Centralizirano upravljanje SOHO usmjerivača preko univerzalnog web sučelja

Baksa, Davor

Undergraduate thesis / Završni rad

2018

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:345052

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

ALGEBRA VISOKO UČILIŠTE

Repository / Repozitorij:

Algebra Univerity College - Repository of Algebra Univerity College

zir.nsk.hr

dabar DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

Centralizirano upravljanje SOHO usmjerivača preko univerzalnog web sučelja

Davor Baksa

Zagreb, veljača 2018.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 01.02.2018.

Davor Baksa

Predgovor

Zahvaljujem se mentoru Vedranu Dakiću za ukazanu podršku, kolegama tvrtke IDE3 d.o.o. na strpljenju i pomoći oko tehničke izvedbe te svojoj ženi Petri na neprekidnoj moralnoj podršci.

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

Sažetak

U ovom se radu obrađuje koncept izrade sustava za centralizirano upravljanje bežičnim usmjernicima u svrhu olakšavanja administracije istih. Posebna pozornost obraća se na funkcionalnost sustava iz korisničke perspektive , razradi sustava visoke dostupnosti, te brizi o sigurnosnim aspektima sustava. Sustav se uspoređuje sa trenutnim konkurentskim rješenjima te se zaključuje o isplativosti izrade i korištenja takvog sustava.

Ključne riječi: centralno upravljanje, oblak, isplativost.

This thesis covers the concept of developing a centralized management system for wireless routers in the purpose of simplifying the administration tasks of those routers. Special notice is being taken on the systems functionality from the users perspective, the high availability setup and the security aspects of the system. The system is compared to current rival solutions and the conclusion on the benefits of making and using such system is made.

Key words: centralized management, cloud, profitability

Sadržaj

1. Uvod 1

2. Oprema - hardver 2

2.1. Modeli po primjeni 2

2.2. Licenciranje sustava 3

2.3. Povezivost 4

2.4. Propagacija klijentskih uređaja 5

3. Centralizirano upravljanje 10

3.1. Mogućnosti sustava 10

3.2. Moduli 11

3.2.1. WiFi modul 11

3.2.2. VPN modul 13

3.2.3. Modul za upravljanje korisnicima 16

3.3. Mehanizam komunikacije 17

4. Sigurnost i zaštita 21

4.1. L2 / L3 zaštita 21

4.2. Web server – upravljačka aplikacija 21

4.3. Baza podataka 22

4.4. Zalihost i sigurnosna pohrana podataka 22

5. Usporedba sustava sa konkurentskim riješenjima 25

Zaključak 28

Popis kratica 29

Popis slika 31

Popis tablica 32

Popis kôdova 33

Literatura 34

1. Uvod

U današnje vrijeme bežična mreža je neizostavan dio svakog kućanstva ili tvrtke te je na tržištu sve više dostupnih pametnih uređaja koji uz osnovnu funkcionalnost emitiranja bežične mreže nude i paletu ostalih funkcija koje prosječan korisnik ne razumije i / ili misli da ne treba. Zbog nerazumijevanja samih funkcionalnosti takvih uređaja nije moguće ni uvidjeti poslovne benefite koje te funkcionalnosti mogu pružati.

Kada je riječ o tvrtkama tu se iz raznih razloga ukazuje i potreba za segmentacijom mreže, upravljanjem ovlastima pristupa pojedinim mrežnim segmentima kao i ostale stvari poput upravljanja propusnošću pojedinog mrežnog segmenta. U ovu svrhu tvrtke zapošljavaju IT stručnjake kako bi brinuli o takvim stvarima, no postoji nebrojeno primjera gdje se koriste takvi sustavi a da nije osigurana adekvatna IT podrška zbog čega sustav ili ne radi optimalno ili se ignoriraju sigurnosne implikacije takvog bazično posloženog sustava.

Najbolji primjer toga bi bili ugostiteljski obrti poput kafića i restorana, te iznajmljivači apartmana. U velikoj većini slučajeva vlasnici takvih tvrtki generalno posežu za najekonomičnijom varijantom te idu linijom manjeg otpora, tj. dijele internet vezu sa svojim klijentima koristeći usmjernik dobiven od ISPa kojeg i sami koriste. U tim se slučajevima klijenti koji koriste takvu mrežu nalaze na istom mrežnom segmentu kao i sustavi za fiskalizaciju, videonadzor sustavi te često i razni serveri za pohranu podataka.

Cilj ovog rada je pokazati kako je moguće razviti sustav za centralno upravljanje jednim ili više bežičnih usmjernika u svrhu izrade zasebnih mrežnih segmenata, te omogućiti krajnjim korisnicima sustava jednostavno upravljanje svojim mrežama putem unificiranog web sučelja bez dodatnog predznanja o tehničkim aspektima mreže koju administriraju. Rezultat ovoga je jednostavno dodavanje novih bežičnih mreža na zasebnim mrežnim segmentima, segregacija od postojeće (primarne) mreže gdje su svi kritični servisi za poslovanje te implemetacija limita na maksimalnu brzinu koju pojedini mrežni segment može koristiti – npr. dodavanje bežične mreže za goste nekog kafića koja je odvojena od glavne mreže sa limitom brzine pristupa internetu kako bi se osiguralo da primarni servisi koji ovise o tom Internet pristupu rade nesmetano (poput A/V strujanja, fiskalizacije i osnovnog pristupa internetu).

Predloženi sustav je trenutno u fazi razvoja od tvrtke IDE3 d.o.o. pod kodnim imenom „WiFi Cloud“ te se javna beta verzija očekuje na ljeto 2018. godine.

2. Oprema - hardver

Sustav je koncipiran tako da dozvoljava BYOD (*Bring Your Own Device*) pristup kao i direktnu nabavu novog uređaja kojeg će upravljati putem sustava za upravljanje. Obzirom na potrebe komunikacije između upravljivog usmjernika i centralnog sustava za upravljanje u obzir dolaze oni modeli bežičnih usmjernika koji zadovoljavaju sljedeće preduvijete:

- mogućnost ostvarivanja kriptiranog tunela preko interneta (IPSEC, oVPN, L2TP w/IPSEC)
- mogućnost pristupa konzoli usmjernika putem telneta ili SSH protola
  ili
- podrška za API

Obzirom na gore navedeno i trenutnu ponudu uređaja koji zadovoljavaju isto, kao primarni preferirani proizvođač koristit će se Mikrotik usmjernici zbog svoje cijene, podržanih mogućnosti i stabilnosti rada. U naknadnim verzijama sustava planirano je dodavanje i potpune podrške za određene Cisco WAP usmjernike kao i Ubiquiti usmjernike.

2.1. Modeli po primjeni

Kao i kod svake nabavke opreme prije svega treba razmotriti zahtjeve klijenta, u ovom slučaju to su sljedeće stvari:

- koliko bežičnih klijenata će se spajati u nekom datom trenutku
  - ovisno o broju klijenata koji će se spajati na bežičnu mrežu odabire se model usmjernika koji je u stanju procesirati zahtjeve svih klijenata kako ne bi došlo do zagušenja prilikom korištenja. Na definiranu brojku treba uzeti u obzir i zalihost od barem 20%.

- kolika je minimalna propusnost koja se treba osigurati
  - ovisno o željenoj propusnosti (koja se može definirati na nivou cijelog mrežnog segmenta ili na nivou pojedinog korisnika bežične mreže) treba uzeti u obzir da odabrani uređaj ima dovoljno procesorske snage za sve korisnike i sve mreže, te

da podržava bežične standarde koji su dovoljni za osiguravanje željene propusnosti (802.11b/g/n/ac)

- kolika je propusnost Internet veze na lokaciji
  - većina jeftinijih usmjernika ima integrirane 100Mbit mrežne priključke, no ukoliko se na lokaciji koristi usluga pristupa internetu brža od 100Mbit potrebno je razmotriti uređaje koji podržavaju i veće brzine (1000Mbit)

- postoje li već neke bežične mreže u okolici lokacije te da li je predviđeni bežični spektar već zagušen[1]
  - jedna od stvari koja se često predvidi je mogućnost interferencije na bežičnom spektru od strane bežičnih usmjernika trećih strana. Iako svi današnji bežični usmjernici koriste svojevrsnu *radar-detect* funkciju koja provjerava zagušenost korištenog kanala te automatski prebacuje emitiranje svoje mreže na manje zagušen kanal u pravilu je velika većina dostupnih mreža i dalje emitirana na 2.4GHz rasponu (802.11b/g/n) što efektivno ne daje željene rezultate jer je cijeli spektar zagušen te najčešće nema dostupnog optimalnog kanala koji bi se mogao koristiti. U ovim slučajevima preporuča se nabavka uređaja koji podržava i 802.11ac protokol (5GHz raspon).

2.2. Licenciranje sustava

Sustav je koncipiran da pruži osnovnu mogućnost upravljanja mrežnim segmentima, bežičnim mrežama i osnovnim sigurnosnim postavkama kao i kvotama za iste.

No, ovisno o korištenom modelu uređaja kojim se upravlja moguće su i dodatne funkcionalnosti – uzeći to u obzir moguće je licenciranje raščlaniti na više faktora.

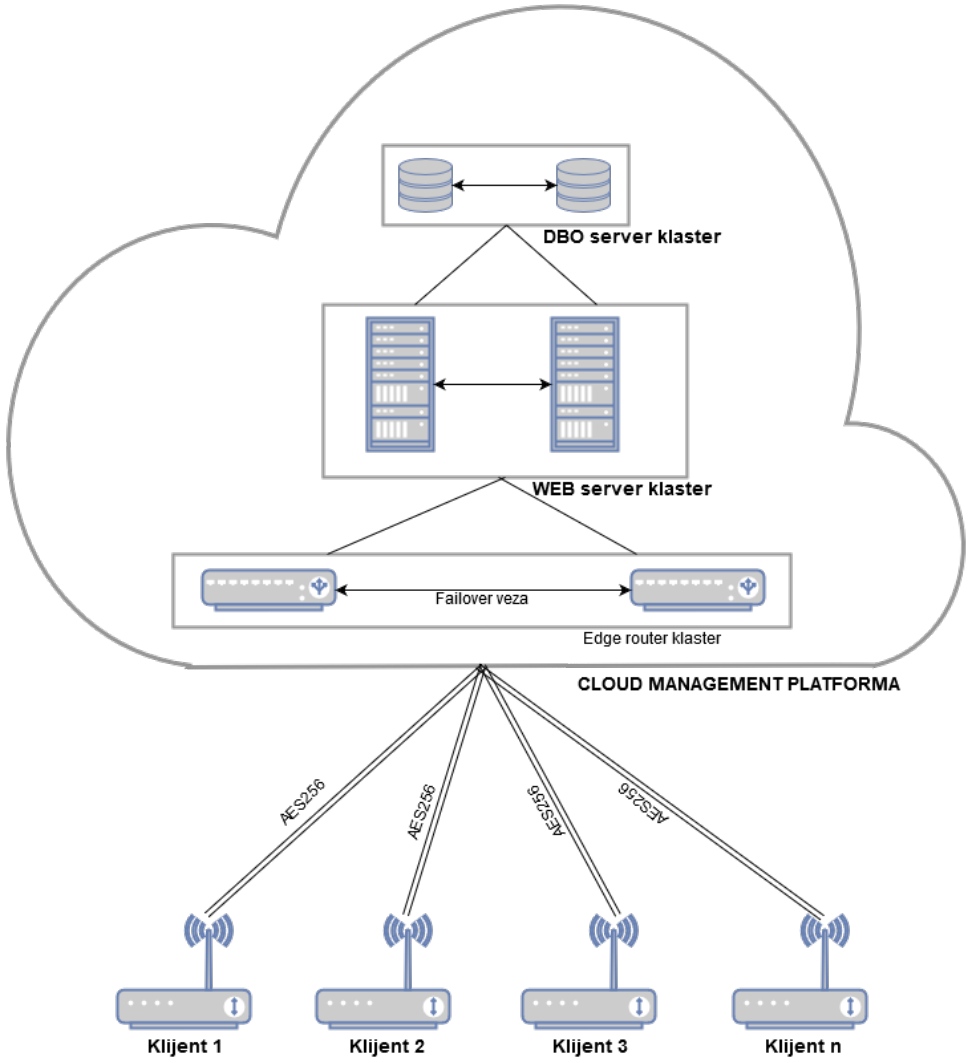
Kao osnovni paket korisniku se pruža mogućnost administriranja mrežnim segmentima. Svaka dodatna funkcionalnost se tretira kao nadogradnja osnovnog paketa u obliku modula koji se plaća zasebno. Na ovaj način krajnji korisnik sustava ima potpunu kontrolu nad troškovima i koristi samo one funkcije sustava koje mu trebaju. Dostupnost modula ovisi i o mogućnostima uređaja koji se koristi.

Licenciranje se odnosi na zakup prava korištenja sustava na jednu godinu, za jedan uređaj.

2.3. Povezivost

Osnovni preduvjet rada sustava je nesmetana komunikacija centralnog sustava za upravljanje i korisničkih usmjernika. Kako bi se to osiguralo na strani centralnog sustava se nalazi VPN server / IPSEC endpoint, dok korisnički usmjernici podižu konekciju prema centralnom sustavu. Na ovaj se način rješavaju problemi sa vatrozidima na korisničkoj strani jer se radi o odlaznom tipu prometa (korisnik inicira konekciju). Također, kako se radi o AES-256 kriptiranim tunelima eliminira se mogućnost vanjskih utjecaja i proboja toka informacija.

Korisnički usmjernici se spajaju na centralni sustav u mrežni segment koji je namijenjen isključivo za upravljanje usmjernika te mogu komunicirati samo sa centralnim sustavom (ne i međusobno).



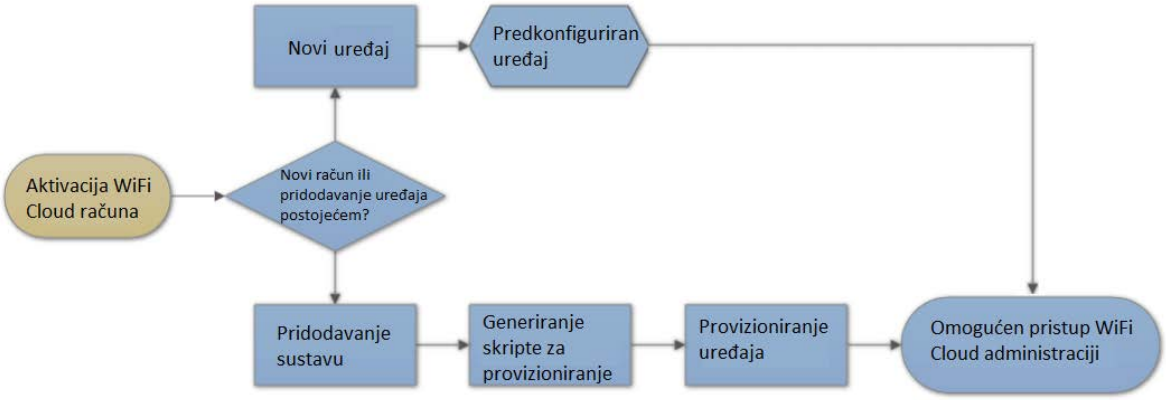
Slika 2.1 Shema komponenti sustava za upravljanje

Prilikom izrade novog korisničkog računa za krajnjeg klijenta automatski se generira i VPN korisničko ime i lozinka za svaki pojedini uređaj kojim će taj korisnik imati ovlasti upravljanja te se kroz skriptu za podešavanje automatski inicira VPN konekcija prema centralnom serveru. Na ovaj se način može pratiti točno koji uređaj pod kojim korisnikom koristi koju IP adresu te se prema toj IP adresi šalju izmjene u konfiguraciji na odgovarajući uređaj (putem kriptiranog tunela) koju korisnik kreira koristeći sustav.

Rezultat ovoga je da krajnji korisnik ne treba imati nikakvo prethodno poznavanje tehnologije niti mora brinuti o vatrozidima sa svoje strane, već je jedini preduvjet koji mora ispuniti taj da se osigura internet povezivost na lokaciji gdje će se koristiti bežični usmjernik.

2.4. Propagacija klijentskih uređaja

Nakon što se korisnik registrira za pristup sustavu istom se izrađuje korisnički račun putem kojeg može administrirati uređaj(e). Ukoliko se radi o novom računu podrazumijeva se da korisnik treba i upravljivi uređaj te se novi uređaj po odabiru korisnika unaprijed podešava i tako pred konfiguriran šalje korisniku sa uputama za spajanje u obliku samo-instalacijskog paketa. Odabir samog modela uređaja može ovisiti o raznim faktorima potreba korisnika, poput količine potrebnih LAN priključaka, propusnosti tih priključaka (100Mbit ili 1000Mbit), količini predviđenih uređaja koji će se spajati na mrežu koja se administrira i sl.



Slika 2.2 Dijagram toka dodavanja upravljivog uređaja sustavu

Ukoliko korisnik već ima korisnički račun te želi sustavu administracije pridodati dodatne kompatibilne uređaje, to može učiniti tako da nakon nabavke uređaja na isti putem skripte provizionira potrebne postavke. Odabirom kompatibilnog modela uređaja u sustavu se

automatski generira skripta za provizioniranje istog te se korisniku nude upute za jednostavno provizioniranje uređaja.

Ukoliko korisnik ima pristup administraciji dodatnog uređaja kojeg spaja na sustav dovoljno je (za Mikrotik uređaje) jednom naredbom preuzeti i implementirati potrebnu skriptu:

```
/tool fetch https://wificloud.hr/primjer.txt; import
primjer.txt; file remove primjer.txt
```

Kôd 2.1 Naredba za provizioniranje usmjernika

Navedena naredba, iako jedinstvena cjelina, se može rasčlaniti na tri dijela:

`/tool fetch https://wificloud.hr/primjer.txt`

- preuzimanje generiranje skripte u memoriju uređaja

`import primjer.txt`

- učitavanje skripte u trajnu memoriju uređaja

`file remove primjer.txt`

- uklanjanje same skripte iz memorije uređaja

Bitno je napomenuti da je za dohvat skripte potrebno osigurati da je korisnik sa svoje vanjske IP adrese ulogiran u sustav centralnog upravljanja te će se samo u tom slučaju dozvoliti pristup generiranoj skripti. Također, ime same datoteke skripte se formira kombinacijom jedinstvenog ID oznake korisnika i ID oznake upravljivog uređaja kojeg se želi provizionirati. Ovime se eliminira neželjen scenarij u kojem neki drugi korisnik može provizionirati svoj uređaj skriptom koja nije bila generirana specifično za tog korisnika i za taj uređaj.

Sama skripta se sastoji od nekoliko koraka koji su potrebni da pojedini uređaj ostvari sigurnu konekciju prema sustavu centralnog upravljanja i to od:

- čišćenja konfiguracije (u slučaju prethodno provizioniranog uređaja)
- ostvarivanja sigurne veze prema sustavu centralnog upravljanja
- izrade korisnika na uređaju koji ima ovlasti pristupa uređaju putem API-ja

Primjer čišćenja konfiguracije:

```
/interface ovpn-client remove [/interface ovpn-client find
name="WIFICLOUD"]
/certificate remove [/certificate find where
name~"wificloud.hr.p12_"]
/ip firewall filter remove [/ip fire filter find
comment="WIFICLOUD management"]
/file remove wificloud.hr.p12
```

Kôd 2.2 Naredbe za uklanjanje zaostale konfiguracije

U ovom se dijelu uklanjaju VPN tuneli prema centralnom serveru, uklanjanju korišteni certifikati te uklanjaju vezana vatrozidna pravila.

Primjer ostvarivanja sigurne veze prema sustavu centralnog upravljanja:

```
/tool fetch http://wificloud.hr/wificloud.ide3.hr.p12
:delay 1
/certificate import file-name=wificloud.hr.p12
passphrase=[generirana lozinka za korisnički cetifikat]
:delay 1
/interface ovpn-client add name=WIFICLOUD user=[korisničko
ime geneirano za VPN tunel pojedinog korisnika]
password=[lozinka za VPN tunel] connect-to=wificloud.hr
mode=ip port=1194 certificate=wificloud.hr.p12_0 disabled=no
auth=sha1 cipher=aes256
:delay 1
/ip firewall filter add chain=input src-address=[IP adresa
centralnog usmjernika sustava za upravljanje putem VPN
tunela] action=accept comment="WIFICLOUD management"
:delay 1
/ip firewall filter move [/ip firewall filter find
comment="WIFICLOUD management"] 0
```

Kôd 2.3 Naredbe za uspostavu veze usmjernika sa centralnim sustavom

U ovom se dijelu preuzimaju i aktiviraju generirani korisnički certifikati, generira se kriptirani VPN tunel prema sustavu centralnog upravljanja te se generiraju adekvatna vatrozidna pravila koja će dozvoljavati komunikaciju prema centralnom sustavu.

Primjer izrade korisnika za potrebe administracije uređaja:

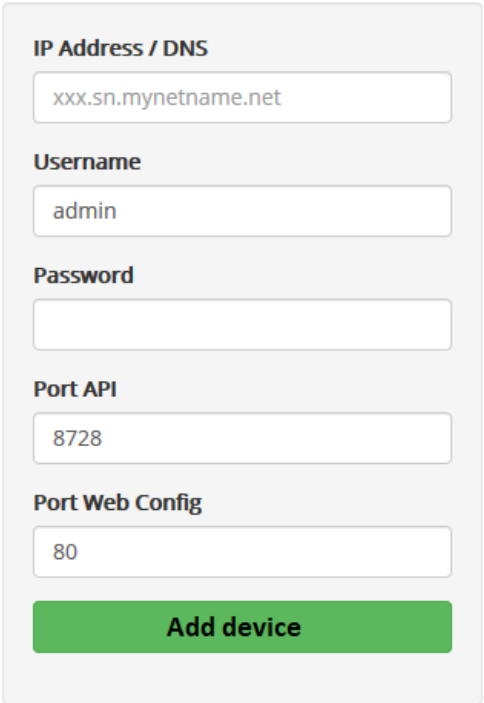
```
/user group add policy=api name=API
/user add name=API-user password=[lozinka za korisnika]
group=API
```

Kôd 2.4 Naredbe za izradu korisnika za administraciju na uređaju

U ovom se dijelu kreira sigurnosna grupa koja ima potrebne ovlasti te korisnik na samom uređaju kojeg se čini članom te grupe.

Rezultat ovoga je da je sa korisničke strane dovoljno izvršiti samo jednu naredbenu liniju dok će se uređaj automatski rekonfigurirati na način da ostvari sigurnu vezu prema sustavu centralnog upravljanja, te osigurati da se putem sigurne veze sa novo kreiranim korisnikom iz tog sustava može uređajem upravljati.

Kao alternativna metoda administracije pojedinog bežičnog usmjernika omogućena je i metoda direktnog dodavanja usmjernika po IP adresi i login podacima korisnika kojem je omogućen pristup (kako se radi o neprovizioniranom usmjerniku to je glavni administratorski račun).



Slika 2.3 Prikaz ručnog dodavanja uređaja u sustav

IP address – IP adresa usmjernika iz perspektive sustava za centralno upravljanje

Username – Korisničko ime koje ima adekvatne ovlasti na usmjerniku

Password – Lozinka za korišteni korisnički račun

Port API – Korišteni API port (za Mikrotik uređaje zadani port je 8728)

Port Web Config – Korišteni port za pristup web administraciji samog uređaja (nativno port 80, no moguće ga je izmjeniti)

3. Centralizirano upravljanje

Današnje prakse pokazuju velik iskorak sustava za centralno upravljanje na tržištu te se baš takvi sustavi jedini mogu dugoročno nositi sa izazovima koje današnje tehnologije donose.

Sve veći broj uređaja koji se moraju administrirati, na sve većem broju lokacija, iziskuje više vremena kako bi se konfigurirali i održavali.

Sustav centraliziranog upravljanja rješava taj problem i premošćuje jaz između sve veće potrebe za pristupom i sve manje resursa za rješavanje zadataka u administraciji opreme i usluga. Obzirom da je centraliziran, sustav je dostupan svim korisnicima, u bilo kojem trenutku, sa bilo kojeg uređaja koji ima pristup internetu te se time znatno olakšava administracija istih.

Također, sučelje takvog sustava ostaje uniformno bez obzira sa kojeg se uređaja pristupa, stoga se korisnici ne moraju privikavati na razlike, ovisno o uređaju sa kojeg pristupaju.

Samo sučelje je koncipirano minimalistički, tako da nudi korisnicima samo one funkcije koje im trebaju, bez da ih, poput većine sustava za centralizirano upravljanje opterećuje svim dostupnim opcijama koje korisniku nisu potrebne.

3.1. Mogućnosti sustava

Obzirom da centralni upravljački sustav ima puni pristup administraciji pojedinog usmjernika, sustav je u konačnici ograničen samo mogućnostima pojedinog uređaja koji se administrira na taj način – uz neke iznimke. No u svrhu standardizacije, krajnjem korisniku sustava je dozvoljen samo pristup mogućnostima koje su univerzalne, tj. dostupne na svim uređajima koje centralni upravljački sustav podržava.

Uz standardnu paletu opcija koje uređaji podržavaju, obzirom da se održava kontinuirana veza između usmjernika i sustava za centralno upravljanje, moguće je i kontinuirano praćenje potrošnje, opterećenja, definiranih kvota i odstupanje od istih, itd. Rezultat toga su izvještaji kojima korisnik može pristupiti iz samog sustava za definirani vremenski period. Primjer praktičnosti takvih izvještaja bi bio da korisnik generira izvještaj opterećenosti propusnosti na kreiranoj WiFi mreži za goste te uvidom u rezultate može procijeniti da li je veza većinski opterećena ili ne. Ukoliko je, kroz sustav upravljanja može jednostavno korigirati limite ograničenja i propustiti veću brzinu ovisno o potrebama i mogućnostima.

3.2. Moduli

Kako bi se dalje raščlanile mogućnosti koje sustav pruža, usluge su podijeljene u kategorije funkcionalnosti – module. Aktivacijom korisničkog računa za pojedinog korisnika tom se korisniku automatski omogućuje pristup osnovnom modulu – „WiFi modul“, koji služi za upravljanje bežičnim mrežama te ograničenjima istih. Svaka dodatna funkcionalnost se tretira kao dodatan modul koji je korisniku dostupan ukoliko se za to odluči, no kao zasebna cjelina koja nudi odvojenu funkcionalnost naplaćuje se dodatno kroz opcije licenciranja.

3.2.1. WiFi modul

Kao osnovni modul „WiFi modul“ je dostupan svim korisnicima sustava. Primarna namjena mu je upravljanje bežičnim mrežama u smislu dodavanja i uklanjanja istih, promjena parametara mreže (SSID i pristupne lozinke), podešavanje kvota propusnosti po mreži te podešavanje sigurnosnih postavki vezanih uz ostatak mreže.

Prilikom dodavanja mreže korisnik mora definirati sljedeće obavezne parametre:

- Ime mreže (SSID)
- Željena lozinka
- Gost mreža (DA/NE)

Ukoliko to želi, korisniku su dostupne i naprednije mogućnosti kod izrade nove mreže, poput definiranja mrežnih parametara (IP adresa usmjernika unutar te mreže, subnet maska, te korištene algoritme za lozinku (WPA/WPA2 – AES/TKIP)).

Detaljnije o opcijama:

Ime mreže (SSID) – korisnik definira željeno ime mreže. Sustav je ograničen na maksimalno 32 znaka obzirom na limitaciju standarda[2].

Željena lozinka – korisnik definira željenu lozinku za svoju mrežu. Prazno polje označava da nema lozinke. Sustav je ograničen na 8-63 znaka obzirom na limitaciju standarda.

Gost mreža (DA/NE) – ukoliko korisnik odabere da mreža koju kreira bude klasificirana kao gost mreža, sustav će automatski podesiti odgovarajuća vatrozidna pravila koja onemogućavaju komunikaciju te mreže (i svih klijenata spojenih na tu mrežu), sa svim ostalim lokalnim mrežama (ukoliko ih ima). Ovime se osigurava da nitko sa javne (gost)

mreže ne može pristupiti glavnoj LAN mreži koja se koristi na lokaciji. Ukoliko pak odabere da mreža nije gost mreža, ta će mreža imati puni pristup svim ostalim mrežama.

Kod odabira naprednih opcija (neobavezno), korisniku su dostupne sljedeće opcije:

Mreža je vidljiva (DA/NE) – ukoliko to želi, korisnik može „sakriti“ svoju mrežu tako da se SSID ne emitira. Ovo rezultira time da se samo osobe koje znaju točan naziv mreže i njenu lozinku mogu na nju spojiti

IP adresa usmjernika – korisnik definira željenu IP adresu usmjernika. Ova opcija je korisna ukoliko se ne radi o gost mreži te korisnik ima već definiranu adresu koju bi htio ili trebao koristiti. Ukoliko se polje ostavi prazno (ili se ne otvaraju napredne opcije kod izrade nove mreže) sustav će automatski pokušati dodijeliti adresu 192.168.1.1, tj. prvu iskoristivu adresu u neiskorištenom mrežnom segmentu C klase (ukoliko se trenutno koristi neka adresa iz 192.168.1.0/24 mrežnog segmenta, sustav će automatski pokušati dodijeliti adresu 192.168.2.1, itd.)

Maska mreže (subnet mask) – korisnik ovdje definira veličinu svoje mreže podešavajući subnet masku. Ukoliko se polje ostavi prazno, sustav pretpostavlja da se koristi /24 maska (255.255.255.0).

Enkripcijski algoritmi – korisnik ovdje bira između WEP, WPA i WPA2 tipa enkripcije, te (u slučaju korištenja WPA i WPA2) između TKIP i AES algoritma. Podrška za WEP je dodana isključivo zbog kompatibilnosti sa starijim uređajima te se korištenje iste ne preporuča zbog gotovo nepostojeće sigurnosti. U kontekstu korištenja WPA i WPA2 preporuča se korištenje AES algoritma obzirom da je jedino putem tog algoritma moguće iskoristiti 802.11n standard u potpunosti (puna propusnost) dok je u slučaju korištenja TKIP algoritma sustav limitiran na 150Mbps.

Postoji i velik broj dodatnih opcija vezanih uz bežične mreže koje je moguće podešavati (poput WMM-a, korištenje isključivo definiranih WiFi kanala, definiranje širine korištenog kanala, itd.) no u svrhu jednostavnosti korištenja, korisnik ima pristup samo osnovnim (gore navedenim) opcijama. Za sve dodatne opcije koje je potrebno konfigurirati, korisnik se obraća svom lokalnom administratoru ili ukoliko takva osoba ne postoji, administratoru sustava za centralno upravljanje.

U budućim revizijama sustava za centralno upravljanje biti će implementirana i podrška za klastering bežičnih usmjerivača. Ukoliko korisnik želi opskrbiti veće područje WiFi signalom biti će potrebno koristiti više bežičnih usmjernika kako bi se osigurala adekvatna pokrivenost. U tu svrhu koristi se klastering – tj. grupiranje više usmjernika za sinkroni rad.

U radu sa klaster grupama koriste se identične opcije kako su navedene u WiFi modulu za zasebne usmjernike no postavke će se primjenjivati na klaster grupu proizvoljnog imena. Dodavanjem upravljivih usmjernika pojedinom korisničkom računu omogućuje se dodavanje tih uređaja u željenu klaster grupu. Ovo rezultira time da više uređaja emitira istu mrežu (ili više njih) te se korisnici tih mreža mogu automatski spajati na bilo koji uređaj koji u datom trenutku emitira kvalitetniji signal.

3.2.2. VPN modul

Kao proširenje osnovnih mogućnosti sustava korisnicima čija oprema to podržava može biti dodatno omogućen pristup i VPN modulu. U VPN modulu korisnik može kreirati neograničen broj korisničkih profila koji se mogu koristiti za vanjsko spajanje na lokalnu mrežu i pristup lokalnim mrežnim resursima (npr. dijeljeni mrežni direktorij, printer, videonadzor, itd.).

Sustav podržava sljedeće VPN konfiguracije: PPTP, L2TP w/ IPSEC, OpenVPN.

PPTP – jednostavna i hardverski najnezahtjevnija opcija, no i najnesigurnija. Koristi se do 128bitna enkripcija koju je vrlo lako moguće dešifrirati uz današnje lako dostupne alate za tu svrhu. Kao takav, uklonjen je kao podržani VPN protokol sa svih MACOS i iOS uređaja (Apple). Unatoč tome, i dalje je jedan od najkorištenijih protokola za VPN spajanje zbog jednostavnosti korištenja i integracijom sa Windows operativnim sustavima.

L2TP w/ IPSEC - kao najbolji omjer brzine, sigurnosti i jednostavnosti korištenja, ova varijanta osigurava sigurnu vezu, ima podršku za autorizaciju certifikatima te je podržana na svim većim platformama (MACOS/iOS, Windows, Linux, Android, …)

OpenVPN – najjednostavnija opcija korištenja VPNa, podjednako sigurna kao i L2TP w/ IPSEC (AES256 – SHA1), no zahtjeva instalaciju dodatnog softvera na uređaj sa kojeg se spaja na VPN mrežu. Nakon instalacije softvera, korisnik sustava mora samo pokrenuti konfiguracijsku datoteku kako bi se sve postavke učitale (nije potrebna nikakva dodatna konfiguracija).

U VPN modulu, korisnik ima uvid u kreirane VPN korisnike, može mijenjati parametre pojedinog korisnika, te istog obrisati. Prilikom dodavanja VPN korisnika mora se definirati sljedeće:

- ime korisnika (username)
- željena lozinka
- željeni protokol

Također, kao i u slučaju WiFi modula, postoji mogućnost izmjene dodatnih naprednih opcija (pristup željenoj mreži, ograničavanje konekcije na jednog korisnika aktivnog korisnika po korisničkom imenu, itd.).

Detaljnije o opcijama:

Ime korisnika (username) – definiranje korisničkog imena za VPN konekciju. Minimalna duljina imena je jedan znak.

Lozinka (password) – definiranje korisničke zaporke. Iako je tehnički limit 1 znak (na opremi), sustav zahtjeva kompleksniju zaporku (minimalno 8 znakova, te minimalno kombinacija dva od sljedećih četiri uvjeta: velika slova, mala slova, brojevi, specijalni znakovi).

Željeni protokol – ovdje se bira između PPTP, L2TP w/IPSEC i OpenVPN sustava.

Od dodatnih opcija tu su:

Pristup željenoj mreži – ovdje korisnik može odabrati kojoj mreži će VPN korisnik imati pristup. Ukoliko korisnik ima više mrežnih segmenata na usmjerniku kojim upravlja, može ih odabrati više. Ukoliko se ova opcija ne aktivira, VPN korisnik nativno ima pristup svim mrežama.

Primjer korištenja ove opcije bi bio da korisnik iznajmljuje poslovni prostor trećoj strani te želi omogućiti trećoj strani vanjski pristup mreži koja je bila kreirana za potrebe unajmljivača prostora (i samo toj mreži).

Limit konekcije po korisniku – ukoliko je to potrebno, korisnik može aktivirati ovu opciju koja će ograničiti VPN korisnika na maksimalno jednu istovremenu konekciju sa svojim korisničkim imenom. Ovo je korisno ukoliko se želi osigurati da se VPN korisničko ime i lozinka ne koristi od strane više ljudi istovremeno te da se može pratiti potrošnja prometa po korisniku.

Limit brzine (U/D) – U ovoj sekciji je moguće definirati limit propusnosti za pojedinog VPN korisnika. Limit se definira odvojeno za upload i download (slanje i primanje podataka od strane VPN servera). Opcija je korisna ukoliko lokacija na kojoj je implementiran usmjernik ima sporu internet vezu pa se želi osigurati da VPN korisnici ne mogu potrošiti svu dostupnu propusnost ili postoje tehnička ograničenja poput korištenja ADSL-a na lokaciji gdje je brzina slanja podataka višestruko manja od brzine primanja te je takav sustav osjetljiv na opterećenja u uploadu (ukoliko se upload na ADSL linku optereti latencija paketa u dolazu (download) će eksponencijalno narasti efektivno onemogućavajući normalan pristup internetu).

Generalno, kod aktivacije VPN modula za pojedinog korisnika sustav automatski konfigurira dostupne VPN servere kako bi krajnji korisnik mogao izrađivati VPN račune i vezati ih za dostupne VPN servere (PPTP, L2TP, OpenVPN).

Kod inicijalne aktivacije VPN servera kreira se zasebni mrežni segment u koji će se spajati svi VPN korisnici (neovisno o korištenoj varijanti VPN servera) te se radi NAT kako bi se omogućio pristup ostalim mrežnim segmentima – ovisno o odabiru korisnika prilikom izrade VPN računa (sekcija *Pristup željenoj mreži*).

Također, kako je sustav koncipiran kao plug-and-play varijanta za što jednostavnije korištenje, tako da se sam usmjernik kojim se upravlja nalazi u lokalnoj mreži ISP usmjernika, stoga je potrebno ili podesiti statičku IP adresu na usmjerniku kojim se upravlja i podesiti prosljeđivanje portova na ISP usmjerniku ili postaviti ISP usmjernik u bridge mod kako bi usmjernik kojim se upravlja bio direktno spojen na internet.

U slučaju prosljeđivanja portova potrebno je propustiti sljedeće portove:

TIP VPN-A	PROTOKOL	PORT	OPIS
PPTP	TCP	1723	PPTP server
PPTP	GRE	n/a	Enkapsulacija PPTP prometa

L2TP W/ IPSEC	UDP	1701	L2TP server
L2TP W/ IPSEC	UDP	500	IKEv1, IKEv2
L2TP W/ IPSEC	UDP	4500	IKEv1, IKEv2
L2TP W/ IPSEC	ESP	n/a	Enkapsulacija IPSEC prometa
OPENVPN	TCP/UDP	1194	OpenVPN server. Ovisno o korištenom uređaju, koristi se ili TCP ili UDP protokol.

Tablica 3.1 - korišteni portovi kod dostupnih VPN servera

3.2.3. Modul za upravljanje korisnicima

Najbitniji modul je modul za upravljanje korisnicima – kao takav dostupan je samo administratorima sustava te se putem ovog modula ne mogu administrirati korisnički usmjernici. Jedina zadaća ovog modula je izrada, aktivacija i deaktivacija korisnika sustava i podešavanje opcija vezanih uz korisnike.

Prilikom izrade novog korisnika definiraju se sljedeće stvari:

Korisničko ime – ovdje se definira korisničko ime za pristup sustavu centralnog upravljanja. Korisničko ime mora biti unikatno te sustav automatski provjerava da li već postoji korisnik istog naziva.

Lozinka – definira se željena lozinka za korisnički račun. Kao i kod izrade VPN korisnika sustav zahtjeva kompleksniju zaporku (minimalno 8 znakova, te minimalno kombinacija dva od sljedećih četiri uvjeta: velika slova, mala slova, brojevi, specijalni znakovi).

Email korisnika – ovdje se unosi email adresa krajnjeg korisnika. Na ovu adresu će dolaziti obavijesti o isteku licence, zaboravljenoj lozinki, te će generalno biti korištena kao primarni kontakt sa korisnikom od strane administratora sustava centralnog upravljanja (ukoliko za to postoji potreba).

Aktivan do – ovdje se unosi datum do kada je korisnički račun aktivan. Za potrebe demo licence definira se rok od jedan mjesec. Standardne opcije licenciranja su jedna, dvije ili tri godine. Moguće je polje ostaviti i prazno te u tom slučaju korisnički račun nema vremenski limit.

Aktivan (DA/NE) – u ovom se dijelu definira je li korisnik aktivan ili ne. Ukoliko istekne definirani vremenski period i korisnik ne odluči produljiti licencu, sustav će tog korisnika automatski označiti kao neaktivnog. Također, status je moguće mijenjati proizvoljno kroz sustav izmjene parametara korisnika.

Prilikom kreacije novog korisnika sustava automatski se za tog korisnika kreira VPN račun prema centralnom serveru te se generiraju skripte za automatsko provizioniranje korisnikovog usmjernika (kako bi se mogao spojiti na centralni sustav za upravljanje).

Skripta se pohranjuje na serveru te je dostupna samo tom korisniku i samo za vrijeme kada je korisnik ulogiran u sustav.

3.3. Mehanizam komunikacije

Sama aplikacija sustava za centralno upravljanje je pisana u PHP kodu i kao takva ne može ostvariti direktnu komunikaciju sa API sučeljem pojedinog usmjernika – taj jaz premošćuje jedna od tri dostupne API PHP klase otvorenog koda [3].

Autor korištene klase je Denis Basta, te je njegova varijanta te klase ona koja omogućuje najlogičniju i time najjednostavniju upotrebu dostupnih naredbi kroz PHP programski jezik.

Korištenjem takve PHP klase moguće je generiranje zahtjeva prema API sustavu pojedinog usmjernika te dohvat i formatiranje povratnih informacija dobivenih od strane API sustava.

Kao primjer možemo sagledati metodu dohvata ukupnog broja IP adresa dodijeljenih putem DHCP-a sa strane API klase i direktno na terminalu uređaja:

API klasa:

```
$ARRAY = $API->comm("/ip/dhcp-server/lease/print", array(
    "count-only"=> "",
    "~active-address" => "192.168.10.",
));
print_r($ARRAY);
```

Kôd 3.1 Primjer funkcije PHP API klase

Terminal uređaja:

```
/ip dhcp-server lease print count-only where active-address
~"192.168.10."
```

Kôd 3.2 Primjer funkcije naredbenog retka samog uređaja

Obje varijante će pokazati isti rezultat, tj. prikazati će ukupan broj najma IP adresa od strane DHCP servera, i to za željeni mrežni segment (192.168.10.0/24).

Metodom korištenja API poziva koristeći navedenu klasu direktno kroz PHP moguće je u potpunosti administrirati podržane uređaje kroz aplikaciju pisanu u PHP programskom jeziku. U kontekstu sustava za centralno administriranje bežičnih mreža jedan od primjera upotrebe je i pregled trenutno spojenih uređaja na mrežu koja se administrira.

Primjer pregleda statistike direktno na samom uređaju (prazna polja izostavljena):

```
/interface wireless registration-table print
```

#	INTERFACE	MAC-ADDRESS	AP	SIGNAL-STRENGTH	TX-RATE	UPTIME
0	wlan1	D4:CA:6D:89:F9:1F	no	-54dBm@1Mbps	240M…	3d12h5m4s
1	wlan1	30:07:4D:A4:6B:C5	no	-59dBm@1Mbps	117M…	4h8s
2	wlan1	00:87:01:62:02:22	no	-59dBm@1Mbps	54Mbps	3h58m16s
3	wlan1	8C:F5:A3:BB:DF:A2	no	-54dBm@24Mbps	144....	3h2m18s

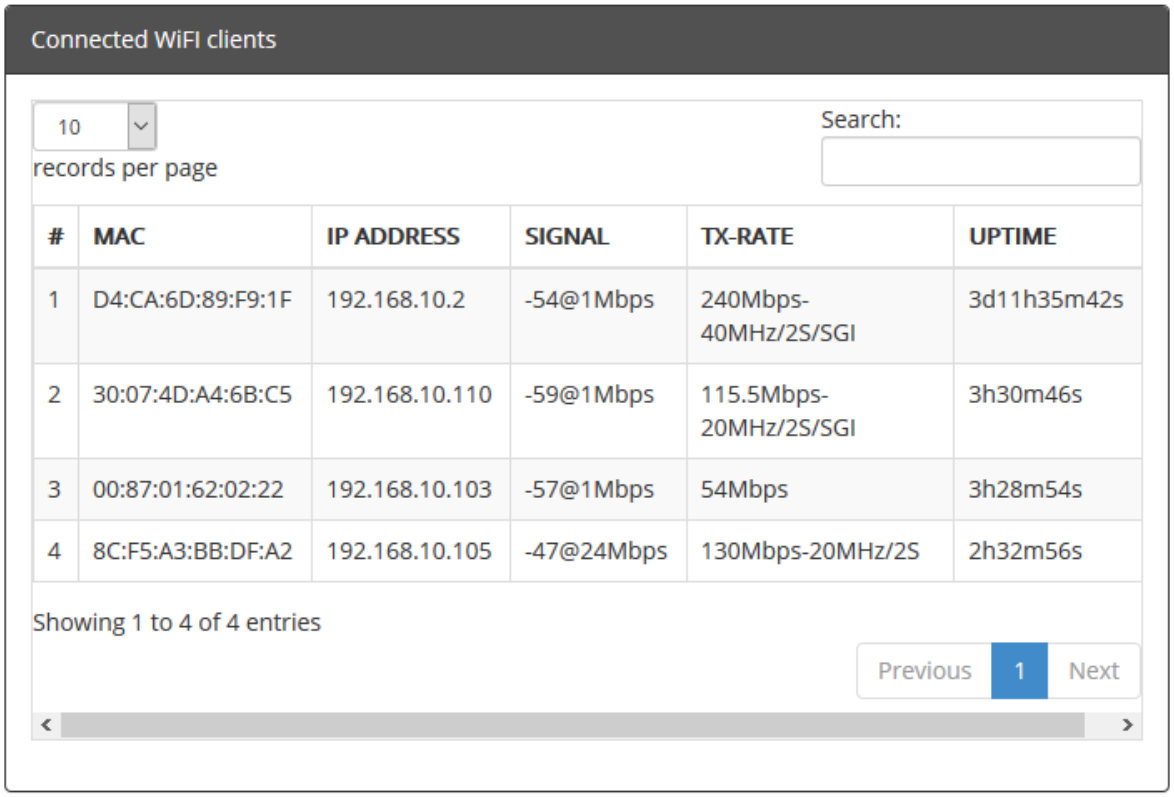
Isti taj upit možemo zadati i putem PHP klase te povratnu informaciju prikazati na način koji nam odgovara:

```
<?php
…
        $ARRAY = $API-
>comm("/interface/wireless/registration-table/print");
?>
…
<table class="table table-striped table-bordered table-hover"
id="dataTables-example">
<thead>
<tr>
```

```
<th>#</th>
<th>MAC</th>
<th>IP ADDRESS</th>
<th>SIGNAL</th>
<th>TX-RATE</th>
<th>UPTIME</th>
</tr>
</thead>
<tbody>
<?php
$num =count($ARRAY);
for($i=0; $i<$num; $i++){
$no=$i+1;
echo "<tr>";
echo "<td>".$no."</td>";
echo "<td>".$ARRAY[$i]['mac-address']."</td>";
echo "<td>".$ARRAY[$i]['last-ip']."</td>";
echo "<td>".$ARRAY[$i]['signal-strength']."</td>";
echo "<td>".$ARRAY[$i]['tx-rate']."</td>";
echo "<td>".$ARRAY[$i]['uptime']."</td>";
echo "</tr>";
}
?>
</tbody>
</table>
```

Kôd 3.3 Primjer PHP implementacije korištenja API poziva

Rezultat:



Slika 3.1 Prikaz rezultata upita sustavu putem PHP klase formatiran kroz željeni CSS

Iz primjera se lako da uvidjeti potencijal takve upotrebe te se po potrebi može omogućiti potpuna kontrola uređaja kroz estetski prihvatljivo korisničko sučelje sa dodatnim funkcionalnostima koje nativno uređaji nemaju (poput dodatnih objašnjenja, primjera, URL hiperlinkova za reference za primjere upotrebe, itd.).

4. Sigurnost i zaštita

Bez obzira na korištenu tehnologiju umrežavanja, korištene protokole i topologiju, uvijek treba brinuti o zaštiti sustava i korisničkih podataka. U tu svrhu bitno je osigurati višeslojnu zaštitu, osigurati zaštitne mehanizme, osigurati zalihost u svakom segmentu sustava te kroz pomno planiranje sustava osigurati optimalan i siguran rad sustava.

4.1. L2 / L3 zaštita

U kontekstu mrežne povezanosti svih komponenti sustava, pa tako i samih klijenata sustava, bitno je osigurati logičnu segmentaciju i segregaciju komponenti sustava već od najnižih slojeva[4]. U tu svrhu svaka se komponenta (server baze podataka, aplikacijski (web) server, edge usmjernik / vatrozid, klijenti, …) nalazi na svom zasebnom mrežnom segmentu te je zadaća glavog usmjernika da kroz *access liste (ACL)* definira koji sustav može pristupiti drugom sustavu[5]. Primjer ovoga bi bio da krajnji klijent može pristupiti aplikacijskom serveru kako bi mogao administrirati svoje uređaje, no ne može pristupiti serveru baze podataka niti ostalim uređajima drugih klijenata.

4.2. Web server – upravljačka aplikacija

Kako bi sustav bio dostupan korisnicima i to sa različitih uređaja/platformi, kao aplikativno rješenje koristi se web aplikacija pisana u PHP kodu. Sama aplikacija se izvodi na CentOS7 serverima, tj. na Apache web poslužitelju zbog smanjenih troškova licenciranja i mogućnosti koje sustav nudi.

Glavne primjenjive značajke takvog sustava su iznimno niski zahtjevi za resursima, mogućnost klasteringa za osiguravanje visoke dostupnosti, kao i integrirana podrška za *selinux* koja pruža dodatni novo zaštite.

Iako se za potrebe web poslužitelja koriste lokalno kolocirani serveri kao dodatni nivo sigurnosti sam PHP kod se kriptira kako bi se minimizirale šanse zloupotrebe. Kriptiranje koda je preporučivo pogotovo ukoliko se koriste vanjski web serveri do kojih pristup imaju treće strane.

4.3. Baza podataka

Obzirom da se radi o sustavu koji mora pamtiti konfiguracije svih upravljivih usmjernika, kao i podatke u klijentima koji ih administriraju, koristi se MariaDB baza podataka. Ova je baza podataka odabrana jer je nativno podržana na CentOS7 operativnom sustavu koji se koristi kao primarni operativni sustav za server baze podataka, podržava sustave visoke dostupnosti, te ne generira dodatne troškove u smislu licenciranja.

Za potrebe podešavanja visoke dostupnosti u sustavu baze podataka koristi se MariaDB Galera klaster sa 3 servera, kako bi se osigurao integritet podataka i izbjegli problemi sa donošenjem kvoruma u slučaju ispada jednog od servera.

Zbog nadolazeće GDPR regulative potrebno je obratiti posebnu pozornost na osobne podatke koji se čuvaju u bazi, tj. omogućiti da se može osigurati *pravo na zaborav* ukoliko klijent to zatraži[6]. U tu svrhu se svi osobni podaci korisnika spremaju u zasebnu kriptiranu tablicu koja je sa klijentom povezana putem ID korisnika (primarni ključ). U slučaju potrebe za uklanjanjem korisnika iz baze (i svih backupova) ukoliko to korisnik zatraži, dovoljno je samo ukloniti tog korisnika iz trenutne verzije baze, obrisati private key za pristup kriptiranim tablicama i generirati novi. Na ovaj način se iz prijašnjih backupova baze ne može pristupiti osobnim podacima (iako oni postoje) jer su kriptirani, i time se može zadovoljiti forma GDPR zahtjeva.

4.4. Zalihost i sigurnosna pohrana podataka

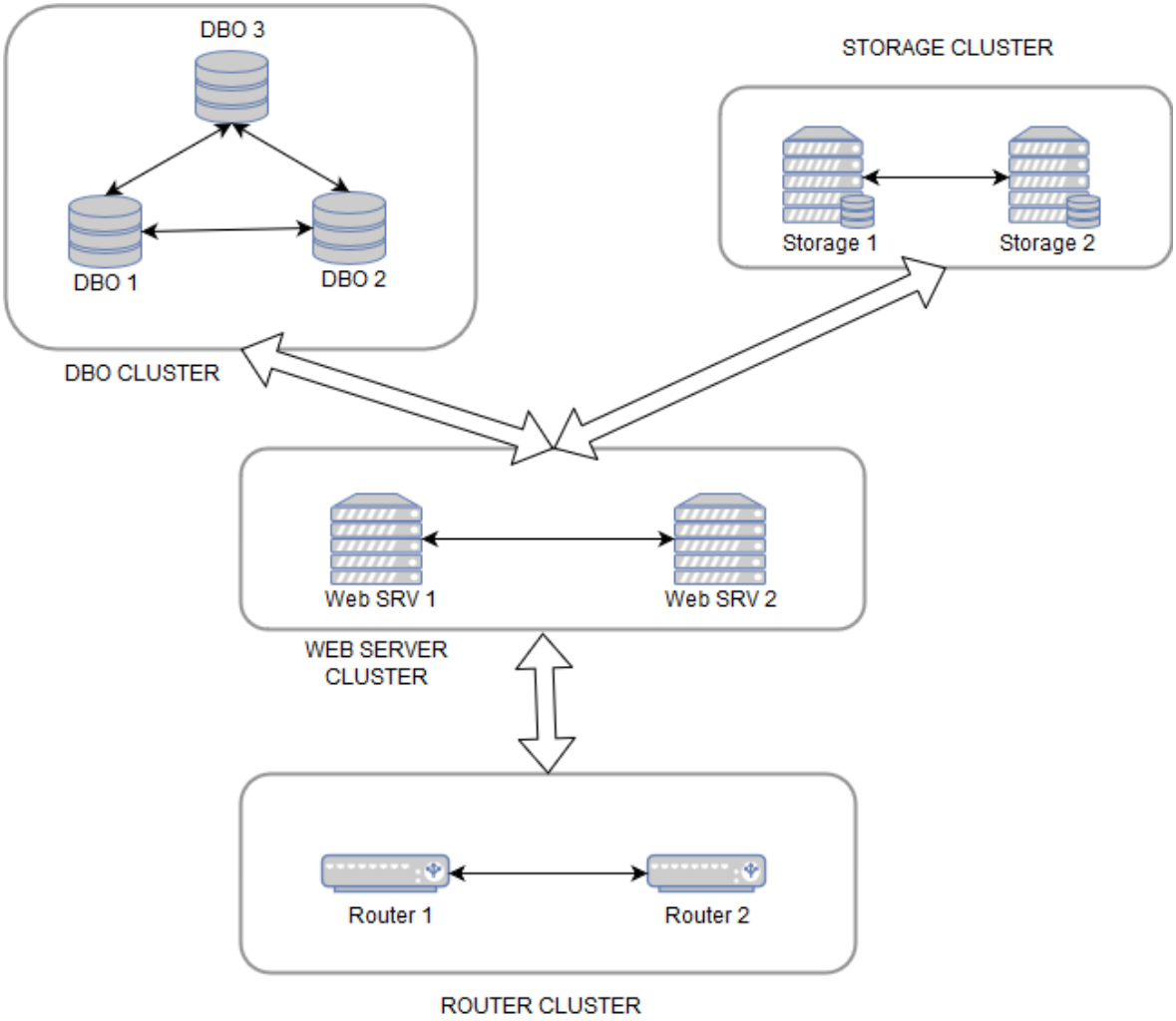
Kako bi se osigurala visoka dostupnost servisa sve komponente sustava moraju imati failover, tj. backup varijantu. U tu svrhu se za svaki dio sustava osigurava minimalno jedan redundantni sustav.

Gledajući sustav izvana, prvi korak za osiguravanje visoke dostupnosti je DNS. Potrebno je koristiti barem 2 DNS servera kako bi se osigurali da klijenti mogu doći do IP adrese usmjernika prilikom spajanja na sustav unatoč ispadu jednog od njih.

Sljedeći korak su usmjernici – kao glavni ulaz u sustav također je potrebno osigurati dostupnost u slučaju kvara opreme, stoga se koriste 2 usmjernika u VRRP grupi (active/standby mod).

Web serveri na kojima se izvodi sama aplikacija također moraju imati podešen sustav visoke dostupnosti, no kako bi to bilo izvedivo moraju koristiti zajedničku pohranu podataka na kojoj će sama aplikacija biti pohranjena. Za potrebe toga se podešava klaster za pohranu sa 2 servera u međusobnoj replikaciji putem ISCSI protokola.

Baza podataka je bazirana na 3 Centos7 servera, tj. na MariaDB Galera klaster sustavu koji su u multi-master modu osiguravajući konstantnu replikaciju podataka kroz sva tri servera uz minimalnu latenciju.



Slika 4.1 Detaljniji shematski prikaz klastera unutar sustava

Ovom se segmentacijom dijelova sustava i osiguravanjem njihovih redundantnih kopija osigurava visoka dostupnost sustava, no to i dalje ne osigurava od gubitka podataka.

Kako bi se doskočilo tom problemu, podešava se automatska sigurnosna pohrana svih komponenti sustava i to u proizvoljnim intervalima ovisno o dinamici izmjene sadržaja

pojedinog sustava. Primjerice, baza podataka se tretira kao visoko dinamičan sustav te je poželjno osigurati što češće sigurnosne kopije – obzirom na ciljano tržište, u godinu dana procijenjena je veličina baze od ~250MB, stoga se baza arhivira svakih 30 minuta. Sama PHP aplikacija se ne mijenja tako često (točnije, isključivo kada se implementira nova funkcionalnost ili ispravlja eventualna postojeća greška u sustavu), stoga je prijedlog da se aplikacija arhivira jednom dnevno. Od ostalih stvari tu su konfiguracije glavnih usmjernika koje se mijenjaju iznimno rijetko, pa nije potrebno raditi česte sigurnosne kopije – dovoljno je jednom mjesečno.

Preporuka za sve sigurnosne kopije je da se spremaju i lokalno na dedicirani sustav za pohranu sigurnosnih kopija i na prostor predviđen za to u oblaku. U obje varijante potrebno je sigurnosne kopije kriptirati kako bi se održao željeni nivo sigurnosti i udovoljilo normama GDPR regulative.

5. Usporedba sustava sa konkurentskim riješenjima

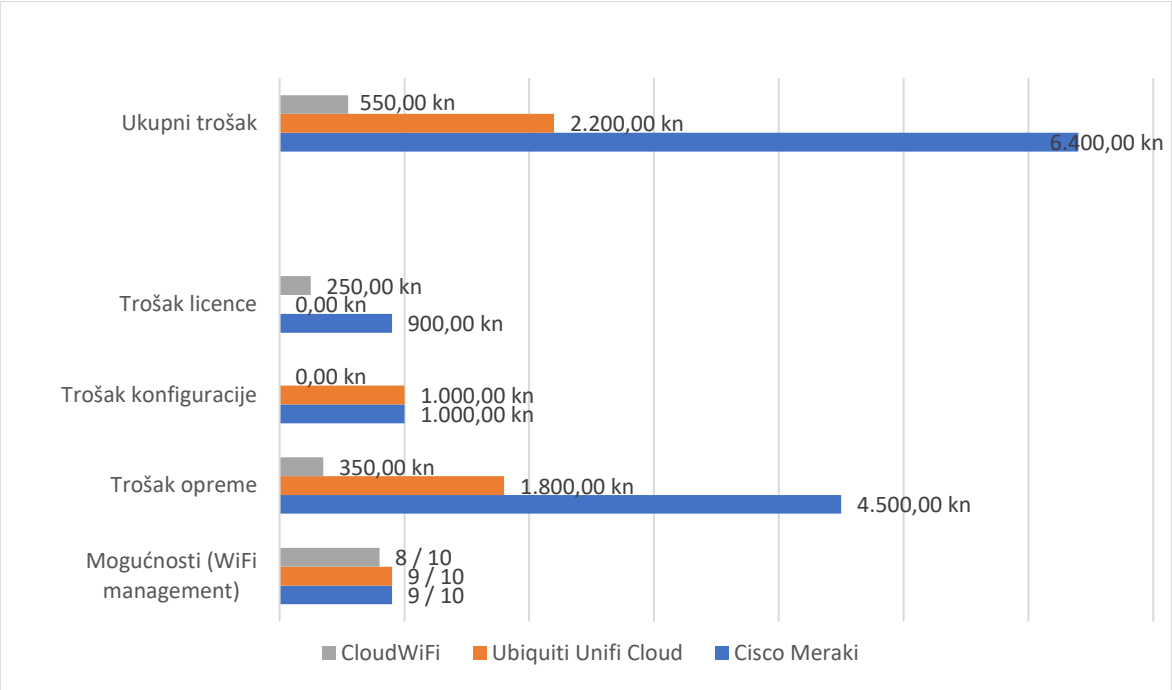
Kao dva glavna konkurentska rješenja mogu se navesti Cisco Meraki i Ubiquiti Unifi Cloud platforme. Iako u suštini u kontekstu bežičnih mreža nude iste stvari kao i sustav koji se obrađuje u ovom radu, bitno se razlikuju od istog.

Konkretno, Cisco Meraki platforma u ovom stadiju razvoja u sebe integrira pregršt dodatnih opcija i naveliko izlazi iz okvira „WiFi cloud management“ platforme sa kojom je sama platforma inicijalno krenula. Za krajnjeg klijenta ovo znači nebrojeno mnogo dodatnih opcija i mogućih načina konfiguracije koje samo zbunjuju ukoliko korisnik nije upoznat sa svim aspektima palete ponude koja se kroz tu platformu nudi. Valja u obzir uzeti i cijenu takve usluge – 900,00kn po uređaju za osnovnu licencu na godinu dana, te dodatnih ~4.500,00kn za pojedini uređaj.

Ubiquiti sa druge strane trenutno ne naplaćuje licencu za korištenje svoje Unifi Cloud usluge (licenca je uključena u paketu sa uređajem), no kako bi se koristila ta usluga potrebno je nabaviti dodatne usmjernike i rekonfigurirati postojeću mrežnu opremu za rad sa novom opremom – ovdje se u potpunosti promašuje pojam plug-and-play rješenja, tj. sustav nije predviđen za tržište kojima je to preduvjet. Također, treba uzeti u obzir i cijenu same opreme – od 1.800,00kn na dalje za osnovni set (bežični usmjernik + centralni usmjernik). Po pitanju samih funkcionalnosti, Unifi Cloud platforma kaska za Cisco Meraki platformom u globalu, no to je i očekivano obzirom da Cisco nudi integraciju sa ostalom paletom proizvoda (vatrozidi, usmjernici, antivirusna rješenja, itd.).

U usporedbi sa dvije gore navedene platforme, ova platforma je minimalistički nastrojena, sa osnovnim setom opcija koji će zadovoljiti barem 90% korisnika koji takvo što traže. Predviđena cijena licence ovog sustava po usmjerniku je 250,00kn godišnje, a cijena kompatibilne opreme se kreće od 150,00kn na dalje po usmjerniku (ovisno o potrebama – best buy od 350,00kn na dalje).

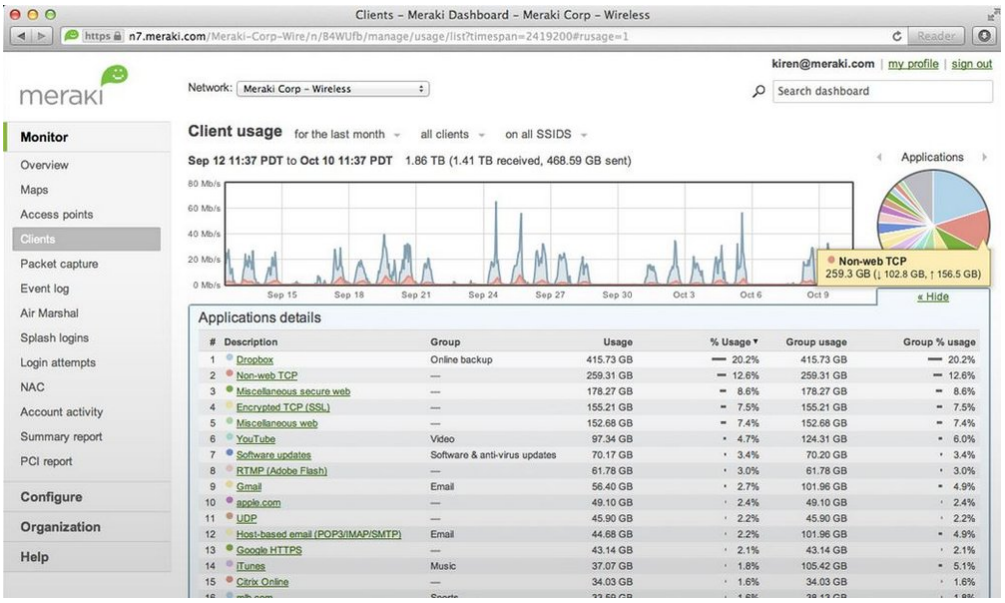
Uzeći u obzir cijenu takve usluge i cijenu kompatibilnih uređaja lako je uvidjeti konkurentnost takve platforme u ciljanim regijama.



Slika 5.1 Usporedba Cloud WiFi rješenja

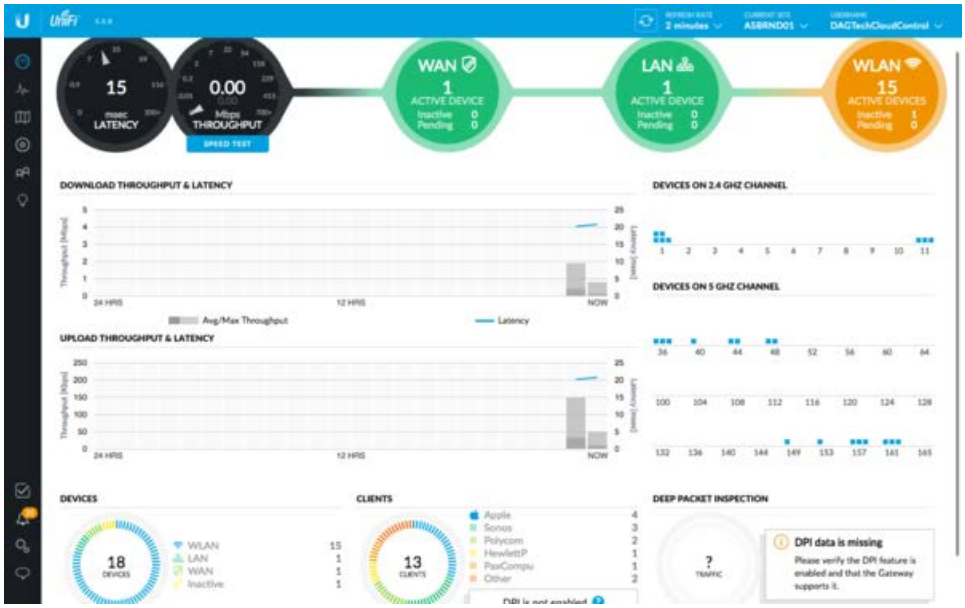
U usporedbi troškova korišteni su best buy modeli za odgovarajuću platformu, tj. za Cisco Meraki je odabran Cisco MR33 uređaj, za Unifi Cloud UAP-AC-LR sa pripadajućim gatewayem, te za CloudWiFi platformu Mikrotik RB952Ui-5ac2nD.

Trošak rada se računao po satnici od 250,00kn po satu te je uzet prosjek od pola radnog dana (4h) za spajanje i konfiguraciju sustava.



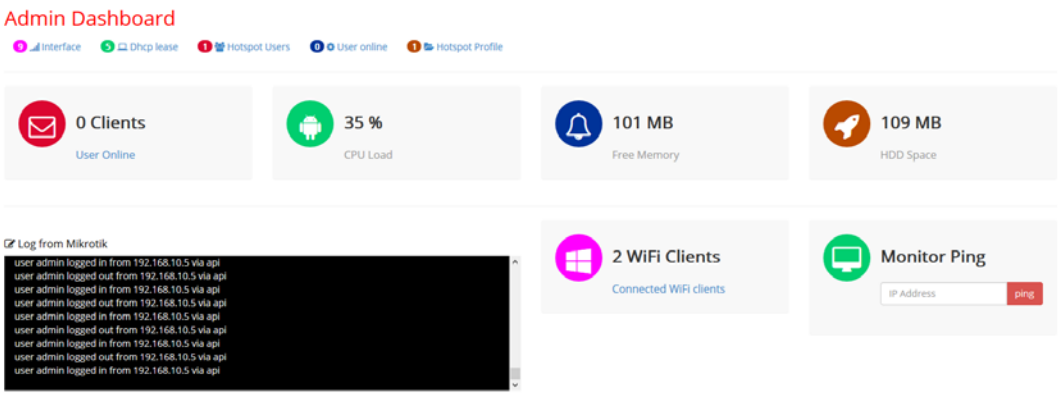
Slika 5.2 Primjer Cisco Meraki konzolnog pregleda

Iz navedene slike (Slika 5.2) vidi se opsežnost Cisco Meraki platforme – unatoč tome što je najnaprednija platforma i nudi razne dodatne funkcionalnosti, čest je odabir tek kod velikih tvrtki u Enterprise segmentu zbog svoje kompleksnosti i cijene.



Slika 5.3 Primjer Unifi Cloud konzolnog pregleda

Unifi Cloud platforma je znatno jednostavnija od Meraki platforme te je zbog toga prihvatljivija manjim tvrtkama, no i dalje nudi velik odabir dodatnih opcija koje korisnicima u SOHO segmentu ne odgovaraju jer ili nemaju potrebe za njima ili nemaju potrebna znanja da ih implementiraju.



Slika 5.4 Primjer CloudWiFi konzolnog pregleda

CloudWiFi platforma nudi samo osnovne opcije oko upravljanja bežičnih mreža, no baš te opcije su one koje korisnicima najviše i trebaju.

Zaključak

Sustavi centralnog upravljanja u današnje vrijeme svakako nisu novost, no predloženi koncept takvog sustava u usporedbi sa ostalim rješenjima koji pokušavaju integrirati što je više moguće opcija u sebe je i više nego dobrodošao. Kad se sagledaju sve potrebne radnje, oprema i licence da se takav sustav osposobi lako je doći do zaključka da se uz sve današnje tehnologije takvo što relativno lako može postići te je isplativost takvog pothvata gotovo garantirana ukoliko se ne radi isključivo o osobnim potrebama administracije tog tipa. Razvoj sustava koji je sa korisničke strane jednostavan i siguran, a sa strane administracije pouzdan i brz, nije nedostižan cilj već realnost današnjice.

Uspoređujući sa ostalim rješenjima, CloudWiFi adekvatno pokriva ciljano tržište (SOHO), dok su ostale navedene platforme, iako funkcionalno nude slične stvari, predviđene za druge tržišne segmente, tj. Cisco Meraki za Enterprise i Unifi Cloud za Mid/Small Business. Uzeći u obzir ukupni trošak, nepostojanje preduvjeta poznavanja mreža i IT sustava, te plug-and-play varijantu korištenja za ovakav se sustav očekuje da će popuniti prazninu u lokalnoj ponudi SOHO tržišta.

Popis kratica

ISP	*Internet Service Provider*	Pružatelj internet usluga
VPN	*Virtual Private Network*	Virtualna L2/L3 mreža koja osigurava siguran protok podataka kroz kriptirani tunel putem interneta
IPSEC	*Internet Protocol Security*	Mrežni protokol koji autentificira i kriptira podatke koji se prenose putem takve mreže
AES-256	*Advanced Encryption Standard*	Zadnji standard za enkripciju, 256bitni
SSID	*Service Set Identifier*	Ime bežične mreže
LAN	*Local Area Network*	Lokalna računalna mreža
Mpbs	*Megabit per second*	Jedinica količine propusnosti podataka
WMM	*WiFi Multimedia*	Dio 802.11e standarda koji je zadužen za prioritizaciju paketa na mreži
ADSL	*Asymmetric digital subscriber line*	Tehnologija mrežne komunikacije
NAT	*Network address translation*	Metoda izmjene dolaznih/odlaznih IP adresa u mrežnom paketu
IKEv1/v2	*Internet Key Exchange*	Sigurnosni protokol korišten od strane IPSEC-a
PPTP	*Point-to-Point Tunneling Protocol*	Mrežni protokol koji se koristi za uspostavu VPN veze
L2TP	*Layer 2 Tunneling Protocol*	Mrežni protokol koji se koristi za uspostavu VPN veze
ACL	*Access Control List*	Lista dozvola ili blokada mrežnog prometa koja se odnosi na jednu ili više mreža
DNS	*Domain Name Server*	Hijerarhijski decentraliziran sustav imenovanja računala
ISCSI	*Internet Small Computer Systems Interface*	IP protokol prenosi SCSI naredbe putem mreže, koristi se za sustave podatkovne pohrane
VRRP	*Virtual Router Redundancy Protocol*	Mrežni protokol koji se koristi za izradu usmjernika

API	*Application programming interface*	Set podrutina, protokola i alata u izgradnji aplikativnog riješenja
URL	*Uniform Resource Locator*	Referenca na web lokaciju
PHP	*Personal Home Page / PHP: Hypertext Preprocessor*	Programski jezik za generalnu upotrebu
SELINUX	*Security-Enhanced Linux*	Linux kernel sigurnosni modul

Popis slika

Slika 2.1 Shema komponenti sustava za upravljanje..... 4

Slika 2.2 Dijagram toka dodavanja upravljivog uređaja sustavu 5

Slika 2.3 Prikaz ručnog dodavanja uređaja u sustav 8

Slika 3.2 Prikaz rezultata upita sustavu putem PHP klase formatiran kroz željeni CSS..... 20

Slika 4.1 Detaljniji shematski prikaz klastera unutar sustava 23

Slika 5.1 Usporedba Cloud WiFi rješenja 26

Slika 5.2 Primjer Cisco Meraki konzolnog pregleda..... 26

Slika 5.3 Primjer Unifi Cloud konzolnog pregleda 27

Slika 5.4 Primjer CloudWiFi konzolnog pregleda 27

Popis tablica

Tablica 3.1 - korišteni portovi kod dostupnih VPN servera 16

Popis kôdova

Kôd 2.1 Naredba za provizioniranje usmjernika 6

Kôd 2.2 Naredbe za uklanjanje zaostale konfiguracije 7

Kôd 2.3 Naredbe za uspostavu veze usmjernika sa centralnim sustavom..... 7

Kôd 2.4 Naredbe za izradu korisnika za administraciju na uređaju 8

Kôd 3.1 Primjer funkcije PHP API klase 17

Kôd 3.2 Primjer funkcije naredbenog retka samog uređaja 18

Kôd 3.3 Primjer PHP implementacije korištenja API poziva 19

Literatura

Svaki autor piše popis literature na kraju rada. Popis literature se piše stilom literatura.

[1] Iwona Dolińska, Mariusz Jakubowski, Antoni Masiukiewicz (2017) - Interference comparison in Wi-Fi 2.4 GHz and 5 GHz bands, ISBN: 978-1-5090-5689-7, Izdavač: IEEE.

[2] 802.11-2016 - IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ISBN: 978-1-5044-3645-8, Izdavač: IEEE.

[3] API PHP package v1.6; Denis Basta; 2016; https://wiki.mikrotik.com/wiki/API_PHP_package

[4] Kevin Wallace; CCNP Routing and switching, ROUTE 300-101; (2014); ISBN: 978-1-58720-559-0.

[5] Jeff Sedayao; Cisco IOS Access Lists; (2001); ISBN: 1565923855; Izdavač: O'Reilly Media, Inc..

[6] REGULATION (EU) 2016/... OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), stavka 65.