e-Škole
RAZVOJ SUSTAVA DIGITALNO ZRELIH ŠKOLA
(II. FAZA)

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

Mrežno rješenje Fortinet

CARNET

2022. GODINA

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

Operativni program KONKURENTNOST I KOHEZIJA

Ovaj priručnik sufinanciran je sredstvima Europska unije iz Europskog fonda za regionalni razvoj u sklopu Operativnog programa 'Konkurentnost i kohezija'.

Sadržaj

Popis kratica

ACL (engl. *Access Control List*) – Lista s pravima pristupa
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 kojim se koriste mrežna 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 okvira Ethernet brzinom od gigabita u sekundi
GIP – Glavni izvedbeni projekt
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, predstavlja najkorišteniji 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 – 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 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 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 i o 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 i svim drugim osobama koje jesu ili će biti angažirane na održavanju funkcionalnog mrežnog sustava u školama, u cilju što boljeg upoznavanja s implementiranim sustavom na operativnoj razini.

2. Osnove mrežnog sustava

Kao preduvjet za administraciju i nadzor računalne mrežne infrastrukture implementirane 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 mrežnog modela OSI (OSI – engl. *Open Systems Interconnection)*, 4 sloja mrežnog modela TCP/IP (engl. *Transmission Control Protocol / Internet Protocol)*,
- adresiranje u računalnim mrežama,
- mrežni protokoli,
- sigurnost lokalnih mreža,
- mrežni uređaji
    - preklopnik L2/L3, 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 dopuštena upotreba postojeće infrastrukture, uključujući mrežne ormare, priključnice, kabelske trase itd., i ta je mogućnost iskorištena u određenom broju škola. Za potrebe novog sustava kabliranja u školama, upotrebljavaju se 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 u okviru projekta „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 u skladu s DIS-om pasivne mrežne infrastrukture škole u kojem je predložen raspored opreme po komunikacijskim ormarima. Razmještaj i eventualna manja preraspodjela postojeće opreme po razdjelnicima izvode se na lokaciji prilikom same instalacije pasivne i prateće aktivne opreme.

U DIS-u pasivne mrežne infrastrukture škole upotrebljavaju se 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 smještanje 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 za 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*), uključujući infrastrukturu vezanu uz pristup na okosnicu CARNET-ove mreže.

Slika 1: Primjer razdjelnika BD

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

Slika 2: Primjer razdjelnika FD

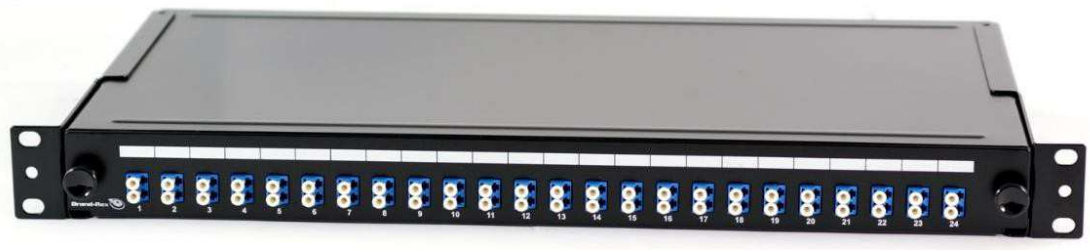
Za potrebe horizontalnog kabliranja koriste se telekomunikacijski priključci (TO – engl. *Telecommunications Outlet*) koji su modularne (ugrađuju se u parapetne kanale) ili nadžbukne (samostojeće) izvedbe. Telekomunikacijskim se priključcima terminiraju kabeli na strani korisničke opreme, ispred bežičnih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

Slika 3: 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. Potreban broj prespojnih panela RJ45 i položaja unutar pojedinog razdjelnika definiran je u DIS-u pasivne mrežne infrastrukture škole. Prespojni panel RJ45 služi za terminiranje svih kabela U/UTP koji gravitiraju razdjelniku u kojemu su terminirani.

Slika 4: Primjer modula RJ45

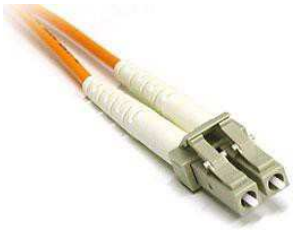
Prespojni paneli namijenjeni su za ugradnju u razdjelnike širine vertikalnih tračnica 19 ". Prespajanje krajnjih točaka kabela međusobno, kao i spajanje aktivnih uređaja na njih, izvedeno je prespojnim kabelima unutar razdjelnika.



Slika 5: Primjer optičkog prespojnog panela LC

Slika 6: Primjer modularnog prespojnog panela UTP

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



Slika 7: Svjetlovodni konektor LC

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

Slika 8: Konektor UTP RJ45

3.2 Sustav označivanja

Oznake komunikacijskih ormara i krajnjih točaka njihove terminacije slijede preporuke norme 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 strukturnog kabliranja lokalne računalne mreže smješteni su po etažama građevine. Svaka od etaža, kao i 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 strukturnog kabliranja čine razdjelnici koji se upotrebljavaju za

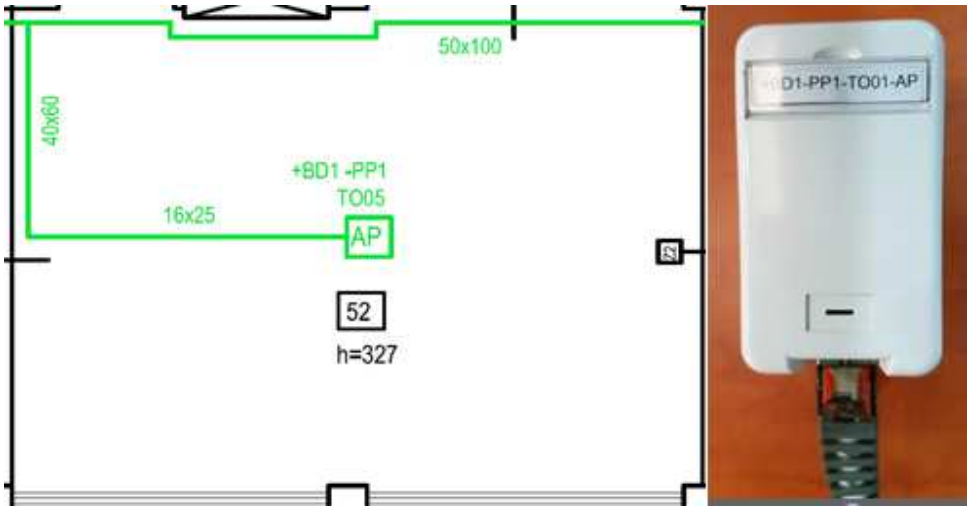
smještanje aktivnih uređaja računalne mreže i opreme za prespajanje segmenata strukturnog kabliranja. U nastavku se nalazi opis funkcija razdjelnika i način označivanja pojedinih dijelova razdjelnika:

- +BD – glavni razdjelnik zgrade – čvor koji povezuje vertikalne razvode (prvi u drugu razinu kabliranja) s horizontalnim razvodom kabela. U razdjelniku je ujedno postavljen i uređaj CPE 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.

Pojedini položaji unutar razdjelnika 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** – predstavlja fizički 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** – predstavlja fizički položaj koji, čitano zdesna nalijevo, označuje priključak **1** na prespojnom panelu **2** (PP2) u razdjelniku **BD** (+BD1).

Slika 9: Primjer označivanja razdjelnika i panela



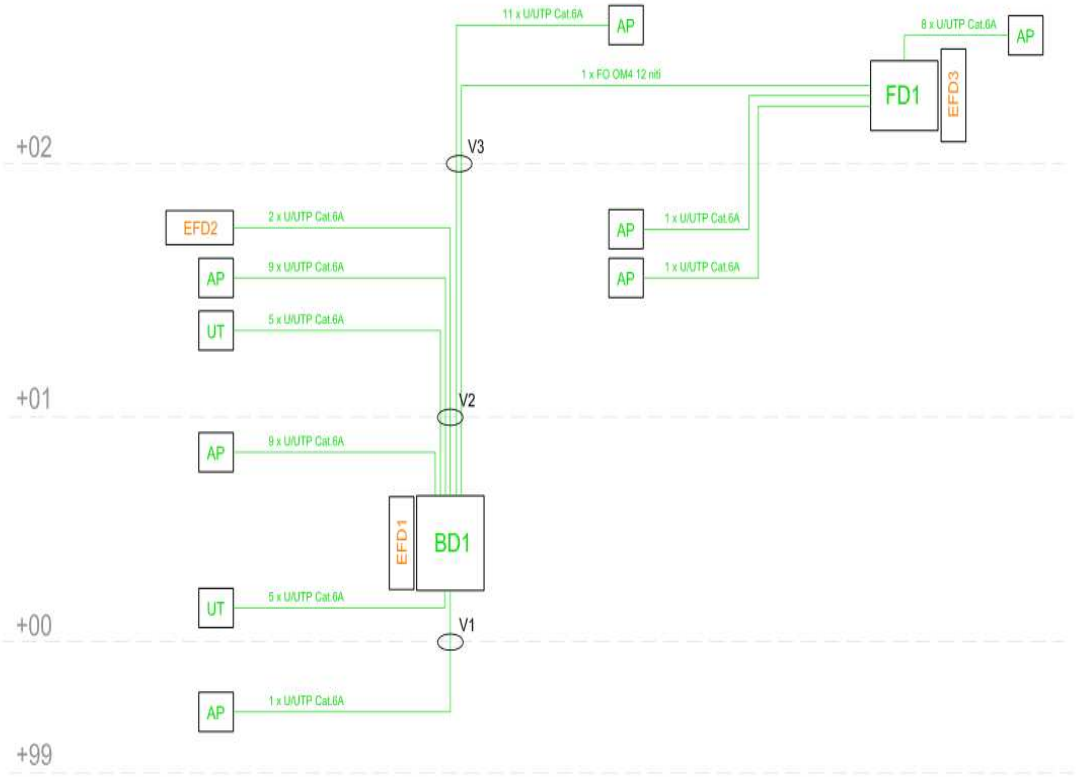
Slika 10: Primjer označivanja priključnica

3.3 Primjeri i načini veza komunikacijskih ormara

Prijenosni mediji kojima se povezuju komunikacijski ormari su:

- višemodni svjetlovodni kabeli kategorije OM4 s 12 niti
- bakreni kabel s četirima paricama (U/UTP) kategorije 6A (Cat. 6A).

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



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

4. Aktivna mrežna oprema u školama

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

Niže u ovome poglavlju opisane su osnovne komponente implementiranog aktivnog mrežnog sustava u školama, isporučeni modeli, njihova uloga i konfiguracijske značajke.

4.1 Arhitektura sustava

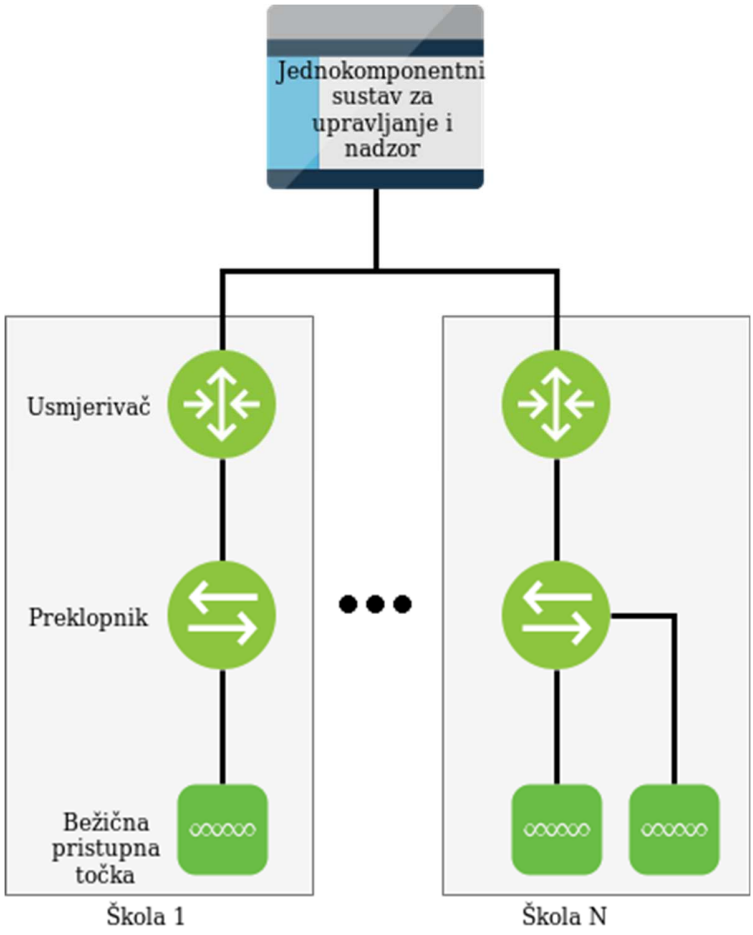
Implementirani mrežni sustav predstavlja jednokomponentno rješenje u kojem se instaliranom mrežnom opremom upravlja putem središnjeg sustava za upravljanje i nadzor mreže. U ovakvom modelu, različitim slojevima lokalne mreže upravlja se i nadzire primjenom jedne komponente nadzorno-upravljačkog sloja.

Implementirani mrežni sustav sastoji se od upravljačkog dijela mreže fizički smještenog na središnjoj lokaciji CARNET-ovih podatkovnih centara i od lokalne mreže škole. U ovom je poglavlju stavljen 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 je škola povezana na CARNET-ovu mrežu kroz koju korisnici ostvaruju pristup potrebnim servisima i internetu. Povezanost na CARNET-ovu mrežu ostvarena je pomoću CARNET-ova uređaja CPE. CARNET-ov uređaj CPE sastoji se od mrežnog usmjerivača, mrežnih preklopnika i bežičnih pristupnih točaka, a na njega je povezana aktivna mrežna oprema škole. 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 su poglavlju opisani mrežni usmjerivač i virtualni LAN-ovi.

4.2.1 Mrežni usmjerivač

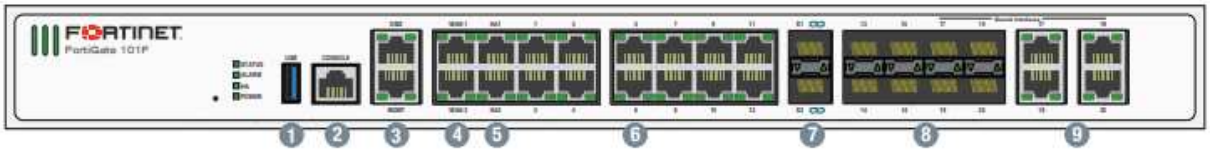
Mrežni usmjerivač omogućuje prijenos podataka između mreža, prilagođavajući pritom podatke za prijenos iz jednog sustava u drugi.

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

Slike u nastavku prikazuju usmjerivač FortiGate 100F i njegova sučelja.

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

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

Usmjerivač FortiGate 100F u sklopu implementiranog mrežnog rješenja ima sljedeće funkcionalnosti:

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

4.2.2 Konfiguracijske značajke sustava

Osnovne konfiguracijske značajke mrežnog usmjerivača navedene su u nastavku.

Tablica 2 prikazuje virtualne LAN-ove (VLAN) i IP adresiranje.

VLAN ID	Naziv 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

Namjene pojedinačnih VLAN-ova su sljedeće:

- 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 se VLAN smješta oprema instalirana u učionicama (poput pametnih ploča). IP adrese iz tog segmenta dobivaju stručnjaci za tehničku

podršku i nastavno osoblje spojeno na mrežu *eduroam*,
- VLAN 11, 12 i 15 služe za povezivanje i logičko odvajanje dodatnih servisa ako na lokaciji postoji potreba za odvajanjem resursa od ostatka postojeće mreže (npr. videonadzor, poslužitelji),
- VLAN 13 služi za povezivanje gostiju na bežičnu mrežu *guest*, pri čemu je brzina ove mreže ograničena na 50 % ukupne brzine internetskog linka,
- VLAN 14 služi za povezivanje učenika i posjetitelja škole koji na svom uređaju imaju dostupnu mrežu *eduroam*, pri čemu je brzina ove mreže ograničena 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 uređaja Fortinet (usmjerivač i preklopnik komuniciranju preko protokola FortiLink).

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

4.3 LAN mreža

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

4.3.1 Mrežni preklopnik

Uloga mrežnih preklopnika jest 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 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 pojedine je škole instalirana 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 uređaji FortiSwitch. Implementirani su sljedeći modeli preklopnika FortiSwitch:

- **FS-224E-PoE**

- **FS-224D-FPoE**
- **FS-248E-FPoE**
- **FS-124E-FPoE**
- **FS-124E-PoE**
- **FS-148E-PoE**
- **FS-108E-PoE**
- **FS-108E-FPoE**

Ovisno o količini i vrsti potrebnih sučelja te o odgovarajućem kapacitetu 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 ima funkcionalnost PoE (engl. *Power Over Ethernet*), i s 4 GE (*engl. Gigabit Ethernet*) SFP sučelja. Maksimalna izlazna snaga (engl. *PoE Output Limit*) na razini preklopnika je 180 W (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 RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 4 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 370 W.

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

Slika 17: Preklopnik FortiSwitch FS-248E-FPoE

Preklopnik FortiSwitch FS-248E-FPoE raspolaže s 48 GE RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 4 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 740 W.

Preklopnik FS-124E-FPoE prikazan je na slici u nastavku.

Slika 18: Preklopnik FortiSwitch FS-124E-FPoE

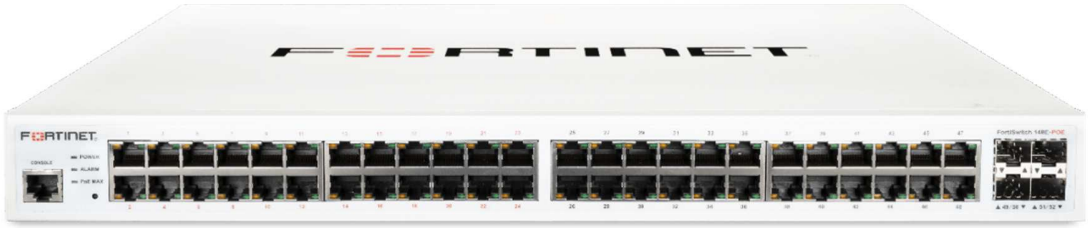
Preklopnik FortiSwitch FS-124E-FPoE raspolaže s 24 GE RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 4 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 370 W.

Preklopnik FS-124E-PoE prikazan je na slici u nastavku.

Slika 19: Preklopnik FortiSwitch FS-124E-PoE

Preklopnik FortiSwitch FS-124E-PoE raspolaže s 24 GE RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 4 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 185 W.

Preklopnik FS-148E-PoE prikazan je na slici u nastavku.



Slika 20: Preklopnik FortiSwitch FS-148E-PoE

Preklopnik FortiSwitch FS-148E-PoE raspolaže s 48 GE RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 4 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 370 W.

Preklopnik FS-108E-PoE prikazan je na slici u nastavku.

Slika 21: Preklopnik FortiSwitch FS-108E-PoE

Preklopnik FortiSwitch FS-108E-PoE raspolaže s 8 GE RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 2 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 65 W.

Preklopnik FS-108E-FPoE prikazan je na slici u nastavku.

Slika 22: Preklopnik FortiSwitch FS-108E-FPoE

Preklopnik FortiSwitch FS-108E-PoE raspolaže s 8 GE RJ45 sučelja, pri čemu sva ova sučelja imaju funkcionalnost PoE, i s 2 GE SFP sučelja. Maksimalna izlazna snaga na razini preklopnika je 130 W.

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

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

Slika 23: Višemodni optički modul FN-TRAN-SX

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

Slika 24: Jednomodni optički modul FN-TRAN-LX

Preklopnik FortiSwitch u sklopu implementiranog mrežnog rješenja ima sljedeće funkcionalnosti:

- centralizirano upravljanje putem sustava za nadzor i upravljanje mrežom,
- tzv. instalaciju uređaja *zero-touch* bez postavljanja početne konfiguracije putem 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.

4.3.2 Konfiguracijske značajke sustava

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
3	management
10	ucionice
11	dodatni_servis1
12	dodatni_servis2

VLAN ID	Naziv VLAN-a
13	gosti
14	eduroam
15	dodatni_servis3
16	postojeca_mreza

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 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 poslužitelja DHCP 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 protokol STP (engl. *Spanning Tree Protocol*) koji prilikom pojave preklopne petlje onemogućuje sučelja kako bi se izbjegle petlje unutar ostatka mrežne topologije.

4.4 Bežična mreža

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

4.4.1 Bežične pristupne točke

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

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

U sklopu implementiranog mrežnog rješenja u školama, ulogu bežične pristupne točke imaju uređaji **FortiAP U431F-E** i **FortiAP U231F-E**

U implementiranom rješenju, bežične pristupne točke koriste funkcionalnost kontrolora 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 25: Bežična pristupna točka FortiAP U431F-E

Bežična pristupna točka FortiAP U431F u sklopu implementiranog mrežnog rješenja ima sljedeće funkcionalnosti:

- centralizirano upravljanje putem sustava za nadzor i upravljanje mrežom,
- tzv. instalaciju uređaja *zero-touch* bez postavljanja početne konfiguracije putem sustava za nadzor i upravljanje mrežom,
- podršku za standarde IEEE 802.11a/b/g/n/ac,
- istovremeni rad na frekvencijskom području od 2,4 i 5 GHz,
- zaseban radio za dedicirano skeniranje koji se ne koristi za prijenos korisničkih podataka, nego isključivo za kontinuiranu analizu WIDS/WIPS te za analizu i optimizaciju upotrebe spektra RF (engl. *Radio Frequency)*,
- automatsku RF optimizaciju mreže,
- upotrebu tehnologije 4 x 4 MU-MIMO,
- funkcionalnosti MU-MIMO i OFDMA u odlaznom (engl. *uplink*) i dolaznom (engl. *downlink*) smjeru,
- podršku za autentikacijske mehanizme 802.1x i enkripciju AES,
- autentikaciju korisnika na mrežu preko zaštitnog portala (engl. *Captive portal*) korištenjem imeničkih sustava,

- podršku za implementaciju mehanizama QoS,
- ograničavanje propusnosti po pojedinom SSID-u i korisniku.

Bežična pristupna točka FortiAP U231F-E prikazana je na slici u nastavku.

Slika 26: Bežična pristupna točka FortiAP U231F-E

Bežična pristupna točka FortiAP U231F u sklopu implementiranog mrežnog rješenja ima sljedeće funkcionalnosti:

- centralizirano upravljanje putem sustava za nadzor i upravljanje mrežom,
- tzv. instalaciju uređaja *zero-touch* bez postavljanja početne konfiguracije putem sustava za nadzor i upravljanje mrežom,
- podršku za standarde IEEE 802.11a/b/g/n/ac,
- istovremeni rad na frekvencijskom području od 2,4 i 5 GHz,
- zaseban radio za dedicirano skeniranje koji se ne koristi za prijenos korisničkih podataka, nego isključivo za kontinuiranu analizu WIDS/WIPS te za analizu i optimizaciju upotrebe spektra RF (engl. *Radio Frequency)*,
- automatsku RF optimizaciju mreže,
- upotrebu tehnologije 2 x 2 MU-MIMO,
- funkcionalnosti MU-MIMO i OFDMA u odlaznom (engl. *uplink*) i dolaznom (engl. *downlink*) smjeru,
- podršku za autentikacijske mehanizme 802.1x i enkripciju AES,
- autentikaciju korisnika na mrežu preko zaštitnog portala (engl. *Captive portal*) korištenjem imeničkih sustava,
- podršku za implementaciju mehanizama QoS,
- ograničavanje propusnosti po pojedinom SSID-u i korisniku.

4.4.2 Konfiguracijske značajke sustava

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

- **eSkole** – služi za povezivanje uređaja u odabranim učionicama na bežičnu mrežu, odnosno za povezivanje uređaja kojima se koristi više različitih osoba,
- **eduroam** – služi za povezivanje učenika, nastavnika i ostalog osoblja na bežičnu mrežu, odnosno za povezivanje uređaja kojim se 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**, primjenjuju 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#),
- enkripcija podataka na pristupnom sloju bežične mreže WPA2 (engl. *Wi-Fi Protected Access*),
- *Captive* portal za autentikaciju korisnika prilikom pristupa internetu. Za autentikaciju se koristi sustav AAI@EduHr,
- nakon pristupa mreži *eSkole*, korisnici pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23.

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

- autentikacija 802.1X enterprise RADIUS uz enkripciju podataka WPA2,
- 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 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, propusnost za navedenu mrežu ograničava se na 50 % ukupne propusnosti linka.

Za pristup mreži **guest**, primjenjuju se sljedeći parametri:

- otvoreni pristup mreži uz mogućnost autentikacije putem *Captive* portala za pristup na okosnicu CARNET-ove mreže,
- za autentikaciju se upotrebljava baza korisnika iz ponuđenog sustava za upravljanje i nadzor. Kako bi stručnjak za tehničku podršku gostu omogućio pristup internetu, u sustav mora unijeti njegovu adresu elektroničke pošte,

- nakon pristupa mreži *guest*, korisnici pripadaju u VLAN 13 i imaju IP adresu iz mreže 192.168.36.0/23,
- za navedenu se mrežu ograničava propusnost na 50 % ukupne propusnosti linka prema internetu.

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

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

- ***Settings*** / ***Connections*** / ***WiFi***,
- Odabrati bežičnu mrežu **eSkole**,
- U polje ***Password*** unijeti PSK – privremeni PSK koji stručnjak za tehničku podršku mreže može po želji zamijeniti je: **eskole123#**
- Prilikom pristupa 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@skole.hr*“ i lozinku)**.

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

- ***Settings*** / ***Connections*** / ***WiFi***,
- Odabrati bežičnu mrežu **eduroam**,
- ***EAP method*** postaviti na ***TTLS***,
- ***PHASE 2 authentication*** postaviti na ***PAP***,
- U polju ***CA certificate*** **nije potrebno mijenjati postavke**,
- U polje ***Indentity*** potrebno je unijeti svoje **korisničko ime za sustav AAI (u obliku „*ime.prezime@skole.hr*“)**,
- Polje ***Anonymus indentity*** **ostaviti prazno**,
- U polje ***Wireless password*** unijeti svoju **lozinku za AAI**.

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

- ***Settings*** / ***Connections*** / ***WiFi***,
- Odabrati bežičnu mrežu **guest**,
- Prilikom pristupa na okosnicu CARNET-ove 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 su poglavlju opisane osnovne sastavnice sustava za upravljanje i nadzor mreže i pregled njegovih glavnih upravljačkih funkcionalnosti.

5.1 Osnovne sastavnice sustava

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

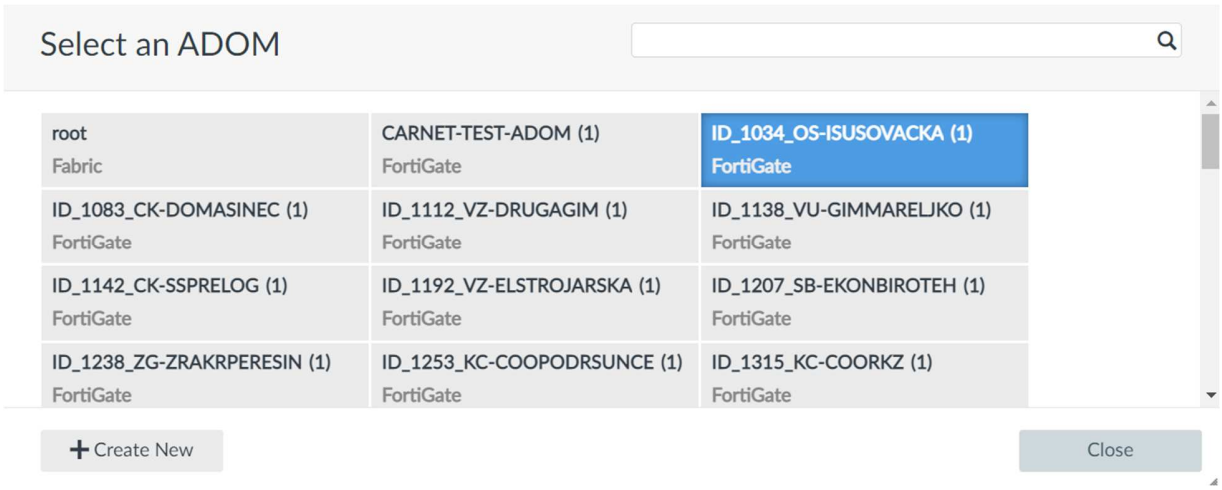
- upravljanje, konfiguraciju i nadzor cjelokupne mrežne infrastrukture instalirane u lokalnoj mreži škole (mrežni usmjerivači, mrežni preklopnici i bežične pristupne točke),
- instalaciju svih mrežnih uređaja i spajanje na sustav za upravljanje i nadzor bez prethodnog spajanja na uređaj i promjene tvorničkih postavki uređaja (engl. *zero-touch deployment*),
- konfiguraciju svih podržanih funkcionalnosti mrežnih uređaja implementiranih u lokalnoj mreži škole,
- odvojenost kontrolne od podatkovne razine sustava, što omogućuje da samo kontrolni promet komunicira izravno s poslužiteljima u podatkovnom centru, dok se korisnički promet usmjerava izravno na CARNET-ovu 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 korisničkog 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**, a njihove su glavne funkcionalnosti objašnjene u nastavku.

FortiManager je rješenje proizvođača Fortinet, a njegova je uloga središnji 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 komponente FortiManager na primarnom i pričuvnom podatkovnom centru.

Jedna od ključnih karakteristika sustava jest arhitektura s 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 i definiranje specifičnosti koje su vezane isključivo uz tu lokaciju (korisnici, pravila). Tako će npr. administrator sustava jedne škole imati uvid samo u uređaje koji su povezani s njegovom školom.



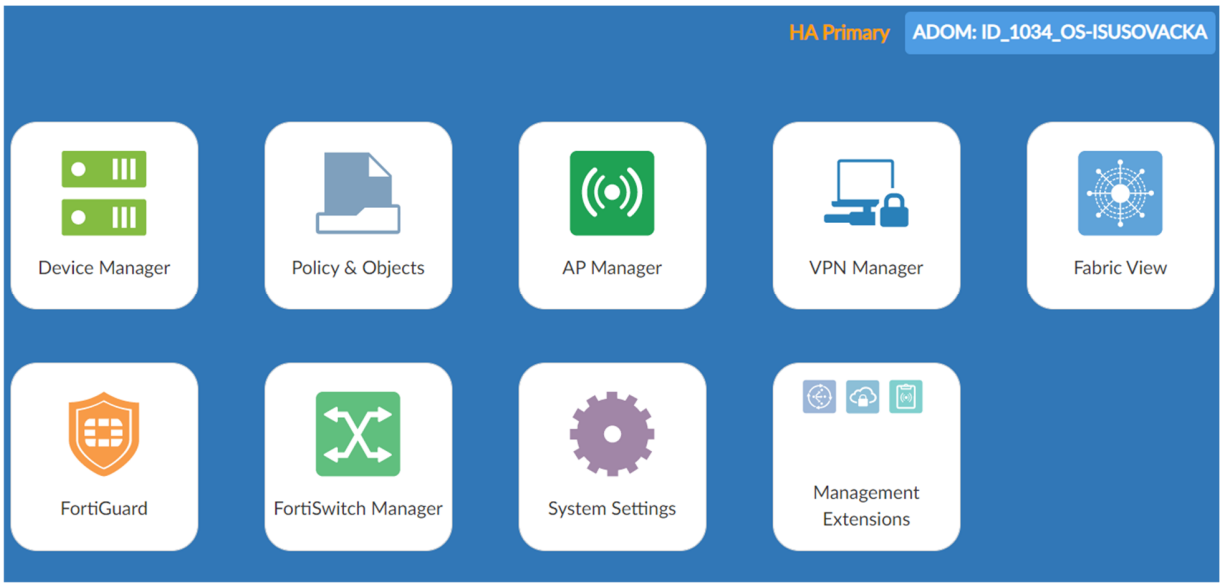
Slika 27: Odabir ADOM-a

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

Funkcionalnosti rješenja FortiManager u sklopu implementiranog mrežnog rješenja su sljedeće:

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

- upravljačka arhitektura s više instanci,
- automatizirana procedura prikupljanja kopija konfiguracija (engl. *backup*),
- vidljivost cjelokupne mreže.



Slika 28: ADOM – kontrolna ploča aplikacije

FortiAnalyzer je rješenje proizvođača Fortinet za središnje prikupljanje i analizu zapisnika događanja (*logova*) te izvještavanje o mrežnim aktivnostima.

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

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

Funkcionalnosti rješenja FortiAnalyzer u sklopu implementiranog mrežnog rješenja su sljedeće:

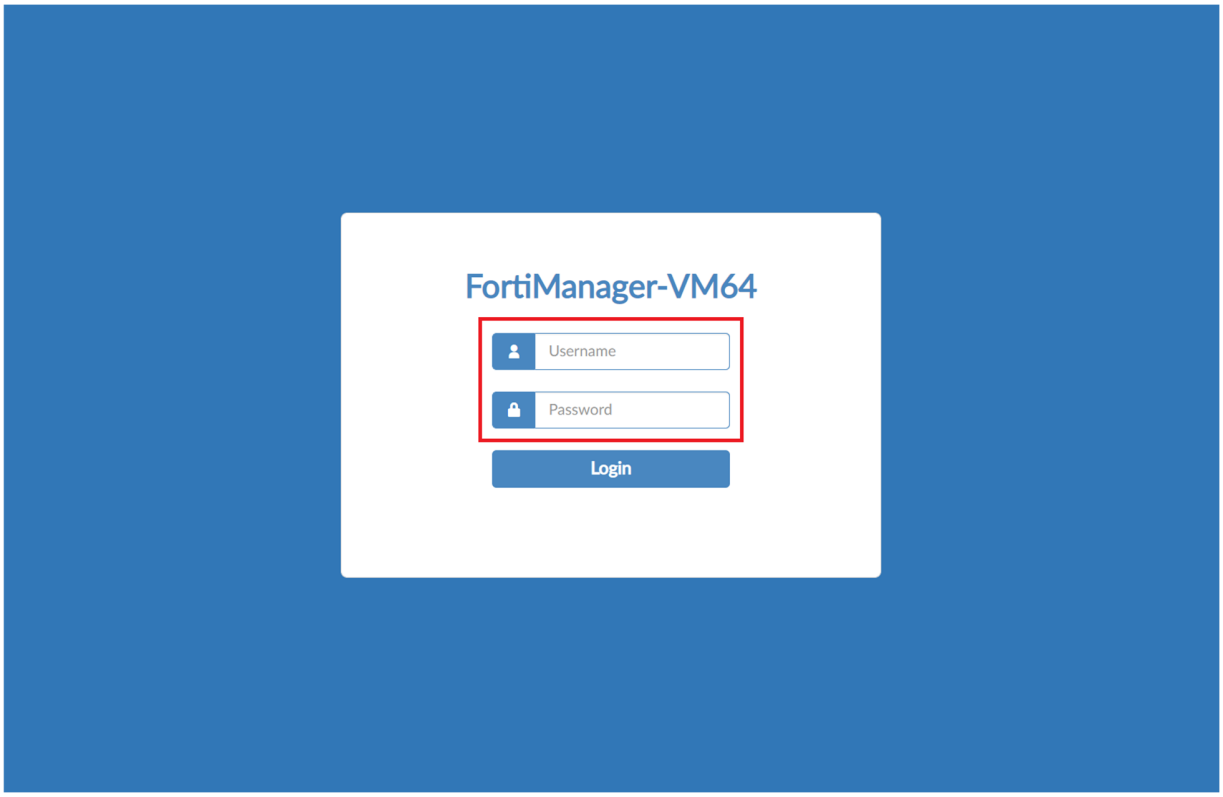
- povećana vidljivost mreže – intuitivne sekcije mrežnog prometa, prijetnji, aplikacija i sl.,
- povećana vidljivost korisnika – korisnici bežične mreže, bežične pristupne točke,
- forenzika – detaljan uvid u mrežnu aktivnost korisnika,
- nadzor u stvarnom vremenu i izvještavanje,
- arhitektura s više instanci (engl. *Multitenancy*),
- prostor za arhivu i analitiku,

- izvještavanje – predefinirani izvještaji, na zahtjev ili unaprijed određeni, fleksibilni formati izvještaja (HTML/CSV/XML/PDF).

5.2 Pregled glavnih upravljačkih funkcionalnosti

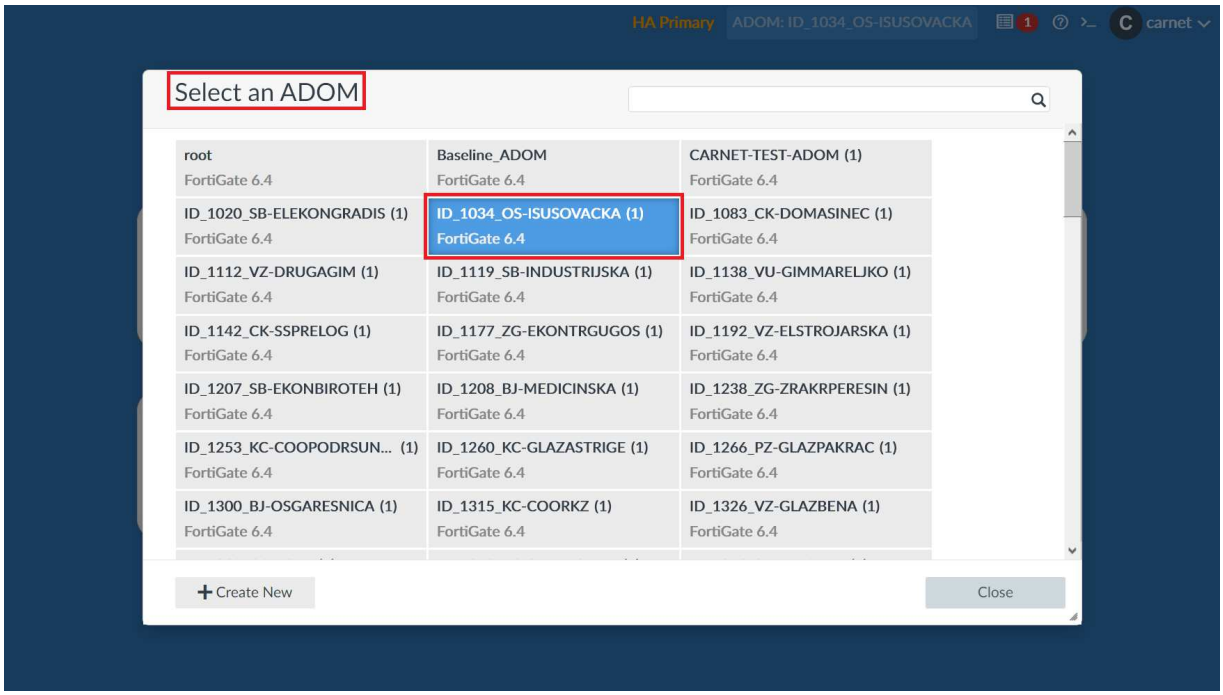
Komponenti središnjeg sustava za upravljanje i nadzor mrežne opreme FortiManager pristupa se putem internetskog preglednika (npr. Google Chrome, Mozilla Firefox, Microsoft Edge i dr.) preko poveznica https://mreza-fm.e-skole.hr i https://mreza-fm2.e-skole.hr , koristeći HTTPS protokol (engl. *Hypertext Transfer Protocol Secure*).

Prijava na sustav vrši se unosom vjerodajnica u obliku korisničkog imena i lozinke koje je administrator sustava ranije odredio.



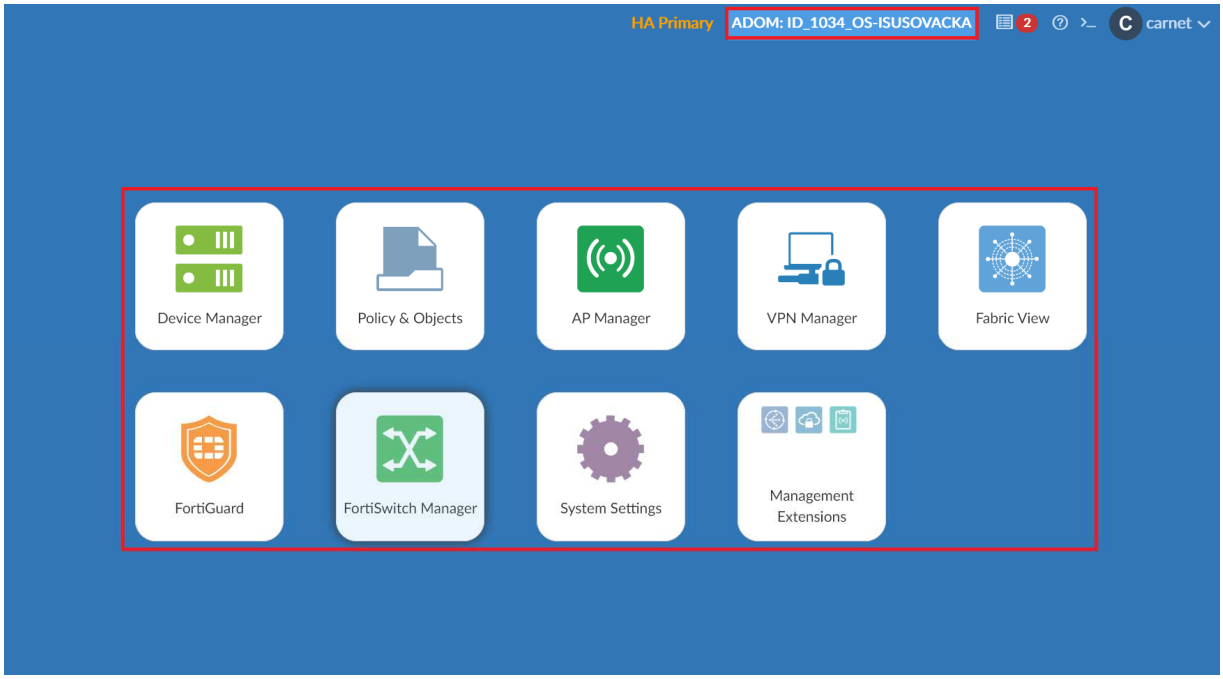
Slika 29: FortiManager – prijava u sustav

Nakon uspješne prijave, prikazuje se izbornik ADOM.



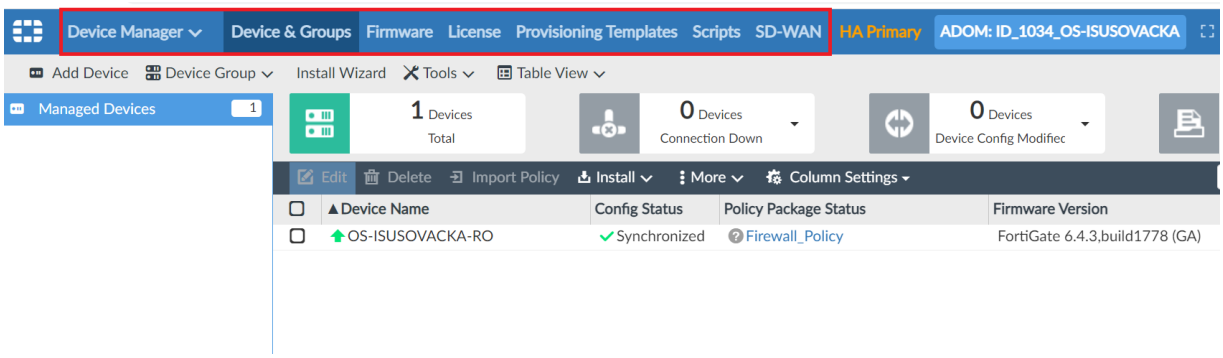
Slika 30: FortiManager ADOM – lista lokacija

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



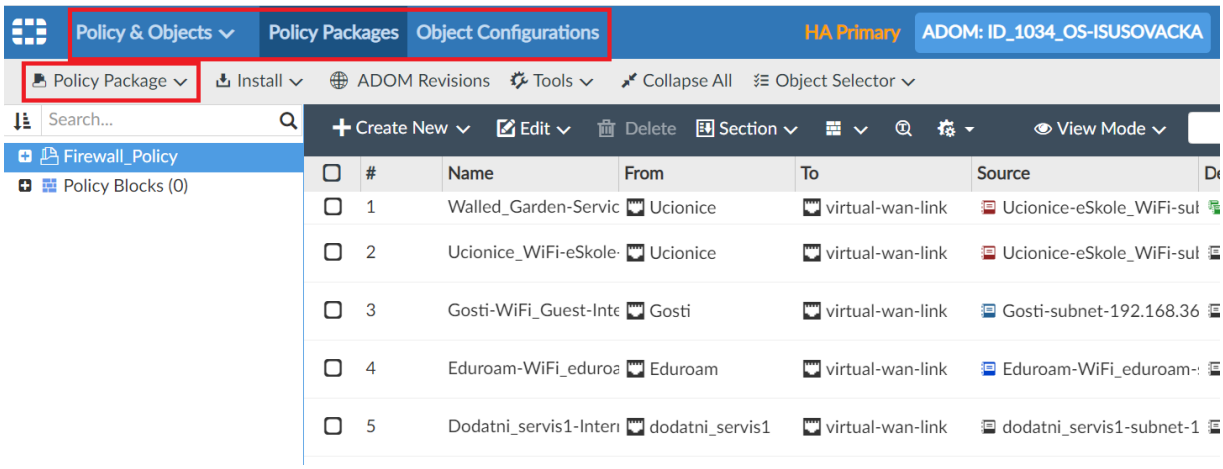
Slika 31: FortiManager ADOM – nadzorna ploča

Izbornik **Device Manager** služi za konfiguraciju svih funkcionalnosti koje su dostupne na usmjerivačima FortiGate. U ovoj se opciji vrši konfiguracija samog uređaja (npr. sučelja, DNS i DHCP servisa), nadogradnja programske podrške, licenciranje uređaja i upravljanje ostalim postavkama.



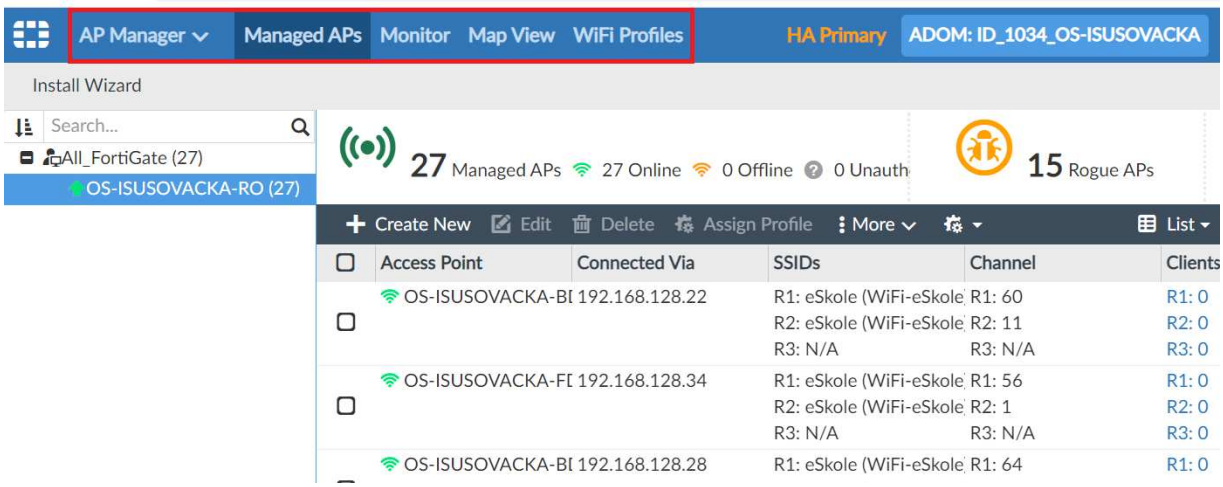
Slika 32: Device Manager – nadzorna ploča

U izborniku ***Policy & Objects*** konfiguriraju se postavke vezane uz vatrozid (npr. objekti, pravila pristupa).



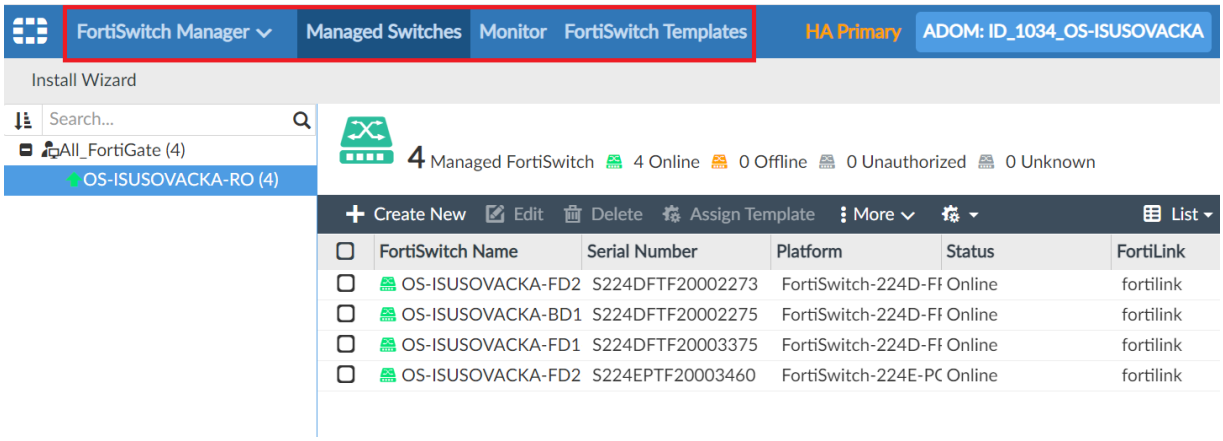
Slika 33: Policy & Objects – nadzorna ploča

Izbornik ***AP Manager*** upotrebljava se za konfiguraciju i nadzor bežičnih pristupnih točaka (npr. naziv, WiFi profil).



Slika 34: AP Manager – nadzorna ploča

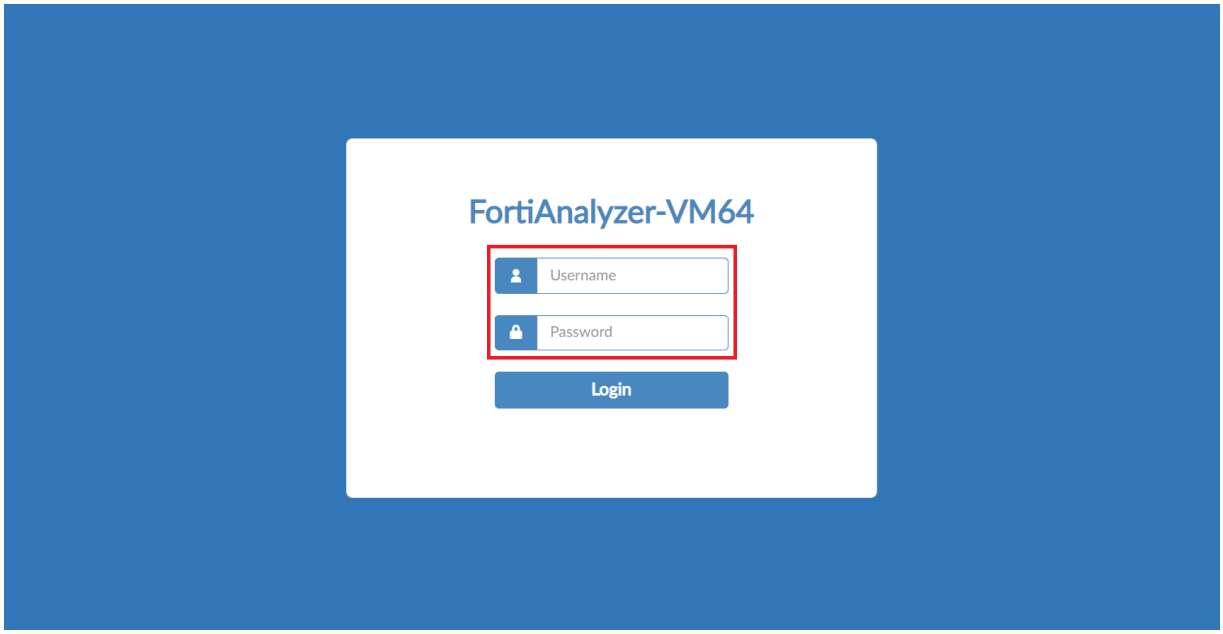
Izbornik ***FortiSwitch Manager*** služi za konfiguraciju i nadzor preklopnika (definiranje VLAN-ova, sučelja preklopnika i ostalih funkcionalnosti kroz konfiguracijski predložak).



Slika 35: FortiSwitch Manager – nadzorna ploča

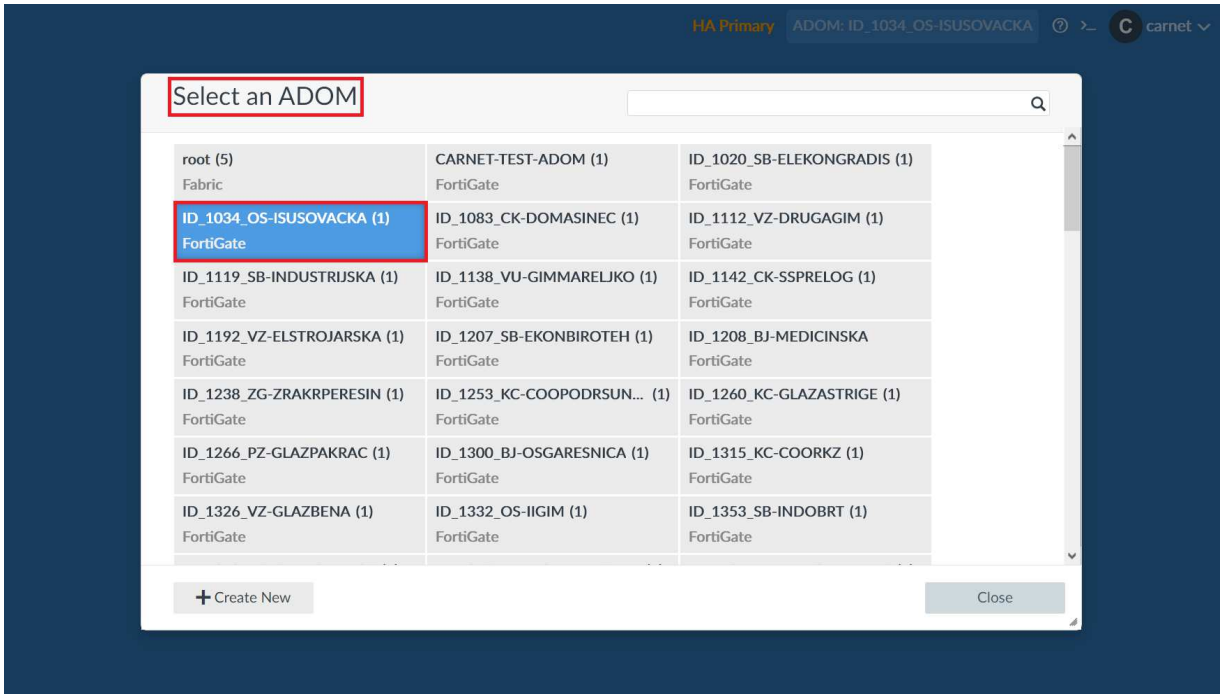
Komponenti središnjeg sustava za prikupljanje podataka, analizu zapisnika događanja (*logova*) i izvještavanje o mrežnim aktivnostima FortiAnalyzer pristupa se putem internetskog preglednika (npr. Google Chrome, Mozilla Firefox, Microsoft Edge i dr.) preko poveznica https://mreza-fm.e-skole.hr i https://mreza-fm2.e-skole.hr) , koristeći HTTPS protokol (engl. *Hypertext Transfer Protocol Secure*).

Prijava na sustav vrši se unosom vjerodajnica u obliku korisničkog imena i lozinke koje je administrator sustava ranije odredio.



Slika 36: FortiAnalyzer – prijava u sustav

Nakon uspješne prijave, prikazuje se izbornik ADOM.

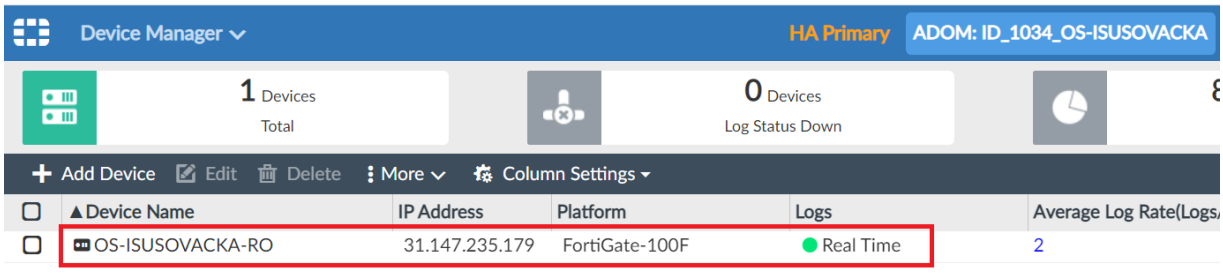


Slika 37: FortiAnalyzer ADOM – lista lokacija

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

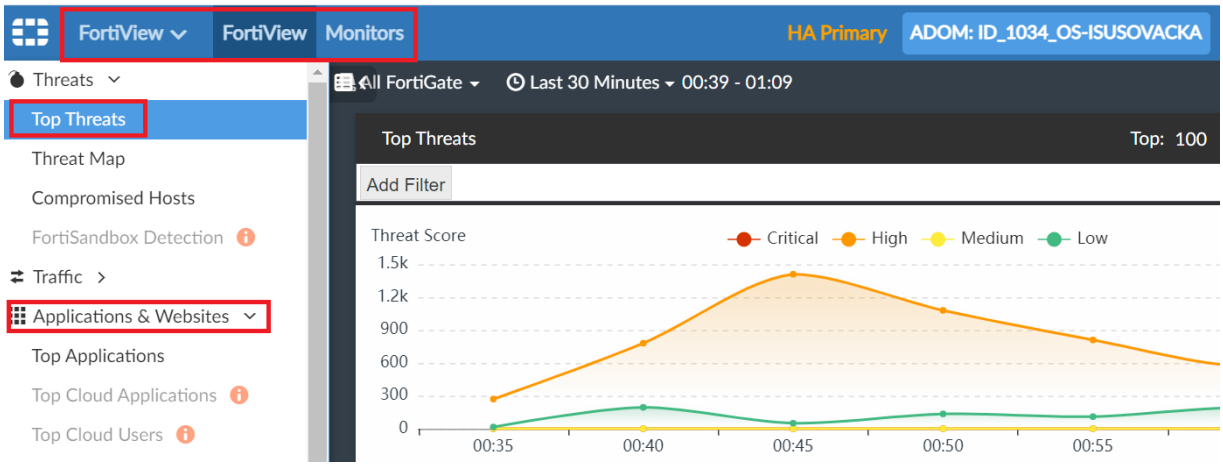
Slika 38: FortiAnalyzer ADOM – nadzorna ploča

Unutar ADOM-a, putem izbornika ***Device Manager*** postavlja se usmjerivač FortiGate koji se nalazi na lokaciji i komunicira direktno s FortiAnalyzerom te mu prosljeđuje informacije o svim mrežnim uređajima potrebnima za analizu i izvještavanje.



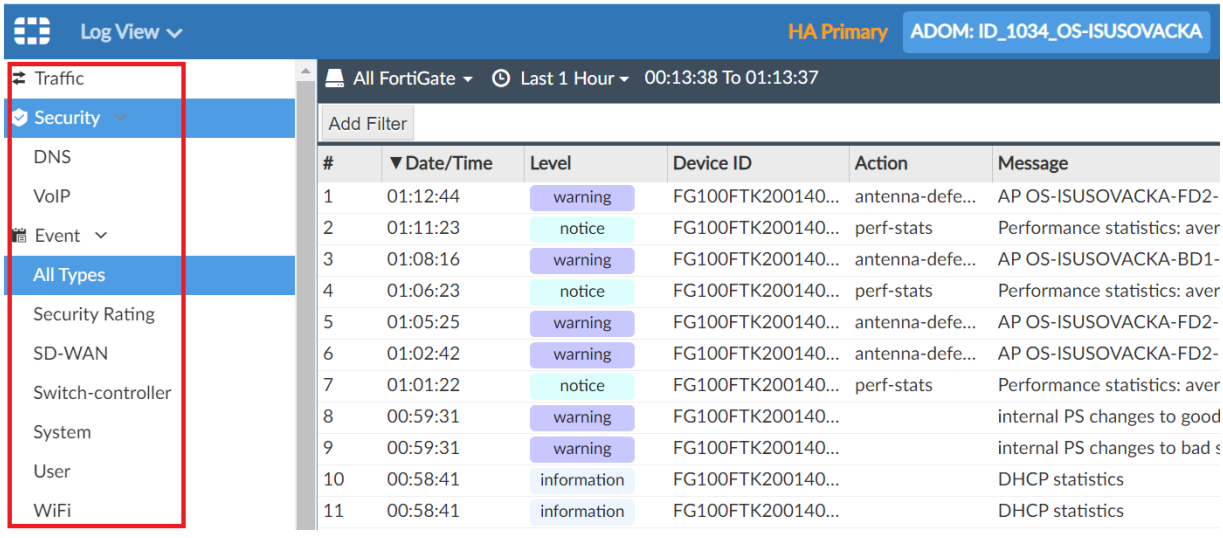
Slika 39: Device Manager – nadzorna ploča

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



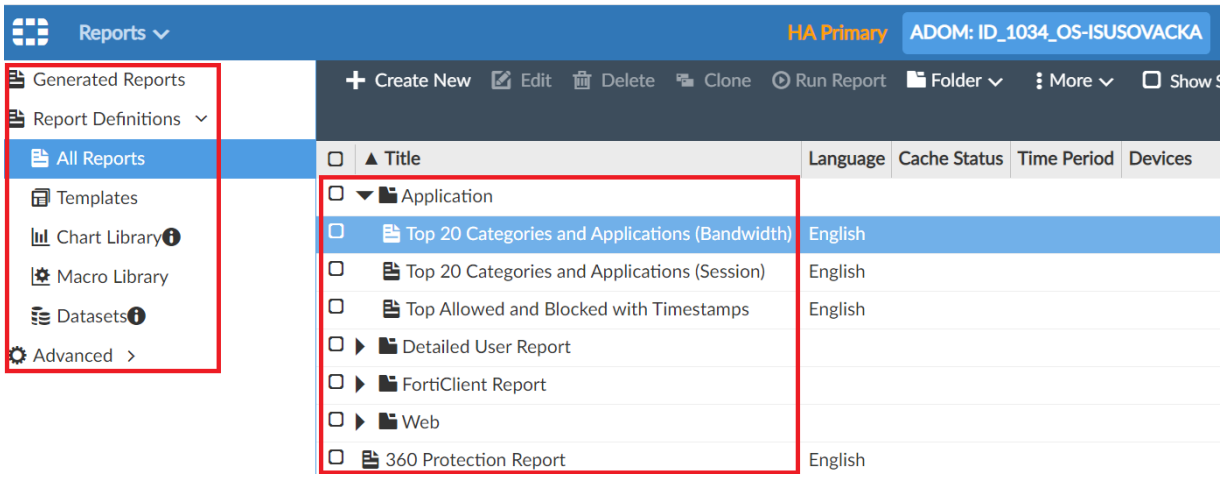
Slika 40: FortiView – nadzorna ploča

Izbornik ***Log View*** upotrebljava se za detaljan pregled prikupljenih zapisnika događanja sa svih mrežnih uređaja Fortinet koji čine računalnu mrežu na pojedinoj lokaciji. Ova je opcija posebno korisna prilikom otklanjanja poteškoća na mrežnim uređajima.



Slika 41: Log View – nadzorna ploča

Izbornik ***Reports*** upotrebljava se za izradu izvještaja pomoću prikupljene metrike sa svih Fortinetovih mrežnih uređaja na lokaciji.



Slika 42: Reports – nadzorna ploča

6. Administracija i održavanje implementirane mrežne infrastrukture škole

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

6.1 Spajanje mrežnog uređaja

Cjelokupni je sustav zasnovan na konceptu upravljanja iz jednog sučelja. Za dodavanje novih uređaja u mrežu, sam uređaj na lokaciji spajanja nije potrebno konfigurirati. Dovoljno je administratora sustava informirati o serijskom broju uređaja, sučelju uređaja na koji se spaja i sučelju novog uređaja kojim će se spojiti kako bi administrator na središnjem upravljačkom sustavu mogao definirati odgovarajuće konfiguracijske postavke (npr. VLAN, STP).

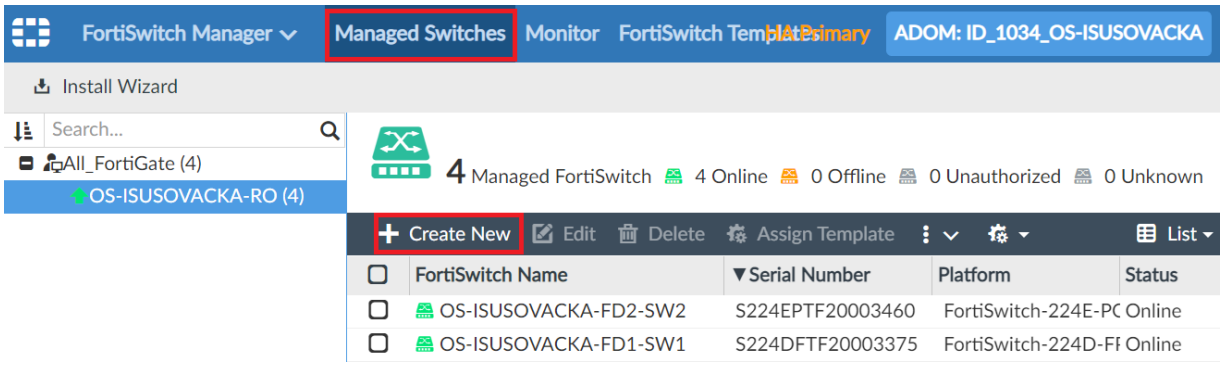
Konfiguracijske postavke uređaja definirane su kroz predloške (engl. *template*) koji se primjenjuju na uređaj. Na taj se način smanjuje količina administrativnih zadataka kod prijave i početne konfiguracije uređaja jer se ranije kreirani predlošci uređaja mogu višestruko upotrebljavati.

Primjer definiranja preklopnika u ormaru BD:

FortiManager / FortiSwitch Manager / Managed Switches / Create New

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

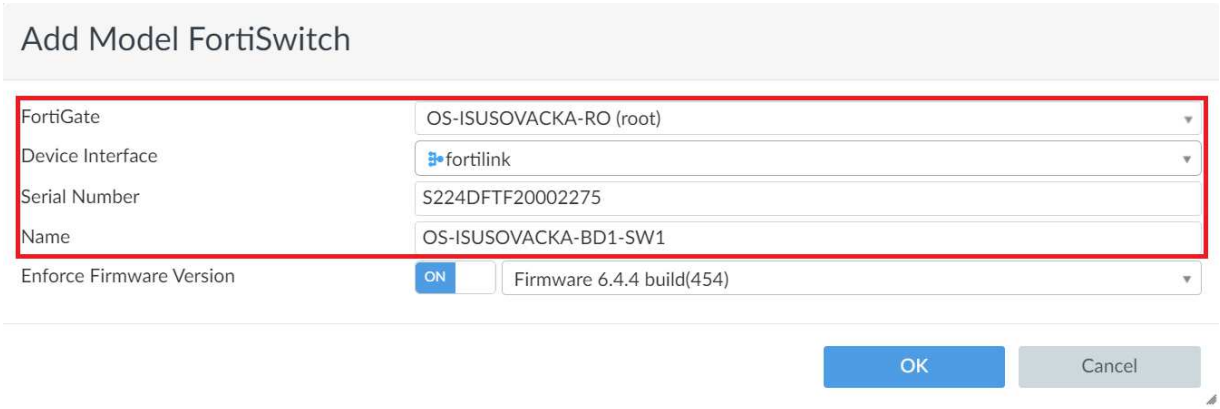
Nakon početnog odabira, odabire se izbornik *Managed Switches* i zatim opcija za dodavanje novog preklopnika (*Create New*).



Slika 43: Prikaz procesa dodavanja preklopnika

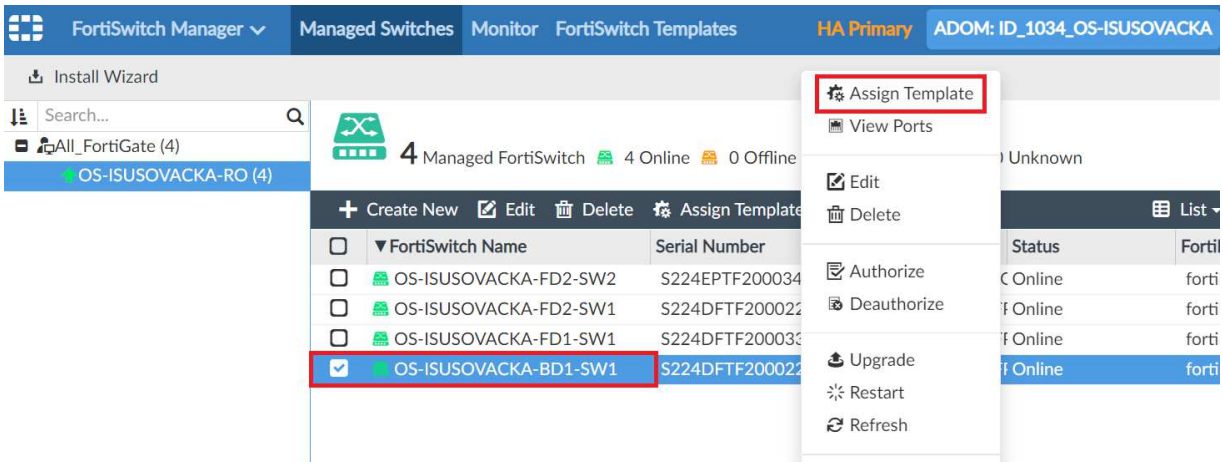
U sljedećem se koraku pojavljuje prozor u kojem se definira:

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



Slika 44: Definiranje preklopnika

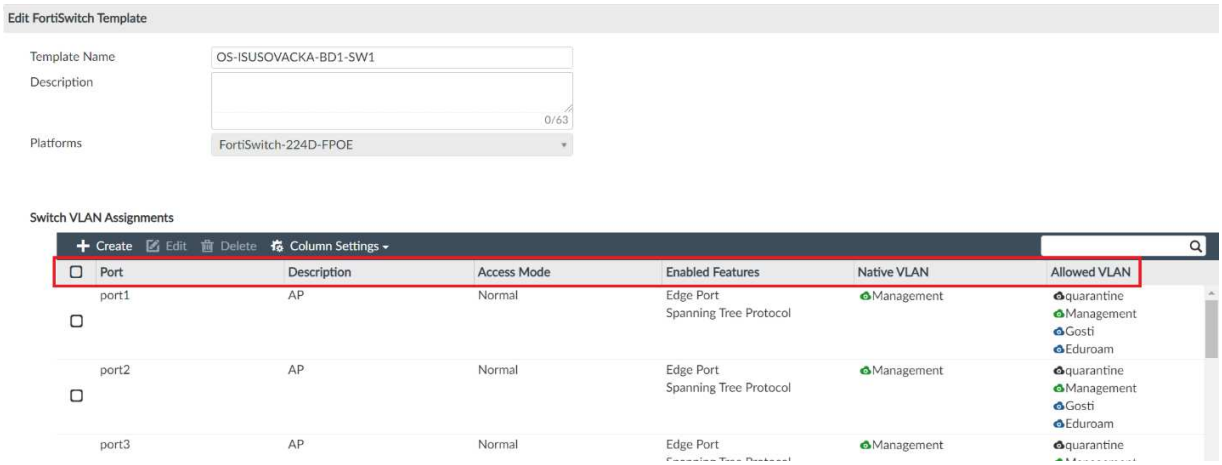
Nakon početnog koraka prijave preklopnika, treba mu pridružiti i pripadajući predložak (engl. *Assign Template*).



Slika 45: Pridruživanje predloška konfiguracije

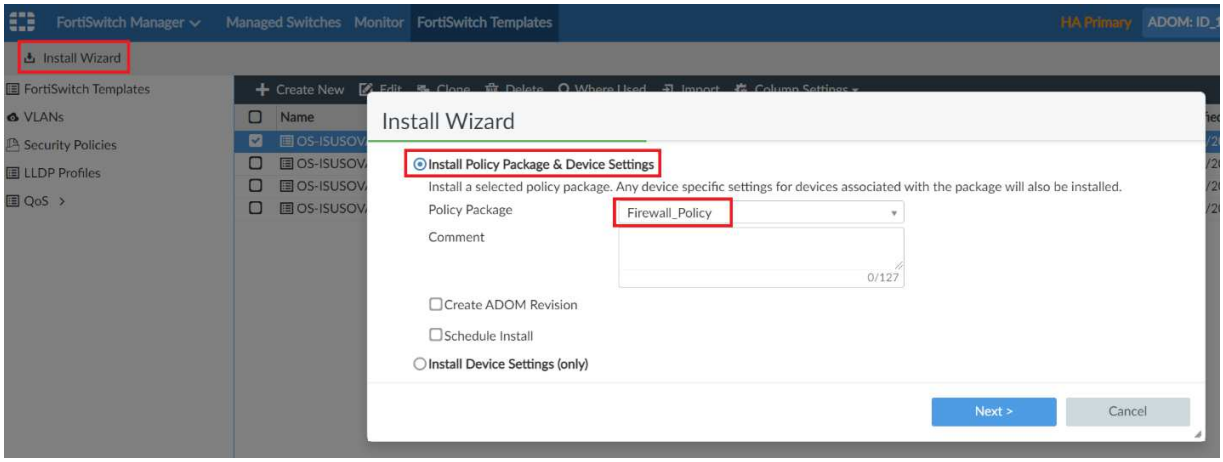
U konfiguracijskom su predlošku početno definirana sva sučelja na preklopniku, odnosno dozvoljene su podmreže. Kroz predložak koji se dodjeljuje preklopniku, definiraju se

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.



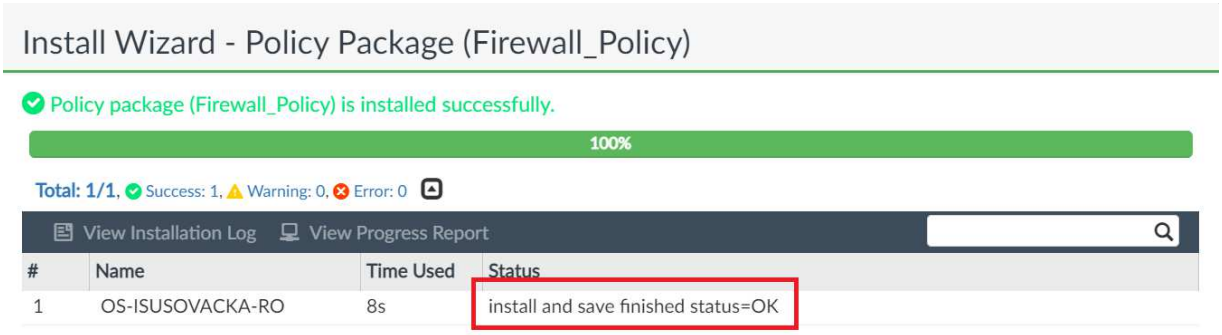
Slika 46: Predložak konfiguracije preklopnika

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



Slika 47: Iniciranje instalacijskog procesa

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



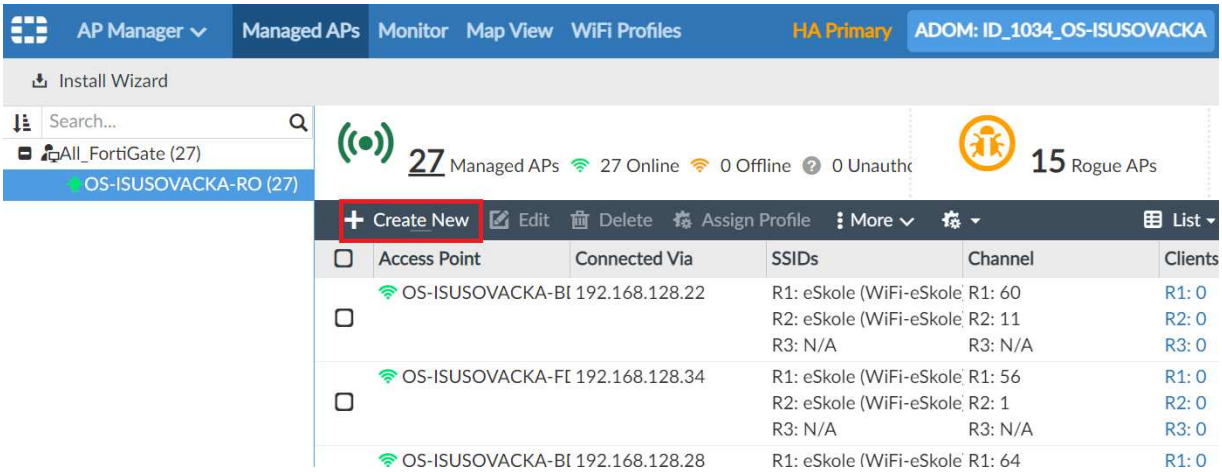
Slika 48: Prikaz uspješnog završetka instalacije

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 u kojem treba dodati navedeni uređaj.

Nakon odabira izbornika, otvara se središnji panel na kojem su vidljive već prijavljene bežične točke na sustav (*Managed APs*). Za dodavanje nove točke, potrebno je odabrati opciju za kreiranje nove točke (*Create New*).

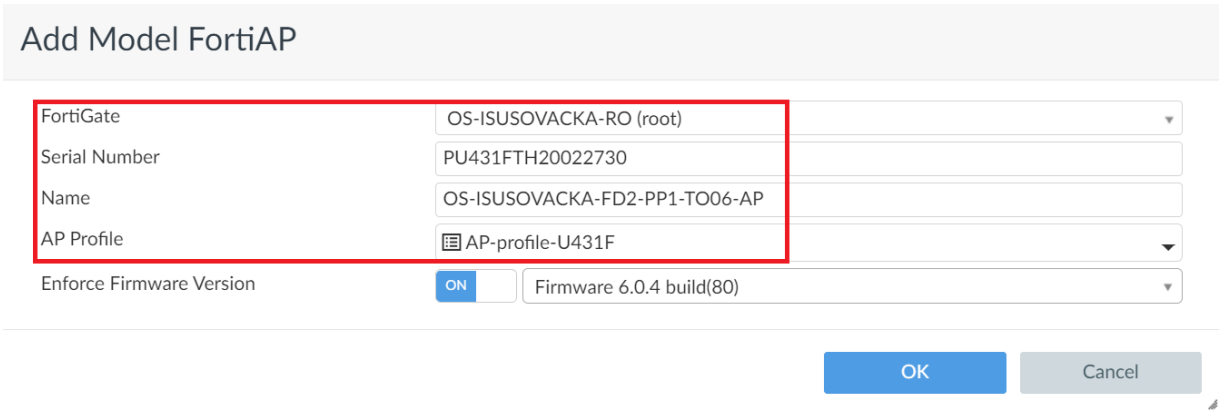


Slika 49: Prikaz prijavljenih bežičnih pristupnih točaka i izbornika za kreiranje nove

U sljedećem se koraku pojavljuje prozor u kojem se definira:

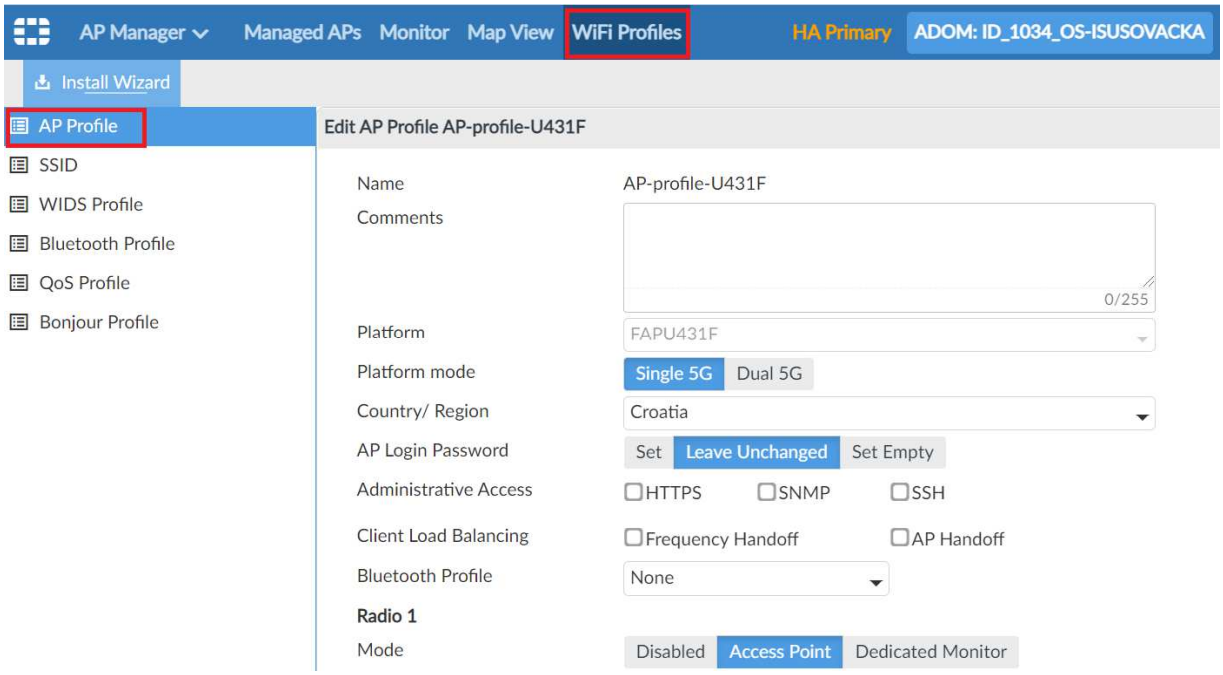
- FortiGate – odabire se pripadajući usmjerivač unutar ADOM-a,

- upisuje se pripadajući serijski broj (engl. *serial number*) bežične pristupne točke,
- naziv uređaja (engl. *name*) prema ranije definiranoj konvenciji imenovanja uređaja u mreži,
- pripadajući profil (*AP Profile*).



Slika 50: Dodavanje nove bežične pristupne točke

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



Slika 51: Prikaz profila bežične pristupne točke

6.2 Vraćanje konfiguracije na tvorničke postavke

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

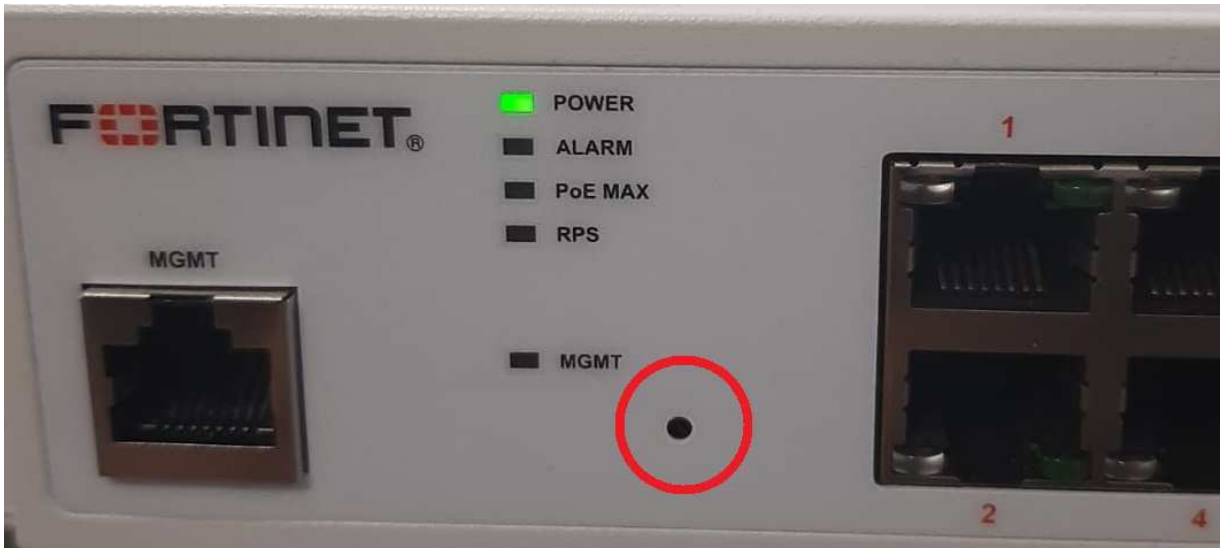
6.2.1 Vraćanje bežične pristupne točke na tvorničke postavke

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

Slika 52: 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 je preklopniku potrebno pritisnuti tipku tankim predmetom i držati je pritisnutu 10 do 15 sekunda dok se ne ugasi lampica *POWER* 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 53: FortiSwitch – tipka za reset

6.2.3 Vraćanje usmjerivača na tvorničke postavke

Vraćanje usmjerivača na tvorničke postavke obavlja se pomoću tipke *reset*. Na uključenom je usmjerivaču potrebno pritisnuti tipku tankim predmetom i držati je pritisnutu 20 sekunda dok lampica *STATUS* ne počne svijetliti narančasto i nakon toga crveno. Nakon puštanja tipke, uređaj je vraćen na tvorničke postavke.

Slika 54: FortiGate – tipka za reset

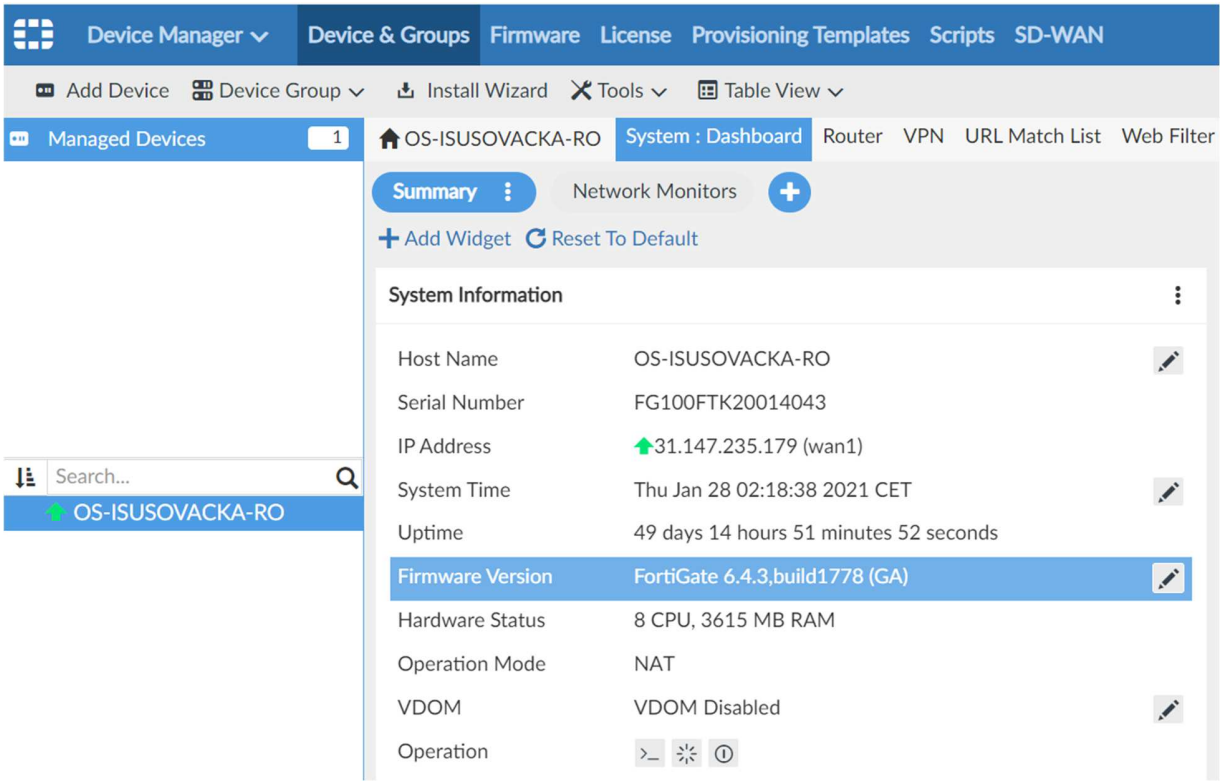
6.3 Nadzor nad mrežnom opremom

Sučelje FortiManagera koristi se za upravljačke funkcionalnosti, ali i kao nadzor i uvid u stanje mrežne opreme u stvarnom vremenu.

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

ADOM / Device Manager

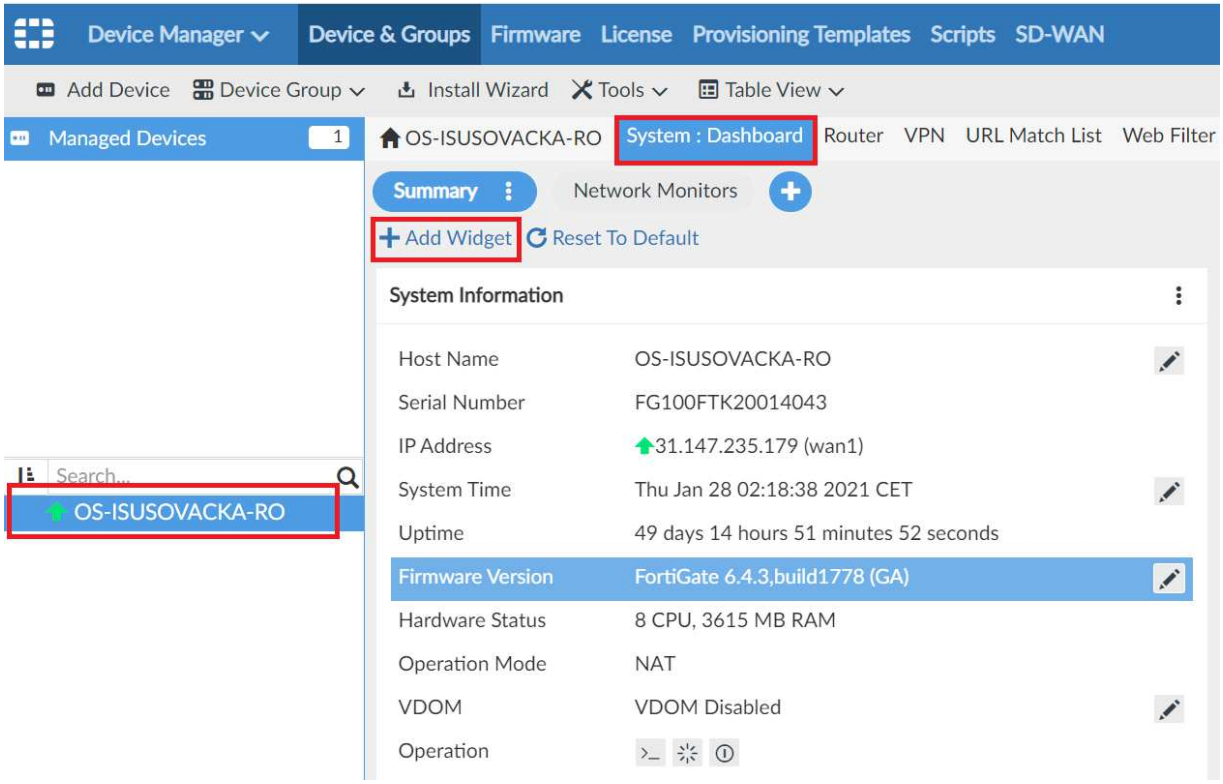
Početna je stranica upravljačka ploča na kojoj se dodaju dodatni alati i mehanizmi koji omogućavaju brz uvid u stanje uređaja i stanja na mrežnoj infrastrukturi.



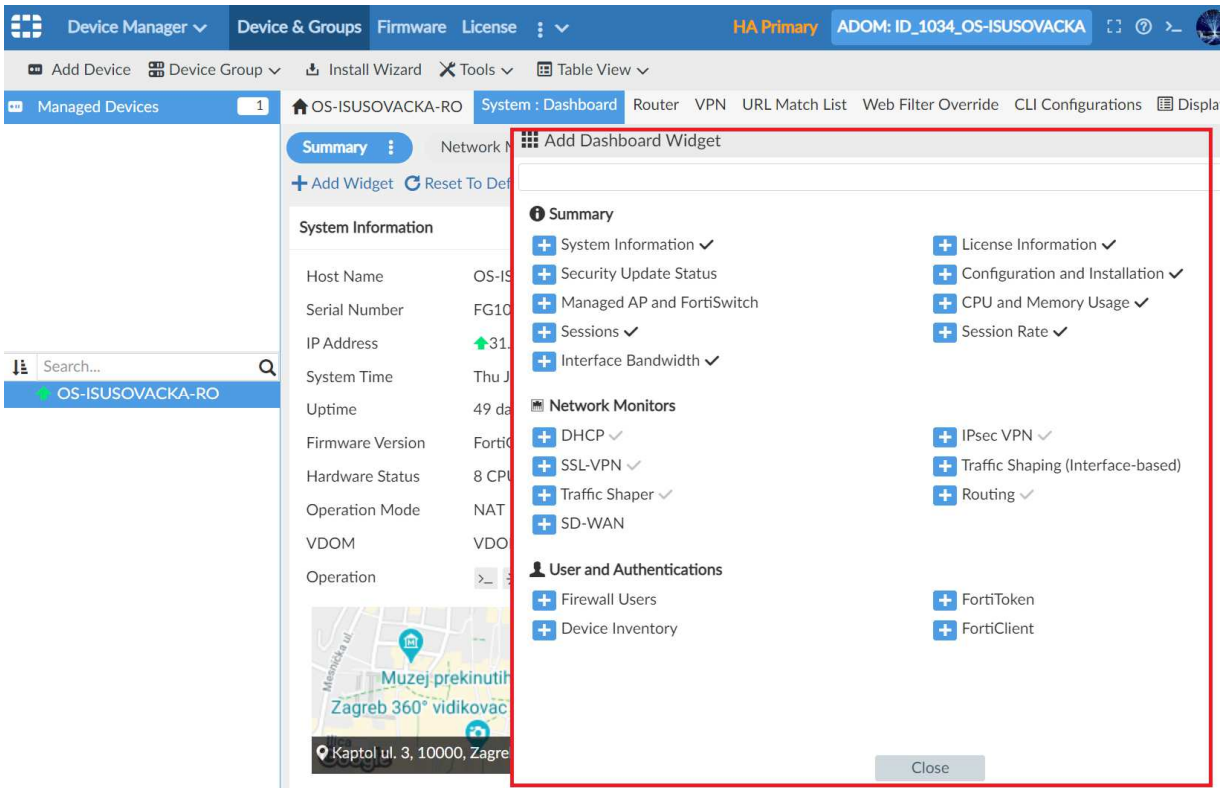
Slika 55: FortiManager – nadzorna ploča

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

System : Dashboard / Add Widget



Slika 56: Dodavanje novog widgeta na upravljačku ploču



Slika 57: Kontrolna ploča FortiManagera – odabir widgeta

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

6.4 Nadzor nad korisnicima na mreži

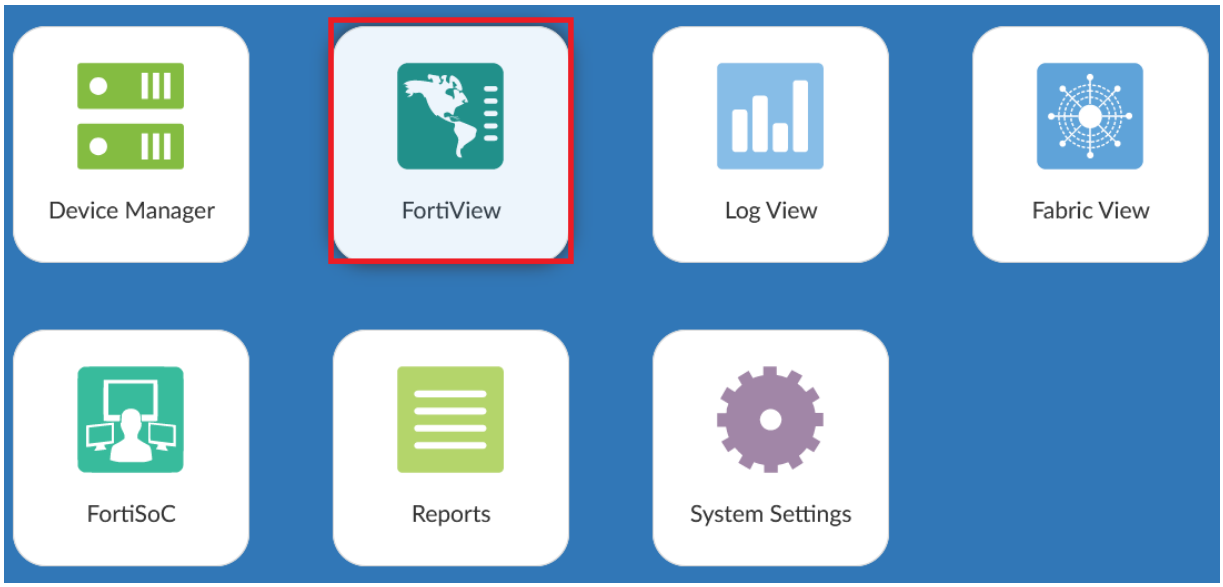
FortiAnalyzer daje uvid u ponašanje korisnika na mreži.

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

Prvi je korak prijava u sustav FortiAnalyzer putem adrese mrežnog sučelja i unosa ranije određenih vjerodajnica.

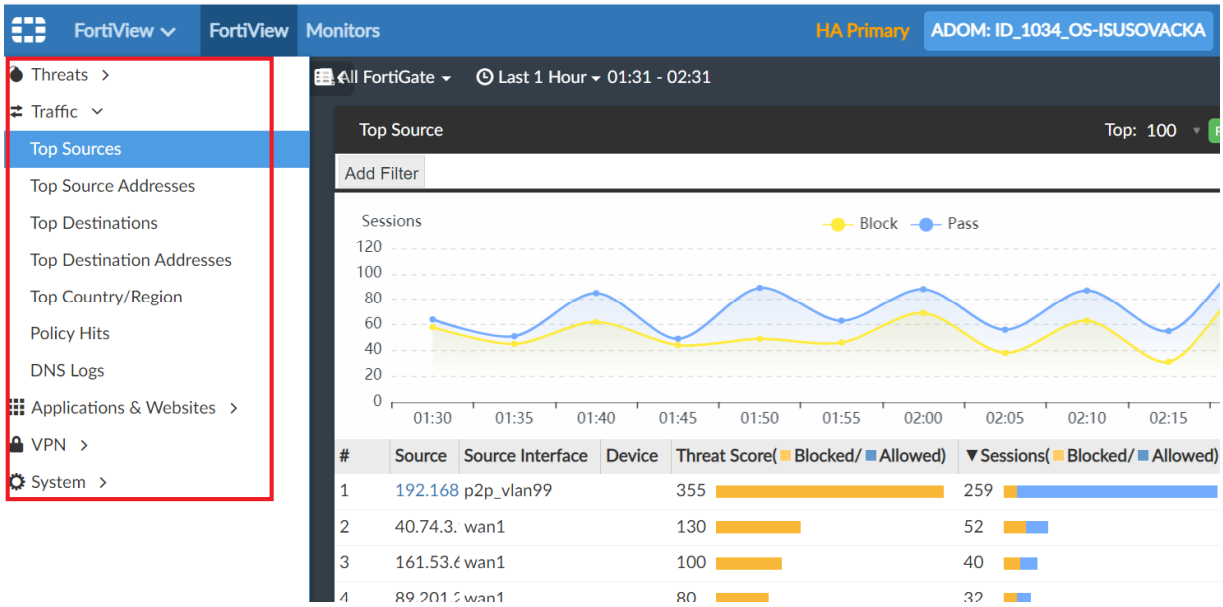
Za pristup nadzoru mreže, odnosno aktivnostima njezinih korisnika, potrebno je odabrati izbornik *FortiView* unutar ADOM-a gdje se izvodi nadzor:

ADOM / FortiView



Slika 58: Prikaz izbornika FortiView unutar ADOM-a

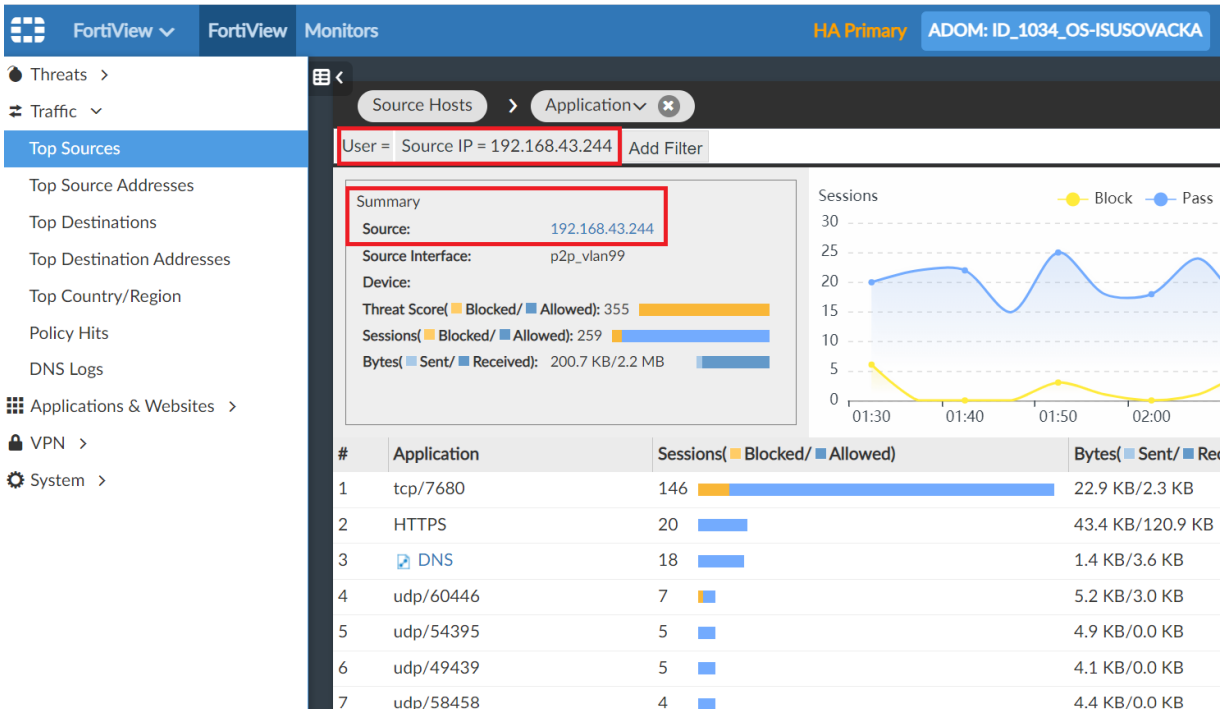
Nakon odabira, na središnjem je panelu prikazana sva mrežna aktivnost, odnosno promet koji je podijeljen u više kategorija.



Slika 59: FortiAnalyzer – izbornik FortiView

Moguće je odabrati mrežni promet prema destinacijama, filtrirati ga prema adresi korisnika, odnosno prema korisnicima koji su prijavljeni u sustav.

Odabirom određenog korisnika ili njegove adrese, pristupa se detaljnijoj analizi prometa i mrežnih protokola koji su inicirani od strane odabranog korisnika.

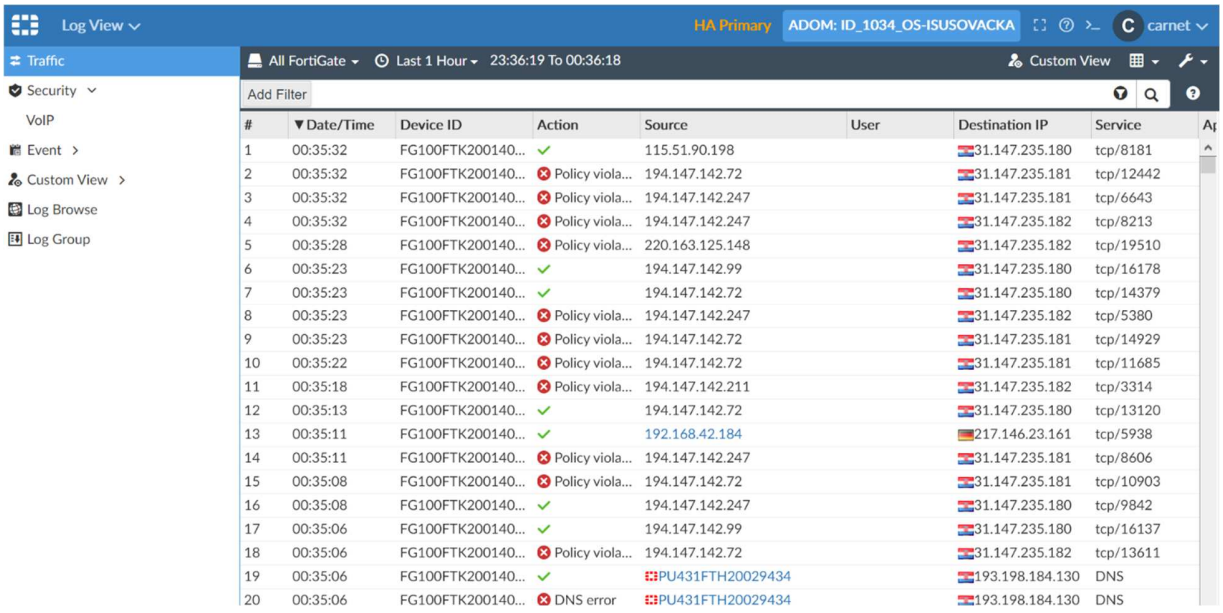


Slika 60: FortiAnalyzer – prikaz detaljne mrežne aktivnosti po korisniku

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

Za pristup navedenom mehanizmu, na FortiAnalayzeru unutar ADOM-a potrebno je odabrati izbornik *Log View.*

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



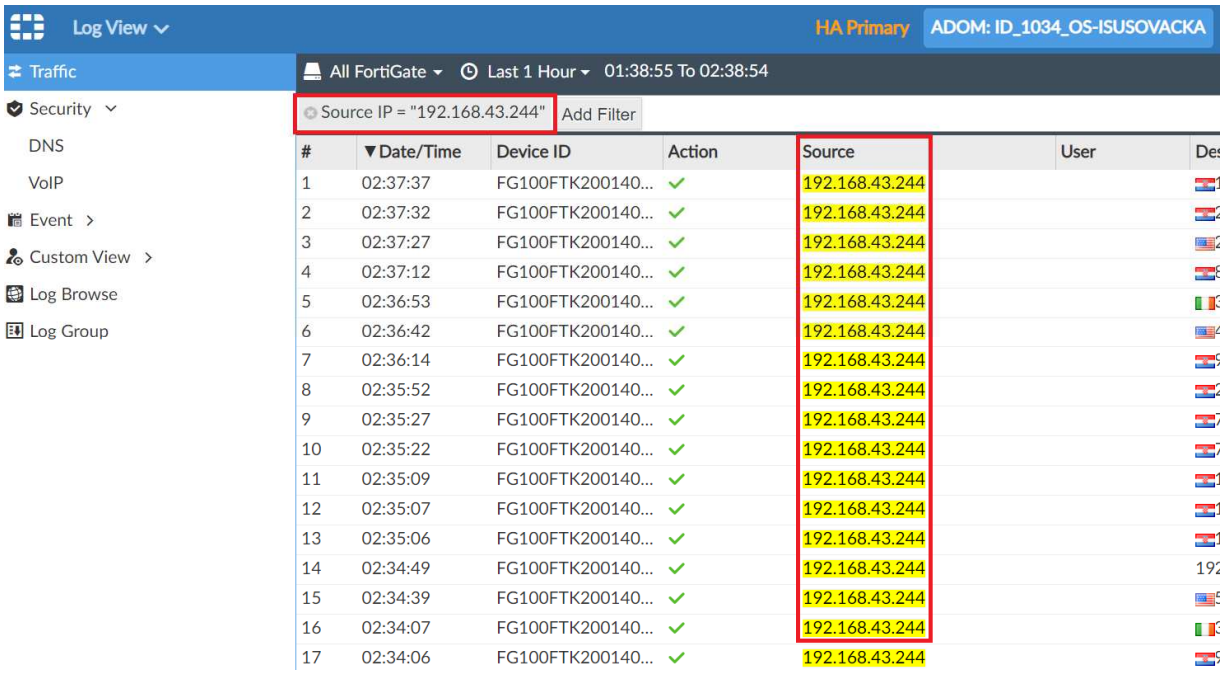
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service
1	00:35:32	FG100FTK200140...	✓	115.51.90.198		31.147.235.180	tcp/8181
2	00:35:32	FG100FTK200140...	Policy viola...	194.147.142.72		31.147.235.181	tcp/12442
3	00:35:32	FG100FTK200140...	Policy viola...	194.147.142.247		31.147.235.181	tcp/6643
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 61: 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 uz tu adresu.



Slika 62: Log View – primjer filtriranog loga po adresi izvora

6.5 Konfiguracija osnovnih postavki na mrežnoj opremi

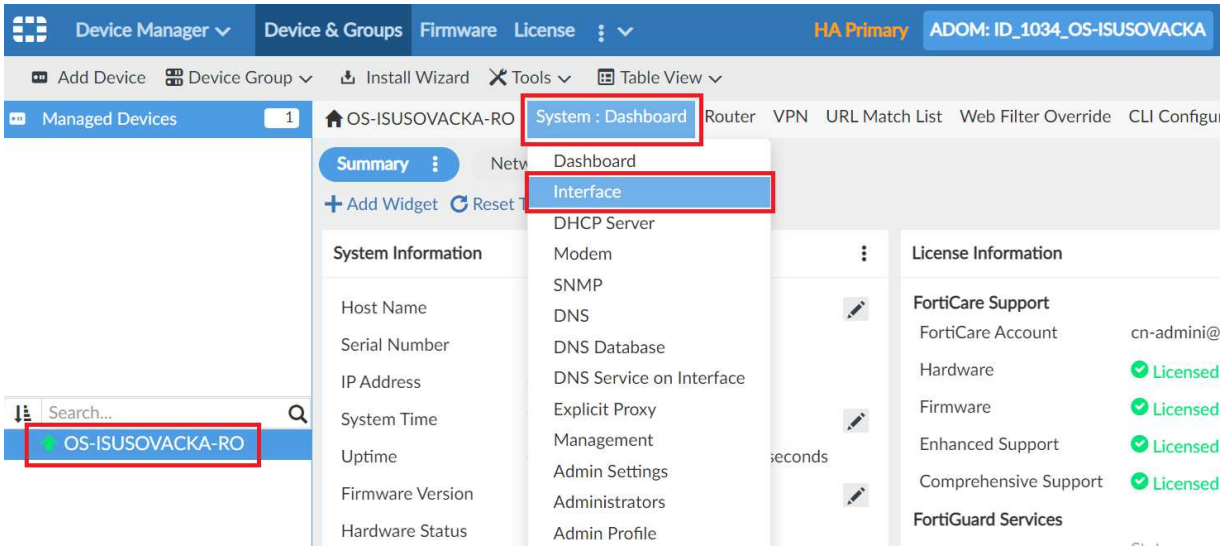
Sve promjene u sustavu i konfiguraciji rade se isključivo u FortiManageru, a ne lokalno na opremi jer u tom slučaju konfiguracija uređaja ne bi bila sinkronizirana s FortiManagerom.

Na mrežne je uređaje postavljena početna konfiguracija i odgovarajući broj SSID-a od strane CARNET-a kako bi se omogućilo optimalno korištenje mrežnih resursa. Nije preporučeno mijenjati početno postavljene konfiguracije!

6.5.1 Primjer konfiguracije sučelja na usmjerivaču

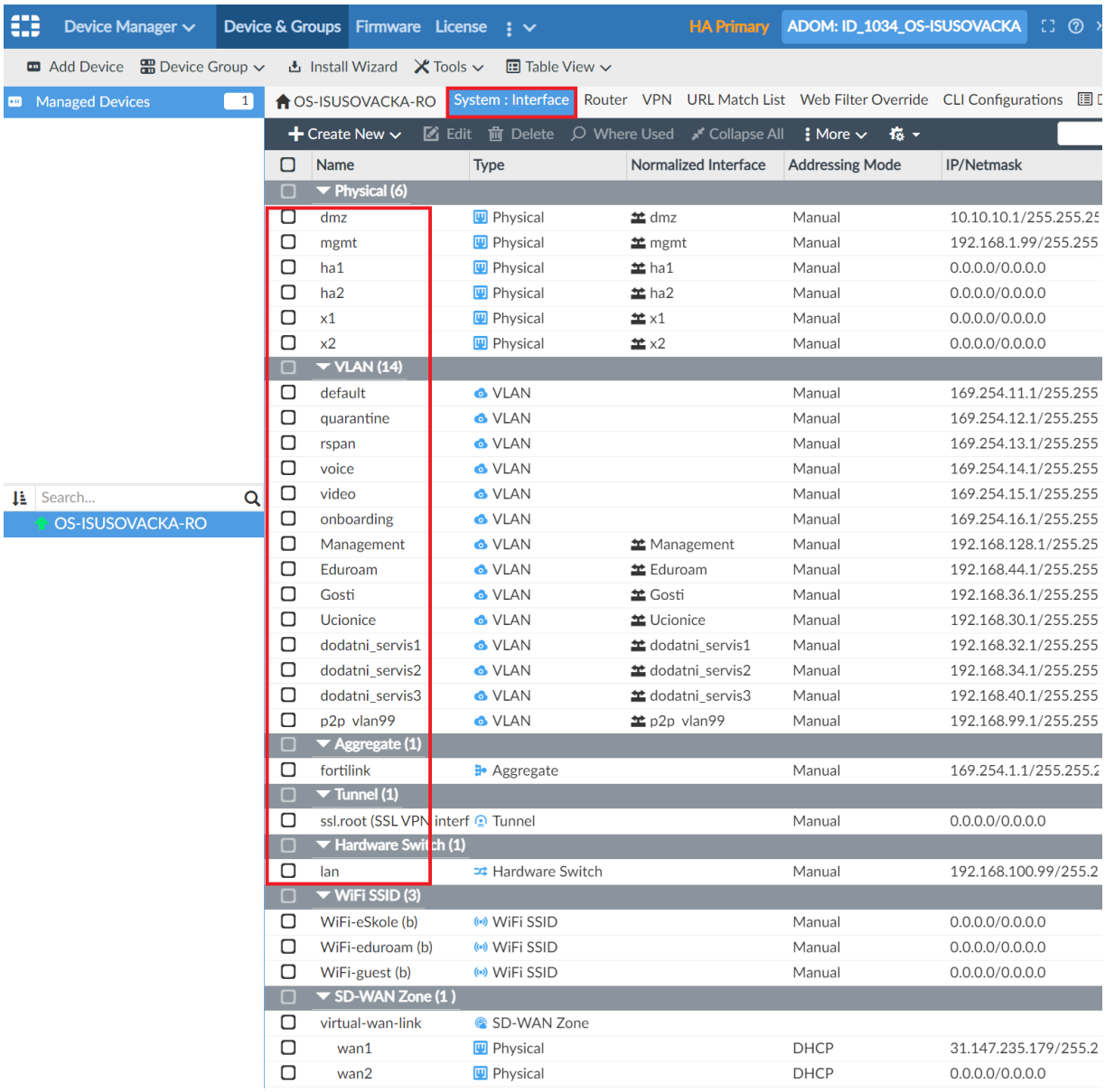
Početni korak u konfiguraciji sučelja jest pristup izborniku *Device Manager* unutar ADOM-a na kojem treba izvršiti promjene u sustavu.

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



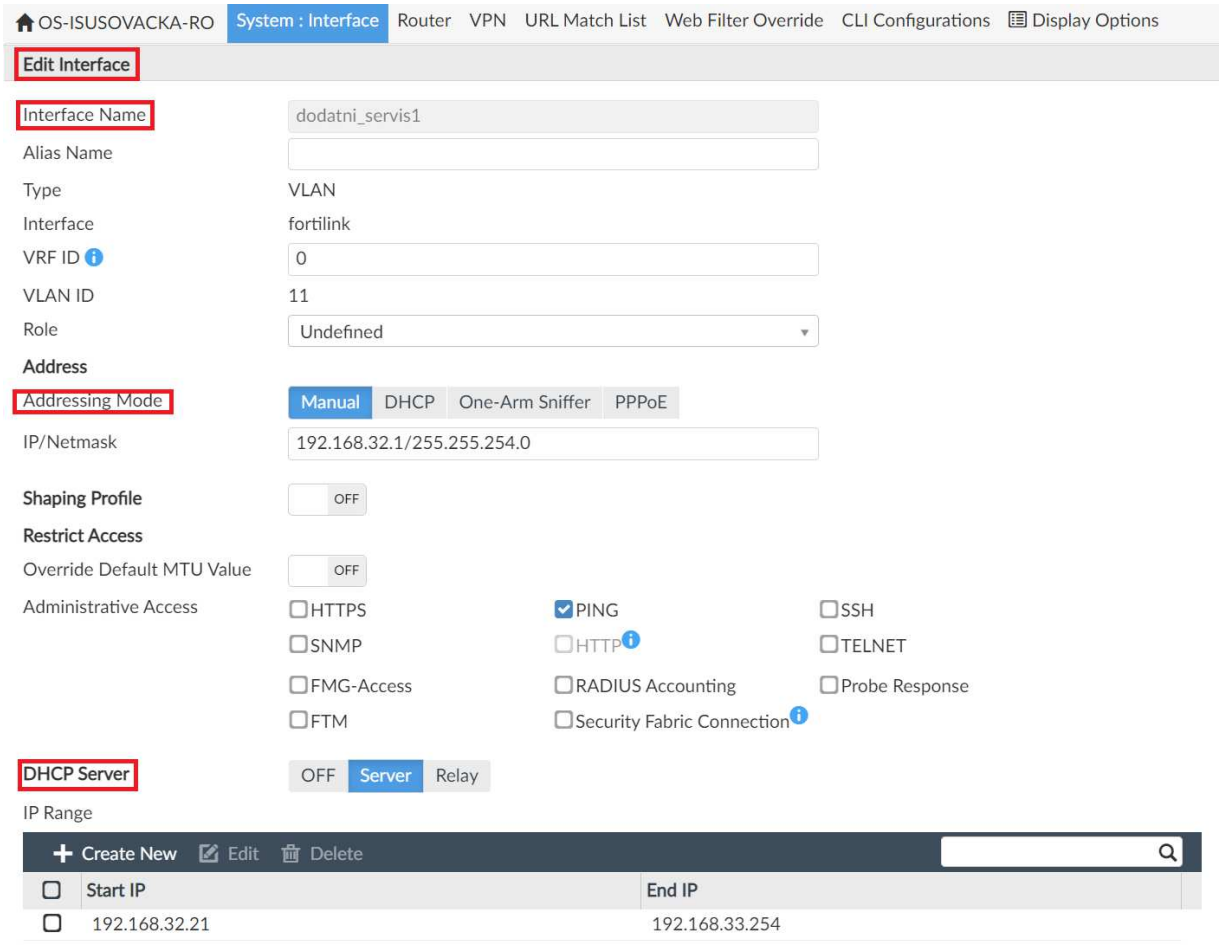
Slika 63: FortiManager – kontrolna ploča za odabir sučelja

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



Slika 64: FortiManager – popis sučelja usmjerivača

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



Slika 65: FortiManager – uređivanje sučelja

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

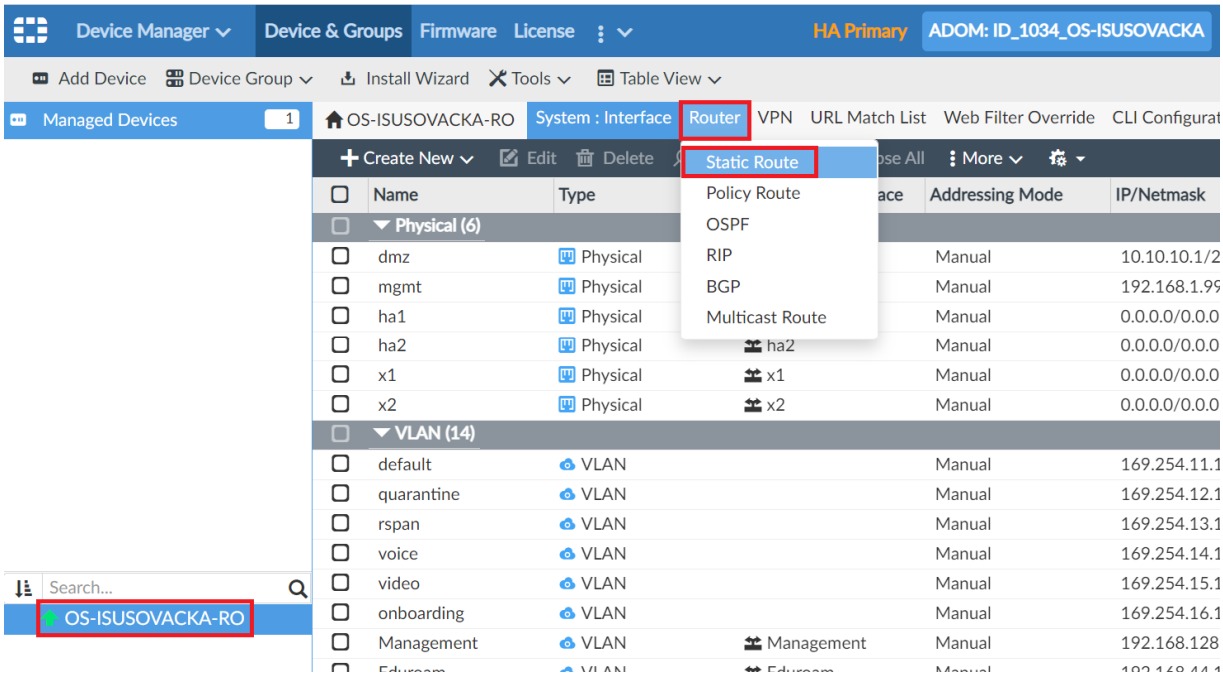
6.5.2 Primjer konfiguracije rute na usmjerivaču

Device Manager / Router / Static Route / Create New

Konfiguracija rute na usmjerivaču realizira se kroz FortiManager centralni sustav za upravljanje i nadzor. Prvi korak je prijava u FortiManager centralni sustav upravljanja, unosom korisničkog imena i lozinke, ranije definiranih od strane administratora sustava

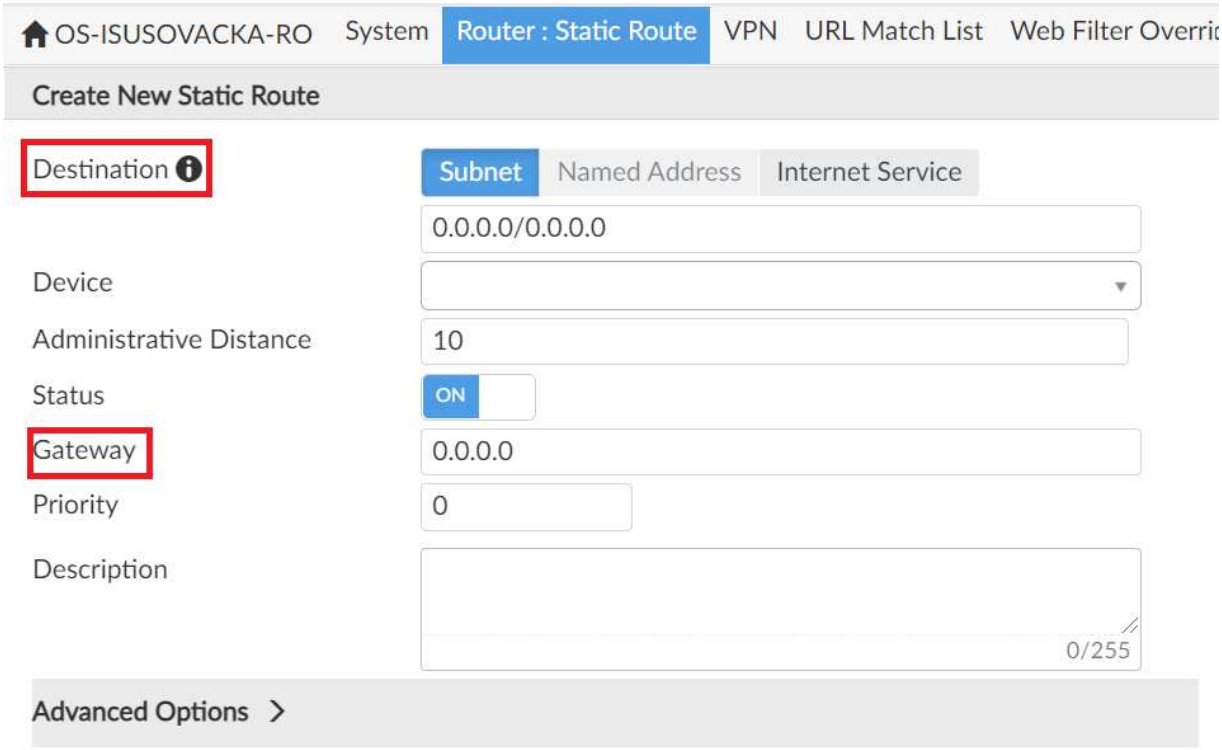
Sljedeći korak u konfiguraciji sučelja je pristup izborniku *Device Manager* unutar ADOM-a na kojem je potrebno izvršiti promjene u sustavu.

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



Slika 66: FortiManager – odabir konfiguracije statičke rute

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



Slika 67: Unos parametra statičke rute

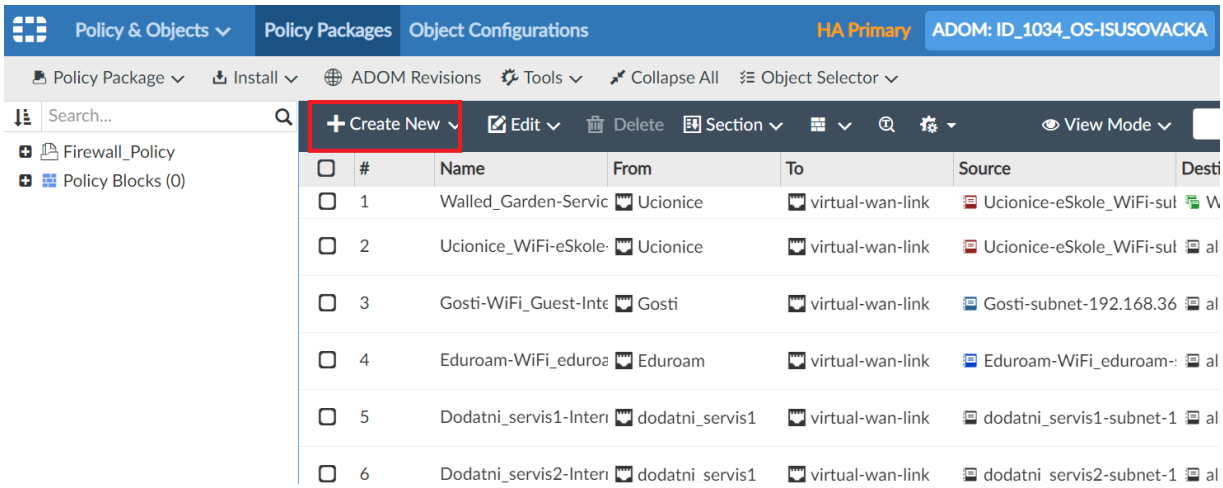
6.5.3 Primjer dodavanja sigurnosnog pravila

FortiManager / Policy & Objects / Create New

Sigurnosno pravilo na usmjerivaču kreira se kroz FortiManager centralni sustav za upravljanje i nadzor. Prvi korak je prijava u FortiManager centralni sustav upravljanja, unosom korisničkog imena i lozinke, ranije definiranih od strane administratora sustava.

Sjedeći korak u kreiranju sigurnosnih pravila je odabir izbornika *Policy & Objects* unutar ADOM-a na kojem je potrebno kreirati sigurnosno pravilo.

Nadalje, potrebno je odabrati opciju za kreiranje novog sigurnosnog pravila (*Create New*).



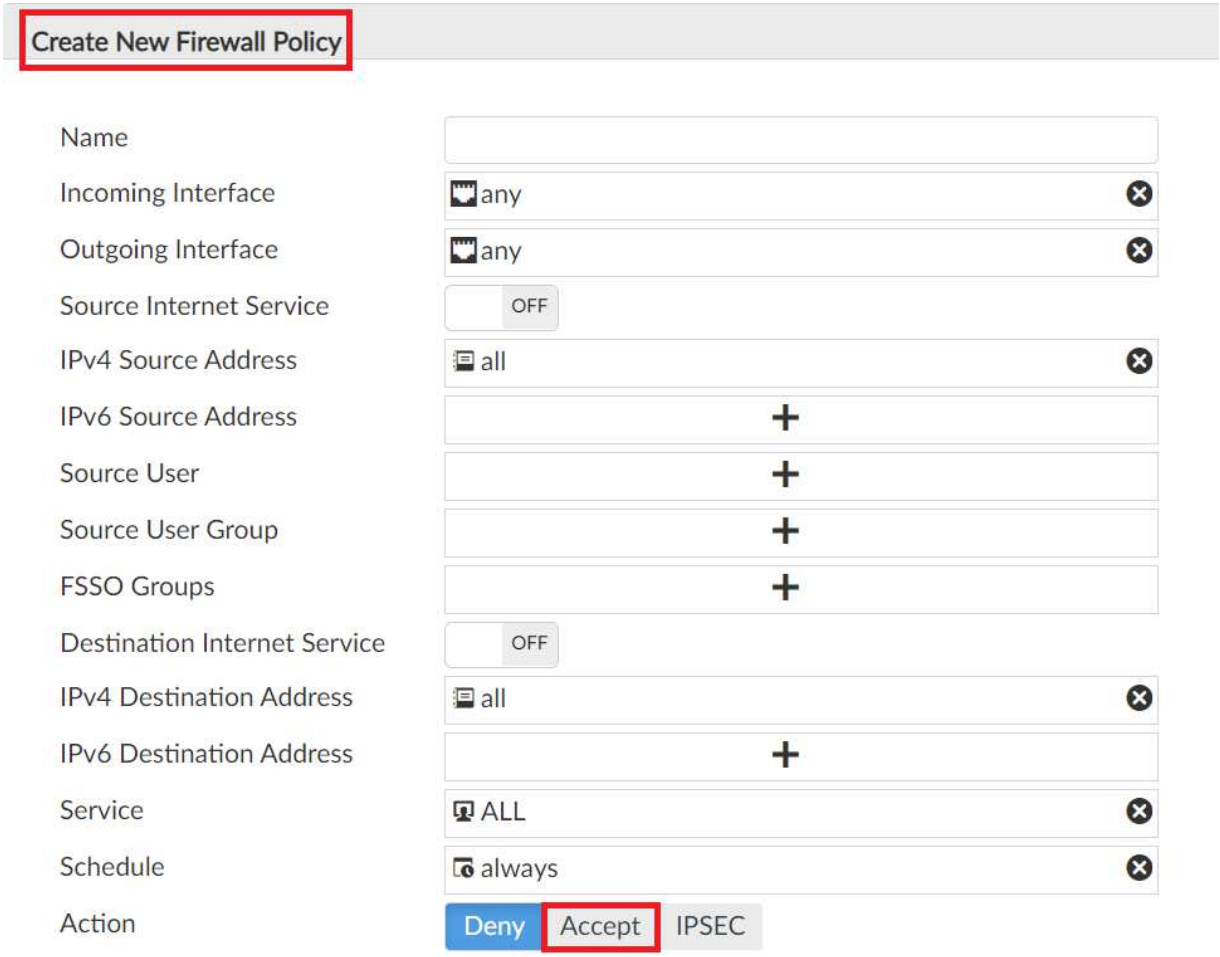
Slika 68: FortiManager – kreiranje sigurnosnog pravila

Otvara se izbornik za kreiranje sigurnosnih pravila (*Policy Package*).

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

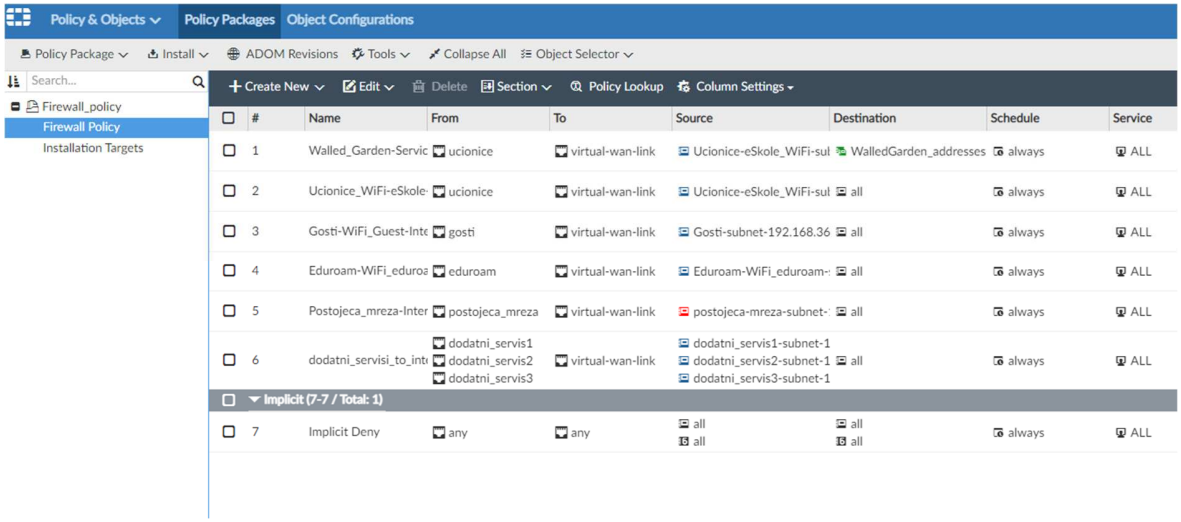
Filtraciju je moguće napraviti i prema odredišnoj, odnosno izvornoj adresi, korisniku na mreži ili grupi.

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



Slika 69: FortiManager – unos parametara za kreiranje sigurnosnog pravila

Provjera konfiguracije vrši se kroz izbornik *Policy Packages* , te navedeni pregled nudi uvid u sva kreirana pravila u sustavu za upravljanje.



Slika 70: Prikaz sigurnosnih pravila pristupa

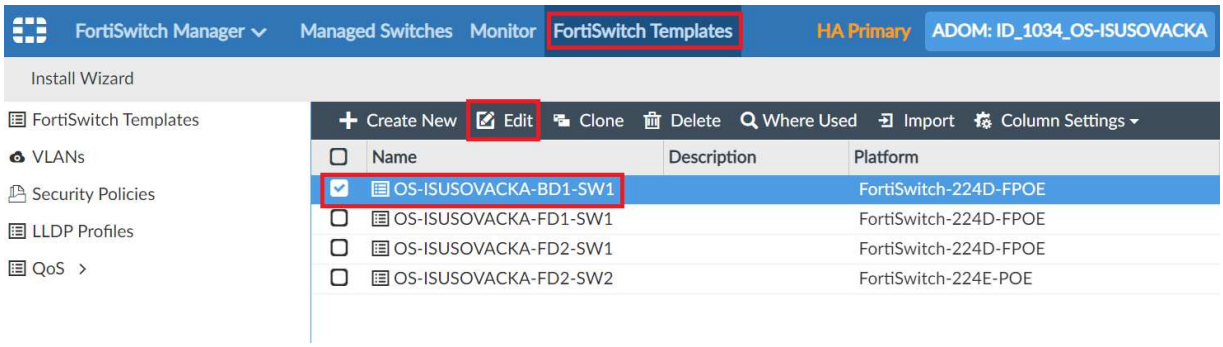
6.5.4 Primjer konfiguracije sučelja preklopnika

FortiManager / FortiSwitch Manager / FortiSwitch Templates / Edit

Prvi korak kod konfiguracije sučelja preklopnika je prijava u centralni sustav upravljanja FortiManager, unosom korisničkog imena i lozinke, ranije definiranih od strane administratora sustava.

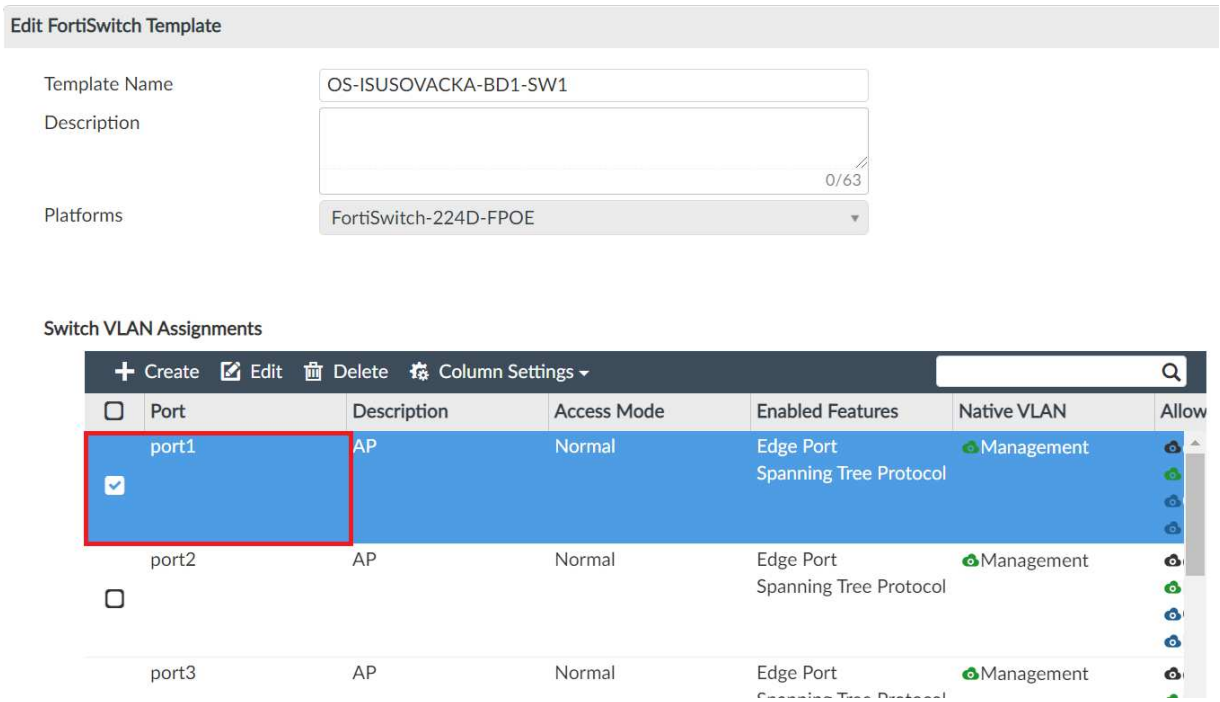
Sljedeći korak u kreiranju predloška za preklopnike je odabir izbornika *FortiSwitch Manager* unutar ADOM-a na kojem treba napraviti navedeni predložak.

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



Slika 71: Uređivanje konfiguracijskog predloška za preklopnik

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



Slika 72: Odabir sučelja unutar konfiguracijskog predloška

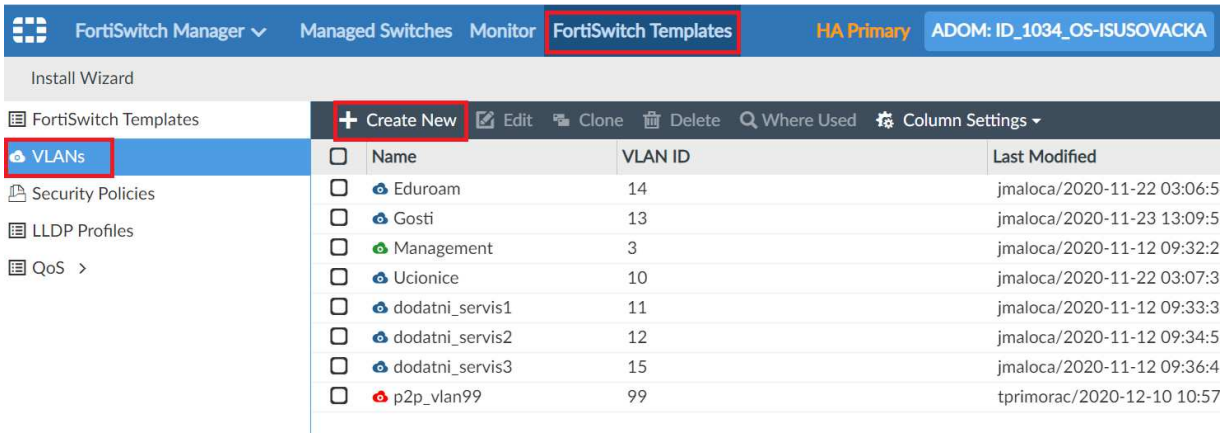
U izborniku su prikazana sva sučelja određena za preklopnik. Odabirom broja i imena sučelja koje je potrebno izmijeniti, prikazuju se konfiguracijske mogućnosti koje je moguće primijeniti, npr. postavka o dozvoljenim VLAN-ovima i drugo.

6.5.5 Primjer kreiranja novog VLAN-a

FortiManager / FortiSwitch Manager / VLANs / Create New

Prvi korak je prijava u Fortimanager centralni sustav upravljanja, unosom korisničkog imena i lozinke, ranije definiranih od strane administratora sustava. Nakon prijave u sustav, na popisu školskih ustanova odabire se ADOM u kojoj se želi kreirati VLAN.

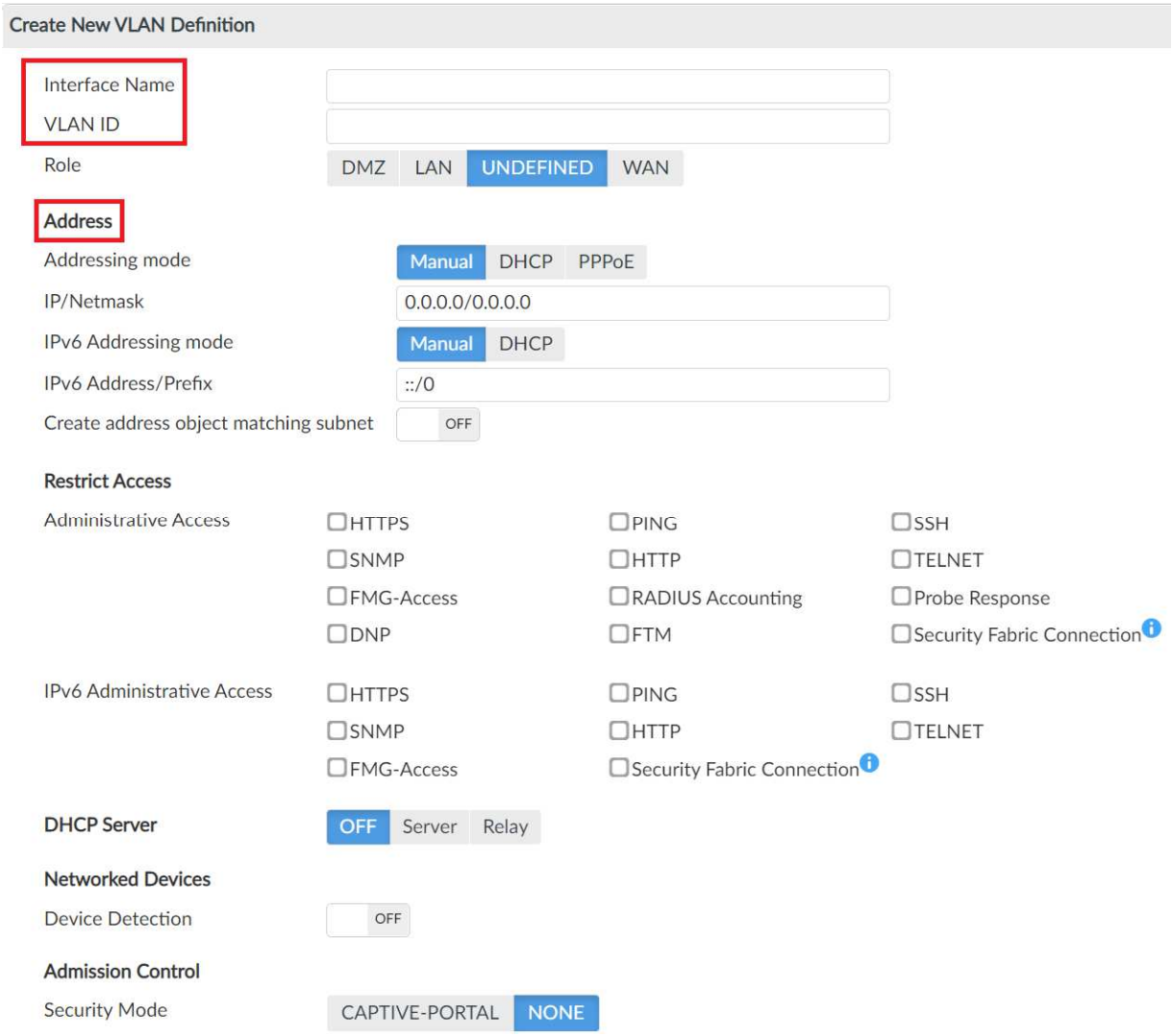
Za kreiranje podmreže, u izborniku *FortiSwitch Manager* potrebno je odabrati opciju za odabir predloška (*FortiSwitch Templates*) i u podizborniku *VLANs* odabrati kreiranje novog VLAN-a (*Create New*).



Slika 73: FortiSwitch – Postupak kreiranja VLAN-a

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

Od dodatnih opcija nudi se mogućnost kreiranja *DHCP* servisa na dediciranom VLAN segmentu odnosno način autentikacije na isti putem *Captive portala.*



Slika 74: Unos postavki prilikom kreiranja VLAN-a

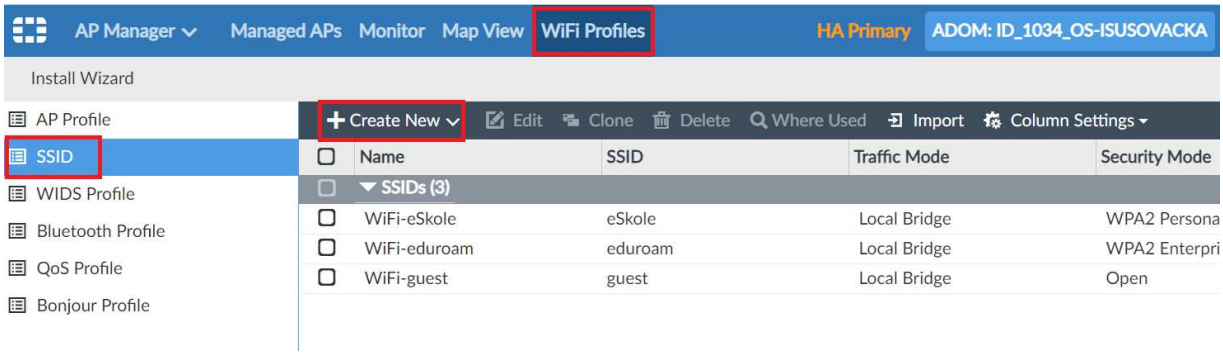
6.5.6 Primjer kreiranja novog SSID-a

FortiManager / AP Manager / WiFi Profiles / SSID

Konfiguracija SSID-a vrši se preko FortiManager centralnog sustava upravljanja. Nakon prijave u sustav, na popisu školskih ustanova, odabire se lokacija u kojoj se želi izvršiti promjena.

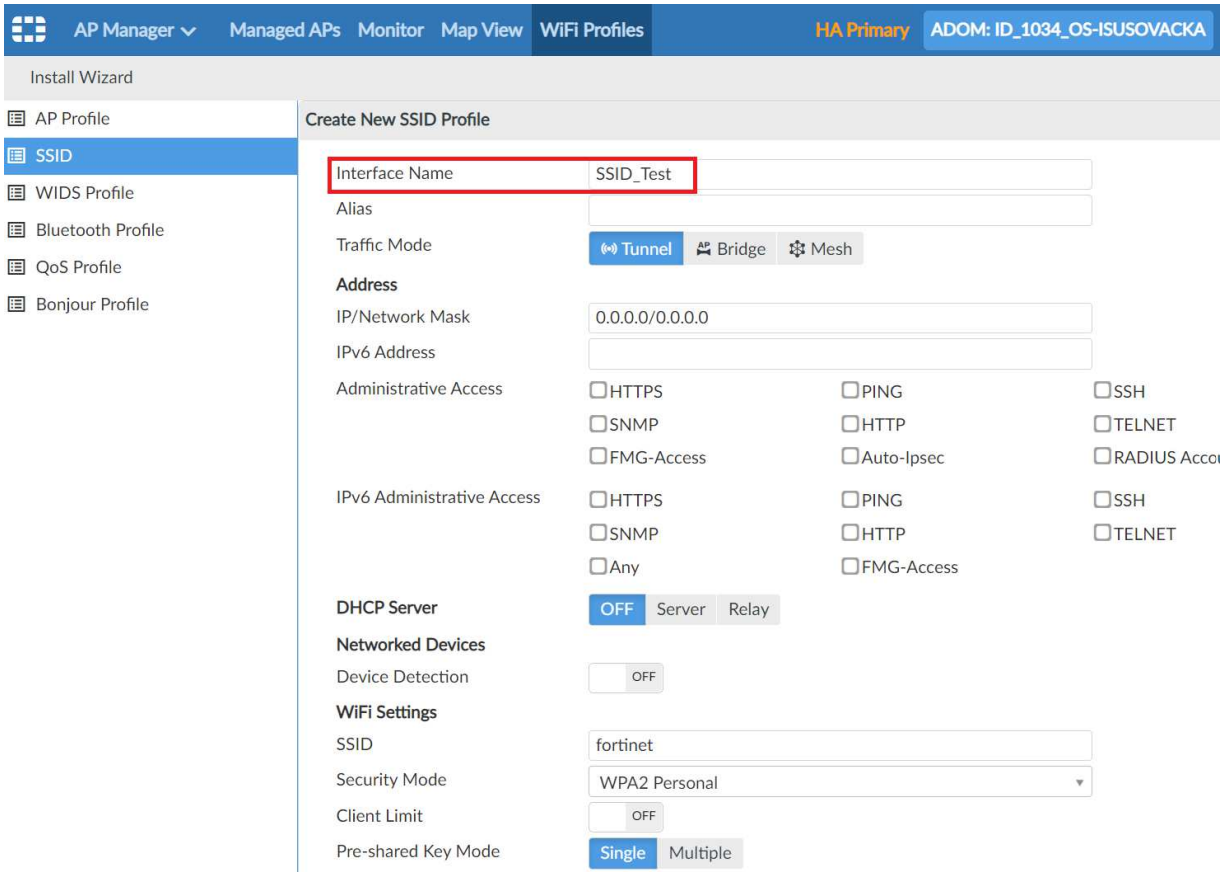
Sljedeći korak u kreiranju novog SSID-a je odabir izbornika *AP manager* unutar ADOM-a gdje treba napraviti zadane promjene.

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



Slika 75: Dodavanje nove bežične mreže – SSID

U novom je izborniku potrebno unijeti informacije o nazivu mreže, adresi, vrsti sigurnosti i načinu autentikacije na mrežu u okviru obveznih podataka, ako je navedena mreža odabrana.



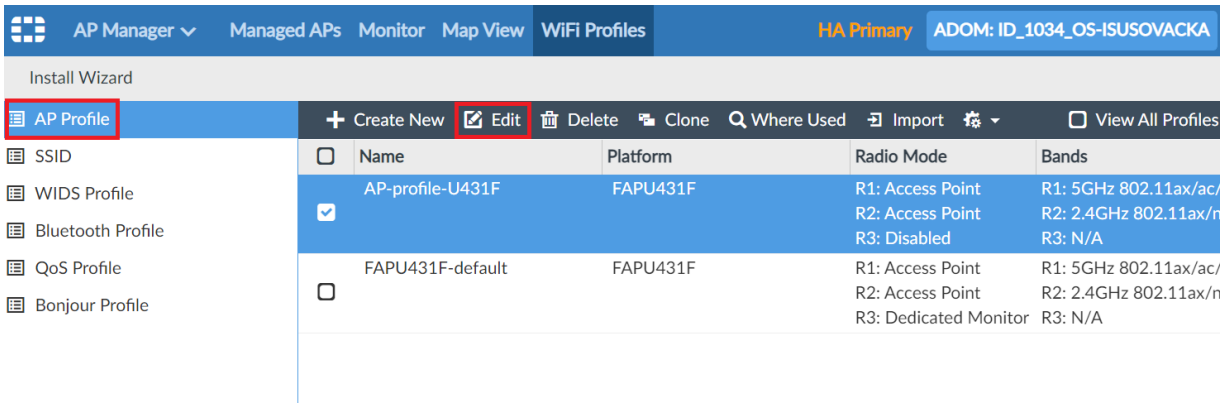
Slika 76: Unos postavki za novu bežičnu mrežu – SSID

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 izborniku *AP Manager* potrebno je odabrati opciju *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 77: Odabir uređivanja profila bežične pristupne točke

Otvara se opcija SSID i na popis mreža koje su trenutno pridružene profilu dodaje se novokreirana mreža.

Slika 78: Pridruživanje novokreirane bežične mreže profilu pristupne točke

6.5.7 Primjer kreiranja novog korisnika za *guest* mrežu

Policy & Objects / Object Configuration / User Definition

Početni korak kod konfiguracije korisnika je prijava u središnji sustav upravljanja putem poveznica https://mreza-fm.e-skole.hr i https://mreza-fm2.e-skole.hr unosom korisničkog imena i lozinke koje je administrator sustava ranije odredio.

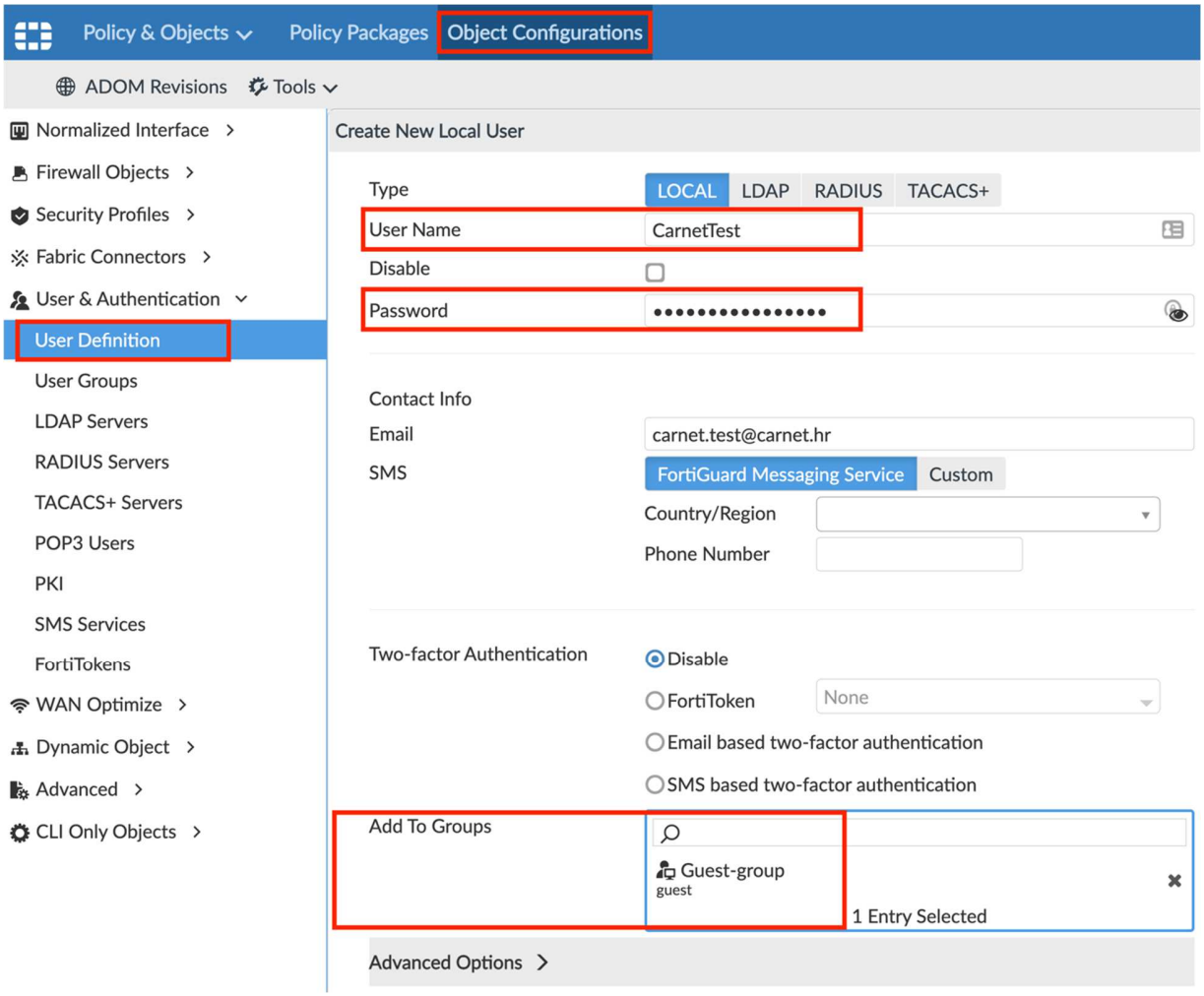
Nakon odabira lokacije, na središnjem se panelu odabire izbornik *Policy & Objects.*

Obrascu za kreiranje korisnika (*User Definition*) pristupa se odabirom opcije *Object Configuration* i nakon toga *Users & Authentication*. Nakon odabira opcije *User Definition*, prikazuje se popis svih kreiranih korisnika te pritiskom na *Create New* započinje proces kreiranja korisnika.

U konfiguracijski se prozor unose sljedeći parametri:

- odabire se *LOCAL*, budući da se radi o lokalnom korisniku,
- ***User Name*** – jedino obvezno polje u kojem se definira korisničko ime,
- ***Password*** – polje nije obvezno, ali se iz sigurnosnih razloga preporučuje definirati lozinku,
- ***Contact Info*** – unose se korisnički podaci (adresa elektroničke pošte, broj telefona, itd.),
- ***Two-factor Authentication*** – po potrebi se definiraju dodatni sigurnosni parametri,

- ***Add To Groups*** – odabire se unaprijed definirana korisnička grupa *Guest-group.*

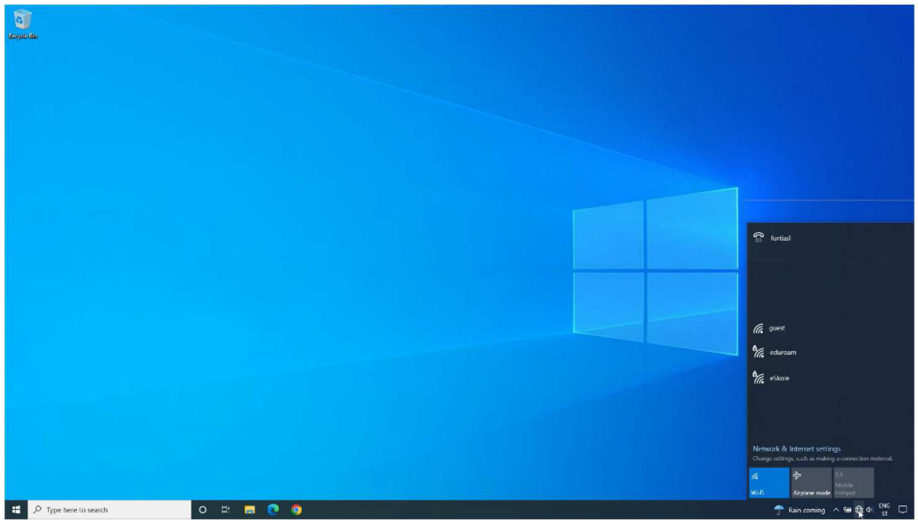


Slika 79: User Definition – obrazac za kreiranje novog korisnika

Nakon unosa svih parametara, pritiskom na *OK*, završava proces kreiranja novog korisnika za *guest* bežičnu mrežu.

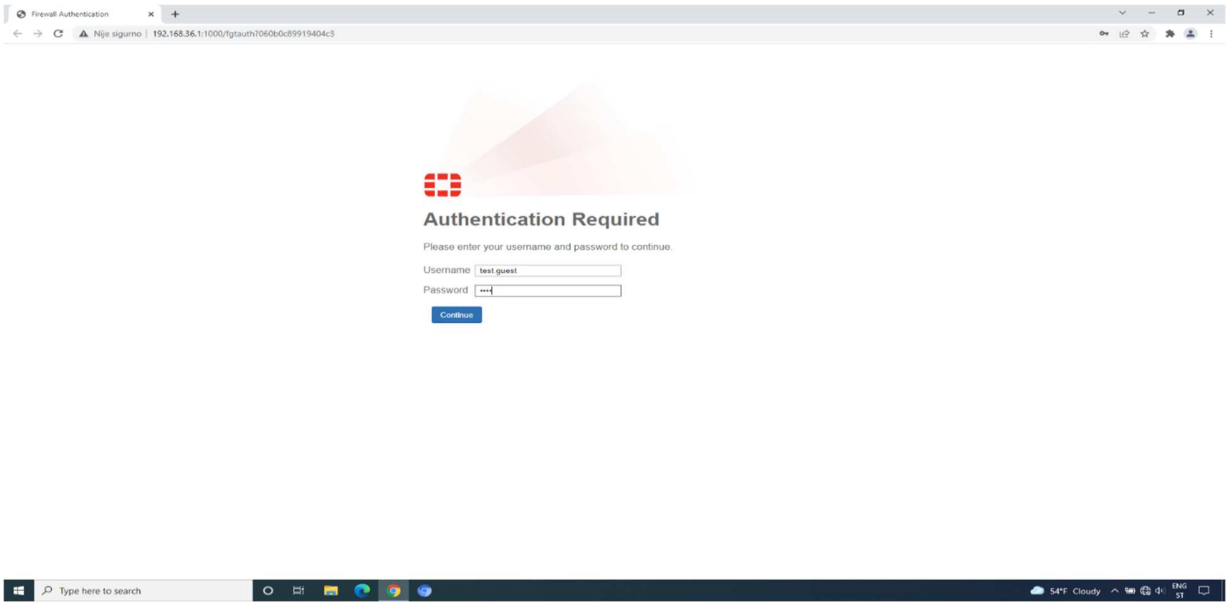
6.5.8 Spajanje na bežičnu mrežu *guest*

Nakon što administrator sustava, odnosno STP, kreira korisnički račun, slijedi prijava korisnika na računalo. Korisnik na računalu odabire bežičnu mrežu *guest* i nakon nekoliko trenutaka, u pregledniku se otvara mrežna stranica gdje treba upisati korisničko ime i lozinku koje je prethodno dobio od administratora sustava.



Slika 80: Spajanje korisnika na bežičnu mrežu guest

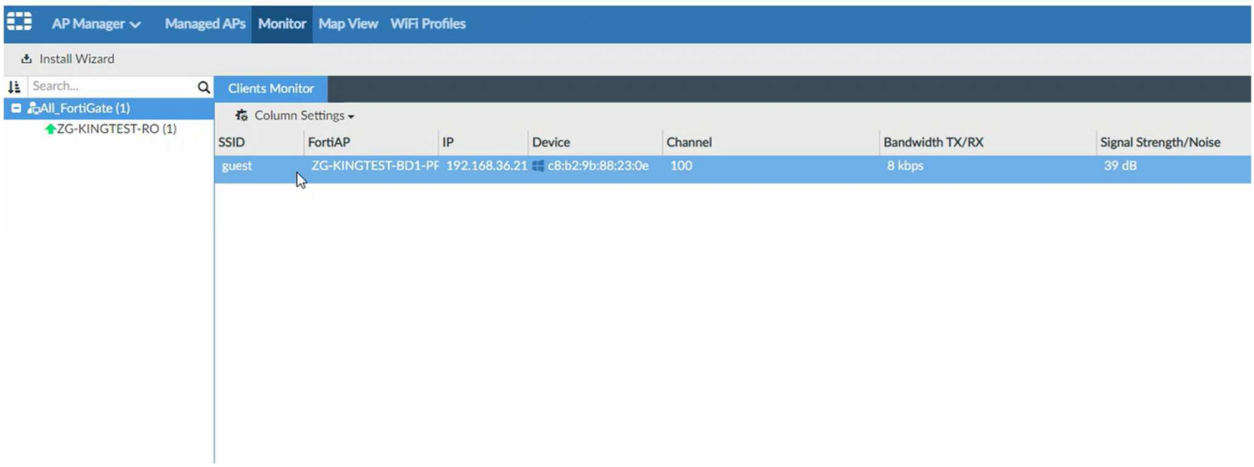
Nakon početnog spajanja na SSID, u pregledniku se otvara mrežna stranica gdje je potrebno upisati korisničko ime i lozinku, nakon čega je korisnik spreman za korištenje navedene mreže.



Slika 81: Pristupni portal – obrazac za prijavu na bežičnu mrežu guest

Nakon uspješne autentikacije, korisniku je omogućen pristup resursima na internetu. Na nadzornoj ploči Monitor u centralnom sustavu za upravljanje FortiManager administratoru sustava pojavljuje se korisnikov klijent i njegovim je odabirom vidljivo da je korisnik uredno spojen na bežičnu mrežu *guest*.

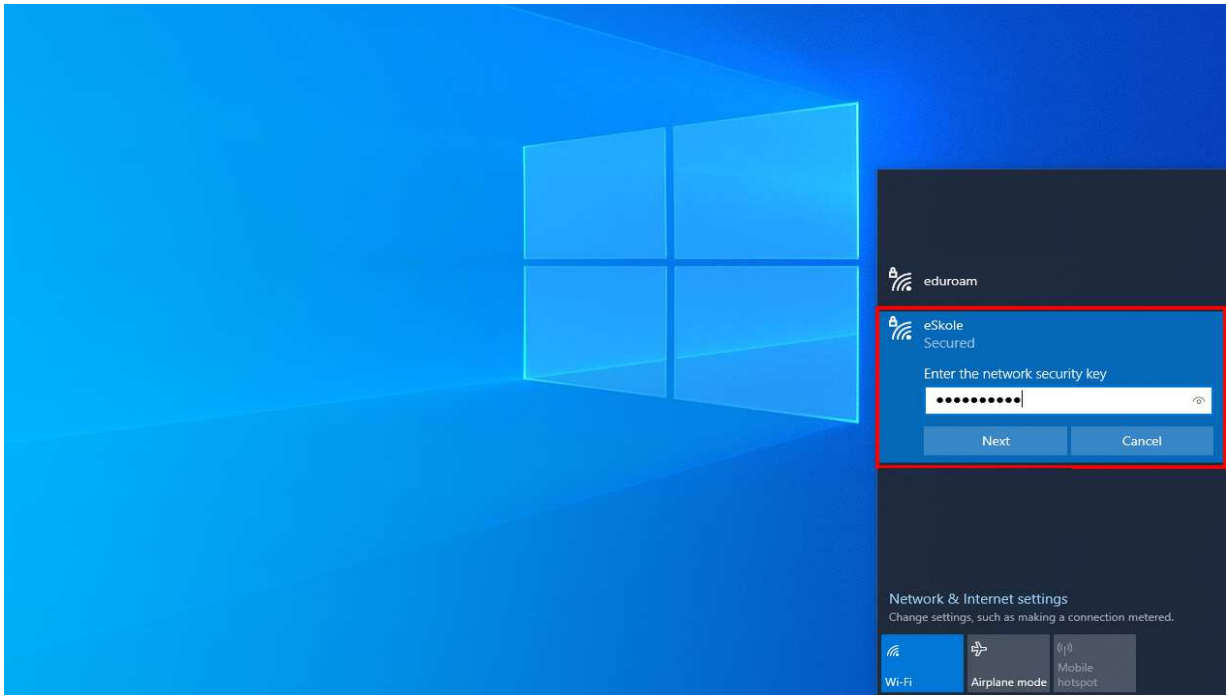
AP Manager / Monitor / Clients Monitor



Slika 82: FortiManager Clients monitor

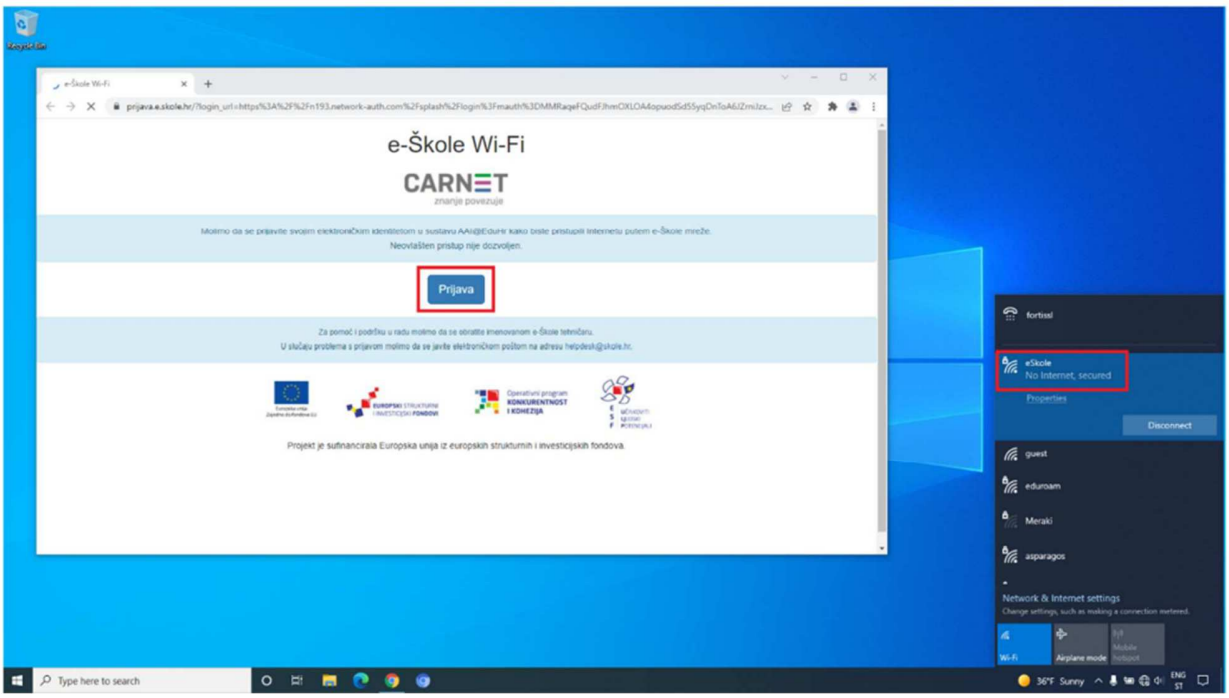
6.5.9 Spajanje na bežične mreže *eSkole* i *eduroam*

Prilikom spajanja korisnika na bežičnu mrežu *eSkole*, na listi dostupnih bežičnih mreža potrebno je odabrati mrežu *eSkole* i upisati *pre-shared key* (PSK) koji je proslijedio administrator sustava (privremeni PSK koji administrator sustava može po želji zamijeniti je eskole123#).



Slika 83: Spajanje korisnika na bežičnu mrežu eSkole

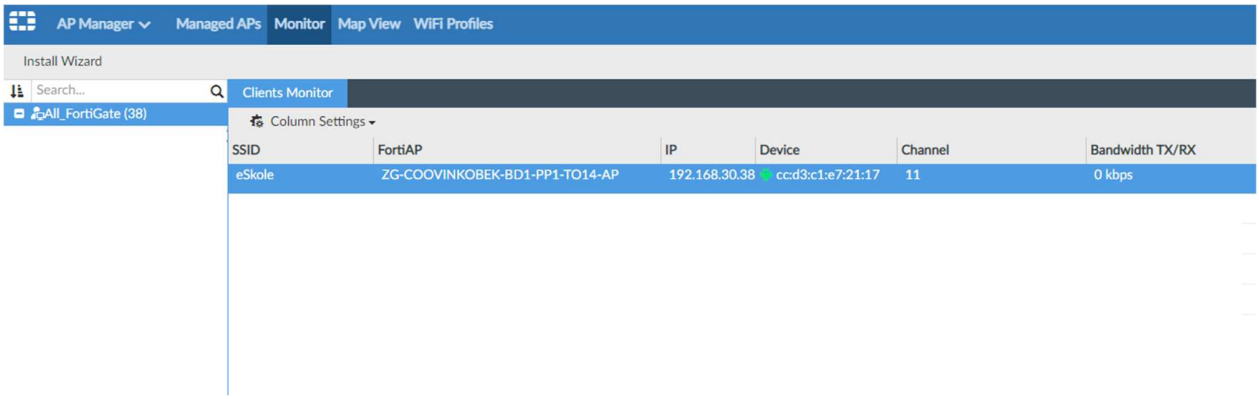
Nakon uspješnog spajanja, otvara se stranica za prijavu na koju se potrebno prijaviti pomoću podataka za sustav AAI@EduHr ako je potreban pristup resursima na internetu.



Slika 84: Prijava na sustav AAI@EduHr

Bez prijave na sustav AAI@EduHr, putem bežične mreže *eSkole* dozvoljeno je pristupati jedino servisima za nadogradnju operacijskog sustava na računalima ili drugim servisima koje CARNET dozvoljava.

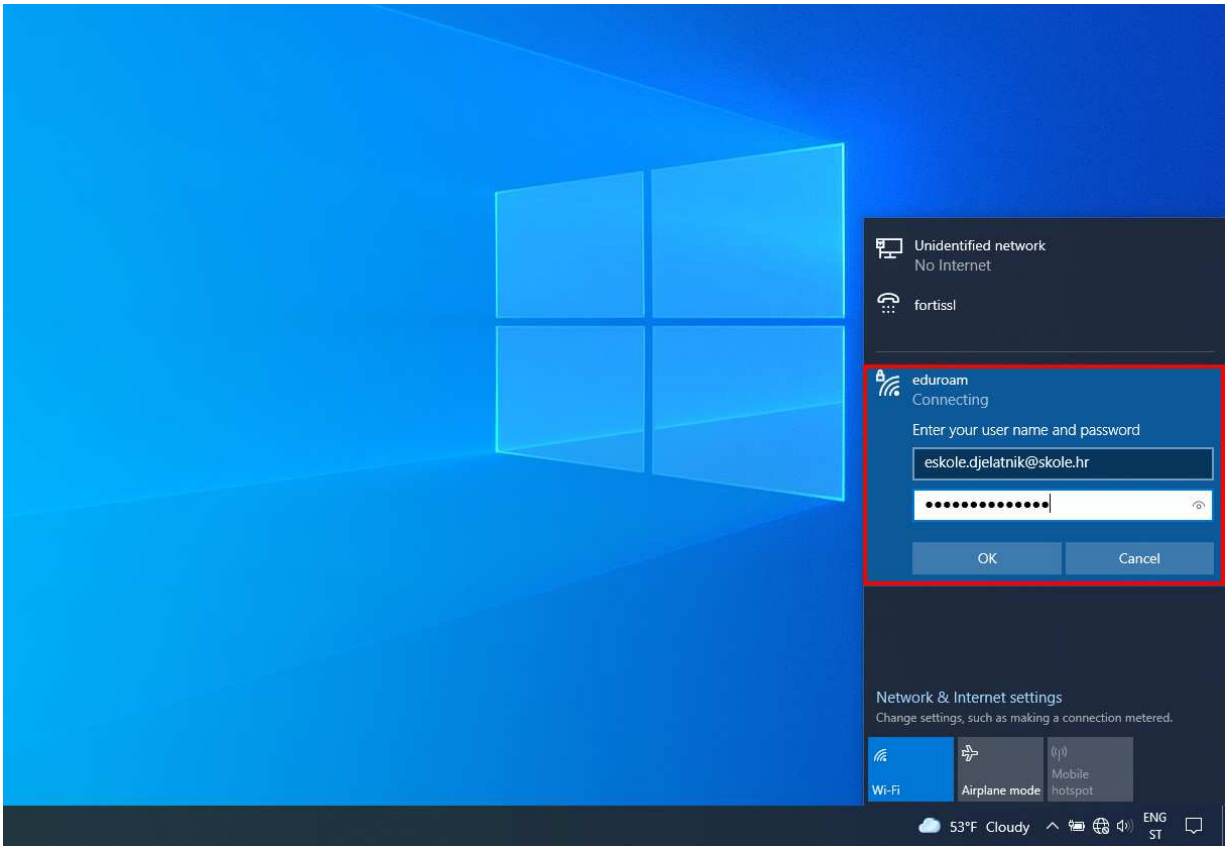
Na nadzornoj ploči Monitor u centralnom sustavu za upravljanje FortiManager administratoru sustava pojavljuje se korisnikov klijent i njegovim je odabirom vidljivo da je korisnik uredno spojen na bežičnu mrežu eSkole.



Slika 85: FortiManager – Monitor Dashboard – eSkole

Korisnik se na bežičnu mrežu *eduroam* može spajati sa ili bez primjene instalacijskog programa *eduroam installer*. Instalacijski se program preuzima na mrežnoj stranici https://installer.eduroam.hr/.

Za spajanje uređaja uz primjenu instalacijskog programa *eduroam installer*, navedeni je program potrebno preuzeti i instalirati na uređaj. Nakon instalacije, na listi dostupnih bežičnih mreža potrebno je odabrati *eduroam* i upisati podatke iz sustava AAI@EduHr.



Slika 86: Spajanje korisnika na bežičnu mrežu eduroam

Za spajanje korisničkog računala bez instalacijskog programa eduroam installer, na listi dostupnih bežičnih mreža potrebno je odabrati eduroam, upisati podatke iz sustava AAI@EduHr i potvrditi ponuđene postavke certifikata.

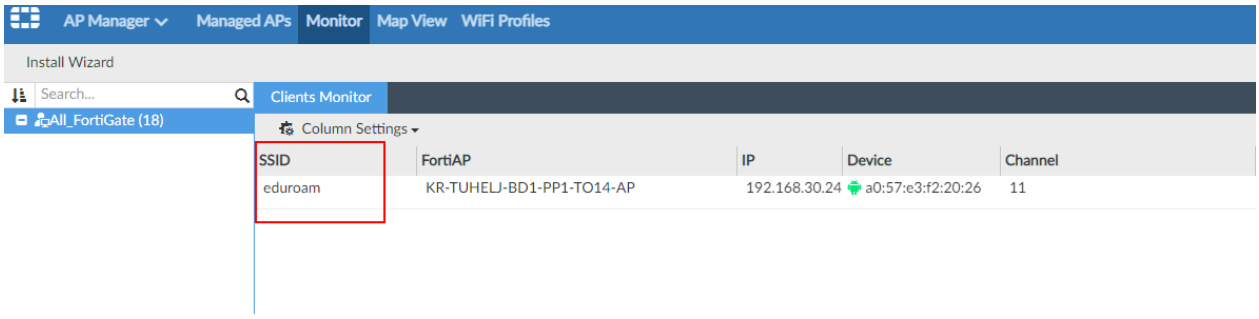
Ako se korisnik na bežičnu mrežu spaja mobilnim uređajem, potrebno je unijeti sljedeće parametre:

- **Settings** / **Connections** / **WiFi**,
- Odabrati bežičnu mrežu **eduroam**,

- **EAP method** postaviti na **TTLS**,
- **PHASE 2 authentication** postaviti na **PAP**,
- U **CA certificate** polju nije potrebno mijenjati postavke,
- U **Indentity** polje unijeti svoje AAI korisničko ime (u obliku „**ime.prezime@skole.hr**“),
- Polje **Anonymus indentity** ostaviti prazno,
- **U Wireless password** polje unijeti svoju **lozinku za AAI.**

Slika 87: Spajanje korisnika na bežičnu mrežu eduroam bez instalacijskog programa

Na nadzornoj ploči Monitor u centralnom sustavu za upravljanje FortiManager administratoru sustava pojavljuje se korisnikov klijent i njegovim je odabirom vidljivo da je korisnik uredno spojen na bežičnu mrežu eduroam.



Slika 88: FortiManager – Monitor Dashboard – eduroam

6.5.10 Postavljanje korisnika na listu blokiranih (*blacklist*)

Korisnika se na listu blokiranih postavlja kako bi mu se onemogućio pristup određenim resursima.

Korisnika je najbolje blokirati pomoću MAC adrese jer se podaci o IP adresama dodjeljuju dinamičkim putem – servisom DHCP. Na taj način postoji mogućnost da se isti korisnik neće predstavljati na mreži svaki put istom IP adresom.

Postupak blokiranja korisnika pomoću MAC adrese podijeljen je u tri osnovna koraka:

1. identifikacija korisnika
2. definiranje korisnika
3. dodavanje korisnika u dedicirano sigurnosno pravilo za zabranu pristupa resursima

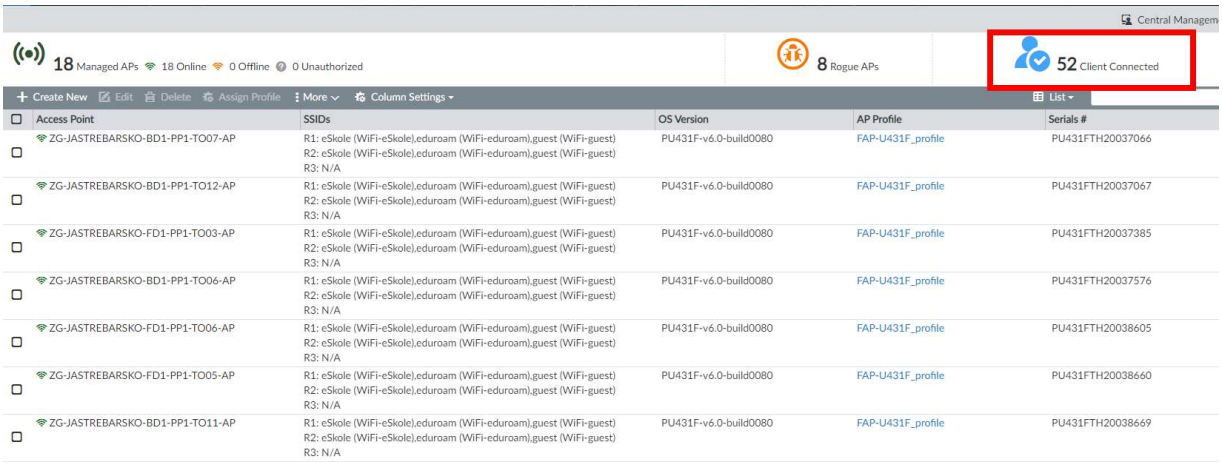
U nastavku su objašnjeni navedeni koraci.

1) Identifikacija korisnika

Identifikacija korisnika provodi se na više načina: fizičkim pristupom uređaju koji se blokira, skeniranjem mreže ili upotrebom sustava FortiManager, odnosno FortiAnalyzer.

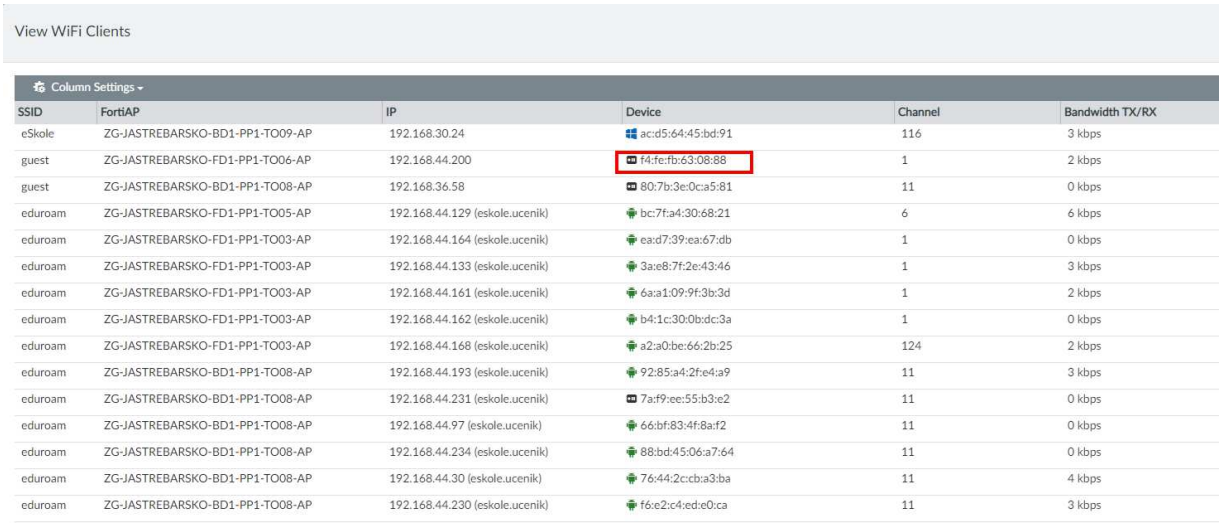
Prvi je korak odabir izbornika *AP Manager* iz pripadajućeg ADOM-a vezanog uz administraciju pripadajuće škole.

U izborniku su vidljive trenutne bežične pristupne točke definirane i autorizirane u sustavu, kao i broj spojenih korisnika.



Slika 89: Prikaz bežične infrastrukture i broj spojenih korisnika

Odabirom korisnika, prikazuje se više detalja o njemu, uključujući **MAC adresu** koja je potrebna za njegovu identifikaciju.



Slika 90: Popis korisnika bežične mreže i pripadajuće adrese

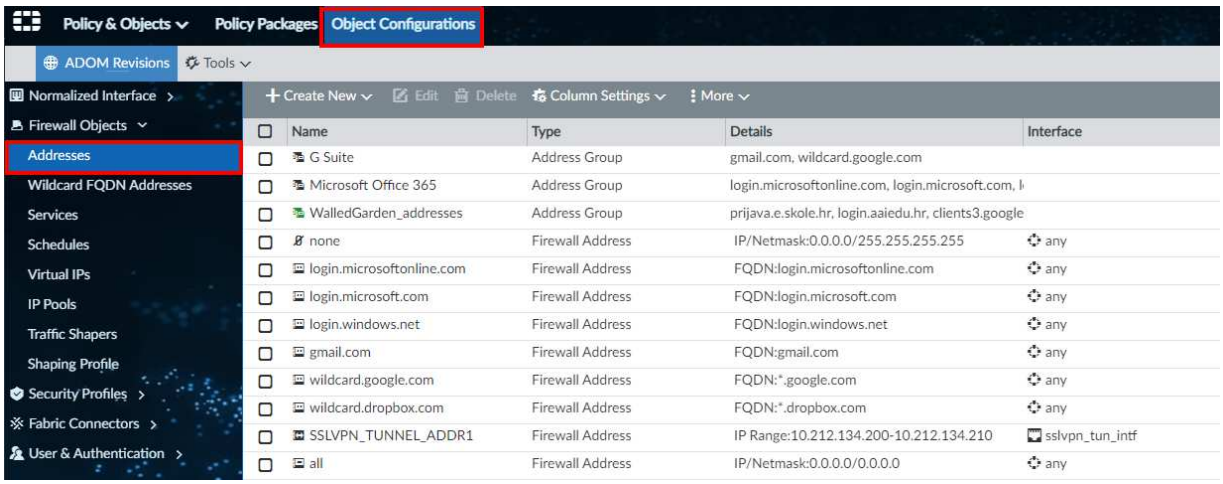
Ovim se korakom završava identifikacija, a ista se informacija koristi u definiranju korisnika.

2) Definiranje korisnika

Nakon identifikacije, korisnika je potrebno definirati u sustavu kako bi ga se u posljednjem koraku moglo uvrstiti u sigurnosno pravilo pristupa resursima.

Navedene se radnje provode tako da se u izborniku pripadajućeg ADOM-a odabire izbornik *Policy & Objects*.

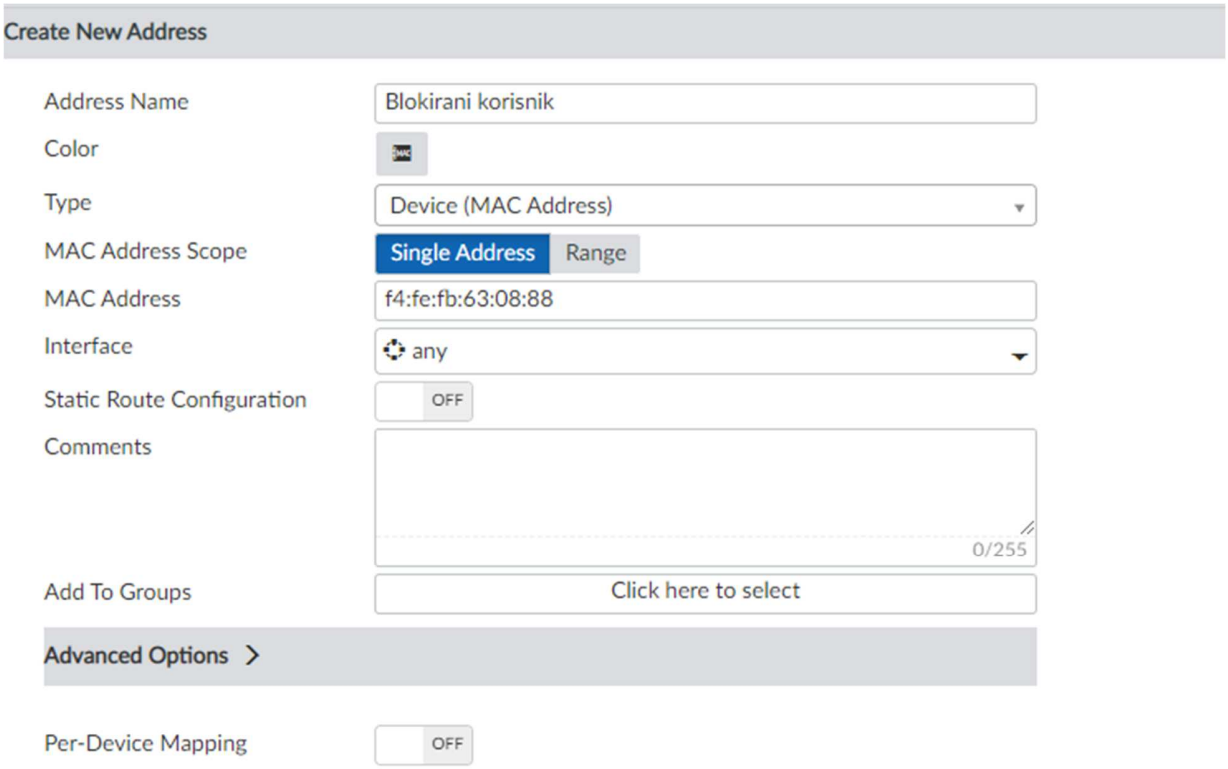
U sljedećem je koraku potrebno odabrati opciju *Object Configurations* i izbornik *Addresses*.



Slika 91: Object Configuration – obrazac za kreiranje novog korisnika

Potrebno je odabrati *Create New* i upisati pripadajuće podatke:

- ***Address name*** – prema vlastitom odabiru, unosi se pojam koji je poveznica na blokiranog korisnika, odnosno uređaj,
- ***Type*** – tip adrese – odabire se *MAC Address* ,
- ***MAC Address*** – upisuje se adresa uređaja koji se dodaje na listu blokiranih.



Slika 92: Addresses – obrazac za kreiranje nove adrese

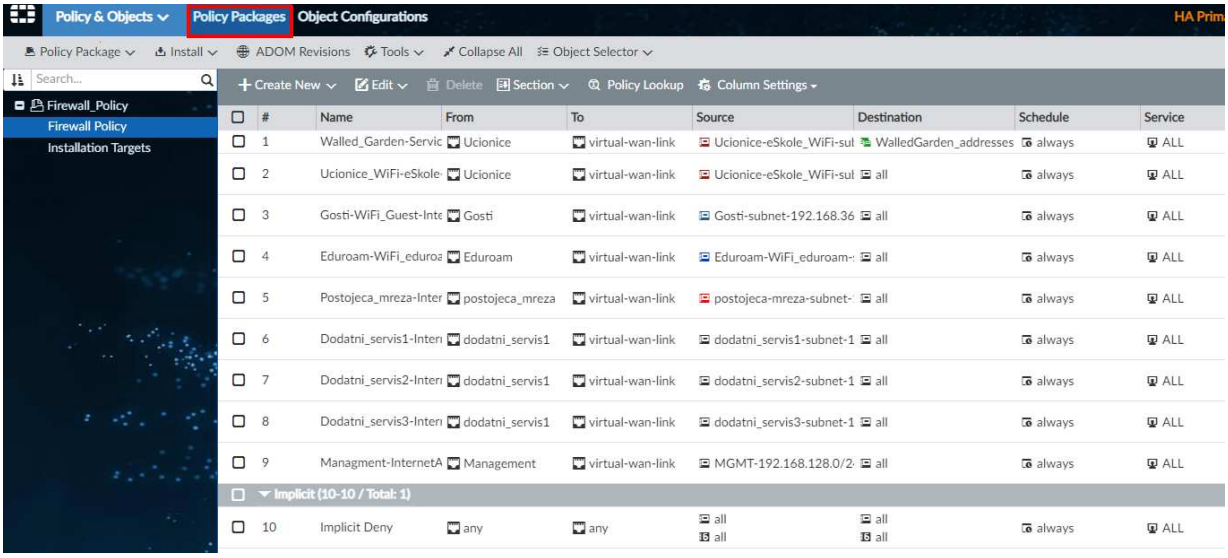
3) Dodavanje korisnika u dedicirano sigurnosno pravilo za zabranu pristupa resursima

Nakon što je definiran, korisnik se dodaje u sigurnosno pravilo pristupa resursima tako što se upotrebljava kao *source* segment, a resurs zabrane pristupa kao *destination*.

Za implementaciju mehanizma, potrebno je dodati sigurnosno pravilo pristupa na niže opisani način.

Potrebno je odabrati izbornik *Policy & Objects* iz pripadajućeg ADOM-a.

U nastavku je potrebno odabrati izbornik *Policy Packages.*

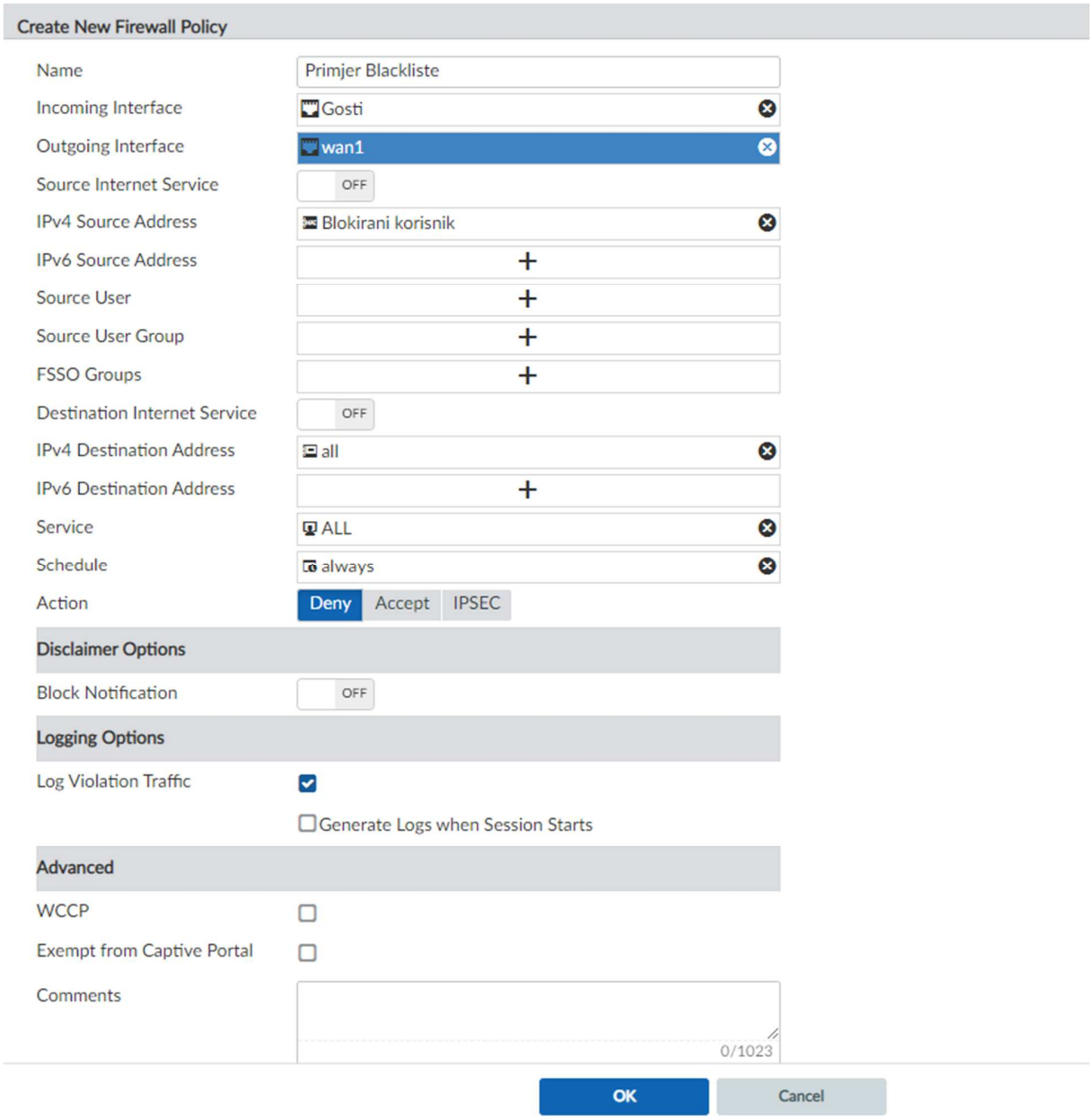


Slika 93: Policy Packages – obrazac za kreiranje novog sigurnosnog pravila

Za kreiranje sigurnosnog pravila, potrebno je odabrati opciju *Create New* koja dovodi do unosa parametara pravila pristupa:

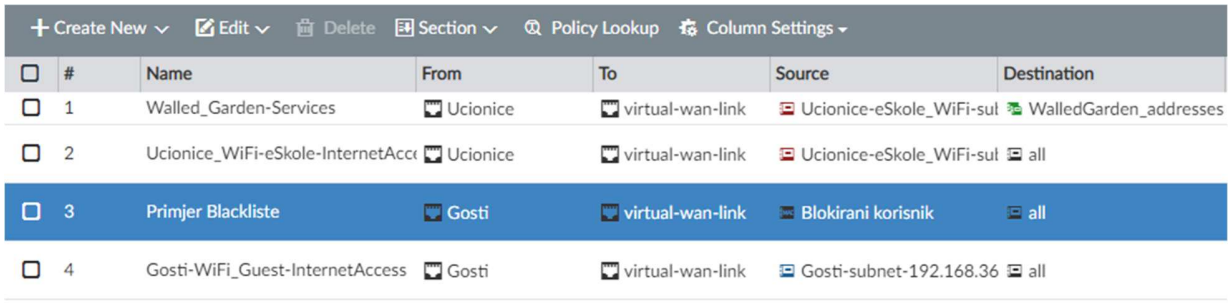
- ***Name*** – tekstualni opis koji upućuje na ulogu dodijeljenog pravila pristupa, postavlja se prema vlastitom izboru,
- ***Incoming Interface*** – segment mreže u kojoj se korisnik nalazi, a u ovom se slučaju radi o WiFi mreži *Gost* pa se stavlja segment VLAN *Gosti*,
- ***Outgoing interface*** – segment mreže na koji se definiranom korisniku brani pristup, a u ovom se slučaju radi o internetskom sučelju (wan1),
- ***IPv4 Source Address*** – MAC adresa, odnosno naziv ranije definiranog korisnika kojem se brani pristup mrežnim resursima, a u ovom se slučaju radi o internetskom sučelju,
- ***Action*** – potrebno je odabrati opciju *Deny* kao akciju potvrde zabrane pristupa sadržajima na internetu.

Na kraju, odabirom opcije *OK* potvrđuje se definiranje zabrane pristupa resursima putem sigurnosnih pravila pristupa.



Slika 94: Prikaz kreiranja novog sigurnosnog pravila pristupa

Novo kreirano pravilo mora biti iznad pravila dozvole pristupa resursima s istih segmenata mreže zbog hijerarhijske strukture sigurnosnih pravila pristupa na vatrozidu i logike kod primjene pravila.



Slika 95: Prikaz kreiranog sigurnosnog pravila pristupa

Posljednji je korak instalacija novih sigurnosnih zapisa. U izborniku je potrebno odabrati *Install* i zatim *Install Wizard.* Sljedeći korak je odabir opcije *Install Policy & Device Settings* i zatim, pod opcijom *Policy Package,* odabir politike vatrozida unutar koje je kreirano sigurnosno pravilo za zabranu pristupa resursima.

6.5.11 Postavljanje korisnika na listu bez ograničenja (*whitelist*)

Korisnici dodani na ovu listu izuzeti su od ograničenja kao što su ograničenje brzine prijenosa podataka i autentikacija putem zaštitnog portala (engl. *Captive portal*). Ova je lista namijenjena prvenstveno za spajanje pametnih ploča, pisača i uređaja koji nemaju mogućnost spajanja unosom korisničkog imena i lozinke iz sustava AAI@EduHr.

Korisnika je na ovu listu najbolje dodati pomoću MAC adrese jer se podaci o IP adresama dodjeljuju dinamičkim putem – servisom DHCP. Na taj način postoji mogućnost da se isti korisnik neće predstavljati na mreži svaki put istom IP adresom.

Postupak dodavanja pristupa korisnika pomoću MAC adrese podijeljen je u tri osnovna koraka:

1. identifikacija korisnika
2. definiranje korisnika
3. dodavanje korisnika u sigurnosno pravilo za dozvolu pristupa.

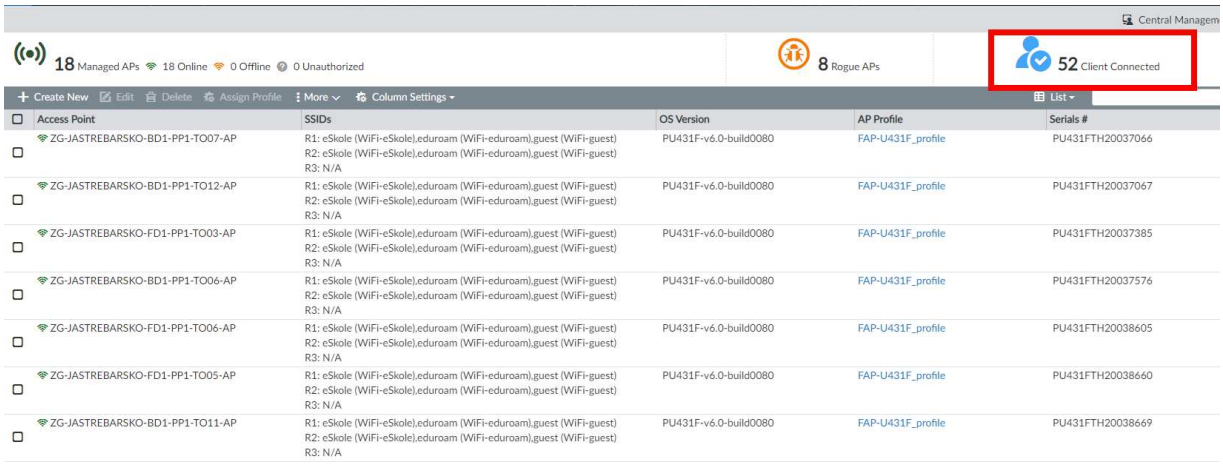
U nastavku su objašnjeni navedeni koraci.

1) Identifikacija korisnika

Identifikacija korisnika provodi se na više načina: fizičkim pristupom uređaju koji se blokira, skeniranjem mreže pomoću jednog od raspoloživih komercijalnih softverskih rješenja i mehanizmima koji stoje na raspolaganju kao dio integralnog rješenja za upravljanje i analizu – FortiManager, odnosno FortiAnalyzer.

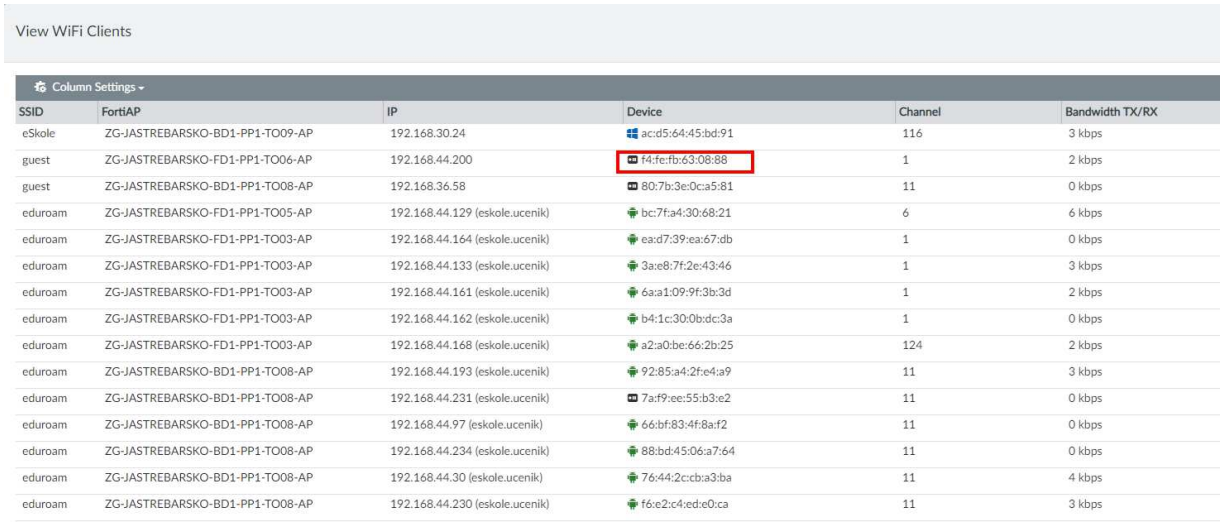
Prvi je korak odabir izbornika *AP Manager* iz pripadajućeg ADOM-a vezanog uz administraciju pripadajuće škole.

U izborniku su vidljive trenutne bežične pristupne točke definirane i autorizirane u sustavu, kao i broj spojenih korisnika.



Slika 96: Prikaz bežične infrastrukture i broj spojenih korisnika

Odabirom korisnika, prikazuje se više detalja o njemu, uključujući MAC adresu koja je potrebna za njegovu identifikaciju.



Slika 97: Popis korisnika bežične mreže i pripadajuće adrese

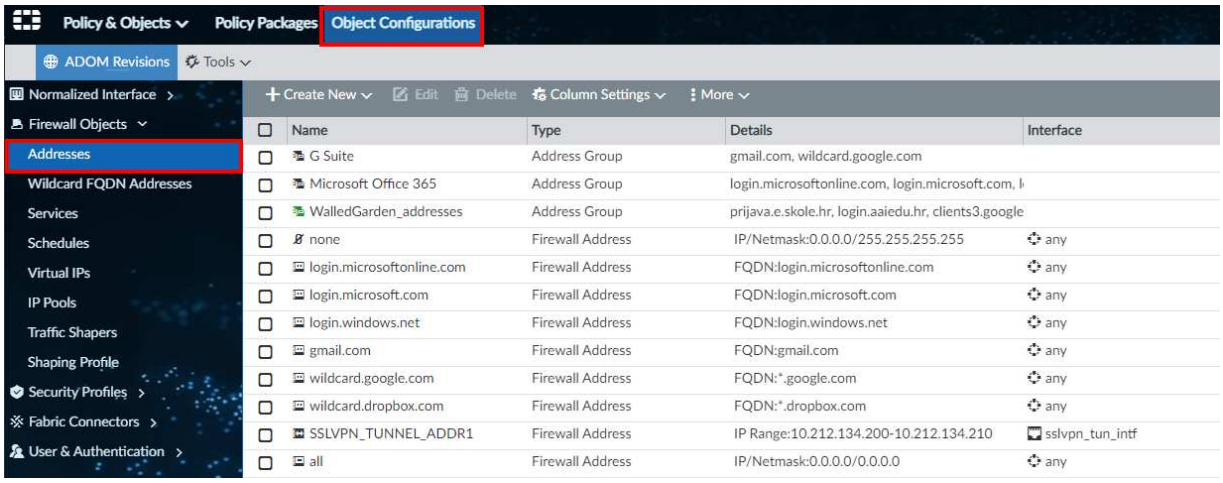
Ovim je korakom završena identifikacija, a ista se informacija koristi u sljedećem koraku.

2) Definiranje korisnika

Nakon identifikacije, korisnika je potrebno definirati u sustavu kako bi ga se u posljednjem koraku moglo uvrstiti u sigurnosno pravilo pristupa resursima.

Navedene se radnje provode tako da se u izborniku pripadajućeg ADOM-a odabire izbornik *Policy & Objects*.

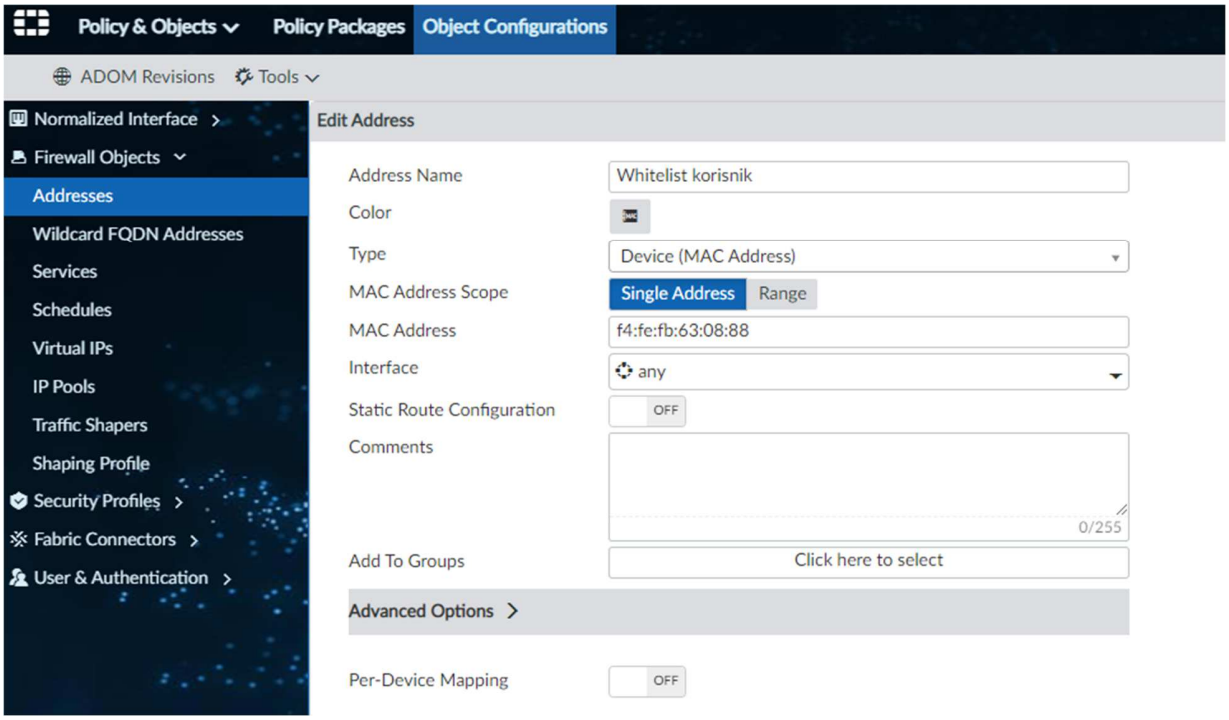
U sljedećem se koraku odabire podizbornik *Object Configurations* i izbornik *Addresses.*



Slika 98: Object Configuration – obrazac za kreiranje novog korisnika

Potrebno je odabrati *Create New* i upisati pripadajuće podatke:

- ***Address name*** – prema vlastitom odabiru, unosi se pojam koji je poveznica na korisnika uređaj kojem treba dopustiti pristup određenom sadržaju.
- ***Type*** – tip adrese – odabire se *MAC Address* i upisuje adresa uređaja koji se dodaje na listu bez ograničenja.



Slika 99: Izbornik Addresses – kreiranje korisnika na listi bez ograničenja

3) Dodavanje korisnika u sigurnosno pravilo za dozvolu pristupa

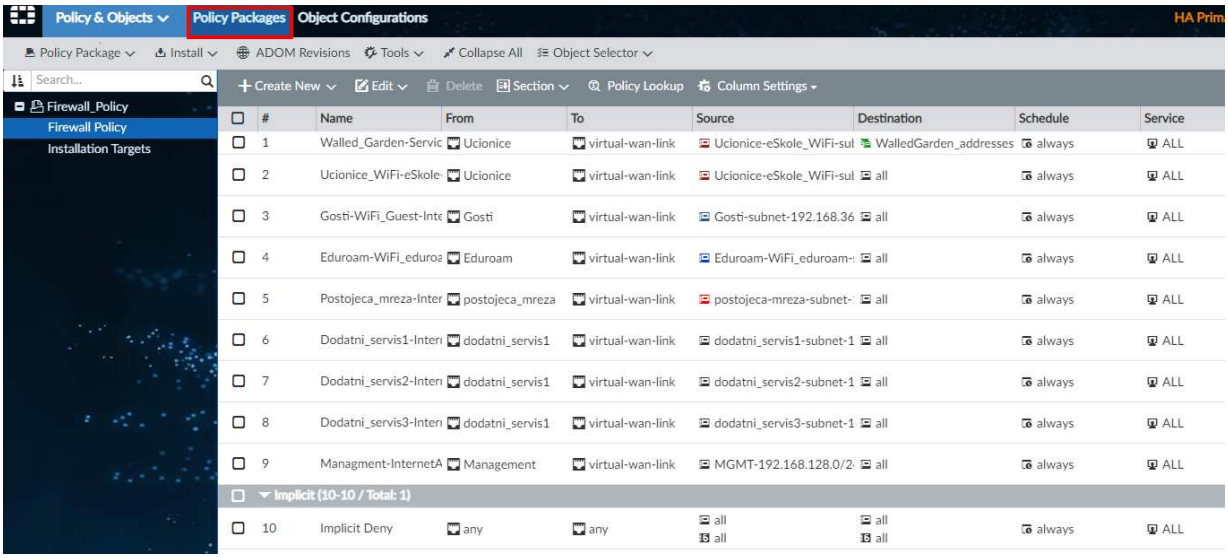
Nakon što je korisnik definiran, potrebno ga je dodati u sigurnosno pravilo pristupa resursima.

Sustav liste bez ograničenja (*whitelist*) koncipiran je tako da se definirani korisnik dodaje u sigurnosno pravilo pristupa resursima tako da se koristi kao *source* segment, a resurs dozvole pristupa kao *destination*.

Za implementaciju mehanizma, potrebno je dodati sigurnosno pravilo pristupa na niže opisani način.

Odabire se izbornik *Policy & Objects* iz pripadajućeg ADOM-a.

U nastavku je potrebno odabrati izbornik *Policy Packages*.

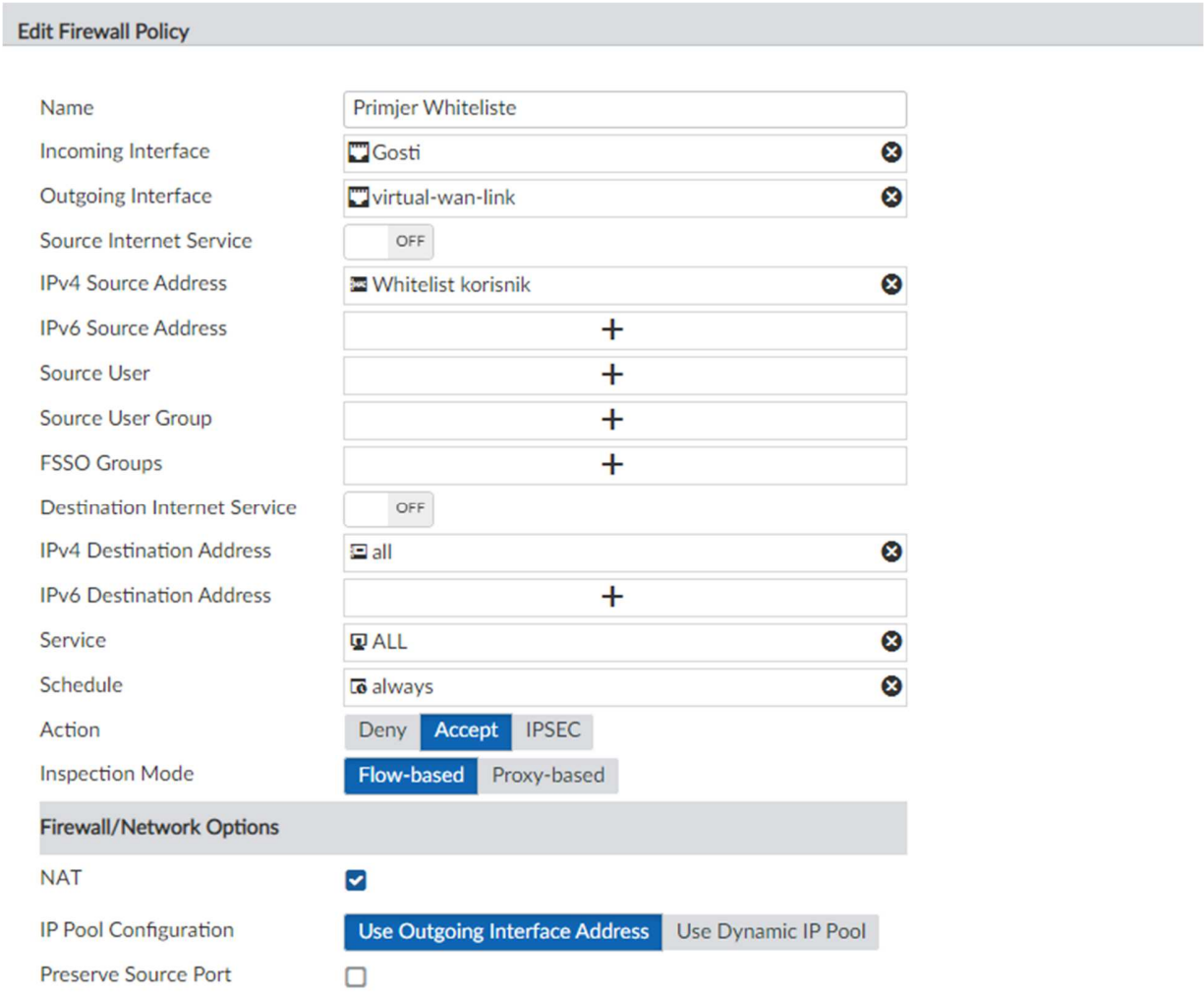


Slika 100: Policy Packages – obrazac za kreiranje novog sigurnosnog pravila

Za kreiranje sigurnosnog pravila, potrebno je odabrati opciju *Create New* koja dovodi do unosa parametara pravila pristupa:

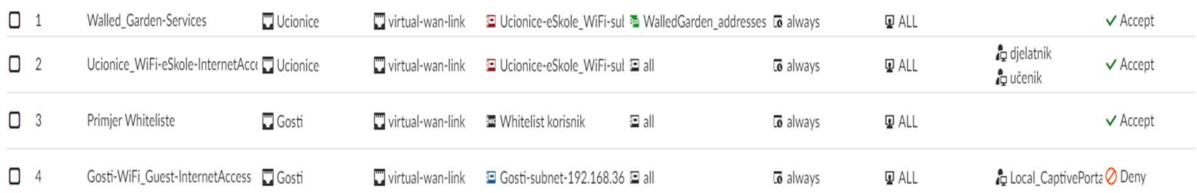
- ***Name*** – tekstualni opis koji upućuje na ulogu dodijeljenog pravila pristupa, a postavlja se prema vlastitom izboru,
- ***Incoming Interface*** – segment mreže u kojoj se korisnik nalazi, a u ovom se slučaju radi o WiFi mreži *Gost*, stoga se stavlja segment VLAN *Gosti*,
- ***Outgoing interface*** – segment mreže na koji se definiranom korisniku dozvoljava pristup, a u ovom se slučaju radi o internetskom sučelju (wan1),
- ***IPv4 Source Address*** – MAC adresa, odnosno naziv ranije definiranog korisnika kojem se dozvoljava pristup mrežnim resursima, a u ovom se slučaju radi o internetskom sučelju,
- ***Action*** – potrebno je odabrati opciju *Allow* kao akciju potvrde dozvole pristupa sadržajima na internetu,
- ***NAT*** – s obzirom na model implementacije, odabire se opcija NAT jer se radi o dozvoli pristupa sadržaju na internetu.

Na kraju, odabirom opcije *OK* potvrđuje se definiranje dozvole pristupa resursima putem sigurnosnih pravila pristupa.



Slika 101: Prikaz kreiranja novog sigurnosnog pravila pristupa

Novo kreirano pravilo mora biti iznad pravila dozvole pristupa resursima s istih segmenata mreže zbog hijerarhijske strukture sigurnosnih pravila pristupa na vatrozidu i logike kod primjene pravila.



Slika 102: Nova sigurnosna pravila pristupa

Posljednji je korak instalacija novih sigurnosnih zapisa. U izborniku je potrebno odabrati *Install* i zatim *Install Wizard.* Sljedeći korak je odabir opcije *Install Policy & Device Settings* i zatim, pod opcijom *Policy Package,* odabir politike vatrozida unutar koje je kreirano sigurnosno pravilo za zabranu pristupa resursima.

6.5.12 Dodavanje novog sigurnosnog pravila pristupa resursima

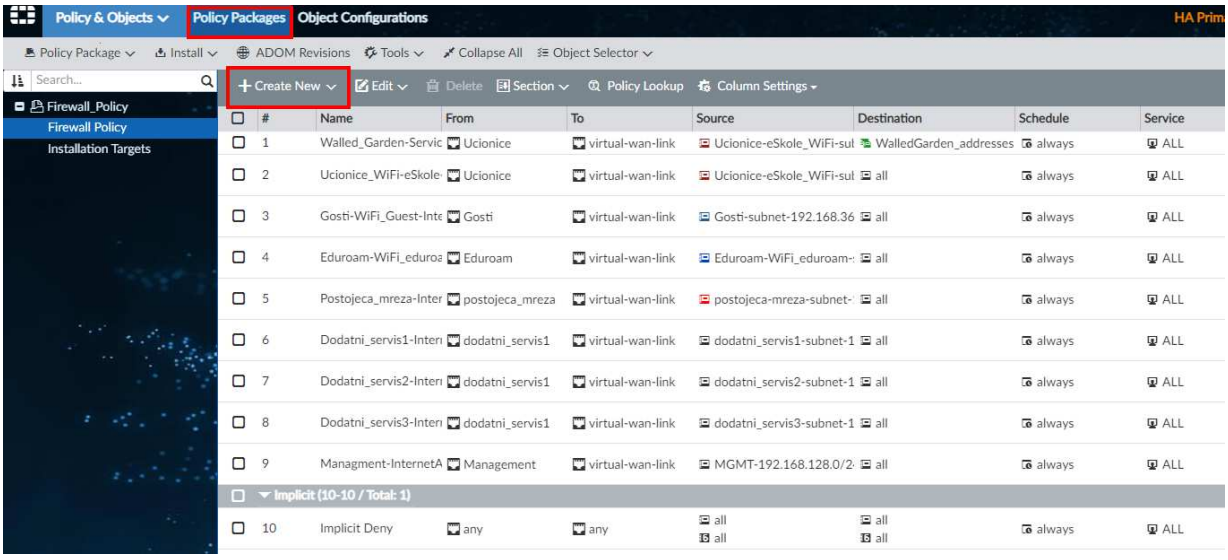
Dodavanje novog sigurnosnog pravila pristupa resursima bazirano je na konceptu definiranja segmenta s kojeg se propušta, odnosno na koji se propušta promet, pritom koristeći opciju NAT.

Mrežni servis NAT (engl. *Network Address Translation*) postupak je pretvaranja IP adrese koja se upotrebljava u jednoj mreži u IP adresu koja se upotrebljava u drugoj mreži. Jedna se mreža naziva unutrašnja, a druga vanjska. NAT se najčešće primjenjuje u okruženjima kada jednu mrežu preko mrežnog prolaza treba spojiti s drugom mrežom kada se adrese iz unutrašnje (lokalne) mreže preslikavaju na jednu ili više vanjskih (globalnih) IP adresa.

Jedna od najčešćih primjena takvog pravila jest definiranje pristupa internetu s unutrašnjih resursa, odnosno segmenta mreže.

Prvi korak u definiranju pravila NAT jest odabir izbornika *Policy & Objects* unutar pripadajućeg ADOM-a.

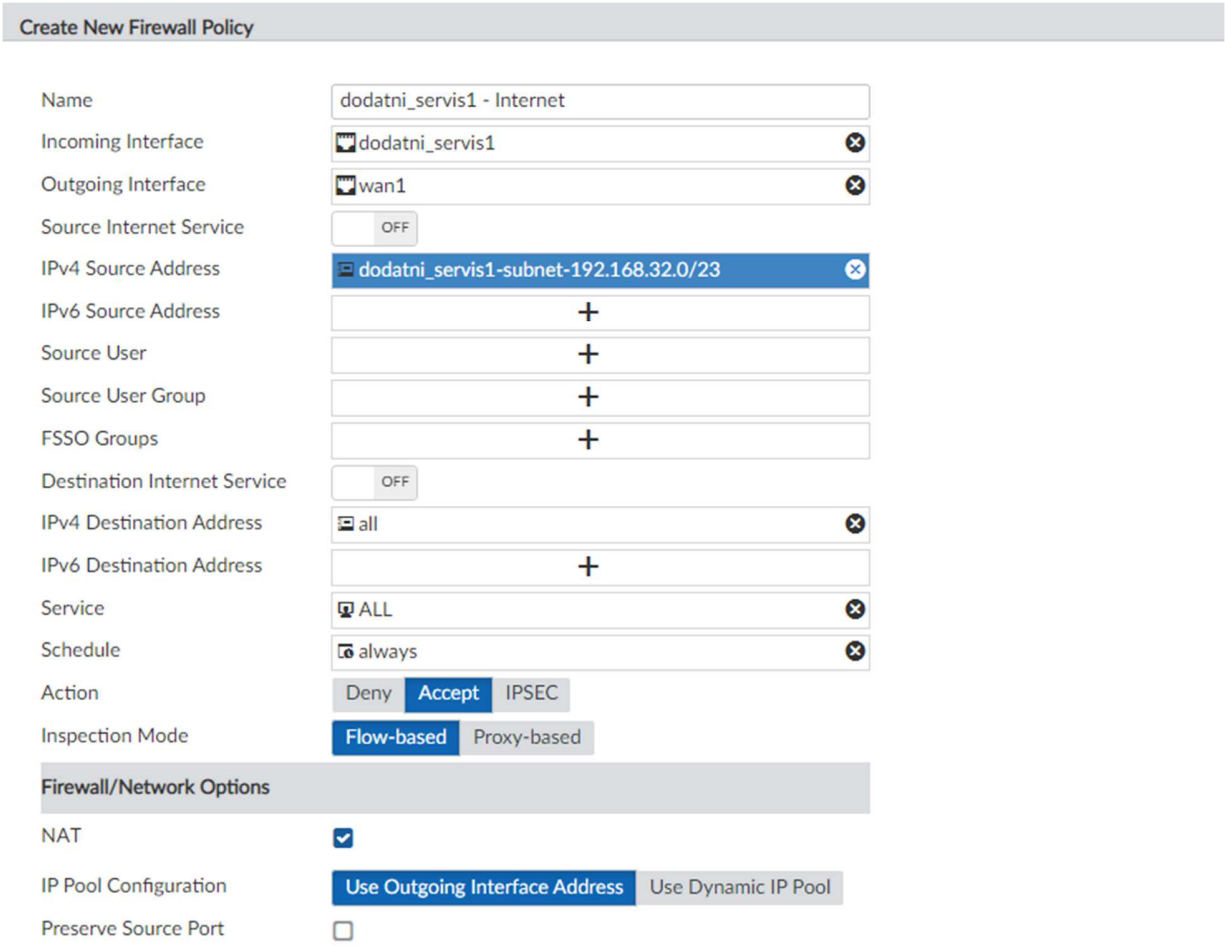
U nastavku je potrebno odabrati izbornik *Policy Packages* i *Create New.*



Slika 103: Izbornik Policy & Objects – obrazac za kreiranje novog sigurnosnog pravila

Potom se otvara izbornik za kreiranje novog pravila pristupa i zadana se polja popunjavaju na sljedeći način:

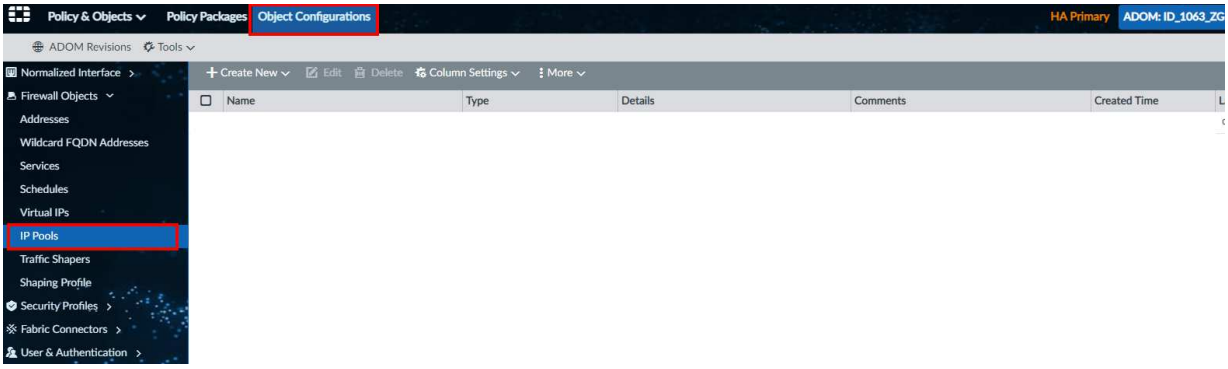
- ***Name*** – tekstualni opis koji upućuje na ulogu dodijeljenog pravila pristupa, postavlja se prema vlastitom izboru,
- ***Incoming Interface*** – mrežni segment s kojeg se propušta promet prema odredištu, a u ovom se primjeru primjenjuje dodatni servis1,
- ***Outgoing Interface*** – mrežno odredište prema kojem se propušta promet, a u ovom se slučaju primjenjuje internet (wan1)
- ***IPv4 Source Address*** – mrežni raspon adresa s kojeg se propušta mrežni promet. Ovaj je parametar najčešće u korelaciji s parametrom *Incoming Interface*,
- ***IPv4 Destination Address*** – mrežni raspon adresa na strani odredišta, a u ovom se slučaju odabire se opcija *All* jer se radi o strani interneta,
- ***Action*** – s obzirom na to da je namjera dozvoljavanje prometa, odabire se opcija *Accept*,
- ***NAT*** – uključenjem opcije *NAT* i *Use Outgoing Interface Address*, s interne se mreže prema internetu predstavlja javnom adresom definiranom na sučelju WAN1.



Slika 104: Prikaz kreiranja novog sigurnosnog pravila pristupa

Dodatna opcija *Use Dynamic Pool* daje mogućnost upotrebe drugog raspona adresa koji je ranije definiran na niže navedeni način.

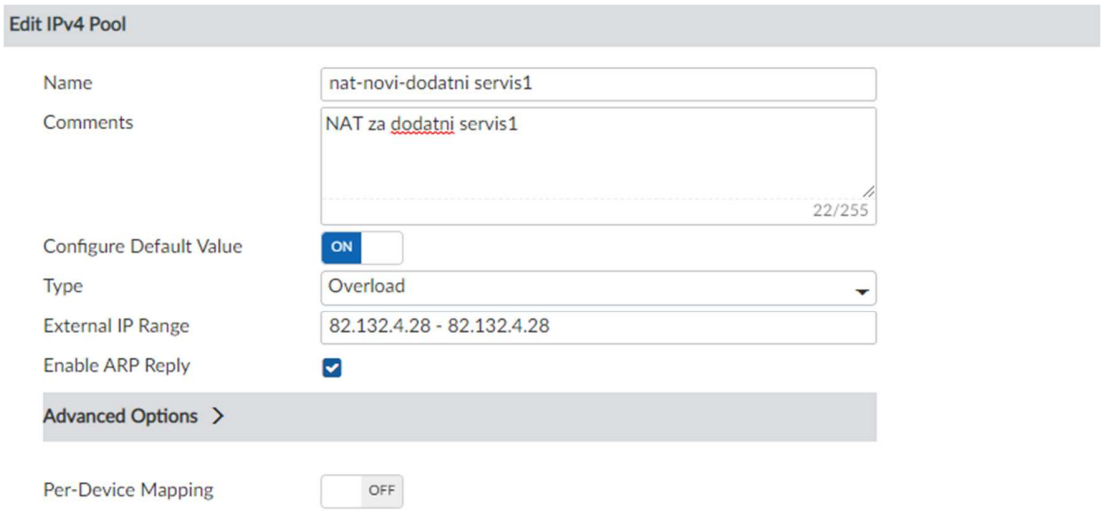
U izborniku *Policy & Objects* potrebno je odabrati opciju *Object Configurations*, potom *IP pools* i *Create New.*



Slika 105: IP Pool – obrazac za kreiranje novog raspona IP adresa

U obrascu za kreiranje novog raspona IP adresa upisuju se sljedeći podaci:

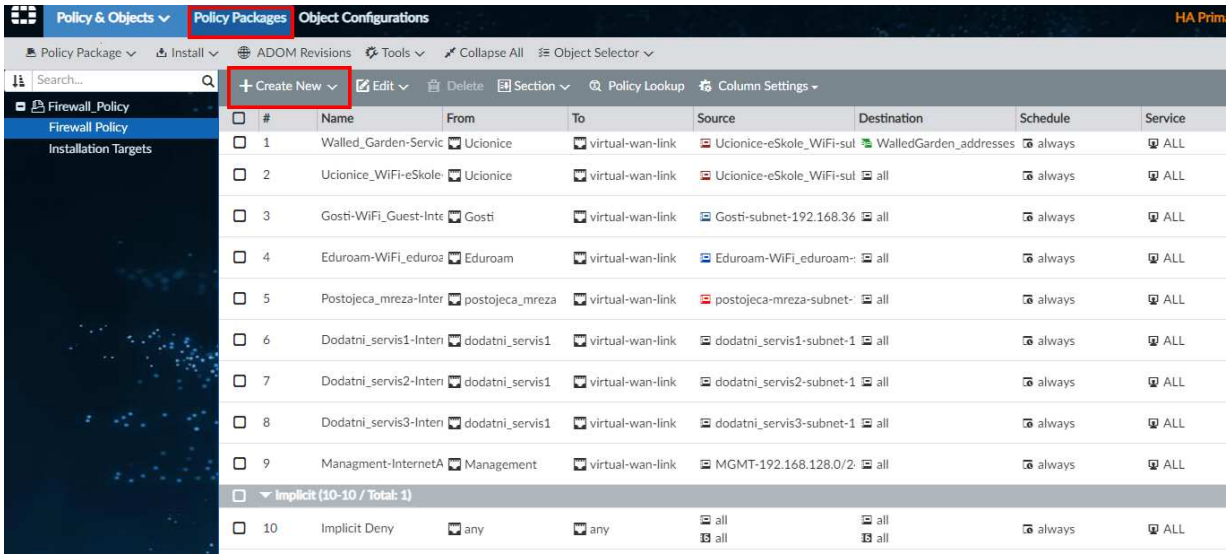
- ***Name*** – tekstualni opis koji upućuje na ulogu dediciranog servisa NAT, a postavlja se prema vlastitom izboru,
- ***Comments*** – tekstualni opis koji upućuje na ulogu dediciranog servisa NAT, a postavlja se prema vlastitom izboru,
- ***Type*** – *Overload*,
- ***External IP Range*** – definira se adresni raspon koji se želi upotrijebiti kod prezentacije jednog IP segmenta prema drugom.



Slika 106: Novi raspon IP adresa za potrebe NAT-a

Nakon definiranja novog raspona adresa, te je adrese potrebno primijeniti u sigurnosnom pravilu pristupa. Za primjer se koristi pravilo kao kod definiranja osnovnog NAT-a.

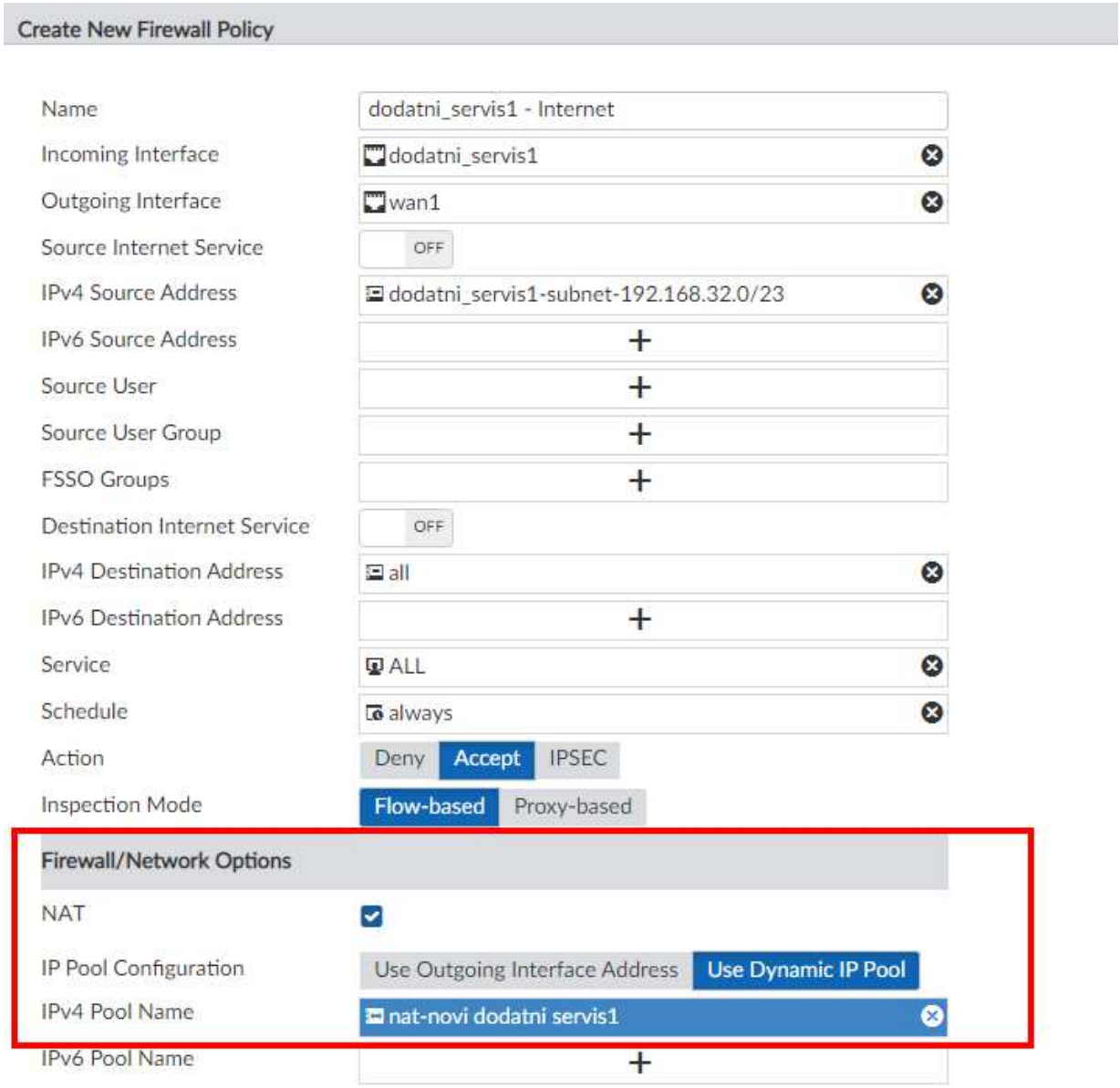
U izborniku *Policy Packages* potrebno je odabrati *Create New*.



Slika 107: Policy Package – obrazac za kreiranje novog sigurnosnog pravila

U obrascu za kreiranje novog sigurnosnog pravila upisuju se sljedeći podaci:

- ***Incoming Interface*** – mrežni segment s kojeg se propušta promet prema odredištu, u ovom se primjeru koristi dodatni servis1,
- ***Outgoing Interface*** – mrežno odredište prema kojem se propušta promet, a u ovom se slučaju primjenjuje internet (wan1),
- ***IPv4 Source Address*** – mrežni raspon adresa s kojeg se propušta mrežni promet. Ovaj je parametar najčešće u korelaciji s parametrom *Incoming Interface*,
- ***IPv4 Destination Address*** – mrežni raspon adresa na strani odredišta. U ovom se slučaju odabire se opcija *All* jer se radi o strani interneta,
- ***Action*** – s obzirom na to da je namjera dozvoljavanje prometa, potrebno je odabrati opciju *Accept*,
- ***NAT*** – uključenjem opcije *NAT* i *Use Dynamic IP Pool*, s interne se mreže prema internetu predstavlja javnom adresom definiranom u prethodnom koraku.



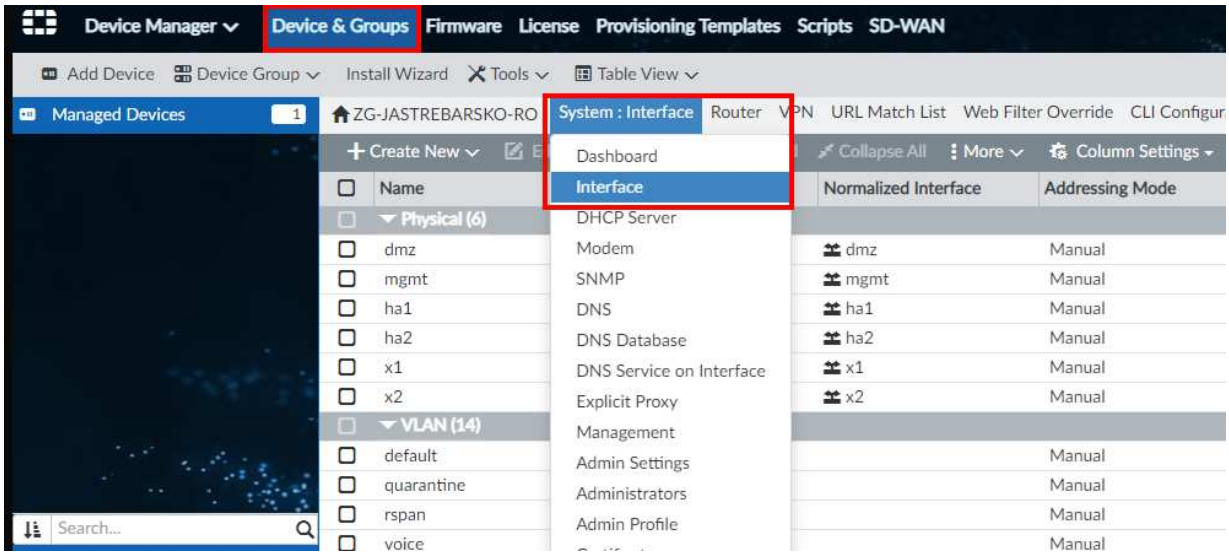
Slika 108: Prikaz odabira novog raspona IP adresa u upotrebi sigurnosnih polica

Posljednji je korak instalacija novih sigurnosnih zapisa. U izborniku je potrebno odabrati *Install* i zatim *Install Wizard.* Sljedeći korak je odabir opcije *Install Policy & Device Settings* i zatim, pod opcijom *Policy Package,* odabir politike vatrozida unutar koje je kreirano sigurnosno pravilo za zabranu pristupa resursima.

6.5.13 Prikaz konfiguracije novog DHCP *poola*

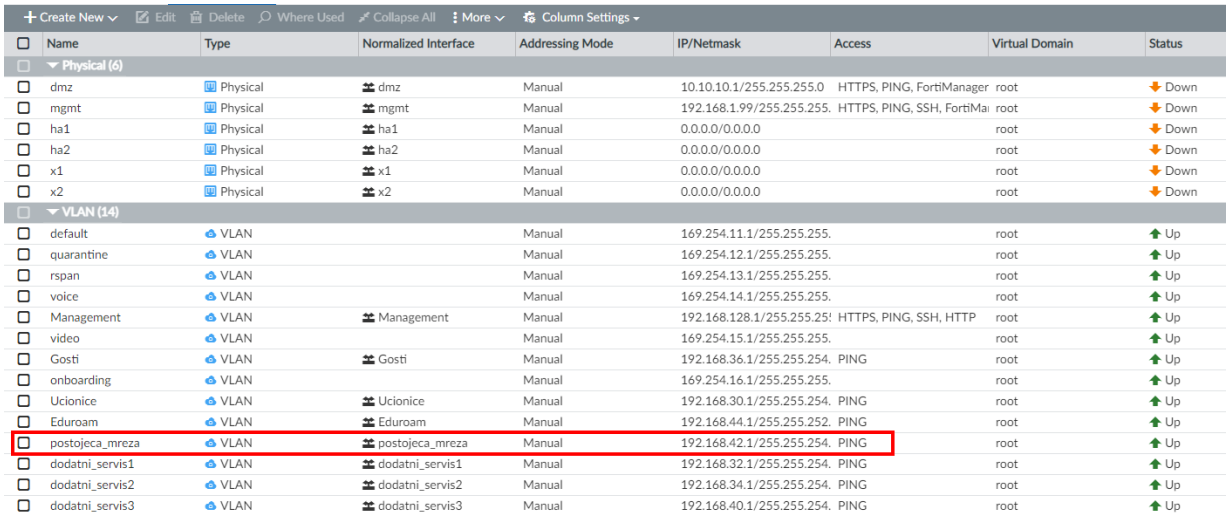
Konfiguracija novog DHCP raspona adresa na usmjerivaču obavlja se kroz centralni sustav za upravljanje i nadzor FortiManager. Prvi je korak prijava u centralni sustav upravljanja FortiManager unosom korisničkog imena i lozinke koje je administrator sustava ranije odredio.

Device Manager / ***Device & Groups*** / ***System:Interface***



Slika 109: System Interface – obrazac za pregled servisa DHCP

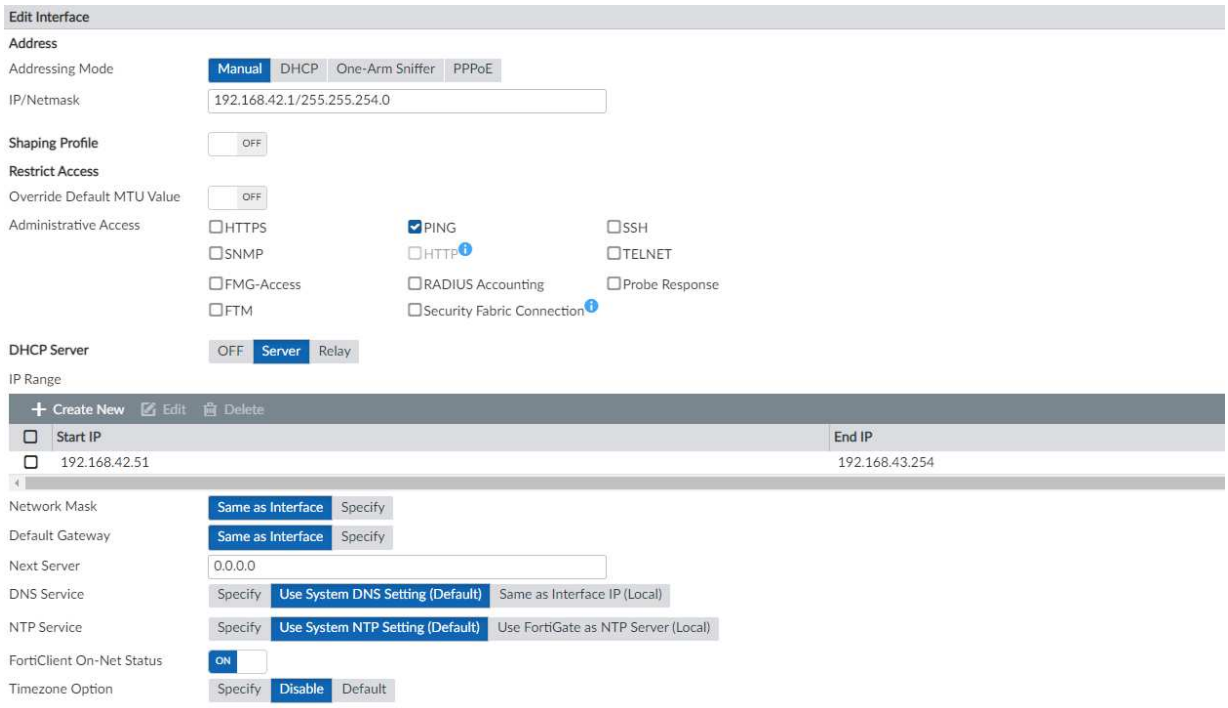
DHCP se definira unutar postavki mrežnog sučelja. Odabrano je sučelje definirano IP adresom 192.168.42.1 i pripadajućom maskom mreže (engl. *Netmask*) 255.255.254.0.



Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access	Virtual Domain	Status
Physical (6)							
dmz	Physical	dmz	Manual	10.10.10.1/255.255.255.0	HTTPS, PING, FortiManager	root	Down
mgmt	Physical	mgmt	Manual	192.168.1.99/255.255.255.	HTTPS, PING, SSH, FortiMa	root	Down
ha1	Physical	ha1	Manual	0.0.0.0/0.0.0.0		root	Down
ha2	Physical	ha2	Manual	0.0.0.0/0.0.0.0		root	Down
x1	Physical	x1	Manual	0.0.0.0/0.0.0.0		root	Down
x2	Physical	x2	Manual	0.0.0.0/0.0.0.0		root	Down
VLAN (14)							
default	VLAN		Manual	169.254.11.1/255.255.255.		root	Up
quarantine	VLAN		Manual	169.254.12.1/255.255.255.		root	Up
rspan	VLAN		Manual	169.254.13.1/255.255.255.		root	Up
voice	VLAN		Manual	169.254.14.1/255.255.255.		root	Up
Management	VLAN	Management	Manual	192.168.128.1/255.255.25!	HTTPS, PING, SSH, HTTP	root	Up
video	VLAN		Manual	169.254.15.1/255.255.255.		root	Up
Gosti	VLAN	Gosti	Manual	192.168.36.1/255.255.254.	PING	root	Up
onboarding	VLAN		Manual	169.254.16.1/255.255.255.		root	Up
Ucionice	VLAN	Ucionice	Manual	192.168.30.1/255.255.254.	PING	root	Up
Eduroam	VLAN	Eduroam	Manual	192.168.44.1/255.255.252.	PING	root	Up
postojeca_mreza	VLAN	postojeca_mreza	Manual	192.168.42.1/255.255.254.	PING	root	Up
dodatni_servis1	VLAN	dodatni_servis1	Manual	192.168.32.1/255.255.254.	PING	root	Up
dodatni_servis2	VLAN	dodatni_servis2	Manual	192.168.34.1/255.255.254.	PING	root	Up
dodatni_servis3	VLAN	dodatni_servis3	Manual	192.168.40.1/255.255.254.	PING	root	Up

Slika 110: Prikaz logičkih sučelja VLAN-ova

Na odabranom je sučelju uključen servis DCHP i definiran raspon adresa koje se dodjeljuju klijentima unutar mrežnog segmenta.



Slika 111: Postavke DHCP servisa

Dodatne opcije nude mogućnosti odabira mrežne maske, zadanog pristupnika i opcija kao što je DNS. DHCP poslužitelj klijentima dodjeljuje IP adrese na unaprijed određeno vrijeme (engl. *Lease Time*) i ukoliko je to vrijeme potrebno produžiti ili skratiti isto se može promijeniti unutar postavki mrežnog sučelja pod *Edit VLAN Definition* te opcijom *Advanced… (DNS, WINS, Custom Options, Exclude Ranges.)*

Parametri su definirani kao vrijednost, odnosno adresa sučelja podmreže jer se usmjeravanje, odnosno manipulacija prometa odvija na vatrozidu kao središnjoj točki sustava.

6.6 Otklanjanje poteškoća na mreži

U ovom su poglavlju opisani postupci koji se primjenjuju kada se pojavi neka poteškoća u radu bežične mreže pa treba snimiti mrežni promet, obaviti pregled detalja bežičnih pristupnih točaka i preklopnika te koristiti *ping* i *cable test* opciju.

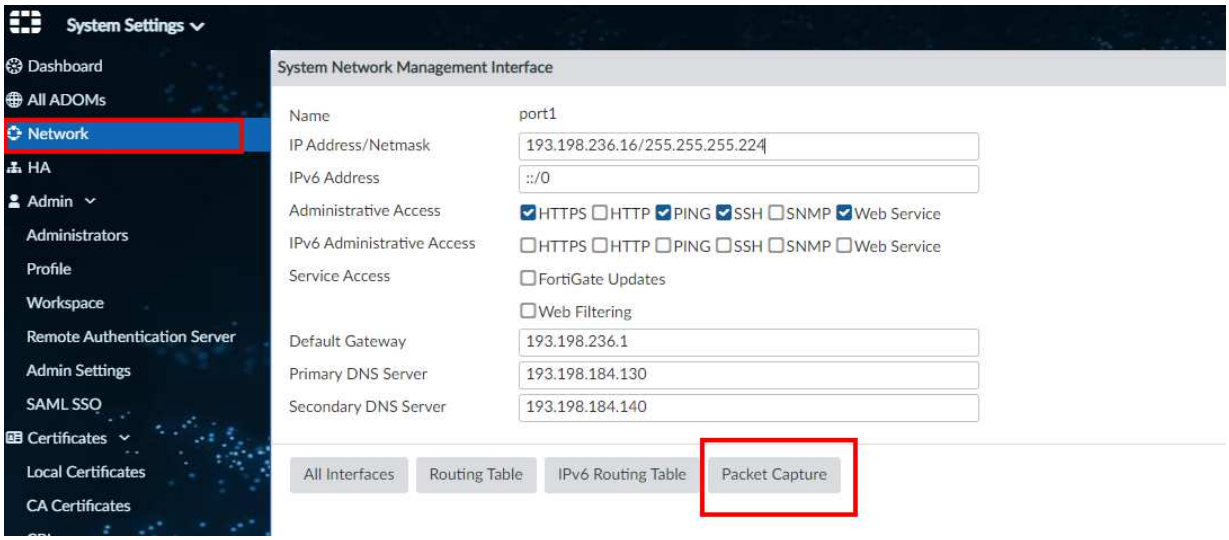
6.6.1 Prikaz snimanja mrežnog prometa

Jedan od alata za otklanjanja poteškoća u radu i funkcioniranju mreže je *Packet capture.*

Svrha *Packet capture* alata je pomoć prilikom dijagnosticiranja i otklanjanja poteškoća na mreži jer navedena opcija omogućuje brzu i detaljnu snimku mrežnog prometa na izabranim sučeljima.

Navedeni je alat sastavni dio integriranog upravljačkog mehanizma FortiManager.

Za pokretanje navedenog mehanizma, potrebno je odabrati izbornik *System Settings* unutar ADOM-a, te zatim izbornik *Network* i opciju *Packet Capture*.

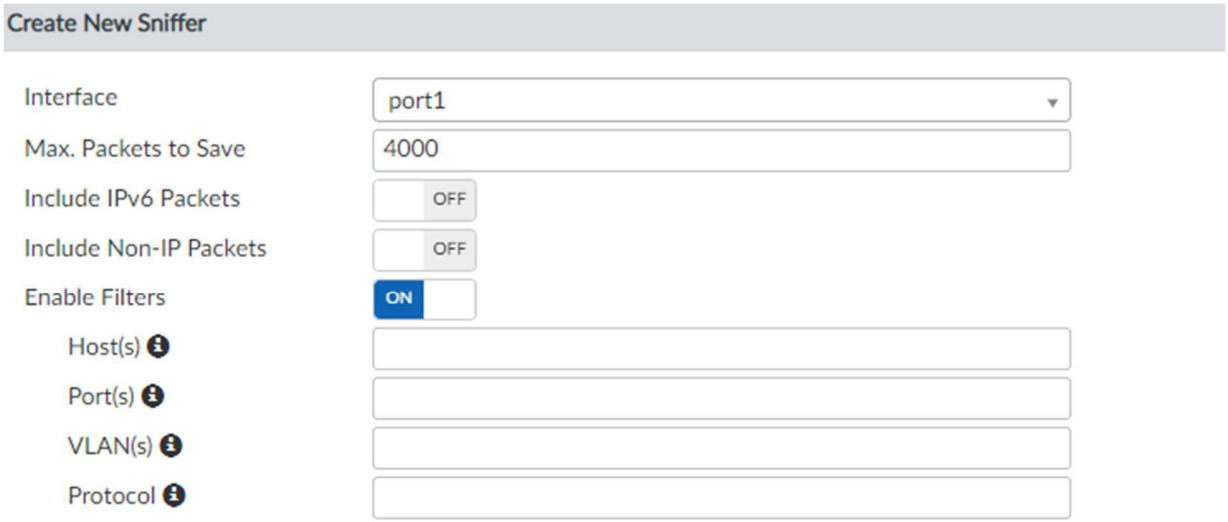


Slika 112: Network – obrazac za pristup mehanizmu Packet Capture

Prilikom kreiranje nove snimke mrežnog prometa, otvaraju se dodatne opcije:

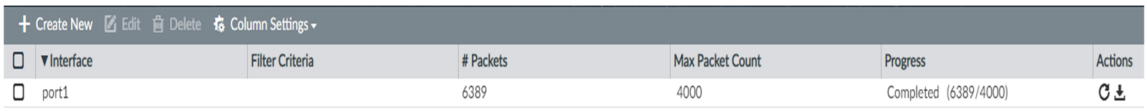
- ***Interface*** – sučelje s kojeg se želi snimati mrežni promet,
- ***Max. Packets to Save*** – broj mrežnih paketa.

Tu su i dodatne opcije, kao što je promet prema određenom *hostu*, promet po određenom portu, VLAN-u i protokolu.



Slika 113: Opcije sučelja na mehanizmu Packet Capture

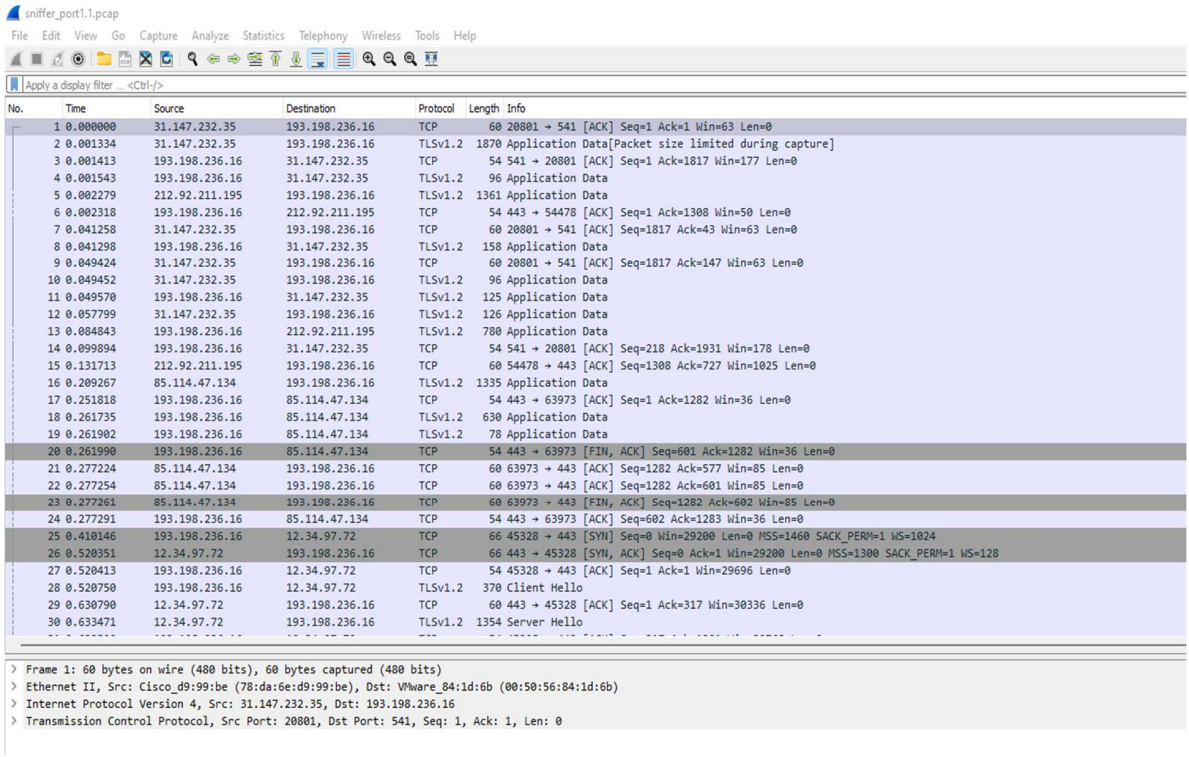
Nakon definiranja parametara za snimku mrežnog prometa na odabranom sučelju, pritiskom na tipku *OK* započinje proces snimanja prometa. Po završetku postupka sustav kreira datoteku u kojoj su sadržane sve informacije i istu je potrebno preuzeti na računalo kako bi se nastavilo s analizom.



Slika 114: Prikaz završetka definiranog mehanizma Packet Capture

Za otvaranje preuzetog zapisa mrežnog prometa, na lokalnom računalu treba imati instaliran softver za analizu preuzetog zapisa, a najčešće se koristi alat *Wireshark.*

Nakon otvaranja datoteke snimljenog mrežnog zapisa u navedenom softverskom rješenju (*Wireshark*), omogućen je detaljni prikaz mrežnog prometa s ranije odabranog sučelja.



Slika 115: Whireshark sučelje – programsko rješenje za analizu

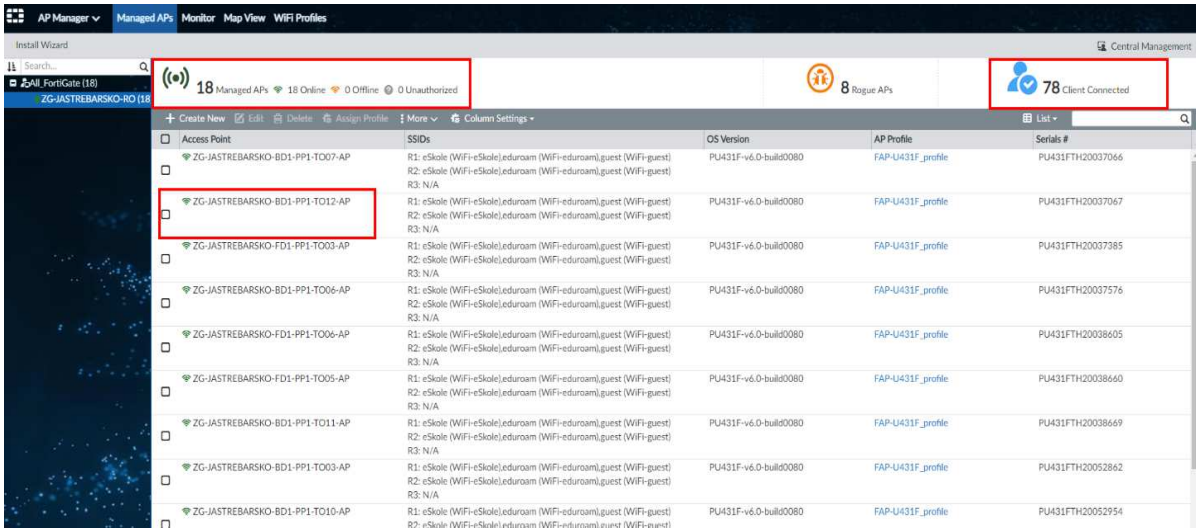
6.6.2 Pregled detalja bežičnih pristupnih točaka

Detaljan nadzor nad bežičnom infrastrukturom, odnosno nad pripadajućim pristupnim točkama, provodi se iz središnjeg sustava za upravljanje FortiManager.

U ADOM-u je potrebno odabrati izbornik *AP Manager*, nakon čega se otvara sučelje za nadzor nad bežičnom pristupnom infrastrukturom.

Početni izbornik *Managed APs* pruža uvid u prijavljene bežične točke na sustav upravljanja, odnosno u njihov status, zajedno s trenutnim brojem spojenih klijenata.

Nakon odabira, prikazuje se stranica s popisom bežičnih pristupnih točaka na lokaciji.



Slika 116: Prikaz bežične infrastrukture i broj spojenih klijenata

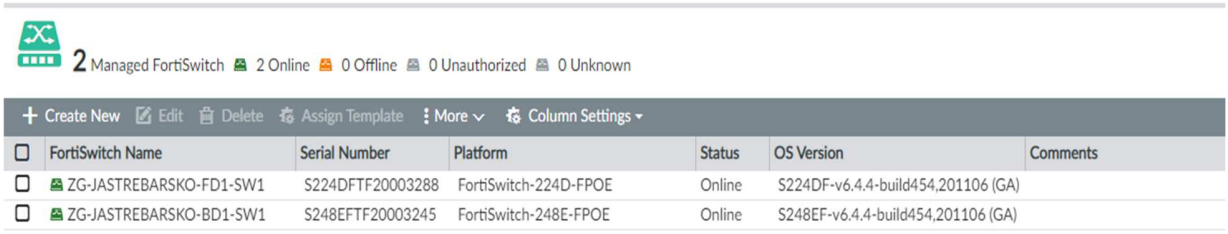
Odabirom određene bežične točke, prikazuju se njezine postavke kao što su status, IP adresa (*Connected Via*), MAC adresa, vrijeme pristupa (*Join Time*), verzija ugrađenog softvera (*Current Firmware*) i dr.

6.6.3 Pregled detalja preklopnika

Detaljan nadzor nad infrastrukturom preklopnika provodi se iz središnjeg sustava za upravljanje FortiManager.

U ADOM-u je potrebno odabrati izbornik *FortiSwitch Manager*, nakon čega se otvara sučelje za nadzor nad integriranim preklopnicima.

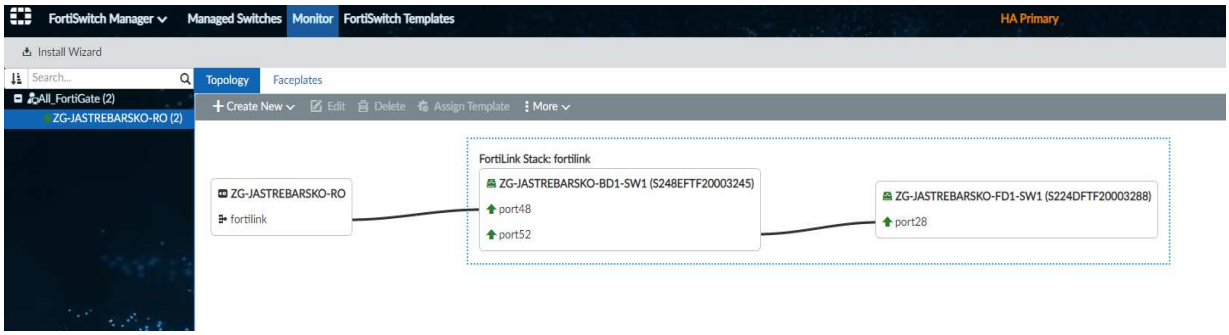
Početni zaslon izbornika pruža prikaz prijavljenih preklopnika na sustav upravljanja, odnosno detalje kao što su naziv preklopnika, serijski broj, model, verzija softvera i dr.



Slika 117: Prikaz prijavljenih preklopnika na sustav

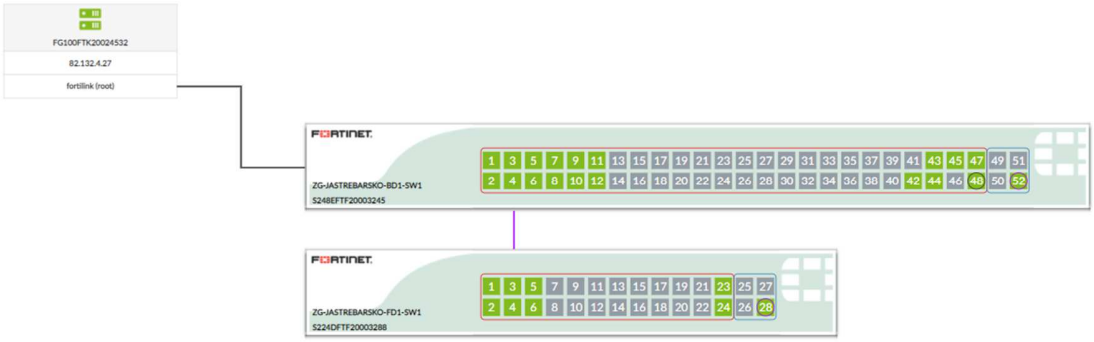
Izbornik *Monitor* nudi opcije *Topology* i *Faceplates.*

Odabirom opcije *Topology* omogućava se uvida u topologiju sustava, odnosno pregled detalja sučelja koje uređaji upotrebljavaju za međusobno povezivanje.



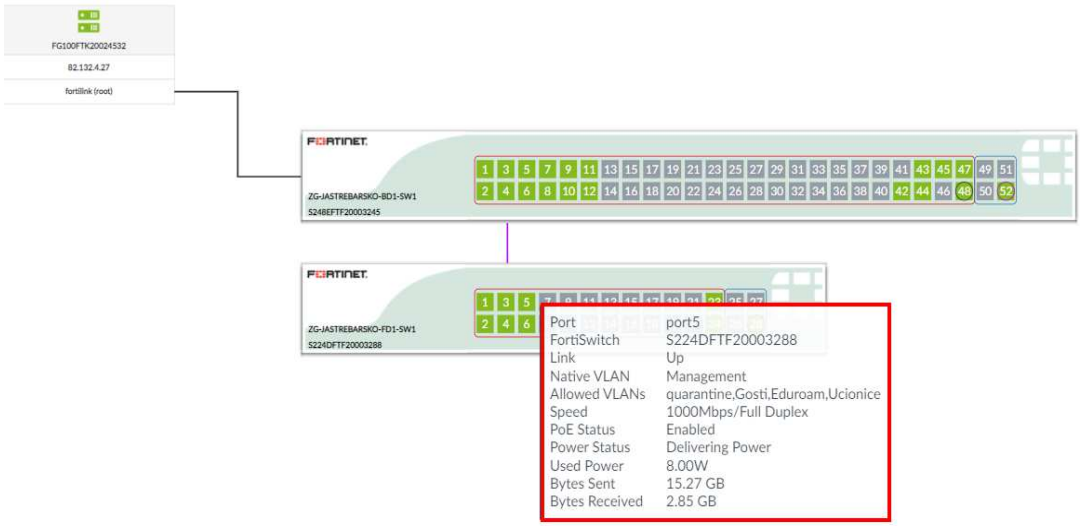
Slika 118: Izbornik Topology – prikaz topologije sustava

Odabirom opcije *Faceplates* omogućava se prikaza preklopnika kod kojeg je prikazan točan raspored zauzetosti sučelja na pojedinom preklopniku.



Slika 119: Izbornik Faceplates – prikaz naličja i sučelja preklopnika

Pozicioniranjem kursora miša preko određenog sučelja prikazuju se informacije o dodatnim detaljima na određenom sučelju.



Slika 120: Izbornik Faceplates – detalj sučelja

6.6.4 Korištenje opcija *ping* i *cable test*

U ovom se poglavlju opisuje način provjere dostupnost raznih IP adresa, prikupljanje informacija, kao i ispitivanje kabela.

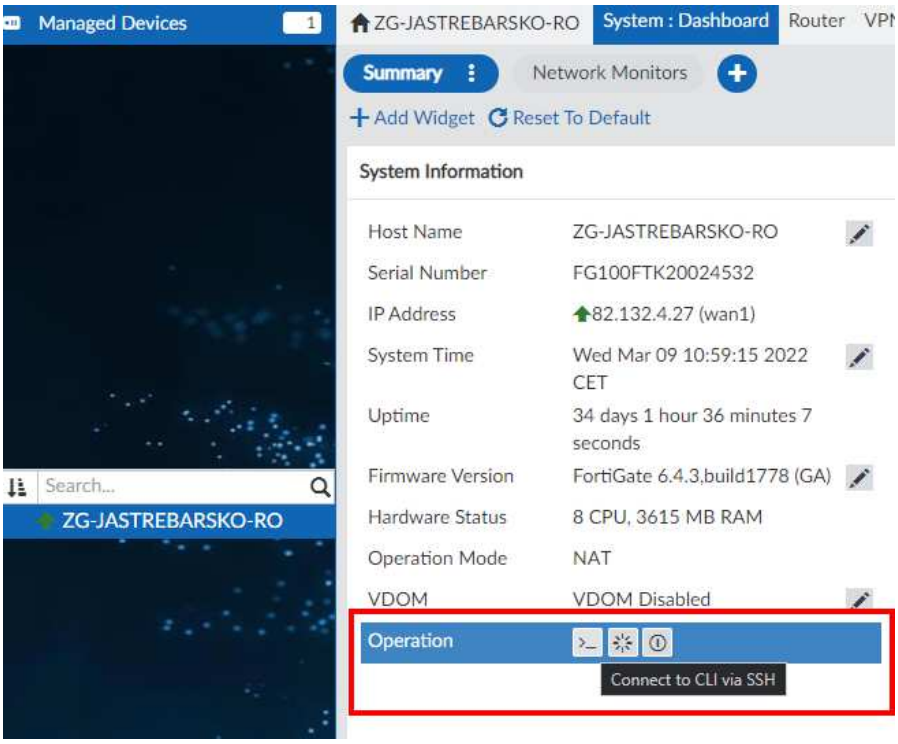
Osnovni koraci u otklanjanju poteškoća su upotreba alata *ping* i opcije *cable test* na usmjerivaču.

Alatom *ping* provjerava se dostupnost javnih IP adresa, privatnih IP adresa žičnih i bežičnih korisnika te dostupnosti internetske adrese.

Primjenom alata *ping* dobivaju se informacije o postotku izgubljenih paketa i latenciji prema resursu čija se dostupnost provjerava.

Alat *ping* dostupan je iz kontrolne ploče (engl. *Dashboard*) sučelja usmjerivača inalazi se u izborniku *Device Manager*.

Nakon odabira izbornika *Device Manager*, otvara se kontrolna ploča gdje se nudi opcija spajanja na usmjerivač preko protokola SSH.



Slika 121: System Dashboard – pristup konzoli SSH

Za prijavu na usmjerivač preko protokola SSH, potrebno je upisati vjerodajnice ranije definirane u sustavu upravljanja.

Za uspješno korištenje mehanizma *ping,* potrebna je informacija o IP adresi uređaja prema kojem se ispituje mrežna povezanost.

Sintaksa koja se koristi u klijentu SSH je „*execute ping x.x.x.x*“, pri čemu „*x.x.x.x*“ predstavlja IP adresu uređaja prema kojem se ispituje mrežna povezanost protokolom ICMP (engl. *Internet Control Message Protocol).*

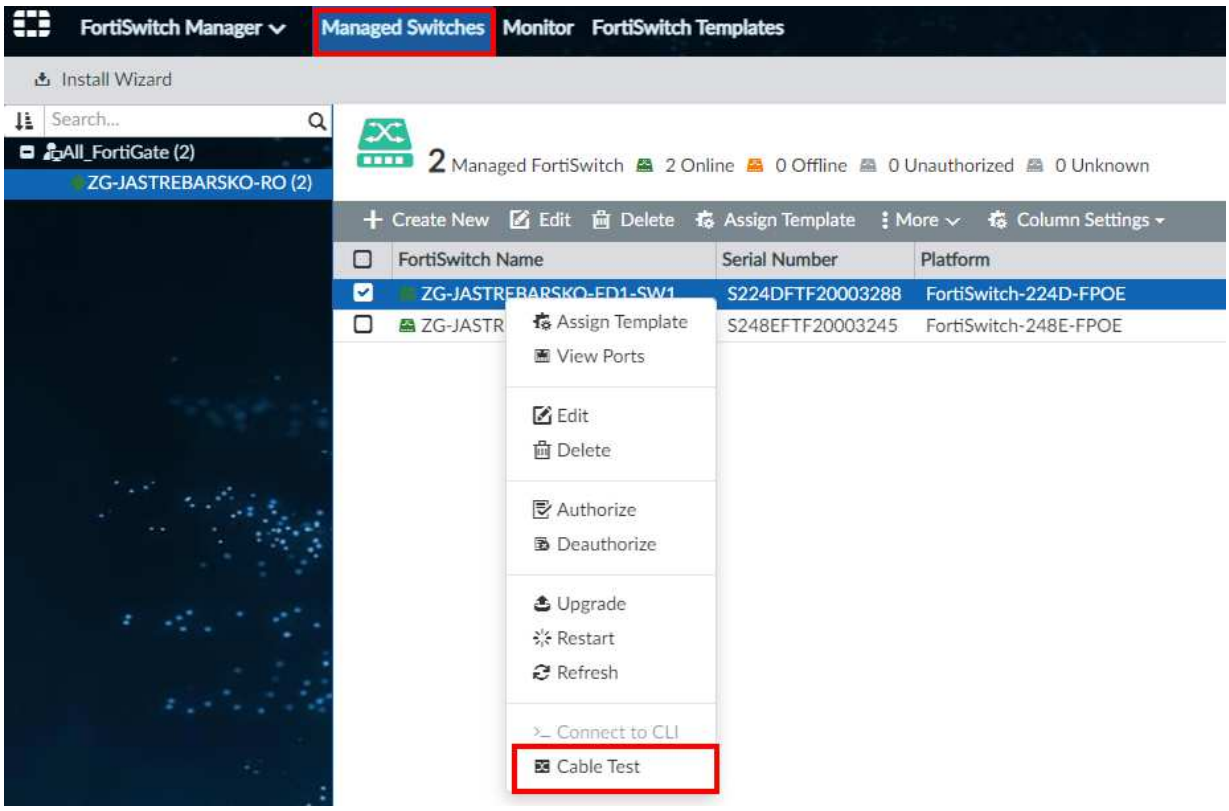
Opcija **Cable test** se koristi za ispitivanje ispravnosti mrežnog kabela koji povezuje sučelje na preklopniku s drugim uređajem na mreži. Ovaj mehanizam ispituje samo fizički spoj i u njega nisu uključeni dodatni utjecaji na rad mreže kao što je utjecaj elektromagnetskih zračenja i gušenja zbog lošeg spoja na krajnjim točkama.

Ovakva vrsta ispitivanja može uzrokovati prekide u radu i preporučeno ju je provoditi kada na mreži nema aktivnih korisnika.

Ova opcija se izvodi iz izbornika *FortiSwitch Manager*.

Potrebna je informacija na koji je preklopnik, odnosno na koje sučelje spojen krajnji uređaj prema kojem se ispituje kvaliteta veze.

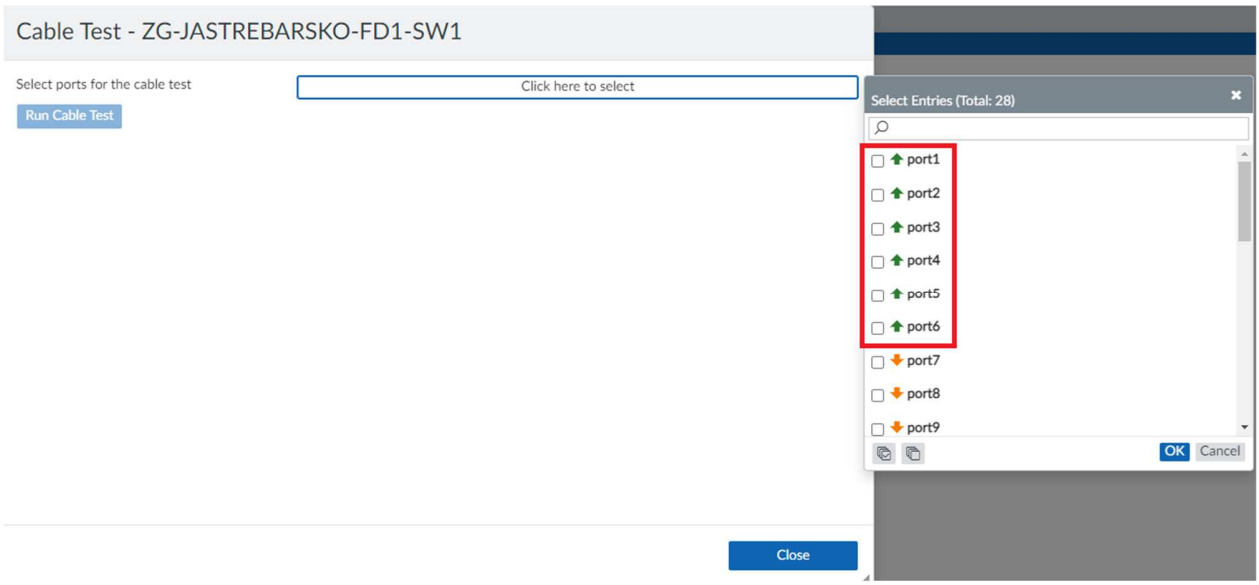
Nakon toga, u izborniku *Managed Switches* i popisu preklopnika odabire se preklopnik, a desnim klikom miša otvara se ispis opcija i potom odabire opcija *Cable Test.*



Slika 122: Managed Switches – izbornik za pokretanje opcije Cable Test

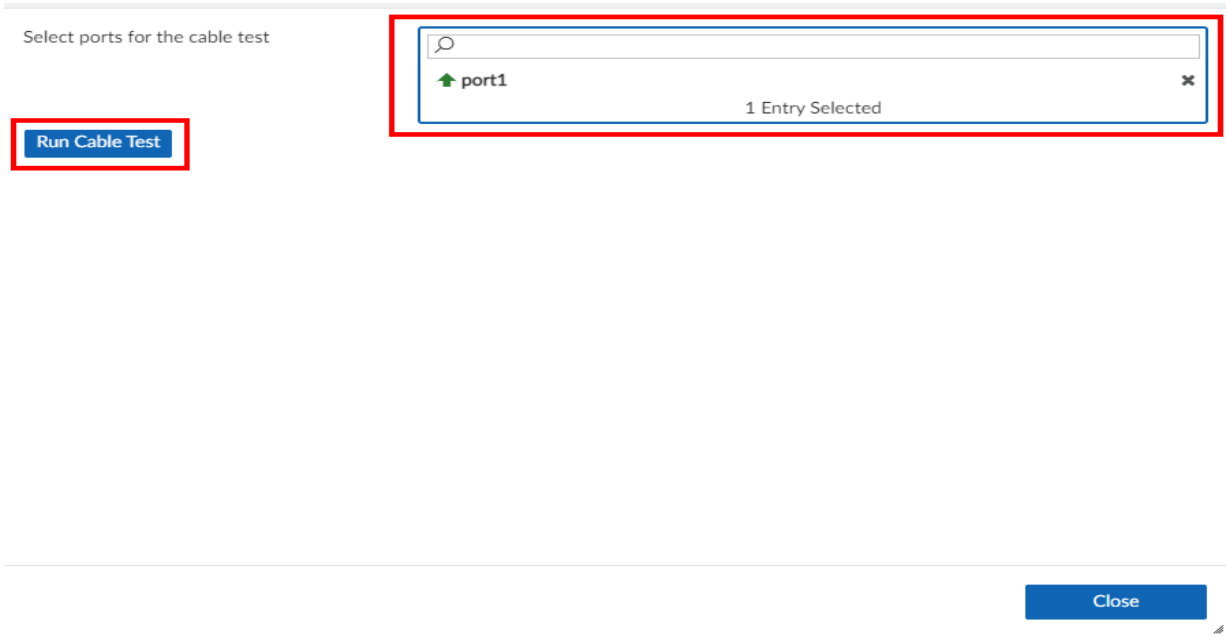
Sljedeći korak pruža popis aktivnih / neaktivnih sučelja.

Kako bi se moglo izvršiti ispitivanje, sučelje mora biti u statusu aktivno (zelena strelica prema gore).



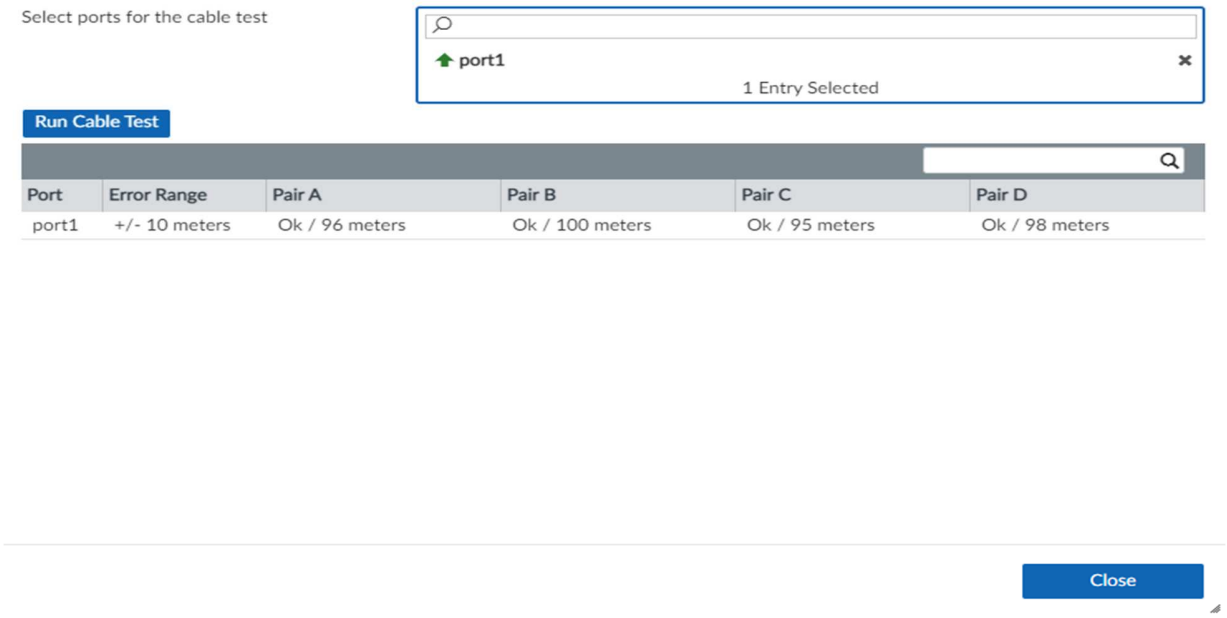
Slika 123: Cable Test – Popis raspoloživih sučelja za testiranje

Potrebno je odabrati aktivno sučelje s liste i pritiskom na *Run Cable Test* započinje postupak provjere. Testom može biti obuhvaćeno jedno ili više sučelja.



Slika 124: Cable Test – pokretanje mehanizma

Nakon završetka ispitivanja, rezultat je sljedeći:



Slika 125: Cable Test – rezultat pozitivnog ispitivanja

Rezultat testa su podatci koji prikazuju status parica mrežnih kabela (*Pair A, Pair B, Pair C i Pair D*) koji su spojeni na odabrana sučelja. Ako je sve u redu, rezultat testa je *Ok*. Ako nešto nije u redu s paricama, rezultat testa je *open*. Udaljenost u metrima računa se od preklopnika prema krajnjem uređaju.

Ovaj mehanizam ispituje samo fizički spoj i u njega nisu uključeni dodatni utjecaji na rad mreže, kao što su preslušavanje parica, utjecaj elektromagnetskih zračenja i gušenja zbog lošeg spoja na krajnjim točkama.

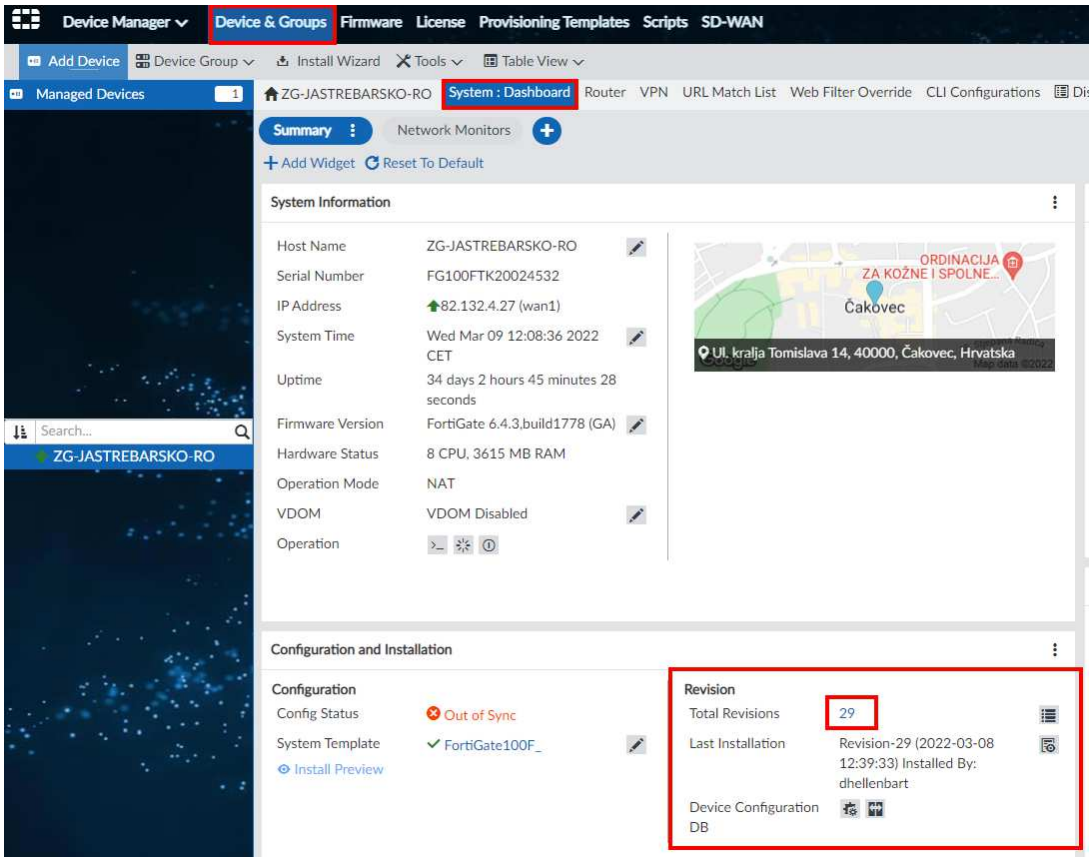
6.6.5 Prikaz vraćanja prethodne konfiguracije na usmjerivaču

U ovom je poglavlju prikazano vraćanje prethodne konfiguracije na usmjerivaču. Ova se situacija u radu može dogoditi ako se pojavi greška u trenutnoj konfiguraciji pa se potrebno vratiti na provjerenu, ispravnu konfiguraciju.

Mehanizam vraćanja na prethodnu konfiguraciju omogućava uvid u prethodne revizije konfiguracije koje su bile instalirane na uređaj unutar određenog ADOM-a i nudi opciju oporavka ranije revizije i ponovnog apliciranja na sam uređaj.

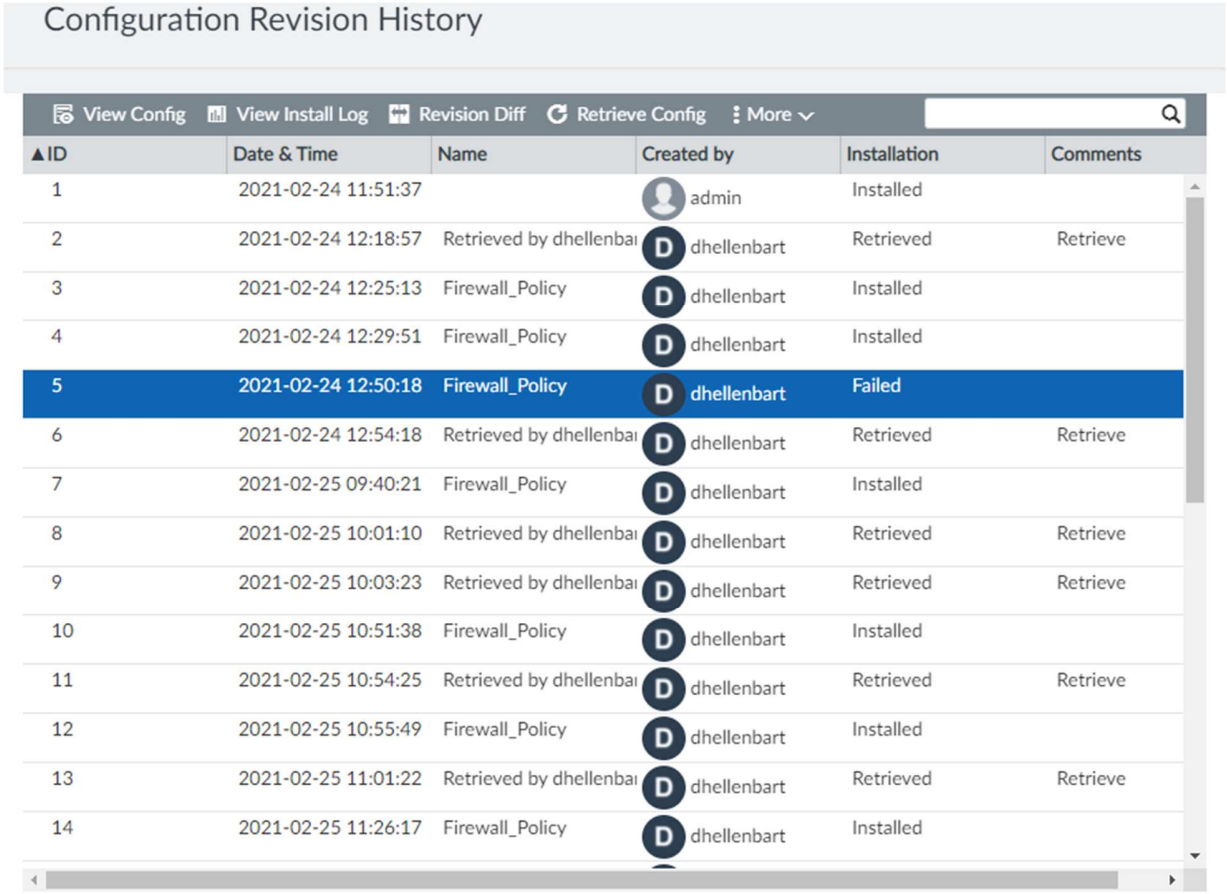
Mehanizam vraćanja nalazi se u izborniku *Device Manager* u kojem je potrebno odabrati opcije *Device & Groups* i *System:Dashboard*.

Na kontrolnoj se ploči (*System:Dashboard*) u izborniku *Revisions* nalazi popis s listom konfiguracija, odnosno pripadajućih revizija za usmjerivač.



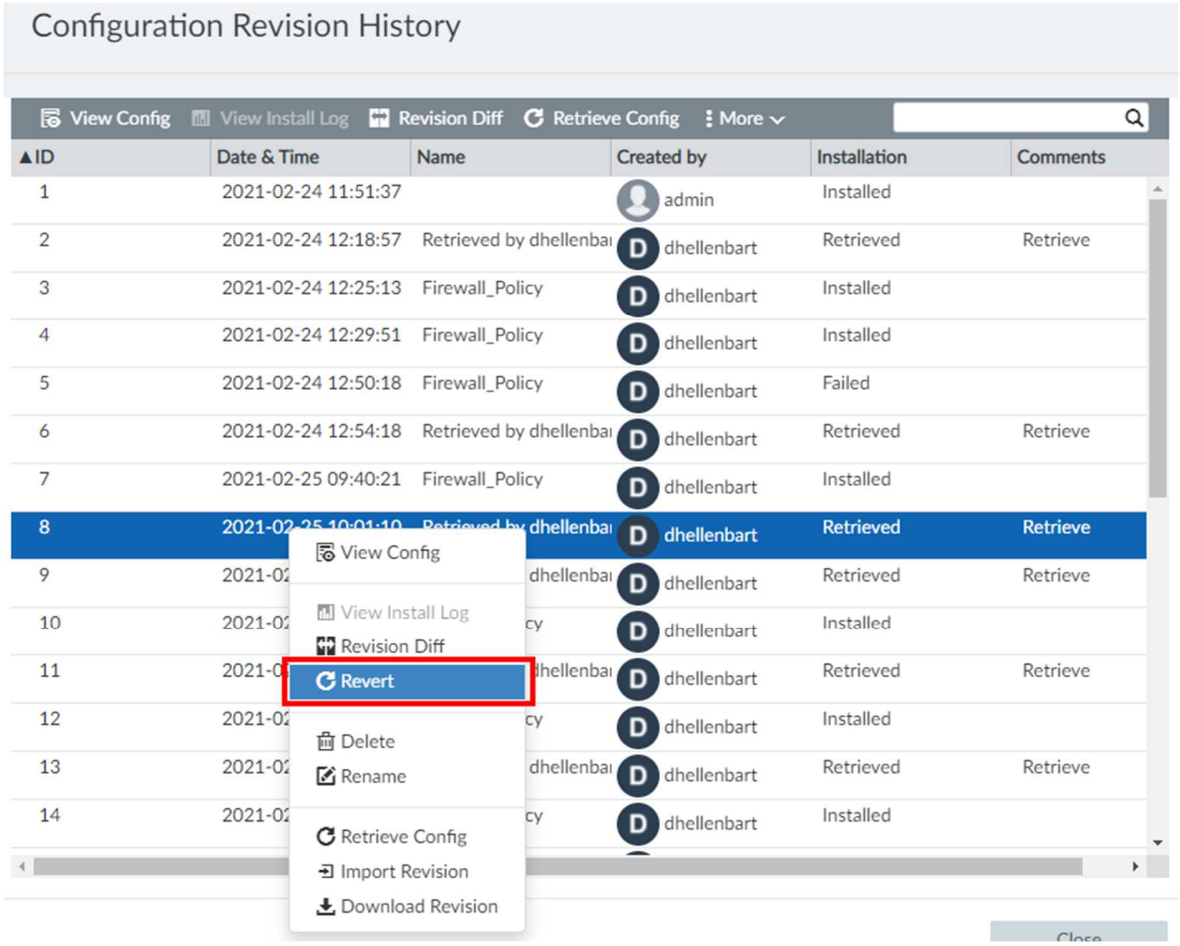
Slika 126: Total Revisions – popis revizija konfiguracija

Odabirom broja revizija, prikazuje se detaljniji popis konfiguracija, odnosno revizija.



Slika 127: Detalji revizija konfiguracije

Vraćanje na raniju reviziju konfiguracije provodi se odabirom revizije koja se želi vratiti te se nakon pritiska na desni klik miša odabire opcija *Revert*.



Slika 128: Revert – opcija za vraćanje željene konfiguracije

6.6.6 Prikaz promjena konfiguracije na usmjerivaču primjenom naredbi CLI

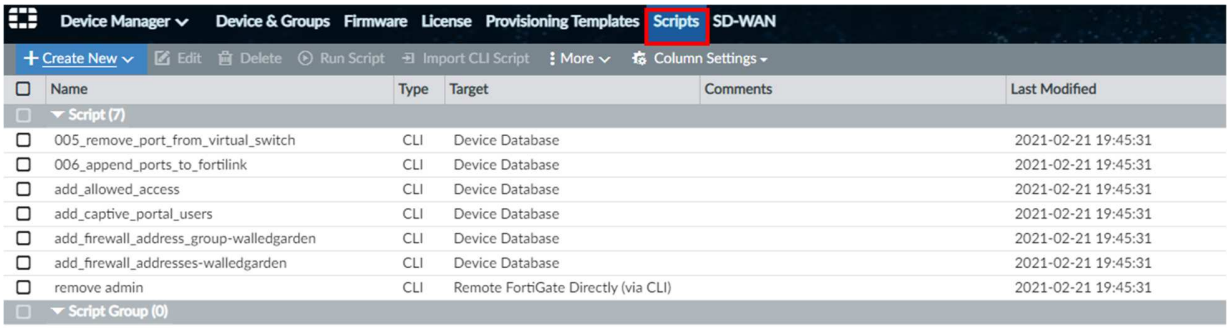
U ovom je poglavlju prikazana promjena konfiguracije primjenom naredbi CLI (predložak).

Konfiguracija uređaja Fortinet podržava i *Command Line Interface*. **Važno je naglasiti da pristup konfiguraciji na ovaj način iziskuje napredno znanje sintakse naredbe, odnosno funkcionalnosti koje se žele postići na samom uređaju.**

Dodatan način automatizacije konfiguracije moguć je grupiranjem naredbi CLI u skripte, odnosno skripte u predloške (*template*).

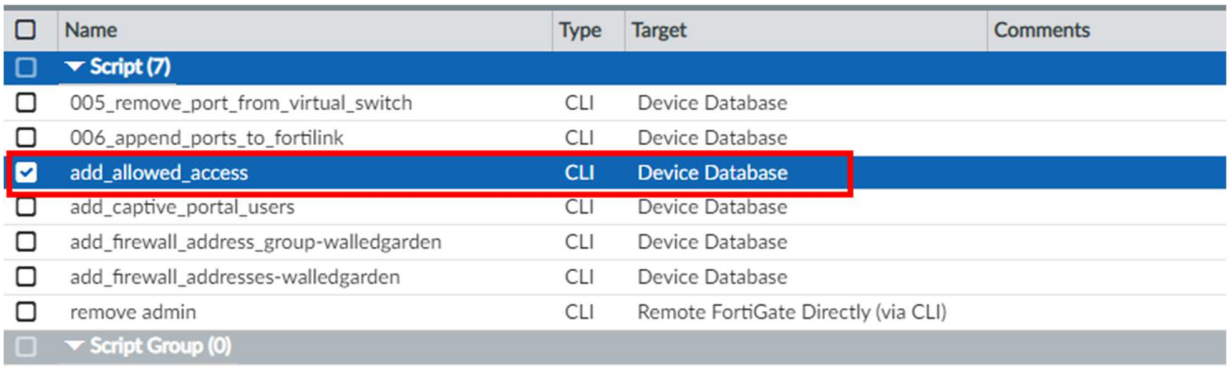
Izbornik za CLI otvara se odabirom izbornika *Device Manager* unutar pripadajućeg ADOM-a.

U izborniku *Device Manager* odabire se podizbornik *Scripts*.



Slika 129: Scripts – obrazac za kreiranje nove CLI Skripte

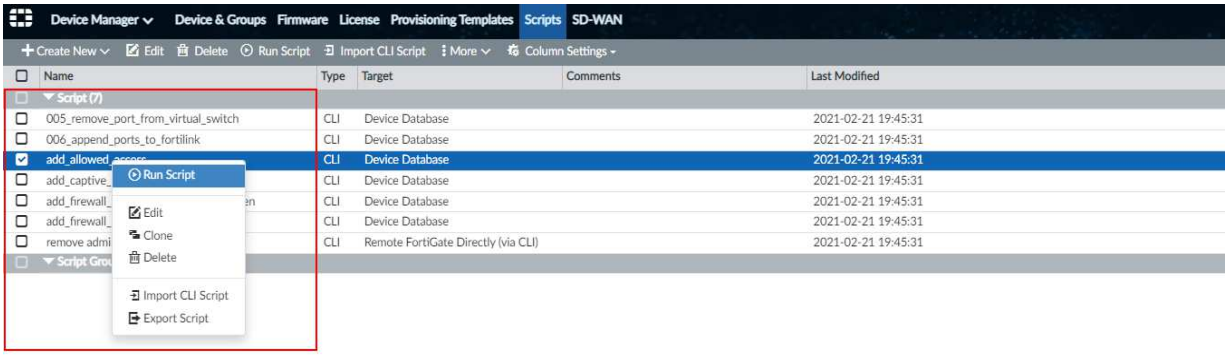
U sustavu su definirane skripte koje su namijenjene početnoj konfiguraciji vatrozida pa se sam koncept objašnjava na njihovu primjeru.



Slika 130: Primjer skripte CLI

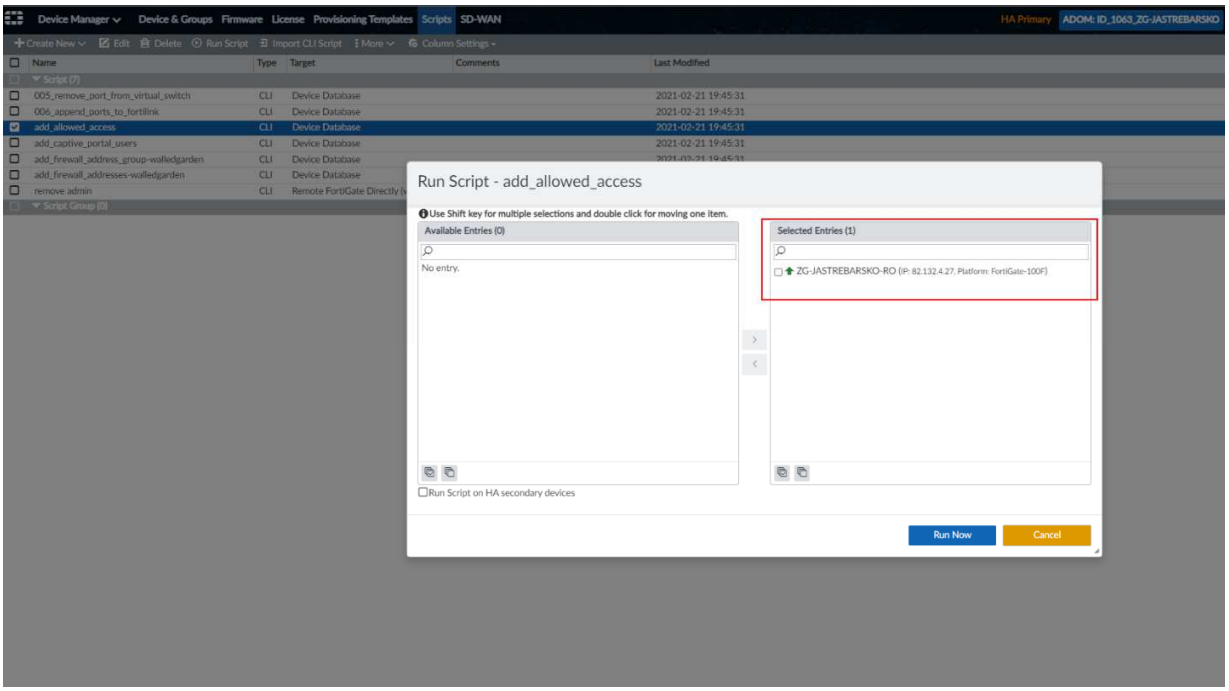
Skripta *add_allowed_access* sadrži sintaksu koja omogućava pristup sučelju WAN1 putem protokola *ping*, *fmfm* (FortiManager), *ssh* i *https*.

Iz popisa skripti odabire se skripta, desnim klikom miša otvara se ispis opcija i odabire se opcija *Run Script*.



Slika 131: Run Script – obrazac za apliciranje željene skripte na usmjerivač

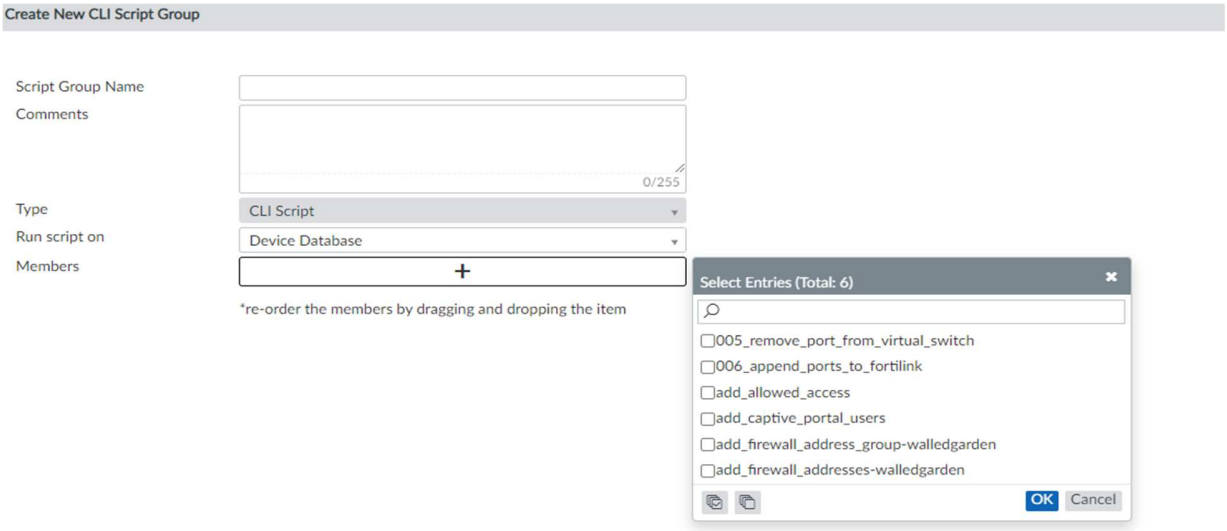
Nakon odabira željene skripte, otvara se izbornik za odabir uređaja na koji se želi primijeniti skripta, a skripta se pokreće pritiskom na *Run Now.*



Slika 132: Prikaz dodijeljene skripte usmjerivaču

Također je moguće grupirati više skripti u grupu, što olakšava i automatizira njihovo izvođenje jer se odjednom može izvršiti više skripti.

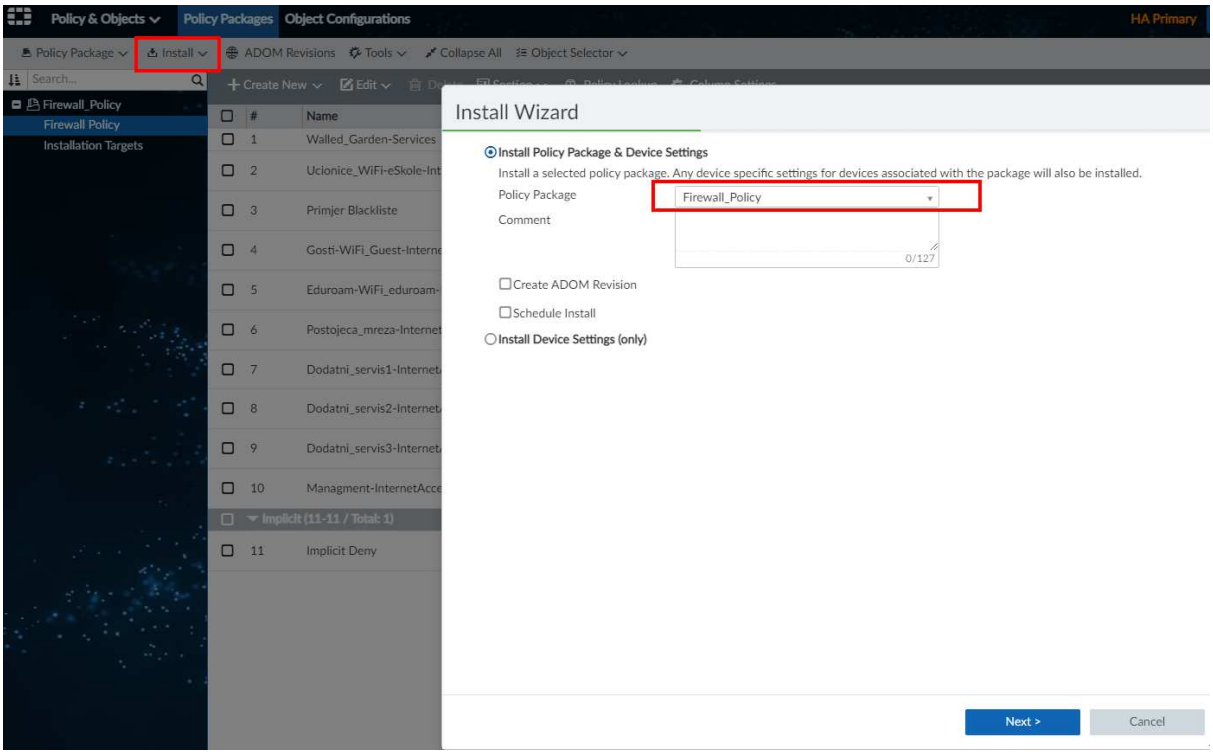
Kreiranje grupe provodi se u izborniku *Scripts*, odnosno u podizborniku *Create New CLI Script Group*.



Slika 133: New CLI Script Group – obrazac za kreiranje nove grupe skripti

Nakon dodjeljivanja inicijalnog naziva, potrebno je dodati pojedinačne skripte koje se žele izvršiti na samom uređaju.

Nakon odabira skripti koje se želi izvršiti, pritiskom na *Next* pokreće se instalacija novih sigurnosnih zapisa i postavki.



Slika 134: Instalacijski proces i primjena skripte na usmjerivač

6.6.7 Smjernice za otklanjanje poteškoća

Otklanjanje poteškoća (engl. *troubleshooting*) predstavlja sustavan pristup rješavanju poteškoća. Njegov je cilj utvrditi zašto nešto ne radi prema očekivanjima i objasniti kako riješiti poteškoću.

Budući da se poteškoćama ne pristupa stihijski i bez plana, definirane su osnovne smjernice, odnosno koraci kojih se potrebno pridržavati u cilju što bržeg i jednostavnijeg postizanja željenog rezultata.

Prvi korak u procesu rješavanja poteškoće je prikupljanje informacija o poteškoći, kao što je neželjeno ponašanje ili nedostatak očekivane funkcionalnosti. Ovaj korak uključuje postavljanje nekoliko osnovnih pitanja:

- Koji su simptomi poteškoće?
- Gdje nastaje poteškoća?
- Kada nastaje poteškoća?
- Može li se poteškoća reproducirati?

Odgovori na ovakva pitanja obično vode do dobrog opisa poteškoće, a to je najbolji način da se započne s njenim rješavanjem.

Komunikacija s korisnikom koji prijavljuje poteškoću je ključna. Ona treba biti prilagođena korisniku kako ne bi došlo do međusobnog nerazumijevanja, odnosno pogrešnog tumačenja dobivenih odgovora. Što se više kvalitetnih informacija prikupi od korisnika, kasnije će se manje vremena provesti u otklanjanju poteškoće.

Drugi je korak analiza na uređajima i provjera u centralnom sustavu za upravljanje.

Kod analize i provjere, ovisno o načinu na koji su spojena klijentska računala, razlikujemo dva niže navedena pristupa.

1) **Klijentska računala spojena mrežnim kabelom**

Kod klijentskih računala spojenih mrežnim kabelom, preporučljivo je započeti provjerom fizičkog (L1) i podatkovnog (L2) sloja kako bismo utvrdili pojavljuje li se poteškoća već kod fizičkog povezivanja računala s ostatkom mreže (npr. prekid mrežnog kabela).

Ako se utvrdi da je na tim slojevima sve u redu, upotrebljavaju se alati na samim računalima, kao što su ipconfig, ping i tracert, koji mogu pomoći u otklanjanju poteškoće bez spajanja na centralni sustav za upravljanje.

Ako navedeno ne rezultira otklanjanjem poteškoće, potrebno se spojiti na centralni sustav za upravljanje jer se iz zapisnika događaja u sustavu i korištenjem alata za otklanjanje poteškoća (troubleshooting) koji su na raspolaganju može precizno detektirati u kojoj fazi i zbog čega nastaje poteškoća u komunikaciji.

2) **Klijentska računala spojena na bežičnu mrežu**

Kod klijentskih računala spojenih na bežičnu mrežu, za analizu se koriste alati na samim računalima kao što su ipconfig, ping i tracert.

Kod ostalih uređaja koji se spajaju isključivo bežičnim putem, informacije se pronalaze u postavkama mrežnih kartica. Kod rješavanja poteškoće s ovakvim tipom uređaja, ključan je centralni sustav za upravljanje pomoću kojeg se prikupljaju informacije o postavkama mrežnih kartica.

Ako osoba koja je angažirana na održavanju funkcionalnog mrežnog sustava u školama nakon prolaska kroz opisane korake i prikupljanje svih relevantnih informacija nije u mogućnosti riješiti poteškoću, preporučljivo je da se obrati CARNET-ovoj službi za podršku (helpdesk).

7. Prijava poteškoća i upita CARNET-ovom *helpdesku*

U slučaju poteškoća u radu sustava i za sva pitanja vezana uz 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

Popis tablica

Popis 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, Karlo Mrazović

Lektorica: Mateja Međeši

Zagreb, ožujak 2022.

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

Ovaj je priručnik izrađen 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.