



e-škole

RAZVOJ SUSTAVA
DIGITALNO ZRELIH ŠKOLA
(II. FAZA)

Upoznavanje s mrežnom
opremom i sustavom za
upravljanje i nadzor mreže:

Mrežno rješenje Fortinet

CARNET

2021. GODINA



Europska unija
Zajedno do fondova EU



EUROPSKI STRUKTURNI
I INVESTICIJSKI FONDOVI



Operativni program
**KONKURENTNOST
I KOHEZIJA**

Sadržaj

Popis korištenih kratica	3
1. Uvodne informacije	5
2. Osnove mrežnog sustava	6
3. Pasivna mrežna oprema u školama	7
3.1 Komunikacijski ormari i priključnice	7
3.2 Sustav označavanja	11
3.2.1 Fizičke pozicije	11
3.2.2 Oznaka etaže	11
3.2.3 Oznaka razdjelnika	11
3.3 Primjeri i načini veza komunikacijskih ormara	13
4. Aktivna mrežna oprema u školama	15
4.1 Arhitektura sustava	15
4.2 WAN mreža	16
4.2.1 Mrežni usmjerivač	16
4.2.2 Konfiguracijske značajke sustava	18
4.3 LAN mreža	19
4.3.1 Mrežni preklopnik	19
4.3.2 Konfiguracijske značajke sustava	22
4.4 Bežična mreža	23
4.4.1 Bežična pristupna točka	23
4.4.2 Konfiguracijske značajke sustava	24
5. Sustav za upravljanje i nadzor mreže	27
5.1 Osnovne sastavnice sustava	27
5.2 Pregled glavnih upravljačkih funkcionalnosti	30
6. Administracija i održavanje implementirane mrežne infrastrukture škole	38
6.1 Spajanje mrežnog uređaja	38
6.2 Vraćanje konfiguracije na tvorničke postavke	44
6.2.1 Vraćanje bežične pristupne točke na tvorničke postavke	44
6.2.2 Vraćanje preklopnika na tvorničke postavke	44
6.2.3 Vraćanje usmjerivača na tvorničke postavke	45
6.3 Nadzor nad mrežnom opremom	46
6.4 Nadzor nad klijentima na mreži	49
6.5 Konfiguracija osnovnih postavki na mrežnoj opremi	54

6.5.1	Primjer konfiguracije sučelja na usmjerivaču	54
6.5.2	Primjer konfiguracije rute na usmjerivaču	57
6.5.3	Primjer dodavanja sigurnosnog pravila	59
6.5.4	Primjer konfiguracije sučelja preklopnika	61
6.5.5	Primjer kreiranja novog VLAN-a.....	63
6.5.6	Primjer kreiranja novog SSID-a.....	65
6.5.7	Primjer kreiranja novog korisnika za <i>guest</i> mrežu	69
7.	Prijava poteškoća i upita CARNET-ovom helpdesku	71
	Popis slika	72
	Popis tablica	74
	Popis korištene literature	74
	Impresum.....	75



Ovo djelo je dano na korištenje pod licencom Creative Commons Imenovanje -Nekomercijalno - Dijeli pod istim uvjetima 4.0 međunarodna.

Popis korištenih kratica

ADOM – Administrativna domena

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

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

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 korišten od strane mrežnih računala za dodjeljivanje IP adresa

DIS – Dokumentacija izvedenog stanja

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

EANE (engl. *Existing Active Network Equipment*) – Postojeća aktivna mrežna oprema

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 Ethernet okvira brzinom od gigabita u sekundi

GIP – Glavni izvedbeni projekt

HTML (engl. *HyperText Markup Language*) – Prezentacijski jezik za izradu web stranica

HTTPS (engl. *Hypertext Transfer Protocol Secure*) – Skup pravila koja se koriste za siguran prijenos hipertekstualnih dokumenata između dva računala

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, predstavlja najkorišteniji apstraktni opis arhitekture mreže

PDF (engl. *Portable Document Format*) – Format zapisa dokumenata kojeg je kreirala kompanija 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 – Stručnjak za tehničku podršku

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 putem IEEE 802.11 bežičnih mreža

XML (engl. *Extensible Markup Language*) – Jezik za označavanje podataka

1. Uvodne informacije

Priručnik o mrežnoj opremi i sustavu za upravljanje i nadzor mreže opisuje aktivnu i pasivnu mrežnu infrastrukturu implementiranu u školama u sklopu druge faze programa “e-Škole: Razvoj sustava digitalno zrelih škola (II. faza)“.

Osim opisa implementirane mrežne infrastrukture priručnik pruža osnovne informacije potrebne za administraciju, praćenje rada, detektiranje i otklanjanje manjih poteškoća u radu implementiranog aktivnog mrežnog sustava koji se zasniva na rješenju proizvođača Fortinet.

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

Priručnik je namijenjen osobama koje pružaju tehničku podršku školama, odnosno stručnjacima za tehničku podršku, administratorima resursa u školama te svim drugim osobama koje jesu ili će biti angažirane na održavanju funkcionalnog mrežnog sustava u školama, a kako bi se što bolje upoznali s implementiranim sustavom na operativnoj razini.

2. Osnove mrežnog sustava

Kao preduvjet za administraciju i nadzor nad računalnom mrežnom infrastrukturom implementiranom u sklopu projekta “e-Škole: Razvoj sustava digitalno zrelih škola (II. faza)“, nužno je da stručnjak za tehničku podršku (STP) zadužen za administraciju sustava bude upoznat s osnovama mrežnog sustava, mrežnim protokolima i servisima, osnovama rada bežične mreže, kao i sa sigurnošću računalnih mreža.

Budući da se od stručnjaka za tehničku podršku očekuje poznavanje osnova mrežnih tehnologija i pripadajućih protokola, u ovom priručniku osnove neće biti dodatno pojašnjene.

Od stručnjaka za tehničku podršku očekuje se osnovno znanje o sljedećim područjima implementacije i održavanja sustava mrežnih tehnologija:

- 7 slojeva OSI mrežnog modela (OSI - engl. *Open Systems Interconnection*), 4 sloja mrežnog TCP/IP (engl. *Transmission Control Protocol / Internet Protocol*) modela,
- adresiranje u računalnim mrežama,
- mrežni protokoli,
- sigurnost lokalnih mreža,
- mrežni uređaji
 - L2/L3 preklopnik, usmjeritelj, vatrozid, bežična pristupna točka (AP – engl. *Access Point*),
- bežična mreža
 - frekvencijski pojas (2,4 GHz, 5 GHz) i kanali,
 - standardi 802.11 a/b/g/n/ac,
 - sigurnost u bežičnim mrežama – autentikacija, autorizacija i enkripcija.

3. Pasivna mrežna oprema u školama

U sklopu projekta “e-Škole: Razvoj sustava digitalno zrelih škola (II. faza)“, u Glavnim izvedbenim projektima (GIP) definirani su parametri kvalitete pasivne mrežne infrastrukture koja se postavlja u školama. Ako u školama postoji dio infrastrukture koji ispunjava nužne parametre kvalitete, projektom je dopušteno korištenje postojeće infrastrukture, uključujući mrežne ormare, priključnice, kabelske trase itd., a ta je mogućnost iskorištena u određenom broju škola. Za potrebe novog sustava kabliranja u školama, koriste se i postojeće trase (kabelski kanali) i postojeći etažni razdjelnici (EFD), u slučaju da raspolažu dovoljnim kapacitetom. Za svaku školu za koju je izvedeno kabliranje u sklopu projekta izgradnje pasivne mrežne infrastrukture u školama, izrađen je i Dokument izvedenog stanja (DIS) pasivne mrežne infrastrukture škole.

Novoizgrađena pasivna infrastruktura omogućuje:

- stabilnu i kvalitetnu pasivnu mrežu
- povezivanje računalne i mrežne opreme nabavljene kroz projekt “e-Škole: Razvoj sustava digitalno zrelih škola (II. faza)“
- integraciju postojeće mreže s novom
- veći kapacitet lokalnih mreža (LAN – engl. *Local Area Network*)
- mogućnost proširenja mreže.

3.1 Komunikacijski ormari i priključnice

Aktivni uređaji, prespojni paneli i sl. smještaju se u razdjelnike sukladno DIS-u pasivne mrežne infrastrukture škole u kojem je predložen raspored opreme po komunikacijskim ormarima. Razmještaj i eventualna manja preraspodjela postojeće opreme po razdjelnicima izvedeni su na lokaciji prilikom same instalacije pasivne i prateće aktivne opreme.

U DIS-u pasivne mrežne infrastrukture škole korištene su sljedeće oznake, odnosno kratice za komponente:

- razdjelnik zgrade (BD – engl. *Building Distributor*)
- etažni razdjelnik (FD – engl. *Floor Distributor*)
- postojeći etažni razdjelnik (EFD – engl. *Existing Floor Distributor*)
- postojeća aktivna mrežna oprema (EANE – engl. *Existing Active Network Equipment*)

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. BD služi za povezivanje s terminalnom opremom za površine koje mu gravitiraju, kao i terminaciju kabela za okosnice zgrade, tj. veze s etažnim razdjelnicima (FD). U svakoj je školi postavljen jedan samostojeći BD u kojem se nalazi veći dio aktivne mrežne opreme, kao i CARNET-ova oprema smještena

na lokaciji korisnika (CPE – engl. *Customer Premises Equipment*), te smještaj infrastrukture vezane uz pristup na okosnicu CARNET-ove mreže.



Slika 1: Primjer razdjelnika BD

Etažni razdjelnik (FD) je optičkim kabelom povezan s glavnim razdjelnikom zgrade (BD), u skladu s namjenom, te služi za smještaj opreme za zaključenje etažnog kabliranja EKM-a opsluživanog područja i pripadajućih sustava za vođenje kabela. U FD ormare instalira se potreban tip i broj mrežnih preklopnika, u skladu s DIS-om.



Slika 2: Primjer razdjelnika FD

Za potrebe horizontalnog kabliranja, koriste se telekomunikacijski priključci (TO – engl. *Telecommunications Outlet*) koji su modularne (ugrađuju se u parapetne kanale) ili nadžbukne (samostojeće) izvedbe. Telekomunikacijskim se priključcima terminiraju kabele na strani korisničke opreme, ispred bežičnih pristupnih točki i na EANE mjestima. To su mjesta u školi na kojima se nalazi aktivna mrežna oprema koja nije smještena u komunikacijskom ormaru. Precizna pozicija svih mjesta završetka kabela, odnosno TO, specificirana je u izvedbenom projektu pasivne mrežne infrastrukture, tj. u njezinoj pratećoj dokumentaciji.



Slika 3: Primjer priključne kutije

Za potrebe horizontalnog kabliranja, koriste se prespojni paneli RJ45 izvedbe za montažu unutar telekomunikacijskih ormara 19" (19 inča), visine 1U, s 24 priključna mjesta za module čiji standard odgovara ugrađenom kabelu. Potreban broj prespojnih panela RJ45 i pozicija unutar pojedinog razdjelnika definiran je u DIS-u pasivne mrežne infrastrukture škole. Prespojni panel RJ45 služi za terminiranje svih U/UTP kabela koji gravitiraju razdjelniku u kojemu su isti terminirani.



Slika 4: 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 prespojnima kablom unutar razdjelnika.



Slika 5: Primjer optičkog LC prespojnog panela



Slika 6: Primjer UTP modularnog prespojnog panela

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



Slika 7: Svjetlovodni LC konektor

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



Slika 8: UTP RJ45 konektor

3.2 Sustav označavanja

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

3.2.1 Fizičke pozicije

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

Radni prostori u kojima se izvode radovi instalacija strukturalnog kabliranja lokalne računalne mreže smješteni su po etažama građevine. Svaka od etaža, kao i pripadajuće fizičke pozicije opreme na pojedinoj etaži, označavaju se odgovarajućom oznakom.

3.2.2 Oznaka etaže

U nastavku je tablica 1 u kojoj su prikazane oznake etaža.

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

Tablica 1: Oznaka etaža

Primjer:

- +01 – označava fizičku poziciju na prvoj etaži (+01).

3.2.3 Oznaka razdjelnika

Čvorište instalacije strukturalnog kabliranja čine razdjelnici koji se koriste za smještaj aktivnih uređaja računalne mreže te opreme za prespajanje segmenata strukturalnog kabliranja. U nastavku je dan opis funkcija razdjelnika i način označavanja pojedinih dijelova razdjelnika:

- +BD – glavni razdjelnik zgrade – čvor koji povezuje vertikalne razvode (prvi u drugu razinu kabliranja) s horizontalnim razvodom kabela. U razdjelniku je ujedno postavljen i CPE uređaj koji služi za terminiranje WAN mreže (WAN – engl. *Wide Area Network*).
- +FD – razdjelnik etaže – čvor koji povezuje horizontalne razvode kabela (treća razina kabliranja) s priključnim mjestima u učionicama i ostalim uredima. U pojedinoj školi može biti više razdjelnika etaže, ali ako svi razvodi kabela završavaju u glavnom razdjelniku, onda ne mora biti nijedan.

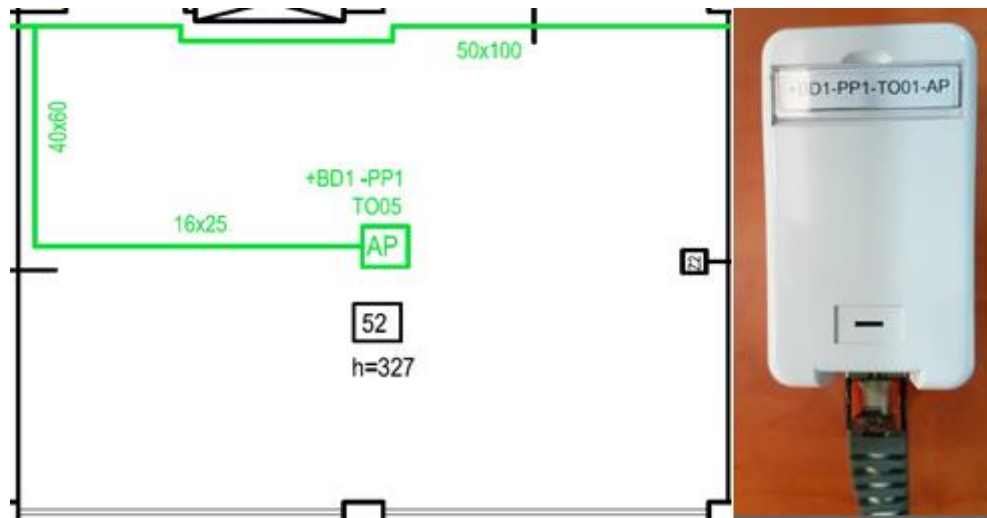
- +EFD – postojeći etažni razdjelnik,
- +EANE – postojeća aktivna mrežna oprema.

Pojedine pozicije unutar razdjelnika definiraju se na sljedeći način:

- **+BDy-PPx-z** – **y** označava broj **BD** razdjelnika, **PP** označava prespojni panel, **x** označava njegov redni broj, dok **z** označava poziciju na panelu, tj. broj porta.
- Primjer:
 - **+BD1-PP1-TO05-AP** – predstavlja fizičku poziciju koja, čitano zdesna nalijevo, označava priključak **5** za bežičnu pristupnu točku (**AP**) na prespojnom panelu **1** (PP1) u razdjelniku **BD** (+BD1)
 - **+BD1-PP2-TO01** – predstavlja fizičku poziciju koja, čitano zdesna nalijevo, označava priključak **1** na prespojnom panelu **2** (PP2) u razdjelniku **BD** (+BD1).



Slika 9: Primjer označavanja razdjelnika i panela



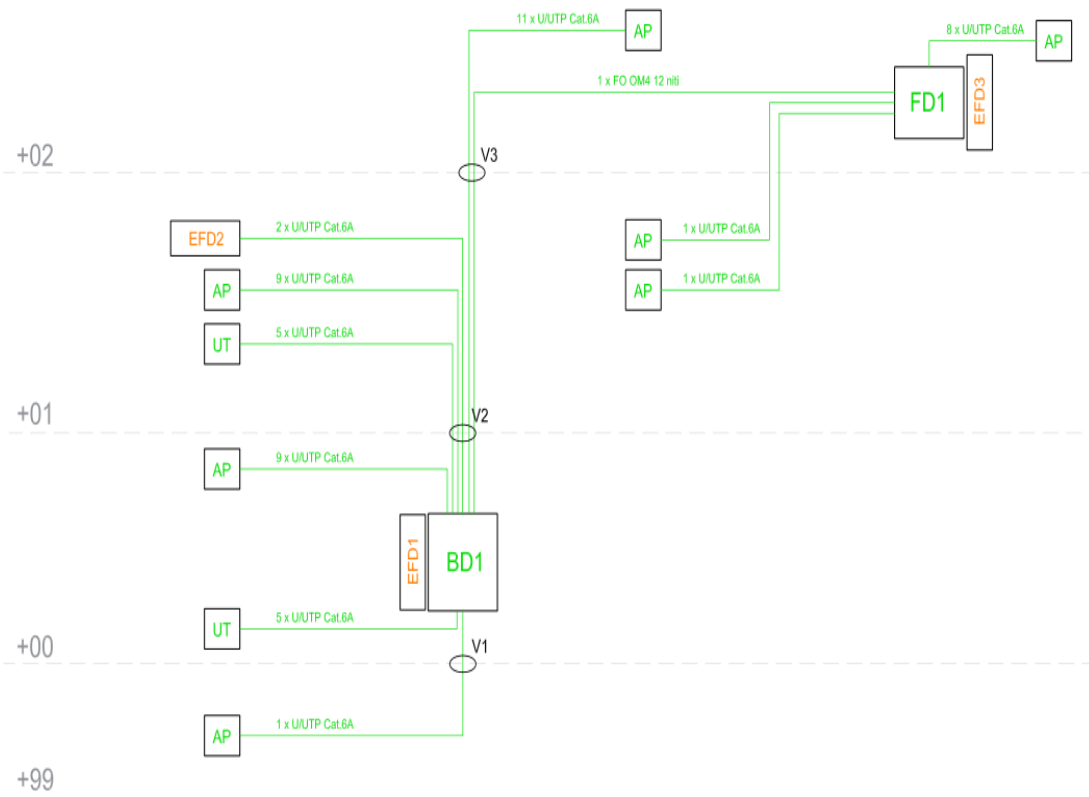
Slika 10: Primjer označavanja priključnica

3.3 Primjeri i načini veza komunikacijskih ormara

Prijenosni mediji kojima se povezuju komunikacijski ormari su:

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

Takvi prijenosni mediji omogućavaju korištenje strukturnog kabliranja tijekom više budućih generacija računalnih mreža koje će raditi na većim brzinama.



Slika 11: Primjer povezivanja BD/FD/EFD komunikacijskih ormara

4. Aktivna mrežna oprema u školama

Implementirani mrežni sustav u cijelosti je zasnovan na rješenjima proizvođača Fortinet.

Osnovne komponente implementiranog aktivnog mrežnog sustava u školama, isporučeni modeli, njihova uloga i konfiguracijske značajke opisani su niže u ovome poglavlju.

4.1 Arhitektura sustava

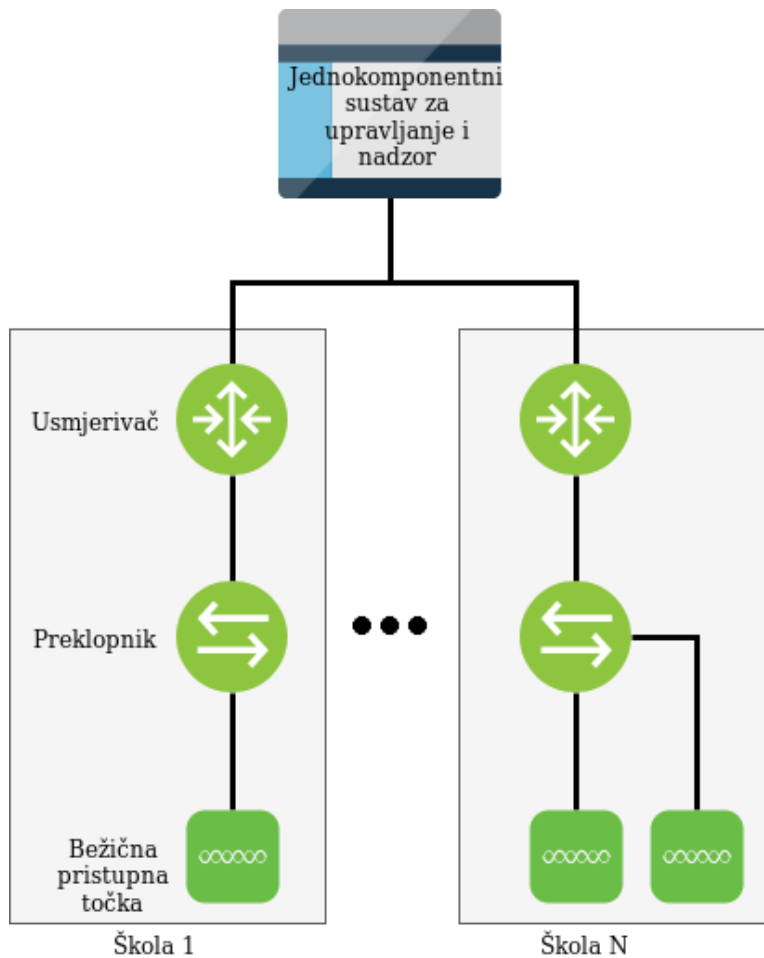
Implementirani mrežni sustav predstavlja jednokomponentno rješenje u kojem se instaliranom mrežnom opremom upravlja putem središnjeg sustava za upravljanje i nadzor mreže. U ovakvom modelu, različitim slojevima lokalne mreže upravlja se i nadzire korištenjem jedne komponente nadzorno upravljačkog sloja.

Implementirani mrežni sustav sastoji se od upravljačkog dijela mreže, fizički smještenog na centralnoj lokaciji CARNET-ovih podatkovnih centara, i lokalne mreže škole. U ovom poglavlju stavljen je naglasak na implementiranu aktivnu mrežnu opremu lokalne mreže škole, dok je upravljački dio implementiranog mrežnog sustava opisan u poglavlju 5 „Sustav za upravljanje i nadzor mreže“.

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

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

Svaka škola povezana je na CARNET mrežu kroz koju klijenti ostvaruju pristup do potrebnih servisa i Interneta. Povezanost na CARNET mrežu ostvarena je korištenjem CARNET-ovog CPE uređaja. Na CARNET-ov CPE uređaj povezana je aktivna mrežna oprema škole, te se sastoji od mrežnog usmjerivača, mrežnih preklopnika i bežičnih pristupnih točaka. Na mrežni usmjerivač povezani su mrežni preklopnici, a na njih su povezane bežične pristupne točke.



Slika 12: Shema implementiranog sustava sa sastavnim blokovima

4.2 WAN mreža

U ovom poglavlju su opisani mrežni usmjerivač i virtualni LAN-ovi.

4.2.1 Mrežni usmjerivač

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

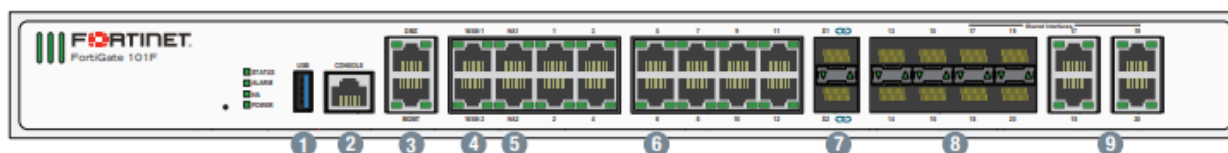
Osnovni zadatak koji usmjerivači obavljaju je provjera odredišne IP adrese za svaki paket koji pristigne na neko od mrežnih sučelja na usmjerivaču, pronalazak gdje treba preusmjeriti taj paket u tablici usmjeravanja te prosljeđivanje paketa na odgovarajuće sučelje.

U sklopu implementiranog mrežnog rješenja u školama, ulogu mrežnog usmjerivača ima uređaj **FortiGate 100F** (u daljnjem tekstu usmjerivač). Ovaj usmjerivač omogućuje povezivanje LAN mreže škole na okosnicu CARNET mreže te na taj način čini granicu između LAN mreže škole i CARNET mreže. Usmjerivač FortiGate 100F se na mrežu povezuje preko tzv. WAN sučelja koje je izravno povezano na CARNET-ov CPE usmjerivač. WAN sučelje usmjerivača FortiGate 100F dobiva IP adresu dinamički putem DHCP (engl. *Dynamic Host Configuration Protocol*) protokola iz CARNET mreže.

Prikaz usmjerivača FortiGate 100F i njegova sučelja vidljivi su na slikama u nastavku.



Slika 13: Usmjerivač FortiGate 100F



Slika 14: Prikaz sučelja usmjerivača FortiGate 100F

Količine i tipovi ugrađenih sučelja usmjerivača FortiGate 100F:

- (1) 1 x USB Port
- (2) 1 x Console Port
- (3) 2 x GE RJ45 MGMT/DMZ Ports
- (4) 2 x GE RJ45 WAN Ports
- (5) 2 x GE RJ45 HA Ports
- (6) 12 x GE RJ45 Ports
- (7) 2 x 10 GE SFP+ FortiLink Slots
- (8) 4 x GE SFP Slots
- (9) 4 x GE RJ45/SFP Shared Media Pairs

Uz funkciju usmjeravanja podatkovnih paketa, usmjerivač FortiGate 100F ima i druge ključne mrežne funkcionalnosti koje su opisane u nastavku.

Funkcionalnosti usmjerivača FortiGate 100F u sklopu implementiranog mrežnog rješenja:

- centralizirano upravljanje uređajem putem sustava za nadzor i upravljanje mrežom,
- tzv. *Zero-touch* instalacija uređaja bez postavljanja inicijalne konfiguracije, putem sustava za nadzor i upravljanje mrežom,
- povezivanje na CPE opremu, odnosno na CARNET mrežu,
- usmjeravanje prometa (IPv4/IPv6),
- segmentiranje lokalne mreže (IPv4/IPv6) – definiranje VLAN-ova i L3 mrežnih segmenata, translaciju privatnih IPv4 adresa u jednu ili više javnih IPv4 adresa,
- definiranje L3/L4 sigurnosnih pravila (IPv4/IPv6),
- osiguravanje kvalitete usluge (QoS – engl. *Quality of Service*), klasificiranje prometa i ograničavanje prometa (engl. *traffic shaping*),
- DHCP servis za LAN klijente,
- kontroler za bežičnu mrežu (engl. *Wireless controller*).

4.2.2 Konfiguracijske značajke sustava

Osnovne konfiguracijske značajke mrežnog usmjerivača navedene su u nastavku.

Virtualni LAN-ovi (VLAN) i IP adresiranje prikazano je u tablici 2.

VLAN ID	Ime VLAN-a	Mrežni raspon
3	management	192.168.128.0/24
10	ucionice	192.168.30.0/23
11	dodatni_servis1	192.168.32.0/23
12	dodatni_servis2	192.168.34.0/23
13	gosti	192.168.36.0/23
14	eduroam	192.168.44.0/22
15	dodatni_servis3	192.168.40.0/23
16	postojeca_mreza	192.168.42.0/23
4094	fortilink	169.254.0.0/16

Tablica 2: VLAN i IP adresiranje

Opis namjene pojedinog VLAN-a:

- VLAN 3 je *management* VLAN i služi za upravljanje bežičnim pristupnim točkama,
- VLAN 10 služi za povezivanje dijeljenih učeničkih uređaja u odabranim učionicama na bežičnu mrežu *eSkole*. U isti VLAN smješta se oprema instalirana u učionicama (poput pametnih ploča). IP adrese iz tog segmenta dobivaju stručnjaci za tehničku podršku i nastavno osoblje spojeni na *eduroam* mrežu,
- VLAN 11, 12 i 15 služe za povezivanje i logičko odvajanje dodatnih servisa ako na lokaciji postoji potreba za odvajanje resursa od ostatka postojeće mreže (npr. video nadzor, poslužitelji),
- VLAN 13 služi za povezivanje gostiju na bežičnu mrežu *guest*. Brzina te mreže

- ograničena je na 50% ukupne brzine internetskog linka,
- VLAN 14 služi za povezivanje učenika i posjetitelja škole koji imaju dostupnu *eduroam* mrežu na svom uređaju. Brzina te mreže ograničena je na 50% ukupne brzine internetskog linka,
 - VLAN 16 služi za povezivanje postojeće mrežne infrastrukture na novu implementiranu mrežnu infrastrukturu,
 - VLAN 4094 služi za komunikaciju između Fortinet uređaja (usmjerivač i preklopnik komuniciranju preko *FortiLink* protokola).

Pristup svim potrebnim resursima omogućen je povezivanjem usmjerivača FortiGate 100F i Mikrotik usmjerivača (CPE). WAN1 sučelje na usmjerivaču FortiGate 100F povezano je na ETH 4 sučelje na Mikrotiku. Usmjerivač FortiGate 100F preko DHCP-a dobiva 3. adresu iz javnog /29 javnog raspona, koja se uz 4. adresu koristi za potrebe NAT-iranja privatnih mreža.

4.3 LAN mreža

U ovom poglavlju su opisani mrežni preklopnik i konfiguracijske značajke mrežnih preklopnika.

4.3.1 Mrežni preklopnik

Uloga mrežnih preklopnika je povezivanje uređaja na mrežnu infrastrukturu u pristupnom sloju mreže te 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 politika za pojedine segmente. Ovakav model implementacije ustaljena je praksa u mrežama i integracijama ovakve složenosti.

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

U sklopu implementiranog mrežnog rješenja u školama, ulogu mrežnih preklopnika imaju FortiSwitch uređaji. Implementirani su sljedeći modeli FortiSwitch preklopnika:

- **FS-224E-PoE**
- **FS-224D-FPoE**
- **FS-248E-FPoE**

Ovisno o količini i vrsti potrebnih sučelja te odgovarajućeg kapaciteta snage za napajanje bežičnih pristupnih točaka putem mrežnih preklopnika, u svaki mrežni ormar u kojem je terminirana nova pasivna mrežna infrastruktura, implementiran je određeni model mrežnog preklopnika.

Preklopnik FS-224E-PoE prikazan je na slici u nastavku.



Slika 15: Preklopnik FortiSwitch FS-224E-PoE

Preklopnik FortiSwitch FS-224E-PoE raspolaže s 24 GE (*engl. Gigabit Ethernet*) RJ45 sučelja, od kojih 12 sučelja ima PoE (*engl. Power Over Ethernet*) funkcionalnost i s 4 GE (*engl. Gigabit Ethernet*) SFP sučelja. Maksimalna izlazna snaga (*engl. PoE Output Limit*) na nivou preklopnika je 180W (*engl. Watt*).

Preklopnik FS-224D-FPoE prikazan je na slici u nastavku.



Slika 16: Preklopnik FortiSwitch FS-224D-FPoE

Preklopnik FortiSwitch FS-224D-FPoE raspolaže s 24 GE (*engl. Gigabit Ethernet*) RJ45 sučelja, sva sučelja imaju PoE (*engl. Power Over Ethernet*) funkcionalnost i sa 4 GE (*engl. Gigabit Ethernet*) SFP sučelja. Maksimalna izlazna snaga (*engl. PoE Output Limit*) na nivou preklopnika je 370W (*engl. Watt*).

Preklopnik FS-248E-FPoE prikazan je na slici u nastavku.



Slika 17: Preklopnik FortiSwitch FS-248E-FPoE

Preklopnik FortiSwitch FS-248E-FPoE raspolaže sa 48 GE (engl. *Gigabit Ethernet*) RJ45 sučelja, sva sučelja imaju PoE (engl. *Power Over Ethernet*) funkcionalnost i sa 4 GE (engl. *Gigabit Ethernet*) SFP sučelja. Maksimalna izlazna snaga (engl. *PoE Output Limit*) na nivou preklopnika je 740W (engl. *Watt*).

Preklopnici unutar BD ormara povezani su direktno na usmjerivač. Svi preklopnici unutar jednog FD ormara povezani su na jedan preklopnik unutar ormara. Veze između BD i FD ormara realizirane su putem optičkih veza, i pomoću višemednih optičkih modula (FN-TRAN-SX) ili jednomodnih optičkih modula (FN-TRAN-LX).

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



Slika 18: Višemedni optički modul FN-TRAN-SX

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



Slika 19: Jednomodni optički modul FN-TRAN-LX

Funkcionalnosti preklopnika FortiSwitch u sklopu implementiranog mrežnog rješenja:

- centralizirano upravljanje putem sustava za nadzor i upravljanje mrežom,
- tzv. *Zero-touch* instalacija uređaja bez postavljanja inicijalne konfiguracije, putem sustava za nadzor i upravljanje mrežom,
- segmentacija mreže na više virtualnih mreža – VLAN-ova,
- STP (engl. *Spanning Tree Protocol*) funkcionalnost,
- prihvat klijentskih računala te bežičnih pristupnih točaka,
- sigurnosne mogućnosti,
- napajanje za spajanje bežičnih pristupnih točaka na sučeljima preklopnika.

4.3.2 Konfiguracijske značajke sustava

Osnovne konfiguracijske značajke mrežnih preklopnika navedene su u nastavku.

Virtualni LAN-ovi (VLAN) koji se primjenjuju na preklopticima prikazani su u tablici 3.

VLAN ID	Ime VLAN-a
3	management
10	ucionice
11	dodatni_servis1
12	dodatni_servis2
13	gosti
14	eduroam
15	dodatni_servis3
16	postojeca_mreza

Tablica 3: Popis i oznake VLAN-ova koji se primjenjuju na preklopticima

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

Integracija postojeće mreže škole 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 16. Putem ove mrežne integracije uređaji na postojećoj mreži dobivaju IP adrese od DHCP poslužitelja s usmjerivača.

Ako je na sučelje spojena bežična pristupna točka, tada je sučelje postavljeno u način rada koji dozvoljava propuštanje više VLAN-ova (engl. *Trunk Mode*), čime je omogućena komunikacija uređajima spojenima na bežične mreže (VLAN-ovi 10, 13 i 14). Na sučeljima je omogućena i opcija PoE (engl. *Power Over Ethernet*) koja osigurava napajanje bežičnih pristupnih točaka preko pasivne mrežne infrastrukture.

Na preklopnicima je konfiguriran i STP protokol (engl. *Spanning Tree Protocol*) koji prilikom pojave preklapne petlje onemogućuje sučelja, kako bi se izbjegle petlje unutar ostatka mrežne topologije.

4.4 Bežična mreža

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

4.4.1 Bežična pristupna točka

Uloga pristupne točke je odašiljanje bežičnog signala za pristup mrežnoj infrastrukturi te služi za pokrivanje prostora unutar škola bežičnim signalom. U svakoj školi instaliran je veći broj bežičnih pristupnih točaka, a implementirani sustav podržava mobilnost klijenata bez prekida u komunikaciji prilikom prijelaza klijenata s jedne na drugu bežičnu pristupnu točku. Raspored i montaža bežičnih pristupnih točki obavljena je sukladno DIS-u pasivne mrežne infrastrukture škole.

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

U sklopu implementiranog mrežnog rješenja u školama, ulogu bežične pristupne točke ima uređaj **FortiAP U431F-E**.

U implementiranom rješenju bežične pristupne točke koriste funkcionalnost kontrolera za bežičnu mrežu u sklopu usmjerivača FortiGate 100F, a objema komponentama se upravlja putem sustava za nadzor i upravljanje mrežom.

Bežična pristupna točka **FortiAP U431F-E** prikazana je na slici u nastavku.



Slika 20: Bežična pristupna točka FortiAP U431F-E

Funkcionalnosti bežične pristupne točke FortiAP U431F u sklopu implementiranog mrežnog rješenja:

- centralizirano upravljanje putem sustava za nadzor i upravljanje mrežom,
- tzv. *Zero-touch* instalacija uređaja bez postavljanja inicijalne konfiguracije, putem sustava za nadzor i upravljanje mrežom,
- podrška za IEEE 802.11a/b/g/n/ac standarde,
- istovremeni rad na 2,4 i 5 GHz frekvencijskom području,
- zasebni radio za dedikirano skeniranje, koji se ne koristi za prijenos korisničkih podataka već isključivo za kontinuiranu WIDS/WIPS analizu te analizu i optimizaciju korištenja RF (engl. *Radio Frequency*) spektra,
- automatska RF optimizacija mreže,
- korištenje 4x4 MU-MIMO tehnologije,
- MU-MIMO i OFDMA funkcionalnosti u odlaznom (engl. *uplink*) i dolaznom (engl. *downlink*) smjeru,
- podrška za 802.1x autentikacijske mehanizme i AES enkripciju,
- autentikacija korisnika na mrežu preko zaštitnog portala (*Captive portal*) korištenjem imeničkih sustava,
- podrška za implementaciju QoS mehanizama,
- ograničavanje propusnosti po pojedinom SSID-u te klijentu.

4.4.2 Konfiguracijske značajke sustava

U svakoj školi definirane su tri bežične mreže, odnosno tri SSID-a:

- **eSkole** – služi za povezivanje uređaja u odabranim učionicama na bežičnu mrežu, odnosno za povezivanje uređaja koje koristi više različitih osoba,
- **eduroam** – služi za povezivanje učenika, nastavnika i ostalog osoblja na bežičnu mrežu, odnosno za povezivanje uređaja koji u pravilu koristi samo jedna osoba,
- **guest** – služi za povezivanje vanjskih posjetitelja i partnera na bežičnu mrežu.

U nastavku su opisani konfiguracijski parametri svake od navedenih mreža.

Za pristup mreži **eSkole** koriste se sljedeći parametri:

- PSK (engl. *pre-shared key*) za autentikaciju korisnika i pristup na ograničenu bežičnu mrežu (*walled garden*, privremeni PSK koji stručnjak za tehničku podršku mreže može po želji zamijeniti je: `eskole123#`),
- WPA2 (engl. *Wi-Fi Protected Access*) enkripcija podataka na pristupnom sloju bežične mreže,
- *Captive portal* za autentikaciju korisnika prilikom pristupa Internetu. Za autentikaciju se koristi `AAI@EduHr` sustav,

- nakon pristupa mreži *eSkole*, korisnici pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23.

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

- 802.1X enterprise RADIUS autentikacija uz WPA2 enkripciju podataka ,
- za pristup mreži *eduroam* koristi se protokol TTLS-PAP. Detaljnije upute se mogu naći na mrežnoj adresi installer.eduroam.hr,
- za autentikaciju se koristi AAI@EduHr sustav,
- korisnici nakon pristupa mreži *eduroam* pripadaju u VLAN 14 i imaju IP adresu iz mreže 192.168.44.0/22, osim ako se radi o nastavnicima koji tada pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23,
- ako se ne radi o nastavnicima, za navedenu se mrežu propusnost limitira na 50 % ukupne propusnosti linka.

Za pristup mreži **guest** koriste se sljedeći parametri:

- otvoren pristup mreži uz mogućnost *Captive* portal autentikacije za pristup na okosnicu CARNET mreže,
- za autentikaciju se koristi baza korisnika iz ponuđenog sustava za upravljanje i nadzor. Kako bi stručnjak za tehničku podršku gostu omogućio pristup Internetu, mora njegovu e-mail adresu unijeti u sustav,
- nakon pristupa mreži *guest*, korisnici pripadaju u VLAN 13 i imaju IP adresu iz mreže 192.168.36.0/23,
- za navedenu mrežu se limitira propusnost na 50 % ukupne propusnosti linka prema Internetu.

U nastavku su navedene upute za spajanje na svaku od navedenih mreža.

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

- **Settings / Connections / Wifi**,
- Odaberi bežičnu mrežu **eSkole**,
- U **Password** polje unijeti PSK – privremeni PSK koji stručnjak za tehničku podršku mreže može po želji zamijeniti je: **eskole123#**
- Prilikom pristupa na okosnicu CARNET mreže u pretraživaču se otvara **Captive portal** za autentikaciju i ovdje je potrebno unijeti svoje **AAI vjerodajnice (korisničko ime u obliku „ime.prezime@skole.hr“ i lozinku)**.

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

- **Settings / Connections / Wifi**,
- Odaberi bežičnu mrežu **eduroam**,
- **EAP method** postaviti na **TTLS**,
- **PHASE 2 authentication** postaviti na **PAP**,
- U **CA certificate** polju **nije potrebno mijenjati postavke**,

- U **Identity** polje unijeti svoje **AAI korisničko ime (u obliku „ime.prezime@skole.hr“)**,
- Polje **Anonymus identity** **ostaviti prazno**,
- U **Wireless password** polje unijeti svoju **lozinku za AAI**.

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

- **Settings / Connections / Wifi**,
- Odabрати bežičnu mrežu **guest**,
- Prilikom pristupa na okosnicu CARNET mreže u pretraživaču se otvara **Captive portal** za autentikaciju i ovdje je potrebno unijeti svoje **vjerodajnice (korisničko ime i lozinku)** koje je prethodno kreirao stručnjak za tehničku podršku.

5. Sustav za upravljanje i nadzor mreže

U ovom poglavlju su opisane osnovne sastavnice sustava i pregled glavnih upravljačkih funkcionalnosti u sustavu za upravljanje i nadzor mreže.

5.1 Osnovne sastavnice sustava

Upravljanje i nadzor mrežne infrastrukture ostvareno je implementacijom redundantnog, centraliziranog sustava koji omogućuje sljedeće:

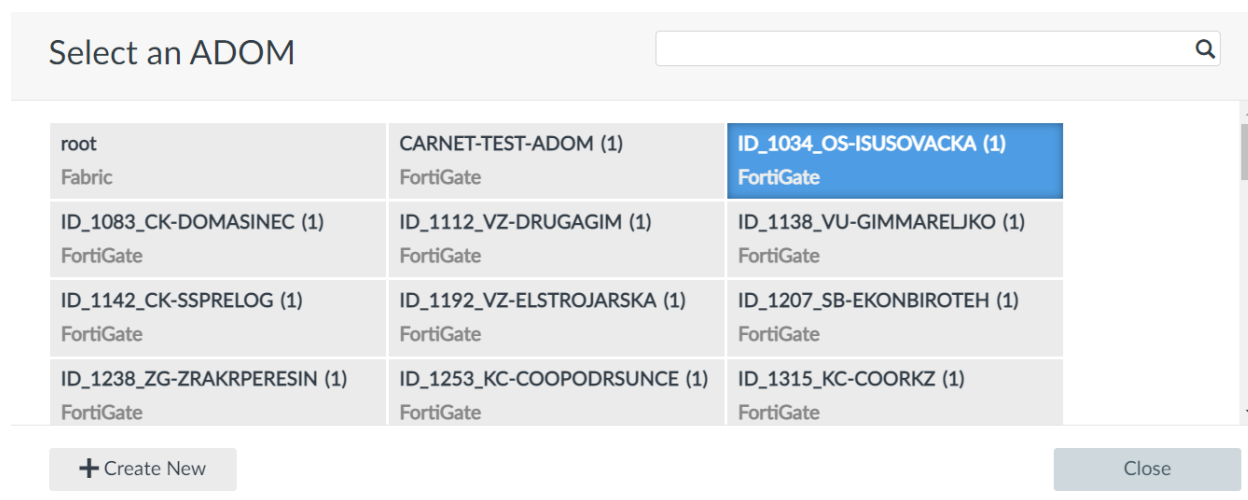
- upravljanje, konfiguraciju i nadzor kompletne mrežne infrastrukture instalirane u lokalnoj mreži škole (mrežni usmjerivači, mrežni preklopnici i bežične pristupne točke),
- instalaciju svih mrežnih uređaja i spajanje na sustav za upravljanje i nadzor bez prethodnog spajanja na uređaj i promjene tvorničkih postavki uređaja (engl. *Zero-touch Deployment*),
- konfiguraciju svih podržanih funkcionalnosti mrežnih uređaja implementiranih u lokalnoj mreži škole,
- odvojenost kontrolne razine od podatkovne razine sustava što omogućuje da samo kontrolni promet komunicira direktno sa serverima u podatkovnom centru, dok se klijentski promet usmjerava direktno na CARNET mrežu, te ne prolazi kroz sustav za upravljanje i nadzor mreže,
- integraciju mrežnog rješenja s autentikacijskom imeničkom infrastrukturom, u svrhu autentikacije na sam sustav za upravljanje i nadzor, kao i u svrhu autentikacije prilikom klijentskog pristupa mreži,
- podjelu sustava za upravljanje i nadzor na više neovisnih organizacijskih cjelina, tako da svaka škola može biti neovisan logički segment unutar sustava za upravljanje i nadzor,
- pristup jednoj ili više organizacijskih cjelina imenovanim administratorima sustava za upravljanje i nadzor,
- dijagnostiku mreže u stvarnom vremenu, udaljeni nadzor mreže, te generiranje redovitih izvještaja o statusu mreže i ponašanju korisnika spojenih na mrežu,
- visoku dostupnost sustava za upravljanje i nadzor.

Osnovne programske sastavnice sustava za upravljanje i nadzor mreže su **FortiManager** i **FortiAnalyzer** čije su glavne funkcionalnosti objašnjene u nastavku.

FortiManager je rješenje proizvođača Fortinet, i njegova uloga je centralni nadzor i upravljanje svim instaliranim uređajima implementiranog mrežnog sustava. Pruža uvid u cjelokupni sustav svih škola, objedinjujući upravljanje i nadzor nad svim mrežnim elementima.

Rješenje je implementirano u visoko dostupnoj konfiguraciji (HA – engl. *High Availability*), s po jednom instancom virtualne FortiManager komponente na primarnom i pričuvnom podatkovnom centru.

Jedna od ključnih karakteristika sustava je arhitektura sa više instanci (engl. *Multitenancy*) – svaka lokacija (škola, ustanova) u sustavu je definirana kao zasebna logička instanca, odnosno administrativna domena (ADOM). Takav pristup omogućuje centralno upravljanje i konfiguriranje svih uređaja na pojedinoj lokaciji, te definiranje specifičnosti koja su vezana isključivo za tu lokaciju (korisnici, pravila). Tako će npr. administrator sustava jedne škole imati uvid samo u uređaje koji su povezani s njegovom školom.



Slika 21: Odabir ADOM-a

FortiManager također podržava kontrolu pristupa sustavu zasnovanu na ulogama (engl. *role-based access*). Takav pristup ima prednosti u kompleksnom okruženju koje zahtjeva kontrolirani pristup računalnim resursima, gdje postoji velik broj korisnika i informacija.

Funkcionalnosti FortiManager rješenja u sklopu implementiranog mrežnog rješenja:

- jedinstveno upravljačko sučelje (engl. *single pane*) – upravljanje svim Fortinetovim mrežnim uređajima, uključujući FortiGate usmjerivače, FortiSwitch preklopnike, FortiAP bežične pristupne točke,
- automatizacija – reduciranje kompleksnosti korištenjem automatiziranih REST API procedura,
- centralno upravljanje sigurnosnim politikama i upravljanje uređajima,
- tzv. *Zero-touch* konfiguracija – orkestracija i automatizirano provizioniranje Fortinet uređaja (usmjerivača, preklopnika i bežičnih pristupnih točaka),
- implementacija i nadzor WAN mreže,
- upravljačka arhitektura sa više instanci,

- automatizirana procedura prikupljanja kopija konfiguracija (engl. *backup*),
- vidljivost kompletne mreže.



Slika 22: ADOM – kontrolna ploča aplikacije

FortiAnalyzer je rješenje proizvođača Fortinet za centralno prikupljanje i analizu logova i centralno izvještavanje o mrežnim aktivnostima.

Rješenje je implementirano u visoko dostupnoj konfiguraciji (HA – engl. *High Availability*), s po jednom instancom virtualne FortiAnalyzer komponente na primarnom i pričuvnom podatkovnom centru.

Kao i FortiManager, i FortiAnalyzer također podržava arhitekturu sa više instanci. FortiAnalyzer podržava granulaciju prava pristupa. Administratori pojedinih administrativnih domena imaju prava pristupa samo svojim cjelinama i mogu pregledavati zapise samo za svoje administrativne cjeline, odnosno škole.

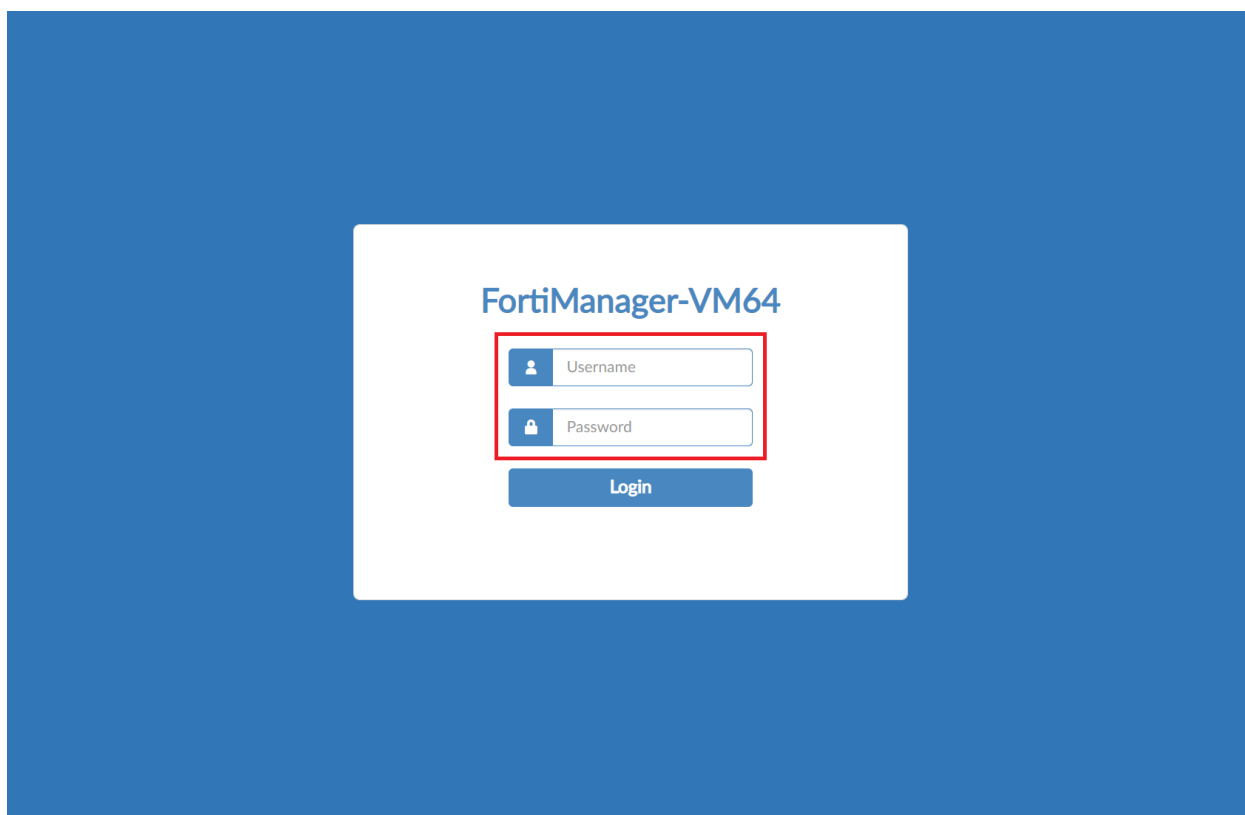
Funkcionalnosti FortiAnalyzer rješenja u sklopu implementiranog mrežnog rješenja:

- povećana vidljivost mreže – intuitivne sekcije mrežnog prometa, prijetnji, aplikacija i sl.,
- povećana vidljivost korisnika – korisnici bežične mreže, bežične pristupne točke,
- forenzika – detaljan uvid u mrežnu aktivnost korisnika,
- nadzor u realnom vremenu i izvještavanje,
- arhitektura sa više instanci (engl. *Multitenancy*),
- prostor za arhivu i analitiku,
- izvještavanje – predefinerani izvještaji, na zahtjev ili unaprijed definirani, fleksibilni formati izvještaja (HTML/CSV/XML/PDF).

5.2 Pregled glavnih upravljačkih funkcionalnosti

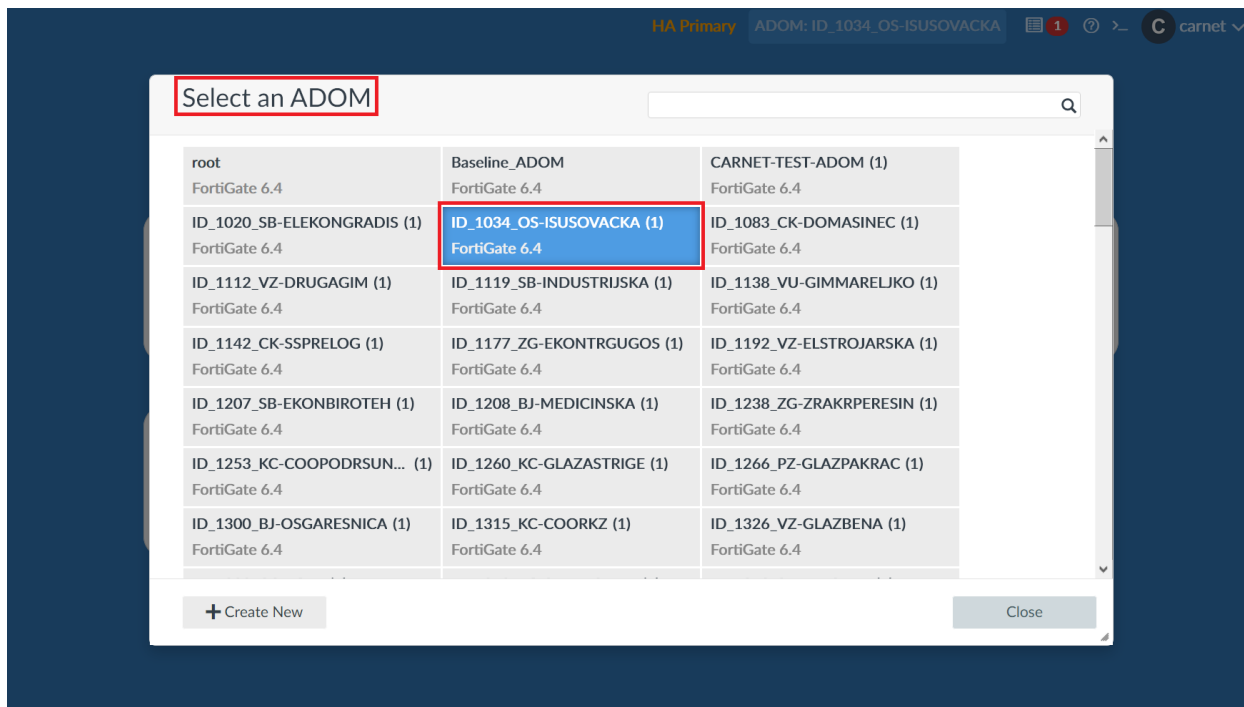
FortiManager komponenti centralnog sustava za upravljanje i nadzor mrežne opreme pristupa se upotrebom internetskog preglednika (poput Google Chrome, Mozilla Firefox, Microsoft Edge i dr.) preko IP adrese 193.198.236.16 (<https://mreza-fm.e-skole.hr>), koristeći HTTPS protokol (engl. *Hypertext Transfer Protocol Secure*).

Prijava na sustav vrši se unosom vjerodajnica u formi korisničkog imena i lozinke prethodno definiranih od strane administratora sustava.



Slika 23: FortiManager – prijava u sustav

Nakon uspješne prijave prikazuje se izbornik ADOM.



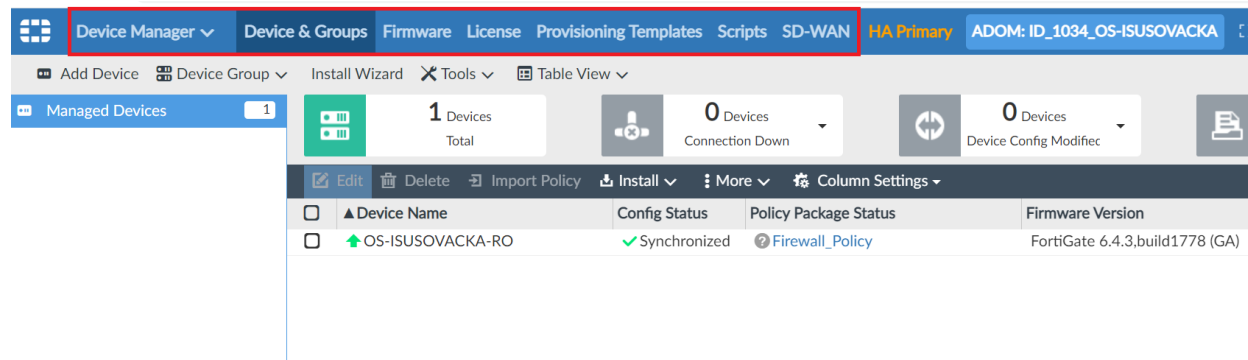
Slika 24: FortiManger ADOM – lista lokacija

Odabirom ADOM-a jedne od škola s popisa prikazuje se nadzorna ploča sa svim dostupnim opcijama unutar FortiManager-a.



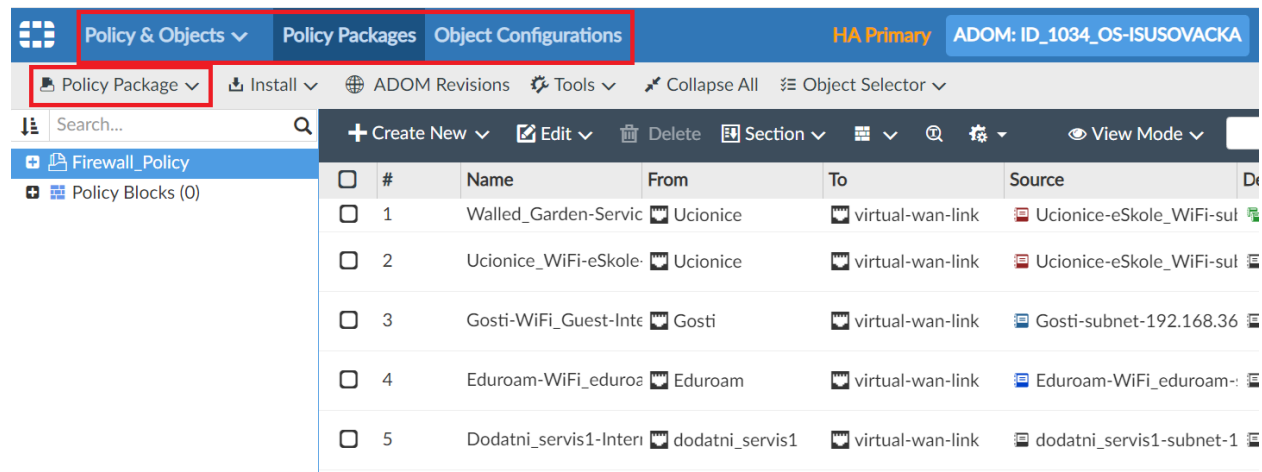
Slika 25: FortiManager ADOM – nadzorna ploča

Device Manager izbornik služi za konfiguraciju svih funkcionalnosti koje su dostupne na FortiGate usmjerivačima. Kroz ovu opciju se vrši konfiguracija samog uređaja (sučelja, DNS i DHCP servisa, itd.), nadogradnja programske podrške, licenciranje uređaja i ostale postavke.



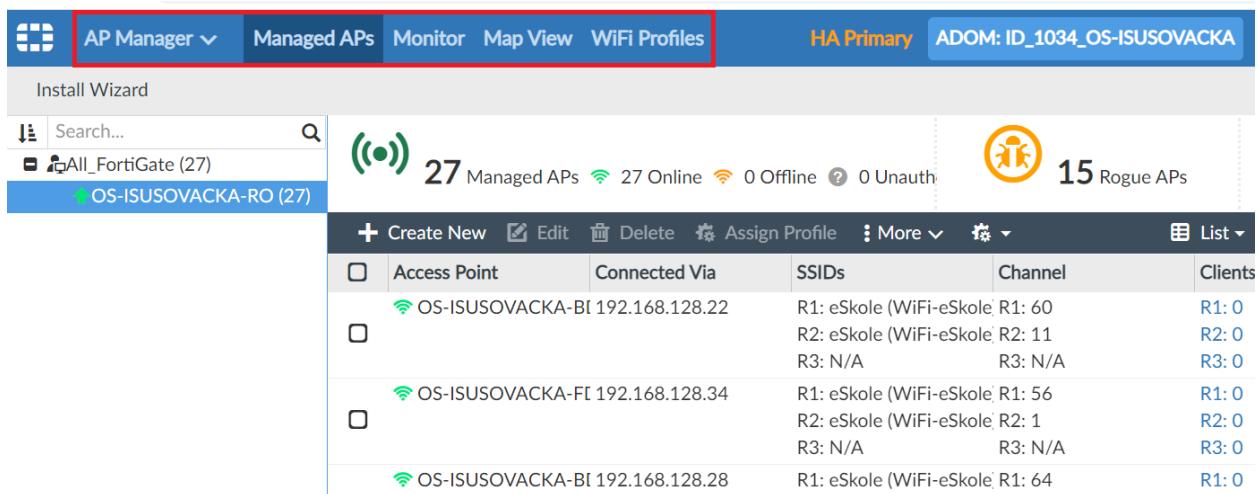
Slika 26: Device Manager – nadzorna ploča

Kroz **Policy & Objects** izbornik konfiguriraju se postavke vezane za vatrozid (objekti, pravila pristupa, itd.).



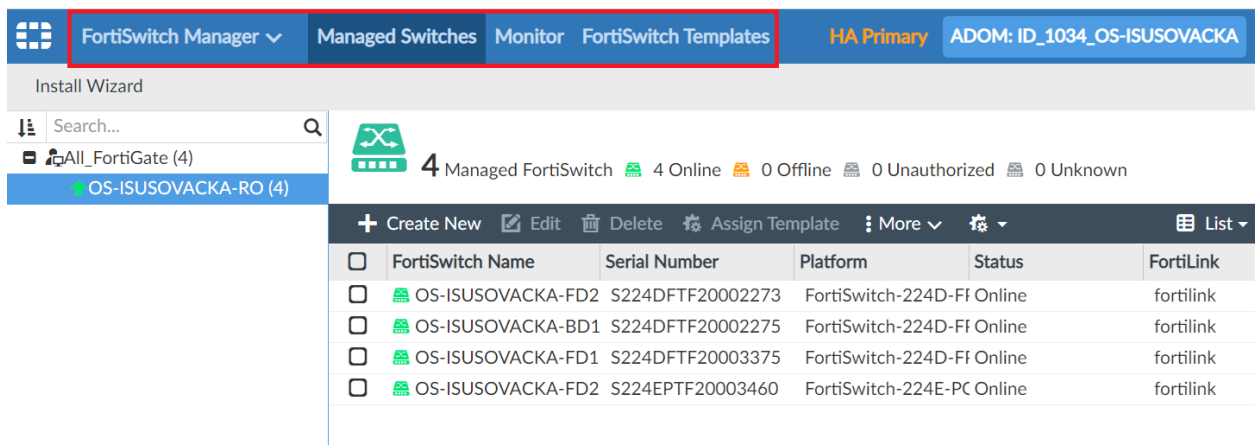
Slika 27: Policy & Objects – nadzorna ploča

AP Manager izbornik koristi se za konfiguraciju i nadzor bežičnih pristupnih točaka (naziv, WiFi profil, itd.).



Slika 28: AP Manager – nadzorna ploča

FortiSwitch Manager izbornik služi za konfiguraciju i nadzor preklopnika (definiranje VLAN-ova, sučelja preklopnika i ostalih funkcionalnosti kroz konfiguracijski predložak).



Slika 29: FortiSwitch Manager – nadzorna ploča

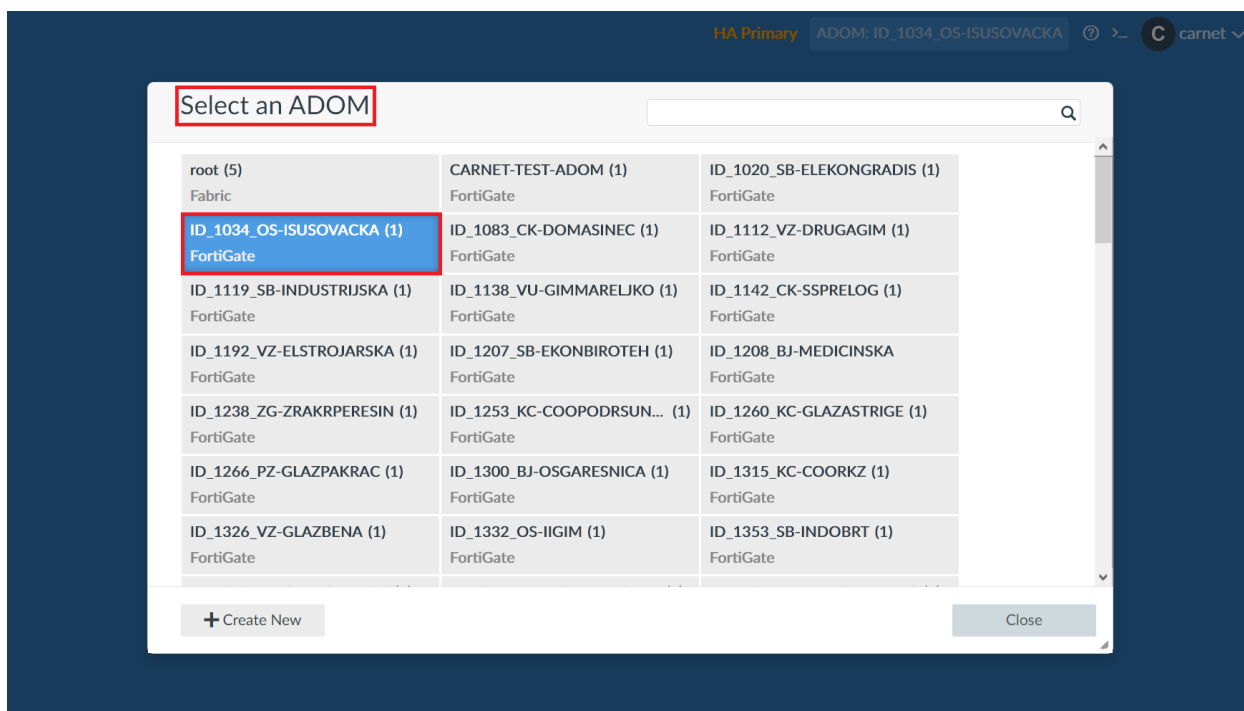
Na FortiAnalyzer komponentu centralnog sustava za prikupljanje i analizu logova i izvještavanje o mrežnim aktivnostima pristupa se upotrebom internetskog preglednika (poput Google Chrome, Mozilla Firefox, Microsoft Edge i dr.) preko IP adrese 193.198.236.20 (<https://mreza-fa.e-skole.hr>), koristeći HTTPS protokol (engl. *Hypertext Transfer Protocol Secure*).

Prijava na sustav vrši se unosom vjerodajnica u formi korisničkog imena i lozinke prethodno definiranih od strane administratora sustava.



Slika 30: FortiAnalyzer – prijava u sustav

Nakon uspješne prijave prikazuje se izbornik ADOM.



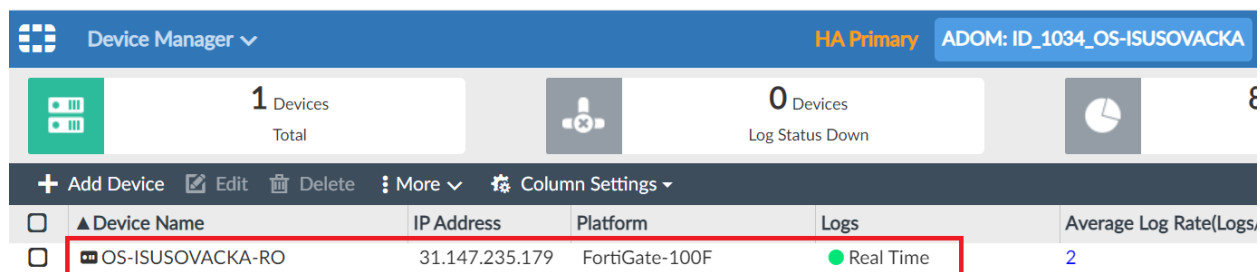
Slika 31: FortiAnalyzer ADOM – lista lokacija

Odabirom ADOM-a jedne od škola s popisa prikazuje se nadzorna ploča sa svim dostupnim mogućnostima FortiAnalyzer-a.



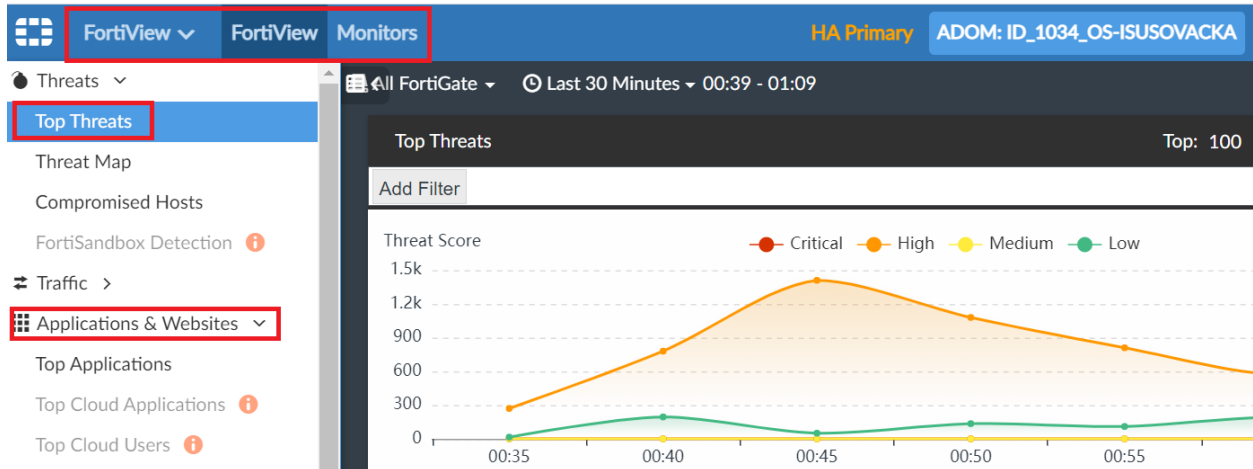
Slika 32: FortiAnalyzer ADOM – nadzorna ploča

Kroz **Device Manager** izbornik se unutar ADOM-a postavlja FortiGate usmjerivač koji se nalazi na lokaciji i komunicira direktno s FortiAnalyzer-om, te mu o svim mrežnim uređajima prosljeđuje informacije potrebne za analizu i izvještavanje.



Slika 33: Device Manager – nadzorna ploča

FortiView izbornik omogućuje praćenje i analizu prometa koji prolazi kroz usmjerivač (udio prometa po aplikacijama, stupanj sigurnosne ugroze, itd.).



Slika 34: FortiView – nadzorna ploča

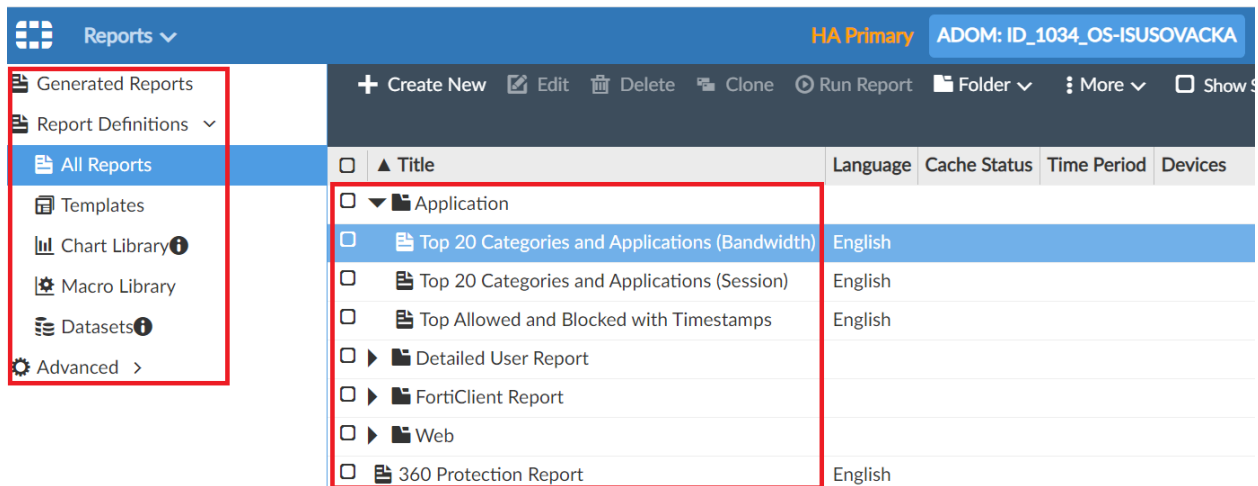
Log View izbornik se koristi za detaljni pregled prikupljenih logova sa svih Fortinet mrežnih uređaja koji čine računalnu mrežu na pojedinoj lokaciji. Ova opcija je posebno korisna prilikom otklanjanja poteškoća na mrežnim uređajima.

The screenshot shows the Log View dashboard. The top navigation bar includes 'Log View' and 'Monitors' tabs. The main content area displays a table of log entries for the last hour. The 'Security' menu item in the sidebar is highlighted. The table has columns for #, Date/Time, Level, Device ID, Action, and Message.

#	Date/Time	Level	Device ID	Action	Message
1	01:12:44	warning	FG100FTK200140...	antenna-defe...	AP OS-ISUSOVACKA-FD2-
2	01:11:23	notice	FG100FTK200140...	perf-stats	Performance statistics: aver
3	01:08:16	warning	FG100FTK200140...	antenna-defe...	AP OS-ISUSOVACKA-BD1-
4	01:06:23	notice	FG100FTK200140...	perf-stats	Performance statistics: aver
5	01:05:25	warning	FG100FTK200140...	antenna-defe...	AP OS-ISUSOVACKA-FD2-
6	01:02:42	warning	FG100FTK200140...	antenna-defe...	AP OS-ISUSOVACKA-FD2-
7	01:01:22	notice	FG100FTK200140...	perf-stats	Performance statistics: aver
8	00:59:31	warning	FG100FTK200140...		internal PS changes to good
9	00:59:31	warning	FG100FTK200140...		internal PS changes to bad s
10	00:58:41	information	FG100FTK200140...		DHCP statistics
11	00:58:41	information	FG100FTK200140...		DHCP statistics

Slika 35: Log View – nadzorna ploča

Reports izbornik se upotrebljava za izradu izvještaja koristeći prikupljene metrike sa svih Fortinet mrežnih uređaja na lokaciji.



Slika 36: Reports – nadzorna ploča

6. Administracija i održavanje implementirane mrežne infrastrukture škole

U ovom poglavlju opisane su najvažnije značajke i koraci koji se primjenjuju prilikom administracije i održavanja mrežnih uređaja.

6.1 Spajanje mrežnog uređaja

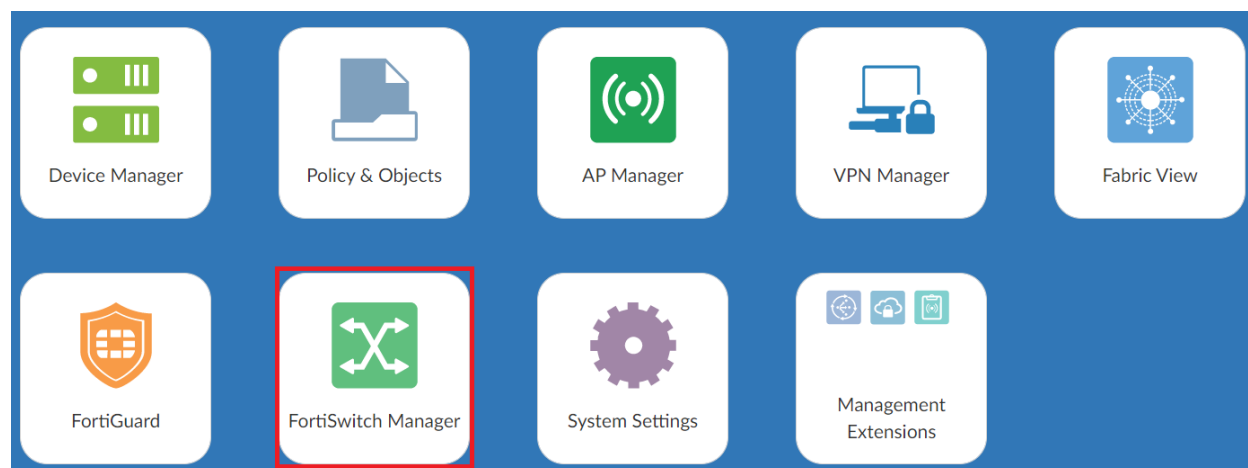
Cjelokupni sustav je zasnovan na konceptu upravljanja iz jednog sučelja. Za dodavanje novih uređaja u mrežu, sam uređaj na lokaciji spajanja nije potrebno konfigurirati, nego je dovoljno administratoru sustava javiti serijski broj uređaja, sučelje uređaja na koji se spaja te sučelje novog uređaja kojim će se spojiti, kako bi administrator na centralnom upravljačkom sustavu mogao definirati odgovarajuće konfiguracijske postavke (VLAN, STP i sl.).

Konfiguracijske postavke uređaja definirane su kroz predloške (engl. *template*) koji se primjenjuju na uređaj. Na taj način se smanjuje količina administrativnih zadataka kod prijave i inicijalne konfiguracije uređaja jer se ranije kreirani predlošci uređaja mogu višestruko koristiti.

Primjer definiranja preklopnika u BD ormaru:

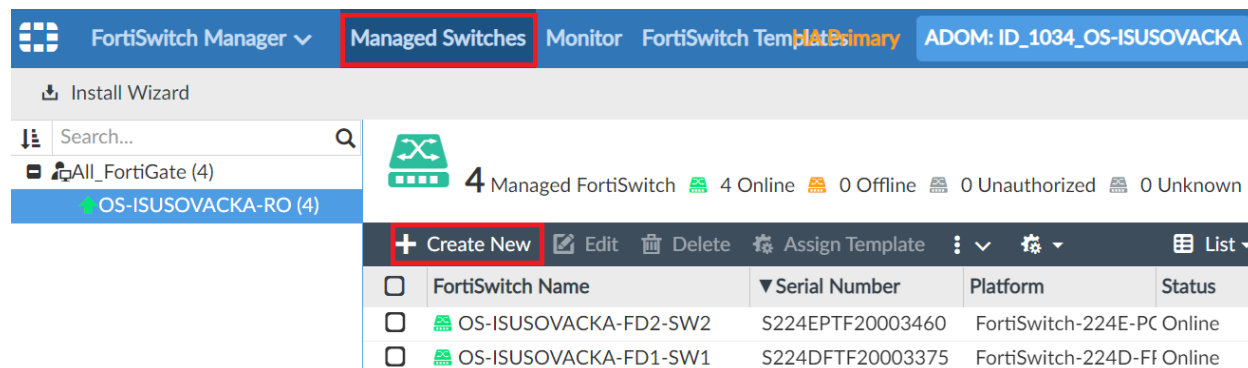
FortiManager / FortiSwitch Manager / Managed Switches / Create New

Za prijavu novog preklopnika u sustav, potrebno je odabrati izbornik *FortiSwitch Manager* unutar ADOM-a (škole).



Slika 37: FortiSwitch panel unutar ADOM-a (škole)

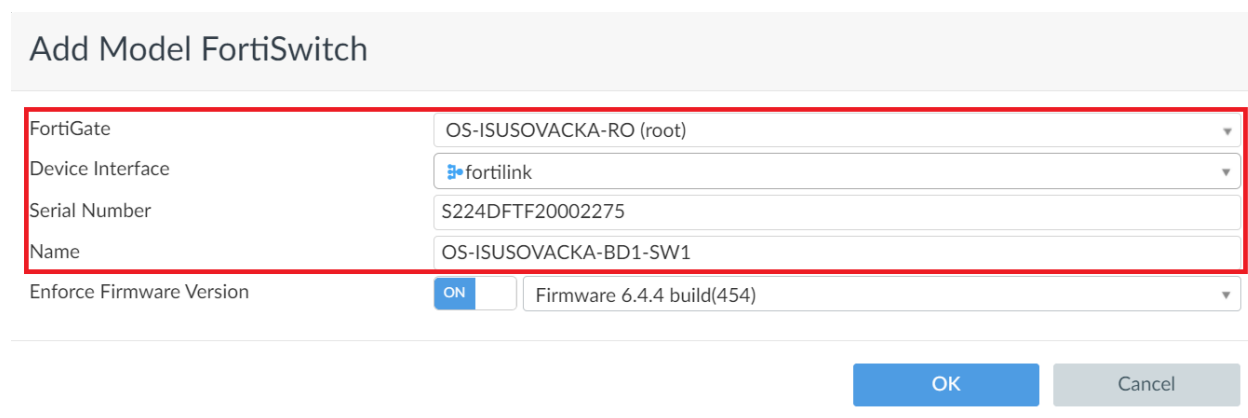
Nakon inicijalnog odabira, odabire se izbornik *Managed Switches* i zatim opcija za dodavanje novog preklopnika (*Create New*).



Slika 38: Prikaz procesa dodavanja preklopnika

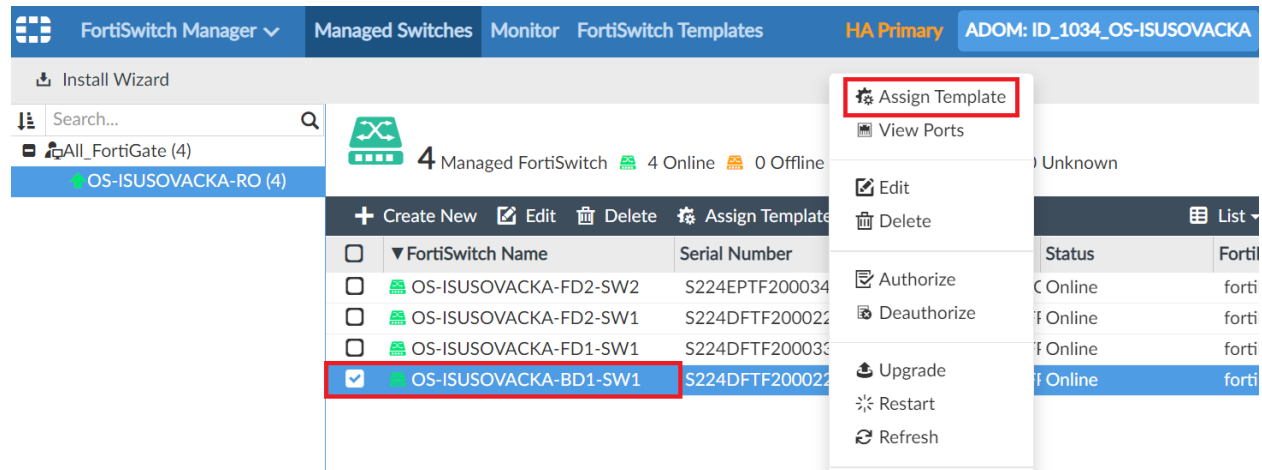
Na sljedećem se koraku pojavljuje prozor u kojem se definira:

- pripadajući usmjerivač na koji se veže preklopnik,
- sučelje,
- serijski broj preklopnika,
- ime uređaja prema definiranoj konvenciji imenovanja.



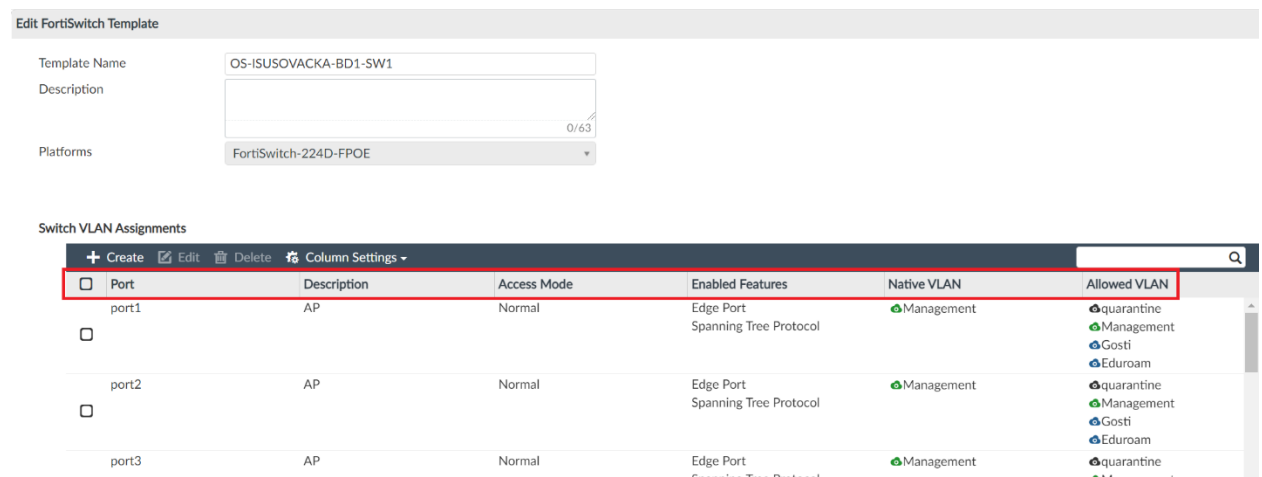
Slika 39: Definiranje preklopnika

Nakon inicijalnog koraka prijave preklopnika, treba mu pridružiti i pripadajući predložak (engl. *Assign Template*).



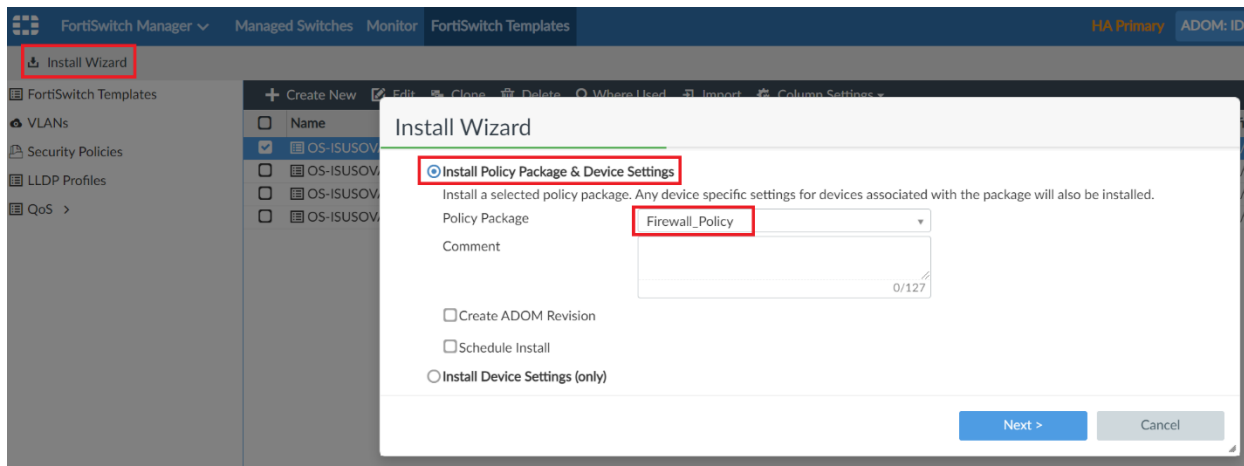
Slika 40: Pridruživanje predloška konfiguracije

U konfiguracijskom predlošku su inicijalno definirana sva sučelja na preklopniku, odnosno dozvoljene su podmreže. Kroz predložak koji se dodjeljuje preklopniku, definiraju se postavke na sučeljima, dozvoljene podmreže i ostala mrežna svojstva. Prijava preklopnika putem pridruživanja konfiguracijskog predloška smanjuje konfiguracijski korak u implementaciji i kasnije znatno pojednostavljuje administraciju samog sustava.



Slika 41: Predložak konfiguracije preklopnika

Nakon definiranja konfiguracijskog predloška i njegova dodjeljivanja pripadajućem preklopniku, potrebno je zadane radnje primijeniti na uređaj kroz instalacijski proces.



Slika 42: Iniciranje instalacijskog procesa

Nakon uspješnog pridruživanja konfiguracije uređaju, dobiva se potvrda od sustava o uspješnom izvršenju postupka (=OK).

Install Wizard - Policy Package (Firewall_Policy)

✔ Policy package (Firewall_Policy) is installed successfully.

100%

Total: 1/1, ✔ Success: 1, ⚠ Warning: 0, ❌ Error: 0

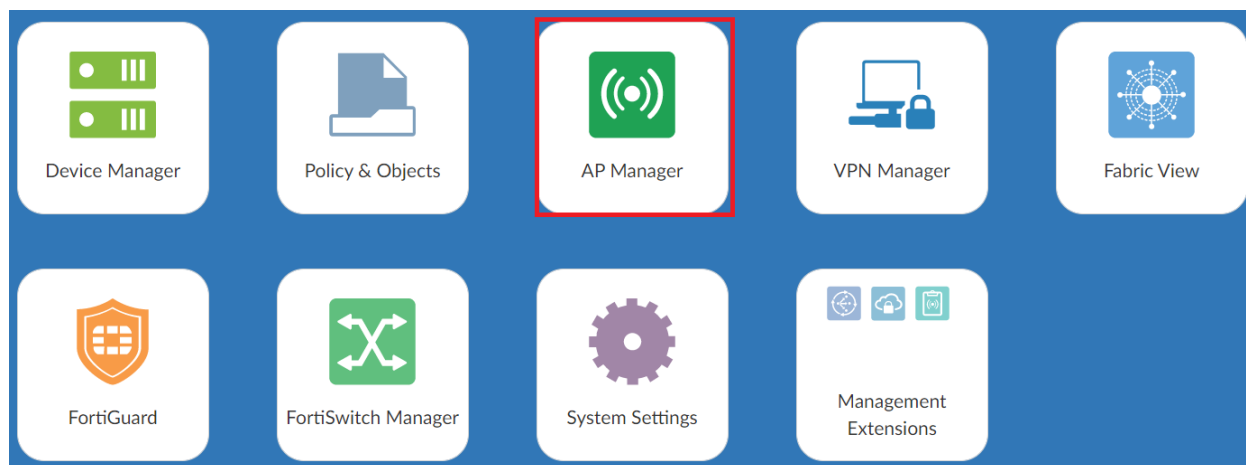
#	Name	Time Used	Status
1	OS-ISUSOVACKA-RO	8s	install and save finished status=OK

Slika 43: Prikaz uspješnog završetka instalacije

Primjer dodavanja bežične pristupne točke:

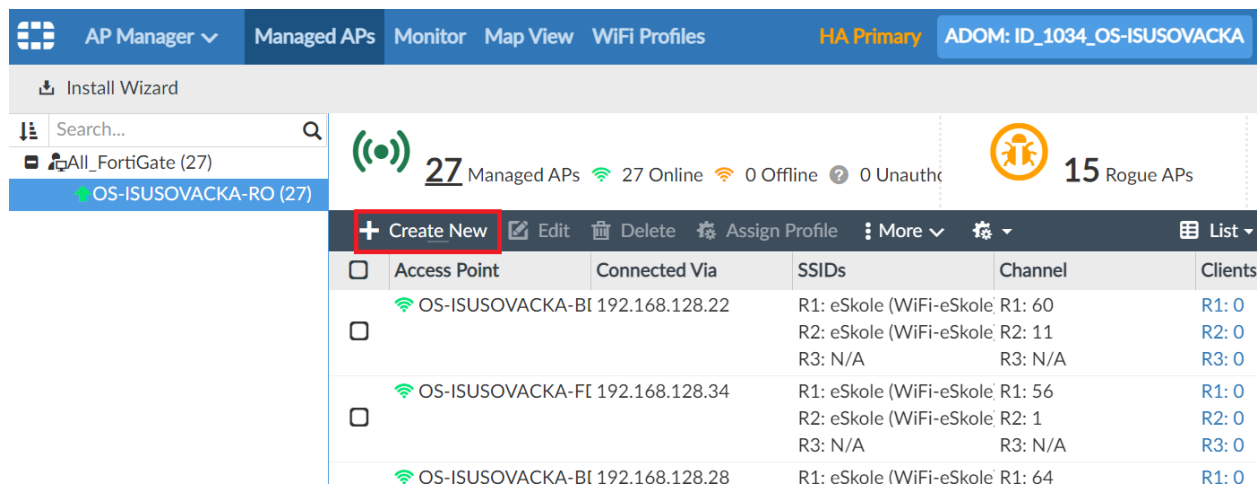
FortiManager / AP Manager / Managed APs / Create New

Za dodavanje bežične pristupne točke, potrebno je odabrati izbornik *AP Manager* unutar ADOM-a (škole) u kojoj treba dodati navedeni uređaj.



Slika 44: Prikaz izbornika AP Manager unutar ADOM-a (škole)

Nakon odabira izbornika, otvara se centralni panel na kojem su vidljive već prijavljene bežične točke na sustav (*Managed APs*). Za dodavanje nove točke, odabere se opcija za kreiranje nove točke (*Create New*).



Slika 45: Prikaz prijavljenih bežičnih pristupnih točaka i izbornika za kreiranje nove

Na sljedećem koraku pojavljuje se prozor pomoću kojeg se definira:

- FortiGate – odabire se pripadajući usmjerivač unutar ADOM-a,
- upisuje se pripadajući serijski broj (engl. *serial number*) bežične pristupne točke,
- ime uređaja (engl. *name*) prema ranije definiranoj konvenciji imenovanja uređaja u mreži,
- pripadajući profil (*AP Profile*).

Add Model FortiAP

FortiGate	OS-ISUSOVACKA-RO (root)	
Serial Number	PU431FTH20022730	
Name	OS-ISUSOVACKA-FD2-PP1-TO06-AP	
AP Profile	AP-profile-U431F	
Enforce Firmware Version	<input checked="" type="checkbox"/> ON	Firmware 6.0.4 build(80)

OK

Cancel

Slika 46: Dodavanje nove bežične pristupne točke

Ako treba kreirati vlastiti profil ili izmijeniti postojeći, odabire se izbornik *WiFi Profiles* i podizbornik *AP Profile*.

The screenshot shows the FortiGate AP Manager interface. The top navigation bar includes 'AP Manager', 'Managed APs', 'Monitor', 'Map View', and 'WiFi Profiles' (highlighted with a red box). The right side of the bar shows 'HA Primary' and 'ADOM: ID_1034_OS-ISUSOVACKA'. Below the navigation bar is an 'Install Wizard' button. On the left, a sidebar menu lists profile types: 'AP Profile' (highlighted with a red box), 'SSID', 'WIDS Profile', 'Bluetooth Profile', 'QoS Profile', and 'Bonjour Profile'. The main area is titled 'Edit AP Profile AP-profile-U431F' and contains the following configuration fields:

- Name: AP-profile-U431F
- Comments: (empty text area, 0/255 characters)
- Platform: FAPU431F
- Platform mode: Single 5G (selected), Dual 5G
- Country/ Region: Croatia
- AP Login Password: Set, Leave Unchanged (selected), Set Empty
- Administrative Access: HTTPS, SNMP, SSH
- Client Load Balancing: Frequency Handoff, AP Handoff
- Bluetooth Profile: None
- Radio 1 Mode: Disabled, Access Point (selected), Dedicated Monitor

Slika 47: Prikaz profila bežične pristupne točke

6.2 Vraćanje konfiguracije na tvorničke postavke

U ovom poglavlju su opisani postupci vraćanja konfiguracije na tvorničke postavke za bežične pristupne točke, preklopnike i usmjerivače.

6.2.1 Vraćanje bežične pristupne točke na tvorničke postavke

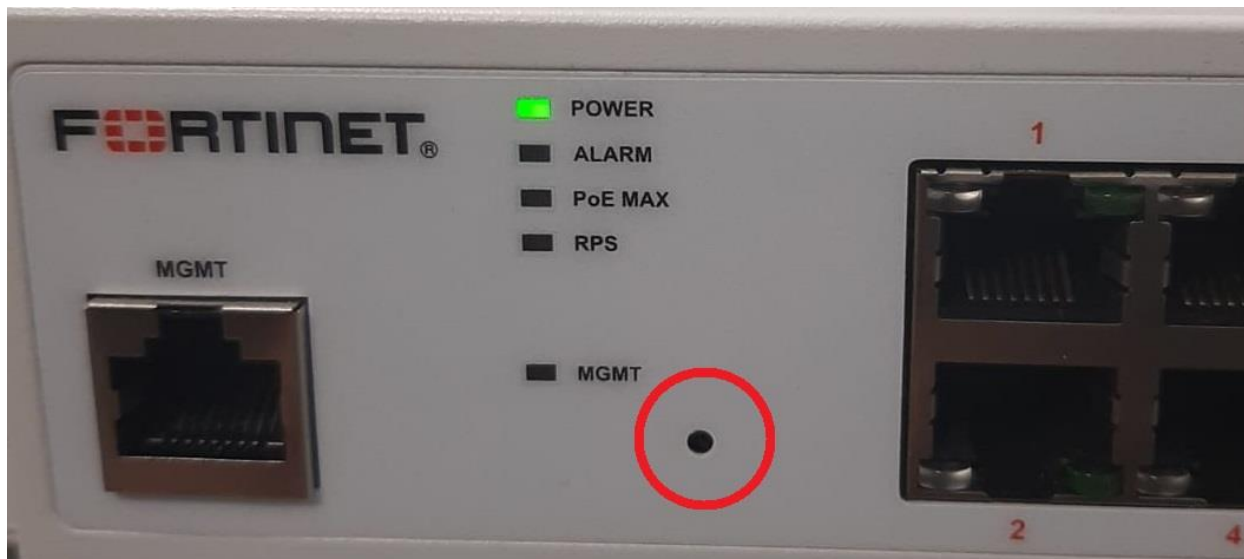
Bežična pristupna točka ima tipku za vraćanje na tvorničke postavke (*reset*). Na uključenom AP-u, pritisne se tipka tankim predmetom i drži 10 do 15 sekundi. Nakon navedenog postupka, slijedi ponovno pokretanje AP-a i treba pričekati 5 do 10 minuta kako bi bio spreman za novo konfiguriranje.



Slika 48: Forti AP – tipka za reset

6.2.2 Vraćanje preklopnika na tvorničke postavke

Vraćanje preklopnika na tvorničke postavke obavlja se pomoću tipke *reset*. Na uključenom preklopniku, pritisne se tipka tankim predmetom i drži 10 do 15 sekundi dok se ne ugasi *power* lampica koja indicira uključenost uređaja. Nakon navedenog postupka, slijedi ponovno pokretanje preklopnika i treba pričekati 5 do 10 minuta kako bi bio spreman za novo konfiguriranje.



Slika 49: FortiSwitch – tipka za reset

6.2.3 Vraćanje usmjerivača na tvorničke postavke

Vraćanje usmjerivača na tvorničke postavke obavlja se pomoću tipke *reset*. Na uključenom usmjerivaču, pritisne se tipka tankim predmetom i drži 20 sekundi dok lampica *STATUS* ne počne svijetliti narančasto i nakon toga crvenom bojom. Nakon popuštanja tipke uređaj je vraćen na tvorničke postavke.



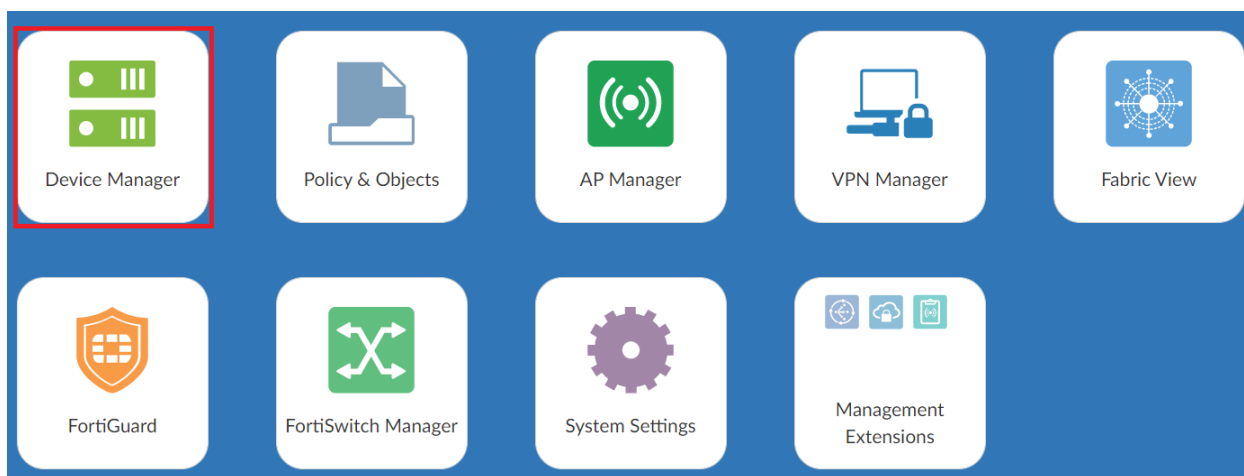
Slika 50: FortiGate – tipka za reset

6.3 Nadzor nad mrežnom opremom

Sučelje FortiManager-a se koristi za upravljačke funkcionalnosti, ali i za nadzor i uvid u stanje mrežne opreme u stvarnom vremenu.

Za uvid u status opreme, potrebno je odabrati opciju *Device Manager* unutar ADOM-a (škole) na kojem treba izvršiti željeni nadzor, odnosno pregled statusa instalirane opreme:

ADOM / Device Manager



Slika 51: Prikaz izbornika *Device Manager* unutar ADOM-a (škole)

Početna stranica je upravljačka ploča na kojoj se dodaju dodatni alati i mehanizmi koji omogućavaju brzi uvid u stanje uređaja i stanja na mrežnoj infrastrukturi.

The screenshot shows the FortiManager interface for a device named OS-ISUSOVACKA-RO. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. Below this is a toolbar with 'Add Device', 'Device Group', 'Install Wizard', 'Tools', and 'Table View'. The main content area is titled 'Managed Devices' and shows a search bar with 'OS-ISUSOVACKA-RO' entered. The device's 'System : Dashboard' is displayed, featuring a 'Summary' widget and a 'System Information' table. The table lists the following details:

System Information	
Host Name	OS-ISUSOVACKA-RO
Serial Number	FG100FTK20014043
IP Address	31.147.235.179 (wan1)
System Time	Thu Jan 28 02:18:38 2021 CET
Uptime	49 days 14 hours 51 minutes 52 seconds
Firmware Version	FortiGate 6.4.3,build1778 (GA)
Hardware Status	8 CPU, 3615 MB RAM
Operation Mode	NAT
VDOM	VDOM Disabled
Operation	> ✖ ⓘ

Slika 52: FortiManager – nadzorna ploča

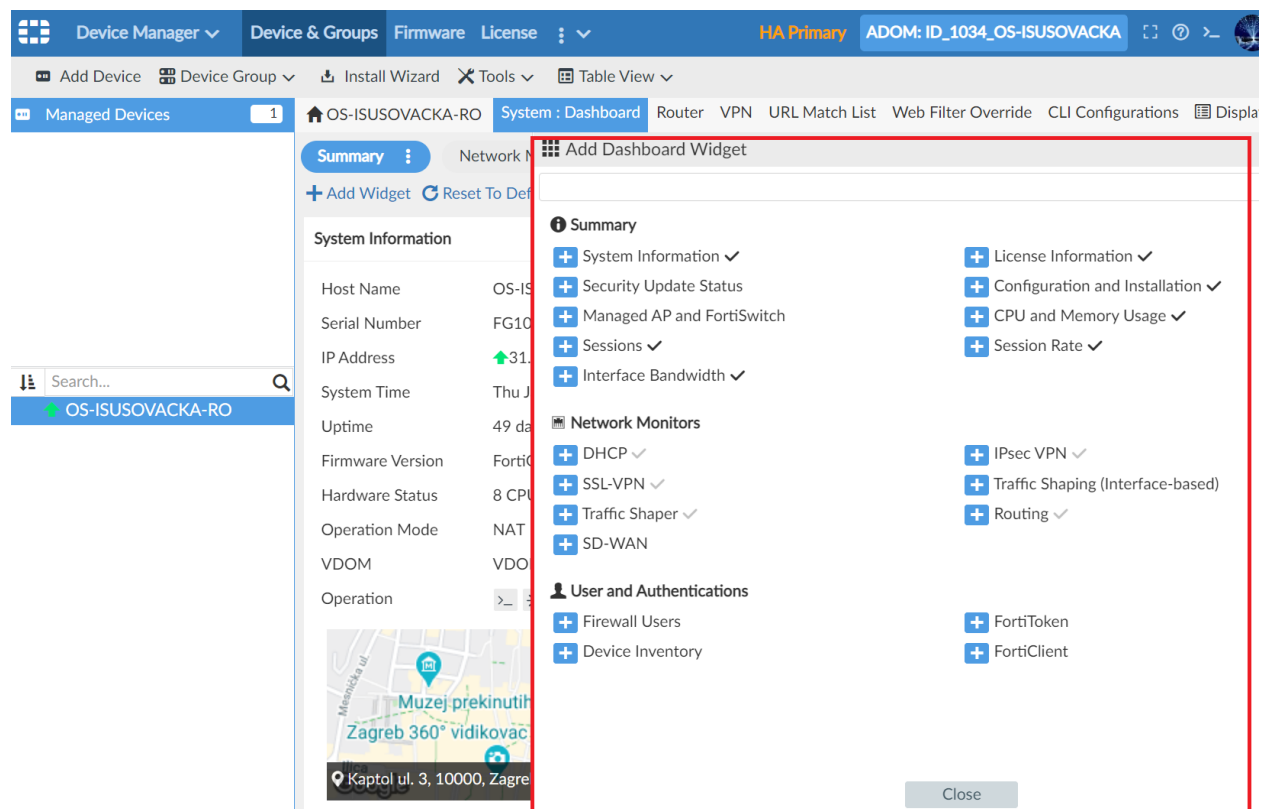
Za dodavanje dodatnih mehanizama, odnosno filtera za uvid u stanje opreme prema određenim parametrima, treba na centralnoj upravljačkoj ploči odabrati opciju:

System : Dashboard / Add Widget

The screenshot shows the Fortinet management console interface. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. Below this, there are buttons for 'Add Device', 'Device Group', 'Install Wizard', 'Tools', and 'Table View'. The main content area is titled 'Managed Devices' and shows a list of devices. The device 'OS-ISUSOVACKA-RO' is selected, and its 'System : Dashboard' is displayed. The dashboard includes a 'Summary' section with a '+ Add Widget' button highlighted in red. Below this is a 'System Information' section with a table of system details.

System Information	
Host Name	OS-ISUSOVACKA-RO
Serial Number	FG100FTK20014043
IP Address	31.147.235.179 (wan1)
System Time	Thu Jan 28 02:18:38 2021 CET
Uptime	49 days 14 hours 51 minutes 52 seconds
Firmware Version	FortiGate 6.4.3,build1778 (GA)
Hardware Status	8 CPU, 3615 MB RAM
Operation Mode	NAT
VDOM	VDOM Disabled
Operation	> * ⓘ

Slika 53: Dodavanje novog widgeta na upravljačku ploču



Slika 54: Kontrolna ploča FortiManagera – odabir widgeta

Informacije koje se nude podijeljene su u nekoliko osnovnih kategorija, kao što je prikazano na slici. Nadzor uređaja i mreže izvodi se kombiniranjem, odnosno odabirom svih ili samo pojedinih kategorija.

6.4 Nadzor nad klijentima na mreži

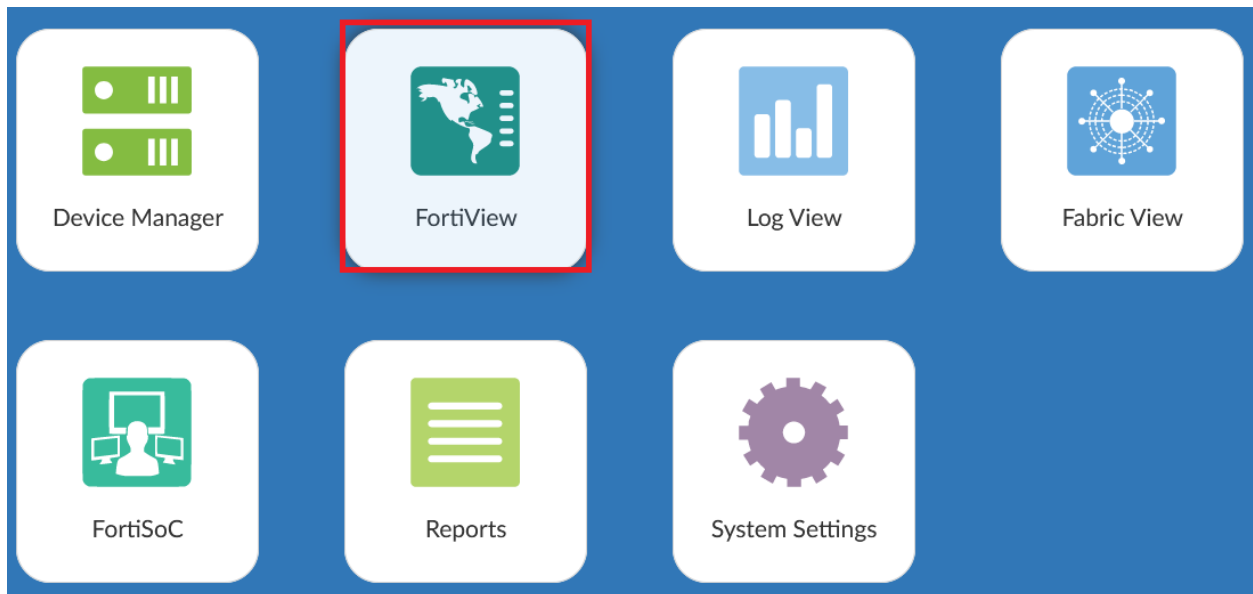
FortiAnalyzer daje uvid u ponašanje klijenata na mreži.

Usmjerivač FortiGate konfiguriran je tako da kod inicijalne prijave i implementacije šalje zapise o mrežnim aktivnostima na komponentu sustava FortiAnalyzer, koja ima ugrađene mehanizme za grupiranje i korelaciju zapisa po predefiniranim kriterijima.

Prvi korak je prijava na sustav FortiAnalyzer putem adrese mrežnog sučelja i unosa ranije definiranih vjerodajnica.

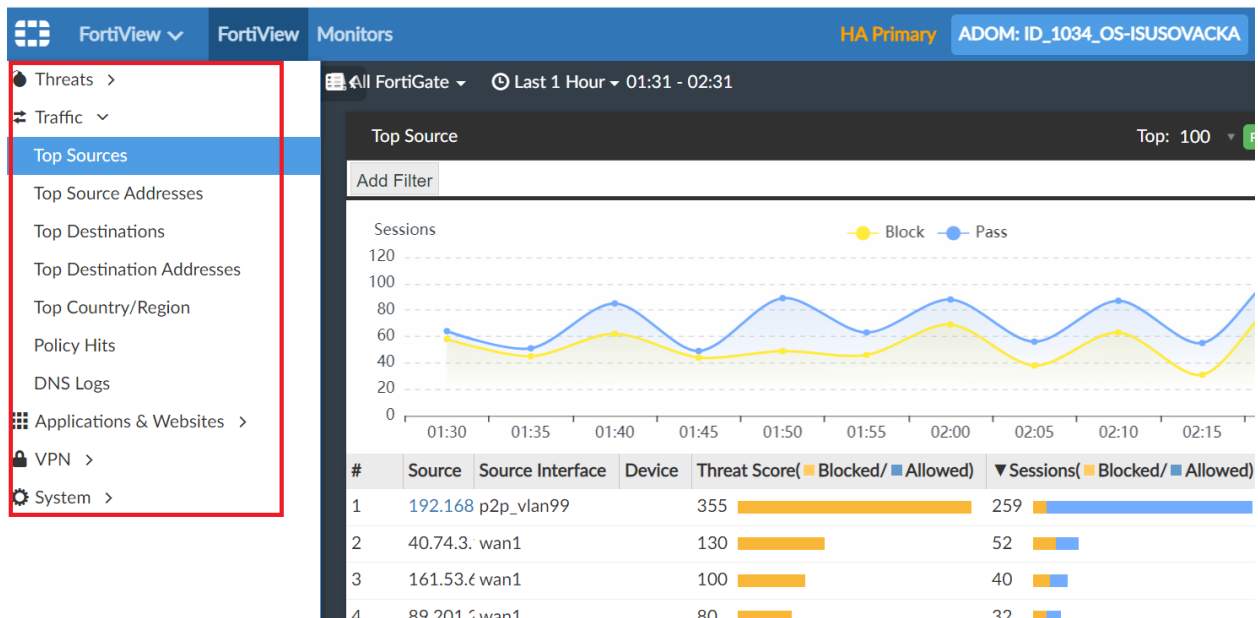
Za pristup nadzoru nad mrežom, odnosno aktivnostima njenih korisnika, potrebno je odabrati izbornik *FortiView* unutar ADOM-a (škole) na kojoj se izvodi nadzor:

ADOM / FortiView



Slika 55: Prikaz izbornika FortiView unutar ADOM-a (škole)

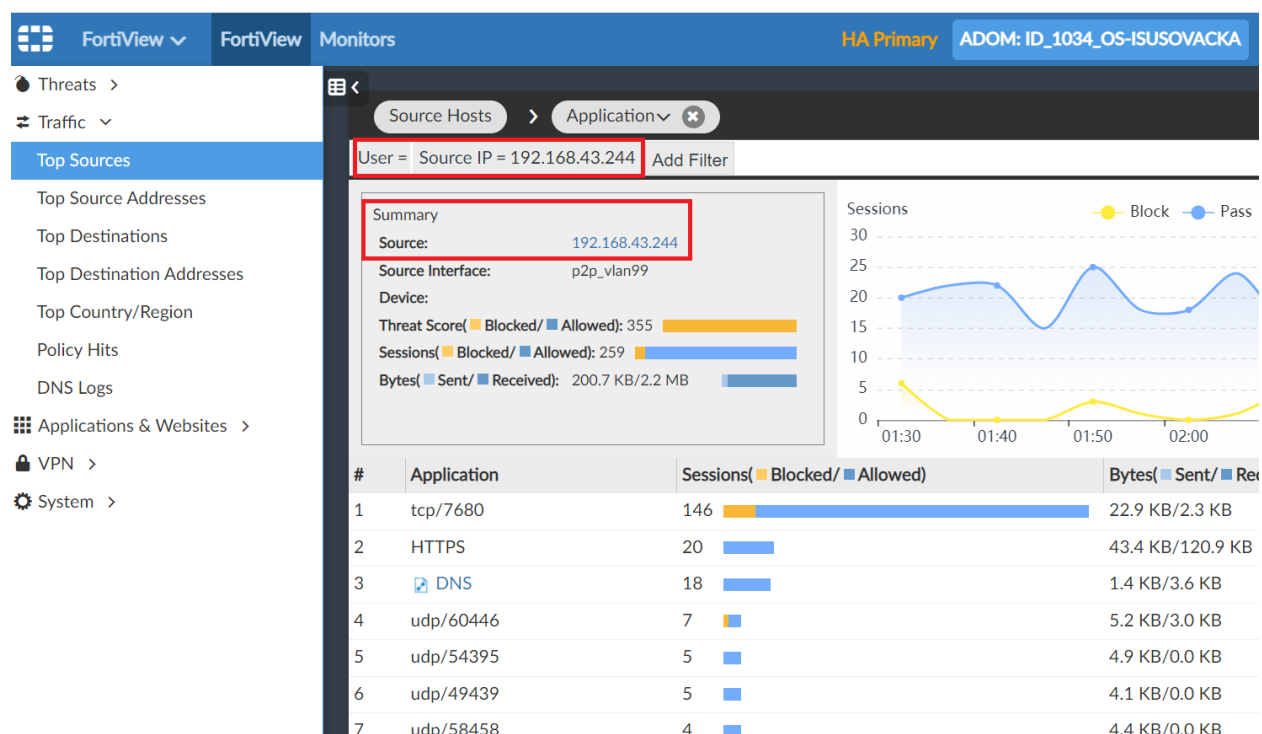
Nakon odabira, na centralnom panelu je prikazana sva mrežna aktivnost, odnosno promet koji je podijeljen u više kategorija.



Slika 56: FortiAnalyzer – izbornik FortiView

Može se odabrati mrežni promet prema destinacijama, odnosno promet filtriran prema adresi korisnika, tj. korisniku koji je prijavljen na sustav. To su ujedno i najčešći filtri koji se koriste u nadzoru nad sustavom.

Odabirom određenog korisnika ili njegove adrese se dolazi do detaljnije analize prometa i mrežnih protokola koji su inicirani od strane odabranog korisnika.

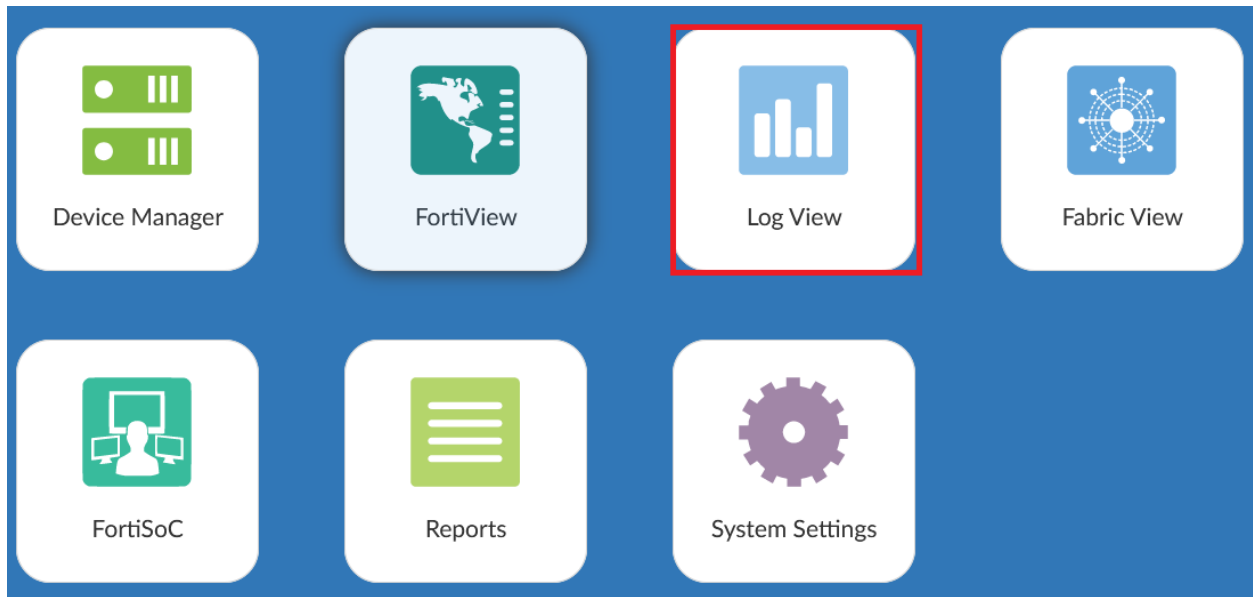


Slika 57: FortiAnalyzer – prikaz detaljne mrežne aktivnosti po korisniku

Za nadzor nad sustavom, na raspolaganju stoji i izbornik *Log View* pomoću kojeg se pregledava i pretražuje kompletan zapis o mrežnim aktivnostima unutar ADOM-a filtriran po raznim kriterijima.

Za pristup navedenom mehanizmu, na FortiAnalyzer-u unutar ADOM-a potrebno je odabrati izbornik *Log View*:

ADOM / Log View



Slika 58: Prikaz izbornika Log View unutar ADOM-a (škole)

Nakon odabira navedene opcije, na centralnom panelu je prikazana cjelokupna mrežna aktivnost u stvarnom vremenu. Aktivnost je podijeljena na više potkategorija i može se filtrirati prema prometu, sigurnosti i pojedinačnim događajima na samoj mreži.

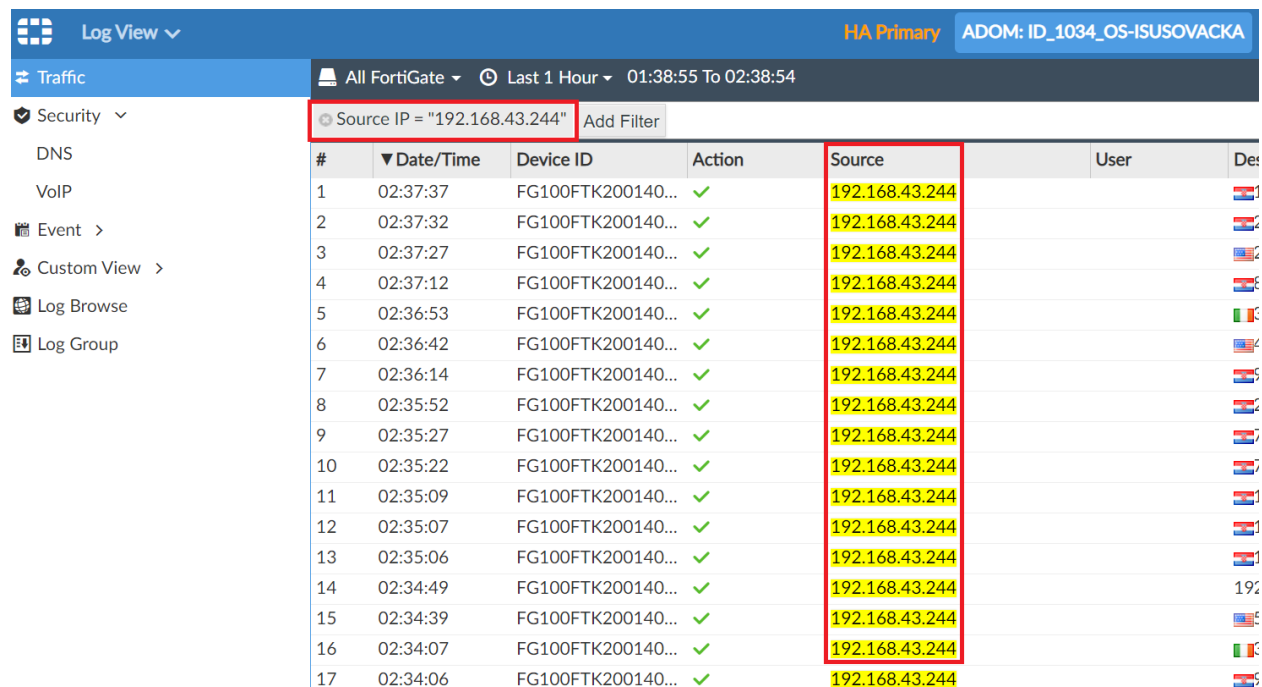
#	▼Date/Time	Device ID	Action	Source	User	Destination IP	Service	Ar
1	00:35:32	FG100FTK200140...	✓	115.51.90.198		31.147.235.180	tcp/8181	
2	00:35:32	FG100FTK200140...	✗ Policy viola...	194.147.142.72		31.147.235.181	tcp/12442	
3	00:35:32	FG100FTK200140...	✗ Policy viola...	194.147.142.247		31.147.235.181	tcp/6643	
4	00:35:32	FG100FTK200140...	✗ Policy viola...	194.147.142.247		31.147.235.182	tcp/8213	
5	00:35:28	FG100FTK200140...	✗ Policy viola...	220.163.125.148		31.147.235.182	tcp/19510	
6	00:35:23	FG100FTK200140...	✓	194.147.142.99		31.147.235.180	tcp/16178	
7	00:35:23	FG100FTK200140...	✓	194.147.142.72		31.147.235.180	tcp/14379	
8	00:35:23	FG100FTK200140...	✗ Policy viola...	194.147.142.247		31.147.235.182	tcp/5380	
9	00:35:23	FG100FTK200140...	✗ Policy viola...	194.147.142.72		31.147.235.181	tcp/14929	
10	00:35:22	FG100FTK200140...	✗ Policy viola...	194.147.142.72		31.147.235.181	tcp/11685	
11	00:35:18	FG100FTK200140...	✗ Policy viola...	194.147.142.211		31.147.235.182	tcp/3314	
12	00:35:13	FG100FTK200140...	✓	194.147.142.72		31.147.235.180	tcp/13120	
13	00:35:11	FG100FTK200140...	✓	192.168.42.184		217.146.23.161	tcp/5938	
14	00:35:11	FG100FTK200140...	✗ Policy viola...	194.147.142.247		31.147.235.181	tcp/8606	
15	00:35:08	FG100FTK200140...	✗ Policy viola...	194.147.142.72		31.147.235.181	tcp/10903	
16	00:35:08	FG100FTK200140...	✓	194.147.142.247		31.147.235.180	tcp/9842	
17	00:35:06	FG100FTK200140...	✓	194.147.142.99		31.147.235.180	tcp/16137	
18	00:35:06	FG100FTK200140...	✗ Policy viola...	194.147.142.72		31.147.235.182	tcp/13611	
19	00:35:06	FG100FTK200140...	✓		PU431FTH20029434	193.198.184.130	DNS	
20	00:35:06	FG100FTK200140...	✗ DNS error		PU431FTH20029434	193.198.184.130	DNS	

Slika 59: Prikaz panela Log View

Sljedeći primjer opisuje filtriranje prometa prema korisniku, odnosno njegovoj adresi.

Iznad popisa mrežne aktivnosti nalazi se traka s definiranim filtrima po kojima se filtriraju mrežne aktivnosti. Dodaje se opcija *Source IP* i upisuje IP adresa za koju treba vidjeti generiranu aktivnost, odnosno događaje.

Nakon unosa adrese, na panelu se prikazuje sav promet vezan na tu adresu.



The screenshot shows the Fortinet Log View interface. The top navigation bar includes 'Log View', 'HA Primary', and 'ADOM: ID_1034_OS-ISUSOVACKA'. The main area is titled 'Traffic' and shows a filter for 'Source IP = "192.168.43.244"'. The log table displays 17 entries, all with a source IP of 192.168.43.244. The table columns are: #, Date/Time, Device ID, Action, Source, User, and Destination. The 'Source' column is highlighted in yellow, and the filter text is enclosed in a red box.

#	Date/Time	Device ID	Action	Source	User	Des
1	02:37:37	FG100FTK200140...	✓	192.168.43.244		
2	02:37:32	FG100FTK200140...	✓	192.168.43.244		
3	02:37:27	FG100FTK200140...	✓	192.168.43.244		
4	02:37:12	FG100FTK200140...	✓	192.168.43.244		
5	02:36:53	FG100FTK200140...	✓	192.168.43.244		
6	02:36:42	FG100FTK200140...	✓	192.168.43.244		
7	02:36:14	FG100FTK200140...	✓	192.168.43.244		
8	02:35:52	FG100FTK200140...	✓	192.168.43.244		
9	02:35:27	FG100FTK200140...	✓	192.168.43.244		
10	02:35:22	FG100FTK200140...	✓	192.168.43.244		
11	02:35:09	FG100FTK200140...	✓	192.168.43.244		
12	02:35:07	FG100FTK200140...	✓	192.168.43.244		
13	02:35:06	FG100FTK200140...	✓	192.168.43.244		
14	02:34:49	FG100FTK200140...	✓	192.168.43.244		192
15	02:34:39	FG100FTK200140...	✓	192.168.43.244		
16	02:34:07	FG100FTK200140...	✓	192.168.43.244		
17	02:34:06	FG100FTK200140...	✓	192.168.43.244		

Slika 60: Log View – primjer filtriranog loga po adresi izvora

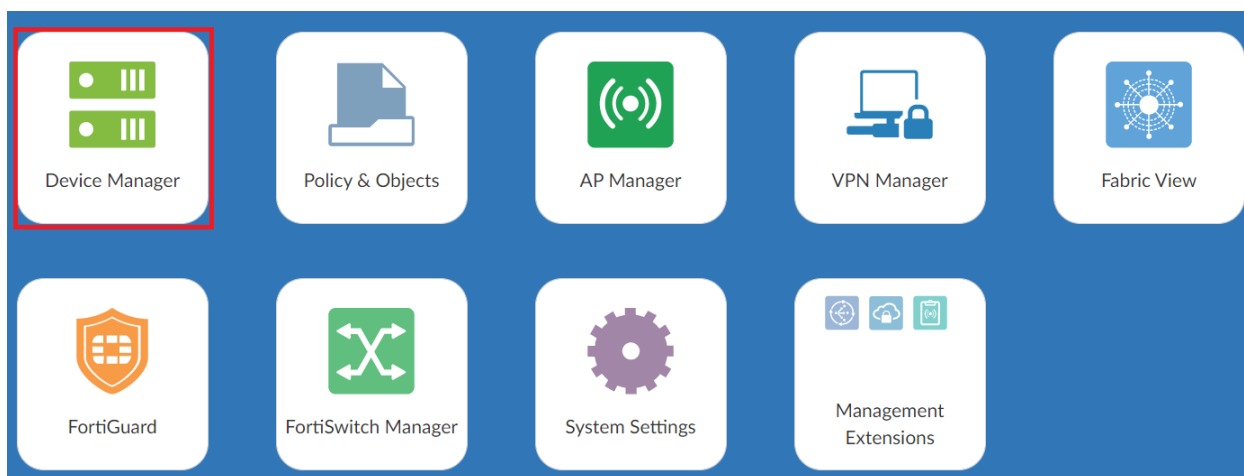
6.5 Konfiguracija osnovnih postavki na mrežnoj opremi

Sve promjene na sustavu i konfiguraciji rade se isključivo na FortiManager-u, a ne lokalno na opremi, jer u suprotnom konfiguracija uređaja ne bi bila sinkronizirana s FortiManager-om.

Na mrežne uređaje je postavljena inicijalna konfiguracija i odgovarajući broj SSID-a od strane CARNET-a kako bi se omogućilo optimalno korištenje mrežnih resursa. Ne preporuča se izmjena inicijalno postavljenih konfiguracija!

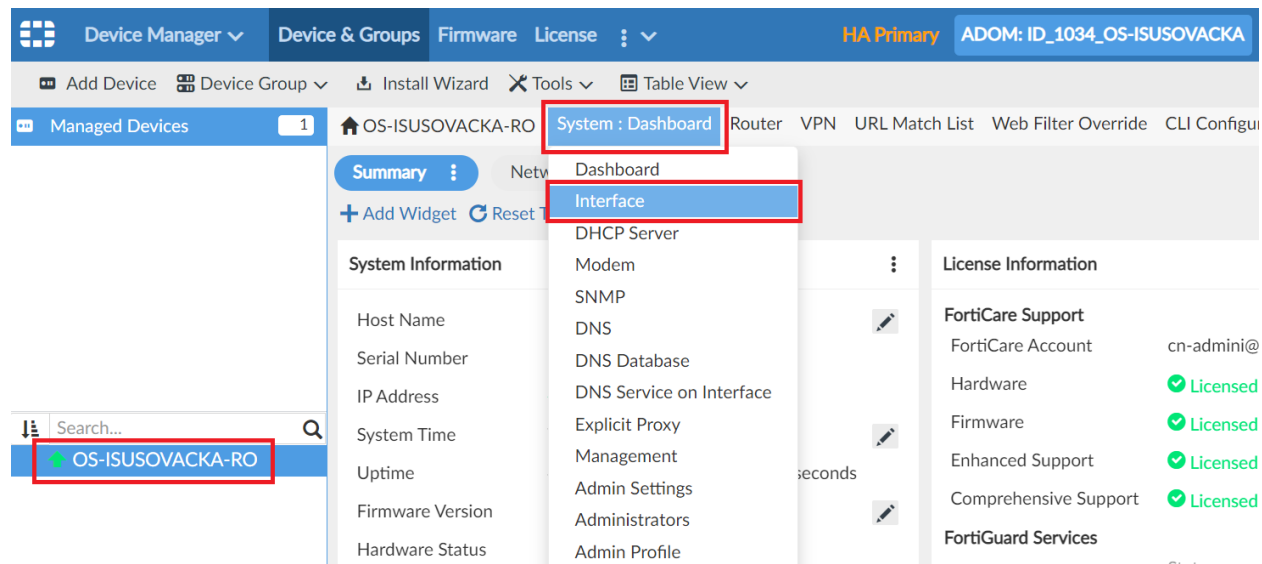
6.5.1 Primjer konfiguracije sučelja na usmjerivaču

Inicijalni korak u konfiguraciji sučelja je pristup izborniku *Device Manager* unutar ADOM-a (škole) na kojem treba izvršiti promjene na sustavu.



Slika 61: Device Manager – Kontrolna ploča

Device Manager / Dashboard / Interface / odabir sučelja koje je potrebno urediti:



Slika 62: FortiManager – kontrolna ploča za odabir sučelja

Nakon odabira opcije sučelja sa centralnog panela, otvara se prikaz popisa svih sučelja, odnosno virtualnih podmreža koje su dedicerane odabranom usmjerivaču.

The screenshot shows the FortiManager interface for configuring system interfaces on device OS-ISUSOVACKA-RO. The 'System : Interface' tab is active, displaying a table of interfaces. A red box highlights the Physical and VLAN interface rows.

<input type="checkbox"/>	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask
Physical (6)					
<input type="checkbox"/>	dmz	Physical	dmz	Manual	10.10.10.1/255.255.255.255
<input type="checkbox"/>	mgmt	Physical	mgmt	Manual	192.168.1.99/255.255.255.255
<input type="checkbox"/>	ha1	Physical	ha1	Manual	0.0.0.0/0.0.0.0
<input type="checkbox"/>	ha2	Physical	ha2	Manual	0.0.0.0/0.0.0.0
<input type="checkbox"/>	x1	Physical	x1	Manual	0.0.0.0/0.0.0.0
<input type="checkbox"/>	x2	Physical	x2	Manual	0.0.0.0/0.0.0.0
VLAN (14)					
<input type="checkbox"/>	default	VLAN		Manual	169.254.11.1/255.255.255.255
<input type="checkbox"/>	quarantine	VLAN		Manual	169.254.12.1/255.255.255.255
<input type="checkbox"/>	rspan	VLAN		Manual	169.254.13.1/255.255.255.255
<input type="checkbox"/>	voice	VLAN		Manual	169.254.14.1/255.255.255.255
<input type="checkbox"/>	video	VLAN		Manual	169.254.15.1/255.255.255.255
<input type="checkbox"/>	onboarding	VLAN		Manual	169.254.16.1/255.255.255.255
<input type="checkbox"/>	Management	VLAN	Management	Manual	192.168.128.1/255.255.255.255
<input type="checkbox"/>	Eduroam	VLAN	Eduroam	Manual	192.168.44.1/255.255.255.255
<input type="checkbox"/>	Gosti	VLAN	Gosti	Manual	192.168.36.1/255.255.255.255
<input type="checkbox"/>	Ucionice	VLAN	Ucionice	Manual	192.168.30.1/255.255.255.255
<input type="checkbox"/>	dodatni_servis1	VLAN	dodatni_servis1	Manual	192.168.32.1/255.255.255.255
<input type="checkbox"/>	dodatni_servis2	VLAN	dodatni_servis2	Manual	192.168.34.1/255.255.255.255
<input type="checkbox"/>	dodatni_servis3	VLAN	dodatni_servis3	Manual	192.168.40.1/255.255.255.255
<input type="checkbox"/>	p2p_vlan99	VLAN	p2p_vlan99	Manual	192.168.99.1/255.255.255.255
Aggregate (1)					
<input type="checkbox"/>	fortilink	Aggregate		Manual	169.254.1.1/255.255.255.255
Tunnel (1)					
<input type="checkbox"/>	ssl.root (SSL VPN interf	Tunnel		Manual	0.0.0.0/0.0.0.0
Hardware Switch (1)					
<input type="checkbox"/>	lan	Hardware Switch		Manual	192.168.100.99/255.255.255.255
WiFi SSID (3)					
<input type="checkbox"/>	WiFi-eSkole (b)	WiFi SSID		Manual	0.0.0.0/0.0.0.0
<input type="checkbox"/>	WiFi-eduroam (b)	WiFi SSID		Manual	0.0.0.0/0.0.0.0
<input type="checkbox"/>	WiFi-guest (b)	WiFi SSID		Manual	0.0.0.0/0.0.0.0
SD-WAN Zone (1)					
<input type="checkbox"/>	virtual-wan-link	SD-WAN Zone			
<input type="checkbox"/>	wan1	Physical		DHCP	31.147.235.179/255.255.255.255
<input type="checkbox"/>	wan2	Physical		DHCP	0.0.0.0/0.0.0.0

Slika 63: FortiManager – popis sučelja usmjerivača

Za uređivanje sučelja, potrebno ga je označiti i odabrati opciju za uređivanje sučelja (*Edit Interface*).

The screenshot shows the 'Edit Interface' configuration page in FortiManager. The breadcrumb trail is 'OS-ISUSOVACKA-RO > System : Interface > Router > VPN > URL Match List > Web Filter Override > CLI Configurations > Display Options'. The 'Edit Interface' button is highlighted with a red box. The interface name is 'dodatni_servis1'. The 'Addressing Mode' section is also highlighted with a red box, showing 'Manual' selected. The IP/Netmask is '192.168.32.1/255.255.254.0'. The 'DHCP Server' section is highlighted with a red box, showing 'Server' selected. Below the configuration fields is a table for IP Range with columns 'Start IP' and 'End IP'. The table contains one entry: Start IP 192.168.32.21 and End IP 192.168.33.254.

OS-ISUSOVACKA-RO System : Interface Router VPN URL Match List Web Filter Override CLI Configurations Display Options

Edit Interface

Interface Name dodatni_servis1

Alias Name

Type VLAN

Interface fortilink

VRF ID 0

VLAN ID 11

Role Undefined

Address

Addressing Mode Manual DHCP One-Arm Sniffer PPPoE

IP/Netmask 192.168.32.1/255.255.254.0

Shaping Profile OFF

Restrict Access

Override Default MTU Value OFF

Administrative Access

HTTPS PING SSH

SNMP HTTP TELNET

FMG-Access RADIUS Accounting Probe Response

FTM Security Fabric Connection

DHCP Server OFF Server Relay

IP Range

Start IP	End IP
<input type="checkbox"/> 192.168.32.21	<input type="checkbox"/> 192.168.33.254

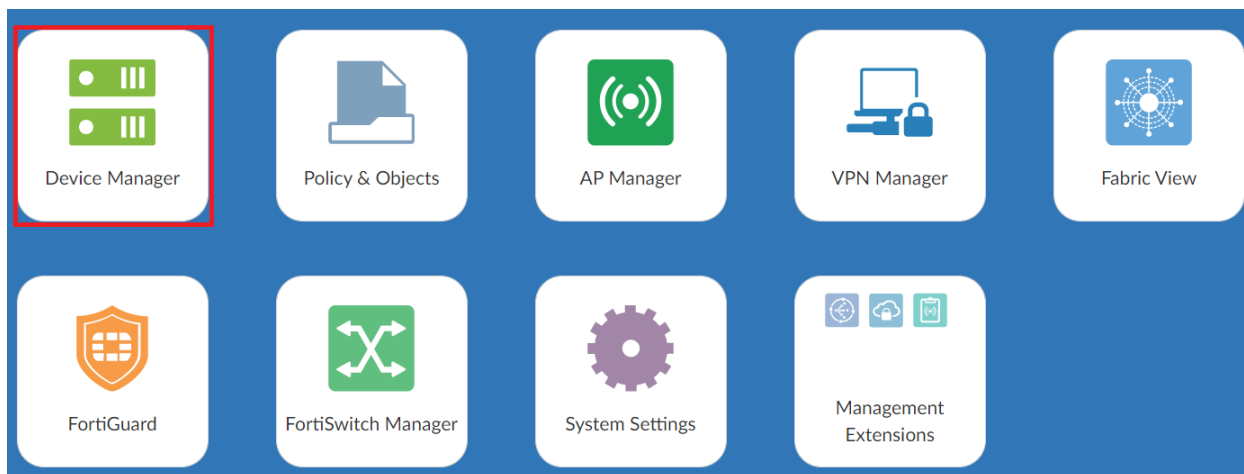
Slika 64: FortiManager – uređivanje sučelja

Upisuje se pripadajuće ime sučelja, odabire brzina i tip adresiranja sučelja statičkom ili dinamičkom dodjelom adrese, a dodatne opcije nude mogućnosti odabira i kreiranja DHCP servera na samom sučelju.

6.5.2 Primjer konfiguracije rute na usmjerivaču

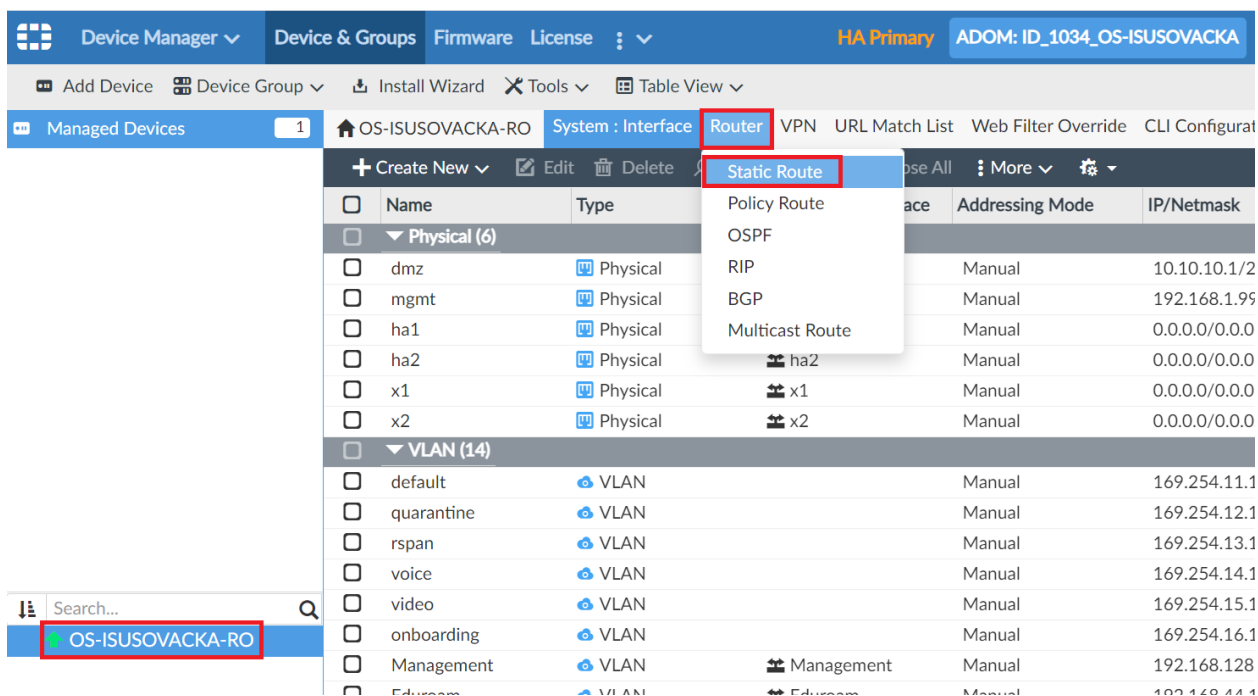
Device Manager / Router / Static Route / Create New

Inicijalni korak u konfiguraciji sučelja je pristup izborniku *Device Manager* unutar ADOM-a (škole) na kojem treba izvršiti promjene na sustavu.



Slika 65: Device Manager izbornik

Nakon odabira škole, na centralnom panelu se odabire opcija za dodavanje nove statičke putanje (*Static Route*).



Slika 66: FortiManager – odabir konfiguracije statičke rute

U novom izborniku se navodi određite nove mreže (*Destination*) za koju se dodaje putanja i obavezno informacija o adresi poveznika (*Gateway*).

OS-ISUSOVACKA-RO System **Router : Static Route** VPN URL Match List Web Filter Overrid

Create New Static Route

Destination **i** Subnet Named Address Internet Service

0.0.0.0/0.0.0.0

Device

Administrative Distance 10

Status **ON**

Gateway 0.0.0.0

Priority 0

Description

0/255

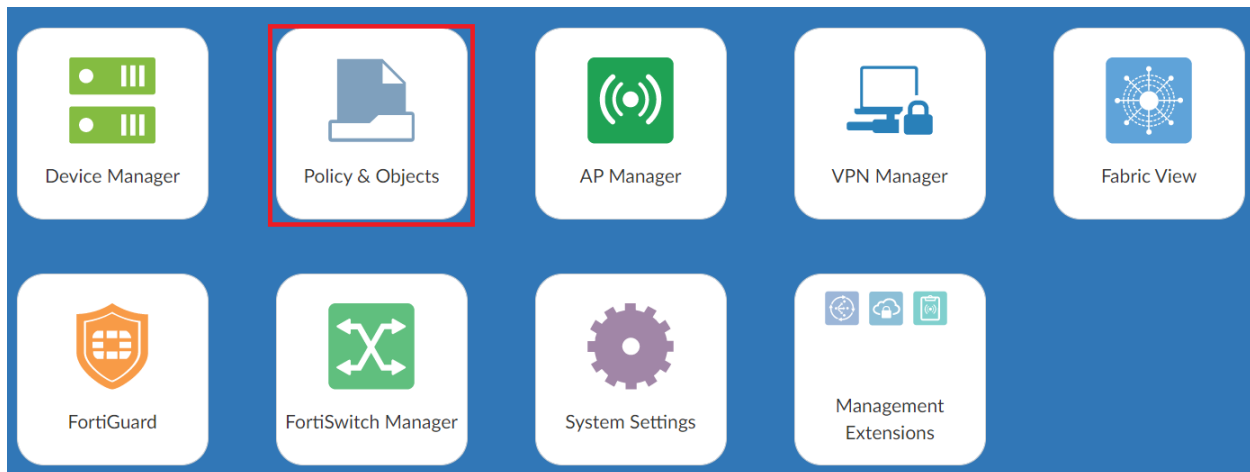
Advanced Options >

Slika 67: Unos parametra statičke rute

6.5.3 Primjer dodavanja sigurnosnog pravila

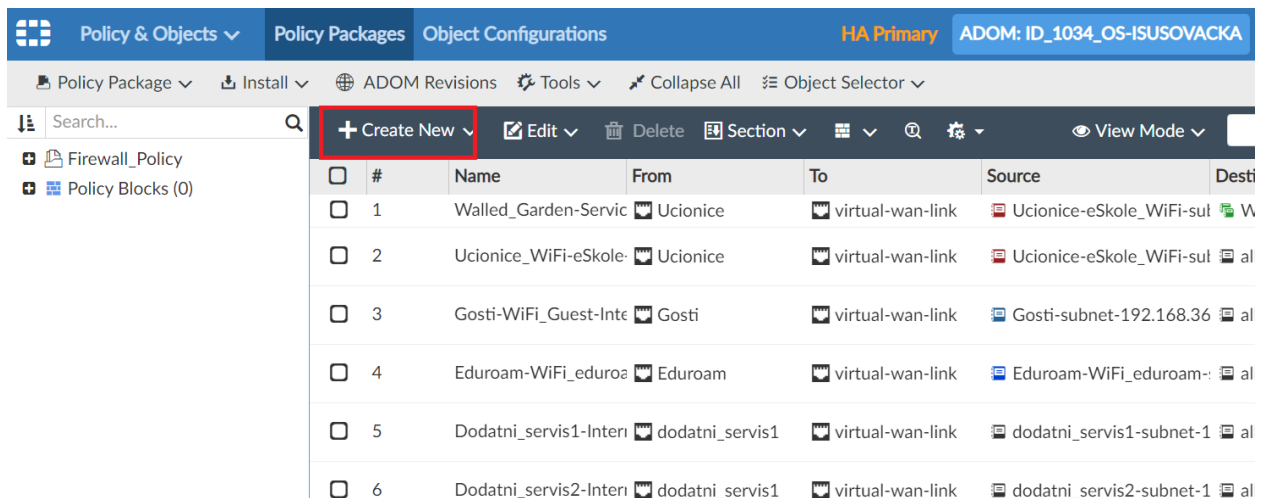
FortiManager / Policy & Objects / Create New

Inicijalni korak u kreiranju sigurnosnih pravila je odabir izbornika *Policy & Objects* unutar ADOM-a (škole) na kojem treba kreirati sigurnosno pravilo.



Slika 68: Izbornik Policy & Objects

Nadalje se odabire opcija za kreiranje novog sigurnosnog pravila (*Create New*).



Slika 69: FortiManager – kreiranje sigurnosnog pravila

Dolazi se do izbornika za kreiranje sigurnosnih pravila (*Policy Package*).

Unosi se ime, definira dolazno sučelje kao sučelje s kojeg treba pristupiti nekom resursu i odlazno sučelje kao sučelje kojem treba pristupiti.

Filtraciju je moguće napraviti i prema odredišnoj, odnosno izvornoj adresi, korisniku na mreži ili grupi.

Odabire se servis koji treba propustiti sa segmenta na segment i potvrđuje unos odabirom opcije prihvatiti (*Accept*).

Create New Firewall Policy

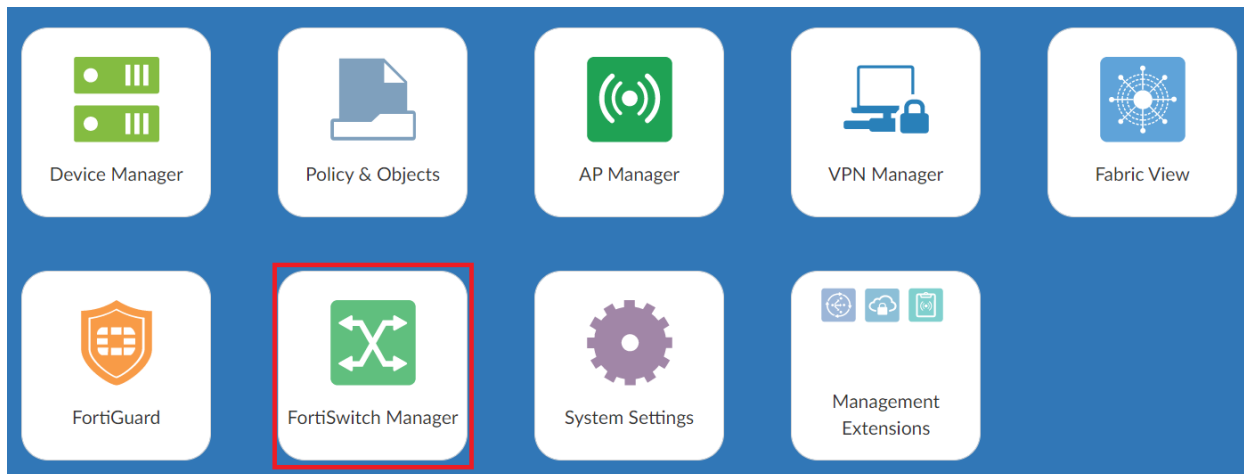
Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/> <input type="button" value="✕"/>
Outgoing Interface	<input type="text" value="any"/> <input type="button" value="✕"/>
Source Internet Service	<input type="checkbox"/> OFF
IPv4 Source Address	<input type="text" value="all"/> <input type="button" value="✕"/>
IPv6 Source Address	<input type="text"/> <input type="button" value="✕"/>
Source User	<input type="text"/> <input type="button" value="✕"/>
Source User Group	<input type="text"/> <input type="button" value="✕"/>
FSSO Groups	<input type="text"/> <input type="button" value="✕"/>
Destination Internet Service	<input type="checkbox"/> OFF
IPv4 Destination Address	<input type="text" value="all"/> <input type="button" value="✕"/>
IPv6 Destination Address	<input type="text"/> <input type="button" value="✕"/>
Service	<input type="text" value="ALL"/> <input type="button" value="✕"/>
Schedule	<input type="text" value="always"/> <input type="button" value="✕"/>
Action	<input type="button" value="Deny"/> <input type="button" value="Accept"/> <input type="button" value="IPSEC"/>

Slika 70: FortiManager – unos parametara za kreiranje sigurnosnog pravila

6.5.4 Primjer konfiguracije sučelja preklopnika

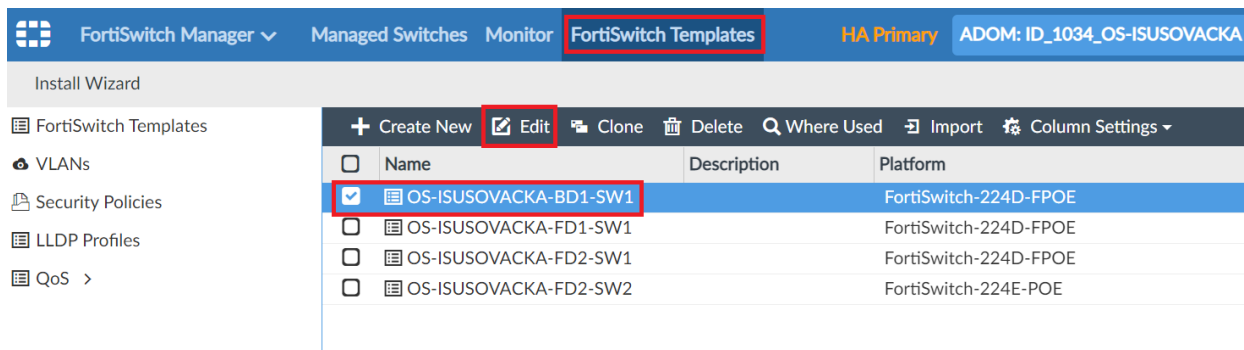
FortiManager / FortiSwitch Manager / FortiSwitch Templates / Edit

Inicijalni korak u kreiranju predloška za preklopnike je odabir izbornika *FortiSwitch Manager* unutar ADOM-a (škole) na kojem treba napraviti navedeni predložak.



Slika 71: Izbornik FortiSwitch Manager unutar ADOM-a

Nakon odabira izbornika, na panelu se odabire predložak (*FortiSwitch Templates*) za uređivanje (*Edit*) te se odabire odgovarajuća opcija.



Slika 72: Uređivanje konfiguracijskog predloška za preklopnik

Odabirom opcije uređivanja konfiguracijskog predloška, dolazi se na izbornik *Edit FortiSwitch Templates*.

Edit FortiSwitch Template

Template Name: OS-ISUSOVACKA-BD1-SW1

Description: 0/63

Platforms: FortiSwitch-224D-FPOE

Switch VLAN Assignments

<input type="checkbox"/>	Port	Description	Access Mode	Enabled Features	Native VLAN	Allow
<input checked="" type="checkbox"/>	port1	AP	Normal	Edge Port Spanning Tree Protocol	Management	
<input type="checkbox"/>	port2	AP	Normal	Edge Port Spanning Tree Protocol	Management	
<input type="checkbox"/>	port3	AP	Normal	Edge Port Spanning Tree Protocol	Management	

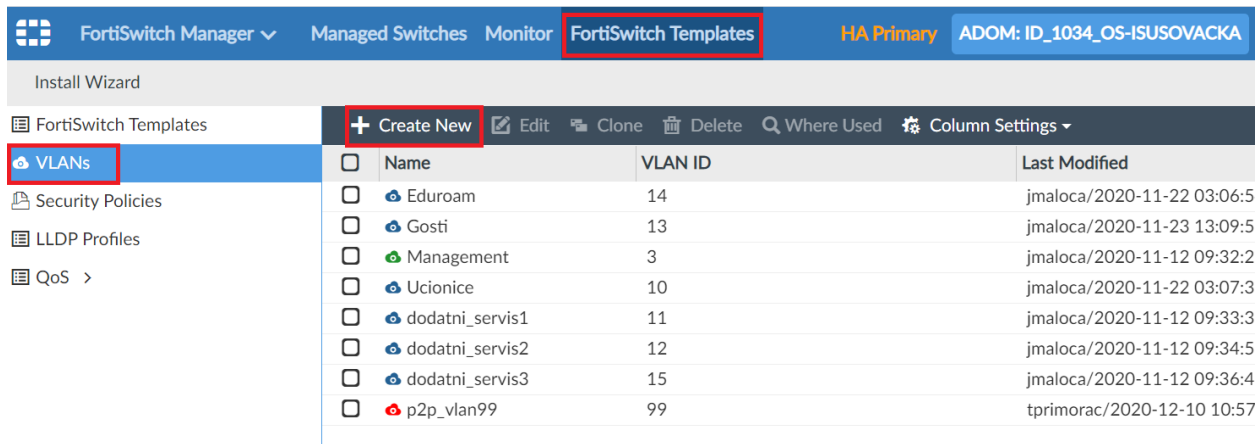
Slika 73: Odabir sučelja unutar konfiguracijskog predloška

U izborniku su prikazana sva sučelja određena za preklopnik. Odabirom broja i imena sučelja koji treba izmijeniti, dolazi se do konfiguracijskih mogućnosti koje je moguće primijeniti, odnosno izmijeniti, kao što je postavka o dozvoljenim VLAN-ovima te druge dodatne mogućnosti.

6.5.5 Primjer kreiranja novog VLAN-a

FortiManager / FortiSwitch Manager / VLANs / Create New

Za kreiranje podmreže, potrebno je iz izbornika FortiSwitch Manager odabrati opciju za odabir predloška (*FortiSwitch Templates*) i u podizborniku VLANs odabrati kreiranje novog VLAN-a (*Create New*).



Slika 74: FortiSwitch – Postupak kreiranja VLAN-a

Unosi se ime VLAN-a (*Interface Name*) i njegov broj (*VLAN ID*) te definiraju opcije adresiranja.

Create New VLAN Definition

Interface Name

VLAN ID

Role DMZ LAN UNDEFINED WAN

Address

Addressing mode Manual DHCP PPPoE

IP/Netmask

IPv6 Addressing mode Manual DHCP

IPv6 Address/Prefix

Create address object matching subnet OFF

Restrict Access

Administrative Access	<input type="checkbox"/> HTTPS	<input type="checkbox"/> PING	<input type="checkbox"/> SSH
	<input type="checkbox"/> SNMP	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET
	<input type="checkbox"/> FMG-Access	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Probe Response
	<input type="checkbox"/> DNP	<input type="checkbox"/> FTM	<input type="checkbox"/> Security Fabric Connection i
IPv6 Administrative Access	<input type="checkbox"/> HTTPS	<input type="checkbox"/> PING	<input type="checkbox"/> SSH
	<input type="checkbox"/> SNMP	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET
	<input type="checkbox"/> FMG-Access	<input type="checkbox"/> Security Fabric Connection i	

DHCP Server OFF Server Relay

Networked Devices

Device Detection OFF

Admission Control

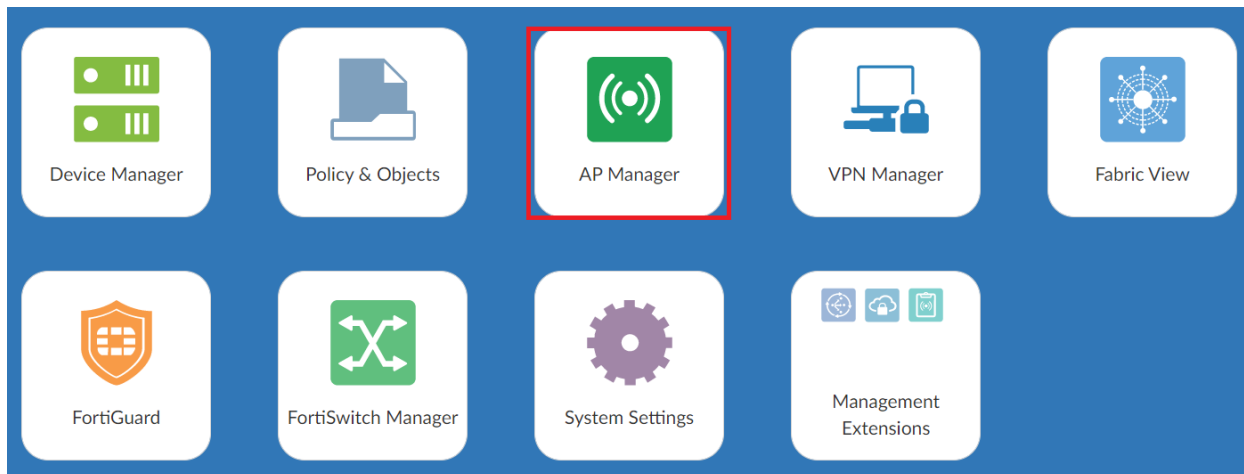
Security Mode CAPTIVE-PORTAL NONE

Slika 75: Unos postavki prilikom kreiranja VLAN-a

6.5.6 Primjer kreiranja novog SSID-a

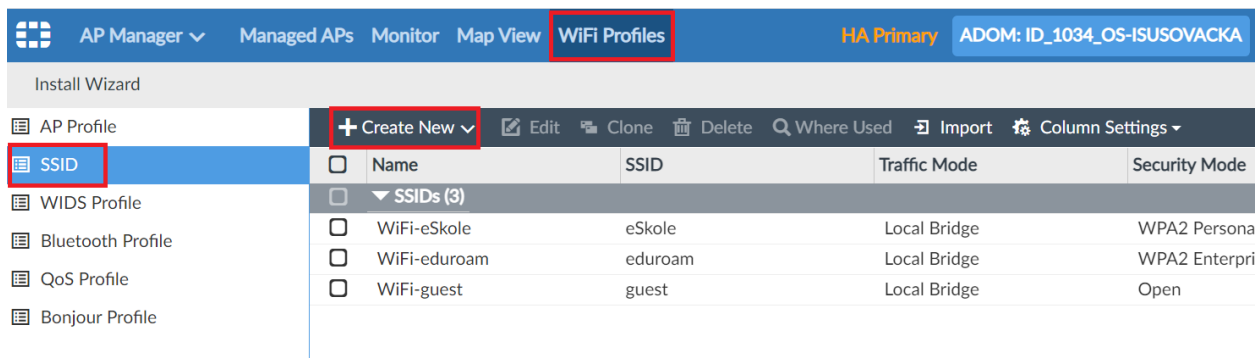
FortiManager / AP Manager / WiFi Profiles / SSID

Inicijalni korak u kreiranju novog SSID-a je odabir izbornika *AP manager* unutar *ADOM*-a (škole) gdje treba napraviti zadane promjene.



Slika 76: Izbornik AP Manager unutar ADOM-a (škole)

Na centralnom panelu odabire se opcija profila bežične mreže (*WiFi Profiles*), podizbornik SSID i opcija za kreiranje novoga SSID-a (*Create New*).



Slika 77: Dodavanje nove bežične mreže – SSID

U novom izborniku je potrebno unijeti informacije o imenu mreže, podatke o adresi, vrstu sigurnosti i način autentikacije na mrežu u okviru obveznih podataka, ako je navedena mreža odabrana.

The screenshot shows the 'Create New SSID Profile' configuration page in the FortiManager AP Manager. The 'Interface Name' field is highlighted with a red box and contains the text 'SSID_Test'. Other visible fields include Alias, Traffic Mode (Tunnel selected), Address (IP/Network Mask: 0.0.0.0/0.0.0.0), Administrative Access (HTTPS, PING, SSH, SNMP, HTTP, TELNET, FMG-Access, Auto-Ipsec, RADIUS Accot), IPv6 Administrative Access (HTTPS, PING, SSH, SNMP, HTTP, TELNET, Any, FMG-Access), DHCP Server (OFF selected), Networked Devices (Device Detection: OFF), WiFi Settings (SSID: fortinet, Security Mode: WPA2 Personal, Client Limit: OFF, Pre-shared Key Mode: Single selected).

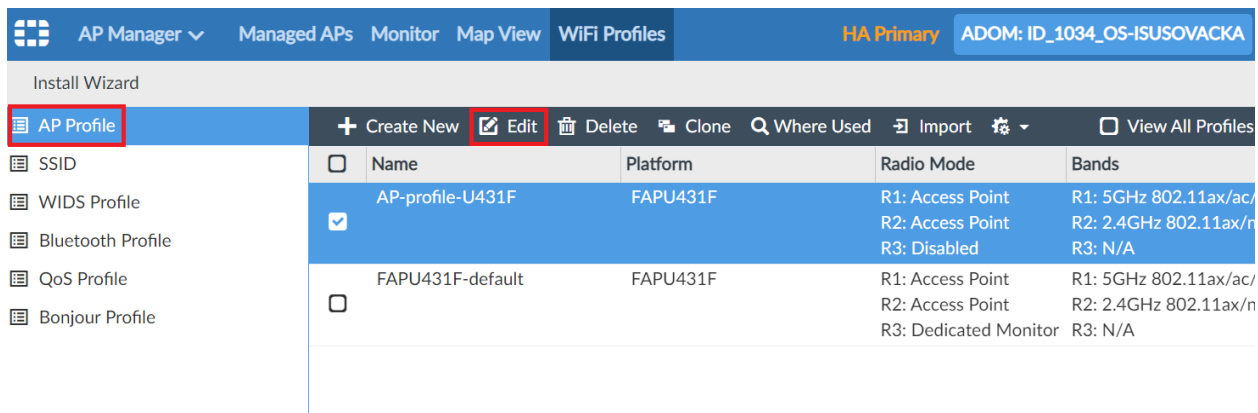
Slika 78: Unos postavki za novu bežičnu mrežu – SSID

Da bi se novokreirani SSID primijenio na bežičnu pristupnu točku, potrebno ga je dodijeliti profilu koji je trenutno primijenjen na sve točke u školi.

Postupak je sljedeći:

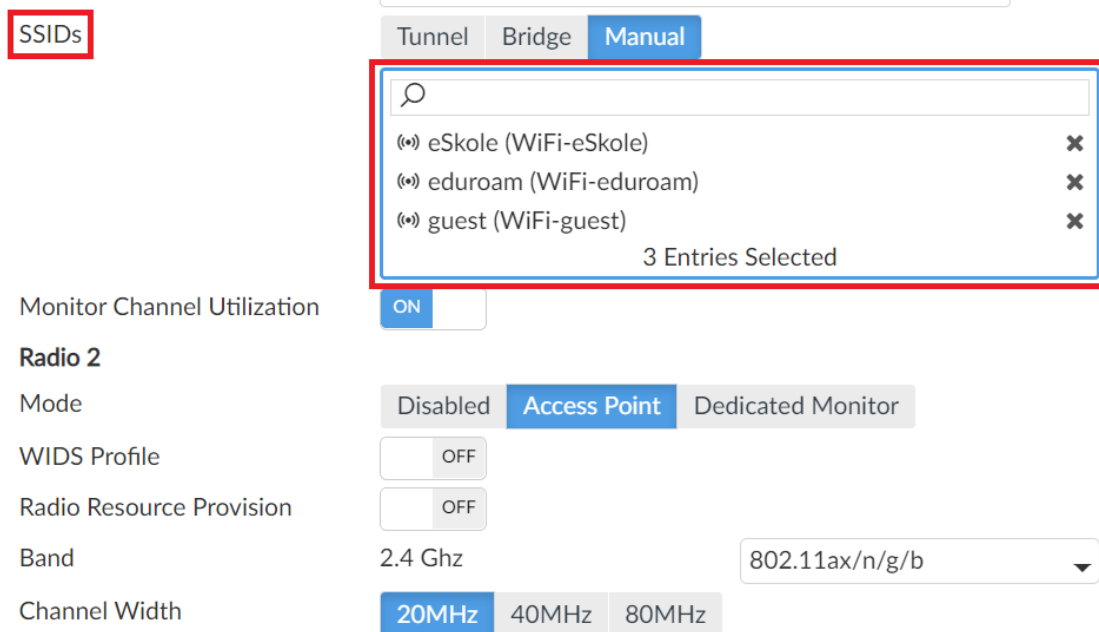
FortiManager / AP Manager / WiFi Profiles / AP Profile

U *AP Manager-u* se odabire opcija *WiFi profil* i podizbornik *AP profil*. Na panelu se nalaze informacije o aktivnom profilu koji je trenutno primijenjen na bežične točke i navedeni se odabire za unos izmjena.



Slika 79: Odabir uređivanja profila bežične pristupne točke

Dolazi se do opcije SSID i na popis mreža koje su trenutno pridružene profilu dodaje se novokreirana mreža.



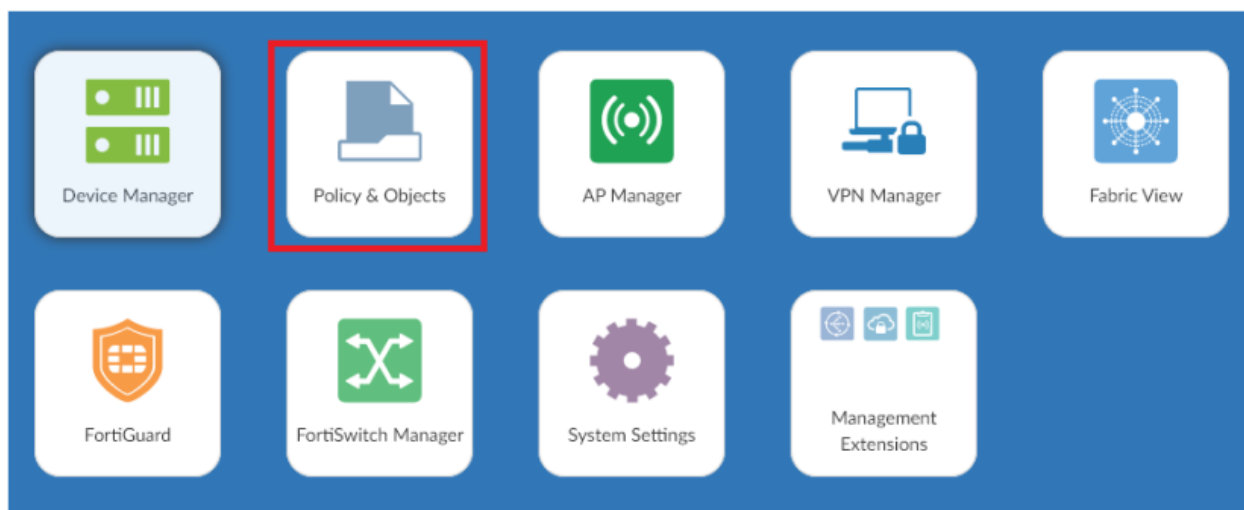
Slika 80: Pridruživanje novokreirane bežične mreže profilu pristupne točke

6.5.7 Primjer kreiranja novog korisnika za *guest* mrežu

Policy & Objects / Object Configuration / User Definition

Inicijalni korak kod konfiguracije korisnika je prijava u centralni sustav upravljanja (<https://mreza-fm.e-skole.hr>), unosom korisničkog imena i lozinke, ranije definiranih od strane administratora sustava.

Nakon prijave, na kontrolnoj ploči je potrebno odabrati lokaciju i nakon toga *Policy & Objects*.



Slika 81: Izbornik *Policy & Objects*

Do forme za kreiranje korisnika (*User Definition*) dolazi se odabirom opcije *Object Configuration* i nakon toga opcije *Users & Authentication*. Nakon odabira opcije *User Definition* prikazuje se popis svi kreiranih korisnika i pritiskom na *Create New* započinje proces kreiranja korisnika.

U konfiguracijskom prozoru je potrebno unijeti sljedeće parametre:

- kako se radi o lokalnom korisniku, potrebno je odabrati *LOCAL*,
- *User Name* – jedino obavezno polje i ovdje se definira korisničko ime,
- *Password* – polje nije obavezno, ali se iz sigurnosnih razloga preporučuje definiranje lozinke,
- *Contact Info* – unose se korisnički podaci (email, broj telefona, itd.),
- *Two-factor Authentication* – po potrebi se definiraju dodatni sigurnosni parametri,
- *Add To Groups* – potrebno je odabrati unaprijed definiranu korisničku grupu *Guest-group*.

The screenshot shows the 'Create New Local User' configuration page in the Fortinet management console. The interface is in the 'Object Configurations' section. The left sidebar shows 'User Definition' selected under 'User & Authentication'. The main form is titled 'Create New Local User' and has several sections:

- Type:** LOCAL (selected), LDAP, RADIUS, TACACS+
- User Name:** CarnetTest
- Disable:**
- Password:** [Redacted]
- Contact Info:**
 - Email:** carnet.test@carnet.hr
 - SMS:** FortiGuard Messaging Service (selected), Custom
 - Country/Region:** [Dropdown]
 - Phone Number:** [Text]
- Two-factor Authentication:**
 - Disable
 - FortiToken (None)
 - Email based two-factor authentication
 - SMS based two-factor authentication
- Add To Groups:** Guest-group (selected), guest

At the bottom, there is an 'Advanced Options' link.

Slika 82: User Definition – forma za kreiranje novog korisnika

7. Prijava poteškoća i upita CARNET-ovom helpdesku

U slučaju poteškoća u radu sustava te za sva pitanja vezana za program “e-Škole” potrebno je obratiti se CARNET-ovom helpdesku:

- telefonski broj podrške: +385 1 6661 500
- adresa elektroničke pošte podrške: helpdesk@skole.hr

Popis slika

Slika 1: Primjer razdjelnika BD	8
Slika 2: Primjer razdjelnika FD	8
Slika 3: Primjer priključne kutije.....	9
Slika 4: Primjer modula RJ45	9
Slika 5: Primjer optičkog LC prespojnog panela	10
Slika 6: Primjer UTP modularnog prespojnog panela.....	10
Slika 7: Svjetlovodni LC konektor	10
Slika 8: UTP RJ45 konektor	10
Slika 9: Primjer označavanja razdjelnika i panela	12
Slika 10: Primjer označavanja priključnica	13
Slika 11: Primjer povezivanja BD/FD/EFD komunikacijskih ormara	14
Slika 12: Shema implementiranog sustava sa sastavnim blokovima	16
Slika 13: Usmjerivač FortiGate 100F.....	17
Slika 14: Prikaz sučelja usmjerivača FortiGate 100F	17
Slika 15: Preklopnik FortiSwitch FS-224E-PoE	20
Slika 16: Preklopnik FortiSwitch FS-224D-FPoE.....	20
Slika 17: Preklopnik FortiSwitch FS-248E-FPoE.....	21
Slika 18: Višemodni optički modul FN-TRAN-SX	21
Slika 19: Jednomodni optički modul FN-TRAN-LX.....	21
Slika 20: Bežična pristupna točka FortiAP U431F-E	23
Slika 21: Odabir ADOM-a.....	28
Slika 22: ADOM – kontrolna ploča aplikacije.....	29
Slika 23: FortiManager – prijava u sustav	30
Slika 24: FortiManger ADOM – lista lokacija	31
Slika 25: FortiManager ADOM – nadzorna ploča	31
Slika 26: Device Manager – nadzorna ploča	32
Slika 27: Policy & Objects – nadzorna ploča	32
Slika 28: AP Manager – nadzorna ploča	33
Slika 29: FortiSwitch Manager – nadzorna ploča	33
Slika 30: FortiAnalyzer – prijava u sustav.....	34
Slika 31: FortiAnalyzer ADOM – lista lokacija	34
Slika 32: FortiAnalyzer ADOM – nadzorna ploča	35
Slika 33: Device Manager – nadzorna ploča	35
Slika 34: FortiView – nadzorna ploča	36
Slika 35: Log View – nadzorna ploča	36
Slika 36: Reports – nadzorna ploča	37
Slika 37: FortiSwitch panel unutar ADOM-a (škole)	38
Slika 38: Prikaz procesa dodavanja preklopnika	39
Slika 39: Definiranje preklopnika	39
Slika 40: Pridruživanje predložka konfiguracije	40

Slika 41: Predložak konfiguracije preklopnika	40
Slika 42: Iniciranje instalacijskog procesa	41
Slika 43: Prikaz uspješnog završetka instalacije	41
Slika 44: Prikaz izbornika AP Manager unutar ADOM-a (škole).....	42
Slika 45: Prikaz prijavljenih bežičnih pristupnih točaka i izbornika za kreiranje nove	42
Slika 46: Dodavanje nove bežične pristupne točke	43
Slika 47: Prikaz profila bežične pristupne točke	43
Slika 48: Forti AP – tipka za reset	44
Slika 49: FortiSwitch – tipka za reset.....	45
Slika 50: FortiGate – tipka za reset	45
Slika 51: Prikaz izbornika Device Manager unutar ADOM-a (škole)	46
Slika 52: FortiManager – nadzorna ploča.....	47
Slika 53: Dodavanje novog widgeta na upravljačku ploču.....	48
Slika 54: Kontrolna ploča FortiManagera – odabir widgeta	49
Slika 55: Prikaz izbornika FortiView unutar ADOM-a (škole).....	50
Slika 56: FortiAnalyzer – izbornik FortiView	50
Slika 57: FortiAnalyzer – prikaz detaljne mrežne aktivnosti po korisniku.....	51
Slika 58: Prikaz izbornika Log View unutar ADOM-a (škole).....	52
Slika 59: Prikaz panela Log View	52
Slika 60: Log View – primjer filtriranog loga po adresi izvora	53
Slika 61: Device Manager – Kontrolna ploča.....	54
Slika 62: FortiManager – kontrolna ploča za odabir sučelja	55
Slika 63: FortiManager – popis sučelja usmjerivača.....	56
Slika 64: FortiManager – uređivanje sučelja.....	57
Slika 65: Device Manager izbornik	58
Slika 66: FortiManager – odabir konfiguracije statičke rute	58
Slika 67: Unos parametra statičke rute.....	59
Slika 68: Izbornik Policy & Objects	60
Slika 69: FortiManager – kreiranje sigurnosnog pravila.....	60
Slika 70: FortiManager – unos parametara za kreiranje sigurnosnog pravila	61
Slika 71: Izbornik FortiSwitch Manager unutar ADOM-a	62
Slika 72: Uređivanje konfiguracijskog predloška za preklopnik	62
Slika 73: Odabir sučelja unutar konfiguracijskog predloška	63
Slika 74: FortiSwitch – Postupak kreiranja VLAN-a.....	64
Slika 75: Unos postavki prilikom kreiranja VLAN-a	65
Slika 76: Izbornik AP Manager unutar ADOM-a (škole)	66
Slika 77: Dodavanje nove bežične mreže – SSID	66
Slika 78: Unos postavki za novu bežičnu mrežu – SSID	67
Slika 79: Odabir uređivanja profila bežične pristupne točke	68
Slika 80: Pridruživanje novokreirane bežične mreže profilu pristupne točke	68
Slika 81: Izbornik Policy & Objects	69
Slika 82: User Definition – forma za kreiranje novog korisnika.....	70

Popis tablica

Tablica 1: Oznaka etaža.....	11
Tablica 2: VLAN i IP adresiranje	18
Tablica 3: Popis i oznake VLAN-ova koji se primjenjuju na preklopnicama.....	22

Popis korištene literature

- *FortiManager - Administration Guide Version 6.4.3 (2020)*, Fortinet Document Library, <https://docs.fortinet.com/document/fortimanager/6.4.3/administration-guide/512210/setting-up-fortimanager>
- *Administration Guide FortiAnalyzer 6.4.3 (2020)*. Fortinet Documentation Library. <https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide/366418/setting-up-fortianalyzer>
- *FortiOS - Administration Guide Version 6.4.3 (2020)*, Fortinet Document Library, <https://docs.fortinet.com/document/fortigate/6.4.3/administration-guide/954635/getting-started>
- *FortiSwitch - Managed by FortiOS 6.4 Version 6.4.3 (2020)*, Fortinet Document Library, <https://docs.fortinet.com/document/fortiswitch/6.4.3/devices-managed-by-fortios/950458/what-s-new-in-fortios-6-4-3>
- *FortiWiFi and FortiAP - Configuration Guide Version 6.4.3 (2020)*, Fortinet Document Library, <https://docs.fortinet.com/document/fortiap/6.4.3/fortiwifi-and-fortiap-configuration-guide/13665/whats-new-in-this-release>
- Pavelin, K. (2017). *Upoznavanje s mrežnom opremom i sustavom za upravljanje i nadzor mreže – MODEL A*. Hrvatska akademska i istraživačka mreža - CARNet. https://pilot.e-skole.hr/wp-content/uploads/2016/12/Prirucnik_Upoznavanje-s-mreznom-opremom-i-sustavom-za-upravljanje-i-nadzor-mreze-%E2%80%93-MODEL-A.pdf

Impresum

Nakladnik: Hrvatska akademska i istraživačka mreža – CARNET

Projekt: e-Škole: Razvoj sustava digitalno zrelih škola (II. faza)

Autori: Dominik Hellenbart, Tomislav Primorac, Karlo Mrazović

Lektori: Mateja Medesi

Zagreb, ožujak, 2021.

Sadržaj priručnika isključiva je odgovornost Hrvatske akademske i istraživačke mreže – CARNET.

Kontakt podatci

Hrvatska akademska i istraživačka mreža – CARNET

Josipa Marohnića 5, 10000 Zagreb

Telefon: +385 1 6661 500

Adresa elektroničke pošte: helpdesk@skole.hr

www.carnet.hr

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

Ovaj priručnik izrađen je s ciljem podizanja digitalne kompetencije korisnika u sklopu projekta „e-Škole: Razvoj sustava digitalno zrelih škola (II. faza)“, koji sufinancira Europska unija iz europskih strukturnih i investicijskih fondova. Nositelj projekta je Hrvatska akademska i istraživačka mreža – CARNET.