake uređaja, spojeva i ormara radi lakšeg snalaženja dokumentaciji, jednostavnijeg održavanja sustava nakon završetka projekta i u svrhu dokumentiranja svega što je u sklopu projekta e-Sveučilišta implementirano.

2. Osnove mrežnog sustava

Kao preduvjet za administraciju i nadzor računalne mrežne infrastrukture implementirane u sklopu projekta „e-Sveučilišta“ nužno je da stručno-tehničko osoblje na ustanovama visokog obrazovanja zaduženo za administraciju sustava bude upoznato s osnovama mrežnog sustava, mrežnim protokolima i servisima, osnovama rada bežične mreže, kao i sa sigurnošću računalnih mreža.

Budući da se od stručno-tehničkog osoblja očekuje poznavanje osnova mrežnih tehnologija i pripadajućih protokola, u ovom priručniku osnove neće biti dodatno objašnjene.

Digitalni priručnik temeljit će se na objašnjenju najčešćih zadataka s kojima se administrator sustava svakodnevno susreće, kao i na objašnjenju složenijih zadataka koje je potrebno odraditi radi sigurnosti organizacije i prometa koji prolazi njezinom mrežnom infrastrukturom. Također će obuhvatiti primjenu alata koji su namijenjeni olakšavanju administracije stručno-tehničkom osoblju.

3. Pasivna mrežna oprema

U sklopu projekta „e-Sveučilišta“ u glavnim izvedbenim projektima (GIP) definirani su parametri kvalitete pasivne mrežne infrastrukture koja se postavlja na sveučilištima.

Za potrebe novog sustava kabliranja na sveučilištima se upotrebljavaju postojeće trase (kabelski kanali) i postojeći etažni razdjelnici (EFD) ako raspolažu dovoljnim kapacitetom. Za svako sveučilište za koje je izvedeno kabliranje u sklopu projekta izgradnje pasivne mrežne infrastrukture izrađen je i dokument izvedenog stanja (DIS) pasivne mrežne infrastrukture sveučilišta.

Ako je prethodno postojeća pasivna infrastruktura bila zadovoljavajuće propusnosti i kvalitete, tada nisu poduzeti dodatni koraci poboljšanja pasivne infrastrukture, no ako nije bila pouzdana, stabilna, dovoljne propusnosti ili je jednostavno bila nepostojeća, u sklopu projekta implementirana je nova pasivna infrastruktura.

Novoizgrađena pasivna infrastruktura omogućuje sljedeća poboljšanja ako nisu bili zadovoljeni parametri postojeće pasivne infrastrukture:

- poboljšano korisničko iskustvo – povećati pouzdanost i brzinu mreže, bolje interakcije uz povećanje zadovoljstva
- povećane performanse mreže – povećati brzine, smanjiti latencije i poboljšati pouzdanost
- unaprijeđena mrežna sigurnost – implementacija sigurnosnih mjera uz omogućeno usklađivanje s propisima o zaštiti osobnih podataka
- povećana skalabilnost – omogućiti jednostavnu skalabilnost i proširenja
- pojednostavnjeno upravljanje – pojednostavniti i centralizirati upravljanje mrežom što je moguće više, olakšavajući praćenje i tijek rješavanja problema
- povećana produktivnost – omogućiti brži pristup informacijama i aplikacijama te napredne alate za suradnju (videokonferencije i aplikacije u oblaku)
- smanjenje troškova – smanjiti troškove eksploatacije i održavanja.

3.1. Komunikacijski ormari i priključnice

Aktivni uređaji, prespojni paneli i sl. smještaju se u razdjelnike u skladu s DIS-om pasivne mrežne infrastrukture sveučilišta u kojem je predložen raspored opreme po komunikacijskim ormarima. Razmještaj i eventualna manja preraspodjela postojeće opreme po razdjelnicima izvode se na lokaciji pri instalaciji pasivne i prateće aktivne opreme.

U DIS-u pasivne mrežne infrastrukture sveučilišta upotrebljavaju se sljedeće oznake, odnosno kratice za komponente:

1. okosnicu zgrade (BB – engl. *Building Backbone*)
2. etažno kabliranje (xF) s funkcionalnim elementima:

a. razdjelnik kampusa (CD – engl. *Campus Distributor*)
b. postojeći razdjelnik kampusa (ECD – engl. *Existing Campus Distributor*)
c. razdjelnik zgrade (BD – engl. *Building Distributor*)
d. postojeći razdjelnik zgrade (EBD – engl. *Existing Building Distributor*)
e. etažni razdjelnik (FD – engl. *Floor Distributor*)
f. postojeći etažni razdjelnik (EFD – engl. *Existing Floor Distributor*);
g. postojeća aktivna oprema koja nije smještena u EFD (EANE – engl. *Existing Active Network Equipment*)
h. razdjelnik računalne učionice (CCD – engl. *Computer Classroom Distributor*)
i. postojeći razdjelnik računalne učionice (ECCD – engl. *Existing Computer Classroom Distributor*)
j. kabel okosnice
k. elementi etažnog kabliranja.

Smještaj pasivne i aktivne mrežne opreme osiguran je u postojećim razdjelnicima objekta, kata i kampusa gdje za to postoje odgovarajući uvjeti. Sustav je projektiran tako da ostaje zalihost slobodnog prostora od minimalno 25 % kapaciteta razdjelnika. Ako nije moguće smjestiti opremu na opisani način, ugrađuje se novi razdjelnik objekta, kata i kampusa minimalnog kapaciteta 12 RU.

U slučaju ugradnje novih razdjelnika FD, BD i CD povezuju se s postojećim komunikacijskim razdjelnicima optičkim kabelom kako bi se omogućili zahtjevi povezivosti i propusnosti okosnice mreže od 10 Gbps. Razdjelnici koji se nalaze u istoj prostoriji smatraju se jednim razdjelnikom ako se krajnje točke u njima mogu povezati s odgovarajućim prespojnim kabelom duljine do 10 m. U suprotnom se smatraju neovisnim razdjelnicima.

Svi razdjelnici obuhvaćeni projektom u kojima je ugrađena mrežna oprema izravno su povezani s razdjelnikom zgrade EBD/BD. Postojeći katni razdjelnici i razdjelnici računalnih učionica u koje se ne ugrađuje oprema iz projekta svjetlovodnim se kabelima povezuju na razdjelnik koji je obuhvaćen projektom. U slučaju popunjenosti postojećih ormara projektirani su ormarići za prespajanje svjetlovodnih kabela. Kad se BD i EBD ne mogu smatrati jednim razdjelnikom, povezuju se optičkim kabelom, pri čemu je u EBD razdjelnik smješten preklopnik koji podržava 10G optička sučelja.

Ako model lokacije zahtjeva opremanje ili zamjenu preklopnika za povezivanje žičnog djela lokalne mreže, tada je u slučajevima nedostatnog kapaciteta u postojećem razdjelniku osigurana mogućnost prespoja postojećih horizontalnih žičnih veza na novu opremu. Ako je u sklopu projekta dogovorena fizička zamjena postojeće opreme s novom zbog nedostatka mjesta u razdjelniku, nova oprema je implementirana, integrirana, a postojeće veze migrirane su tako da mreža nakon završetka radova ostane funkcionalna.

Glavni razdjelnik zgrade (BD) služi za smještaj aktivne mrežne opreme i pratećih sredstava nužnih za osiguranje pune funkcionalnosti dijela elektroničke komunikacijske mreže (EKM) za dio zgrade koji opslužuju.

Slika 1. Primjer razdjelnika BD

Etažni je razdjelnik (FD) optičkim kabelom povezan s glavnim razdjelnikom zgrade (BD) u skladu s namjenom.

Slika 2. Primjer razdjelnika FD

Razdjelnik kampusa (CD) optičkim je kabelom povezan s glavnim razdjelnikom zgrade (BD) u skladu s namjenom. Namjena ovog razdjelnika je povezivanje kampusa optičkim međuvezama.

Slika 3. Primjer razdjelnika CD

Razdjelnik računalne učionice (CCD) optičkim je kabelom povezan s glavnim razdjelnikom zgrade (BD) u skladu s namjenom. Primarna namjena ormara je dovođenje mrežnih instalacija do računalnih učionica na ustanovama.

Slika 4. Primjer razdjelnika CCD

Za potrebe horizontalnog kabliranja koriste se telekomunikacijski priključci (TO – engl. *Telecommunications Outlet*) koji su modularne (ugrađuju se u parapetne kanale) ili nadžbukne (samostojeće) izvedbe.

Slika 5. Primjer priključne kutije

Za potrebe horizontalnog kabliranja upotrebljavaju se prespojni paneli izvedbe RJ45 za montažu unutar telekomunikacijskih ormara 19" (19 inča), visine 1U, s 24 priključna mjesta za module čiji standard odgovara ugrađenom kabelu.

Slika 6. Primjer modula RJ45

Prespojni paneli namijenjeni su za ugradnju u razdjelnike širine vertikalnih tračnica 19". Prespajanje krajnjih točaka kabela međusobno, kao i spajanje aktivnih uređaja na njih, izvedeno je prespojnim kabelima unutar razdjelnika.

Slika 7. Primjer optičkoga prespojnog panela LC

Slika 8. Primjer modularnoga prespojnog panela UTP

Svjetlovodni prespojni kabeli imaju dvije niti (engl. *duplex*). Oni su zaključeni svjetlovodnim konektorima tipa LC.

Slika 9. Svjetlovodni konektor LC

Prespojni kabeli kategorije U/UTP 6A (Cat. 6A) s obje su strane zaključeni konektorima RJ45.

Slika 10. Konektor UTP RJ45

3.2. Sustav označivanja

Oznake komunikacijskih ormara i krajnjih točaka njihove terminacije slijede preporuke za strukturno kabliranje, ali prilagođavaju se specifičnostima prostora. U nastavku je iznesen detaljan opis sustava označivanja.

3.2.1. Fizički položaji

Fizičkim položajima prethodi znak „+“. Položaji građevina, komunikacijskih razdjelnika i opreme prikazani su u dispozicijskim nacrtima.

Radni prostori u kojima se izvode radovi instalacija strukturnoga kabliranja lokalne računalne mreže smješteni su po etažama građevine. Svaka od etaža te pripadajući fizički položaji opreme na pojedinoj etaži označuju se odgovarajućom oznakom.

3.2.2. Oznaka etaže

Tablica 1 u nastavku prikazuje oznake etaža.

ETAŽA	OZNAKA
1. kat	+01
prizemlje	+00
podrum	+99

Tablica 1. Oznaka etaža

Primjer:

- +01 – označuje fizički položaj na prvoj etaži (+01).

3.2.3. Oznaka razdjelnika

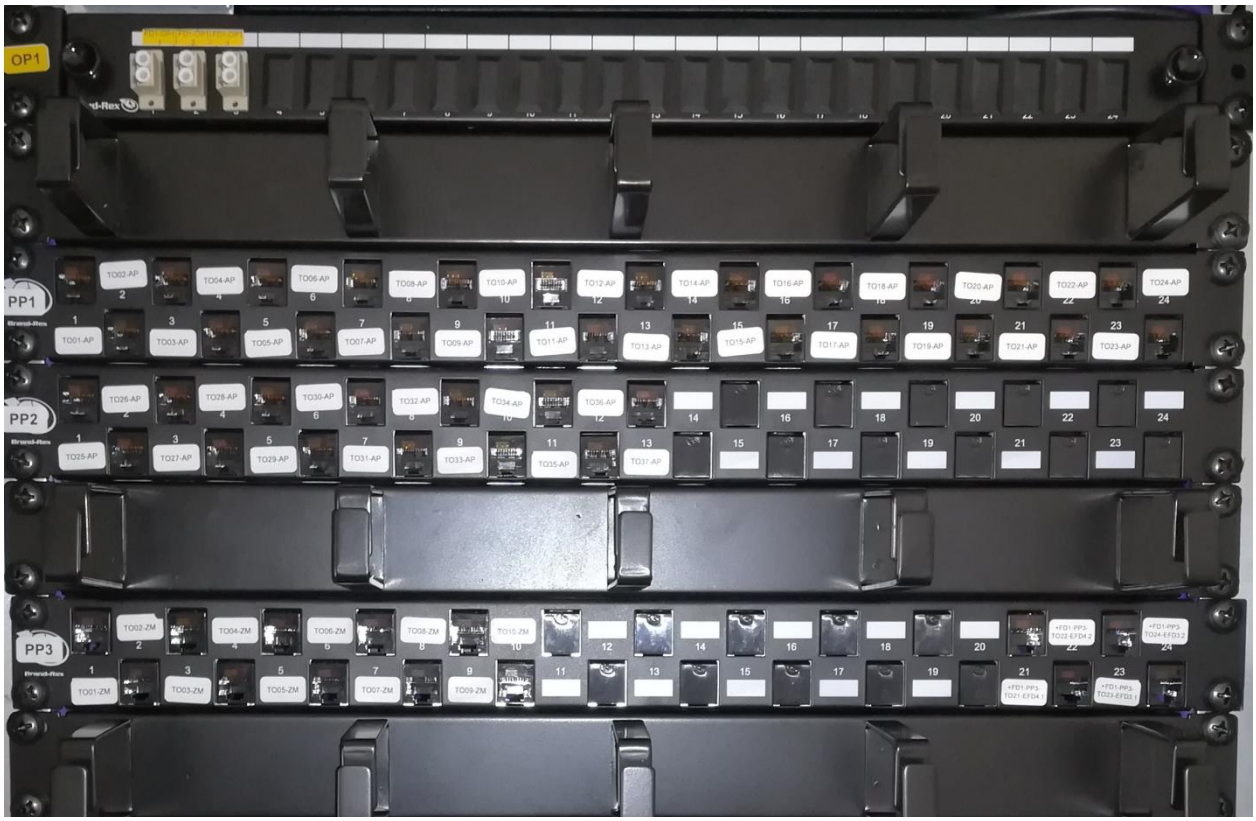
Čvorište instalacije strukturnoga kabliranja čine razdjelnici koji se upotrebljavaju za smještanje aktivnih uređaja računalne mreže i opreme za prespajanje segmenata strukturnoga kabliranja. U nastavku se nalazi opis funkcija razdjelnika i način označivanja pojedinih dijelova razdjelnika:

- +BD – glavni razdjelnik zgrade – čvor koji povezuje vertikalne razvode s horizontalnim razvodom kabela. U razdjelniku je ujedno postavljen i uređaj CPE koji služi za terminiranje WAN mreže (WAN – engl. *Wide Area Network*).
- +FD – razdjelnik etaže – čvor koji povezuje horizontalne razvode kabela s priključnim mjestima u učionicama i ostalim uredima.
- +CD – razdjelnik kampusa – čvor koji povezuje zgrade kampusa, odnosno udaljene lokacije ustanova.
- +CCD– razdjelnik računalne učionice – čvor koji povezuje horizontalne razvode kabela od računalnih učionica do opreme na lokaciji ustanove
- +EFD – postojeći etažni razdjelnik
- +EBD – postojeći razdjelnik zgrade
- +ECD – postojeći razdjelnik kampusa
- +ECCD – postojeći razdjelnik računalne učionice.

Pojedini položaji u razdjelniku definiraju se na sljedeći način:

- **+BDy-PPx-z** – **y** označuje broj razdjelnika **BD**, **PP** označuje prespojni panel, **x** označuje njegov redni broj, dok **z** označuje položaj na panelu, tj. broj porta.
- Primjer:

- **+BD1-PP1-TO05-AP** – fizički je položaj koji, čitano zdesna nalijevo, označuje priključak **5** za bežičnu pristupnu točku (**AP**) na prespojnom panelu **1** (PP1) u razdjelniku **BD** (+BD1)
- **+BD1-PP2-TO01** – fizički je položaj koji, čitano zdesna nalijevo, označuje priključak **1** na prespojnom panelu **2** (PP2) u razdjelniku **BD** (+BD1).



Slika 11. Primjer označivanja razdjelnika i panela

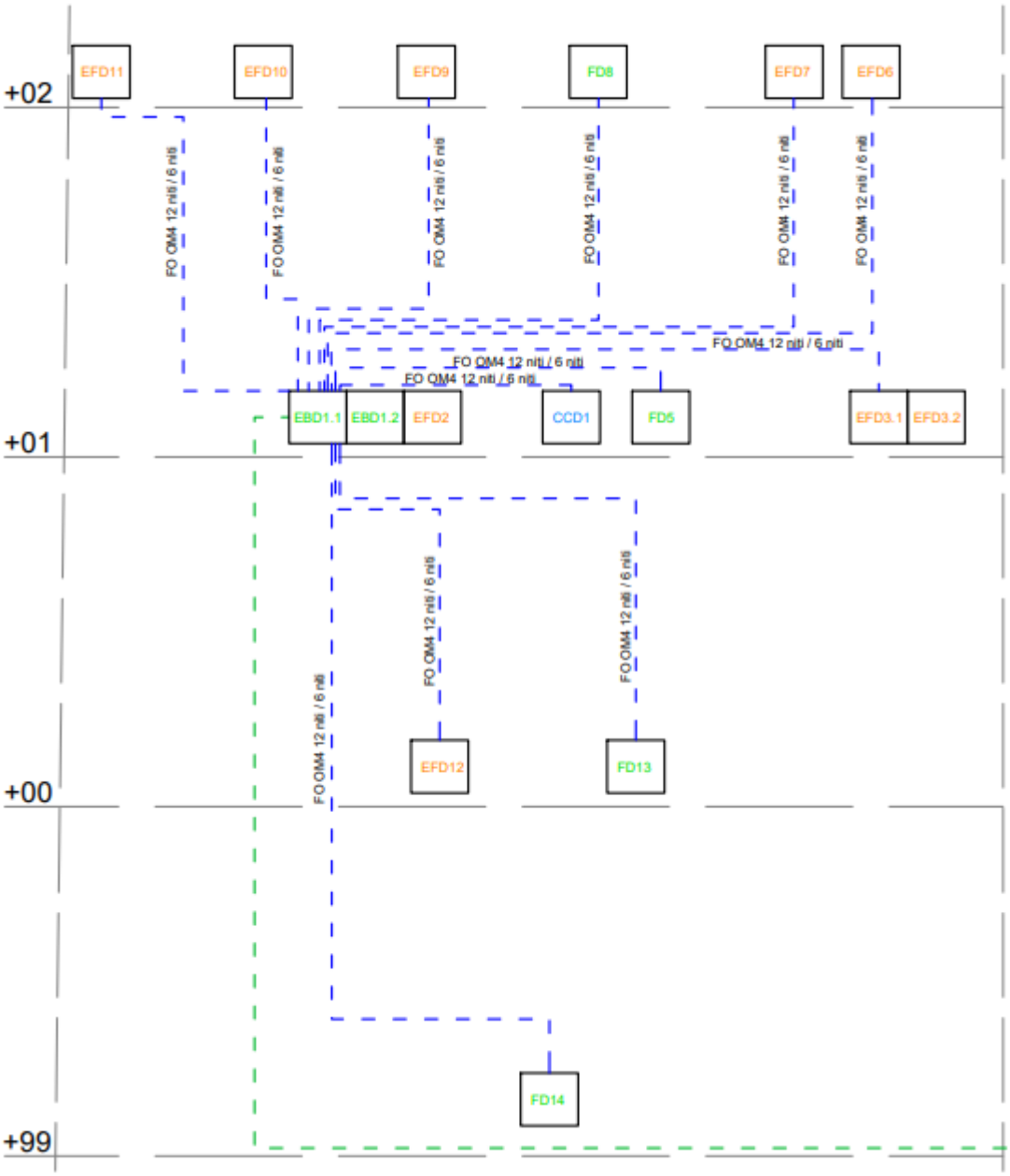
Slika 12. Primjer označivanja priključnica

3.3. Primjeri i načini veza komunikacijskih ormara

Prijenosni mediji kojima se povezuju komunikacijski ormari su:

- višemodni svjetlovodni kabeli kategorije OM4 s 12 niti
- jednomodni svjetlovodni kabeli kategorije OS2 s 12 niti
- bakreni kabel s četiri parice (U/UTP) kategorije 6A (Cat. 6A).

Takvi prijenosni mediji omogućuju primjenu strukturnoga kabliranja tijekom više budućih generacija računalnih mreža koje će raditi na većim brzinama.



Slika 13. Primjer povezivanja komunikacijskih ormara

4. Aktivna mrežna oprema

Implementirani mrežni sustav zasnovan je na rješenjima proizvođača Fortinet i Cisco.

U ovom poglavlju opisane su osnovne komponente implementiranoga aktivnog mrežnog sustava na javnoobrazovnim ustanovama u visokom obrazovanju, isporučeni modeli, njihova uloga i konfiguracijske značajke.

4.1. Arhitektura sustava

Implementirani mrežni sustav je više komponentno rješenje u kojem se instaliranom mrežnom opremom upravlja s pomoću središnjeg sustava za upravljanje i nadzor mreže. U ovakvom modelu različitim se slojevima lokalne mreže upravlja i nadzire primjenom jedne komponente nadzorno-upravljačkog sloja. Pri implementaciji Fortinet i Cisco rješenja imamo dva ekosustava koja imaju dva nadzorno-upravljačka alata.

Implementirani mrežni sustav sastoji se od upravljačkog dijela mreže i od lokalne mreže sveučilišta. U ovom je poglavlju stavljen naglasak na implementiranu aktivnu mrežnu opremu lokalne mreže sveučilišta, dok je upravljački dio implementiranoga mrežnog sustava opisan u poglavljima za nadzorne upravljačke sustave.

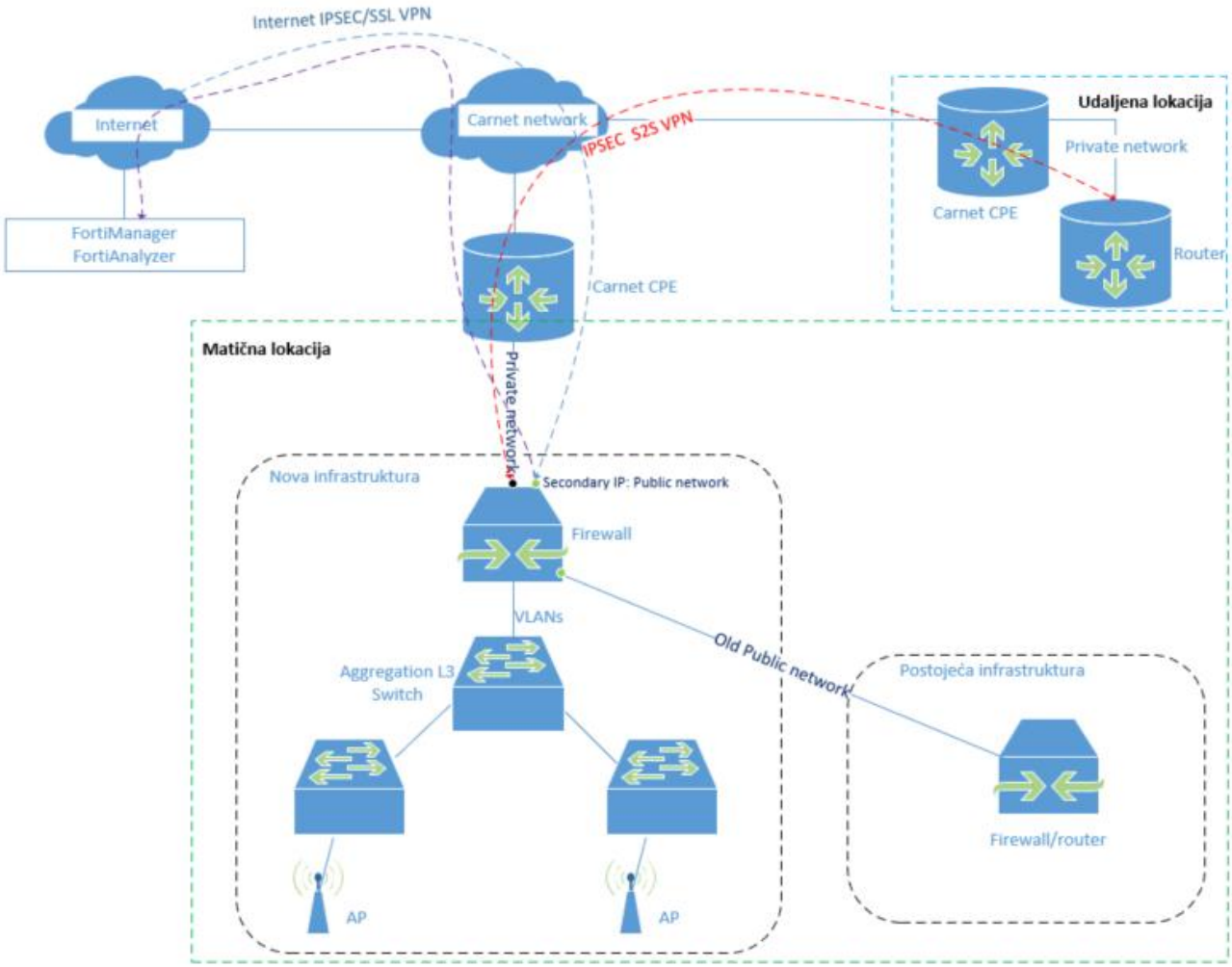
Sve aktivne mrežne komponente sveučilišta čine logičku cjelinu pristupnog sloja, a sastoje se od:

- mrežnog vatrozida (žični pristup)
- mrežnog usmjerivača (žični pristup)
- mrežnih preklopnika (žični pristup)
- bežičnih pristupnih točaka (bežični pristup).

Svako je sveučilište povezano na CARNET-ovu mrežu kojom korisnici ostvaruju pristup potrebnim servisima i internetu. Povezanost na CARNET-ovu mrežu ostvarena je s pomoću CARNET CPE-a (engl. *customer premises equipment*) koji se može nalaziti i na drugoj ustanovi u neposrednoj blizini koja je povezana lokalnim spojem. Na njega je povezan glavni vatrozid implementiran u sklopu projekta. U slučaju odrade implementacije ustanove koja nema udaljene lokacije mrežna oprema spojena je na vatrozid preko distribucijskog uređaja, odnosno distribucijskog preklopnika koji skuplja promet ostalih preklopnika u ustanovi. Na ostale preklopnike povezane su bežične pristupne točke.

U slučaju ustanove koja ima nekolicinu udaljenih lokacija koriste se usmjerivači FortiGate. Ovi uređaji su vatrozidi na kojima se ne odrađuje sigurnosna inspekcija, već se sav promet šalje s udaljene lokacije na primarnu lokaciju s pomoću enkriptiranog tunela kako bi se održao integritet i sigurnost podataka. U slučaju gubitka veze sa središnjim vatrozidom na

matičnoj lokaciji usmjerivač FortiGate povezan je sa sekundarnim linkom koji služi u svrhu redundancije. Navedeni link terminira se na uređaju CARNET CPE.



Slika 14. Shema implementiranog sustava sa sastavnim blokovima

4.2. Sigurnosna mrežna oprema

4.2.1. Vatrozid – tehničke značajke FortiGate uređaja

Vatrozid (engl. *firewall*) jest sigurnosni element računalne mreže koji omogućuje kontrolu dolaznoga i odlaznog prometa između različitih mrežnih segmenata. U sklopu sustava e-Sveučilišta implementirani su vatrozidni uređaji proizvođača Fortinet, serije FortiGate, različitih modela (90G, 100F, 200F, 200G, 400F i 600F), ovisno o veličini i potrebama ustanove.

FortiGate uređaji integriraju više sigurnosnih funkcija u jednom uređaju:

- Stateful firewall s mogućnošću filtriranja prometa na razini slojeva 3 i 4 OSI modela
- dubinska inspekcija paketa (DPI) i prepoznavanje aplikacija
- antivirus, Antispam i web filtering
- Intrusion Prevention System (IPS) – sustav za sprečavanje upada
- VPN podrška (IPSec i SSL)
- NAT (Network Address Translation) funkcionalnosti
- kontrola prometa i propusnosti (QoS)
- segmentacija mreže preko VLAN-ova
- *zero-touch provisioning* – automatska konfiguracija preko FortiManagera
- integrirani bežični kontroler (Wireless LAN controller)
- podrška za visoku dostupnost (HA – High Availability).

FortiGate 90G je suvremeno rješenje iz kategorije vatrozida nove generacije (NGFW – Next Generation Firewall). Ovaj uređaj objedinjuje osnovne mrežne funkcije s naprednim sigurnosnim tehnologijama koje koriste umjetnu inteligenciju i strojno učenje za prepoznavanje i sprečavanje prijetnji. Namijenjen je manjim i srednje velikim organizacijama, uključujući obrazovne institucije, gdje djeluje kao centralna točka mrežne sigurnosti. Njegova uloga je zaštita interne mreže, nadzor i analiza mrežnog prometa te upravljanje pristupom prema internetu i drugim vanjskim mrežnim resursima. Zahvaljujući integriranim sigurnosnim mehanizmima, poput detekcije upada, filtriranja internetskog sadržaja i zaštite od zlonamjernog softvera, omogućuje pouzdanu zaštitu i stabilno funkcioniranje mrežne infrastrukture.

Tehničke značajke:

• IPS propusnost: 4,5 Gbps

• NGFW propusnost: 2,5 Gbps

• propusnost zaštite od prijetnji (Threat Protection): 2,2 Gbps

• IPv4 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 28 / 28 / 27,9 Gbps

• Firewall latencija (64 bajta, UDP): 3,23 µs

• Firewall performanse (paketa u sekundi): 41,85 Mpps

• maksimalan broj istovremenih sesija (TCP): 3 milijuna

• nove sesije u sekundi (TCP): 124.000

• Firewall pravila: 5.000
• IPsec VPN propusnost (512 bajta): 25 Gbps
• Gateway-to-Gateway IPsec VPN tuneli: 200
• Client-to-Gateway IPsec VPN tuneli: 2.500
• SSL-VPN propusnost: 1,4 Gbps
• maksimalan broj SSL-VPN korisnika: 200
• SSL inspekcija (prosjek HTTPS): 2,6 Gbps
• SSL inspekcija CPS: 1.400
• maksimalne SSL inspekcijske sesije: 300.000
• propusnost kontrole aplikacija (HTTP 64K): 6,7 Gbps
• CAPWAP propusnost: 23,6 Gbps
• virtualne domene (VDOMs): 10 (maksimalno)
• maksimalan broj FortiSwitch uređaja: 24
• maksimalan broj FortiAP uređaja: 128 (ukupno) / 64 (tunelirani)
• maksimalan broj FortiToken uređaja: 500
• visoka dostupnost: Active-Active, Active-Passive, Clustering

Fizička sučelja:

• 2 × 10/5/2.5/1 GE RJ45 ili 10GE/GE SFP+ dijeljeni (*shared media*) portovi – mogu se koristiti kao WAN ili LAN sučelja
• 8 × GE RJ45 portova za povezivanje lokalnih mrežnih uređaja
• 1 × RJ45 konzolni port za lokalnu administraciju uređaja
• 1 × USB port za upravljanje i servisne funkcije

Ostale značajke:

• oblik kućišta: Desktop
• dimenzije (V × Š × D): 42 × 216 × 178 mm
• težina: 1,12 kg
• napajanje: 12 V DC, 3 A (mogućnost redundantnog napajanja s do dva vanjska adaptera)
• AC adapter: 100–240 V AC, 50/60 Hz
• potrošnja energije: 19,9 W (prosjek) / 20,53 W (maks.)

• otpornost na toplinu: 70,0 BTU/h

• radna temperatura: 0 °C do 40 °C

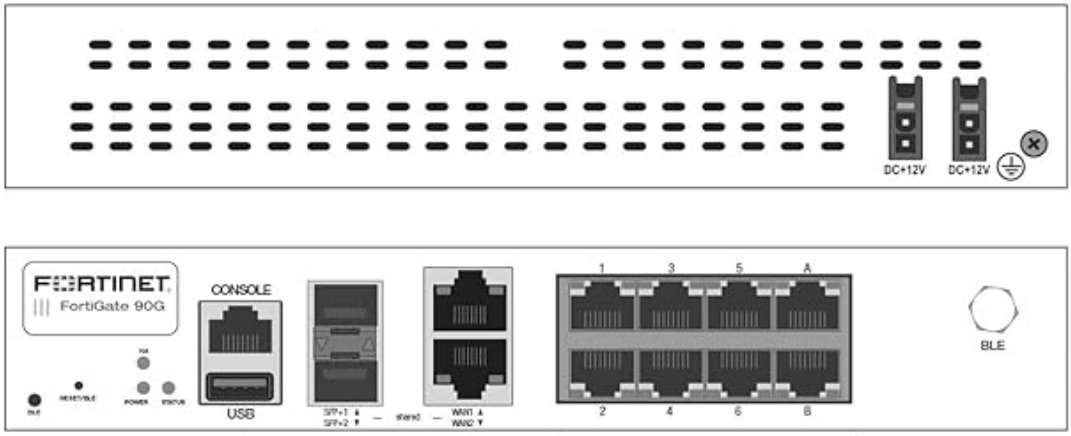
• skladišna temperatura: –35 °C do 70 °C

• vlažnost: 10 % do 90 % (bez kondenzacije)

• razina buke: 21,73 dBA

• maksimalna radna visina: 3.048 m (10.000 ft)

• certifikati: FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB, USGv6/IPv6



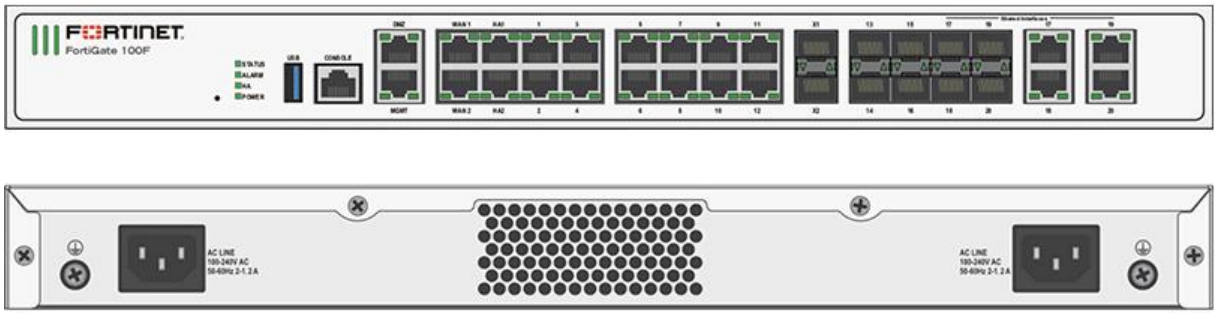
Slika 15. FortiGate 90G

FortiGate 100F je napredni uređaj nove generacije vatrozida (NGFW – *Next Generation Firewall*) koji kombinira klasične mrežne funkcionalnosti s naprednim sigurnosnim značajkama temeljenima na umjetnoj inteligenciji i strojnom učenju. Uređaj je prilagođen srednje velikim okruženjima poput obrazovnih ustanova, a koristi se kao središnja sigurnosna komponenta za zaštitu lokalne mreže i kontrolu pristupa prema vanjskim resursima.

Tehničke značajke:

- IPS propusnost: 2,6 Gbps
- NGFW propusnost: 1,6 Gbps
- propusnost zaštite od prijetnji (Threat Protection): 1 Gbps
- IPv4 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 20 / 18 / 10 Gbps
- Firewall latencija (64 bajta, UDP): 4,97 µs
- Firewall performanse (paketa u sekundi): 15 Mpps
- maksimalan broj istovremenih sesija (TCP): 1,5 milijuna
- nove sesije u sekundi (TCP): 56.000

- Firewall pravila: 10.000
- IPsec VPN propusnost (512 bajta): 11,5 Gbps
- SSL-VPN propusnost: 1 Gbps
- maksimalan broj SSL-VPN korisnika: 500
- SSL inspekcija (prosjek HTTPS): 1 Gbps
- SSL inspekcija CPS: 1.800
- maksimalne SSL inspekcijske sesije: 135.000
- propusnost kontrole aplikacija (HTTP 64K): 2,2 Gbps
- CAPWAP propusnost: 15 Gbps
- virtualne domene (VDOMs): 10 (maksimalno)
- maksimalan broj FortiSwitch uređaja: 32
- maksimalan broj FortiAP uređaja: 128 (ukupno) / 64 (tunelirani)
- maksimalan broj FortiToken uređaja: 5.000
- visoka dostupnost: Active-Active, Active-Passive, Clustering.



Slika 16. FortiGate 100F

Fizička sučelja:

- GE RJ45 portovi: 12
- GE RJ45 upravljački / HA / DMZ portovi: 1 / 2 / 1
- GE RJ45 WAN portovi: 2
- GE SFP portovi: 4
- 10 GE SFP+ FortiLink portovi (default): 2
- GE RJ45 ili SFP dijeljeni portovi: 4

- USB port: 1
- konzolni port: 1
- ugrađeno spremište:
    - FG-100F: bez diska

Ostale značajke:

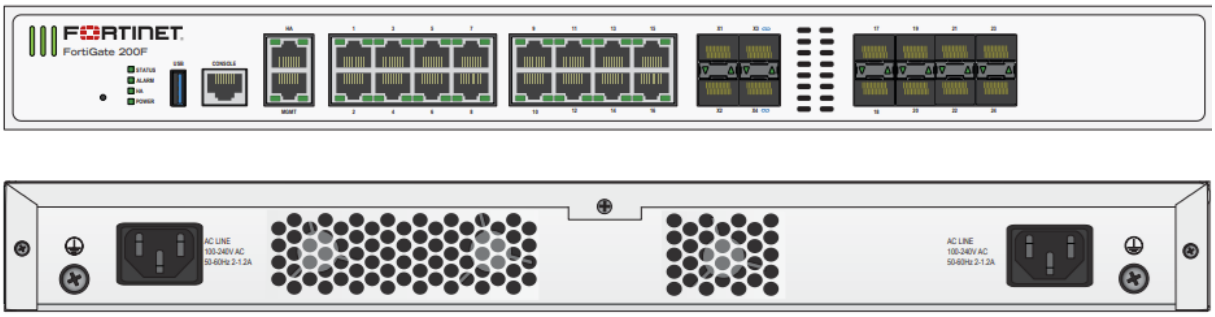
- oblik kućišta: Rack Mount, 1 RU
- dimenzije (V x Š x D): 44 x 432 x 254 mm
- težina:
    - FG-100F: 3,29 kg
- napajanje: 100–240 V AC, 50/60 Hz
- potrošnja energije:
    - FG-100F: 26,5 W (prosjek) / 29,5 W (maks.)
- otpornost na toplinu: 100,6 – 121,13 BTU/h
- redundantno napajanje: Da (dualno, neizmjenjivo, 1+1 redundancija)
- radna temperatura: 0 °C do 40 °C
- skladišna temperatura: –35 °C do 70 °C
- vlažnost: 10 % do 90 % (bez kondenzacije)
- razina buke: 40,4 dBA
- maksimalna radna visina: 3.048 m (10.000 ft)
- certifikati: FCC Part 15B Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI, USGv6/IPv6.

FortiGate 200F je uređaj nove generacije vatrozida (NGFW) koji pruža naprednu zaštitu, visoku propusnost i mogućnosti mrežne segmentacije u okruženjima srednjega do većeg kapaciteta, poput većih sveučilišnih ustanova. Ovaj je model dizajniran za obradu velikog broja istovremenih veza i za implementaciju naprednih sigurnosnih servisa, bez većeg utjecaja na performanse.

Tehničke značajke:

- IPS propusnost: 5 Gbps
- NGFW propusnost: 3,5 Gbps
- propusnost zaštite od prijetnji (Threat Protection): 3 Gbps
- IPv4 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 27 / 27 / 11 Gbps
- Firewall latencija (64 bajta, UDP): 4,78 µs

- Firewall performanse (paketa u sekundi): 16,5 Mpps
- maksimalan broj istovremenih sesija (TCP): 3 milijuna
- nove sesije u sekundi (TCP): 280.000
- Firewall pravila: 10.000
- IPsec VPN propusnost (512 bajta): 13 Gbps
- SSL-VPN propusnost: 2 Gbps
- maksimalan broj SSL-VPN korisnika: 500
- SSL inspekcija (prosjek HTTPS): 4 Gbps
- SSL inspekcija CPS: 3.500
- maksimalne SSL inspekcijske sesije: 300.000
- propusnost kontrole aplikacija (HTTP 64K): 13 Gbps
- CAPWAP propusnost: 20 Gbps
- virtualne domene (VDOMs): 10 (zadano) / 25 (maksimalno)
- maksimalan broj FortiSwitch uređaja: 64
- maksimalan broj FortiAP uređaja: 256 (ukupno) / 128 (tunelirani)
- maksimalan broj FortiToken uređaja: 5.000
- visoka dostupnost: Active-Active, Active-Passive, Clustering.



Slika 17. FortiGate 200F

Fizička sučelja:

- GE RJ45 portovi: 16
- GE RJ45 upravljački / HA portovi: 1 / 1
- GE SFP portovi: 8
- 10 GE SFP+ FortiLink portovi (default): 2

- 10 GE SFP+ portovi: 2
- USB port: 1
- konzolni port: 1
- ugrađeno spremište:
    - FG-200F: bez diska

Ostale značajke:

- oblik kućišta: Rack Mount, 1 RU
- dimenzije (V x Š x D): 44 x 432 x 342 mm
- težina:
    - FG-200F: 4,5 kg
- napajanje: 100 – 240 V AC, 50/60 Hz
    - potrošnja energije:FG-200F: 101,92 W (prosjek) / 118,90 W (maks.)
- otpornost na toplinu: 405,7 – 436,98 BTU/h
- redundantno napajanje: Da (dualno, neizmjenjivo, 1+1 redundancija)
- radna temperatura: 0 °C do 40 °C
- skladišna temperatura: –35 °C do 70 °C
- vlažnost: 20 % do 90 % (bez kondenzacije)
- razina buke: 49,9 dBA
- maksimalna radna visina: 3.048 m (10.000 ft)
- certifikati: FCC Part 15B Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI, USGv6/IPv6.

FortiGate 200G je napredni uređaj vatrozida nove generacije (NGFW – Next Generation Firewall) koji objedinjuje klasične mrežne funkcije s naprednim sigurnosnim tehnologijama temeljenima na umjetnoj inteligenciji i strojnom učenju. Uređaj je namijenjen srednje velikim i većim organizacijama te se koristi kao središnja sigurnosna komponenta za zaštitu mrežne infrastrukture. Integracijom funkcija poput zaštite od mrežnih napada, filtriranja mrežnog sadržaja, kontrole aplikacija i sigurnog pristupa mrežnim resursima omogućuje potpunu kontrolu i nadzor mrežnog prometa. Zahvaljujući operacijskom sustavu FortiOS i integraciji s Fortinet Security Fabric platformom uređaj pruža visoku razinu sigurnosti, jednostavno upravljanje i učinkovitu zaštitu od suvremenih kibernetičkih prijetnji.

Tehničke značajke:

• IPS propusnost: 9 Gbps
• NGFW propusnost: 7 Gbps
• propusnost zaštite od prijetnji (Threat Protection): 6 Gbps
• IPv4 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 39 / 39 / 26,5 Gbps
• Firewall latencija (64 bajta, UDP): 4,36 µs
• Firewall performanse (paketa u sekundi): 39,75 Mpps
• maksimalan broj istovremenih sesija (TCP): 11 milijuna
• nove sesije u sekundi (TCP): 400.000
• Firewall pravila: 10.000
• IPsec VPN propusnost (512 bajta): 36 Gbps
• Gateway-to-Gateway IPsec VPN tuneli: 2.000
• Client-to-Gateway IPsec VPN tuneli: 16.000
• SSL-VPN propusnost: 3 Gbps
• maksimalan broj SSL-VPN korisnika: 500
• SSL inspekcija (prosjek HTTPS): 7 Gbps
• SSL inspekcija CPS: 7.100
• maksimalne SSL inspekcijske sesije: 900.000
• propusnost kontrole aplikacija (HTTP 64K): 27,8 Gbps
• CAPWAP propusnost: 37,5 Gbps
• virtualne domene (VDOMs): 10/25 (standardno/maksimalno)
• maksimalan broj FortiSwitch uređaja: 64
• maksimalan broj FortiAP uređaja: 256 (ukupno) / 128 (tunelirani)
• maksimalan broj FortiToken uređaja: 5.000
• visoka dostupnost: Active-Active, Active-Passive, Clustering

Fizička sučelja:
• 8 × GE RJ45 portova (switch portovi)
• 8 × 5/2.5/GE RJ45 portova (switch portovi)
• 1 × GE RJ45 management port
• 1 × GE RJ45 HA port
• 4 × GE SFP slotova

• 8 × 10GE SFP+ FortiLink slotova

• 1 × USB port

• 1 × RJ45 konzolni port

Ostale značajke:

• oblik kućišta: Rack Mount, 1 RU

• dimenzije (V × Š × D): 44.45 × 432 × 254 mm

• težina: 6,5 kg

• napajanje: 100 – 240 V AC, 50/60 Hz

• potrošnja energije: 145 W (prosjek) / 175 W (maks.)

• otpornost na toplinu: 597.12 BTU/h

• redundantno napajanje: Da (dualno AC napajanje, 1+1 redundancija)

• radna temperatura: 0 °C do 40 °C

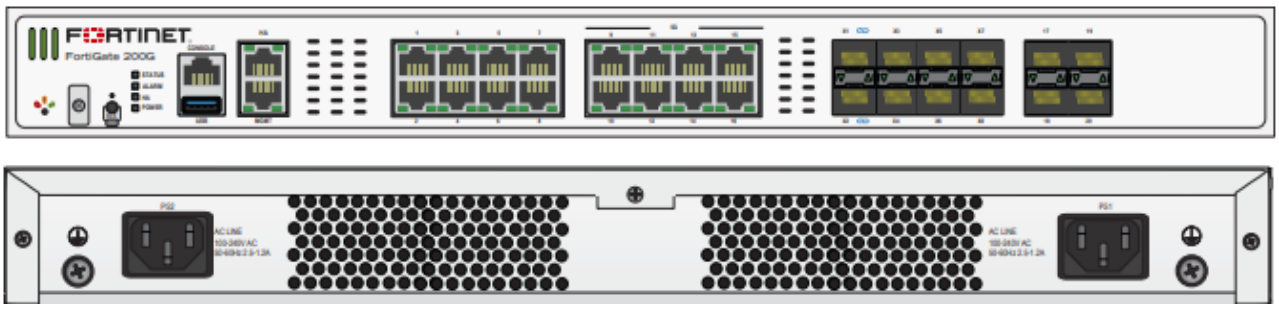
• skladišna temperatura: –35 °C do 70 °C

• vlažnost: 5 % – 90 % (bez kondenzacije)

• razina buke: 48 dBA

• maksimalna radna visina: 3.048 m (10.000 ft)

• certifikati: FCC Part 15 Class A, CE, RCM, VCCI, UL/cUL, CB, USGv6/IPv6



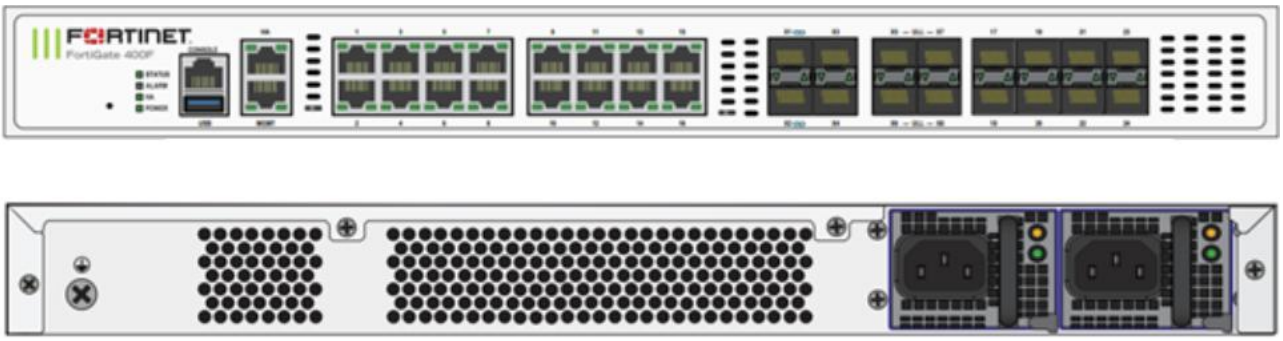
Slika 18. FortiGate 200G

FortiGate 400F je uređaj nove generacije vatrozida (NGFW) namijenjen srednje velikim do velikim ustanovama koje zahtijevaju visoku mrežnu propusnost, naprednu segmentaciju i snažne sigurnosne funkcionalnosti. Zahvaljujući Fortinet SPU arhitekturi i integriranim AI/ML

sigurnosnim servisima 400F model omogućuje pouzdanu zaštitu bez kompromisa u performansama.

Tehničke značajke:

- IPS propusnost: 12 Gbps
- NGFW propusnost: 10 Gbps
- propusnost zaštite od prijetnji (Threat Protection): 9 Gbps
- IPv4 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 79,5 / 78,5 / 70 Gbps
- IPv6 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 79,5 / 78,5 / 70 Gbps
- Firewall latencija (64 bajta, UDP): 4,19 µs / 2,5 µs*
- Firewall performanse (paketa u sekundi): 105 Mpps
- maksimalan broj istovremenih sesija (TCP): 7,8 milijuna
- nove sesije u sekundi (TCP): 500.000
- Firewall pravila: 10.000
- IPsec VPN propusnost (512 bajta): 55 Gbps
- maksimalan broj VPN tunela:
    - Gateway-to-Gateway: 2.000
    - Client-to-Gateway: 50.000
- SSL-VPN propusnost: 3,6 Gbps
- maksimalan broj SSL-VPN korisnika: 5.000
- SSL inspekcija (prosjek HTTPS): 8 Gbps
- SSL inspekcija CPS: 6.000
- maksimalne SSL inspekcijske sesije: 800.000
- propusnost kontrole aplikacija (HTTP 64K): 28 Gbps
- CAPWAP propusnost: 65 Gbps
- virtualne domene (VDOMs): 10 (zadano) / 25 (maksimalno)
- maksimalan broj FortiSwitch uređaja: 96 (uz FortiOS 7.6.1+, inače 72)
- maksimalan broj FortiAP uređaja: 512 (ukupno) / 256 (tunelirani)
- maksimalan broj FortiToken uređaja: 5.000
- visoka dostupnost: Active-Active, Active-Passive, Clustering.



Slika 19. FortiGate 400F

Fizička sučelja:

- GE RJ45 portovi: 16
- GE RJ45 upravljački / HA portovi: 2
- GE SFP portovi: 8
- 10 GE SFP+ portovi: 4
- 10 GE SFP+ ultra-low latency portovi: 4
- USB port: 1
- konzolni port: 1
- ugrađeno spremište:
    - FG-400F: bez diska

Ostale značajke:

- oblik kućišta: Rack Mount, 1 RU
- dimenzije (V x Š x D): 44,45 x 432 x 380 mm
- težina:
    - FG-400F: 6,4 kg
- napajanje:
    - AC: 100 – 240 V, 50/60 Hz
    - DC: 48 – 60 VDC (ovisno o modelu)
- potrošnja energije:
    - FG-400F: 154,8 W (prosjek) / 189,2 W (maks.)
- otpornost na toplinu: 645 – 672 BTU/h
- redundantno napajanje: Da (hot-swappable dual PSU)

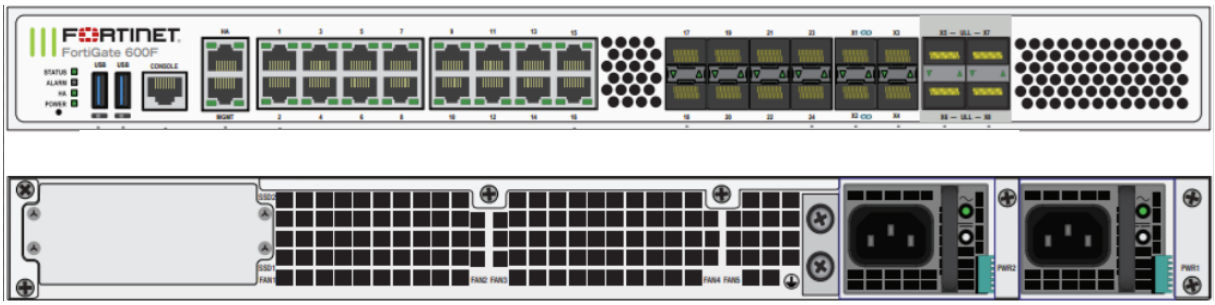
- radna temperatura: 0 °C do 40 °C
- skladišna temperatura: –35 °C do 70 °C
- vlažnost: 5 % do 90 % (bez kondenzacije)
- razina buke: LPA 48 dBA / LWA 55 dBA
- protok zraka: bočno i sprijeda prema natrag
- maksimalna radna visina: 3.048 m (10.000 ft)
- certifikati: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, USGv6/IPv6.

FortiGate 600F je visoko performansni uređaj nove generacije vatrozida (NGFW) namijenjen velikim ustanovama i okruženjima s intenzivnim mrežnim prometom. Opremljen je naprednim sigurnosnim funkcijama temeljenima na umjetnoj inteligenciji, s podrškom za segmentaciju, SSL inspekciju i centralizirano upravljanje.

Tehničke značajke:

- IPS propusnost: 14 Gbps
- NGFW propusnost: 11 Gbps
- propusnost zaštite od prijetnji (Threat Protection): 9 Gbps
- IPv4 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 155 / 155 / 100 Gbps
- IPv6 Firewall propusnost (UDP, 1518 / 512 / 64 bajta): 155 / 155 / 100 Gbps
- Firewall latencija (64 bajta, UDP): 2.1 µs
- Firewall performanse (paketa u sekundi): 150 Mpps
- maksimalan broj istovremenih sesija (TCP): 15 milijuna
- nove sesije u sekundi (TCP): 500.000
- Firewall pravila: 100.000
- IPsec VPN propusnost (512 bajta): 135 Gbps
- maksimalan broj VPN tunela:
    - Gateway-to-Gateway: 20.000
    - Client-to-Gateway: 50.000
- SSL-VPN propusnost: 4,8 Gbps
- maksimalan broj SSL-VPN korisnika: 10.000
- SSL inspekcija (prosjek HTTPS): 9 Gbps
- SSL inspekcija CPS: 6.500
- maksimalne SSL inspekcijske sesije: 900.000
- propusnost kontrole aplikacija (HTTP 64K): 35 Gbps

- CAPWAP propusnost: 75 Gbps
- virtualne domene (VDOMs): 10 (zadano) / 500 (maksimalno)
- maksimalan broj FortiSwitch uređaja: 256
- maksimalan broj FortiAP uređaja: 1,024 (ukupno) / 512 (tunelirani)
- maksimalan broj FortiToken uređaja: 20.000
- visoka dostupnost: Active-Active, Active-Passive, Clustering.



Slika 20: FortiGate 600F

Fizička sučelja:

- GE RJ45 portovi: 16
- GE RJ45 upravljački / HA portovi: 2
- GE SFP portovi: 16
- 10 GE SFP+ portovi: 4
- 25 GE SFP28 portovi: 2
- USB port: 1
- konzolni port: 1
- ugrađeno spremište:
    - FG-600F: bez diska

Ostale značajke:

- oblik kućišta: Rack Mount, 2 RU
- dimenzije (V x Š x D): 88,1 x 432 x 480 mm
- težina:
    - FG-600F: 12,4 kg

- napajanje: 100 – 240 V AC, 50/60 Hz (dual hot-swappable PSU)
- potrošnja energije:
    - FG-600F: 200 W (prosjek) / 240 W (maks.)
- otpornost na toplinu: 820 – 850 BTU/h
- redundantno napajanje: Da (hot-swappable dual PSU)
- radna temperatura: 0 °C do 40 °C
- skladišna temperatura: –35 °C do 70 °C
- vlažnost: 10 % do 90 % (bez kondenzacije)
- razina buke: 58 dBA
- protok zraka: sprijeda prema natrag
- maksimalna radna visina: 3.048 m (10.000 ft)
- certifikati: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, USGv6/IPv6.

4.2.2. Konfiguracijske značajke

FortiGate uređaji podržavaju fleksibilnu i granularnu konfiguraciju sigurnosnih pravila, mrežnih servisa i upravljanja prometom. Konfiguracija se može provoditi preko mrežnog sučelja (FortiGate GUI), komandne linije (CLI) te centralizirano preko uređaja FortiManager. U nastavku su navedene konfiguracijske mogućnosti koje su važne za implementaciju u okruženju e-Sveučilišta.

1. Sigurnosna pravila vatrozida (engl. *Firewall policies*)

- Moguće je definirati detaljna pravila na temelju izvorišne i odredišne adrese, portova, protokola, korisnika, aplikacija i vremenskih rasporeda.
- Pravila mogu uključivati dodatne sigurnosne profile (npr. antivirus, web filtering, IPS).
- Pravila se mogu grupirati i organizirati po zonama, interfaceima ili VDOM-ovima.

2. Zone i segmentacija

- FortiGate omogućuje definiranje sigurnosnih zona za logičku podjelu mrežnih segmenata.
- Podržana je VLAN segmentacija i virtualne domene (VDOMs) za dodatnu fleksibilnost i izolaciju mrežnih servisa.

3. NAT (engl. *Network Address Translation*)

- Podrška za SNAT i DNAT pravila za upravljanje prijevodom adresa i portova.

- Mogućnost automatskoga i ručnog dodjeljivanja javnih IP adresa korisnicima ili servisima.

4. Usluge inspekcije i filtriranja
   - Konfiguracija inspekcije prometa preko IPS-a, antivirusnih filtera, mrežnog i aplikacijskog filtra.
   - Pojedinačne funkcije mogu se dodavati prema pravilima prometa (*policy-based*).
   - SSL/TLS inspekcija omogućuje pregledavanje šifriranog prometa bez ugrožavanja sigurnosti.

5. Upravljanje pristupom i autentikacija
   - Integracija s lokalnim korisničkim bazama, LDAP/Active Directory ili RADIUS poslužiteljima.
   - Mogućnost implementacije ZTNA pravila za kontrolirani pristup aplikacijama.

6. VPN konfiguracija
   - Podrška za IPsec i SSL VPN konfiguraciju u klijentskom i *site-to-site* načinu.
   - Mogućnost definiranja pravila prema korisnicima, grupama ili aplikacijama.
   - VPN konfiguracija može uključivati segmentaciju i ograničavanje propusnosti.

7. Visoka dostupnost (HA)
   - FortiGate podržava HA konfiguraciju u aktivno-aktivnom ili aktivno-pasivnom načinu.
   - Konfiguracija uključuje sinkronizaciju konfiguracije, *failover* mehanizme i *load balancing*.

FortiGate konfiguracijske značajke omogućuju izradu detaljno definiranih, kontekstualnih sigurnosnih pravila koja odgovaraju različitim vrstama prometa i korisničkim scenarijima u ustanovama visokog obrazovanja.

4.3. WAN mreža

U ovom su poglavlju opisani mrežni usmjerivač i virtualni LAN-ovi. Mrežno rješenje izvedeno je tako da je na dijelu lokacija mrežni usmjerivač i vatrozid jedan uređaj. Dio ustanova implementirane su preko usmjerivača te nemaju FortiGate vatrozid u svojoj topologiji kao vatrozid i kao usmjerivač, već samo kao usmjerivač koji sav promet tunelira do matične lokacije gdje se odrađuje sigurnosna inspekcija. Glavna uloga usmjerivača je povezivanje lokacija na centralni vatrozid kako bi se osigurala napredna sigurnost toka prometa, a uz navedeno usmjerivač ima funkciju redundancije u slučaju prekida mrežne povezanosti prema centralnom vatrozidu.

4.3.1. Mrežni usmjerivač

Mrežni usmjerivač omogućuje prijenos podataka između mreža, prilagođavajući pritom podatke za prijenos iz jednog sustava u drugi.

Osnovni zadatak koji usmjerivači obavljaju jest provjera odredišne IP adrese za svaki paket koji pristigne na neko od mrežnih sučelja na usmjerivaču, pronalazak njegova potrebnog preusmjeravanja u tablici usmjeravanja i prosljeđivanje paketa na odgovarajuće sučelje.

U sklopu implementiranoga mrežnog rješenja na sveučilištima ulogu mrežnog usmjerivača imaju uređaji **FortiGate 90G, FortiGate 100F, FortiGate 200F i FortiGate 200G**. Navedeni usmjerivači omogućuju povezivanje LAN mreže sveučilišta na okosnicu CARNET-ove mreže i tako čine granicu između LAN mreže sveučilišta i CARNET-ove mreže. Usmjerivači se na mrežu povezuju preko tzv. WAN sučelja koje je izravno povezano na CARNET-ov usmjerivač CPE. WAN sučelje usmjerivača konfigurirano je s IP adresom iz CARNET-ove mreže. Ako na lokaciji nema CARNET CPE-a – lokalni spoj s usmjerivača ostvaruje se vezom do nositelja linka, na čijoj se lokaciji nalazi CARNET-ov CPE.

Mrežni usmjerivači implementirani su na istoj opremi koja se koristi za vatrozid. Razlika je u njihovoj ulozi na pojedinoj lokaciji. Na lokaciji nositelja linka, odnosno matičnoj lokaciji provode se filtriranje prometa i sigurnosne inspekcije. Na udaljenim lokacijama provodi se usmjeravanje prometa prema matičnoj ustanovi, a u slučaju prekida mrežne povezanosti s matičnom lokacijom promet se usmjerava prema CARNET CPE-u kako bi rad lokacije bio neometan.

FortiGate uređaji kao L3 uređaji koriste iste funkcionalnosti usmjeravanja kao i vatrozidi, samo bez dodatnih inspekcijskih koraka, a zbog specifičnosti implementacije koriste se i za podizanje IPSEC VPN tunela prema matičnim lokacijama, odnosno nositeljima linka. Budući da je riječ primarno o vatrozidima, osigurava se integritet podataka i njihova sigurnost zbog ugrađenih funkcionalnosti u uređaju.

4.3.2. Konfiguracijske značajke sustava

Sustav radi tako da su udaljene lokacije povezane s matičnom lokacijom *site-to-site* IPsec tunelima i time imaju središnju točku za izlaz na internet (usmjerivač nema NextGen

funkcionalnosti ili licencije, dok vatrozid ima). Kako se ne bi koristili dvostruki NAT-ovi, svaka lokacija ima zasebne subnete i VLAN-ove za servise koji će biti pretkonfigurirani na svakoj lokaciji. Raspon IP adresa ovisi o dogovoru s CARNET-ovim inženjerom.

VLAN ID	Naziv VLAN-a
1110	MGMT
1111	eduroam
1112	gosti
1113	servis1
1114	servis2
1115	servis3
4094	fortilink

Tablica 2. VLAN ID i naziv

Namjene pojedinačnih VLAN-ova su sljedeće:

- VLAN 1110 je *management* VLAN i služi za upravljanje bežičnim pristupnim točkama
- VLAN 1111 je *eduroam* VLAN i služi za povezivanje studenata, djelatnika i posjetitelja sveučilišta koji na svojem uređaju imaju dostupnu mrežu *eduroam*
- VLAN 1112 je *gosti* VLAN i služi za povezivanje gostiju na bežičnu mrežu *gosti*
- VLAN-ovi 1113,1114 i 1115 su *servis* VLAN-ovi i služe za povezivanje i logičko odvajanje dodatnih servisa ako na lokaciji postoji potreba za odvajanjem resursa od ostatka postojeće mreže
- VLAN 4094 je *FortiLink VLAN i* služi za komunikaciju između uređaja Fortinet (usmjerivač i preklopnik komuniciranju preko protokola FortiLink).

Matična lokacija označena je prefiksom *M* u nazivu VLAN-a, a udaljena prefiksom *U*. Također VLAN-ovi koji pripadaju udaljenoj lokaciji imaju ID uvećan za 10 u odnosu na VLAN matične lokacije. Pristup svim potrebnim resursima omogućen je povezivanjem vatrozida ili usmjerivača Fortinet i CARNET-ovog CPE-a.

4.4. LAN mreža

U ovom su poglavlju opisani mrežni preklopnici i njihove konfiguracijske značajke.

Uloga mrežnih preklopnika je povezivanje uređaja na mrežnu infrastrukturu u pristupnom sloju mreže i međusobno povezivanje udaljenih mrežnih ormara optičkim i bakrenim vezama.

Osim toga, uloga preklopnika je logičko razdvajanje mrežnih segmenata u zasebne domene, odnosno VLAN-ove, u svrhu optimizacije i primjene sigurnosnih pravila za pojedine segmente. Ovakav model implementacije ustaljena je praksa u mrežama i integracijama ovakve složenosti.

Ovisno o veličini sveučilišta i načinu izvedbe pasivne infrastrukture, na pojedina sveučilišta instalirana je optimalna kombinacija modela i broja preklopnika čiji ukupan broj sučelja optimalno prati i broj priključaka na segmentu pasivne mrežne opreme.

Oprema je podijeljena na dvije grupe, klasični preklopnici i agregacijski uređaji. Agregacijski uređaji uz ulogu klasičnih preklopnika odrađuju agregiranje linkova na jednome mjestu kako bi omogućili adekvatan kapacitet preklapanja za svaku mikrolokaciju na području ustanove te omogućili implementaciju mreže u jednoj točki. Uređaji su Cisco C9300X serije, a ovisno o broju veza koje se agregiraju implementirane su 12 ili 24 portne inačice uređaja.

U sklopu implementiranog mrežnog rješenja na sveučilištima, ulogu mrežnih preklopnika imaju uređaji Cisco Meraki i Cisco Catalyst. Implementirani su sljedeći modeli preklopnika:

- **Cisco MS130-8P**
- **Cisco MS130-24X**
- **Cisco MS130-48X**
- **Cisco C9300X-12Y**
- **Cisco C9300X-24Y.**

Preklopnik Cisco MS130-8P prikazan je na slici u nastavku.

Slika 21. Preklopnik Cisco MS130-8P

Preklopnik Cisco MS130-8P raspolaže s 8 GE (engl*. Gigabit Ethernet*) RJ45 sučelja koja imaju funkcionalnost PoE+ (engl. *Power Over Ethernet Plus*) i s 2 GE SFP sučelja. Maksimalna izlazna snaga (engl. *PoE Output Limit*) na razini preklopnika je 120 W (engl. *Watt*).

Preklopnik Cisco MS130-24X prikazan je na slici u nastavku.

Slika 22. Preklopnik Cisco MS130-24X

Preklopnik Cisco MS130-24X raspolaže s 18 GE (engl*. Gigabit Ethernet*) RJ45 sučelja koja imaju funkcionalnost PoE+ (engl. *Power Over Ethernet Plus*), 6 mGE (engl*. Multi Gigabit Ethernet*) RJ45 sučelja koja imaju funkcionalnost PoE+ (engl. *Power Over Ethernet Plus*) i s 4 10GE SFP+ sučelja. Maksimalna izlazna snaga (engl. *PoE Output Limit*) na razini preklopnika je 370 W (engl. *Watt*).

Preklopnik Cisco MS130-48X prikazan je na slici u nastavku.

Slika 23. Preklopnik Cisco MS130-48X

Preklopnik Cisco MS130-24X raspolaže s 40 GE (engl*. Gigabit Ethernet*) RJ45 sučelja koja imaju funkcionalnost PoE+ (engl. *Power Over Ethernet Plus*), 8 mGE (engl*. Multi Gigabit Ethernet*) RJ45 sučelja koja imaju funkcionalnost PoE+ (engl. *Power Over Ethernet Plus*) i s 4 10GE SFP+ sučelja. Maksimalna izlazna snaga (engl. *PoE Output Limit*) na razini preklopnika je 740 W (engl. *Watt*).

Preklopnik Cisco C9300X-12Y prikazan je na slici u nastavku.

Slika 24. Preklopnik Cisco C9300X-12Y

Preklopnik Cisco C9300X-12Y raspolaže s 12 1/10/25 G (engl. *Gigabit*) SFP28 sučelja i kapacitet preklapanja od 1000Gbps (engl. *Gigabit per second)*.

Preklopnik Cisco C9300X-24Y prikazan je na slici u nastavku.

Slika 25. Preklopnik Cisco C9300X-24Y

Preklopnik Cisco C9300X-12Y raspolaže s 12 1/10/25 G (engl. *Gigabit*) SFP28 sučelja i kapacitet preklapanja od 2000Gbps (engl. *Gigabit per second)*.

Preklopnici Cisco Meraki u sklopu implementiranog mrežnog rješenja imaju sljedeće funkcionalnosti:

- centralizirano upravljanje s pomoću sustava za nadzor i upravljanje mrežom
- tzv. instalaciju uređaja *zero-touch* bez postavljanja početne konfiguracije s pomoću sustava za nadzor i upravljanje mrežom
- segmentaciju mreže na više virtualnih mreža – VLAN-ova
- funkcionalnost STP (engl. *Spanning Tree Protocol*)
- prihvat korisničkih računala i bežičnih pristupnih točaka
- sigurnosne mogućnosti
- napajanje za spajanje bežičnih pristupnih točaka na sučeljima preklopnika.

Preklopnici unutar ormara BD povezani su izravno na usmjerivač ili vatrozid. Svi preklopnici unutar jednog ormara FD povezani su na jedan preklopnik unutar ormara.

Veze između ormara BD i FD realizirane su s pomoću optičkih veza:

- višemodnih optičkih modula (FN-TRAN-SX, FN-TRAN-SFP+SR, MA-SFP-1GB-SX, MA-SFP-10GB-SR, GLC-SX-MMD=, SFP-10G-SR-S=) ili
- jednomodnih optičkih modula FN-TRAN-LX, FN-TRAN-SFP+LR, MA-SFP-1GB-LX10, MA-SFP-10GB-LR, GLC-LH-SMD=, SFP-10G-LR-S=).

Višemodni optički modul **FN-TRAN-SX** prikazan je na slici u nastavku.

Slika 26. Višemodni optički modul FN-TRAN-SX

Jednomodni optički modul **FN-TRAN-LX** prikazan je na slici u nastavku.

Slika 27. Jednomodni optički modul FN-TRAN-LX

Višemodni optički modul FN-TRAN-SFP+SR prikazan je na slici u nastavku.

Slika 28. Višemodni optički modul FN-TRAN-SFP+SR

Jednomodni optički modul FN-TRAN-SFP+LR prikazan je na slici u nastavku.

Slika 29. Jednomodni optički modul FN-TRAN-SFP+LR

Višemodni optički modul MA-SFP-1GB-SX prikazan je na slici u nastavku.

Slika 30. Jednomodni optički modul MA-SFP-1GB-SX

Višemodni optički modul MA-SFP-10GB-SR prikazan je na slici u nastavku.

Slika 31. Jednomodni optički modul MA-SFP-10GB-SR

Višemodni optički modul GLC-SX-MMD= prikazan je na slici u nastavku.

Slika 32. Jednomodni optički modul GLC-SX-MMD=

Višemodni optički modul SFP-10G-SR-S= prikazan je na slici u nastavku.

Slika 33. Jednomodni optički modul SFP-10G-SR-S=

Jednomodni optički modul MA-SFP-1GB-LX10 prikazan je na slici u nastavku.

Slika 34. Jednomodni optički modul MA-SFP-1GB-LX10

Jednomodni optički modul MA-SFP-10GB-LR prikazan je na slici u nastavku.

Slika 35. Jednomodni optički modul MA-SFP-10GB-LR

Jednomodni optički modul GLC-LH-SMD= prikazan je na slici u nastavku.

Slika 36. Jednomodni optički modul GLC-LH-SMD=

Jednomodni optički modul SFP-10G-LR-S= prikazan je na slici u nastavku.

Slika 37. Jednomodni optički modul SFP-10G-LR-S=

Osnovne konfiguracijske značajke mrežnih preklopnika navedene su u nastavku. Tablica 3 prikazuje virtualne LAN-ove (VLAN) koji se primjenjuju na preklopnicima.

VLAN ID	Naziv VLAN-a
1110	MGMT
1111	eduroam
1112	Gosti
1113	Servis1
1114	Servis2
1115	Servis3
4094	fortilink

Tablica 3. Popis i oznake VLAN-ova koji se primjenjuju na preklopnicima

Ovisno o potrebama na lokaciji, sučeljima na preklopnicima pridružuju se VLAN-ovi navedeni u tablici 3.

Integracija postojeće mreže sveučilišta s novom mrežnom opremom obavlja se preko sučelja na preklopniku. Sučelja su konfigurirana u pristupnom načinu rada (engl. *Access Mode*) i dodijeljen im je VLAN 1113/1114/1115. S pomoću ove mrežne integracije uređaji na postojećoj mreži dobivaju IP adrese od DHCP poslužitelja konfiguriranog na vatrozidu koji je središnja točka ugrađena na lokaciji nositelja linka.

Ako je na sučelje spojena bežična pristupna točka, tada je sučelje postavljeno u način rada koji dopušta propuštanje više VLAN-ova (engl. *Trunk Mode*), čime je omogućena komunikacija uređajima spojenima na bežične mreže (VLAN-ovi 1111 i 1112). Na sučeljima je omogućena i opcija PoE (engl. *Power Over Ethernet*) koja osigurava napajanje bežičnih pristupnih točaka preko pasivne mrežne infrastrukture.

4.5. Bežična mreža

U ovom su poglavlju opisane bežične pristupne točke i konfiguracijske značajke bežičnih mreža.

4.5.1. Bežične pristupne točke

Uloga pristupne točke je odašiljanje bežičnog signala za pristup mrežnoj infrastrukturi, a služi za pokrivanje prostora unutar sveučilišta bežičnim signalom. Na svakom sveučilištu instaliran je veći broj bežičnih pristupnih točaka, a implementirani sustav podržava mobilnost korisnika bez prekida u komunikaciji pri njihovu prijelazu s jedne na drugu bežičnu pristupnu točku. Raspored i montaža bežičnih pristupnih točaka obavljaju se u skladu s DIS-om pasivne mrežne infrastrukture sveučilišta.

U navedenom sustavu implementiran je model različitih bežičnih mreža (SSID – *engl*. *Service Set Identifier*) s različitim konfiguracijskim postavkama, načinima autentikacije i pravima pristupa spajanjem na pojedinačnu mrežu.

U sklopu implementiranoga mrežnog rješenja na sveučilištima ulogu bežične pristupne točke ima uređaj **Cisco MR36.**

U implementiranom rješenju bežične pristupne točke koriste funkcionalnost kontrolora za bežičnu mrežu u sklopu sustava za nadzor i upravljanje mrežom.

Bežična pristupna točka **Cisco MR36** prikazana je na slici u nastavku.

Slika 38. Bežična pristupna točka Cisco MR36

Bežična pristupna točka Cisco MR36 u sklopu implementiranoga mrežnog rješenja ima sljedeće funkcionalnosti:

- centralizirano upravljanje s pomoću sustava za nadzor i upravljanje mrežom
- tzv. instalaciju uređaja *zero-touch* bez postavljanja početne konfiguracije s pomoću sustava za nadzor i upravljanje mrežom
- podršku za standarde IEEE 802.11a/b/g/n/ac/ax
- istovremeni rad na frekvencijskom području od 2,4 GHz i 5 GHz
- podršku za 2x2 MU-MIMO tehnologiju radi boljeg upravljanja istovremenim vezama korisnika
- sigurnosne značajke koje uključuju autentikacijske mehanizme 802.1x i enkripciju AES

- autentikaciju korisnika na mrežu preko zaštitnog portala (engl. *Captive portal*) s integracijom imeničkih sustava
- mogućnost implementacije QoS mehanizama za osiguranje kvalitete usluge
- ograničavanje propusnosti po SSID-u i korisniku.

4.5.2. Konfiguracijske značajke sustava

Na svakom sveučilištu definirane su bežične mreže, odnosno SSID-a:

- **eduroam** – služi za povezivanje studenata, profesora i ostalog osoblja na bežičnu mrežu, odnosno za povezivanje uređaja kojim se u pravilu koristi samo jedna osoba
- **gosti** – služi za povezivanje gostiju na bežičnu mrežu *gosti.*

U nastavku su opisani konfiguracijski parametri svake navedene mreže.

Za pristup mreži **eduroam** primjenjuju se sljedeći parametri:

- autentikacija DOT11.X-RADIUS uz enkripciju podataka s 802.1X sa izborom postavke prilagođenog RADIUS-a
- za pristup mreži *eduroam* primjenjuje se protokol TTLS-PAP. Detaljnije se upute mogu naći na mrežnoj adresi installer.eduroam.hr
- za autentikaciju se primjenjuje sustav AAI@EduHr
- korisnici nakon pristupa mreži *eduroam* pripadaju u VLAN 1111 i imaju IP adresu iz mreže koja im je dodijeljena u dogovoru s CARNET-om
- pri pristupu na okosnicu CARNET-ove mreže u pretraživaču se otvara ***Captive* portal** za autentikaciju i ovdje je potrebno unijeti svoje **vjerodajnice za sustav AAI (korisničko ime u obliku „*ime.prezime@domena_sveučilišta.hr*“ i lozinku)**.

Upute za spajanje na bežičnu mrežu **eduroam**:

- Otvorite mrežni preglednik i posjetite službenu stranicu eduroam.hr/installer.
- Kliknite na gumb "Preuzimanje postavki"
- Prijavite se koristeći svoj **AAI@EduHr korisnički identitet** (korisnička oznaka, npr. `ime.prezime@ustanova.hr`, i lozinka) koji ste dobili od matične ustanove.
- Nakon prijave odaberite operacijski sustav koji koristite na svojem uređaju (Windows, macOS, Android, iOS itd.).
- Slijedite upute za preuzimanje i pokretanje instalacijskog programa (ili konfiguracijskog profila na mobilnim uređajima).
- Pokrenite instalaciju i potvrdite sve potrebne korake. Aplikacija će automatski postaviti potrebne mrežne postavke i certifikate.
- Nakon uspješne instalacije vaš bi se uređaj trebao automatski moći povezati na bežičnu mrežu pod nazivom **eduroam**.

Za pristup mreži **gosti** primjenjuju se sljedeći parametri:

- autentikacija s pomoću lozinke (postavljena u dogovoru sa sveučilištem) uz enkripciju podataka s WPA2
- za pristup mreži *gosti* primjenjuje se protokol TTLS-PAP
- korisnici nakon pristupa mreži *gosti* pripadaju u VLAN 1112 (*gosti*) ili VLAN 1113/1114/1115 (*servis*) i imaju IP adresu iz mreže koja im je dodijeljena u dogovoru s CARNET-om.

4.6. Sustav za upravljanje i nadzor vatrozida

Za potrebe centraliziranog upravljanja i nadzora FortiGate vatrozida u sklopu sustava e-Sveučilišta koristi se rješenje FortiManager. Ovaj sustav omogućuje jedinstveno mjesto za upravljanje sigurnosnim pravilima, praćenje konfiguracija i provođenje nadzora nad velikim brojem distribuiranih uređaja.

FortiManager pruža skalabilnost, konzistentnost i sigurnost centraliziranim upravljanjem koje znatno pojednostavnjuje administraciju velikih mrežnih sustava.

4.6.1. Tehničke značajke FortiManagera

FortiManager dostupan je kao fizički uređaj, virtualna instanca ili servis u oblaku. U kontekstu projekta e-Sveučilišta koristi se kao središnji alat za upravljanje svim FortiGate uređajima na razini mreže sveučilišta. U sustavu e-Sveučilišta koristi se *cloud* rješenje koje je dostupno na poveznici https://fmg.global.king-cloud.eu/ui/login/.

Tehničke značajke:

- podrška za tisuće FortiGate uređaja (ovisno o modelu)
- centralizirano upravljanje konfiguracijama, firmwareima i licencijama
- verzioniranje i revizija promjena konfiguracija
- distribucija sigurnosnih pravila (*policy package*)
- integracija s FortiAnalyzerom za naprednu analitiku i izvještavanje
- REST API podrška za automatizaciju
- podrška za višekorisnički rad i granularne razine pristupa.

4.6.2. Prednosti i mogućnosti FortiManager platforme

FortiManager omogućuje centralizirano i sveobuhvatno upravljanje FortiGate uređajima, pružajući administratorima snažan alat za standardizaciju, kontrolu i nadzor sigurnosne infrastrukture. U području upravljanja konfiguracijama FortiManager omogućuje izradu i primjenu predložaka koji se mogu distribuirati na velik broj uređaja, što uvelike

pojednostavnjuje administraciju i smanjuje mogućnost pogreške. Administratori mogu pregledavati razlike između konfiguracija, testirati nove postavke prije primjene i, prema potrebi, brzo izvršiti povrat *(*engl. *„rollback“)* na prethodnu verziju konfiguracije.

U segmentu upravljanja sigurnosnim pravilima FortiManager služi kao središnje mjesto za izradu, uređivanje i raspodjelu sigurnosnih pravila prema različitim lokacijama ili organizacijskim jedinicama. Upotrebom zajedničkih objekata i grupa olakšava se standardizacija pravila, a ugrađeni mehanizmi validacije omogućuju da se pravila primjenjuju dosljedno i bez konfiguracijskih grešaka.

FortiManager također pojednostavnjuje upravljanje uređajima. Uređaji se mogu registrirati, kategorizirati i grupirati prema različitim kriterijima, a sustav pruža detaljan uvid u njihov status, povezanost i verzije firmwarea. Centralizirano upravljanje ažuriranjima i sigurnosnim kopijama dodatno pridonosi učinkovitosti i sigurnosti.

Podrška za administrativne domene (ADOM) omogućuje logičku segmentaciju platforme, što je posebno korisno u većim organizacijama ili ustanovama koje zahtijevaju decentralizirano upravljanje. Svaka ADOM jedinica može imati vlastiti skup pravila, korisnika i uređaja, čime se osigurava fleksibilnost i jasnoća u upravljanju.

Također FortiManager ima važnu ulogu u kontinuitetu rada jer omogućuje čuvanje sigurnosnih kopija konfiguracija i brzo vraćanje sustava u prethodno stanje u slučaju incidenta. Dodatne mogućnosti poput replikacije i redundancije omogućuju pouzdanost i dostupnost sustava čak i u složenim mrežnim okruženjima.

FortiManager u sustavu e-Sveučilišta predstavlja okosnicu sigurnosnog nadzora, upravljanja i standardizacije konfiguracija za sve lokacije, omogućujući skalabilan i pouzdan rad cijele mrežne infrastrukture.

4.6.3. Tehničke značajke FortiAnalyzera

FortiAnalyzer je centralizirana platforma za prikupljanje, analizu i korelaciju logova iz Fortinet sigurnosnih uređaja. U sustavu e-Sveučilišta koristi se kao sustav za napredno izvještavanje, analitiku i forenzičko praćenje sigurnosnih događaja na razini cijele mrežne infrastrukture. Dostupan je kao fizički uređaj, virtualna instanca ili servis u oblaku. U sustavu e-Sveučilišta koristi se *cloud* rješenje dostupno na poveznici https://faz.global.king-cloud.eu.

Tehničke značajke:

• centralizirano prikupljanje i pohrana logova iz FortiGate, FortiManager, FortiAuthenticator i drugih Fortinet uređaja

• skalabilna arhitektura (od nekoliko stotina do više tisuća uređaja, ovisno o modelu)

• napredna analitika i vizualizacija sigurnosnih podataka

• korištenje FortiSOC modula za detekciju incidenata i odgovor (SIEM/UEBA mogućnosti)

• forenzička analiza prometa i sigurnosnih događaja

• izrada prilagođenih izvještaja i automatizirano slanje izvještaja

• integracija s FortiManagerom za objedinjeno upravljanje i izvještavanje
• podrška za REST API i automatizacijske procese
• podrška za višekorisnički rad i granularne razine pristupa
• redundantna i distribuirana pohrana za visoku dostupnost.

Pregled upravljačkih i analitičkih funkcionalnosti:
1. Prikupljanje i obrada logova
• prikupljanje svih vrsta logova (prometni, sigurnosni, sustavni, događaji)
• normalizacija i indeksiranje logova radi bržeg pretraživanja
• prikaz logova u realnom vremenu
• filtriranje i korelacija događaja

2. Analitika i izvještavanje
• korištenje predefiniranih i prilagođenih izvještaja za administratore i sigurnosne timove
• izrada grafikona, trendova i sigurnosnih statistika
• automatizirano generiranje i slanje izvještaja (dnevno, tjedno, mjesečno)
• analiza ponašanja korisnika i uređaja (UEBA – gdje je dostupno)

3. Upravljanje sigurnosnim incidentima (FortiSOC modul)
• detekcija prijetnji i anomalija s pomoću korelacije logova
• podrška za automatizirani odgovor na incidente (*playbooks*)
• upravljanje incidentima i evidencijom (*ticketing* funkcionalnost)
• integracija s vanjskim SIEM sustavima

4. Upravljanje uređajima i log-pohranom
• registracija uređaja i upravljanje log-retencijom
• prikaz statusa pohrane, zasićenosti i performansi
• replikacija logova i mogućnost arhiviranja
• kontrola integriteta logova za potrebe forenzike

5. Podrška za administrativne domene (ADOM)
• logička segmentacija sustava za različite fakultete, odjele ili ustanove
• svaka ADOM jedinica dobiva zasebne izvještaje, log-baze i analitičke postavke

• omogućuje decentraliziran pristup bez kompromitiranja sigurnosti

6. Uloga u kontinuitetu rada

• centralizirano arhiviranje logova kao dio planova kontinuiteta i forenzike
• mogućnost vraćanja logova i analitičkih podataka nakon incidenta
• redundantna pohrana i podrška za HA konfiguracije.

5. Vatrozidna infrastruktura e-Sveučilišta

Vatrozidna infrastruktura osnova je sigurnosne arhitekture projekta *e-Sveučilišta* jer osigurava zaštitu lokalnih mreža svih ustanova uključenih u sustav. Riječ je o distribuiranom, ali centralno upravljanom sustavu sigurnosnih uređaja (FortiGate) koji omogućuje potpunu kontrolu mrežnog prometa, zaštitu od vanjskih prijetnji, upravljanje pristupom i segmentaciju mreže.

Na svakoj lokaciji ustanova, matična ili udaljena, predviđena je implementacija jednog ili više FortiGate uređaja, ovisno o veličini, prometnom opterećenju i funkcionalnim potrebama ustanove. Sustav je dizajniran tako da omogućuje visoku razinu sigurnosti, skalabilnosti i pouzdanosti, pri čemu svi vatrozidi komuniciraju sa središnjim sustavom za upravljanje (FortiManager).

Vatrozidna infrastruktura obuhvaća sljedeće funkcionalne cjeline:

- filter prometa prema unaprijed definiranim sigurnosnim pravilima (*firewall policies*)
- segmentaciju mreže po logičkim i funkcionalnim cjelinama (VLAN, VDOM)
- VPN komunikaciju između udaljenih ustanova i matične ustanove
- praćenje i analizu prometa s pomoću FortiAnalyzera
- automatsko ažuriranje prijetnji s pomoću FortiGuard sigurnosnih servisa.

Korištenjem naprednih funkcionalnosti FortiGate uređaja i njihovom integracijom u Fortinet Security Fabric osigurava se dosljedna primjena sigurnosnih pravila na svim lokacijama, brza reakcija na incidente te jasno upravljanje pristupima i resursima.

U sljedećim poglavljima detaljno se opisuje način integracije FortiGate uređaja, sigurnosna pravila, NAT funkcionalnosti, nadzor te operativne i administrativne prakse koje omogućuju pouzdan rad i visoku razinu zaštite u okruženju digitalnog sveučilišta.

5.1. Uloga i važnost vatrozida u sustavu e-Sveučilišta

U sklopu projekta e-Sveučilišta vatrozidi imaju ulogu u uspostavi i održavanju sigurne, pouzdane i kontrolirane mrežne komunikacije između lokalnih sustava ustanova, međusobno povezanih lokacija i vanjskih mrežnih resursa, uključujući internet i oblake. Implementacija FortiGate uređaja omogućuje sveučilištima dosljednu provedbu sigurnosnih pravila u okruženju koje je vrlo dinamično i heterogeno.

5.2. Način integracije FortiGate uređaja u mrežnu topologiju sveučilišta

Integracija FortiGate uređaja u mrežnu topologiju sveučilišta izvedena je tako da osigura visoku razinu sigurnosti, dostupnosti i fleksibilnosti, uz mogućnost jednostavnog upravljanja i nadzora iz centralnog sustava. Uređaji su pozicionirani kao perimetarski sigurnosni čvorovi između unutarnjih mrežnih segmenata i vanjskih mreža, ali i između postojeće mreže ustanove i ostalih mreža.

Fortigate uređaj u osnovi dijeli mrežu na tri segmenta:

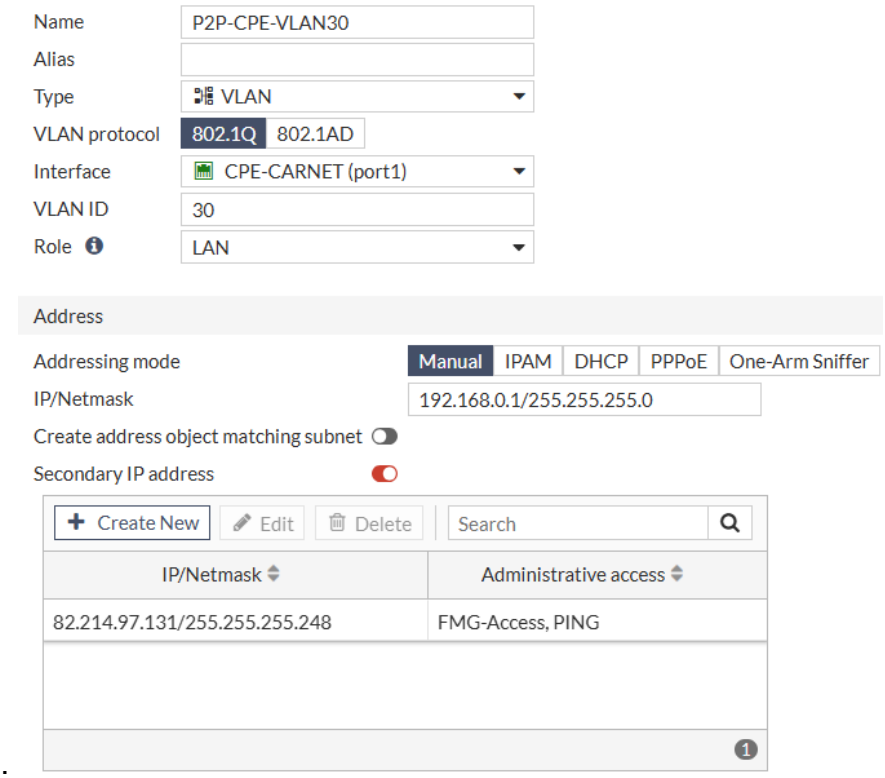
- vanjska mreža – spoj prema CARNET CPE
- naslijeđena mreža
- nova bežična mreža.

5.2.1. Spoj prema CARNET-ovoj mreži i internetu

FortiGate uređaj na sebi ima konfigurirane javne adrese te je poveznica s internetom i potrebnim servisima u sklopu projekta. Uređaji se na centralni sustav upravljanja (*FortiManager*) spajaju i predstavljaju s pomoću javne IP adrese.

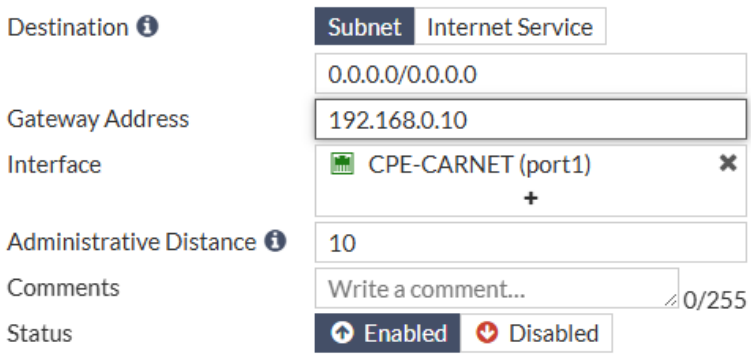
Komunikacija s CARNET-ovim CPE ostvaruje se preko fizičkog sučelja izravnim priključkom na CARNET-ov CPE. U slučajevima kada je veza realizirana optički, FortiGate uređaj koristi X1 sučelje s odgovarajućim SFP modulom. Ako se komunikacija uspostavlja UTP kabelom, povezivanje na FortiGate uređaju provodi se preko sučelja **port1**.

Mrežno sučelje FortiGate uređaja koje je povezano prema CARNET-ovom mrežnom sustavu konfigurirano je s VLAN oznakom 30. Na tom sučelju javna IP adresa nije primarna, već je dodijeljena kao sekundarna adresa, dok se osnovna komunikacija između FortiGate uređaja i CARNET-ova CPE-a odvija preko P2P (engl. *point-to-point*) veze čije IP adrese pripadaju privatnom rasponu.



Slika 39. Primjer konfiguracije P2P mrežnog sučelja

Na FortiGate uređaju namještena je statička zadana ruta 0.0.0.0/0.0.0.0 koja je usmjerena prema privatnoj adresi CARNET-ova mrežnog uređaja.



Slika 40. Primjer statički zadane rute

5.2.2. Spoj prema novoj bežičnoj mreži

FortiGate uređaj na matičnim je lokacijama s novom bežičnom mrežom povezan preko agregacijskog preklopnika optičkim prespojnim kabelom u port X2. Za sam spoj korišten je

10G višemodni SFP optički modul. Mrežno sučelje na FortiGateu postavljeno je u *trunk* način rada, pri čemu su izrađena potrebna VLAN L3 sučelja.

Samo fizičko sučelje postavljeno je kao unaprijed definirani upravljački VLAN (*default management* VLAN) te ujedno služi kao L3 sučelje za VLAN 1.

Dodatno su definirani sljedeći VLAN-ovi:

Rb.	VLAN ID	VLAN naziv	IP opseg	Namjena
1.	1110	M-MGMT	10.110.0.0/23	Upravljački VLAN
2.	1111	M-EDUROAM	10.111.0.0/20	Eduroam WiFi
3.	1112	M-GOSTI	10.112.0.0/23	Mreža za goste
4.	1113	M-SERVIS1	10.113.0.0/23	Dodatni servis 1
5.	1114	M-SERVIS2	10.114.0.0/23	Dodatni servis 2
6.	1115	M-SERVIS3	10.115.0.0/23	Dodatni servis 3

Tablica 4. Popis VLAN-ova na matičnoj lokaciji

Treba napomenuti da je tablica 4 popis VLAN-ova na matičnoj lokaciji te se oni razlikuju na udaljenim lokacijama. U tablici 5 je primjer M-EDUROAM mreže na udaljenim lokacijama.

Rb.	VLAN ID	VLAN naziv	IP opseg	Namjena
1.	1121	U1-EDUROAM	10.121.0.0/20	Eduroam WiFi
2.	1131	U2-EDUROAM	10.131.0.0/20	Eduroam WiFi
3.	1141	U3-EDUROAM	10.141.0.0/20	Eduroam WiFi

Tablica 5. Popis VLAN-ova na udaljenoj lokaciji

Istom logikom odrađeni su i drugi VLAN-ovi na udaljenim lokacijama. Podjela VLAN-ova u različite IP opsege izvedena je radi povezivanja udaljenih lokacija s matičnom lokacijom IPSEC tunela, što će poslije biti opisano. Svaki VLAN na lokaciji, bez obzira na to je li riječ o matičnoj ili udaljenoj lokaciji, ima definiran DHCP poslužitelj koji dodjeljuje IP adrese uređajima u zadanom VLAN-u.

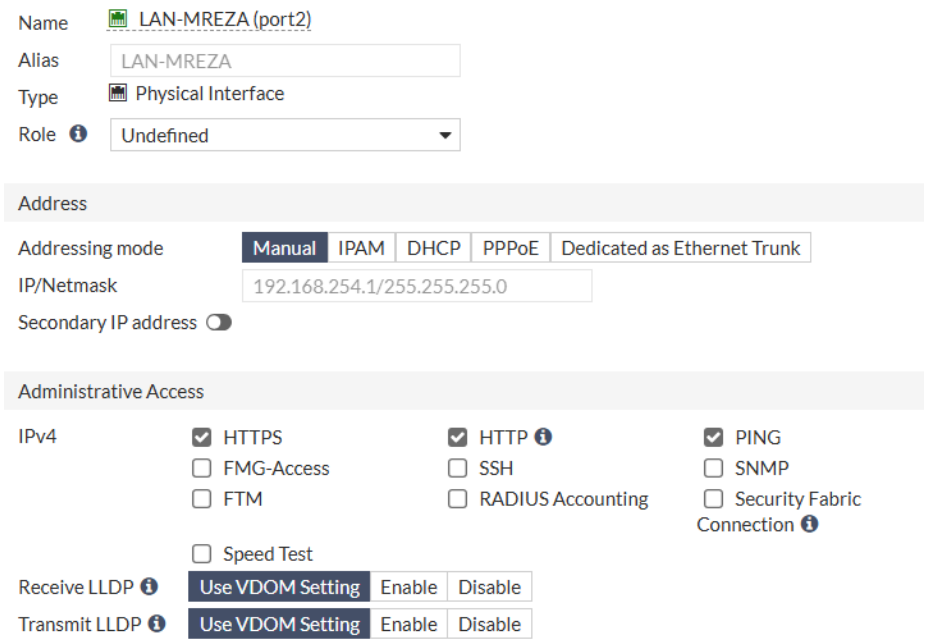
Rb.	VLAN ID	VLAN naziv	DHCP opseg	Namjena
1.	1110	M-MGMT	10.110.0.2-10.110.1.254	Upravljački VLAN
2.	1111	M-EDUROAM	10.111.0.21-10.111.15.254	Eduroam WiFi
3.	1112	M-GOSTI	10.112.0.21-10.112.1.254	Mreža za goste
4.	1113	M-SERVIS1	10.113.0.2-10.113.1.254	Dodatni servis 1

Tablica 6. Tablica raspodjele IP adresa DHCP-a

5.2.3. Spoj prema naslijeđenoj mreži

Ovisno o lokaciji i načinu dosadašnjeg spajanja naslijeđene mreže, spoj se provodi UTP mrežnim kabelom na FortiGate port2 mrežno sučelje, a ako se koristi optički prespojni kabel,

onda na mrežno sučelje port17. Neke lokacije zbog specifičnosti spoja mogu biti drukčije spojene.



Slika 41. Primjer konfiguracije mrežnog sučelja prema postojećoj mreži ustanove

Na mrežnom sučelju omogućuje se DHCP poslužitelj kako bi oprema ustanove mogla komunicirati s novoinstaliranim vatrozidom.

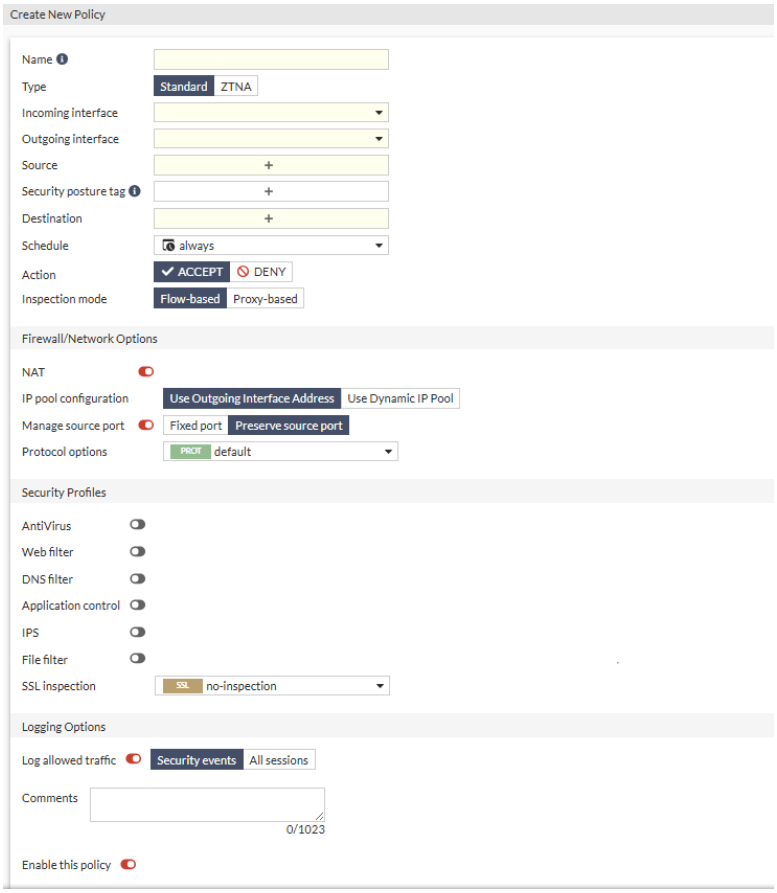
5.3. Sigurnosna pravila

Sigurnosna pravila (engl. *firewall policies*) definiraju način na koji FortiGate uređaj upravlja mrežnim prometom – dopuštanjem, odbijanjem ili inspekcijom – između različitih mrežnih zona. U kontekstu e-Sveučilišta, pravilno definirana i konzistentno primijenjena sigurnosna pravila ključna su za zaštitu korisnika, resursa i servisa u mreži.

Elementi sigurnosnih pravila

Svako sigurnosno pravilo u FortiGate uređaju uključuje sljedeće parametre:

- izvorišna zona i adresa (npr. LAN, VLAN studenti)
- odredišna zona i adresa (npr. internet, poslužitelji)
- protokol i portovi (npr. TCP/443, UDP/53)
- korisnici ili grupe korisnika
- sigurnosni profili – antivirus, *web filtering*, IPS, aplikacijska kontrola itd.
- akcija – *accept* ili *deny*.



Slika 42. Izrada sigurnosnih pravila

Pravila se evaluiraju sekvencijalno, od vrha prema dnu, što znači da njihov redoslijed izravno utječe na ponašanje uređaja. Zbog toga bi specifičnija pravila, primjerice izvorišta ili odredišta, trebala biti među prvima.

Inicijalne postavke sigurnosnih pravila u slučaju e-Sveučilišta definirana su tako da svaki VLAN unutar ustanove ima pravo pristupiti internetu po svim protokolima bez ograničenja.

Policy	From	To	Source	Service	Action	NAT	Security Profiles
LAN MREZA na INTERNET (1)	LAN-MREZA (port2)	P2P-CPE-VLAN30	OBJ_U3-LAN-MREZA	ALL	ACCEPT	NAT	SSL no-inspection
EDUROAM na INTERNET (2)	U3-EDUROAM	P2P-CPE-VLAN30	OBJ-U3-EDUROAM-VLAN1141	ALL	ACCEPT	NAT	SSL no-inspection
GOSTI na INTERNET (3)	U3-GOSTI	P2P-CPE-VLAN30	OBJ_U3-GOSTI-VLAN1142	ALL	ACCEPT	NAT	SSL no-inspection
MANAGEMENT na INTERNET (4)	U3-MGMT	P2P-CPE-VLAN30	OBJ_U3-MGMT-VLAN1140	ALL	ACCEPT	NAT	SSL no-inspection
SERVIS1 na INTERNET (5)	U3-SERVIS1	P2P-CPE-VLAN30	OBJ_U3-SERVIS1-VLAN1143	ALL	ACCEPT	NAT	SSL no-inspection
SERVIS2 na INTERNET (6)	U3-SERVIS2	P2P-CPE-VLAN30	OBJ_U3-SERVIS2-VLAN1144	ALL	ACCEPT	NAT	SSL no-inspection
SERVIS3 na INTERNET (7)	U3-SERVIS3	P2P-CPE-VLAN30	OBJ_U3-SERVIS3-VLAN1145	ALL	ACCEPT	NAT	SSL no-inspection
implicit_deny (0)	any	any	all	ALL	DENY		

Slika 43. Inicijalna sigurnosna pravila

5.4. NAT funkcionalnosti i segmentacija prometa

U kontekstu mrežne sigurnosti i kontrole pristupa, NAT (engl. *Network Address Translation*) i segmentacija prometa ključne su funkcionalnosti FortiGate uređaja. Omogućuju zaštitu unutarnje mreže, izolaciju različitih korisničkih skupina i kontrolu smjera komunikacije između mrežnih zona.

5.4.1. NAT funkcionalnosti

FortiGate podržava različite vrste NAT funkcionalnosti koje omogućuju:

- skrivanje privatnih IP adresa internih korisnika pri pristupu internetu (tzv. *source NAT*)
- usmjeravanje vanjskog prometa prema specifičnim unutarnjim servisima (tzv. *destination NAT* ili *port forwarding*)
- implementaciju više javnih IP adresa s različitim pravilima prevođenja
- automatsku ili ručnu dodjelu izlazne adrese, ovisno o scenariju i složenosti pravila.

NAT pravila mogu biti dio pravila vatrozida (tzv. *policy-based NAT*) ili se definiraju kao zasebni objekti u naprednijim konfiguracijama. NAT također omogućuje stvaranje virtualnih IP adresa (VIP) za objavu unutarnjih servisa prema vanjskom svijetu uz potpunu kontrolu pristupa i inspekciju prometa.

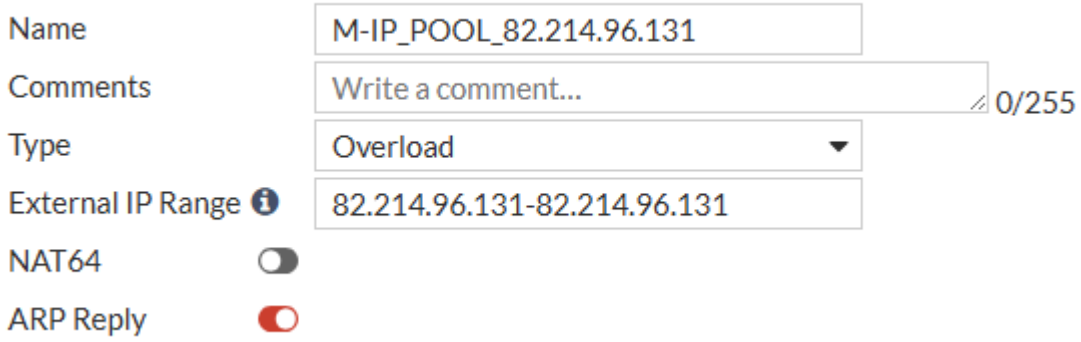
Na projektu e-Sveučilišta matične lokacije kontroliraju izlazni promet prema internetu, i za matičnu lokaciju i za udaljene lokacije, koje se s pomoću IPSEC-a spajaju na matičnu te tako ostvaruju pristup internetu.

Inicijalna konfiguracija vatrozida na, primjerice, matičnoj lokaciji NAT za pristup internetu provodi se s pomoću sigurnosnih pravila uz stvaranje bazena adresa (*pool*). Bazen adresa sadržava raspon javnih adresa kojima će se ustanova koristiti na internetu. Raspon javih adresa može biti više adresa koje se određuju pri kreiranju dinamičkog bazena IP adresa. Naravno, raspon može biti i jedna adresa, što je slučaj i na matičnim i na udaljenim lokacijama e-Sveučilišta. Javne adrese na matičnim lokacijama dodjeljuju se tako da svaka lokacija dobije dvije javne adrese. Dvije javne adrese dodjeljuju se matičnoj lokaciji, jedna za mreže Eduroam i MgMt, a druga za ostale mreže.

Prva udaljena lokacija (U1) dobiva sljedeće dvije javne adrese na korištenje istim principom dodjele kao i za matičnu lokaciju. Primjer je naveden u tablici.

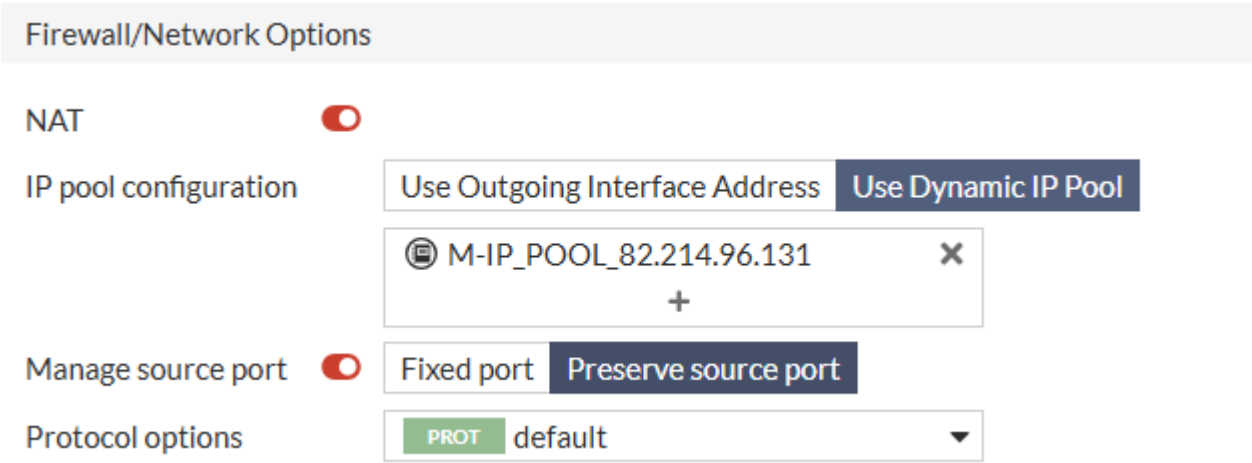
Lokacija	Eduroam i mgmt	Ostale mreže
Matična	82.214.96.131	82.214.96.132
Udaljena 1	82.214.96.133	82.214.96.134

Udaljena 2	82.214.96.135	82.214.96.136



Slika 44. Izrada bazena javnih adresa

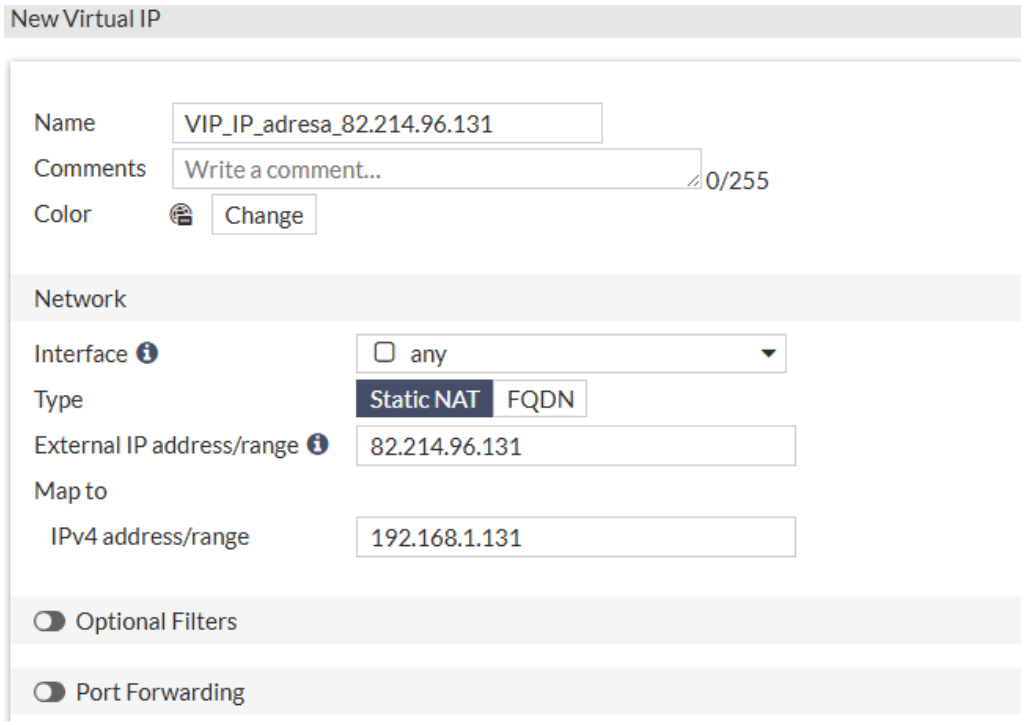
Na slici je prikazana izrada bazne javne adrese 82.214.96.131, koja se potom primjenjuje u sigurnosnim pravilima. Odabirom opcije *Use Dynamic IP pool* omogućuje se odabir prethodno izrađenog bazena adresa. Sav promet koji zadovoljava uvjete sigurnosnih pravila bit će preusmjeren na javnu adresu i proslijeđen odredištu.



Slika 45. Primjena bazena javnih adresa u sigurnosnim pravilima

Pri izradi odredišnog prevođenja adresa *(DNAT – destination NAT)* potrebno je kreirati virtualni IP objekt koji će se primijeniti u sigurnosnim pravilima. Ova konfiguracija primjenjuje se kada želimo da poslužitelj u mreži bude dostupan s interneta, kao i u nekim drugim slučajevima.

Potreban nam je objekt Virtual IPs koji će se primijeniti u sigurnosnim pravilima.



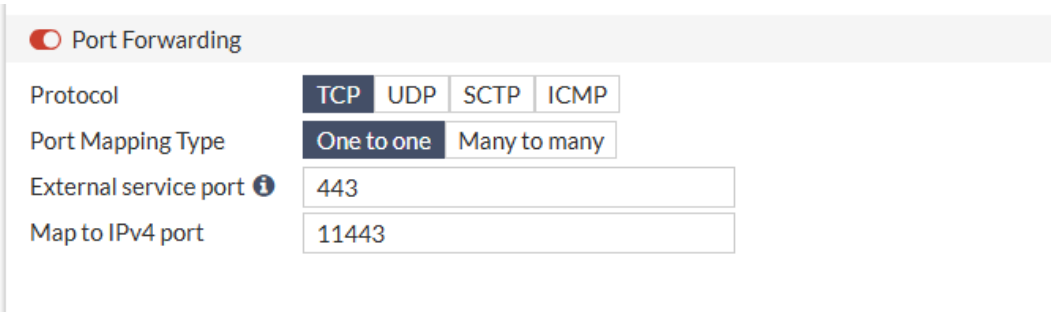
Slika 46. Izrada objekta virtualne IP adrese

Pri izradi objekta potrebno je obratiti pozornost na:

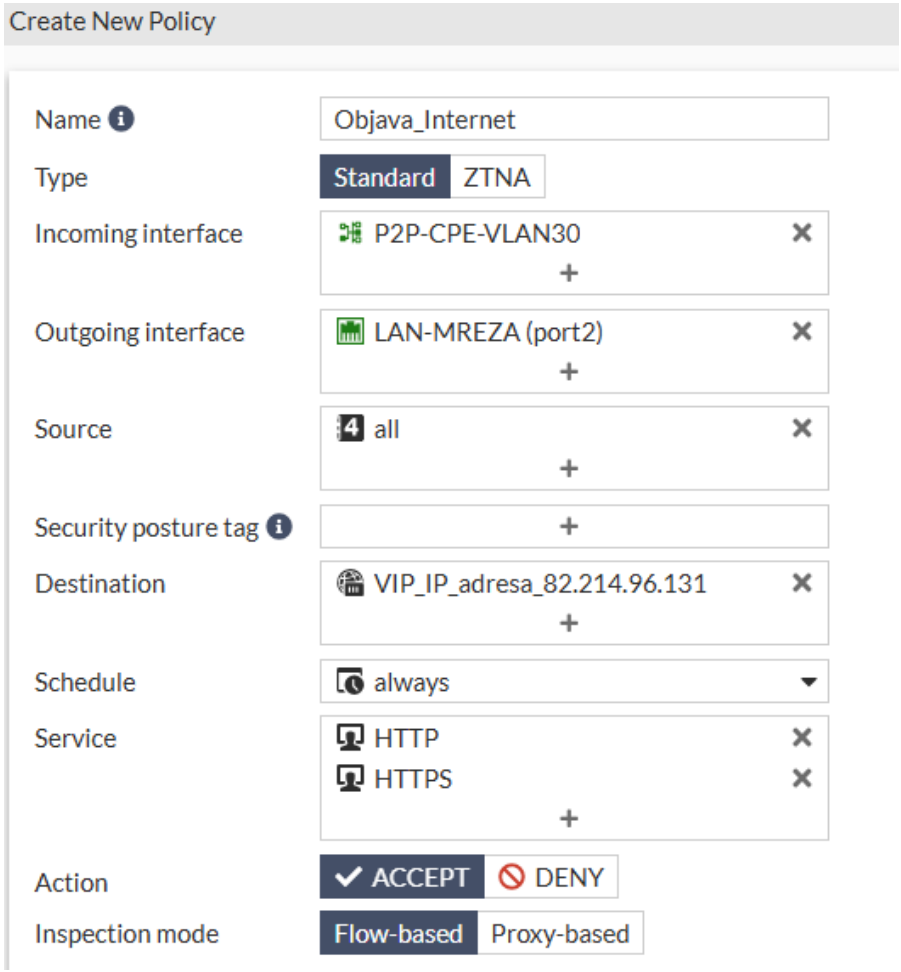
- External IP address/range – adresa koja će biti objavljena na internetu
- Map to – stvarna privatna adresa poslužitelja.

Kada se izradi Virtrual IPs objekt, treba ga primijeniti u sigurnosnim pravilima kako bi adresa bila dostupna s interneta.

Opcija Port Forwarding primjenjuje se kad se više servisa treba dodijeliti jednoj javnoj adresi na više različitih privatnih adresa, kao i kada se javni promet na jednom portu, primjerice 443, treba preusmjeriti na neki drugi port, primjerice 11443.



Slika 47. Primjer port forwardinga



Slika 48. Primjena objekta virtualne IP adrese

5.4.2. Segmentacija prometa

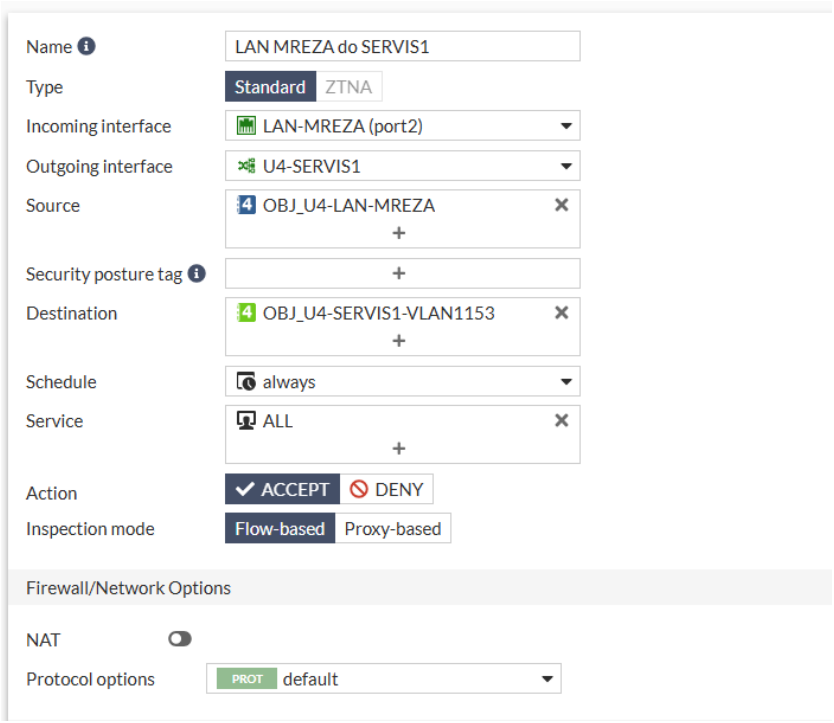
Segmentacija prometa omogućuje odvajanje mrežnih resursa i korisnika u logičke i sigurnosne zone kojima se može upravljati neovisno. FortiGate uređaji podržavaju:

- VLAN-ove – virtualne LAN-ove za fizičko odvajanje korisnika i servisa po portovima ili grupama uređaja
- zone (engl. *security zones*) – logičke cjeline koje grupiraju više sučelja sa sličnim pravilima
- virtualne domene (VDOMs) – potpuno izolirane logičke instance FortiGate uređaja s vlastitim konfiguracijama, korisnicima i pravilima
- segmentaciju prema funkcionalnosti (npr. nastava, administracija, serveri, gosti) i razini povjerenja.

Segmentacija omogućuje primjenu različitih sigurnosnih pravila za svaki mrežni segment te sprečava neželjeno kretanje prometa između korisničkih zona, čime se znatno povećava ukupna sigurnost sustava.

Inicijalna konfiguracija u sustavima e-Sveučilišta postavljena je tako da sprečava komunikaciju između različitih zona, VLAN-ova ili nekih drugih segmentiranih dijelova mreže. Pritom FortiGate uređaji ujedinjuju funkcionalnosti usmjeravanja, zaštite i logičke separacije, čime mrežna infrastruktura postaje sigurnija i otpornija na prijetnje.

U primjeru je prikazano propuštanje postojeće LAN mreže prema mreži SERVIS1.



Slika 49. Propuštanje komunikacije unutar privatne mreže

Sigurnosna pravila izrađuju se identično kao i u dosadašnjim primjerima. Od konfiguracije potrebno je odrediti:

- izvorišno sučelje
- odredišno sučelje
- objekt izvorišnog IP opsega ili jedne adrese
- objekt odredišnog IP opsega ili jedne adrese
- servis (http, https, dns…)
- akciju, *accept* ili *deny*.

Dodatno je važno isključiti NAT jer se komunikacija unutar privatne mreže ne mora prevoditi u javne adrese ni u neke druge.

5.5. Servisi na FortiGate uređaju

FortiGate uređaji, osim osnovnih funkcionalnosti vatrozida, integriraju niz naprednih sigurnosnih i mrežnih infrastrukturnih servisa, čime se omogućuje objedinjena kontrola prometa, sigurnosti i funkcionalnosti mreže iz jednog uređaja.

Sigurnosni servisi FortiGate uređaja koji se primjenjuju u sigurnosnim pravilima uključuju:

- **antivirus** – inspekcija sadržaja u realnom vremenu radi otkrivanja i blokiranja zlonamjernoga koda.
- **web filter** – kategorizacija i kontrola pristupa internetskim sadržajima.
- **DNS filter** – blokiranje pristupa zlonamjernim i neželjenim domenama na razini DNS-a.
- **Application control** – identifikacija i upravljanje mrežnim aplikacijama neovisno o portovima.
- **IPS** – zaštita od mrežnih prijetnji i pokušaja iskorištavanja ranjivosti.
- **File filter** – kontroliranje protoka različitih vrsta datoteka koje prolaze uređajem FortiGate.
- **SSL inspection** – inspekcija šifriranog prometa uz podršku za najnovije protokole.

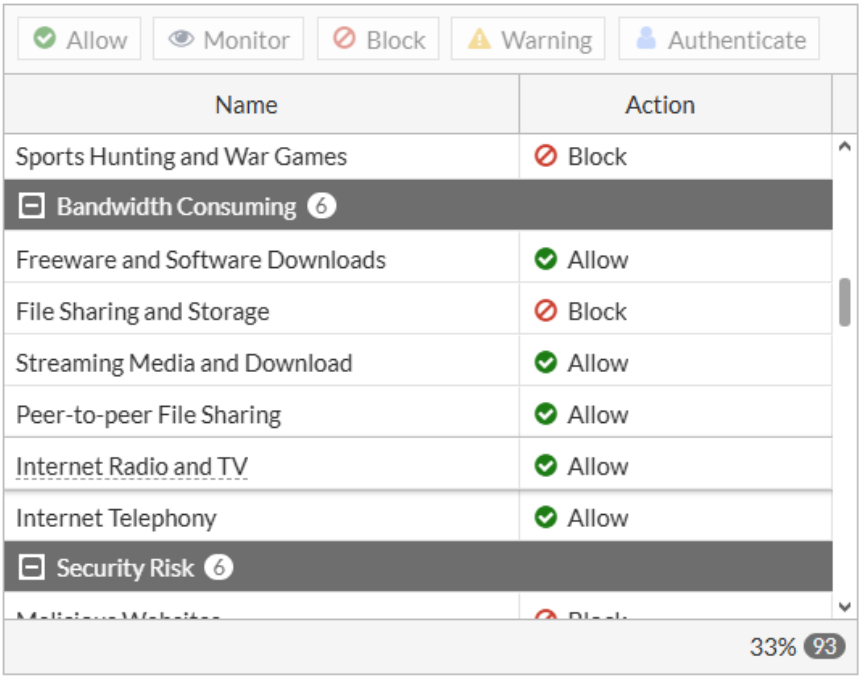
Svaki od navedenih sigurnosnih servisa ima unaprijed definirane profile koji se mogu odmah primijeniti u sigurnosnim pravilima. Naravno, svaki od profila može se kreirati i prilagoditi specifičnim potrebama.

5.5.1. Web filter

Izrada prilagođenoga sigurnosnog profila web filtera počinje kreiranjem novoga ili kloniranjem postojećega, koji se prilagođava vlastitim potrebama.

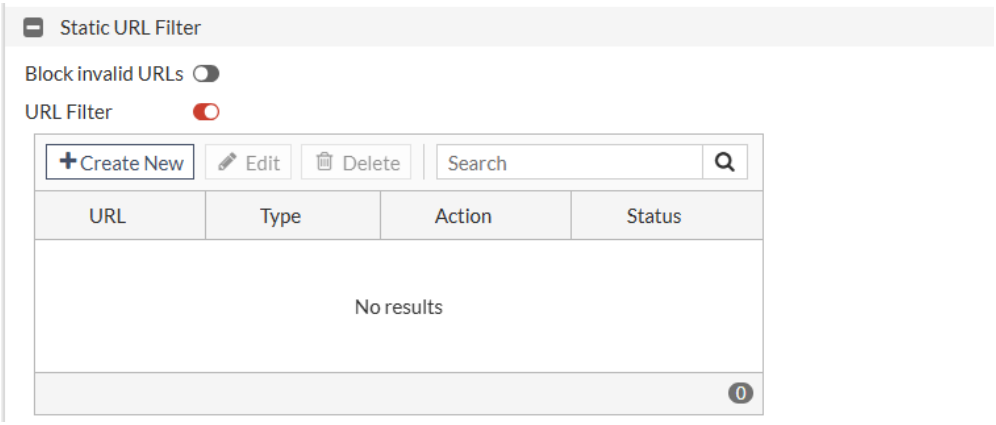
Svaki unaprijed definirani sigurnosni profil sadržava određene skupine mrežnog sadržaja razvrstane po kategorijama koje je odredio proizvođač vatrozida. Katkad se mogu pojaviti mrežni sadržaji koji su pogrešno kategorizirani, stoga je potrebno promijeniti kategoriju ili definirati iznimku. Osim pojedinačnih mrežnih stranica ista se pravila mogu primijeniti na cijelu kategoriju.

Na slici vidimo primjer promjene akcije na kategoriju *File Sharing and Storage* iz Allow u Block.



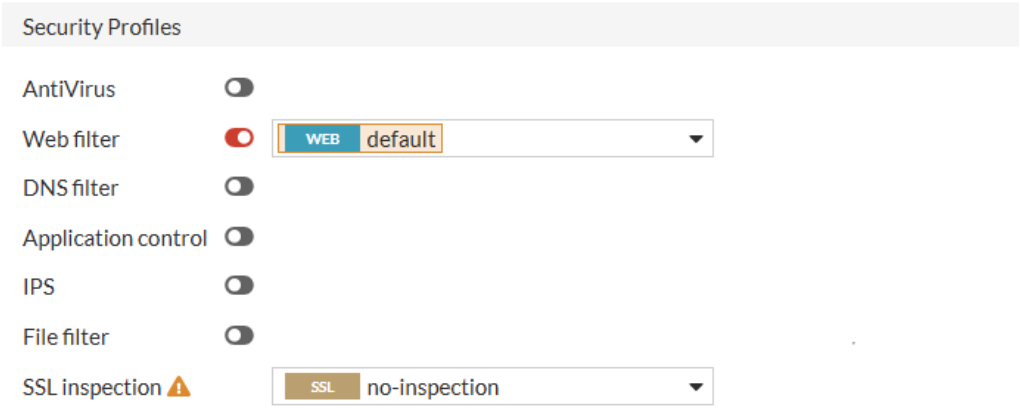
Slika 50. Promjena akcije na određenoj mrežnoj kategoriji

Web filter, kao i iznimke, mogu se definirati i za pojedinačne mrežne stranice u samom profilu. Odabirom opcije URL Filter te dodavanjem stranice na jedan od unaprijed definiranih načina unosom mrežne stranice možemo promijeniti akciju.



Slika 51. Statički unos mrežne stranice

Uređivanje sigurnosnih pravila te primjenjivanje upravo izrađene sigurnosnih pravila web filtera.



Slika 52. Primjena web filtera

Za primjenu web filtera preporučuje se SSL inspekcija kako bi se povećala mogućnost čitanja odredišnih mrežnih stranica u kriptiranom prometu.

5.5.2. DNS filter

U sigurnosnim pravilima možemo primijeniti filtriranje DNS kategorija za kontrolu pristupa korisnika *web*-resursima. Također možemo prilagoditi zadani profil ili stvoriti vlastiti za upravljanje pristupom mrežnih korisnika i primijeniti ga na pravila vatrozida.

Ako su u sigurnosnim pravilima konfigurirani web filter i DNS filter, DNS filter ima prednost, što znači da će sigurnosna pravila prvo pregledati DNS pravila pa potom WEB-ova.

DNS filter ima sljedeće značajke:

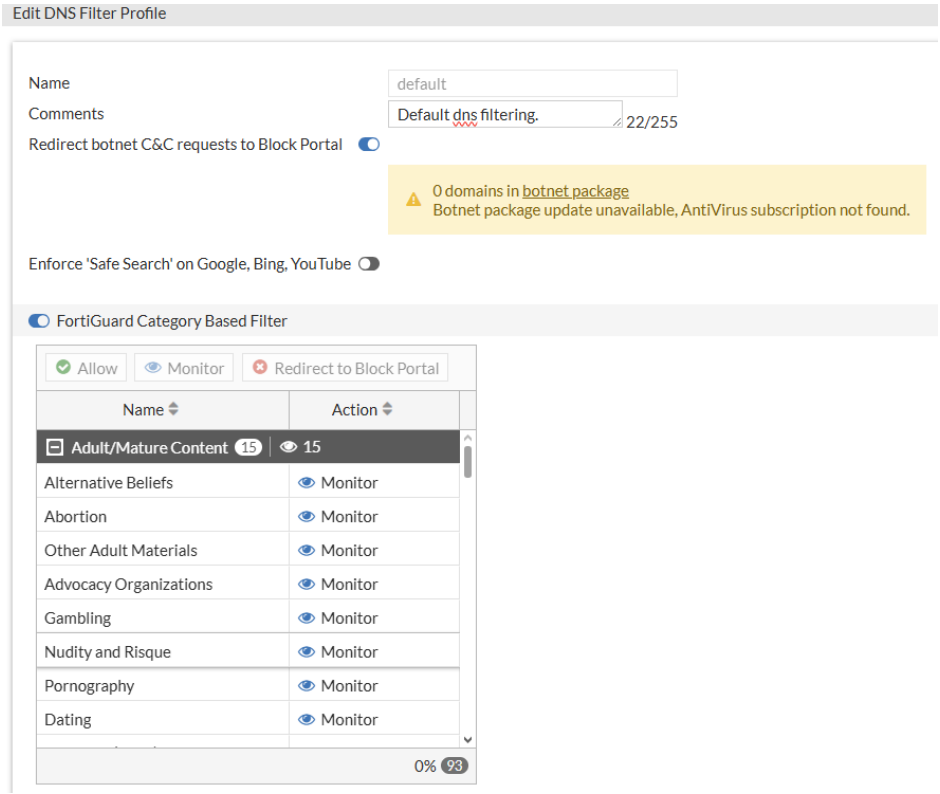
- FortiGuard filtriranje: filtrira DNS zahtjeve na temelju FortiGuard ocjene domene.
- Blokiranje C&C domene botneta: blokira DNS zahtjeve za poznate C&C domene botneta.
- Vanjsko dinamičko filtriranje domena kategorija: omogućuje nam definiranje vlastite kategorije domene.
- Sigurno pretraživanje DNS-a: provodi sigurne adrese Googlea, Binga i YouTubea za roditeljski nadzor.
- Filter lokalnih domena: omogućuje definiranje vlastitog popisa domena koje želite blokirati ili dopustiti.
- Popis blokiranih vanjskih IP adresa: omogućuje nam definiranje popisa blokiranih IP adresa za blokiranje razriješenih IP adresa koje odgovaraju ovom popisu.
- DNS prijevod: mapira riješeni rezultat na drugu IP adresu koju definirate.

Za izradu vlastitog DNS filter profila koriste se *clone* unaprijed definirana sigurnosna pravila DNS filtera, koja se potom prilagođavaju vlastitim potrebama.

Osim promjene akcija po kategorijama stranica, mogu se izraditi i statički filteri za određene domene te na njima primijeniti željene akcije.

Akcije u filterima dijele se na:

- Allow
- Monitor
- Redirect to Block Portal.

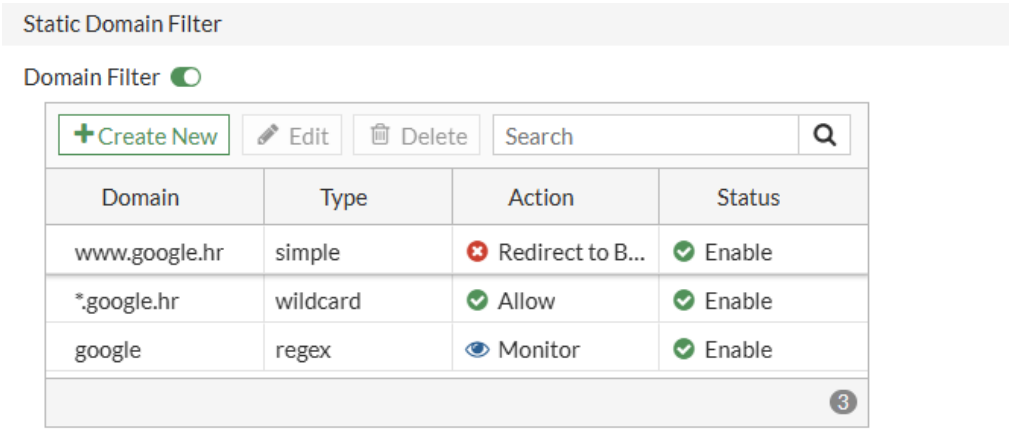


Slika 53. Uređivanje DNS filter profila

Statičkim filterom moguće je postaviti iznimku za pojedinu domenu na tri načina unosa:

- Simple
- Wildcard
- Regex.

Na slici su napisana sva tri načina za istu domenu.



Slika 54. Statički DNS filter

5.5.3. Kontrola aplikacije

FortiGate može prepoznati mrežni promet koji generira velik broj aplikacija. Senzori za kontrolu aplikacija određuju koje je radnje potrebno poduzeti s prometom aplikacije. Kontrola aplikacija koristi dekodere IPS protokola koji analiziraju mrežni promet kako bi otkrili promet aplikacije, čak i kad promet koristi nestandardne portove ili protokole.

Postoje već izrađeni filteri aplikacija koji se mogu koristiti ili klonirati i prilagoditi vlastitim potrebama. Na unaprijed definirane kategorije mogu se primijeniti četiri akcije:

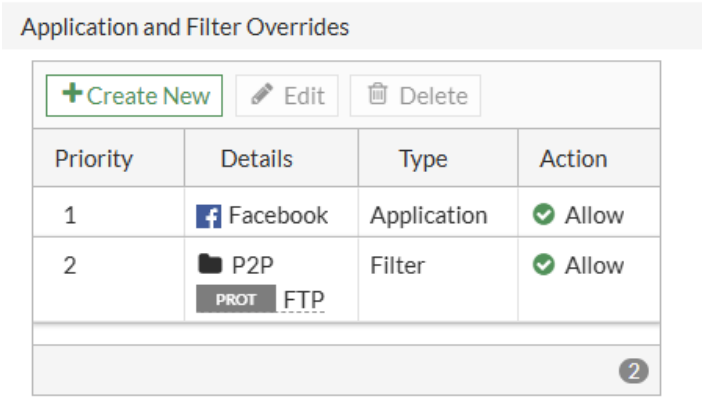
- Monitor – propušta promet i generira poruku zapisnika.
- Allow – propušta promet, ali ne generira poruku zapisnika.
- Block – blokira detektirani promet i generira poruku zapisnika.
- Quarantine – blokira promet s IP adrese napadača do isteka vremena i generira poruku zapisnika.

Kao i u prijašnjim primjerima, i na aplikacijskim filterima mogu se primijeniti iznimke na željenim aplikacijama.

Iznimka se može raditi na dva načina, i to:

- vrsti aplikacije
- kategoriji + protokolu ili ponašanju ili tehnologiji ili proizvođaču ili popularnosti ili riziku.

Prema vrsti aplikacije odabere se, primjerice Facebook, te joj se dodjeljuje željena akcija. Ako želimo napraviti iznimku na drukčiji način, potrebno je odrediti i prilagoditi kategoriju aplikacije i dodatni kriterij. Tako smo, primjerice, dopustili promet koji je kategoriziran kao P2P (engl. *peer to peer*) i koji se odvija preko FTP-a.



Slika 55. Primjer iznimki u aplikacijskom filteru

Za primjenu aplikacijskog filtera preporučuje se SSL inspekcija kako bi se povećala mogućnost čitanja aplikacija u kriptiranom prometu.

5.5.4. SSL inspekcija

Skeniranje i pregled sadržaja preko SSL protokola (engl. *Secure Sockets Layer protocol)* omogućuje primjenu antivirusnog skeniranja, *web*-filtriranja i filtriranja e-pošte na šifrirani promet. Profili SSL inspekcije mogu se primijeniti na sigurnosna pravila vatrozida.

FortiOS uključuje četiri unaprijed definirana SSL/SSH inspekcijska profila, od kojih su tri samo za čitanje i mogu se klonirati:

- pregled certifikata
- dubinska inspekcija
- bez pregleda.

Prilagođeni profil dubinske inspekcije može se uređivati ili se može stvoriti vlastiti SSL/SSH profil inspekcije.

Dubinska inspekcija (također poznata kao SSL/SSH inspekcija) obično se primjenjuje na izlazna sigurnosna pravila, kad su odredišta nepoznata. Ovisno o zahtjevima pravila, moguće je konfigurirati sljedeće:

- koji će se CA certifikat koristiti za dešifriranje SSL šifriranog prometa
- koji će se SSL protokoli pregledavati
- koji će portovi biti povezani s kojim SSL protokolima za inspekciju
- treba li dopustiti nevažeće SSL certifikate

- hoće li se SSH promet pregledavati
- koje adrese ili popisi dopuštenih *web*-kategorija mogu zaobići SSL inspekciju.

5.6. Praćenje i analiza prometa s pomoću Log & Report

Zapisivanje i izvještavanje korisne su komponente koje pomažu razumjeti što se događa na mreži i obavještavaju o određenim mrežnim aktivnostima, kao što su otkrivanje virusa, posjet nevažećoj mrežnoj stranici, upad, neuspjeli pokušaj prijave i bezbroj drugih.

Zapisivanjem se bilježi promet koji prolazi uređajem FortiGate, počinje s njega ili završava na njemu te se bilježe radnje koje je FortiGate poduzeo tijekom procesa skeniranja prometa. Nakon što se te informacije zabilježe u poruci zapisnika, pohranjuju se u datoteku zapisnika koja se pohranjuje na uređaju za zapisnik (središnje mjesto za pohranu poruka zapisnika). FortiGate podržava nekoliko uređaja za zapisnik, kao što su FortiAnalyzer, FortiGate Cloud i *syslog* poslužitelji. Otprilike 5 % memorije koristi se za međuspremnik zapisnika poslanih FortiAnalyzeru. Sistemska memorija i lokalni disk FortiGatea također se mogu konfigurirati za pohranu zapisnika, pa se i oni smatraju uređajem za zapisnik.

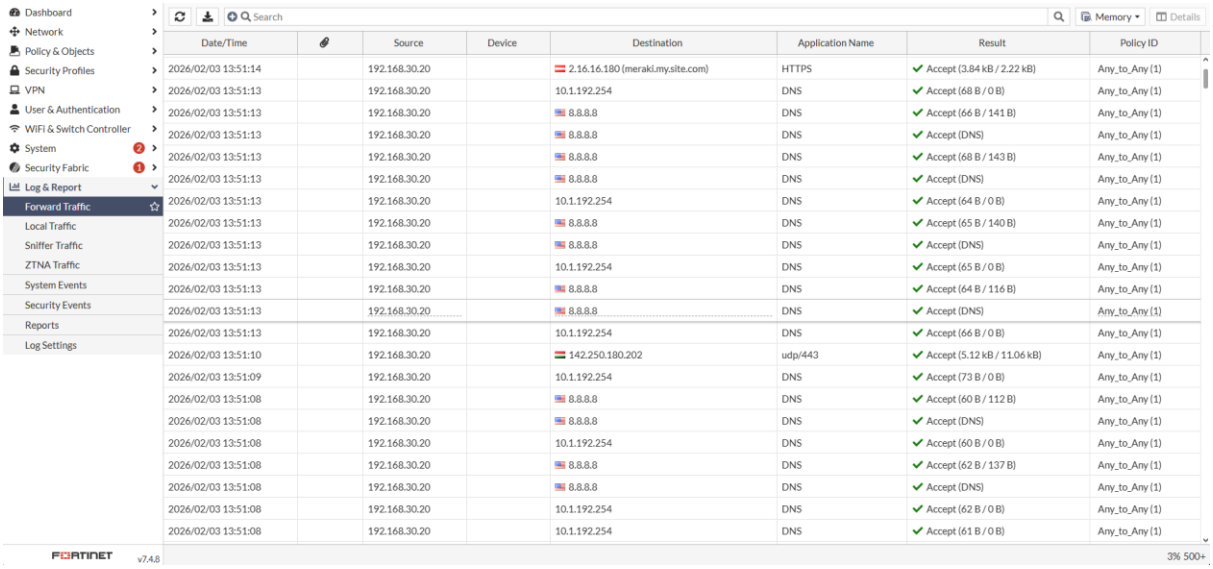
FortiGate omogućuje različite vrste logova, ovisno o tipu aktivnosti i potrebi praćenja:

- Traffic logovi: bilježe sav mrežni promet, uključujući izvor, odredište, portove i korištene protokole.
- Event logovi: prate sistemske događaje, npr. promjene konfiguracije, restart uređaja ili pogreške sustava.
- Security logovi: bilježe sigurnosne incidente, kao što su napadi, otkrivanje virusa, upadi ili neuspjeli pokušaji prijave.
- Web filter logovi: bilježe pristup mrežnim stranicama koje su blokirane ili dopuštene prema pravilima filtriranja.

FortiGate podržava više opcija za pohranu i centralizirano upravljanje logovima:

- FortiAnalyzer: specijalizirani uređaj za centralno prikupljanje, analizu i izvještavanje logova.
- FortiGate Cloud: *cloud* rješenje za pohranu i analizu logova iz FortiGate uređaja.
- Syslog serveri: standardni serveri za prikupljanje logova preko *syslog* protokola.
- Lokalna pohrana na FortiGateu: koristi sistemsku memoriju ili lokalni disk za privremenu pohranu logova.
- FortiGate koristi oko 5 % svoje memorije za međuspremnik logova koji se šalju na FortiAnalyzer.

- Lokalna pohrana omogućuje brzu dostupnost logova za internu analizu, ali za dugoročno arhiviranje preporučuje se slanje logova na FortiAnalyzer, FortiGate Cloud ili *syslog* server.
- Omogućuje praćenje mrežnog prometa i otkrivanje sumnjivih aktivnosti.
- Pomaže u rješavanju problema i *incident responseu* jer administrator može detaljno pregledati sve aktivnosti i sustavne događaje.
- Olakšava sukladnost s regulativama jer se logovi mogu koristiti za *audite* i izvještaje o sigurnosti.



Slika 56. Logovi na FortiGate vatrozidu

5.7. Izrada sigurnosne kopije konfiguracije i vraćanje konfiguracije

U samostalnom sustavu upravljanja, kao što je FortiGate, izrada sigurnosne kopije konfiguracije ključni je element održavanja mrežne stabilnosti, zaštite od gubitka podataka te brzog oporavka u slučaju pogrešaka ili hardverskih kvarova. FortiGate omogućuje ručno i automatsko *backupiranje* konfiguracije, kao i jednostavno vraćanje (engl. *restore*) prethodnih verzija konfiguracije iz lokalne memorije ili udaljenih spremišta.

1. Izrada sigurnosne kopije konfiguracije

FortiGate omogućuje generiranje i pohranu sigurnosnih kopija konfiguracije na nekoliko načina:

Ručno (engl. *Manual Backup*) – administrator može u bilo kojem trenutku izvesti trenutačnu konfiguraciju uređaja preko web GUI-a ili CLI-a (komandom *execute backup config*).

Konfiguracija se može spremiti lokalno na računalo ili na udaljeni poslužitelj (TFTP, FTP, SFTP).

Automatski (engl. *Scheduled Backup*) – moguće je postaviti raspored (npr. dnevno, tjedno) za automatsko spremanje konfiguracije. Automatski *backup* može se slati na definirano udaljeno spremište radi sigurnosti i arhiviranja.

Po verzijama (engl. *Versioned Backup*) – FortiGate automatski čuva različite verzije konfiguracije svaki put kad se napravi promjena i spremi konfiguracija. Administrator može u svakom trenutku pregledati ili preuzeti stariju verziju.

Konfiguracijske kopije mogu se pohraniti lokalno na uređaj, na USB memoriju (ako je dostupna) ili na udaljene servise (TFTP, FTP, SFTP, SCP). Preporučuje se korištenje udaljenog repozitorija radi dodatne zaštite i lakšeg oporavka u slučaju fizičkog kvara uređaja.

2. Vraćanje konfiguracije (*engl. Restore*)

FortiGate podržava fleksibilne metode vraćanja sigurnosne kopije konfiguracije, ovisno o potrebama administratora:

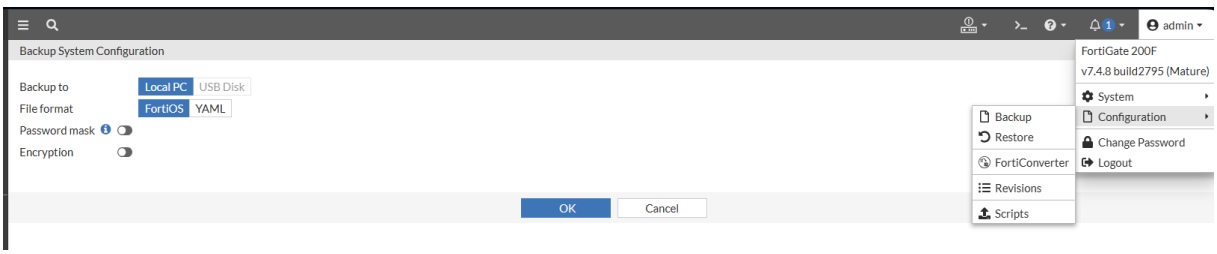
Potpuno vraćanje konfiguracije (engl. *Full Restore*)

Ova opcija vraća cijelu konfiguraciju uređaja na prethodno spremljenu verziju. Koristi se u situacijama kada je konfiguracija oštećena, pogrešno promijenjena ili nakon zamjene uređaja istim modelom. Vraćanje se može izvesti preko web GUI-a (engl. *Upload Configuration File*) ili CLI-a (engl. *execute restore config*).

Djelomično vraćanje konfiguracije (engl. *Partial Restore*)

Administrator može vratiti samo određene dijelove konfiguracije – primjerice *firewall* pravila, VPN postavke, DHCP konfiguraciju ili sistemske parametre. Ova mogućnost omogućuje brzu korekciju pojedinog segmenta bez potrebe za potpunim vraćanjem cijelog sustava.

Prije vraćanja konfiguracije preporučuje se izrada trenutačne sigurnosne kopije kako bi se omogućio povratak u izvorno stanje u slučaju nepredviđenih problema



Slika 57. Izrada sigurnosne kopije konfiguracije FortiGate uređaja

5.8. Konfiguracija FortiGate uređaja

Tijekom upravljanja uređajima koji su integrirani s FortiManagerom (FM) preporučuje se da se sve konfiguracijske promjene rade isključivo kroz FortiManager. Razlog tomu je način na koji FortiManager upravlja konfiguracijom i održava sinkronizaciju s FortiGate uređajima.

Ako se konfiguracija mijenja izravno na FortiGate uređaju, FortiManager te promjene ne mora odmah ili potpuno prepoznati. U takvim situacijama može doći do nesinkroniziranog stanja (*out-of-sync*) između konfiguracije na FortiManageru i stvarne konfiguracije na FortiGateu. Posljedica toga može biti:

- FortiManager prikazuje zastarjelu ili nepotpunu konfiguraciju
- pri sljedećem *Policy package installa* ili *Device installa* FortiManager može prepisati lokalne promjene napravljene direktno na FortiGateu
- može doći do konflikata u konfiguraciji ili neočekivanog ponašanja nakon instalacije konfiguracije.

Ovaj je izazov posebno uočen u scenarijima kada se konfiguracijom uređaja djelomično održava s pomoću FortiManagera, a djelomično izravno na FortiGateu.

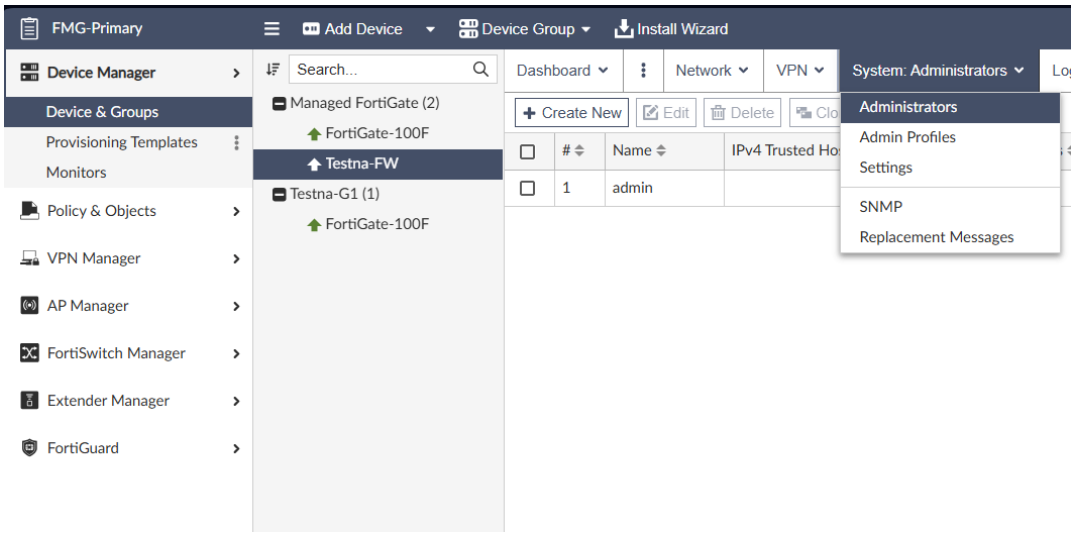
Zbog toga vrijede sljedeće preporuke:

- sve konfiguracijske promjene treba raditi isključivo preko FortiManagera
- izravne promjene na FortiGateu treba izbjegavati kada je uređaj već pod upravljanjem FortiManagera
- ako je iznimno potrebno napraviti promjenu izravno na FortiGateu (npr. u hitnim situacijama), zatim je potrebno ručno provjeriti i uskladiti konfiguraciju u FortiManageru prije sljedeće instalacije konfiguracije.

Tako se zadržava konzistentnost konfiguracije i izbjegavaju problemi sa sinkronizacijom između FortiManagera i FortiGate uređaja.

Za administraciju FortiGate uređaja izvan FortiManagera potrebno je prethodno omogućiti odgovarajući pristup. Preporučeni način je kreiranje lokalnoga administratorskog računa preko FortiManagera kako bi upravljanje pristupima ostalo centralizirano.

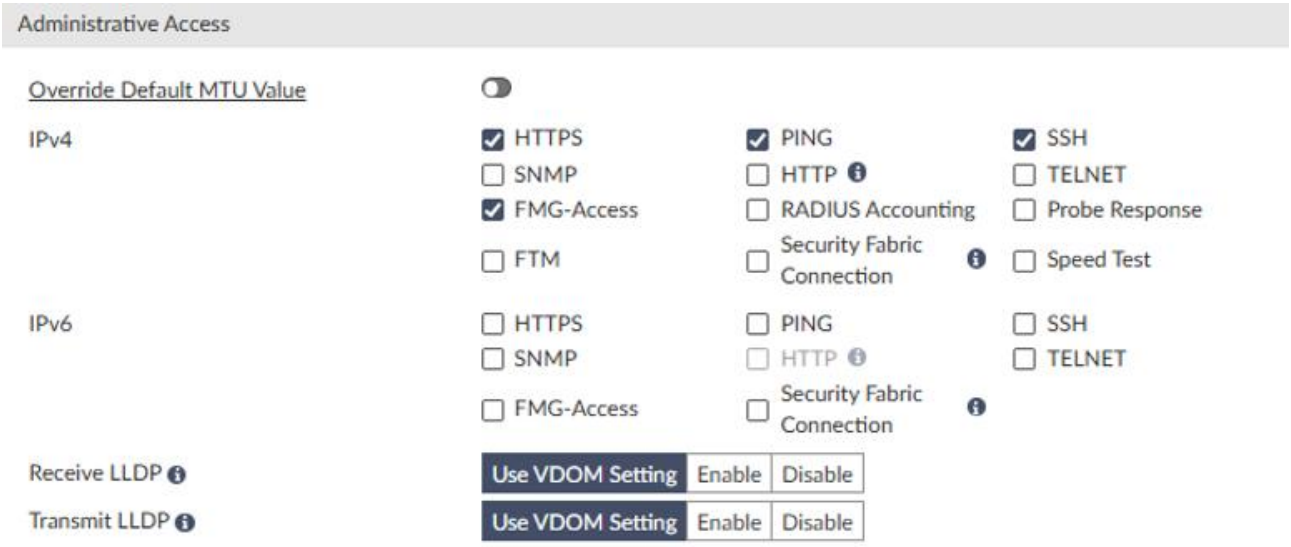
- U FortiManageru otvoriti *Device Manager* i odabrati željeni FortiGate uređaj.
- U sekciji za konfiguraciju sustava (*System Settings*) definirati novoga administratorskog korisnika.
- Dodijeliti odgovarajuće privilegije (preporučeno: ograničiti na minimalno potrebne ovlasti).
- Izvršiti *Install wizard* kako bi se korisnički račun primijenio na FortiGate uređaju.



Slika 58. Dodavanje lokalnog administratora za administrativno upravljanje FortiGate uređajem

Preporuka je da lozinka za lokalni račun mora biti u skladu s modernim sigurnosnim standardima (minimalno 12 znakova, kombinacija velikih i malih slova, brojeva i specijalnih znakova).

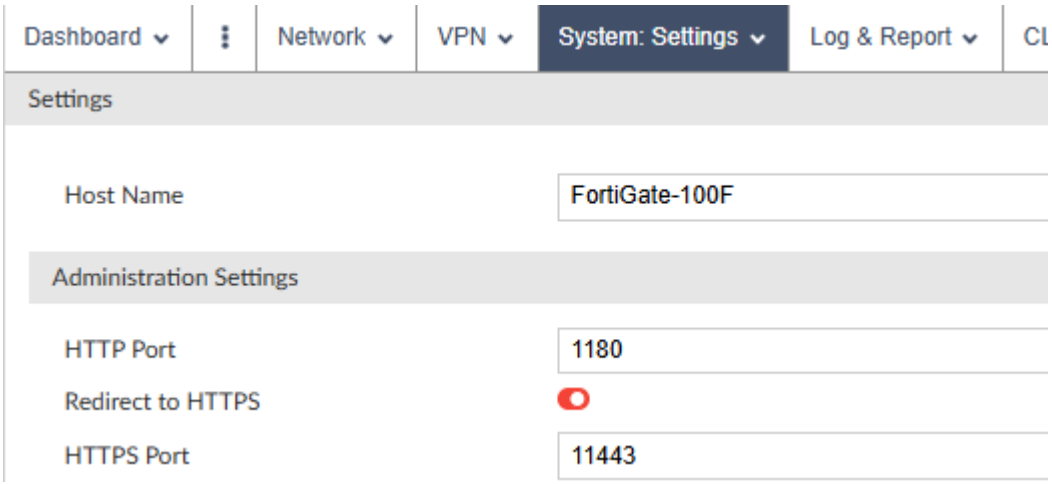
Pristup lokalnom GUI-u FortiGate uređaja ostvaruje se preko mrežnog sučelja na kojemu je administrativni pristup omogućen (slika 59).



Slika 59. Administrativni pristup na mrežnom sučelju

- Pristup se ostvaruje preko HTTPS veze na sučelju na kojemu je administrativni pristup omogućen (npr. https://<management-ip>:PORT).
- Prijava se provodi s prethodno definiranim lokalnim korisničkim računom.

Port je postavljen kao 11443 za spajanje preko HTTPS-a, a način za promjenu samog porta je navigiranje u izbornik *Device Manager*, odabir željenog uređaja te pod *System* rubrikom odabir podizbornika *Settings*. Nakon toga moguće je prepraviti sve portove u bilo koji drugi željeni port.

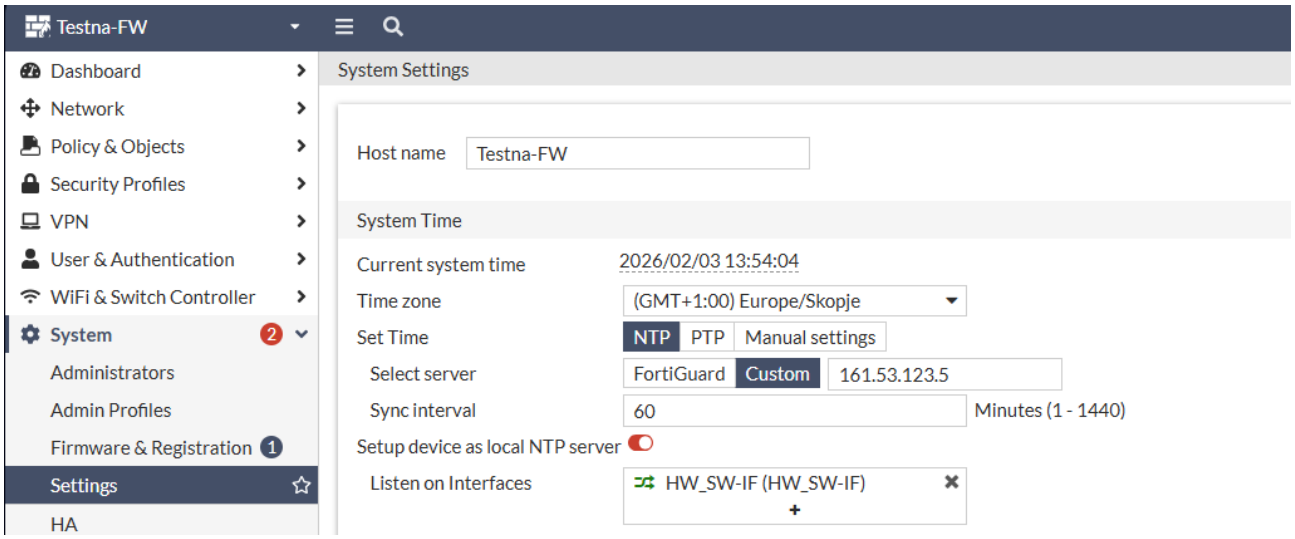


Slika 60. Primjer promjene HTTPS port postavke

Ovakav pristup treba koristiti isključivo u iznimnim situacijama, uz obaveznu naknadnu sinkronizaciju s FortiManagerom kako bi se izbjegli problemi u upravljanju konfiguracijom.

5.8.1. Postavljanje Hostnamea

1. Prijavite se na FortiGate mrežno sučelje s administratorskim računom.
2. U izborniku odaberite: System > Settings.
3. U polje Hostname unesite željeni naziv uređaja (npr. OS-BIOKAMPUS-FW).
4. Kliknite *Apply* za spremanje postavki.
5. Promjene Hostnamea vidljive su odmah u GUI-u i CLI-u, ali za potpuni prikaz u mrežnim logovima preporučuje se *restart* sesije.



Slika 61. Primjer promjene Hostname postavke

Postavljanje Hostnamea preko CLI-a

1. Spojite se na FortiGate preko konzole, SSH-a ili mrežnog terminala.
2. Unesite sljedeće naredbe:

   config system global

   set hostname FGT-UniZG-01

   end
3. Provjerite promjenu naredbom:

   get system status
4. Novi Hostname pojavit će se u statusu uređaja i svim logovima.

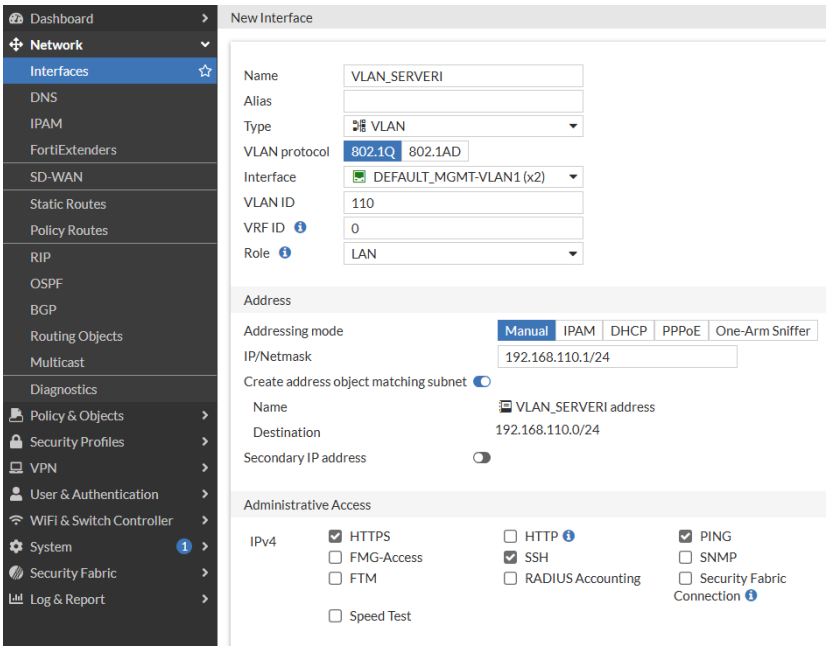
5.8.2. Konfiguracija VLAN sučelja

VLAN (engl. *Virtual Local Area Network*) sučelje omogućuje logičku segmentaciju mrežnog prometa unutar istoga fizičkog okruženja. Na FortiGate uređaju VLAN-ovi se definiraju kao virtualna sučelja povezana na fizički port ili agregirani link, što omogućuje odvajanje mrežnih segmenata (npr. studenti, administracija, serverski segment) uz primjenu zasebnih sigurnosnih pravila.

Konfiguracija VLAN sučelja preko GUI-a

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite izbornik Network > Interfaces.

3. Kliknite Create New > Interface.
4. U polje Name unesite naziv sučelja (npr. VLAN_SERVERI).
5. U polju Type odaberite VLAN.
6. U polju Interface odaberite fizički port na kojem se VLAN konfigurira (npr. port3).
7. U polje VLAN ID unesite odgovarajući VLAN broj (npr. 110).
8. U odjeljku IP/Netmask definirajte IP adresu i masku podmreže za VLAN (npr. 192.168.110.1/24).
9. Prema potrebi uključite Administrative Access opcije (HTTPS, PING, SSH…) za upravljanje.
10. Kliknite *OK* za spremanje postavki.



Slika 62. Primjer izrade VLAN sučelja

Konfiguracija VLAN sučelja preko CLI-a

1. Spojite se na FortiGate preko CLI-a.
2. Unesite:

```
config system interface
  edit VLAN_Students
    set vdom root
    set ip 192.168.30.1 255.255.255.0
    set allowaccess ping https ssh
```

```
        set interface port3
        set vlanid 30
    next
end
```

3. Provjerite status VLAN-a naredbom:

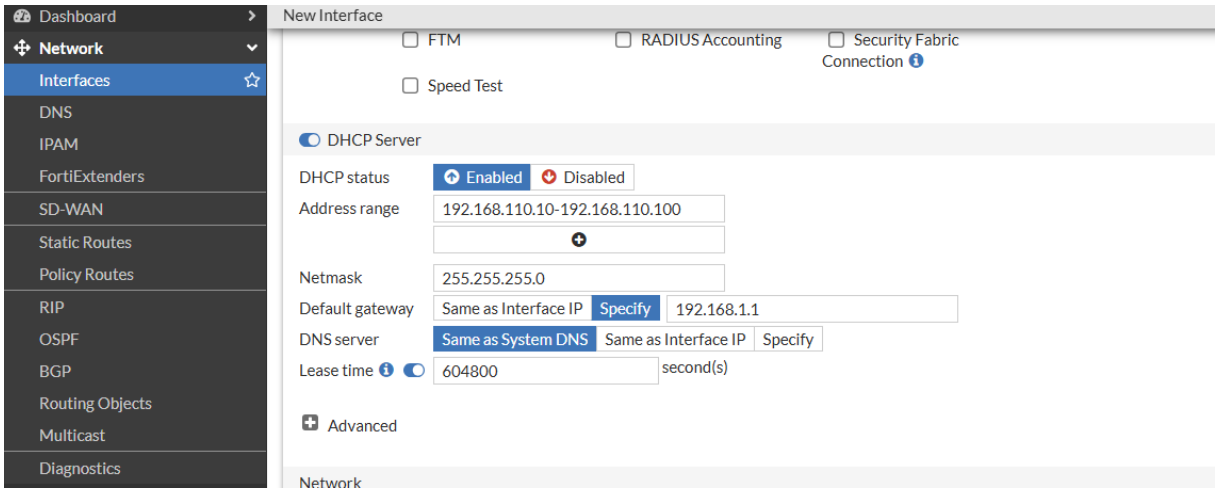
   get system interface physical.

5.8.3. DHCP poslužitelj – rezervacija adrese

DHCP (engl. *Dynamic Host Configuration Protocol*) poslužitelj na FortiGate uređaju automatski dodjeljuje IP adrese, *gateway* i druge mrežne postavke klijentima unutar određenoga mrežnog segmenta. Funkcija rezervacije adrese omogućuje da određeni uređaj uvijek dobiva istu IP adresu, što je korisno za mrežnu opremu, servere ili uređaje s posebnim pravilima pristupa.

Konfiguracija DHCP poslužitelja s rezervacijom preko GUI-a

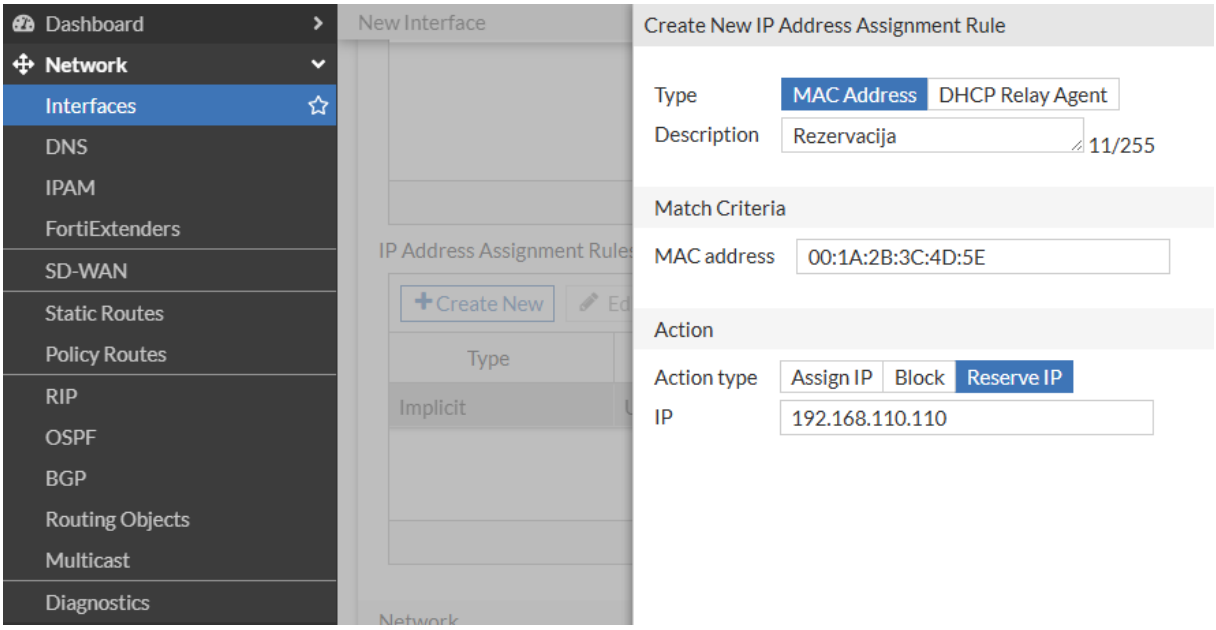
1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Network > Interfaces.
3. Odaberite mrežno ili VLAN sučelje na kojem želite aktivirati DHCP.
4. U odjeljku DHCP Server odaberite *Enable*.
5. Definirajte:
   - IP Range (raspon adresa, npr. 192.168.110.10 – 192.168.110.100).
   - Netmask (npr. 255.255.255.0).
   - Default Gateway (npr. 192.168.110.1 – IP sučelja).
   - DNS Servere (može biti FortiGate ili vanjski DNS).



Slika 63. Postavke DHCP poslužitelja na mrežnom sučelju

Dodavanje rezervacije IP adrese:

1. Kliknite Advanced kako biste dodali Static MAC-IP Mapping:
   - MAC Address: fizička adresa uređaja (npr. 00:1A:2B:3C:4D:5E).
   - IP Address: rezervirana IP adresa (izvan dinamičkog raspona ili unutar njega, npr. 192.168.110.110).
2. Spremite postavke klikom na OK.



Slika 64. Rezervacija IP adrese

Konfiguracija DHCP rezervacije preko CLI-a

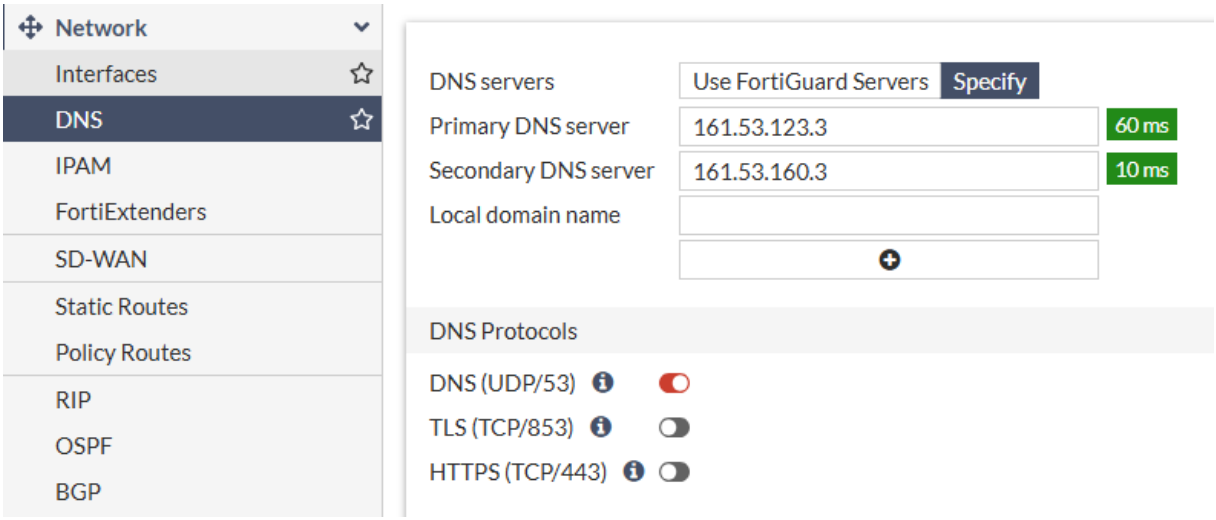
1. Spojite se na FortiGate preko CLI-a.
2. Unesite:

```
config system dhcp server
  edit 1
    set interface "VLAN_SERVERI"
    set lease-time 86400
    config ip-range
      edit 1
        set start-ip 192.168.30.10
        set end-ip 192.168.30.100
      next
    end
    config reserved-address
      edit 1
        set mac 00:1A:2B:3C:4D:5E
        set ip 192.168.30.110
      next
    end
  next
end
```

5.8.4. Konfiguracija DNS postavki

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Network > DNS.
3. U odjeljku DNS Server odaberite jednu od opcija:
    - Retrieve from System – koristi DNS postavke od davatelja internetske usluge (ISP).
    - Specify – ručno definirajte primarni i sekundarni DNS poslužitelj.
        - Primjer:
        - Primary DNS: 8.8.8.8 (Google DNS)
        - Secondary DNS: 1.1.1.1 (Cloudflare DNS)

4. Po želji uključite DNS over TLS radi enkripcije DNS upita.
5. Kliknite *Apply* za spremanje postavki.



Slika 65. DNS postavke

Konfiguracija DNS postavki preko CLI-a

1. Spojite se na FortiGate preko CLI-a.
2. Unesite:

   config system dns

   set primary 8.8.8.8

   set secondary 1.1.1.1

   set dns-over-tls enable

   end
3. Provjerite postavke naredbom:

   get system dns.

5.8.5. NTP postavke

NTP (engl. *Network Time Protocol*) osigurava sinkronizaciju vremena FortiGate uređaja s pouzdanim vremenskim poslužiteljima. To je ključno za točno bilježenje događaja u logovima, ispravno funkcioniranje certifikata i koordinaciju s drugim mrežnim uređajima.

1. Prijavite se na FortiGate mrežno sučelje.

2. Otvorite System > Settings.

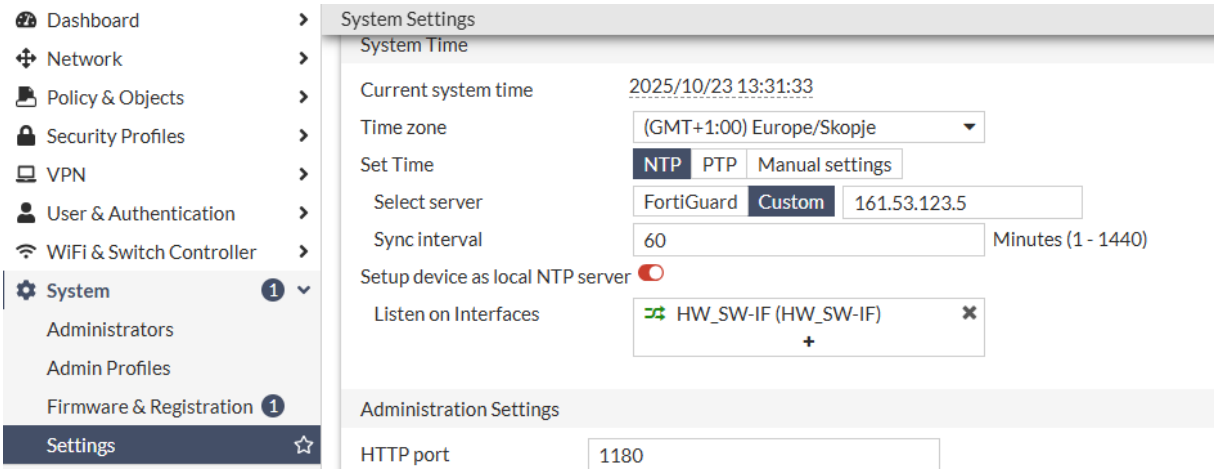
3. U odjeljku System Time odaberite opciju *Synchronize with NTP Server.*

4. U polje NTP Server unesite adresu pouzdanog NTP poslužitelja (npr. pool.ntp.org ili nacionalni NTP poput time.cloudflare.com).

5. Prema potrebi odaberite više poslužitelja radi redundancije.

6. Definirajte vremensku zonu (npr. GMT+1 za Hrvatsku).

7. Kliknite *Apply* za spremanje.



Slika 66: NTP postavke

Konfiguracija NTP postavki preko CLI-a

1. Spojite se na FortiGate preko CLI-a.

2. Unesite:

```
config system ntp
    set ntpsync enable
    set type custom
    config ntpserver
        edit 1
            set server "pool.ntp.org"
        next
        edit 2
            set server "time.cloudflare.com"
        next
```

```
    end
    set syncinterval 60
end
```

- syncinterval je vrijeme (u minutama) između dvije sinkronizacije (npr. 60 = 1 h).

3. Provjerite status naredbom:

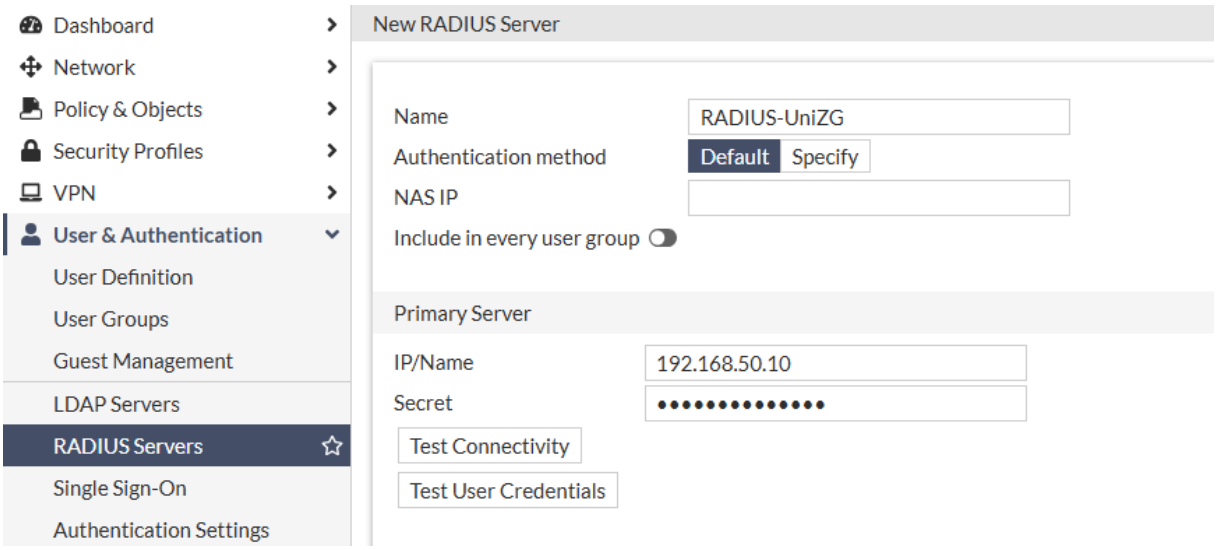
   diagnose sys ntp status.

5.8.6. RADIUS konfiguracija

RADIUS (engl. *Remote Authentication Dial-In User Service*) protokol je koji omogućuje centraliziranu autentikaciju, autorizaciju i evidenciju korisnika pri pristupu mreži ili administraciji FortiGate uređaja. U sustavu e-Sveučilišta koristi se za integraciju s postojećim identitetskim sustavima (npr. Active Directory, FreeRADIUS) radi jedinstvene prijave (engl. *single sign-on*) i upravljanja korisničkim ovlastima.

Dodavanje RADIUS poslužitelja preko GUI-a

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite User & Authentication > RADIUS Servers.
3. Kliknite *Create New*.
4. Unesite:
   - Name – naziv RADIUS poslužitelja (npr. RADIUS-UniZG).
   - IP Address – IP adresa RADIUS poslužitelja (npr. 192.168.50.10).
   - Secret – zajednički ključ (engl. *shared secret*) koji se mora podudarati s onim na RADIUS poslužitelju.
5. Kliknite *OK* za spremanje.



Slika 67. RADIUS postavke

Dodavanje RADIUS poslužitelja preko CLI-a

1. Spojite se na FortiGate preko CLI-a.
2. Unesite:

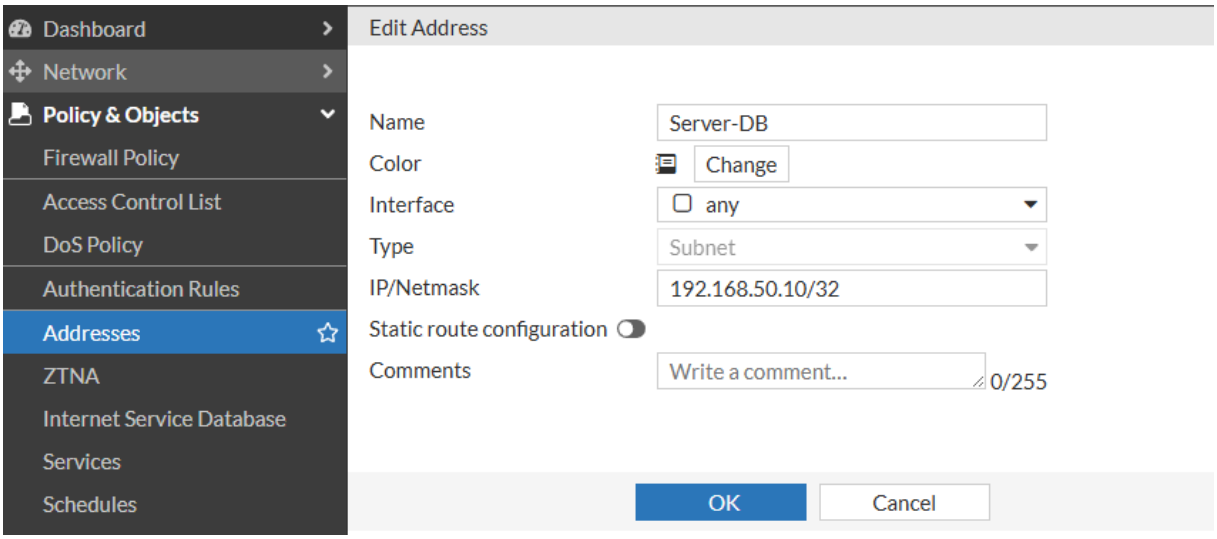
```
config user radius
  edit "RADIUS-UniZG"
    set server 192.168.50.10
    set secret <shared_secret>
    set auth-type auto
    set port 1812
  next
end
```

5.8.7. Izrada IP objekta

IP objekti u FortiGate uređaju koriste se za jednostavnije i preglednije definiranje pravila u *firewall* sigurnosnim pravilima. Umjesto da se IP adrese unose ručno u svako pravilo, one se definiraju kao objekti i koriste više puta, što povećava preglednost i smanjuje mogućnost pogreške.

Izrada IP objekta preko GUI-a:

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Policy & Objects > Addresses.
3. Kliknite Create New > Address.
4. Unesite:
   - Name – naziv objekta (npr. Server-DB).
   - Type – IP/Netmask, Range ili FQDN:
     - IP/Netmask – za pojedinačnu adresu ili mrežu (npr. 192.168.50.10/32).
     - Range – za raspon adresa (npr. 192.168.50.10 – 192.168.50.20).
     - FQDN – za definiranje objekta preko naziva domene (npr. server.unizg.hr).
   - Interface – odaberite na kojem je sučelju objekt dostupan (ili ostavite Any).
5. Kliknite *OK* za spremanje.



Slika 68. IP objekt

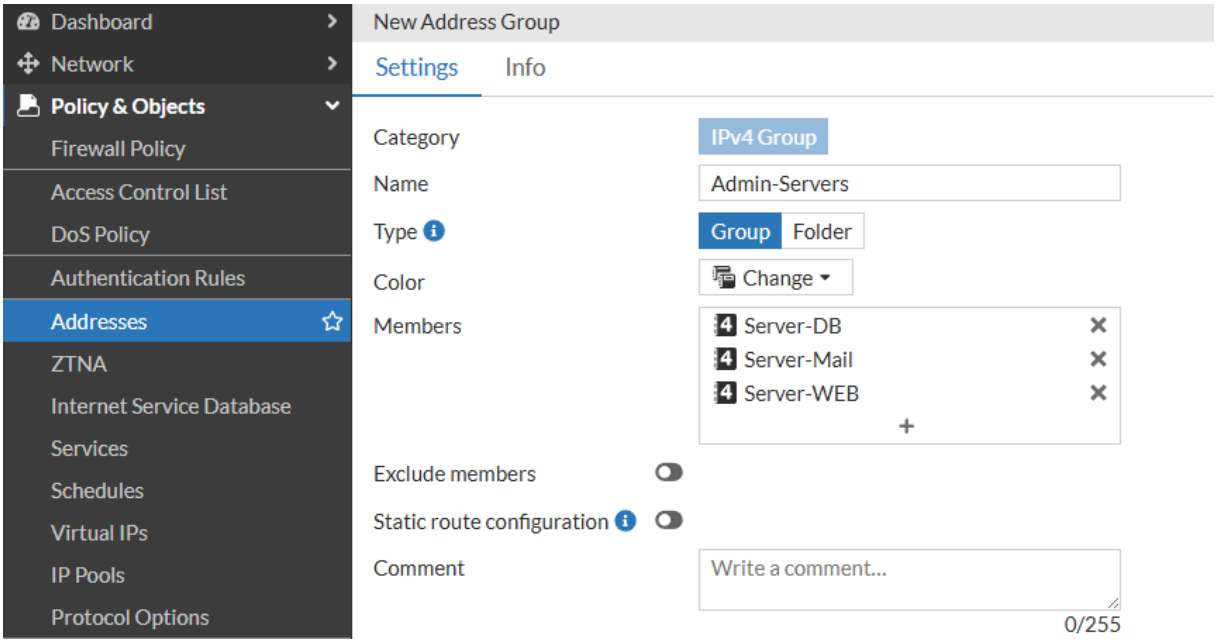
5.8.8. Izrada grupe IP objekata

Grupe IP objekata omogućuju objedinjavanje više pojedinačnih IP adresa, mreža ili FQDN-ova u jedan logički entitet. To olakšava upravljanje *firewall* pravilima jer se jedno pravilo može primijeniti na cijelu skupinu umjesto na svaki objekt pojedinačno.

Izrada grupe IP objekata preko GUI-a:

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Policy & Objects > Addresses.

3. Kliknite Create New > Address Group.
4. Unesite:
   - Name – naziv grupe (npr. Admin-Servers).
   - Members – odaberite IP objekte koje želite uključiti u grupu (npr. Server-DB, Server-Web, Server-Mail).
5. Kliknite *OK* za spremanje.



Slika 69. Grupa IP objekata

Izrada grupe IP objekata preko CLI-a

1. Spojite se na FortiGate preko CLI-a.
2. Unesite:

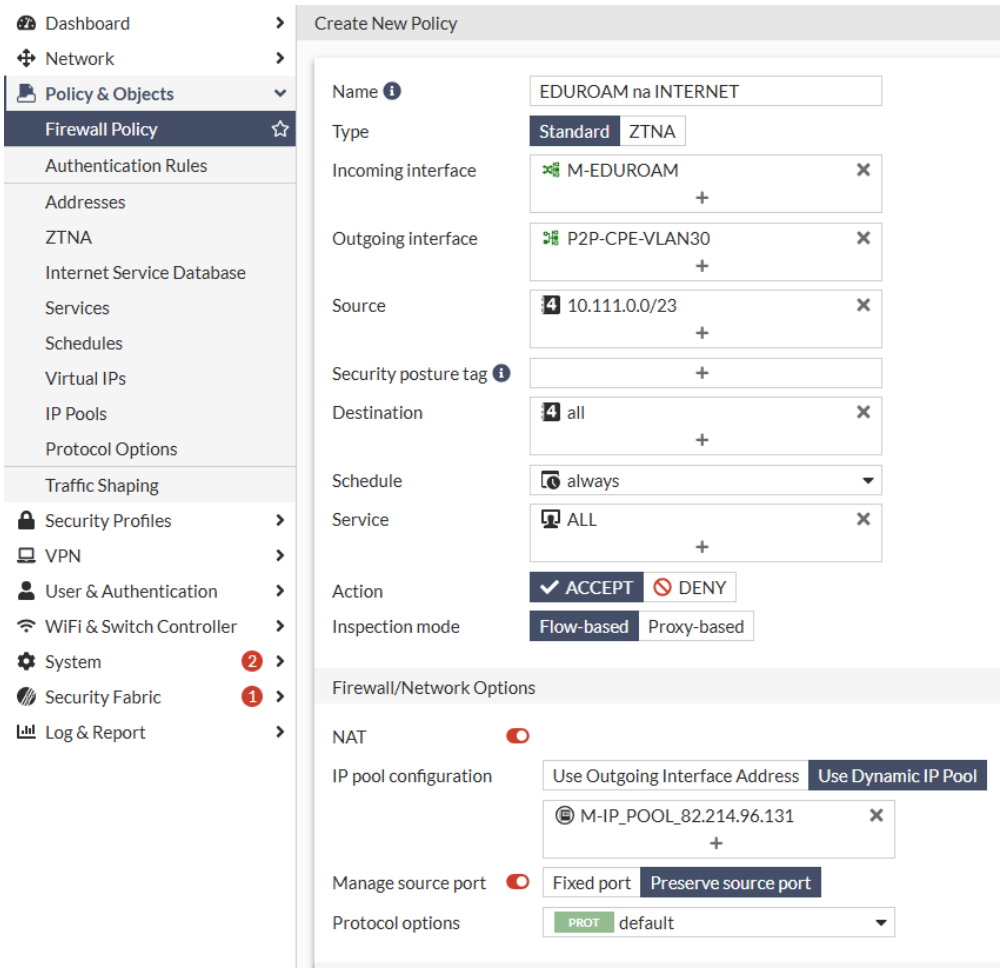
```
config firewall addrgrp
  edit "Admin-Servers"
    set member "Server-DB" "Server-Web" "Server-Mail"
  next
  end
```

5.8.9. Izrada sigurnosnih pravila vatrozida

Sigurnosna pravila vatrozida (engl. *firewall policy*) definiraju kako će uređaj FortiGate obrađivati promet između mrežnih segmenata ili prema internetu. Pravila određuju smjer prometa, dopuštene ili blokirane servise, sigurnosne profile i uvjete pristupa.

Izrada sigurnosnih pravila preko GUI-a

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Policy & Objects > Firewall Policy.
3. Kliknite *Create New*.
4. Unesite:
   - Name – naziv pravila (npr. LAN_to_Internet).
   - Incoming Interface – sučelje ili VLAN odakle promet dolazi (npr. VLAN_Students).
   - Outgoing Interface – sučelje kojim promet izlazi (npr. wan1).
   - Source – odaberite IP objekte ili grupe (npr. Students_Network).
   - Destination – odaberite IP objekte ili grupe (npr. all).
   - Schedule – odaberite *Always* ili vremensko ograničenje.
   - Service – odaberite servise (npr. ALL, HTTP, HTTPS).
   - Action – odaberite *Accept* (dopusti) ili *Deny* (zabrani).
5. Prema potrebi uključite NAT ako se promet preusmjerava na internet.
6. Kliknite *OK* za spremanje.



Slika 70. Sigurnosna pravila

Izrada sigurnosnih pravila preko CLI-a

1. Spojite se na FortiGate preko CLI-a.
2. Unesite:

```
config firewall policy
    edit 6
        set name "EDUROAM na INTERNET"
        set srcintf "M-EDUROAM"
        set dstintf "P2P-CPE-VLAN30"
        set action accept
        set srcaddr "10.111.0.0/23"
        set dstaddr "all"
        set schedule "always"
```

```
        set service "ALL"
        set logtraffic all
        set nat enable
        set ippool enable
        set poolname "M-IP_POOL_82.214.96.131"
    next
end
```

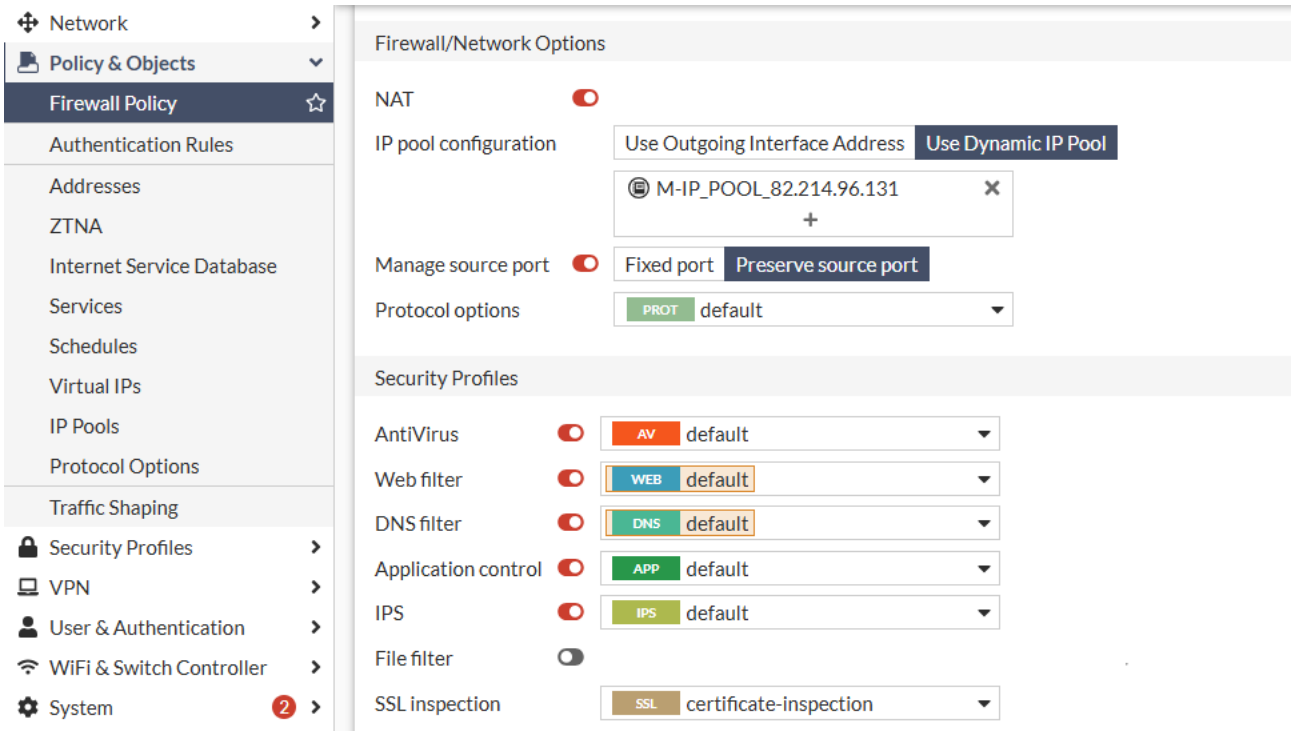
5.8.10. Dodavanje sigurnosnih profila (antivirus, web filter, DNS filter, Application Control, IPS, SSL Inspection)

Sigurnosni profili omogućuju uređaju FortiGate da, osim osnovne kontrole prometa, analizira i filtrira sadržaj kako bi spriječio prijetnje, blokirao nepoželjan sadržaj i osigurao usklađenost s pravilima upotrebe mreže.

Sigurnosni profili ne primjenjuju se samostalno – dodaju se unutar postojećih *firewall* pravila kako bi promet između izvora i odredišta bio inspekcijski obrađen.

Dodavanje sigurnosnog profila preko GUI-a

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Policy & Objects > Firewall Policy.
3. Odaberite postojeće pravilo (npr. LAN_to_Internet) i kliknite Edit.
4. U sekciji Security Profiles uključite željene profile:
    - antivirus – zaštita od zlonamjernih datoteka i virusa.
    - web filter – filtriranje mrežnih stranica po kategorijama ili URL listama.
    - DNS filter – blokiranje zlonamjernih domena na razini DNS upita.
    - Application Control – kontrola pristupa aplikacijama i protokolima.
    - IPS (engl. *Intrusion Prevention System*) – detekcija i sprečavanje mrežnih napada.
    - SSL/SSH Inspection – inspekcija šifriranog prometa radi primjene sigurnosnih pravila.
5. Za svaki profil odaberite postojeći predložak ili kreirajte novi klikom na *Create New*.
6. Kliknite *OK* za spremanje promjena.



Slika 71. Sigurnosni profili na pravilima vatrozida

Dodavanje sigurnosnog profila preko CLI-a

Primjer dodavanja profila na pravilo:

```
config firewall policy
  edit 1
    set av-profile "default"
    set webfilter-profile "default"
    set dnsfilter-profile "default"
    set application-list "default"
    set ips-sensor "default"
    set ssl-ssh-profile "certificate-inspection"
  next
end
```

5.8.11. IPSEC

IPsec (engl. *Internet Protocol Security*) skup je protokola i mehanizama koji omogućuju sigurno uspostavljanje komunikacije preko IP mreža, uključujući javni internet. Koristi se kako bi se podaci koji putuju mrežom zaštitili od presretanja, izmjene ili neovlaštenog pristupa. IPsec radi na mrežnom sloju OSI Layer 3, što znači da može štititi promet bez obzira na aplikaciju ili protokol koji se koristi.

Glavne značajke IPsec-a su:

- **Autentikacija**
  Osigurava da su krajnje točke tunela (npr. dva udaljena ureda ili korisnik i mreža) zaista one za koje se predstavljaju. Najčešći mehanizmi su *pre-shared key* (PSK) i digitalni certifikati.

- **Integritet podataka**
  IPsec provjerava da podaci nisu izmijenjeni tijekom prijenosa. Ovaj mehanizam sprečava manipulaciju paketima i napade tipa *man-in-the-middle*.

- **Enkripcija**
  Podaci se šifriraju tako da ih treće strane ne mogu pročitati, čak i ako presretnu mrežni promet. U praksi se koriste algoritmi poput AES-a.

- **Zaštita od ponovnog slanja (engl. *anti-replay*)**
  IPsec sprečava napade u kojima bi napadač pokušao ponovno poslati legitimne pakete kako bi poremetio sesiju.

- **Fleksibilnost i interoperabilnost**
  IPsec je industrijski standard, pa omogućuje povezivanje različitih uređaja i sustava — što je posebno važno u heterogenim mrežama.

Zbog svoje robusnosti, široke podrške i visokog stupnja sigurnosti, IPsec je danas jedan od najčešće korištenih protokola za izgradnju sigurnih VPN tunela u poslovnim okružjima.

U sklopu projekta e-Sveučilišta IPSEC tuneli se koriste za povezivanje udaljenih lokacija s matičnom te se tako ostvaruje sigurna veza i komunikacija između svih lokacija (matična i udaljene) koje su spojene u jednu logičnu cjelinu. Također je svim udaljenim lokacijama primarna veza pristup internetu upravo preko IPSEC te u slučaju ispada matične lokacije pristup internetu ostvaruje se preko internetske veze na udaljenoj lokaciji. Redundancija je ostvarena na razini statičkih predefiniranih usmjerničkih putanja (eng. *default route*) tako da putanja kroz IPSEC ima nižu administrativnu distancu te je prvi izbor za vatrozid pri odabiru za usmjeravanje. Treba naglasiti da svaka udaljena lokacija ima dodatnih statičkih putanja

koje se usmjeravaju na izravno internetski pristup, a ne preko IPSEC-a radi ispravnog rada servisa na lokaciji. U tablici su navedene statičke putanje svake udaljene lokacije i namjena.

Rb.	Mreža	Predefinirani usmjerivač	Namjena
1.	209.237.148.197/32	Privatna p2p adresa CARNET CPE-a	FortiManager
2.	209.237.148.196/32	Privatna p2p adresa CARNET CPE-a	FotiAnalyzer
3.	161.53.123.3/32	Privatna p2p adresa CARNET CPE-a	DNS
4.	161.53.123.5/32	Privatna p2p adresa CARNET CPE-a	NTP
5.	161.53.160.3/32	Privatna p2p adresa CARNET CPE-a	DNS
6.	161.53.160.5/32	Privatna p2p adresa CARNET CPE-a	NTP
7.	31.147.206.151/32	Privatna p2p adresa CARNET CPE-a	RADIUS*
8.	p2p privatna matične lokacije	Privatna p2p adresa CARNET CPE-a	IPSEC**

Tablica 7. Popis statičkih usmjerivačkih putanja

* RADIUS IP adresa ovisi o lokaciji samog servisa

** IPSEC adresa potrebna za pregovaranje IPSEC tunela

Seq. #	Destination	Gateway	Interface	Distance	Priority	Status	Description
IPv4 (10)							
1	0.0.0.0/0.0.0.0	172.16.3.125	P2P-CPE-VLAN30	15	1	Enable	DEFAULT ROUTE LOCAL
2	209.237.148.197/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	FMG
3	209.237.148.196/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	FAZ
4	161.53.123.3/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	DNS1
5	161.53.160.3/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	DNS2
6	161.53.123.5/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	NTP1
7	161.53.160.5/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	NTP2
8	31.147.206.151/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	RADIUS
9	172.16.9.154/255.255.255.255	172.16.3.125	P2P-CPE-VLAN30	10	1	Enable	IPSEC negotiation
10727	0.0.0.0/0.0.0.0	0.0.0.0	S2S-VPN_1 (To-the-	10	2	Enable	DEFAULT ROUTE IPSEC

Tablica 8. Primjer statičkih putanja na vatrozidu

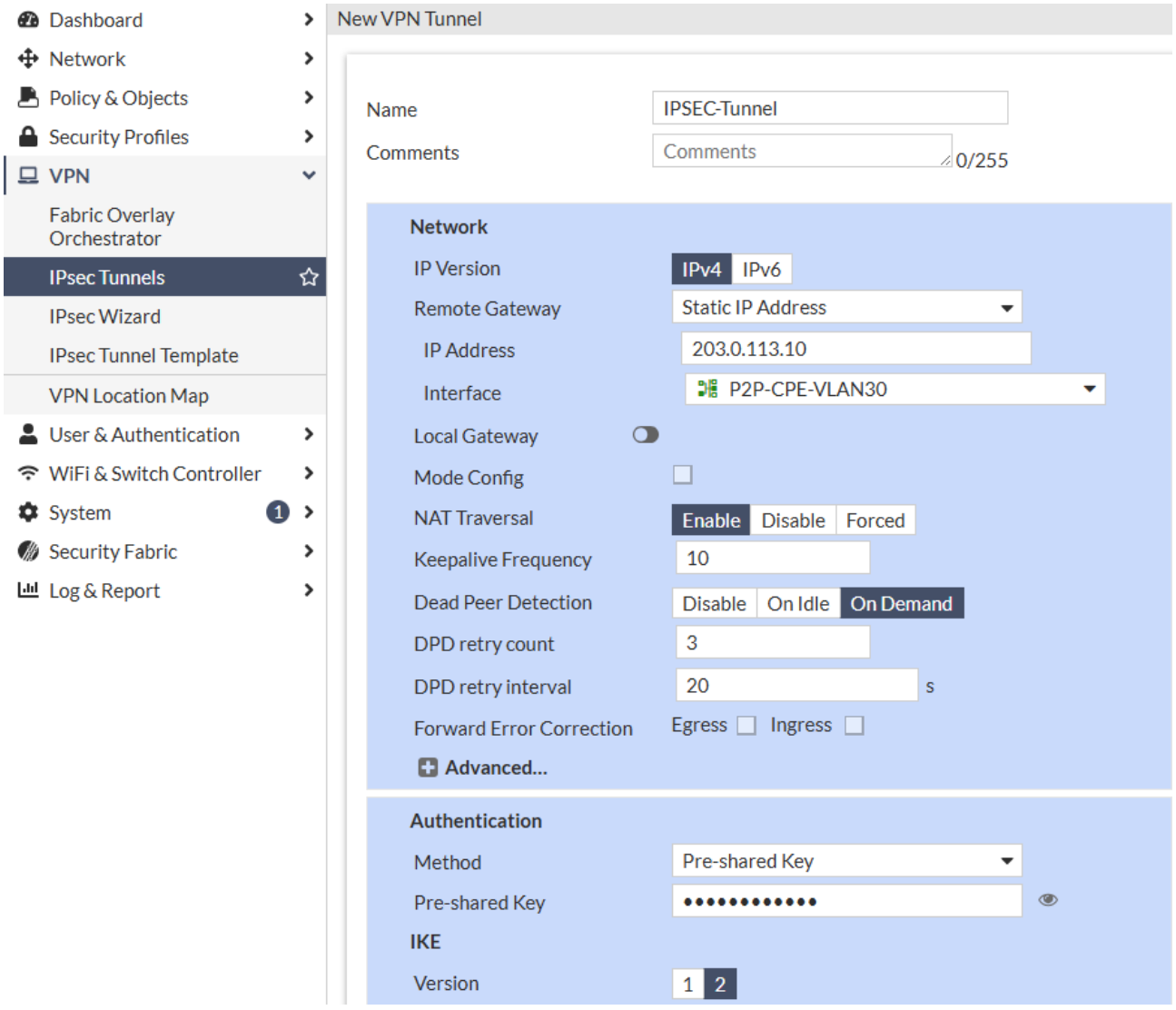
Kreiranje IPsec tunela (Phase 1 i Phase 2) preko GUI sučelja

Korak 1: Prijavite se na FortiGate web mrežno sučelje.

1. Otvorite VPN > IPsec Tunnels.
2. Kliknite Create New.

3. Odaberite IPsec Tunnel.
4. Odaberite predložak Custom (Prilagođeno) i kliknite Next.
5. Ime (Name): unesite naziv za tunel (npr. FG_A_to_FG_B).
6. Remote Gateway (Udaljeni pristupnik):
7. IP Version: odaberite IPv4.

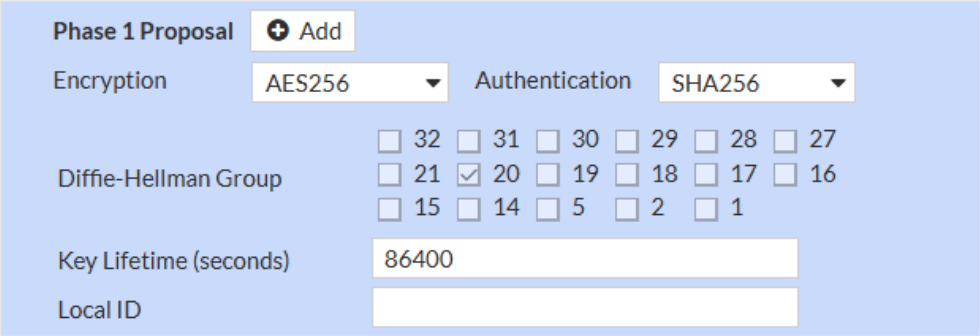
- IP Address: odaberite Static IP Address.
- Remote IP Address: unesite javnu IP adresu udaljenog FortiGatea (FortiGate B) (npr. 203.0.113.10).
- Interface: odaberite vanjsko sučelje FortiGatea A (npr. wan1).
- NAT Traversal: ostavite Disable ako je potrebno.
- Authentication: odaberite Pre-shared Key i unesite tajni ključ.



Slika 72. IPSEC postavke

8. Phase 1 Proposal (Prijedlog Faze 1):

- Encryption: odaberite željene algoritme (npr. AES256).
- Authentication: odaberite željene algoritme (npr. SHA256).
- Diffie-Hellman Groups (npr. 20)
- Key Lifetime: ostavite zadano ili prilagodite (npr. 86400 sekundi).
- Local ID: (Opcionalno) može se ostaviti prazno ili unijeti FQDN/IP.



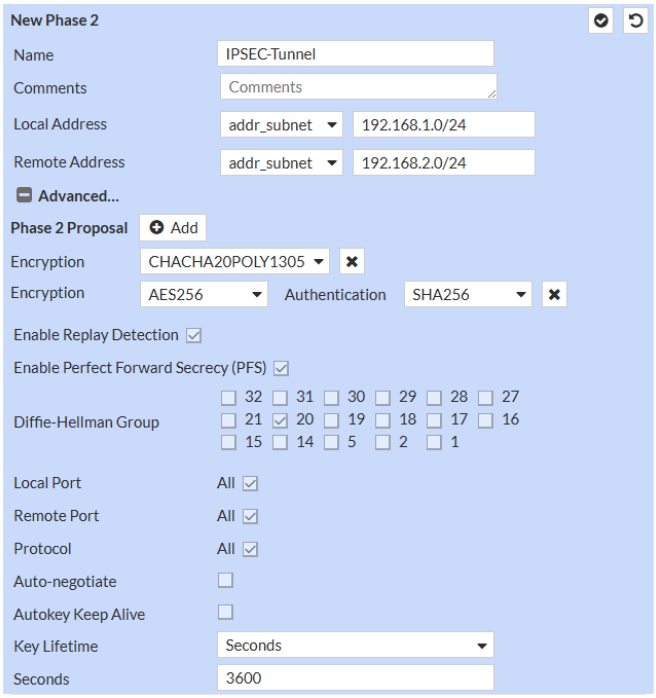
Slika 73. IPSEC postavke IKE faze 1

9. Phase 2 Selectors (Selektori Faze 2):

- Name: unesite naziv za Phase 2 (npr. FG_A_to_FG_B_p2).
- Remote Subnet: unesite mrežu iza udaljenog FortiGatea B (npr. 192.168.2.0/24).
- Local Subnet: unesite mrežu iza lokalnog FortiGatea A (npr. 192.168.1.0/24).

10. Phase 2 Proposal (Prijedlog Faze 2):

- Encryption: odaberite željene algoritme (npr. AES256).
- Authentication: odaberite željene algoritme (npr. SHA256).
- PFS (Perfect Forward Secrecy): preporučuje se uključiti i odabrati jaču grupu (npr. Diffie-hellman-group-20).
- Key Lifetime: ostavite zadano ili prilagodite (npr. 3600 sekundi).



Slika 74. IPSEC postavke IKE faze 2

11. Kliknite OK za spremanje IPsec tunela.

Korak 2.: dodavanje statičke rute

1. Otvorite Network > Static Routes.
2. Kliknite Create New.
3. Destination: odaberite Subnet.
4. Destination IP/Mask: unesite udaljenu mrežu FortiGatea B (npr. 192.168.2.0/24).
5. Device: odaberite novokreirani IPsec VPN tunel kao sučelje (npr. FG_A_to_FG_B).
6. Kliknite OK za spremanje rute.

Korak 3.: Kreiranje sigurnosnih pravila

1. Otvorite Policy & Objects > Firewall Policy.
2. Kliknite Create New za pravila prometa iz lokalne mreže prema VPN-u.

- Name: LAN_to_FG_B
- Incoming Interface: lokalno sučelje LAN-a (npr. lan).
- Outgoing Interface: IPsec VPN tunel sučelje (npr. FG_A_to_FG_B).
- Source: adresni objekt za lokalnu mrežu (npr. 192.168.1.0/24 ili all).
- Destination: adresni objekt za udaljenu mrežu (npr. 192.168.2.0/24).
- Service: odaberite potrebne usluge ili ALL.
- Action: ACCEPT.

- NAT: isključite (Disable). (Ključno, jer promet mora zadržati izvornu IP adresu za povrat).
- Security Profiles: (Opcionalno, ali preporučljivo) uključite željene sigurnosne profile (antivirus, IPS, Application Control itd.).
- Kliknite OK.

3. Kliknite Create New za pravila povratnog prometa iz VPN-a prema lokalnoj mreži.

- Name: FG_B_to_LAN
- Incoming Interface: IPsec VPN tunel sučelje (npr. FG_A_to_FG_B).
- Outgoing Interface: lokalno sučelje LAN-a (npr. lan).
- Source: adresni objekt za udaljenu mrežu (npr. 192.168.2.0/24).
- Destination: adresni objekt za lokalnu mrežu (npr. 192.168.1.0/24).
- Service: odaberite potrebne usluge ili ALL.
- Action: ACCEPT.
- NAT: isključite (Disable).
- Kliknite OK.

Napomena: Identična, ali inverzna konfiguracija (s obrnutim lokalnim i udaljenim IP adresama i mrežama) mora se izraditi i na FortiGate B da bi tunel bio funkcionalan.

Kreiranje IPsec tunela (Phase 1 i Phase 2) preko CLI sučelja

Faza 1

```
config vpn ipsec phase1-interface
  edit "FG_A_to_FG_B"
    set interface "P2P-CPE-VLAN30"
    set type static
    set ip-version 4
    set remote-gw 203.0.113.10
    set psksecret "OVDJE_UNESI_PSK"
    set proposal aes256-sha256
    set dpd on-idle
    set dhgrp 20
    set keylife 86400
    set nat-traversal disable
  next
```

```
    end
```

Faza 2

```
    config vpn ipsec phase2-interface
      edit "FG_A_to_FG_B_p2"
        set phase1name "FG_A_to_FG_B"
        set proposal aes256-sha256
        set src-subnet 192.168.1.0 255.255.255.0
        set dst-subnet 192.168.2.0 255.255.255.0
        set pfs enable
        set dhgrp 20
        set keylife 3600
      next
    end
```

Dodavanje statičke rute:

```
    config router static
      edit 0
        set dst 192.168.2.0 255.255.255.0
        set device "FG_A_to_FG_B"
      next
    end
```

Dodavanje sigurnosnih pravila:

```
    config firewall policy
      edit 0
        set name "LAN_to_FG_B"
        set srcintf "lan"
        set dstintf "FG_A_to_FG_B"
        set srcaddr "192.168.1.0/24"
        set dstaddr "192.168.2.0/24"
        set action accept
        set service ALL
```

```
        set nat disable
    next
end
```

Dodavanje povratnih sigurnosnih pravila:

```
config firewall policy
    edit 0
        set name "FG_B_to_LAN"
        set srcintf "FG_A_to_FG_B"
        set dstintf "lan"
        set srcaddr "192.168.2.0/24"
        set dstaddr "192.168.1.0/24"
        set action accept
        set service ALL
        set nat disable
    next
end
```

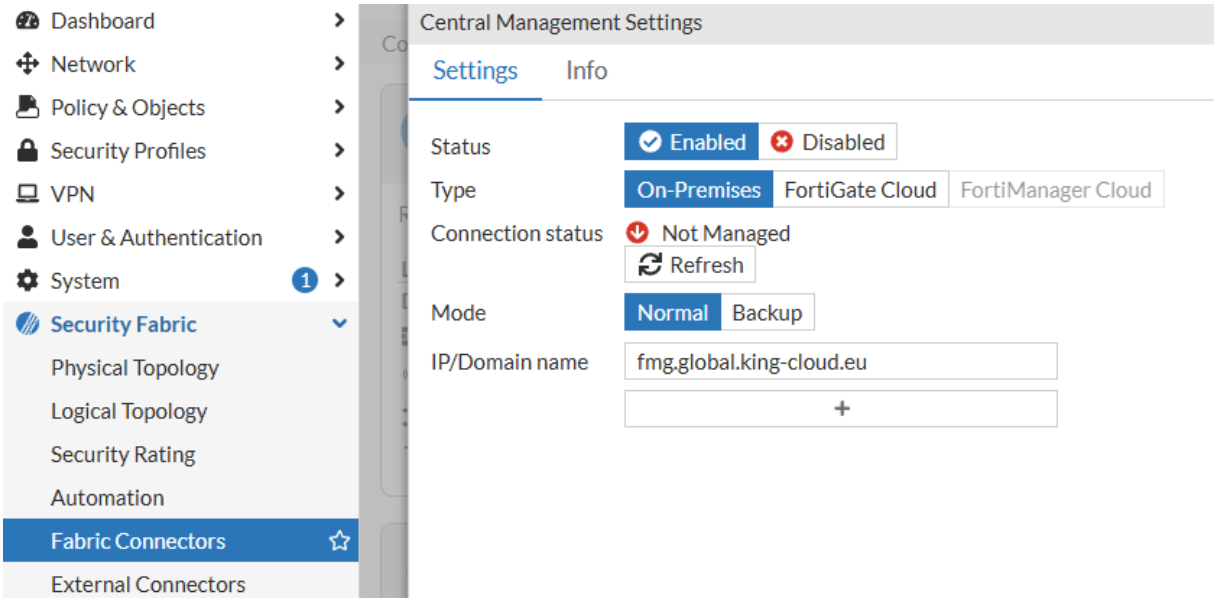
5.8.12. Spajanje FortiGatea na FortiManager GUI

Konfiguracija spajanja preko GUI-a (FortiGate strana)

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Security Fabric > Fabric Connectors.
3. Kliknite Central Management> FortiManager.
4. Unesite:
   - Status > Enabled
   - Type > On-Premises
   - Mode > Normal
   - IP/Domain name – IP adresa FortiManager servera.

5. Kliknite OK za spremanje.

6. Na FortiManageru odobrite novi uređaj u Unauthorized Devices listi i dodijelite mu odgovarajući ADOM.



Slika 75. Dodavanje FortiManagera

Treba napomenuti da je potrebno dodati izvorišnu adresu koja se prijavljuje na FortiManager sustav jer se nalazi na sučelju na kojem se primarno koristi privatna IP adresa. To se obavlja u komandnoj liniji.

Spajanje FortiGatea na FortiManager CLI

```
config system central-management
        set type fortimanager
        set serial-number " FMG-VMTM00000000" "FMG-VMTM00000001"
        set fmg "fmg.global.king-cloud.eu"
        set fmg-source-ip 82.214.96.131  <-- sekundarna IP
        end
```

6. Sustav za centralizirano upravljanje vatrozidima

U sklopu sustava e-Sveučilišta FortiManager je implementiran kao središnji upravljački alat za koordinaciju sigurnosnih postavki između različitih ustanova i mrežnih lokacija uključenih u sustav. Njegova uporaba omogućuje provođenje jedinstvenih sigurnosnih pravila na razini cijelog sustava, uz istodobno očuvanje autonomije pojedinih ustanova u sklopu definiranih ovlasti.

Primjena FortiManagera u ovom kontekstu usmjerena je ponajprije na operativno upravljanje i organizaciju administrativnih procesa. Uz jasno definiranu upravljačku cjelinu omogućeno je razdvajanje odgovornosti između središnje IT službe i lokalnih administratora, čime se osigurava učinkovito upravljanje bez narušavanja sigurnosnih standarda.

Centralizirani pristup upravljanju omogućuje brzu i koordiniranu provedbu promjena u slučaju sigurnosnih incidenata, regulatornih zahtjeva ili promjena u mrežnoj arhitekturi. Time se smanjuje vrijeme reakcije i povećava ukupna otpornost sustava na sigurnosne prijetnje.

FortiManager u sustavu e-Sveučilišta također služi kao osnova za dugoročni razvoj sigurnosne infrastrukture jer omogućuje jednostavno uključivanje novih ustanova i mrežnih segmenata bez potrebe za većim promjenama postojećeg modela upravljanja.

6.1. Uloga FortiManager sustava u mrežnoj infrastrukturi

U mrežnoj infrastrukturi e-Sveučilišta FortiManager ima ulogu koordinacijskog i nadzornog sustava koji povezuje distribuirane sigurnosne uređaje u jedinstveno upravljačko okružje. Njegova primarna zadaća nije tehnička konfiguracija sama po sebi, već uspostava kontroliranog procesa upravljanja sigurnosnim pravilima i odgovornostima.

Jedan od ključnih aspekata njegove uloge jest omogućivanje hijerarhijskog modela upravljanja, u kojem središnja razina definira osnovne sigurnosne smjernice, dok se njihova primjena i prilagodba odvijaju unutar unaprijed zadanih granica. Takav model omogućuje usklađenost cijelog sustava uz zadržavanje fleksibilnosti na lokalnoj razini.

FortiManager također podržava proces nadzora i praćenja stanja sigurnosne infrastrukture, pružajući središnji uvid u primjenu pravila i operativni status uređaja. U kombinaciji s analitičkim alatima omogućuje se pravodobno prepoznavanje potencijalnih sigurnosnih problema i koordinirana reakcija.

U kontekstu kontinuiteta rada FortiManager ima važnu ulogu u osiguravanju brze obnove sustava nakon poremećaja ili incidenta jer omogućuje standardizirani pristup vraćanju sigurnosnih postavki i ponovnom uspostavljanju normalnog rada.

Zahvaljujući ovakvoj ulozi FortiManager predstavlja bitan element mrežne sigurnosne arhitekture e-Sveučilišta, povezujući tehničke mogućnosti platforme s organizacijskim i operativnim zahtjevima sustava.

FortiManager time postaje središnja lokacija sigurnosne administracije sustava e-Sveučilišta, osiguravajući ne samo operativnu učinkovitost i kontrolu već i pouzdanu, skalabilnu i dugoročno održivu arhitekturu upravljanja vatrozidima.

FortiManager time postaje srce sigurnosne administracije sustava e-Sveučilišta, osiguravajući ne samo operativnu učinkovitost i kontrolu već i pouzdanu, skalabilnu i dugoročno održivu arhitekturu upravljanja vatrozidima.

6.2. Administrativne domene (ADOM) i logička podjela sustava

ADOM je virtualno upravljačko okruženje unutar FortiManager sustava, koje može sadržavati:

- vlastiti skup FortiGate uređaja
- zasebna sigurnosna pravila
- odvojene predloške konfiguracija
- vlastite korisničke ovlasti i administratore.

Tako svaki ADOM djeluje kao izolirana jedinica upravljanja, dok sve i dalje ostaje unutar jednoga fizičkog FortiManager sustava.

Prednosti korištenja ADOM-ova u e-Sveučilištu:

1. delegacija upravljanja po ustanovama

   Svaka obrazovna ustanova unutar sustava može imati svoj ADOM, čime lokalni administratori imaju pristup samo svojem FortiGate uređaju i pripadajućim konfiguracijama.

2. zasebna sigurnosna pravila i konfiguracije

   ADOM omogućuje svakoj ustanovi definiranje vlastitih pravila, predložaka i strukture, neovisno o drugim ustanovama, uz zadržavanje mogućnosti centralnog nadzora.

3. sigurnost i izolacija

   Promjene napravljene unutar jednog ADOM-a ne utječu na druge domene. Time se smanjuje rizik od nenamjernih pogrešaka i olakšava testiranje novih pravila ili konfiguracija.

4. učinkovitija organizacija velikih sustava

   U sustavu s desecima ustanova i uređaja ADOM-ovi omogućuju jasnu strukturu, bolju preglednost i jednostavnije održavanje.

Struktura i upravljanje ADOM-ovima:

- ADOM-ovi se kreiraju i konfiguriraju u FortiManager sučelju.

- Svakom ADOM-u mogu se dodijeliti:
    - uređaji (FortiGate)
    - administratori s različitim razinama ovlasti (*read-only, full access, audit*)
- vlastiti sigurnosni paketi i konfiguracijski predlošci.
- Jedan korisnik FortiManager sustava može imati pristup više administrativnih domena (ovisno o ulozi i pravima).

6.3. Upravljanje FortiGate uređajima s pomoću FortiManagera

FortiManager omogućuje središnje upravljanje svim FortiGate uređajima unutar sustava e-Sveučilišta, čime se pojednostavnjuje administracija, poboljšava nadzor i osigurava dosljedna primjena sigurnosnih pravila na svim lokacijama. Uređaji se registriraju i organiziraju unutar FortiManager sučelja, gdje ih je moguće pratiti, konfigurirati i nadzirati u realnom vremenu.

Proces upravljanja FortiGate uređajima obuhvaća:

1. dodavanje uređaja (engl. *Device onboarding*)
    - FortiGate uređaji mogu se ručno dodati s pomoću IP adrese i administratorskih vjerodajnica ili automatski prepoznati preko FortiManager agenta.
    - Nakon dodavanja uređaj se može pridružiti odgovarajućem ADOM-u (administrativnoj domeni).
2. prikupljanje konfiguracije i statusa
    - FortiManager redovito dohvaća trenutačnu konfiguraciju uređaja, njegov status, *firmware* verziju i logove.
    - svaka promjena na uređaju bilježi se u povijesti, čime se omogućuje verzioniranje i usporedba (engl. *diff*) konfiguracija.
3. centralna primjena promjena
    - Administrator može izraditi promjene lokalno unutar FortiManagera i zatim ih implementirati na jedan ili više uređaja istodobno.
    - Prije implementacije moguće je provesti validaciju pravila i pregled promjena koje će se primijeniti.
4. grupiranje i kategorizacija uređaja
    - Uređaji se mogu grupirati prema tipu, lokaciji, modelu ili ustrojstvenoj jedinici, što olakšava preglednost i masovno upravljanje.

5. praćenje stanja uređaja u stvarnom vremenu
    - FortiManager omogućuje pregled *online/offline* statusa uređaja, razinu iskorištenosti resursa (CPU, RAM, promet) te sigurnosne događaje koji se odnose na taj uređaj.
6. *Firmware* upravljanje i nadogradnje
    - S pomoću FortiManagera moguće je upravljati verzijama *firmwarea*, planirati nadogradnje i održavati dosljednost softverskih verzija u cijelom sustavu.

6.4. Upravljanje paketom sigurnosnih pravila (*policy package*)

Upravljanje sigurnosnim pravilima u FortiManager sustavu temelji se na konceptu *policy packagea*, koji omogućuje izradu, organizaciju i primjenu pravila prometa (pravila vatrozida) na jedan ili više FortiGate uređaja. Ovaj pristup omogućuje standardizaciju, skalabilnost i preciznu kontrolu sigurnosnih pravila u cijelom sustavu e-Sveučilišta.

Policy package je skup sigurnosnih pravila i objekata koji se definiraju unutar FortiManagera i zatim distribuiraju na jedan ili više FortiGate uređaja. Paket uključuje:

- *Firewall* pravila (*ingress* i *egress*)
- NAT pravila
- sigurnosne profile (antivirus, IPS, web filter itd.)
- objekte (IP adrese, grupe, usluge, zone)
- DNS, VPN i druge definicije (ovisno o strukturi paketa).

Funkcionalnosti upravljanja sigurnosnim pravilima:

1. izrada i uređivanje pravila
    - Pravila se kreiraju unutar FortiManager sučelja te organiziraju prema zonama, redoslijedu evaluacije i funkcionalnosti.
    - Moguće je koristiti predefinirane objekte ili ih izrađivati ručno.
2. validacija pravila
    - FortiManager provodi provjeru konzistencije prije primjene (npr. redoslijed pravila, konfliktne postavke, nepotpuni objekti).
3. primjena (engl. *install*) na uređaje
    - Nakon validacije sigurnosnih pravila instaliraju se (*deploy*) na jedan ili više FortiGate uređaja unutar pripadajućeg ADOM-a.
    - Moguće je selektivno instalirati samo promijenjene dijelove, čime se štedi vrijeme i smanjuje rizik od pogrešaka.

4. verzioniranje i povijest promjena
    - Svaka se izmjena bilježi, a prijašnje verzije paketa moguće je pregledati, usporediti i vratiti prema potrebi.
5. ponovna uporaba i skalabilnost
    - Jedno sigurnosno pravilo može se koristiti na više uređaja (npr. sve ustanove iste razine), uz mogućnost manjih lokalnih prilagodbi s pomoću *policy overrides*.

Prednosti pristupa sigurnosnih pravila:

- centralizirano definiranje pravila za sve ustanove i lokacije
- brza implementacija promjena na velik broj uređaja
- dosljedna primjena sigurnosnih pravila u cijelom sustavu
- pojednostavnjeno održavanje i praćenje sigurnosne strategije
- revizija i audit zahvaljujući zapisima svih promjena i verzijama paketa.

U kontekstu e-Sveučilišta sigurnosna pravila mogu sadržavati:

- standardna pravila za pristup internetu za studente, nastavnike i administraciju
- pravila za VPN promet između ustanova i prema središnjim servisima
- zajednička pravila filtriranja prometa
- specifična pravila za pojedine ustanove, uz mogućnost lokalne nadogradnje paketa.

Ovakav pristup omogućuje balans između centralne kontrole i lokalne fleksibilnosti.

U sustavu e-Sveučilište pri izradi i primjeni sigurnosnih pravila na FortiGate uređaje koristi se standardna konvencija imenovanja objekata.

Cilj je ovog pristupa omogućiti jedinstvene i prepoznatljive nazive objekata (npr. adresa, servisa, grupa, zone) između različitih lokacija – matične i udaljenih – čime se olakšava upravljanje, preglednost i održavanje konfiguracije.

1. Konvencija imenovanja

Sam naziv sigurnosnog pravila sadržava ID ustanove te CARNET ID čime se dobiva jedinstven naziv pravila koji je u konačnici dodijeljen uređaju koji se nalazi na ID lokaciji.

Primjer naziva pravila ID_999_1000_ZG-TESTNA, na svako pravilo kao *instalation target* dodijeljen je pripadajući FortiGate uređaj.

U sustavu je dogovoreno da predznak u nazivu objekta označava lokaciju kojoj objekt pripada:

- M- → označava matičnu lokaciju
- U1-, U2-, U3- → označavaju udaljene lokacije (prema njihovu rednom broju ili nazivu ustanove).

Tako svi objekti imaju jedinstvena i lako prepoznatljiva imena bez mogućnosti preklapanja između lokacija.

2. Primjeri objekata

Primjeri objekata na matičnoj lokaciji:

- M-EDUROAM
- M-GOSTI
- M-MGMT
- M-SERVIS1
- M-SERVIS2
- M-SERVIS3.

#	Name	Hit Count	From	To	NAT
1	LAN MREZA na INTERNET		port2	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131
2	MANAGEMENT na INTER...		M-MGMT	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131
3	EDUROAM na INTERNET		M-EDUROAM	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131
4	GOSTI na INTERNET		M-GOSTI	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131
5	SERVIS1 na INTERNET		M-SERVIS1	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131
6	SERVIS2 na INTERNET		M-SERVIS2	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131
7	SERVIS3 na INTERNET		M-SERVIS3	P2P-CPE-VLAN30	M-IP_POOL_82.214.96.131

Slika 76. Objekti i konvencija imenovanja

Primjeri objekata na udaljenim lokacijama:

- Lokacija 1: U1-EDUROAM, U1-GOSTI, U1-MGMT, U1-SERVIS1
- Lokacija 2: U2-EDUROAM, U2-GOSTI, U2-MGMT, U2-SERVIS1

3. Prednosti ovakvog pristupa

- Jedinstvenost i preglednost svih objekata unutar sigurnosnih pravila.
- Lakše održavanje i ažuriranje konfiguracije na više FortiGate uređaja.
- Jasna povezanost objekata s lokacijom kojoj pripadaju.
- Manja mogućnost grešaka pri sinkronizaciji i primjeni konfiguracija.

Prema istom načelu imenovanja kao i kod ostalih objekata u sustavu e-Sveučilište izrađuju se i IP Pool objekti koji se koriste za NAT-iranje prometa.

Nazivi IP Pool objekata prate konvenciju lokacijskog predznaka (npr. M-IP_POOL_XXX.YYY.ZZZ.WWW, U1-POOL_XXX.YYY.ZZZ.WWW), čime se jasno razlikuje kojem uređaju i mrežnom segmentu pripadaju.

Na matičnim lokacijama IP Poolovi definiraju se tako da:

za EDUROAM i MGMT mrežu koriste prvu dostupnu IP adresu, dok se za ostale mreže (npr. SERVIS1, SERVIS2, GOSTI) koristi sljedeća slobodna IP adresa iz dodijeljenog raspona.

Ova konvencija omogućuje dosljednost i jednostavnije upravljanje mrežnim pravilima u cijelom sustavu e-Sveučilište, posebno u okruženjima s više povezanih FortiGate uređaja.

6.5. Upravljanje konfiguracijama i predlošcima (*template*)

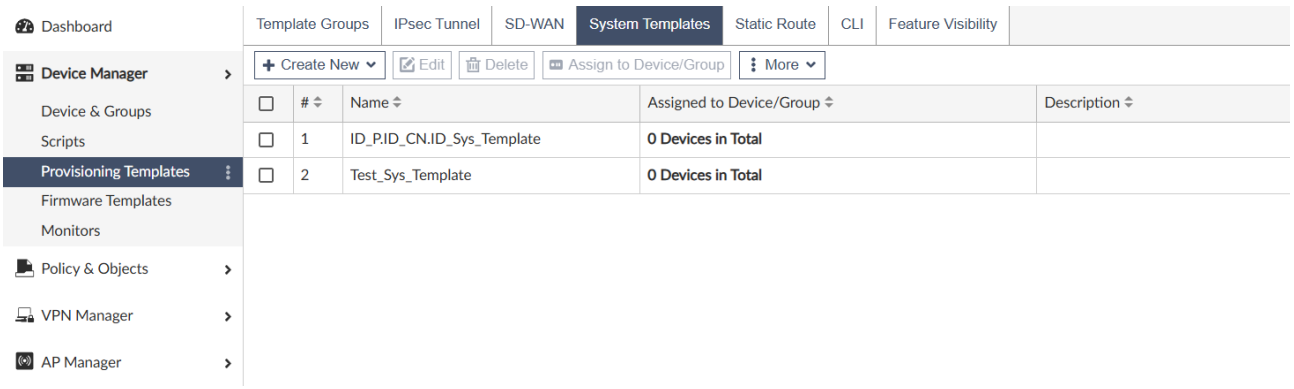
U ovom je poglavlju opisana izrada sistemskim predložaka kao i upravljanje konfiguracijama.

6.5.1. Izrada predložaka

Za svaki FortiGate unutar sustava e-Sveučilište izrađuje se poseban System Template koji sadržava osnovne parametre uređaja:

- CARNET DNS i NTP poslužitelji koriste se kao zadane postavke za sve uređaje, čime se osigurava sinkronizacija vremena i pouzdano razrješavanje domena.
- U *templateu* se definira izvorišni IP (*source* IP) na sekundarnu IP adresu koja je konfigurirana na P2P sučelju prema CARNET CPE uređaju. Tako sav promet prema CARNET servisima koristi ispravan izvorni IP.

Ovakva struktura predloška omogućuje brzu implementaciju novih uređaja i smanjuje mogućnost konfiguracijskih pogrešaka.



Slika 77. System Template na FortiManageru

6.5.2. Normalizacija sučelja u FortiManageru

Normalizacija sučelja (engl. *Interface Normalization* ili *Interface Mapping*) označava mehanizam u sustavu FortiManager koji omogućuje primjenu jedinstvenih sigurnosnih pravila i konfiguracijskih predložaka na više FortiGate uređaja, neovisno o njihovim fizičkim razlikama u nazivu i rasporedu mrežnih sučelja.

U praksi, različiti modeli FortiGate uređaja mogu imati različite nazive fizičkih portova (npr. *port1*, *wan1*, *internal*, *lan1*). Bez normalizacije sučelja, svako bi se sigurnosno pravilo moralo prilagođavati konkretnom uređaju, što bi znatno povećalo složenost upravljanja u okruženju s više lokacija.

Normalizacija sučelja uvodi logički (apstraktni) sloj između sigurnosnog pravila i stvarnoga fizičkog sučelja uređaja.

Svrha normalizacije sučelja

Osnovna svrha normalizacije je:

- omogućiti korištenje jedinstvenih naziva sučelja unutar *policy* paketa
- osigurati da se isti *policy package* može instalirati na više uređaja
- pojednostavniti upravljanje različitim modelima uređaja
- smanjiti mogućnost pogreške pri implementaciji konfiguracije.

Umjesto uporabe stvarnih naziva portova (npr. *port1*), u pravilima se koristi normalizirani naziv, primjerice:

- WAN
- LAN
- MGMT.

Tijekom instalacije konfiguracije FortiManager automatski mapira logički naziv na odgovarajuće fizičko sučelje ciljanog uređaja.

Način funkcioniranja u FortiManageru

Normalizacija sučelja konfigurira se unutar modula za upravljanje uređajima u FortiManageru.

Postupak se sastoji od sljedećih koraka:

1. Definiranje logičkih sučelja unutar ADOM-a.
2. Kreiranje ili uređivanje *Interface Mapping* tablice.
3. Mapiranje logičkog sučelja na konkretno fizičko sučelje pojedinog FortiGate uređaja.
4. Primjena konfiguracije postupcima instalacije (*Install Wizard*).

Primjer mapiranja:

Logičko sučelje	**Uređaj A**	**Uređaj B**
WAN	port1	wan1
LAN	internal	port2
MGMT	port3	port3

U ovom primjeru sigurnosno pravilo definirano kao „WAN → LAN“ bit će pravilno prevedeno na odgovarajuća fizička sučelja svakog uređaja.

Povezanost s *policy* paketima i predlošcima

Normalizacija sučelja izravno je povezana s:

- *Policy Package* konfiguracijom
- *Device Template* konfiguracijom
- centraliziranim upravljanjem više lokacija.

Ako se u *policy* paketu koristi normalizirano sučelje (npr. WAN), isti se paket može instalirati na različite FortiGate uređaje bez potrebe za izmjenom pravila.

Bez ovog mehanizma bilo bi potrebno izrađivati zasebne *policy* pakete za svaki model ili lokaciju, što bi povećalo administrativno opterećenje i rizik od nekonzistentne konfiguracije.

Prednosti primjene normalizacije

Primjena normalizacije sučelja u sustavu FortiManager donosi sljedeće prednosti:

- centralizirano i skalabilno upravljanje
- jedinstvena struktura sigurnosnih pravila
- lakša implementacija novih lokacija
- smanjena mogućnost konfiguracijskih pogrešaka
- jednostavnija zamjena uređaja bez izmjene *policy* paketa.

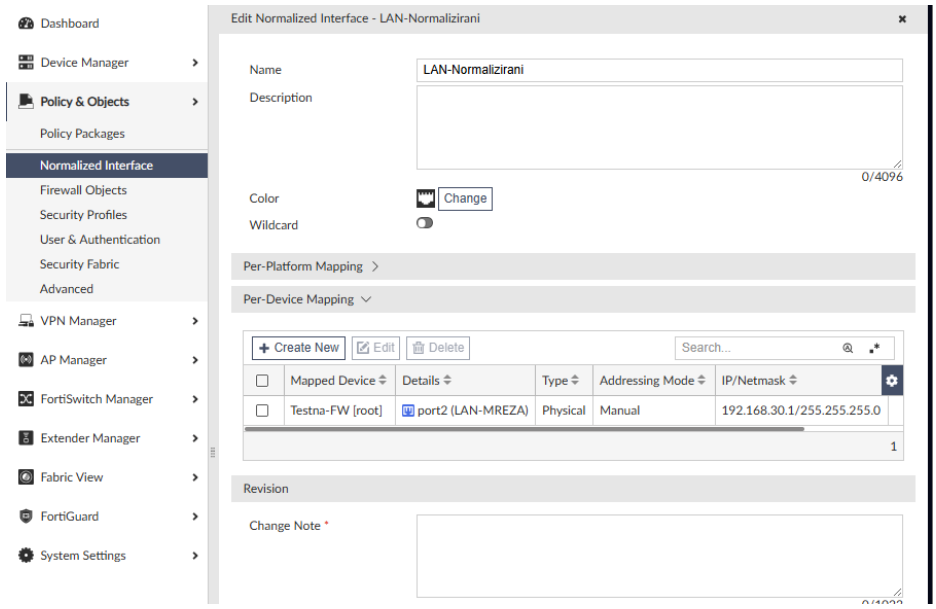
Normalizacija sučelja je mehanizam za učinkovito upravljanje većim brojem FortiGate uređaja unutar jedinstvenog FortiManager sustava, osobito u distribuiranim okruženjima s više lokacija i različitim modelima uređaja.

Konfiguracija normalizacije mrežnog sučelja

1. Podizbornik *Policy & Objects* > *Normalized Interface*

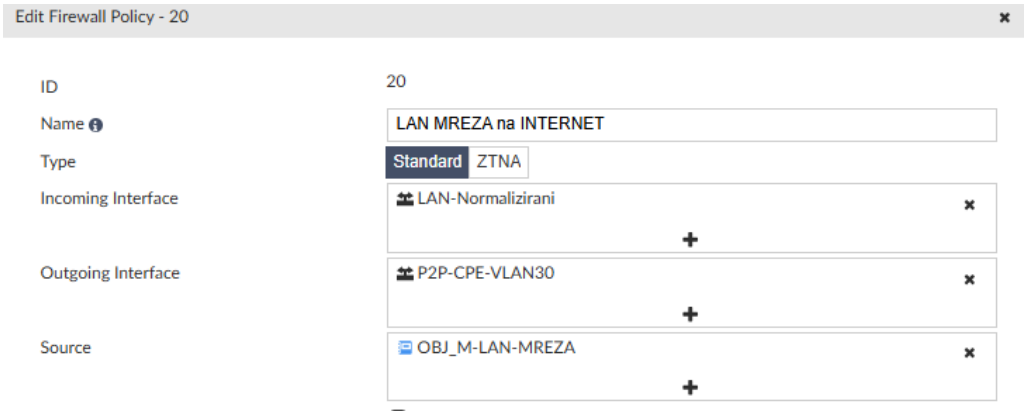
- Napravi novo (*eng. Create New*)

2. Unesi željeni naziv sučelja (npr. LAN-Normalizirani)
3. U izborniku Per-Device Mapping napraviti novo te mapirati željeni uređaj i fizičko sučelje
4. Snimiti trenutačne postavke



Slika 78. Normalizacija sučelja

Nakon što je učinjena konfiguracija, odnosno normalizacija mrežnog sučelja na željenom uređaju, možemo je primijeniti na sigurnosna pravila.



Slika 79. Primjena normaliziranog sučelja u sigurnosnim pravilima

6.6. Upravljanje pristupom i korisničkim ulogama

Upravljanje pristupom i korisničkim ulogama (engl. *„Access and Role Management“*) jedan je od ključnih segmenata sigurnosne arhitekture Fortinet rješenja. Njegov je cilj osigurati da

samo ovlaštene osobe imaju pristup administrativnim sučeljima, konfiguracijama i dijelovima mrežne infrastrukture te da razine pristupa budu definirane u skladu s njihovim odgovornostima i funkcijama.

6.6.1. Koncept upravljanja pristupom

FortiGate i FortiManager uređaji omogućuju granularnu kontrolu pristupa preko više razina autentikacije i autorizacije. U sklopu sustava e-Sveučilišta upravljanje pristupom provodi se centralizirano preko FortiManagera, dok FortiGate uređaji na pojedinim lokacijama provode autentikaciju korisnika prema definiranim pravilima i povezanim RADIUS poslužiteljima.

Autentikacija i dodjela prava temelje se na sljedećim načelima:

- načelo najmanjih privilegija (engl. „*Least Privilege*“) – korisnici imaju samo one ovlasti koje su nužne za obavljanje njihovih zadataka
- centralizirana kontrola – administratori pristupaju svim FortiGate uređajima preko FortiManagera s jasno definiranim ulogama
- reverzibilnost – svi pristupi, promjene i konfiguracijske izmjene bilježe se preko FortiManager logova.

6.6.2. Vrste korisnika i autentikacijski mehanizmi

FortiGate uređaji podržavaju više tipova korisnika i mehanizama autentikacije:

- lokalni korisnici – definirani izravno na FortiGate uređaju ili u FortiManager bazi. Koriste se u manjim okruženjima ili kao *fallback* mehanizam.
- RADIUS korisnici – autentikacija preko vanjskog RADIUS poslužitelja, najčešće korištena u sustavu e-Sveučilišta za pristup SSID-u *eduroam* te administrativni pristup sustavu.
- LDAP / Active Directory korisnici – omogućuju integraciju s postojećim korisničkim servisima ustanove.
- Administrator accounts (admin) – korisnici s ovlastima pristupa konfiguracijskim sučeljima FortiGate i FortiManager sustava.

FortiManager dodatno omogućuje kreiranje administrativnih domena (ADOM), unutar kojih se definiraju zasebni setovi korisnika i prava pristupa, čime se omogućuje neovisno upravljanje različitim ustanovama unutar jedinstvenog sustava.

6.6.3. Administratorske uloge

Administratori u FortiManager sustavu imaju različite razine privilegija, ovisno o funkciji i odgovornosti. Prema preporuci Fortineta i internim pravilima projekta e-Sveučilišta, definirane su osnovne uloge navedene u Tablici 9.

Uloga	Opis i prava
Restricted_User	Profil *Restricted User* nema omogućene sistemske privilegije te ima **isključivo *read-only* (samo za čitanje) pristup** svim privilegijama nad uređajima.
Super_User	Profil *Super User* ima **omogućene sve sistemske i uređajne privilegije**. Ovaj profil **nije moguće uređivati**.
Package_User	Profil *Package User* ima **read/write pristup pravilima (*policies*) i objektima**, dok za sistemske i ostale privilegije ima **samo *read-only* pristup**.
Password_Change_User	Profil *Password Change User* može **isključivo mijenjati lozinke** preko CLI-a ili API-a te **nema pristup FortiManager GUI-u niti drugim funkcionalnostima**.
No_Permission_User	Profil *No Permission User* nema omogućene **nikakve sistemske niti uređajne privilegije**.

Tablica *9*. Osnovne uloge

Uloge se mogu dodatno prilagoditi definiranjem *custom roles*, čime se precizno određuje pristup pojedinim dijelovima sustava (npr. Device Manager, Policy & Objects, FortiView).

6.6.4. Kreiranje korisnika i dodjela prava

U sustavu e-Sveučilišta navedena funkcionalnost realizirana je preko SAML SSO integracije s imeničkom infrastrukturom pojedine ustanove. Dodjela i uklanjanje administratorskih ovlasti provodi se izradom korisničkih računa i definiranjem pripadajućih prava u imeničkom sustavu pojedine ustanove, bez potrebe za ručnim kreiranjem administratorskih računa unutar FortiManager sustava.

Postupak ručnog dodavanja administratora opisan u nastavku odnosi se na administraciju središnjeg FortiManager sustava te nije dio standardnih administrativnih aktivnosti na razini ustanove.

Dodavanje korisnika u FortiManager sustav provodi se unutar izbornika System Settings → Administrators → Create New.

Pri kreiranju novoga korisnika definiraju se:

- Username – jedinstveno korisničko ime, preporučeno u formatu *ime.prezime*.

- Authentication type – lokalna lozinka, RADIUS, ili LDAP.
- Admin profile – izbor administratorske uloge prema tablici 6.7-1.
- ADOM access – odabir administrativne domene kojoj korisnik pripada.

U CLI načinu rada primjer definiranja lokalnog administratora s ograničenim pristupom izgleda ovako:

```
config system admin
  edit "lokalni_admin"
    set password <snažna_lozinka>
    set accprofile "read-only"
    set vdom "root"
  next
end
```

Za RADIUS autentikaciju koristi se unaprijed konfigurirani RADIUS poslužitelj, čija su namještanja opisana u poglavlju *Konfiguracija RADIUS servera za SSID eduroam.*

6.6.5. Autentikacija i integracija s RADIUS sustavom

U sustavu e-Sveučilišta autentikacija administratora i korisnika bežičnih mreža provodi se preko RADIUS poslužitelja ustanove ili centralnog SRCE/CARNET sustava. RADIUS poslužitelj definira se na FortiGate uređaju uz sljedeće parametre:

- IP adresa RADIUS poslužitelja
- port 1812 (autentikacija)
- *shared secret* između FortiGate uređaja i RADIUS-a
- *source IP* – javna IP adresa FortiGate uređaja.

Integracijom RADIUS-a u sustav omogućuje se centralno upravljanje korisničkim identitetima te jedinstvena autentikacija korisnika za više servisa (FortiGate, eduroam).

6.7. Nadogradnja komponenti sustava

Redovita nadogradnja (engl. *upgrade*) svih Fortinet komponenti ključna je za održavanje stabilnosti, sigurnosti i kompatibilnosti sustava e-Sveučilišta. Cilj je nadogradnje omogućiti da svi uređaji koriste podržane verzije *firmwarea*, s uklonjenim sigurnosnim ranjivostima i poboljšanim performansama te potpunom usklađenošću s funkcionalnostima Fortinet Security Fabric okruženja.

U sklopu projekta eSveučilišta nadogradnje odrađuje izvođač te se savjetuje da CARNET-ov sistemski inženjeri ovaj dio ne odrađuju samostalno kako bi se osigurao kontinuiran rad i spriječio eventualni gubitak funkcionalnosti ili stabilnosti rada uređaja. Izvođač će omogućiti

da se svaka nadogradnja ili sigurnosne zakrpe odrade pravovremeno uz *backup* konfiguracije u slučaju potrebe za vraćanjem prethodne verzije na uređaje.

Nadogradnje i sigurnosne zakrpe provodit će izvan radnog vremena istodobno na svim uređajima u sklopu projekta eSveučilišta te će se takav način održavanja primjenjivati tijekom cijelog razdoblja održavanja sustava. Redovite nadogradnje provodit će se uz pravovremenu najavu CARNET-ovim sistemskim inženjerima kako bi se omogućila pravovremena komunikacija i umanjio bilo kakav utjecaj na produkcijsku mrežu. Izvanredne nadogradnje provodit će se prema istom postupku, uz moguće kraće razdoblje najave zbog hitnosti primjene ažuriranja.

Da pri nadogradnji sustava ne bude problema, izvođač će detaljno pregledati napomene o izdanju (*release notes*) za svako ažuriranje radi provjere stabilnosti nove verzije i eventualnih konfiguracijskih funkcionalnosti koje donosi. Svaka nadogradnja zahtijeva prethodnu nadogradnju središnjeg sustava za upravljanje prije nadogradnje samih uređaja kako bi se izbjegli prekidi u funkcionalnostima.

6.7.1. Načela i preporuke za nadogradnju

Fortinet preporučuje provođenje nadogradnji u skladu s načelom postupnosti i provjere, uz prethodno testiranje u kontroliranom okruženju (npr. na testnoj lokaciji). U sklopu projekta e-Sveučilišta nadogradnje se provode **centralno preko FortiManager sustava**, čime se osigurava jedinstven nadzor, revizija promjena i mogućnost povratka na prethodnu verziju konfiguracije (engl. *rollback*).

Prije svake nadogradnje potrebno je:

- izraditi **sigurnosnu kopiju konfiguracije** svih uređaja (vidi poglavlje 6.11)
- provjeriti verziju *firmwarea* i kompatibilnost uređaja
- provjeriti dostupnost i status povezanosti između FortiManagera i uređaja
- osigurati stabilnu mrežnu povezanost i napajanje (posebno na udaljenim lokacijama).

6.7.2. Nadogradnja FortiGate uređaja

FortiGate uređaji čine središnji sigurnosni sloj mreže te njihova nadogradnja izravno utječe na dostupnost prometa. Zbog toga se nadogradnje planiraju izvan radnog vremena, uz prethodnu provjeru konfiguracijskih razlika i spremnost *rollback* mehanizma.

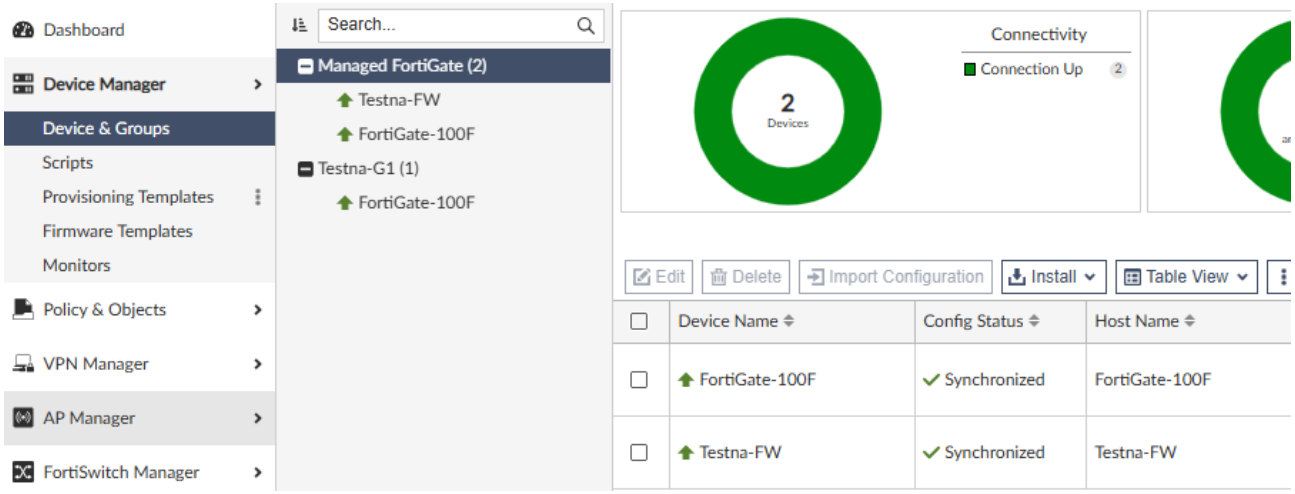
Postupak nadogradnje:

1. U FortiManageru otvoriti izbornik **Device Manager → Firmware Management**.
2. Odabrati FortiGate uređaj koji se nadograđuje.
3. Provjeriti trenutačnu verziju *firmwarea* i dostupne nove verzije (npr. *FortiOS 7.6.x*).
4. Odabrati opciju **Upgrade** i potvrditi pokretanje procesa.

Nakon dovršetka FortiGate se automatski ponovno pokreće te se povezuje s FortiManagerom.

6.7.3 Provjera i sinkronizacija nakon nadogradnje

Nakon svake nadogradnje važno je provjeriti usklađenost konfiguracija i povezanost uređaja.
U FortiManageru se to radi s pomoću izbornika **Device Manager → Config Status**.



Slika 80. Prikaz postavki Sync Status poruke

Statusi mogu biti:

- **In Sync** – konfiguracija uređaja i FortiManagera je usklađena.
- **Out of Sync** – konfiguracija na uređaju razlikuje se od pohranjene u FortiManageru.
- **Modified** – napravljene su promjene koje još nisu primijenjene.

Ako se pojavi upozorenje o nesinkroniziranosti, potrebno je odabrati:

Retrieve Config → OK

kako bi FortiManager povukao ažuriranu konfiguraciju s uređaja.

6.8. Izrada sigurnosne kopije konfiguracije i vraćanje konfiguracije

Redovita izrada sigurnosne kopije konfiguracije (engl. *Backup and Restore Configuration*) ključna je za održavanje operativne stabilnosti i sigurnosti sustava e-Sveučilišta. Sigurnosna kopija omogućuje brzo vraćanje sustava u funkcionalno stanje u slučaju greške, neuspješne nadogradnje, nepravilne izmjene konfiguracije ili fizičkog kvara uređaja.

U sklopu Fortinet infrastrukture kopije konfiguracija izrađuju se **centralno s pomoću FortiManager sustava**, a prema potrebi i lokalno na pojedinim uređajima (FortiGate, FortiSwitch, FortiAP).

6.8.1. Načela i preporuke

Fortinet preporučuje redovito kreiranje sigurnosnih kopija prema sljedećim pravilima:

- **prije svake nadogradnje** *firmwarea* ili većih promjena konfiguracije
- **nakon završetka implementacije** nove lokacije ili uređaja
- **periodično** (npr. jedanput tjedno ili mjesečno)
- **prije vraćanja na staru verziju *firmwarea*** (*rollback*).

Sigurnosne kopije konfiguracija trebaju biti:

- pohranjene na **sigurnoj lokaciji** (FortiManager server, NAS ili sigurnosni repozitorij)
- **verzionirane** – s jasnom oznakom uređaja, datuma i verzije *firmwarea*
- dostupne samo ovlaštenim osobama (primjena načela *least privilege access*).

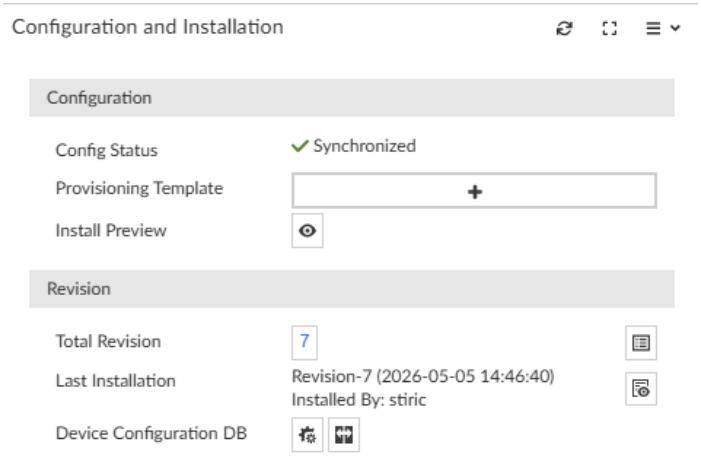
6.8.2. Izrada sigurnosne kopije s pomoću FortiManager sustava

FortiManager omogućuje centralizirano kreiranje i pohranu sigurnosnih kopija svih uređaja koji su pod njegovim nadzorom.

Postupak se izvodi preko **Device Manager** modula i može biti ručan ili automatiziran.

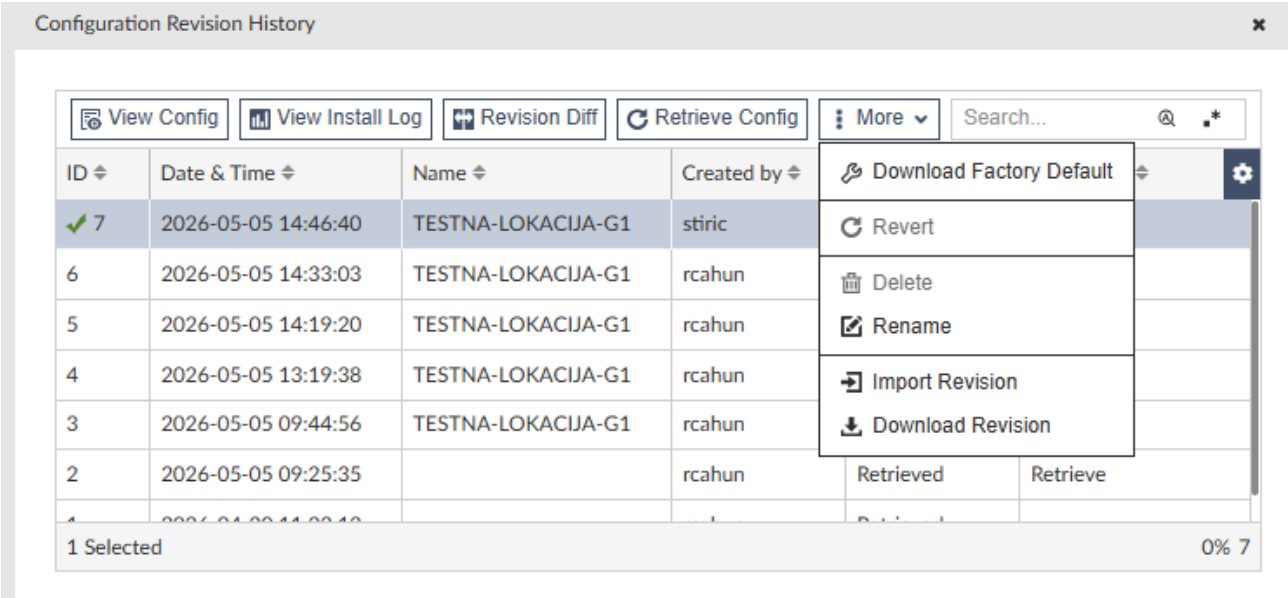
Svaki uređaj ima postavljeno automatsko kreiranje kopije sustava pri spremanju izmjena. Riječ je o sustavu revizija koji se unutar sustava FortiManager prikazuje kao sigurnosna kopija (*backup*) konfiguracije te administratorima omogućuje spremanje trenutačne konfiguracije ili vraćanje na neku od prethodnih inačica.

Administratori u svakom trenutku mogu pristupiti revizijama preko widgeta *Configuration and Installation.*



Slika 81. Prikaz postavki widgeta Configuration and Installation.

Kako bi se pristupilo reviziji na uređaju, potrebno je kliknuti na broj naveden pod Total Revision unutar kojega se otvara dodatni izbornik s mogućnostima pregleda i uređivanja revizija, odnosno sigurnosnih kopija uređaja.



Slika 82. Prikaz postavki widgeta Configuration and Revision

Za pregled trenutačne revizije, odnosno sigurnosne kopije konfiguracije uređaja moguće je odabrati *View Config* ili *Installation Log.* Tako se mogu provjeriti eventualni problemi koji su se pojavili pri kreiranju revizije ili tijekom primjene konfiguracije na uređaje u produkcijskom okruženju. Osim toga, pod izbornikom *Revision Diff* dostupna je usporedba promjena koja prikazuje sve izmjene učinjene u odabranoj inačici konfiguracije u odnosu na prethodnu verziju. U istom se sučelju nalazi izbornik *Retrieve Config* kojim se konfiguracija može dohvatiti izravno s uređaja ako je na uređaju išta bilo konfigurirano.

Sustav također omogućuje uvoz (*Import*) i preuzimanje (*Download*) revizija, odnosno sigurnosnih kopija konfiguracije, čime je omogućeno i ručno arhiviranje *backupa*. U slučaju potrebe za vraćanjem na prethodnu inačicu konfiguracije, potrebno je odabrati željenu reviziju, otvoriti izbornik *More* te odabrati podizbornik *Revert*. Time se na uređaj primjenjuje odabrana prethodna verzija konfiguracije.

Nova revizija automatski se kreira pri svakom spremanju konfiguracije, odnosno primjene izmjena na uređajima, čime je omogućeno automatizirano upravljanje sigurnosnim kopijama uz mogućnost ručnog odabira inačice konfiguracije koju administrator želi koristiti na uređaju.

6.8.3. Izrada lokalne sigurnosne kopije na FortiGate uređaju

Osim središnje pohrane, moguće je napraviti lokalnu kopiju konfiguracije izravno na FortiGate uređaju.

Ovaj pristup koristan je u slučajevima lokalne administracije ili izvanrednih intervencija.

GUI postupak:

1. Prijaviti se na FortiGate mrežno sučelje.
2. Odabrati Dashboard → System Information → System Configuration → Backup.
3. Odabrati način pohrane:
    - To File – preuzimanje konfiguracije na lokalno računalo
    - To USB Disk – ako je USB memorija spojena na uređaj
    - To FortiManager – centralno spremanje.

CLI primjer:

execute backup config tftp FGATE_BACKUP_20251026.conf 192.168.10.10

pri čemu je 192.168.10.10 IP adresa TFTP poslužitelja.

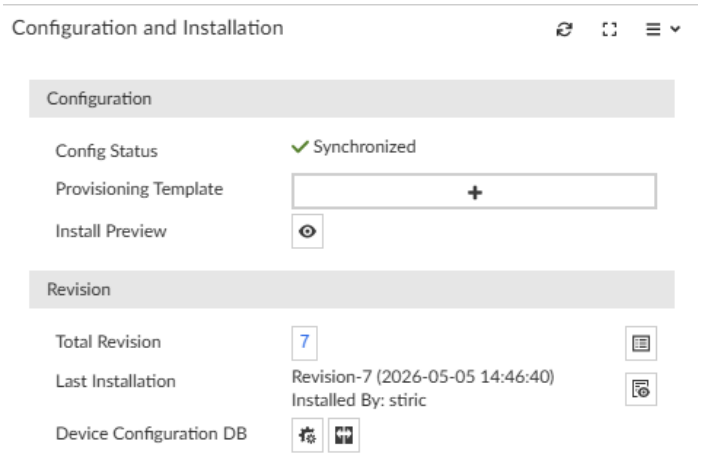
6.8.4. Vraćanje konfiguracije (*Restore*)

Vraćanje konfiguracije koristi se u slučaju potrebe za obnovom sustava na poznatu stabilnu verziju.
Konfiguracija se može vratiti iz FortiManager repozitorija ili s lokalne datoteke.

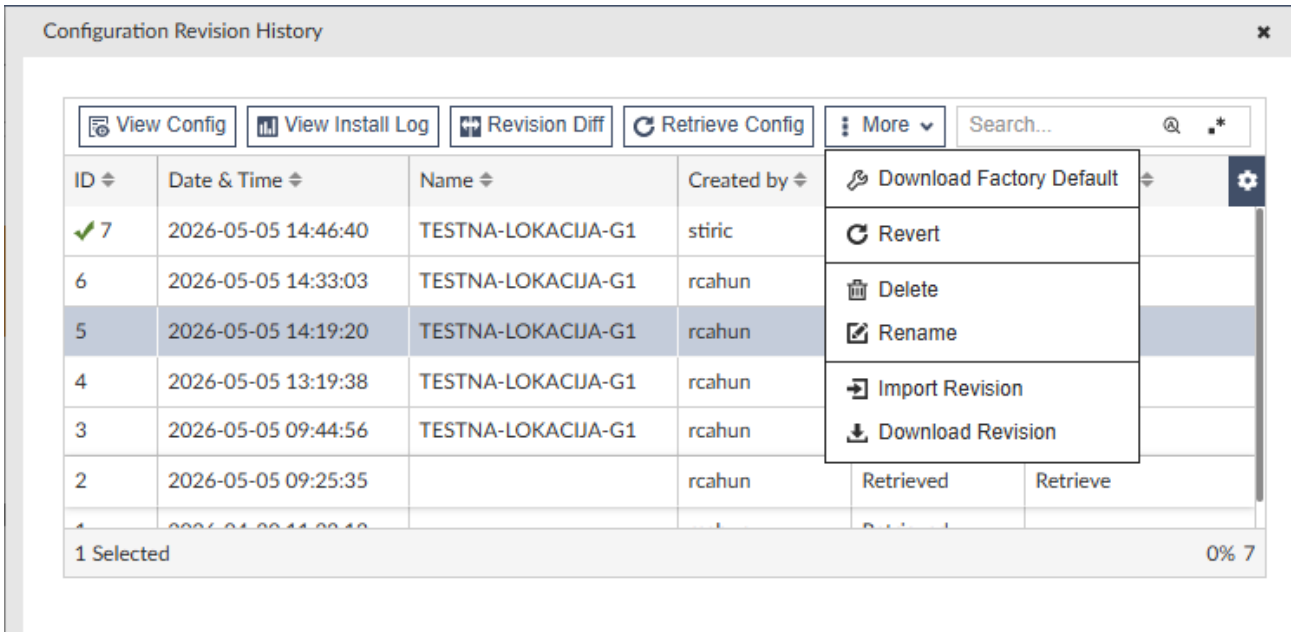
Vraćanje preko FortiManagera

1. U **Device Manager** odabrati uređaj.
2. Navigiranje do widgeta Configuration and Installation
3. Klik na brojku trenutačne revizije
4. Kliknuti **Revert** → **Configuration**.
5. Odabrati prethodno spremljenu verziju konfiguracije.
6. Potvrditi vraćanje i pokrenuti instalaciju.

FortiManager preuzet će konfiguracijsku datoteku na uređaj i pokrenuti postupak sinkronizacije.



Slika 83. Prikaz postavki vraćanja konfiguracije



Slika 84. Prikaz postavki Revert opcije

Vraćanje preko CLI-a

Ako nije dostupan FortiManager, vraćanje se može napraviti izravno s uređaja:

execute restore config tftp FGATE_BACKUP_20251026.conf 192.168.10.10

Nakon završetka uređaj će se automatski ponovno pokrenuti i primijeniti novu konfiguraciju.

6.8.5 Provjera integriteta i testiranje nakon vraćanja

Nakon vraćanja konfiguracije preporučuje se provesti sljedeće korake:

- provjeriti status povezanosti uređaja u FortiManageru (mora biti *In Sync*)
- pregledati logove i potvrditi uspješnu sinkronizaciju
- testirati ključne funkcionalnosti (internetska povezanost, VLAN-ovi, SSID-evi, RADIUS autentikacija)
- napraviti ping testove prema *gateway* adresama i FortiManageru.

U slučaju nesukladnosti moguće je vratiti stariju sigurnosnu kopiju (*rollback*).

7. Sustav za centralizirano upravljanje preklopnicima i bežičnim pristupnim točkama

Zbog kompleksnosti infrastrukture na projektu eSveučilišta implementiran je sustav Meraki Dashboard. Peko središnje upravljačke konzole sustav omogućuje upravljanje svim preklopnicima i bežičnim pristupnim točaka, bilo na razini pojedine ustanove, više ustanova ili cijele organizacije. Uz potrebnu skalabilnost za infrastrukture koja predviđa širenje usluga ili broja korisnika, Meraki Dashboard nudi mogućnosti automatizacije, revizije i jednostavan način za upravljanje kompletnom mrežnom infrastrukturom na razini preklopnika i bežičnih pristupnih točaka, kao i praćenje logova i zdravlja korisnika spojenih na mrežu. Spajanje na Meraki Dashboard odrađuje se preko mrežnog preglednika po želji stručnog osoblja, a preporučeni preglednici su: Chrome, Firefox, Edge i Safari. Dodatan uvjet je korištenje preglednika koji su ažurirani na zadnju verziju aplikacija. Korištenje zastarjelog softvera nije preporučljivo jer u tom slučaju Cisco ne jamči da će sve vizualne funkcije biti prikazane. Preglednikom se spajamo na https://e-sveucilista.sso.meraki.com gdje je potrebno napraviti račun kojim će se stručno osoblje ulogirati i administrirati svoju organizaciju.

Prednosti centraliziranog upravljanja:

- konzistentnost propuštenih mreža na svim uređajima, neovisno o lokaciji
- brza primjena izmjena i novi sigurnosni paketi bez potrebe za lokalnim pristupom uređajima
- centralna kontrola konfiguracija, *firmwarea*, korisničkih prava i logova
- smanjenje administrativnog opterećenja i mogućnost podjele odgovornosti dodjeljivanjem organizacija i pripadnosti organizacijama
- bolja skalabilnost u slučaju budućeg proširenja sustava.

Osnovne funkcionalnosti Meraki Dashboard sustava:

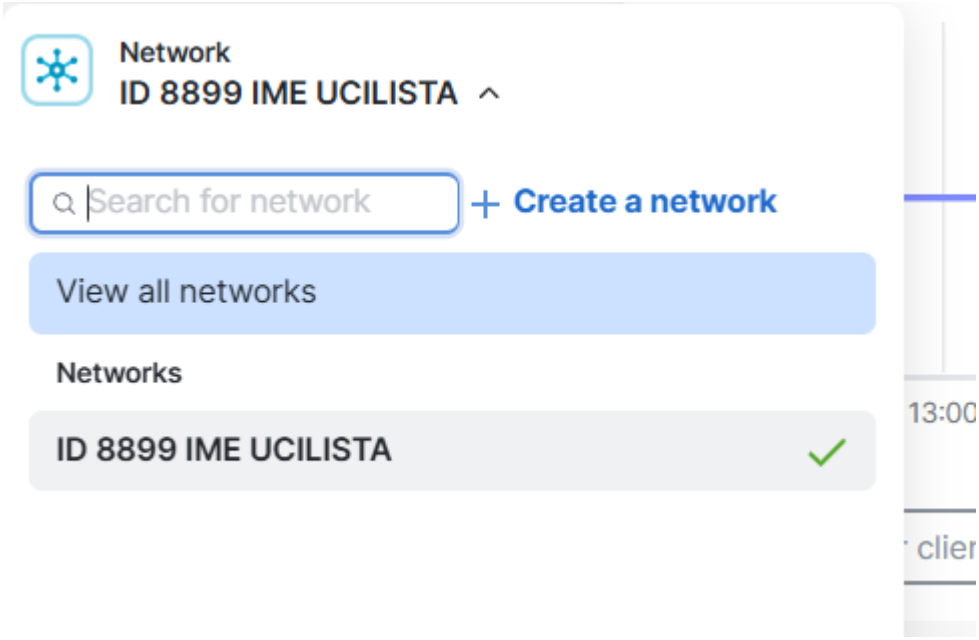
- upravljanje konfiguracijama i pravilima svih Cisco uređaja u sklopu projekta
- upravljanje vatrozidima i nadogradnjama
- upravljanje korisničkim pristupom i ovlastima
- pregled i analiza mrežnih i sigurnosnih događaja
- upravljanje preklopnicima i bežičnim pristupnim točkama s Cisco Meraki softverom.

Administrator sustava može dodati jednu organizacijsku jedinicu unutar Cisco Meraki dashboarda te njome upravljati. Na navedenu organizaciju povezane su mreže, odnosno Network lokacije koje simboliziraju ogranke neke institucije. Ogranci su raspodijeljeni tako

lokacija koja je sastavljena od jednog vatrozida, određenog broja preklopnika i određenog broja bežičnih pristupnih točaka može imati samo jednu organizacijsku i mrežnu jedinicu.

Ako ustanova ima nekoliko udaljenih lokacija, a svaka od njih ima neku vrstu usmjerivača ili vatrozida na svojem perimetru, svaka dodana lokacija bit će izdvojena mreža, odnosno nalazit će se pod izdvojenim izbornikom Network koji nam daje granularan pregled udaljenih lokacija na sveučilištu.

Izdvojena varijanta je kada lokacija ima nekolicinu lokalnih prespoja, takva lokacija bit će dodana kao jedna mreža jer je riječ o provučenoj L2 domeni, odnosno mreži koja ne zahtijeva korištenje IP protokola kako bi se povezala sa središnjom lokacijom.



Slika 85. Prikaz izbornika za kretanje po organizacijama i mrežama ustanove

U sljedećim poglavlja detaljno ćemo obraditi sve važnije funkcije Cisco Meraki sustava, uključujući upravljanje konfiguracijama, korisnicima i mrežnim uređajima.

7.1. Cisco Meraki preklopnici

Cisco Meraki preklopnici sastavni su dio mrežne infrastrukture te se u sustavu e-Sveučilišta koriste kao pristupni preklopnici koji omogućuju povezivanje krajnjih uređaja i bežičnih pristupnih točaka u jedinstvenu sigurnosnu mrežu pod nadzorom Cisco Meraki Dashboarda.

7.2. Konfiguracija Cisco Meraki preklopnika

Preko Cisco integracije sustava u Meraki Dashboard moguće je dodati sve uređaje koji podržavaju Meraki inačicu vatrozida. Tako je moguće dodati sve Cisco uređaje isporučene unutar projekta e-Sveučilišta. Prema potrebi i postojeća oprema na lokacijama može migrirati u Meraki okruženje te administrirati preko istoga nadzornog alata.

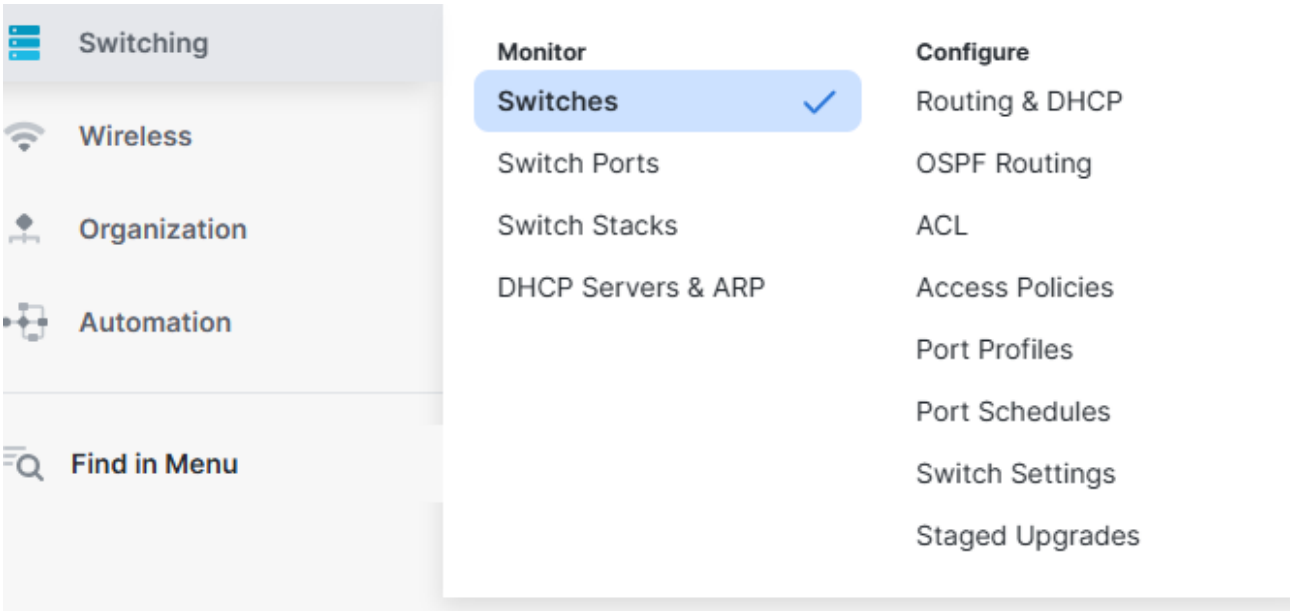
Konfiguracija sustava intuitivna je i dopušta administratorima upravljanje mrežom velikog razmjera s minimalnim utroškom vremena.

7.2.1. Dodavanje novog preklopnika u Meraki Dashboard

Koraci koje slijedimo kako bismo dodali novi uređaj na Meraki sustav su sljedeći:

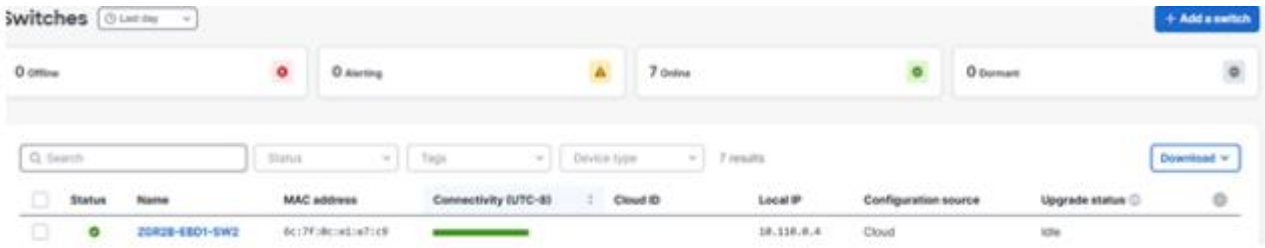
1) navigacija unutar organizacijske jedinice
2) navigacija unutar mrežne jedinice
3) navigacija unutar izbornika *Switching*, odnosno preklapanje
4) odabir opcije preklopnik, odnosno *Switch*
5) odabir opcije *Add a switch*, odnosno dodaj preklopnik.

Na slici ispod teksta označen je izbornik unutar kojega se odabire pristup konfiguraciji i dodavanju novih preklopničkih uređaja unutar Meraki Dashboarda. Odabirom opcije *Switches* dobivamo prikaz trenutačno postavljenih uređaja koji su aktivni na lokaciji i pristup izborniku za dodavanje novog uređaja na ustanovu.



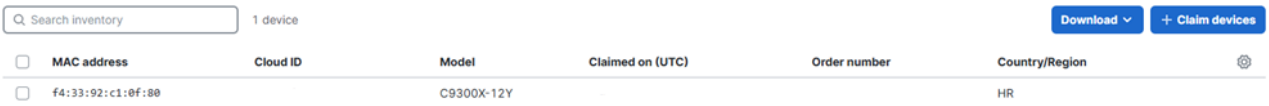
Slika 86. *Prikaz izbornika za prikaz preklopničke opreme ustanove*

Naveden je prikaz preklopničke opreme na ustanovi gdje je vidljivo upravljanje preklopnicima, gumb za dodavanje nove preklopničke opreme kao i osnovne informacije o opremi.



Slika 87. Prikaz izbornika za izlist aktivne preklopničke opreme ustanove

Odabirom opcije *Add a switch*, odnosno dodavanjem preklopnika sustav nas vodi u izbornik unutar kojega se nalaze neregistrirani uređaji koje dodajemo ustanovi. Uređaj je moguće dodati njegovim dodavanjem i klikom na *Claim devices*, odnosno dodaj uređaj. Izbornik za dodavanje uređaja priložen je u slici ispod teksta.

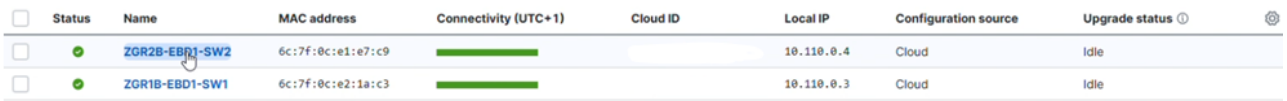


Slika 88. Prikaz izbornika za dodavanje uređaja na organizaciju

Administratorima sustava napominjemo da će uređaje dodavati vanjski suradnici koji će raditi na održavanju, stoga smo opisali proceduru dodavanja novog uređaja u mrežu kako bi se olakšao taj proces.

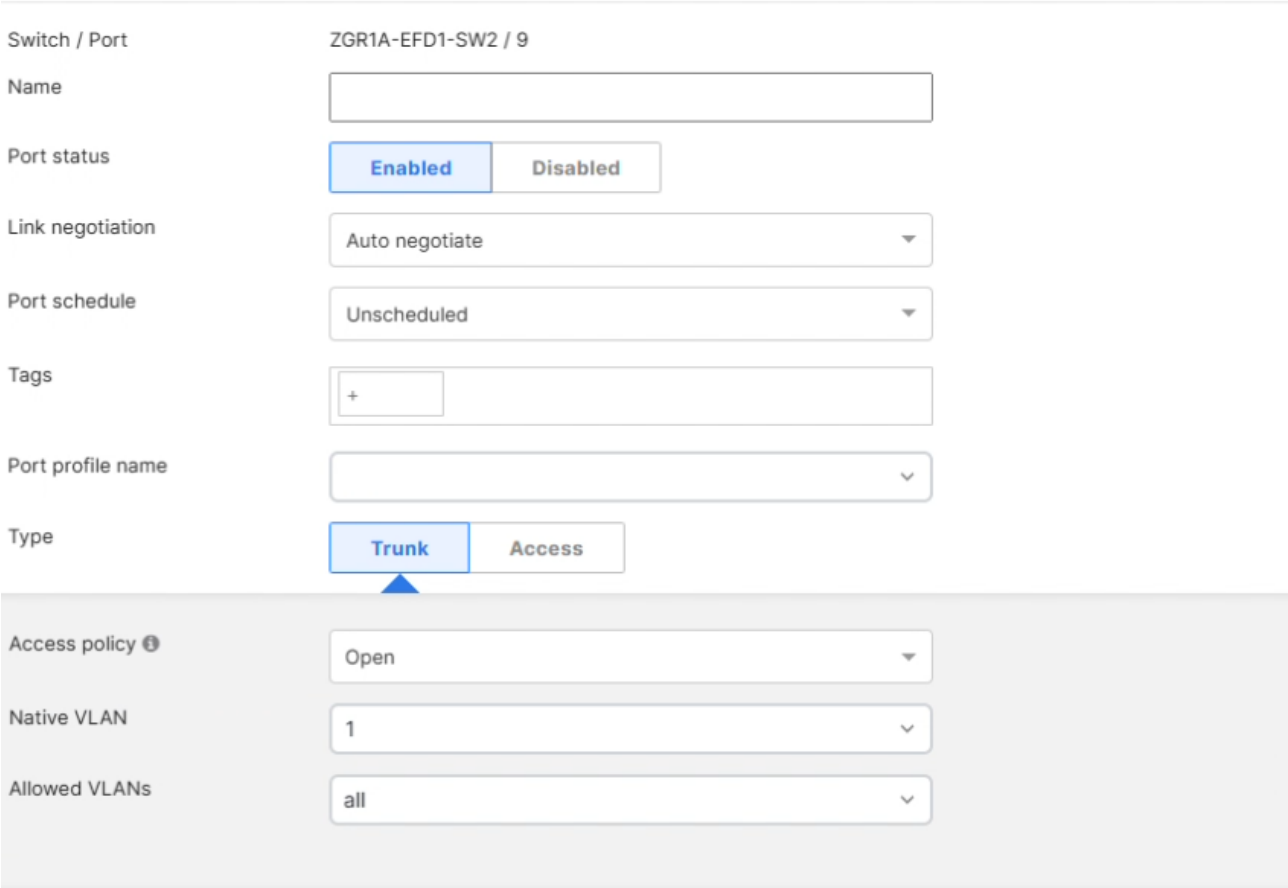
7.2.2. Konfiguracija sučelja

Konfiguracija sučelja na uređajima pod kontrolom Meraki Dashboard upravljačkog sučelja odrađuje se tako da se u izborniku *Switching* odabere podizbornik *Switches*. Odabirom podizbornika dobivamo prikaz svih aktivnih mrežnih preklopnika dodanih na mrežu korisnika. Takav pregled nalazi se ispod teksta te nam omogućuje konfiguraciju svakog preklopnika koji je dodan unutar mrežne organizacijske jedinice.



Slika 89. Prikaz izbornika Switches

Klikom na preklopnik kojim želimo administrirati dolazimo do kratkog sažetka podataka o uređaju, a u izborniku *Ports* pojavljuje se opcija *Configure ports on this switch.* Na ovaj način biramo koje sučelje želimo konfigurirati iz izbornika. Nakon odabira sučelja pojavljuje se opcija odabira konfiguracije koja se nalazi ispod teksta.



Slika 90. *Prikaz izbornika za konfiguraciju fizičkog sučelja Meraki preklopnika*

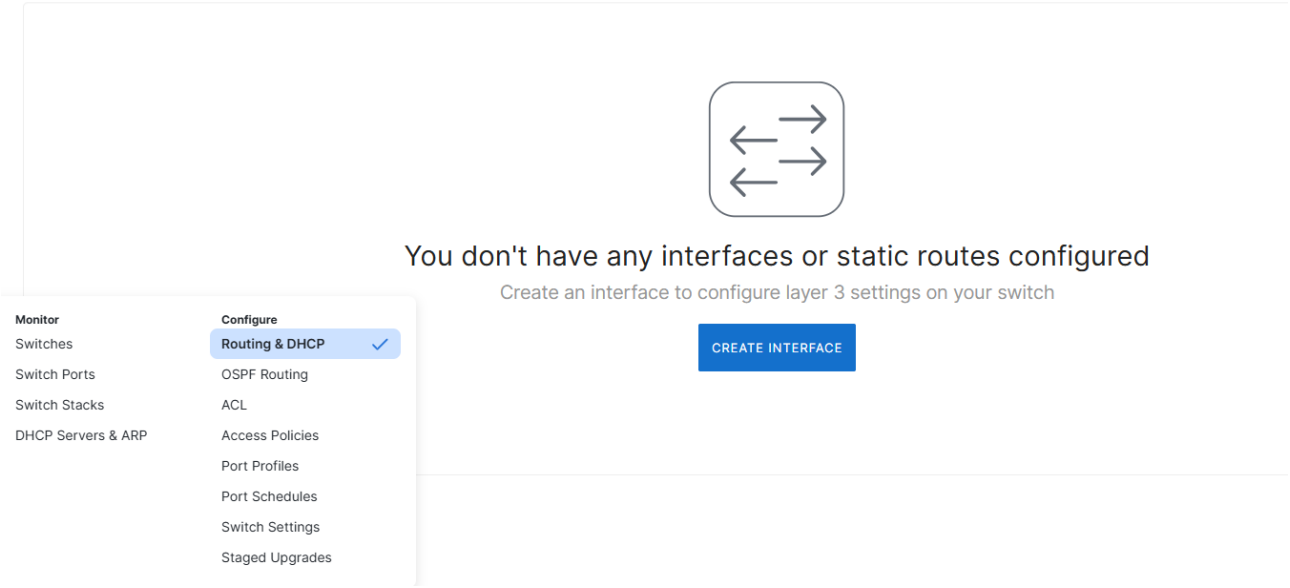
Možemo konfigurirati svaku stavku fizičkog sučelja, dodavati novo ime za svako sučelje, omogućiti ili onemogućiti rad sučelja, odrediti brzinu kojom želimo da sučelje radi ili da koristi opciju automatskog pregovora o brzini s drugim uređajima. Uz to, možemo konfigurirati svako sučelje da radi samo u željenom intervalu, tagirati promet sa sučelja i stavljati posebne profile na sučelje, kao i omogućiti ili onemogućiti rad STP-a, odnosno Spanning tree protokola. Prikazana je mogućnost uključivanja i isključivanja PoE funkcionalnosti u slučajevima kad je potrebno testirati ispravnost rada uređaja koji koriste mrežno napajanje.

Za svako sučelje moguće je odabrati dvije opcije rada: *Trunk* i *Access*. U *Trunk* načinu rada administrator može odabrati odgovarajući *Access policy* koji će biti pridružen sučelju, definirati nativnu mrežu koja će prolaziti sučeljem bez „tagiranja“ te odraditi popis dopuštenih mreža. Opcije dostupne u načinu rada *Access* slične su onima u načinu rada *Trunk.*

Administrator može odabrati *Access policy* koji će biti pridružen sučelju te VLAN koji će se koristiti na tom sučelju. Moguće je definirati i *Voice VLAN*, odnosno mrežu namijenjenu telefonskim uređajima kako bi se glasovni promet mogao ispravno prepoznati i označiti, što omogućuje pravilnu primjenu QoS (Quality of Service) funkcionalnosti i odgovarajuće prioritiziranje prometa.

7.2.3. Kreiranje virtualnih sučelja na Meraki preklopnicima

Kreiranje sučelja na Meraki preklopnicima odrađuje se odabirom izbornika *Switching*, nakon čega se odabire podizbornik *Routing & DHCP*. Odabirom izbornika nudi se opcija kreiranja virtualnog sučelja na koje je moguće dodati IP adresu te može služiti kao DHCP poslužitelj koji klijentima daje IP adrese koje mogu koristiti. Zbog specifičnog načina implementacije opreme unutar projekta većina virtualnih točaka postavljena je na vatrozidima te se ondje određuje IP adresni prostor, funkcionalnosti DHCP-a i pravila propuštanja za pojedine mreže, dok je većina preklopnika ovdje kako bi funkcionirala tako da odrađuju *switching*, ne i *forwarding* opciju, odnosno rade na drugom sloju OSI modela, dok vatrozidi preuzimaju funkcionalnosti viših slojeva OSI modela.

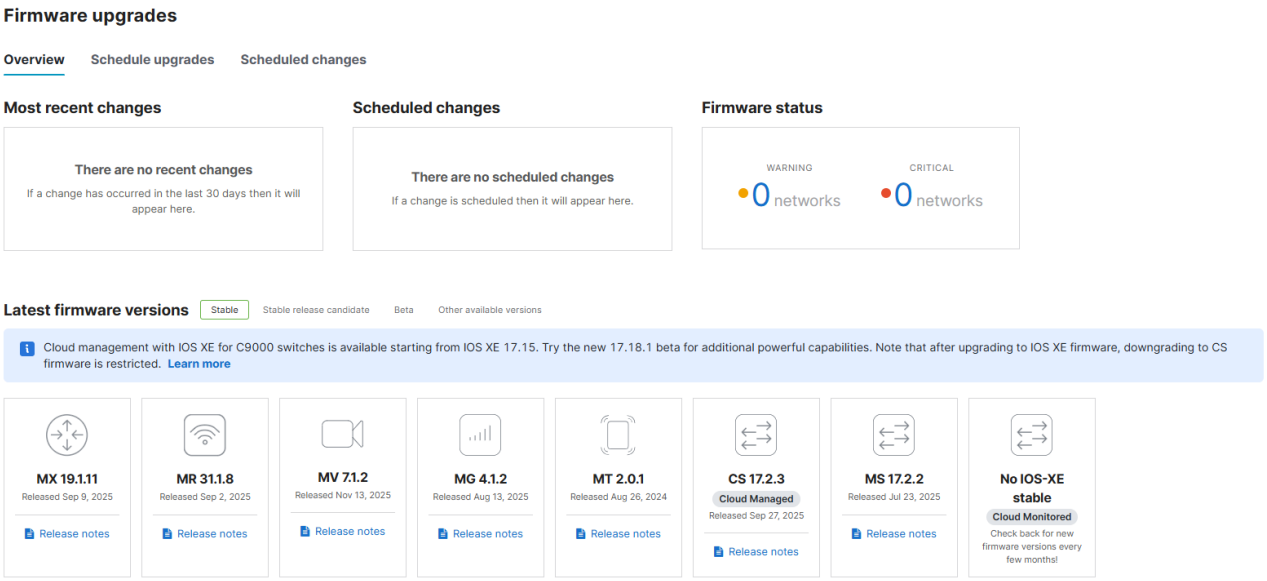


Slika 91. *Prikaz izbornika za konfiguraciju virtualnog sučelja Meraki preklopnika*

7.2.4. Nadogradnja Cisco Meraki uređaja

Nadogradnja Cisco Meraki uređaja kontrolira se preko upravljačke konzole Meraki Dashboard, bilo odmah ili s vremenskim odmakom, kako bi se pojednostavnilo upravljanje velikom količinom uređaja, smanjila mogućnost pogrešaka pri nadogradnji sustava i olakšalo

vraćanje konfiguracije na prethodne postavke u slučaju neuspjele nadogradnje. Upravljanje nadogradnjama odrađuje se preko izbornika *Firmware upgrades* koji se nalazi u izborniku *Organization*.



Slika 92. Prikaz izbornika za ažuriranje Firmwarea

7.2.5. Spremanje konfiguracije na Cisco Meraki uređajima

Spremanje konfiguracije na Cisco Meraki uređajima kontrolira se preko upravljačke konzole Meraki Dashboard. Izmjene se primjenjuju na uređaje potvrđivanjem odgovarajućih opcija unutar pojedinog izbornika. Ako se promjene odnose na jedan uređaj, primjenjuju se isključivo na njega. Međutim, kada se uređuje funkcionalnost koja je zajednička za više uređaja ili se istodobno upravlja većim brojem uređaja, promjene se primjenjuju na sve uređaje na kojima se navedena funkcionalnost koristi. U slučaju izmjena *Access Policy* pravila koja su definirana na razini organizacije promjene će se automatski primijeniti na svim uređajima i lokacijama na kojima je pridružen odgovarajući profil.

Cisco Meraki preklopnici ključni su dio mrežne infrastrukture te se u sustavu e-Sveučilišta koriste kao pristupni preklopnici koji omogućuju povezivanje krajnjih uređaja i bežičnih pristupnih točaka u jedinstvenu sigurnosnu mrežu pod nadzorom Cisco Meraki Dashboarda.

Preko Cisco integracije uređaja u Meraki Dashboard unutar kojega je moguće dodati svaki uređaj koji na sebi ima Meraki inačicu vatrozida moguće je dodati sve Cisco uređaje isporučene unutar projekta e-Sveučilišta. Prema potrebi, opremu koja se već nalazi na lokacijama, a nije obuhvaćena projektom e-Sveučilišta, moguće je prebaciti na Meraki okruženje te ju administrirati preko istoga nadzornog alata. Jedini uvjet za ovakvo prebacivanje je stavljanje Meraki vatrozida na takve uređaje.

Sama konfiguracija intuitivna je i dopušta administratorima upravljanje mrežom velikog razmjera s minimalnim utroškom vremena.

7.3. Konfiguracija Meraki bežičnih pristupnih točaka

Cisco Meraki bežične pristupne točke ključni su dio mrežne infrastrukture te se u sustavu e-Sveučilišta koriste kao pristupni uređaji koji omogućuju povezivanje krajnjih uređaja u jedinstvenu sigurnu mrežu pod nadzorom Cisco Meraki Dashboarda.

Sama konfiguracija intuitivna je i dopušta administratorima upravljanje mrežom velikog razmjera s minimalnim utroškom vremena.

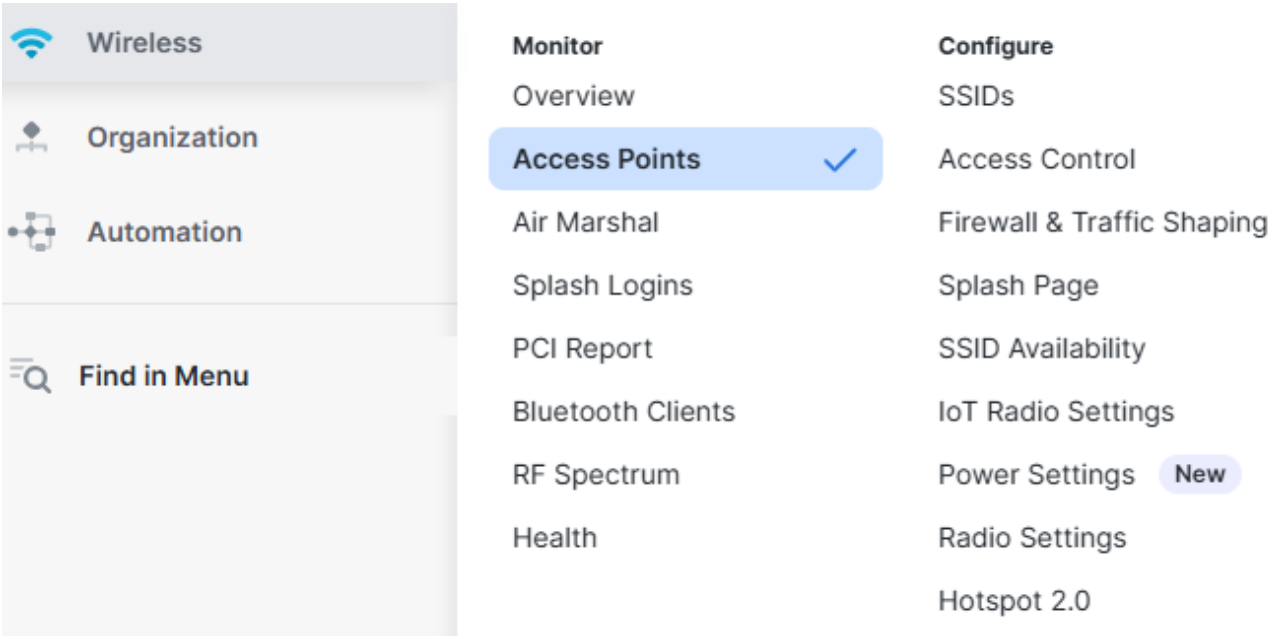
Meraki Dashboard konfigurira nadzor nad svakom pristupnom točkom, nadzor nad korisnicima i odrađuje funkcionalnost upravljačkog središta za bežičnu mrežu.

7.3.1. Dodavanje nove bežične pristupne točke u Meraki Dashboard

Koraci koje slijedimo kako bismo dodali novi uređaj na Meraki sustav su sljedeći:

1) navigacija unutar organizacijske jedinice
2) navigacija unutar mrežne jedinice
3) navigacija unutar izbornika Wireless, odnosno bežično
4) odabir opcije *Access Points*, odnosno bežična pristupna točka
5) odabir opcije *Add access point*, odnosno dodaj pristupnu točku.

Na slici ispod teksta označen je izbornik unutar kojega se odabire pristup konfiguraciji i dodavanje novih pristupnih točaka unutar Meraki Dashboarda. Odabirom opcije *Wireless* dobivamo prikaz trenutačno postavljenih uređaja koji su aktivni na lokaciji i pristup izborniku za dodavanje novog uređaja na ustanovu.

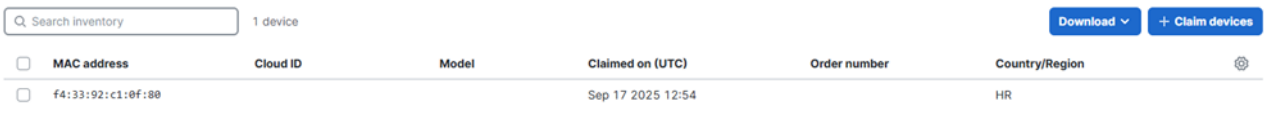


Slika 93. *Prikaz izbornika kod konfiguriranja bežičnih pristupnih točaka*

Niže je naveden prikaz bežičnih pristupnih točaka na ustanovi gdje je vidljivo upravljanje pristupnim točkama, gumb za dodavanje novih pristupnih točaka kao i osnovne informacije o opremi.

Slika 89. Prikaz uređaja dodanih u bežične pristupne točke

Odabirom opcije *Add access point*, odnosno dodavanjem pristupne točke, sustav nas vodi u izbornik u kojem se nalaze neregistrirani uređaji koje dodajemo ustanovi. Uređaj je moguće dodati njegovim dodavanjem i klikom na *Claim devices*, odnosno dodaj uređaj. Izbornik za dodavanje uređaja priložen je slici ispod teksta.

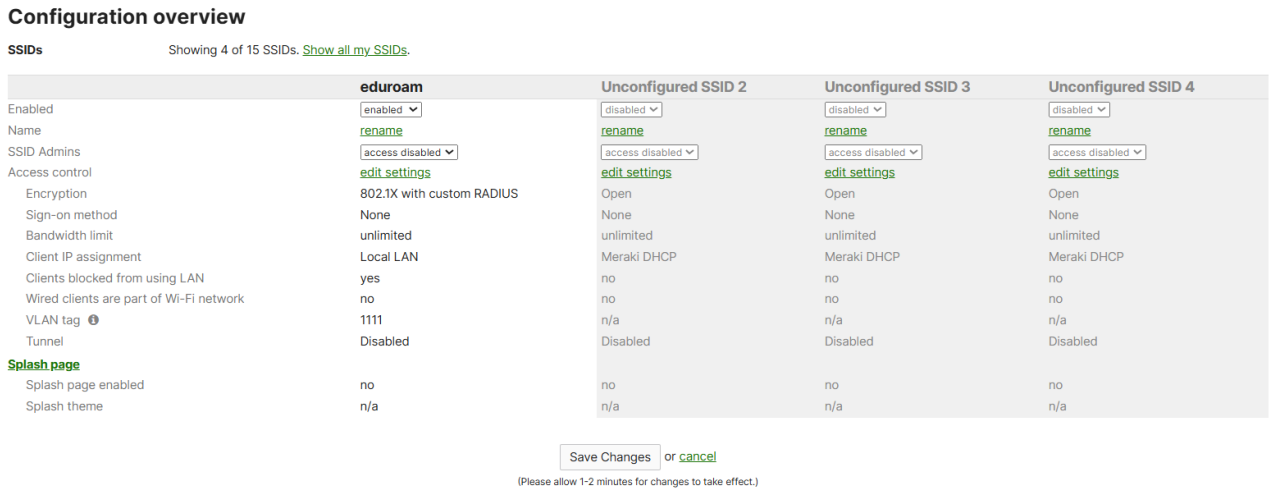


Slika 94. *Prikaz izbornika za dodavanje uređaja na organizaciju*

Napomena za administratore sustava: dodavanje novih uređaja u mrežu dodavat će vanjski suradnici zaduženi za održavanje sustava. Unatoč tomu opisan je postupak dodavanja novog uređaja kako bi se administratorima olakšao proces dodavanja novih uređaja.

7.3.2. Konfiguracija SSID-a

Konfiguracija SSID-a unutar Meraki Dashboarda drastično je pojednostavnjena. Sama konfiguracija počinje navigacijom u izbornik Wireless i odabirom SSIDs podizbornika za konfiguraciju uređaja. Prikazan je izbornik kako bi se pojednostavnilo shvaćanje navigacije po izbornicima.



Slika 95*. Prikaz izbornika za upravljanje SSID-evima*

Unutar izbornika možemo vidjeti trenutačno kreirane SSID-eve, upravljati njima i kreirati nove ovisno o potrebi.

Funkcionalnosti koje možemo primijeniti su uključivanje i isključivanje SSID-a, imenovanje SSID-a ako želimo samo promijeniti ime mreže koja se prikazuje korisnicima, ograničiti ili dopustiti administrativni pristup preko bežične mreže ili provjeriti osnovne konfiguracijske značajke svakog trenutačno konfiguriranog SSID-a. Odabirom opcije *Edit Settings* dobivamo prikaz izbornika za upravljanje SSID-evima, pri čemu je izbornik podijeljen u nekoliko skupina unutar kojih su smještene međusobno povezane ili srodne funkcionalnosti kako bi se pojednostavnila administracija mreže i smanjila potreba za navigiranjem kroz više različitih izbornika.

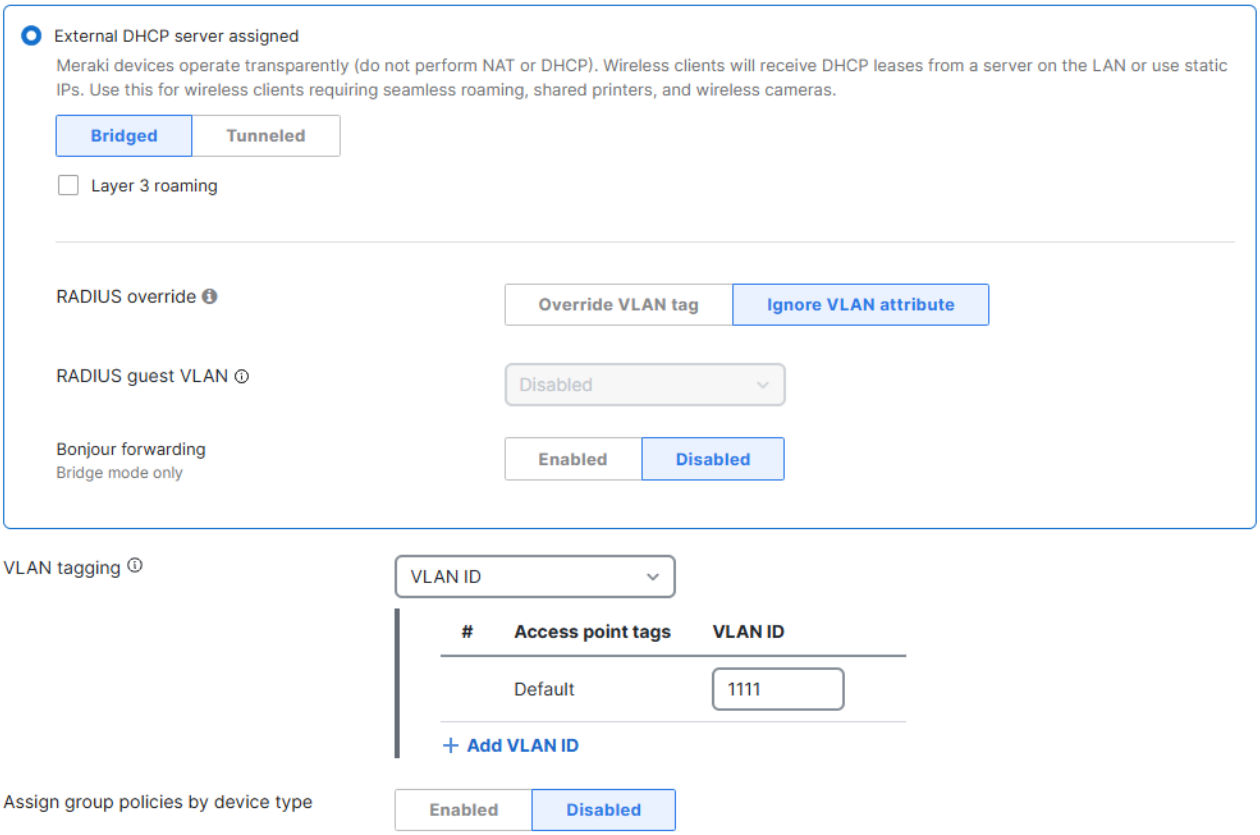
Ulaskom u opciju uređivanja postavki možemo mijenjati ime, uključiti ili isključiti i odabrati opciju prikaza SSID-a ili skrivanja našeg SSID-a pri skeniranju dostupnih bežičnih mreža.

Nadalje, sljedeći dio izbornika posvećen je sigurnosti, odnosno načinu autorizacije krajnjih korisnika na mrežu. Autorizacija na mrežu može biti odrađena na sve načine: od otvorene mreže dostupne svima koji ju vide do posjedovanja dijeljene tajne zajedno s korištenjem RADIUS poslužitelja. Uz navedene opcije, moguće je odabrati i WPA enkripciju ovisno o našim potrebama i zahtjevima, mogućnost forsiranja DHCP opcije i kontrole nad dodatnim funkcionalnostima kao što su 802.11r i 802.11w sigurnosni standardi.

Nakon odabira sigurnosnih postavki moguć je i odabir opcije *Splash page*, odnosno stranice koja se prikazuje korisnicima pri spajanju na mrežu.

Osim navedenih opcija nalaze se i opcije povezane s RADIUS autentikacijom.

Također je moguće odrediti način dodjele IP adresa klijentima preko DHCP-a. Budući da na lokacijama postoje DHCP poslužitelji, odabire se opcija *External DHCP server assigned.* Moguće je definirati hoće li komunikacija biti u *Bridge* ili *Tunneled* načinu rada, a na kraju imamo i opciju pridruživanja kreiranog VLAN-a SSID-u.



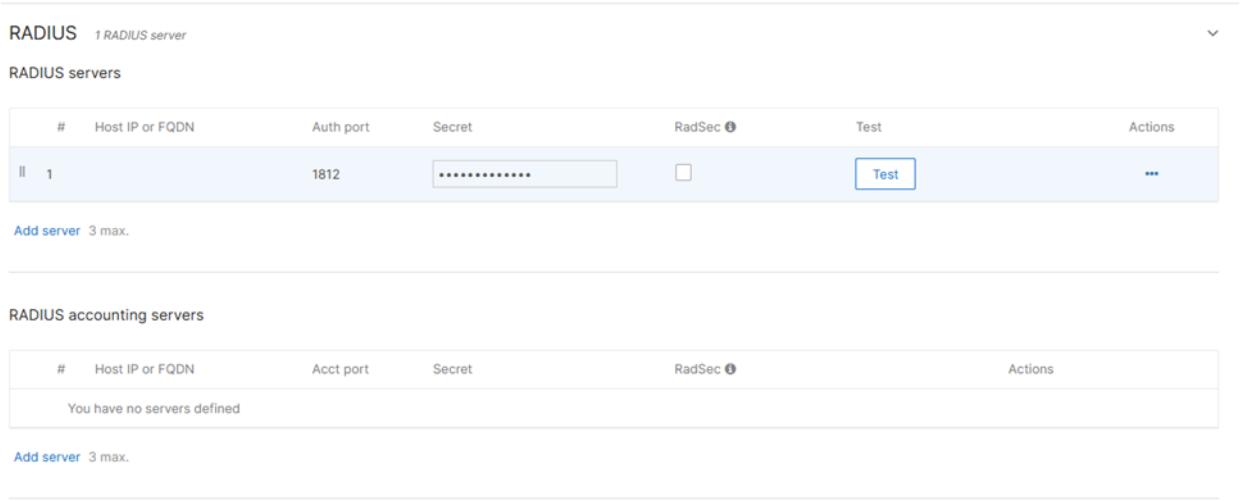
Slika 96. *Prikaz izbornika za pridruživanje VLAN-ova SSID-evima*

Nakon izmjene konfiguracijskih značajki na SSID-u ili kreiranja novog SSID-a potrebno je kliknuti na *Save* gumb na dnu stranice kako bi se izmjene spremile za cijelu mrežnu

organizaciju. Kako se izmjena šalje na cijelu mrežu, moguće je da će izmjene napravljene novom konfiguracijom biti dostupne tek za nekoliko minuta, ovisno naravno o veličini mreže.

7.3.3. Konfiguracija RADIUS postavki

Kako je spomenuto, konfiguracija RADIUS postavki odrađuje se unutar izbornika za administraciju SSID-eva. Izbornik o kojemu je bila riječ prikazan je na slici 97 zbog lakšeg snalaženja unutar teksta.



Slika 97. *Prikaz izbornika za upravljanje postavka RADIUS-a*

Konfiguracija RADIUS servera provodi se tako da unesemo IP adresu ili FQDN zapis RADIUS servera kako je prikazano na slici klikom na opciju *Add server*, s maksimalnim odabirom do tri RADIUS servera. U slučaju korištenja opcije RADIUS Accounting također je potrebno dodati RADIUS server do maksimalno 3 dodana uređaja. Nakon dodavanja uređaja preko *IP adrese* ili *FQDN zapisa* RADIUS servera potrebno je odrediti *autorizacijski port*, odnosno virtualno sučelje kojim uređaji komuniciraju u zatvorenom i sigurnom kanalu i odrediti *Secret* polje, odnosno upisati zaporku poznatu administratorima kako bi uređaj imao pristup zapisima koji se nalaze iza RADIUS servera i imao ovlasti za autorizacije i prema potrebi za dodatne funkcije od RADIUS poslužitelja. Nakon unašanja potrebnih parametara preporuka je pokušati odraditi test mrežne povezanosti i ispravnosti podataka preko gumba *Test* koji provjera mogu li oba uređaja međusobno komunicirati te jesu li podaci koji su zapisani u konfiguraciji odgovarajući.

7.3.4. Spremanje konfiguracije na Cisco Meraki bežičnim pristupnim točkama

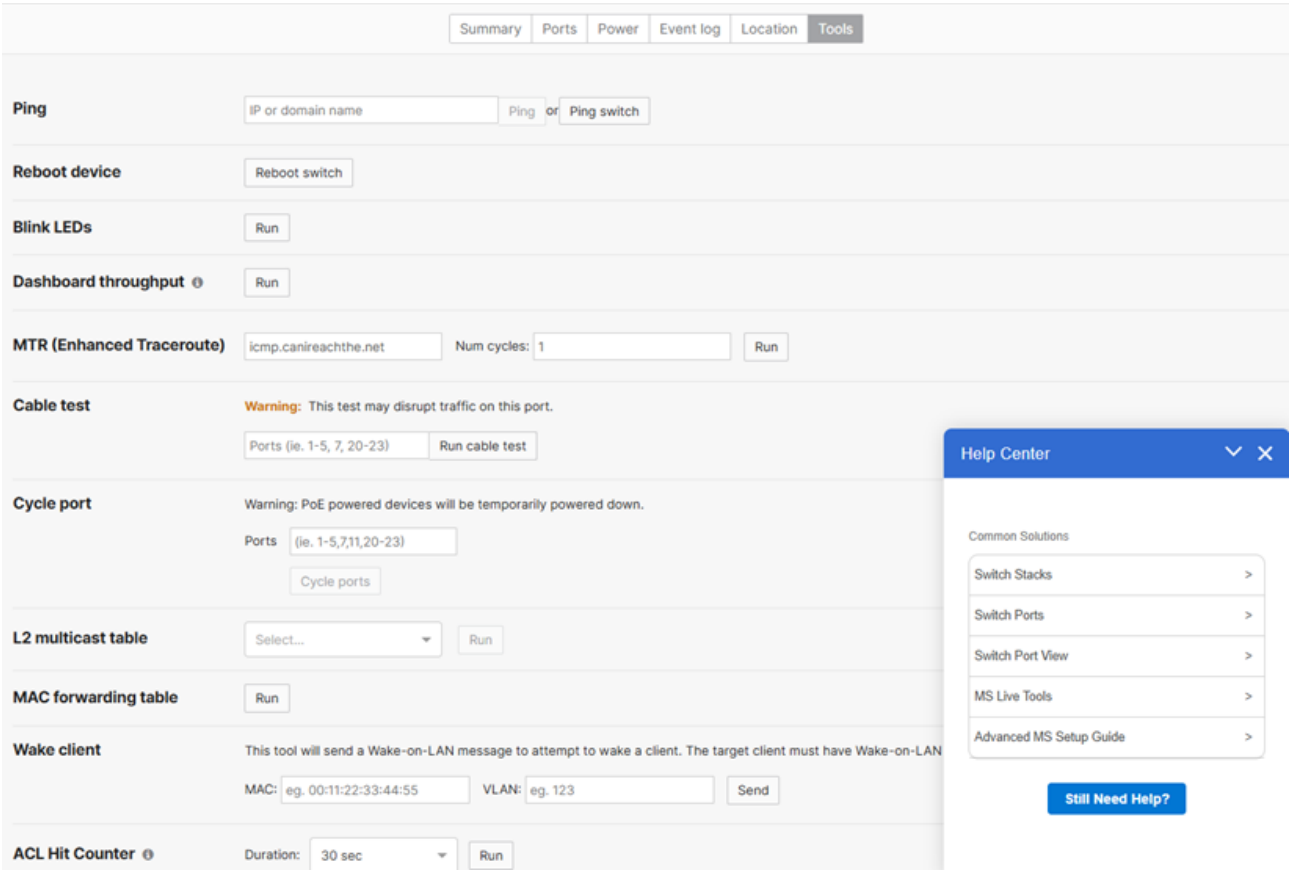
Konfiguracijske promjene na uređajima prethodno su opisane, a svaka konfiguracijska promjena koju smo spremili klikom na *Save* ili *OK* automatski se šalje na uređaje dodane u našu organizacijsku, odnosno mrežnu jedinicu. Takvi uređaji nakon određenog vremena na sebi imaju novu konfiguraciju s novim funkcionalnostima koje su konfigurirane. Konfiguracija se sprema na više uređaja istodobno te nije promijenjena iste sekunde kada se klikne *Save* ili *OK* koji potvrđuju naš izbor, već tijekom minute kada se na sve uređaje pošalje konfiguracijski set koji se na njih primjenjuje.

7.4. Pregled korisničkog prometa preko Meraki Dashboard sustava

Uz korištenje FortiManager pregleda za informacije o korisničkom prometu, ispravnosti slanja i sličnome, moguće je odraditi i početno utvrđivanje uzroka problema na Meraki upravljačkoj ploči. Ploča ima nekoliko funkcionalnosti, poput osnovnih alata kao što su *ping* opcija ili prikaz MAC adresne tablice, provjera zdravlja klijenata i uređaja te provjera količine prometa uređaja spojenih na mrežu. U sljedećim poglavljima prolazit ćemo kroz ove funkcionalnosti sustava.

7.4.1. Osnovni alati za pronalazak grešaka u radu mreže na Meraki sustavu

Sustav Meraki Dashboard ima ugrađene alate za nadzor prometa i otklanjanje poteškoća u radu mreže te će u ovome poglavlju biti obrađene osnove korištenja alata unutar Meraki Dashboarda. Kako bismo lakše navigirali do alata za traženje uzroka problema, potrebno je navigirati kroz izbornik *Switches* do uređaja na kojemu radimo provjere. Nakon klika na ime uređaja treba kliknuti na podizbornik *Tools*, koji je prikazan na slici 98, kako bi se olakšalo razumijevanje ponuđenih izbornika.



Slika 98. *Prikaz izbornika za upravljanje alatima dostupnim unutar Meraki Dashboarda*

Unutar ovog izbornika možemo zadati osnovne komande kao što su *ping* ili *traceroute* koje nam omogućuju pronalazak osnovnih grešaka pri gubitku mrežne povezanosti. Uz njih su dostupni i alati koji nam olakšavaju fizičko baratanje uređajima kao što su *Reboot* opcija koja omogućuje isključivanje i ponovno uključivanje uređaja u kontroliranim uvjetima bez fizičke prisutnosti uređaja. Za lakši pronalazak uređaja unutar serverskog ormara postoji opcija *Blink LEDs* koja uključuje i isključuje lampice na uređaju kako bismo znali koji uređaj tražimo.

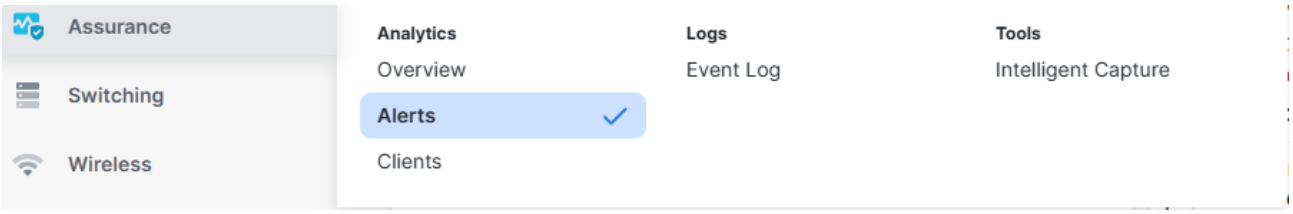
Korisna funkcija je i *Cable test* koja provjera ispravnost fizičke veze sa sučelja preklopnika do drugog povezanog uređaja, a u slučaju neispravnosti fizičke veze daje točne informacije o tome što nije ispravno na samoj fizičkoj vezi i koja je udaljenost od sučelja do mjesta na kojemu se događa prekid. Uz to postoje i mogućnosti za buđenje uređaja na mreži za lakše otklanjanje grešaka bez potrebe da se uređaj nađe i fizički uključi, uključivanje i isključivanje sučelja na uređaju i prikaz MAC tablice sa zapisima o MAC adresama kojima uređaj barata.

Uz sve navedene funkcionalnosti imamo i pristup *Help Center* widgetu koji nam daje savjete i najčešća rješenja problema koji se pojavljuju na mreža, a prikazuje se čim uđemo u *Tools* izbornik.

7.4.2. Osnovni alati za provjeru stanja mreže na Meraki dashboard sustavu

Unutar izbornika *Assurance* moguće je vidjeti trenutačno zdravlje mreže, najčešće probleme s kojima se mreža susreće te u slučaju bilo kakvih problema točan presjek problema koji se učestalo pojavljuju.

Klikom na izbornik pokazuju nam se tri mogućnosti provjere analitike: *Overview*, *Alerts* i *Clients*. Također postoji opcija provjere logova klikom na izbornik *Event Log* ili dodatnih alata preko izbornika *Intelligent Capture*. Prikaz izbornika je niže radi lakšeg snalaženja.

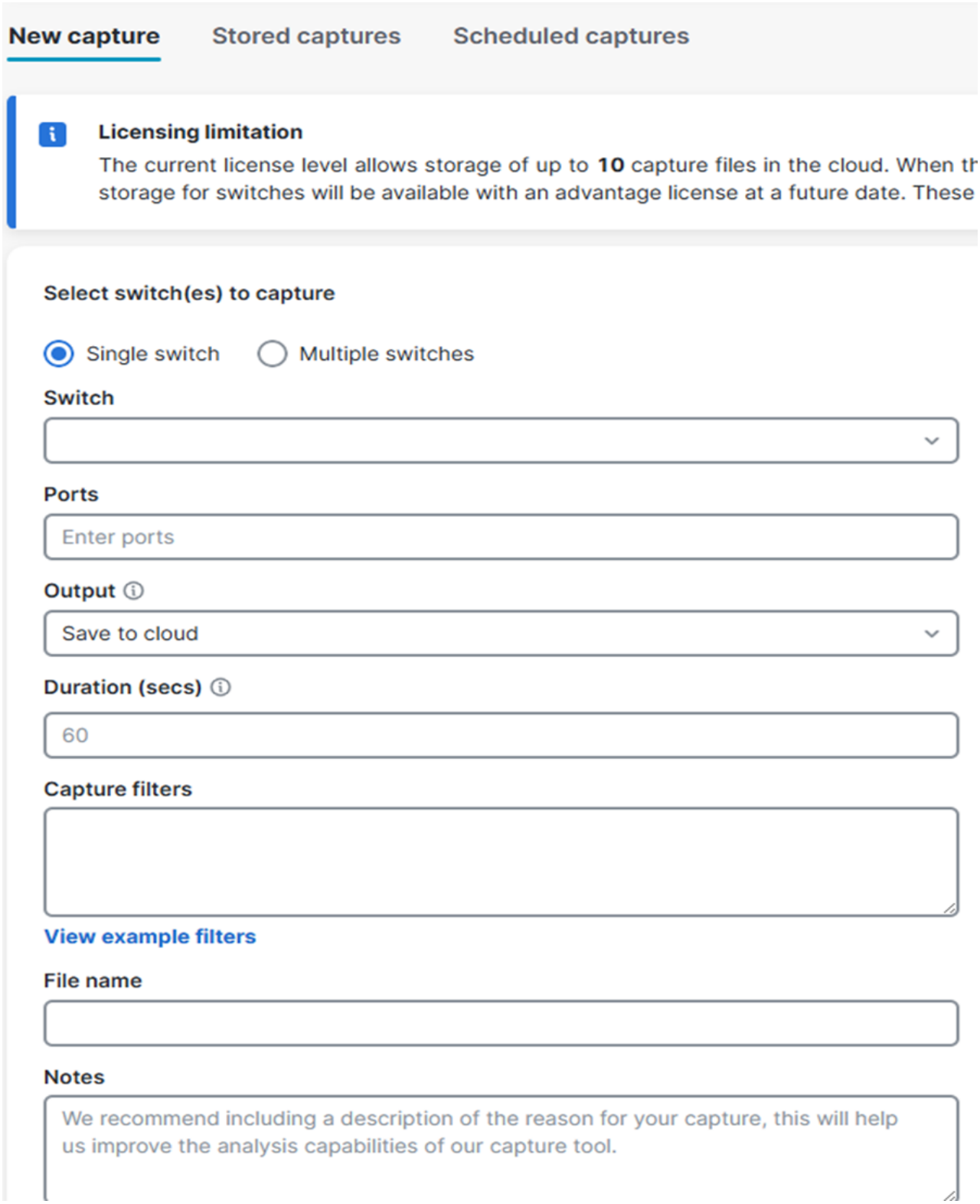


Slika 99. Prikaz izbornika za provjeru analitika i logova na uređajima

Unutar izbornika *Analytics* imamo pristup vizualno raspoređenim podacima koji nam služe za lakše uočavanje problema, provjeru zdravlja mreže i klijenata koji su trenutačno na mreži.

Opcija *Event Logs* daje nam uvid u logove uređaja koji se nalaze unutar naše mrežne organizacije i pomažu u filtriranju podataka sa specifičnih uređaja.

Opcija *Intelligent Capture* daje nam pristup jednostavnom snimanju prometa sa specifičnih sučelja. Unutar izbornika imamo opciju biranja između uređaja na kojima želimo da se promet snima, točnih sučelja na kojima snimamo promet, gdje se ispis sprema i kako želimo da ispis izgleda, odnosno koji promet filtriramo unutar tog ispisa. Uz to je moguće odrediti i snimanje prometa s vremenskim odmakom i pregledavati prethodna snimanja prometa koja su se na mreži odvila. Za jednostavnost razumijevanja izbornika slika se nalazi ispod teksta.



Slika 100. *Prikaz izbornika Inteligent Capture*

8. FortiAnalyzer u sustavu e-Sveučilišta

FortiAnalyzer u sustavu e-Sveučilišta služi kao centralizirana platforma za prikupljanje, pohranu i analizu logova koje generiraju FortiGate uređaji na svim lokacijama, i matičnim (gdje FortiGate radi kao vatrozid) i udaljenim (gdje uređaj radi u ulozi usmjerivača). Njegova glavna svrha je omogućiti jedinstveno mjesto na kojem se konsolidiraju sigurnosni, sustavni i mrežni događaji iz cijelog okruženja, čime se administratorima daje potpuni uvid u stanje sigurnosti i mrežne aktivnosti na svim ustanovama koje su dio e-Sveučilišta.

Korištenjem FortiAnalyzera postiže se standardizirano i pouzdano praćenje prometa, incidenata i ponašanja mrežnih uređaja te se znatno olakšava dijagnostika problema. Centralizirano prikupljanje logova omogućuje i detaljnu analitiku, kreiranje izvještaja, praćenje trendova te otkrivanje nepravilnosti koje bi inače bile teško vidljive kada su podaci raspršeni po različitim lokacijama.

FortiAnalyzer također djeluje kao komponenta sigurnosnog nadzora jer podržava korelaciju događaja, detekciju prijetnji i pregled potencijalnih incidenata. U kombinaciji s FortiManagerom omogućuje potpunu kontrolu, nadzor i forenzičku analizu, što je posebno važno u složenim i distribuiranim sustavima poput e-Sveučilišta.

U konačnici, njegova uloga u infrastrukturi nije samo operativna, već i strateška – pruža temelj za pouzdanu sigurnosnu analitiku, kontinuirani nadzor i donošenje informiranih odluka o upravljanju mrežom i zaštitom podataka.

8.1 Integracija FortiAnalyzera s FortiGate uređajima

U sustavu e-Sveučilišta FortiAnalyzer je povezan sa svim FortiGate uređajima raspoređenima na matičnim i udaljenim lokacijama. Bez obzira na ulogu, vatrozid ili usmjerivač, svaki FortiGate uređaj obvezno šalje svoje logove prema centralnom FortiAnalyzeru.

Integracija se temelji na sigurnoj komunikaciji preko mreže e-Sveučilišta, pri čemu je FortiAnalyzer konfiguriran kao centralni log-server za sve lokacije. FortiGate uređaji šalju više vrsta logova, uključujući prometne, sigurnosne, sustavne i događajne zapise. Time se omogućuje jedinstven i dosljedan nadzor cijele infrastrukture, bez obzira na geografski razdvojene lokacije.

U ovoj arhitekturi FortiAnalyzer djeluje kao zajednički analitički sloj koji prikupljene podatke pretvara u pregledne informacije i statistike. Administratori mogu u stvarnom vremenu vidjeti status uređaja, ponašanje prometa i sigurnosne događaje za svaku instituciju i njezine

udaljene lokacije. Svi logovi obrađuju se na jedinstven način, što osigurava konzistentnost i olakšava analizu.

Ovakav model centraliziranog prikupljanja i obrade logova ključan je za brzu dijagnostiku incidenata, praćenje nepravilnosti i dugoročno planiranje sigurnosnih pravila na razini cijelog e-Sveučilišta.

8.2. Organizacija ADOM-ova u FortiAnalyzeru

U FortiAnalyzeru je implementirana struktura ADOM-ova koja omogućuje jasnu organizaciju i odvajanje logova za svaku ustanovu unutar e-Sveučilišta. Svaka matična lokacija ima vlastiti ADOM, a unutar tog ADOM-a nalaze se i sve pripadajuće udaljene lokacije povezane na istu matičnu jedinicu. Na taj način ADOM predstavlja logičku i administrativnu cjelinu jedne ustanove.

Ovakva organizacija omogućuje da se logovi, analitika i izvještaji pregledavaju zasebno za svaki kampus ili ustanovu, bez miješanja podataka s drugih lokacija. Time se postiže bolja preglednost, jednostavnije upravljanje te povećana sigurnost, posebno u situacijama kada različiti administratori imaju pristup svojim ADOM-ovima.

Svaki ADOM ima vlastitu bazu logova, analitičke postavke i zasebne mogućnosti izvještavanja, što olakšava decentralizirano upravljanje u većem i distribuiranom okruženju poput e-Sveučilišta. Ovakav pristup omogućuje i skalabilnost – dodavanje novih lokacija ili promjena u strukturi ne utječe na ostale ADOM-ove, čime se održava stabilnost sustava i pojednostavnjuje daljnji razvoj.

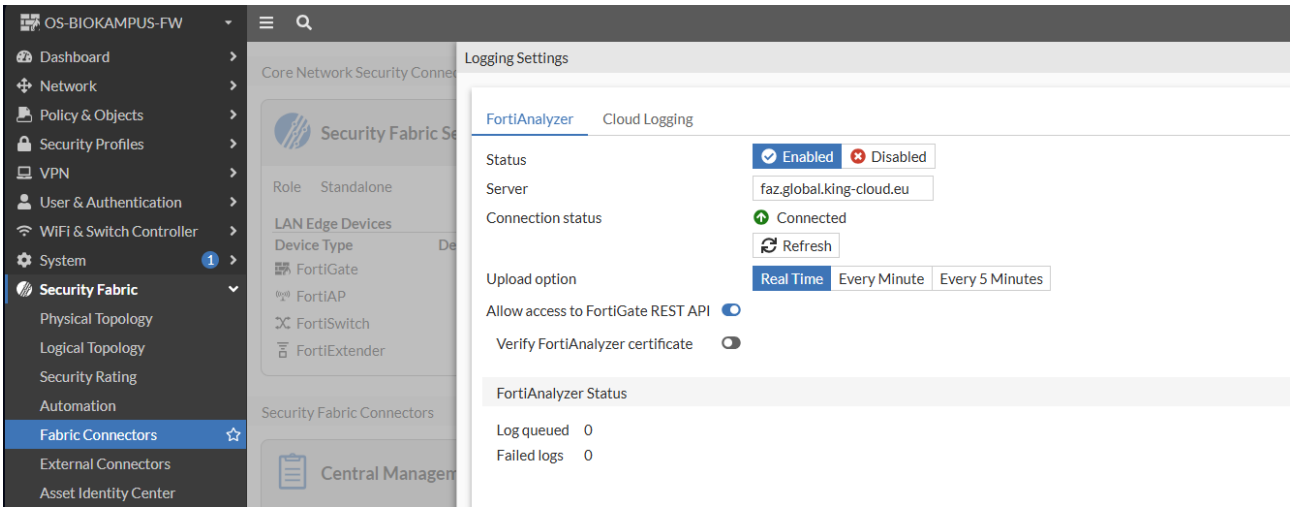
8.3. Dodavanje FortiGate uređaja na FortiAnalyzer

Dodavanje FortiGate uređaja na FortiAnalyzer uključuje nekoliko koraka. Prvo je potrebno osigurati da uređaj ima stabilnu mrežnu povezanost s FortiAnalyzerom i da je omogućeno slanje logova. Matične lokacije šalju logove preko interneta predefiniranom rutom, dok je na udaljenim lokacijama FortiAnalyzerova IP adresa dodana u statičke putanje kako bi logovi dolazili s ispravne IP adrese. Udaljene lokacije rade na ovakav način jer se u postavkama pri dodavanju FortiAnalyzera forsira izvorišna IP adresa koja pripada udaljenoj lokaciji. Ako se komunikacija odvija kroz IPSEC, promet se NAT-ira i ne prikazuje ispravno u FortiAnalyzer sustavu.

Nakon pripreme FortiGate uređaja registracija se provodi s pomoću sučelja FortiAnalyzer. Administrator u Device Manager odjeljku pronalazi pripremljeni FortiGate te ga smješta u odgovarajući ADOM.

Konfiguracija spajanja preko GUI-a (FortiGate strana)

1. Prijavite se na FortiGate mrežno sučelje.
2. Otvorite Security Fabric > Fabric Connectors.
3. Kliknite Logging & Analytics> FortiAnalyzer.
4. Unesite:
   - Status > Enabled
   - Server > faz.global.king-cloud.eu
   - Upload option > Real time
5. Kliknite OK za spremanje.



Slika 101. Postavke FortiGate za povezivanje s FortAnalyzerom

Zbog nemogućnosti konfiguracije izvorišne IP adrese preko GUI sučelja opciju je potrebno postaviti s pomoću CLI naredbe:

config log fortianalyzer setting

set source-ip 82.214.96.131 (javna adresa koja se nalazi na FortiGateu)

- Na FortiManageru odobrite novi uređaj u Unauthorized Devices listi i dodijelite mu odgovarajući ADOM.

Dodavanje FortiAnalyzera CLI naredbama:

config log fortianalyzer setting

set status enable

set server "faz.global.king-cloud.eu"

set certificate-verification disable

set serial "FAZ-VMTM00000000" "FAZ-VMTM00000001"

set source-ip "82.214.96.131" (javna adresa uređaja)

set upload-option realtime

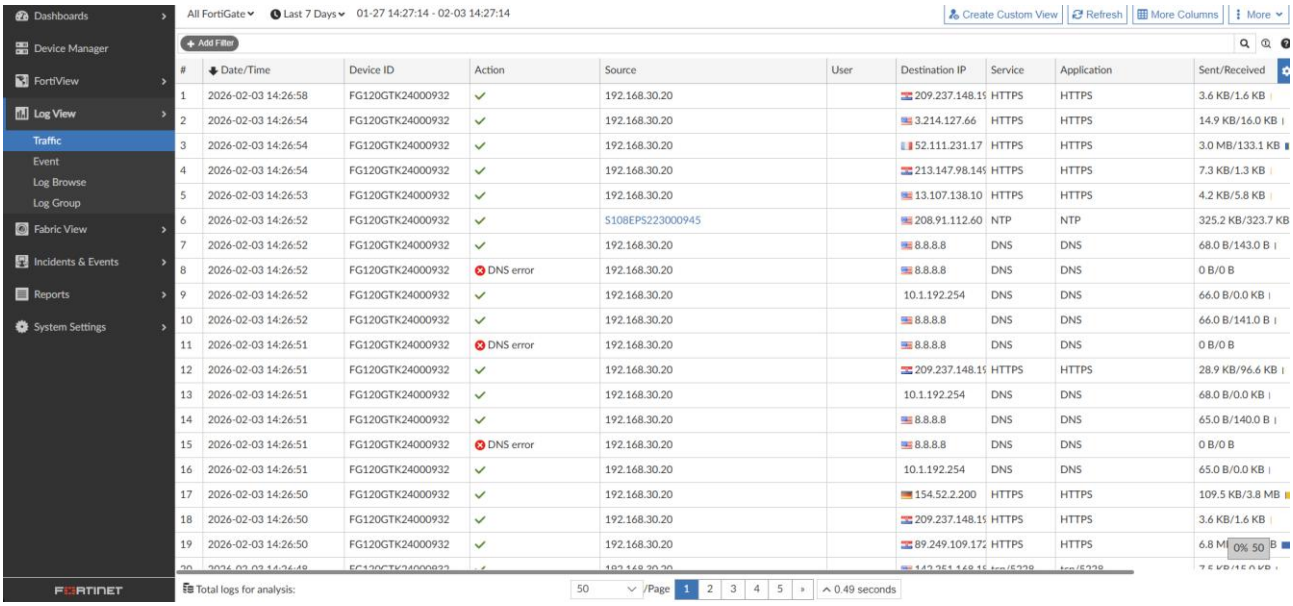
end

8.4. Analitika, izvještavanje i vizualizacija prometa

FortiAnalyzer omogućuje detaljnu analizu mrežnoga i sigurnosnog prometa prikupljenim logovima sa svih FortiGate uređaja unutar sustava e-Sveučilište. Korištenjem analitičkih funkcionalnosti administratori i sigurnosni timovi mogu pratiti događaje u realnom vremenu, izrađivati izvještaje, pratiti trendove i vizualizirati podatke s pomoću grafikona i statistika.

- Pregled događaja u stvarnom vremenu (*Real-time)*

FortiAnalyzer pruža mogućnost praćenja logova i sigurnosnih događaja u stvarnom vremenu. Administrator može filtrirati događaje prema tipu (sigurnosni, prometni, sistemski), prioritetu ili lokaciji te odmah reagirati na potencijalne prijetnje. Prikaz u stvarnom vremenu omogućuje brzo uočavanje anomalija, kao što su neuobičajeni promet, pokušaji neovlaštenog pristupa ili neuspjeli logini.



Slika 102. Logovi u stvarnom vremenu

- Izrada sigurnosnih izvještaja

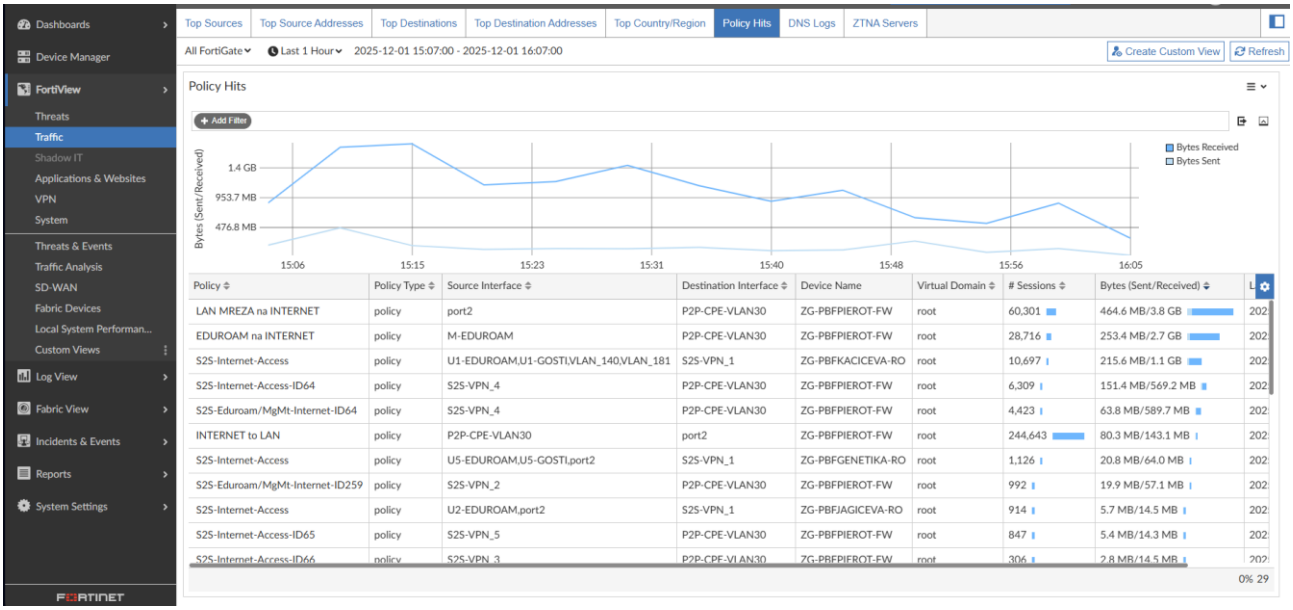
FortiAnalyzer nudi predefinirane izvještaje koji pokrivaju najčešće potrebe nadzora i analize sigurnosti. Uz to, moguće je kreirati i prilagođene izvještaje prema specifičnim zahtjevima e-Sveučilišta, primjerice za pojedine kampuse ili odjele. Izvještaji uključuju detalje o sigurnosnim incidentima, prometnim obrascima, upotrebi aplikacija i aktivnostima korisnika.

- Statistike prometa, trendovi i grafički prikazi

Analitika prometa omogućuje vizualizaciju podataka s pomoću grafova, trendova i statističkih prikaza. Administratori mogu pratiti:

  - ukupan promet po lokaciji ili segmentu mreže
  - trendove u vremenskim intervalima (dnevni, tjedni, mjesečni)
  - učestalost određenih događaja ili tipova prometa.

Navedeni prikazi olakšavaju donošenje odluka i prepoznavanje potencijalnih sigurnosnih rizika.



Slika 103. Prikaz korištenja sigurnosnih pravila na vatrozidu

- Automatizirano slanje izvještaja

FortiAnalyzer omogućuje automatizirano generiranje i slanje izvještaja administratorima i sigurnosnim timovima. Izvještaji se mogu konfigurirati da stižu dnevno, tjedno ili mjesečno, a mogu uključivati kombinaciju predefiniranih i prilagođenih analiza. Ova funkcionalnost osigurava da relevantne informacije uvijek budu dostupne bez potrebe za ručnim kreiranjem izvještaja.

Korištenjem ovih funkcionalnosti FortiAnalyzer omogućuje sustavu e-Sveučilište proaktivno praćenje sigurnosti, učinkovitu analizu mrežnog prometa i kvalitetno izvještavanje za sve razine administracije.

9. Prijava poteškoća i upita CARNET-ovu *helpdesku*

U slučaju poteškoća u radu sustava i za sva pitanja koja se odnose na program „e-Sveučilišta“ potrebno je obratiti se CARNET-ovu *helpdesku*:

- telefonski broj podrške: +385 1 6661 555
- e-adresa podrške: e-sveucilista@carnet.hr

Popis slika

Popis tablica

Popis literature

- *FortiManager – Administration Guide Version 7.6.4. (2025)*, Fortinet Document Library, https://docs.fortinet.com/document/fortimanager/7.6.4/administration-guide/512210/setting-up-fortimanager
- *Administration Guide FortiAnalyzer 7.6.4. (2025),* Fortinet Documentation Library. https://docs.fortinet.com/document/fortianalyzer/7.6.4/administration-guide/366418/setting-up-fortianalyzer
- *FortiGate/FortiOS – Administration Guide Version 7.6.4. (2025),* Fortinet Document Library, https://docs.fortinet.com/document/fortigate/7.6.4/administration-guide/954635/getting-started
- FortiGate 100F Series, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf
- FortiGate 200F Series, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-200f-series.pdf
- Cloud-Managed Wi-Fi Access Points, https://meraki.cisco.com/products/wi-fi/
- Cloud-Managed Network Switches, https://meraki.cisco.com/products/switches/
- Cisco Networking Platform, https://www.cisco.com/site/us/en/products/networking/networking-cloud/index.html
- MS130 Datasheet, https://documentation.meraki.com/Switching/MS_-_Switches/Product_Information/Overviews_and_Datasheets/MS130_Datasheet
- Cisco Catalyst 9300 Series Switches Data Sheet, https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html
- UPUTE ZA SPAJANJE NA Internet, https://arhiva.scri.uniri.hr/files/smjestaj/UPUTE%20ZA%20SPAJANJE%20NA%20INTERNET.pdf

Impresum

Nakladnik: Hrvatska akademska i istraživačka mreža – CARNET

Projekt: e-Sveučilišta

Autori: Tina Klisura, Goran Matanić, Robert Cahun

Koautori: Lidija Jakovčić, Vedran Antolović, Josip Ramić

Lektorica: Jasminka Juzbašić

Zagreb, studeni 2025.

Podaci za kontakt

Hrvatska akademska i istraživačka mreža – CARNET

Josipa Marohnića 5, 10000 Zagreb

Telefon: +385 1 6661 500

E-adresa: helpdesk@carnet.hr i www.carnet.hr

Više informacija o fondovima Europske unije možete pronaći na mrežnim stranicama Ministarstva regionalnoga razvoja i fondova Europske unije: www.strukturnifondovi.hr.

Ovaj je priručnik izrađen radi podizanja digitalne kompetencije korisnika u sklopu projekta „e-Sveučilišta“ koji sufinancira Europska unija iz europskih strukturnih i investicijskih fondova. Nositelj projekta je Hrvatska akademska i istraživačka mreža – CARNET.