PRISTUP I NADZOR DISTRIBUIRANIH MREŽA

Jonjić, Ivan

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Specijalistički diplomski stručni studij Informacijske tehnologije

IVAN JONJIĆ

Z A V R Š N I R A D

PRISTUP I NADZOR DISTRIBUIRANIH MREŽA

Split, rujan 2021.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Specijalistički diplomski stručni studij Informacijske tehnologije

Predmet: Upravljanje poslužiteljima otvorenog koda

Z A V R Š N I R A D

Kandidat: Ivan Jonjić

Naslov rada: Pristup i nadzor distribuiranih mreža

Mentor: dipl.ing Valentini Kožica, predavač

Split, rujan 2021.

SADRŽAJ

SAŽETAK

Cilj ovog završnog rada je implementacija sustava koji omogućava pristup distribuiranim mrežama i nadzor istih. Nakon uvodnog dijela, predstavljene su tehnologije i sastavnice koje su korištene u samoj implementaciji, čiji je postupak spajanja i postavljanja opisan u trećem poglavlju.

Za izgradnju sustava korišten je MikroTIk RouterOS Cloud Hosted Router, inačica usmjernika kojeg je moguće pokrenuti na virtualnom stroju, te Checkmk, sustav nadzora otvorenog koda koji omogućuje upravljanje cjelokupnom IT infrastrukturom. MikroTik Cloud Hosted Router služi kao centralna točka ovog sustava te omogućava upravljanje njegovim mrežnim komponentama. Nadzor i pristup klijentskim uređajima i sustavu Checkmk, omogućen je pomoću virtualnog PPTP tunela, od glavnog usmjernika prema krajnjem uređaju. Checkmk omogućuje centralizirani nadzor mrežnih uređaja i usluga, pružajući pritom veliki stupanj fleksibilnosti konfiguracije svih aspekata nadzora. Kao dodatna funkcionalnost, implementiran je sustav obavijesti koji putem elektroničke poruke obavještava administratora o promjenama koje se događaju na Checkmk sustavu.

Ključne riječi:

sustav nadzora, Checkmk, MikroTik Cloud Hosted Router, PPTP

SUMMARY

Access and monitoring of distributed networks

The goal of this final paper is to implement a system that allows access and monitoring of distributed networks. After the introductory part, a detailed overview of the technologies and components used in the development of the system is given, while the process of system implementation is described in the third chapter.

MikroTik RouterOS Cloud Hosted Router, a router that can be run on virtual machines, and Checkmk, an open-source monitoring system that allows management of the entire IT infrastructure, were used to build the system. MikroTik Cloud Hosted Router serves as the central point of this system and enables the management of its network components. Monitoring and access to the client devices and the Checkmk system itself is enabled via a virtual PPTP tunnel, from the main router to the end device. Checkmk offers centralized monitoring of network devices and services while providing a high degree of configuration flexibility in all aspects of monitoring. As an additional function, a notification system that notifies the administrator via e-mail about changes that occur on the Checkmk system, has been implemented.

Keywords:

monitoring system, Checkmk, MikroTik Cloud Hosted Router, PPTP

1. UVOD

U današnje vrijeme, bilo kakav vid poslovanja zahtijeva moderni pristup kada govorimo o načinu realizacije istog. Neovisno o tome kakav je tip poslovanja, bio on u privatnom ili javnom sektoru ili se pak radi o infrastrukturnim projektima kao primjerice izgradnja ili obnova novog hotela, studentskog doma, laboratorija, bolnice, skladišnog prostora itd., potrebno je provesti njihovu informatizaciju. Jedna od sastavnica informatizacije poslovanja je zasigurno i uvođenje lokalne računalne mreže koja se kasnije može koristiti za implementaciju različitih sustava, bilo da se radi od bežičnim (WiFi) mrežama, videonadzoru ili primjerice vatrodojavnim I protuprovalnim sustavima koji koriste internet kako bi bili povezani na centralu. Veličina lokalnih mreža odnosno sustava ovisi o potrebama i može sadržavati više stotina ili tisuća uređaja različite namjene poput mrežnih usmjernika i preklopnika, poslužitelja, kamera, pristupnih točaka, primopredajnih antena, UPS uređaja, pisača ili osobnih računala. No, to mišljenje je često pogrešno, i postoji više razloga za to.

Prvi razlog je sama fizička udaljenost mreže koja se nadzire od lokacije osobe koja održava tu istu mrežu. Zamislite da ta osoba treba svaki dan putovati od Splita do Zagreba ili u drugu državu samo kako bi provjerila radi li mrežni preklopnik ispravno ili postoji li problem sa sustavom videonadzora, što je čest slučaj. Drugi razlog je mogućnost prekida radnog odnosa osobe koja održava tu mrežu te sve informacije o toj mreži se na taj način izgube, poput broja uređaja, vrste, lokacijama, logičkoj shemi itd. Osoba koja dođe na njegovu poziciju zapravo počinje od nule, bez ikakve spoznaje o kakvoj se mreži radi, koliko je složena ili gdje se uređaji nalaze. Također, ljudska ograničenost kada govorimo o vođenju statističkih podataka pokazuje da čovjek nije u stanju aktivno pratiti sve događaje koji se odvijaju na određenom uređaju. Ako se radi o sustavu reda veličine stotine uređaja, za koje je potrebno imati statistiku rada u posljednjih mjesec dana za svaki uređaj pojedinačno ili skupno za cijeli sustav, takav posao nije namijenjen za jednu osobu. Četvrti razlog se odnosi na izmjenu postavki na uređajima. Primjerice, korisnici mreže zahtijevaju otvaranje određenog porta (priključka) na mrežnom usmjerniku kako bi mogli pristupiti poslužitelju na kojem se nalazi poslovna aplikacija koju koriste. Zbog takve male izmjene na postavkama tehničar bi trebao svaki put fizički doći na lokaciju, pristupiti usmjerniku te napraviti potrebne izmjene. Zbog gore navedenih razloga rade se centralizirani sustavi koji omogućuju udaljeni pristup i nadzor mreža.

U ovom završnom radu biti će prikazan postupak izrade samog sustava i prikaz funkcionalnosti sustava za pristup i nadzor mreža. U drugom poglavlju objasnit će se pojmovi koji se vežu uz ovaj sustav i dobiti općenitiji pregled tehnologija koji se koriste u izgradnji takvog sustava. U trećem poglavlju biti će opisana tehnička izvedba izgradnje samog sustava, počevši od osnovnih postavki do onih dodatnih, koji proširuju funkcionalnost istog te čine sami sustav fleksibilnijim.

2. PREGLED KORIŠTENIH TEHNOLOGIJA I SASTAVNICA

2.1. Virtual Private Server (VPS)

Virtual Private Server (VPS) ili virtualni privatni poslužitelj je tehnologija koje se temelji na kreiranju jednog ili više virtualnih poslužitelja na jednom ili više fizičkih poslužitelja. Iako je sama izvedba poslužitelja virtualna, iz perspektive krajnjeg korisnika poslužitelj se ponaša kao i fizički, jedina razlika je što se ne nalazimo u prostoriji u kojem je smješten fizički poslužitelj, već se virtualne instance kreiraju i upravljaju udaljeno. Riječ „privatni“ u nazivu odnosi se na fiksno rezervirane resurse za pojedini virtualni poslužitelj, što znači da pružatelj usluge jamči da će kreirani poslužitelj imati rezervirane resurse u svakom trenutku, bez dijeljenja istih sa ostalim korisnicima, što nije slučaj kod pružatelja web usluga (eng. web hosting) gdje više korisnika istovremeno dijeli jedan ili više poslužitelja.

Kod pružatelja web usluga nedostatak je manjak fleksibilnosti, drugim riječima, korisniku nije omogućeno naprednije podešavanje sustava kao primjerice konfiguracije baze podataka ili instalacija dodatnih servisa aplikacija. Isto tako, resursi koje nudi web hosting su ograničeni, pa se potrebe većine naprednijih korisnika prerastu jako brzo. Suprotno tome, moguće je nabaviti ili iznajmiti namjenski poslužitelj (eng. dedicated server) koji je u suštini fizički poslužitelj na kojeg je moguće instalirati virtualizacijski servis (VMware vSphere, Microsoft Hyper-V, Xen, Red Hat Enterprise Virtualization (RHEV), KVM itd.) te po potrebi na njemu kreirati više virtualnih poslužitelja te ih kasnije konfigurirati po želji sa punim administratorskim ovlastima. U slučaju da ne želimo koristiti virtualizaciju, moguće je na fizički poslužitelj instalirati željeni operacijski sustav kojem bi svi dostupni resursi bili na raspolaganju. Mana namjenskih poslužitelja je u prevelikoj cijeni, te u slučaju da korisnik posjeduje osobni fizički poslužitelj, i u relativno brzom starenju komponenti poslužitelja. Problem starenja komponenti nije prisutan kod pružatelja usluga namjenskih poslužitelja gdje je u cijenu, iako dosta visoku, uključen i prelazak na noviju i bržu opremu (nove generacije procesora, radne memorije, diskova, dodavanje novih tehnologija i mogućnosti itd.)

Virtualni privatni poslužitelj po svom načinu rada je sličan dediciranom poslužitelju, međutim, za puno manju cijenu. Korisniku omogućuje rezervaciju i nadogradnju resursa prema potrebi, instalaciju željenog operacijskog sustava, puni administratorski pristup, jednu ili više

javnih i privatnih adresa, pristupu velikom broju postavki (pravila vatrozida, slika operacijskog sustava, pričuvna kopija, DNS zapisi itd.). Za svrhe ovog završnog rada, iznajmljena su dva virtualna privatna poslužitelja sa sljedećim resursima:

- Jedna virtualna jezgra Intel procesora posljednje generacije
- 2 GB radne memorije
- 55 GB prostora na SSD disku
- 2 TB prometa mjesečno
- 1 javna adresa

Na prvom poslužitelju će biti instaliran MikroTik Cloud Hosted Router, dok će drugi služiti za instalaciju i postavljanje Checkmk okruženja i ostalih servisa.

2.2. MikroTik

MikroTik je tvrtka koja se bavi razvojem mrežne opreme, s naglaskom na razvoj usmjernika. Osnovana je 1996. godine u glavnom gradu Latvije, Rigi. Već 1997. godine, MikroTik je razvio vlastiti operacijski sustav za usmjernike, RouterOS, koji pruža visoki nivo stabilnosti, fleksibilnosti i upravljanja usmjerivačkom komponentom mreže. Pet godina nakon, MikroTik razvija vlastito čvrsto sklopovljeza usmjernike, pod nazivom RouterBoard. MikroTik nudi više od 160 različitih modela mrežne opreme i posluje u 145 zemalja svijeta, a njegova rješenja koriste velike tvrtke i institucije poput Motorole, NASA-e, Ericssona, Vodafone, Siemensa, Nokije, vlade SAD-a itd.

2.2.1. RouterBoard

Kao što je već prethodno spomenuto, RouterBoard je elektronska komponenta svih MikroTik-ovih proizvoda. Ovisno o funkciji uređaja, prilagođava se izrada tiskane ploče pa tako RouterBoard može biti prilagođen funkcionalnostima pristupnih točaka, preklopnika (eng. switch), vatrozida, usmjernika itd. Zajednička osobina gotovo svih modela je napajanje pomoću pasivnog PoE adaptera ili klasično, putem strujnog adaptera.

RouterBoard modeli se dijele na potrošačke modele:

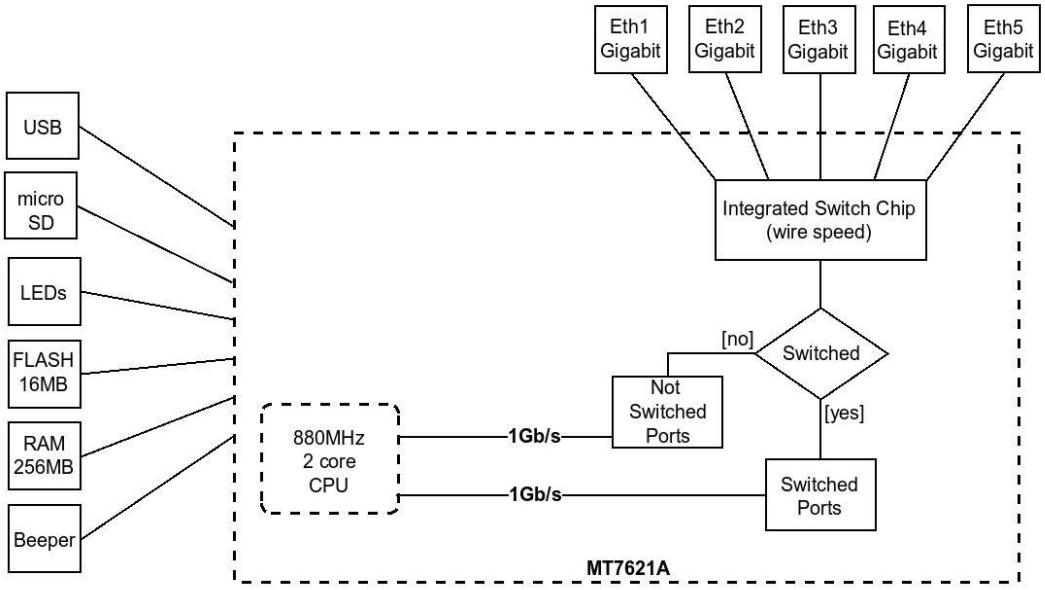
- hEX i hAP - usmjernici početne razine,

- Audience - pristupne točke sa funkcijom MESH tehnologije,
- Chateau LTE12 - višenamjenske pristupne točke sa mogućnošću povezivanja na Internet putem LTE tehnologije,
- mAP - pristupne točke malih dimenzija,
- cAP - pristupne točke za postavljanje na strop,
- wAP - pristupne točke za postavljanje na zidove,
- PWR-LINE - uređaji koji se povezuju putem kućne električne mreže.

Postoje i modeli koji se koriste u telekomunikacijske svrhe:

- RB, CCR, CRS i CSS - usmjernici i preklopnici koji se koriste u srednjim i visokim razinama mreže,
- PowerBox i FiberBox - vanjski usmjernici sa Ethernet i SFP sučeljima s PoE izlazom,
- netPower - vanjski preklopnici velike propusnosti s PoE izlazom,
- OmniTIK - vanjske pristupne točke s ugrađenom omnidirekcijskom antenom,
- SXT, SEXTANT i DISC - antena za okosnicu s ugrađenom usmjerenom antenom,
- mANTBox - vanjska bazna stanica s ugrađenim LTE usmjernikom i usmjerenom antenom,
- Cube Lite60 - vanjska antena za povezivanje od točke do više točke za okruženja malog faktora frekvencijske propusnosti i frekvencijskom spektru od 60 GHz,
- LHG, DynaDish i Wireless Wire - vanjska antena s ugrađenom paraboličnom antenom, za povezivanje od točke do točke na velikim udaljenostima,
- LDF - vanjska antena za povezivanje od točke do točke na velike udaljenosti, za upotrebu unutar standardnih paraboličnih TV antena.
- BaseBox, NetBox i NetMetal - višenamjenski vanjski bežični uređaji s RP-SMA konektorima, koji se koriste s antenama mANT ili drugih proizvođača,
- Groove i Metal - višenamjenski vanjski bežični uređaji u cjevastoj izvedbi, koji se koriste s omni ili yagi antenama,
- LtAP - pristupna točka, LTE usmjernik i GPS uređaj za kretanje vozila.

Primjera radi, u nastavku se nalazi logička blok shema (Slika 1.) koja prikazuje rad RouterBoard tiskane pločice za hEX RB750Gr3 model usmjernika, koji će se koristiti u praktičnom dijelu ovog rada.



Slika 1. Prikaz logičke blok sheme MikroTIk hEX RB750Gr3 usmjernika [1]

Iz dijagrama se može vidjeti da uz standardni procesor koji vrši obradu paketa, MikroTik je implementirao i prespojni modul (eng. switch chip) modul koji preuzima obradu određenih značajki usmjernika, čime se znatno smanjuje opterećenje nad procesorom. Rad prespojnog modula se može i isključiti pri čemu svu kontrolu nad radom pojedinih ethernet sučelja vrši procesor. Veza između čipa i procesora u nekim modelima RouterBoarda ima veću propusnost za razliku od veza između pojedinih sučelja i procesora kada propusnost može biti 1Gbps ili 100 Mbps.

Značajke koje prespojni modul modul može obraditi su:

- blokiranje distribuiranih napada uskraćivanjem resursa(eng. DDOS) korištenjem pravila vatrozida koje funkcioniraju kao crna rupa (eng. black hole rule),
- usmjeravanje među mrežnim mostovima (eng.bridge),
- usmjeravanje među virtualnim mrežama (eng. VLAN),
- spajanje više fizičkih sučelja u jedno logičko sučelje (eng. bonding),

- obrada veza koje su izostavljene od prolaska kroz pravila vatrozida (eng. fasttrack connections)
- obrada pravila usmjeravanja (eng. NAT rules) koja se odnose na ubrzane (eng. fasttrack) konekcije.

Za ostale modele uređaja, izgled logičke sheme je sličan, uz eventualno dodavanje ili uklanjanje modula (moduli za antene, ethernet sučelja ,SFP sučelja, switch čipovi, jezgre procesora itd.).

2.2.2. RouterOS Cloud Hosted Router

RouterOS je operacijski sustav primarno razvijen za MikroTik RouterBoard uređaje različitih namjena. Svi RouterBoard uređaji dolaze sa odgovarajućom verzijom RouterOS-a i licencom. Postoje 6 razina licenciranja, a njihove razlike su prikazane na slici 2.

Tablica 1. Prikaz razlika u licencama RouterOS-a [2]

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	not sold separately	$45	$95	$250
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

RouterOS-u je moguće pristupiti putem SSH i Telnet klijenata te putem web pretraživača i WinBox alata, koji nude olakšani pristup grafičkom sučelju istog (slika 3.).

Slika 2. Prikaz grafičkog sučelja RouterOS putem WinBox klijenta

CHR ili usmjernik smješten u oblaku (eng. Cloud Hosted Router) je softverska verzija RouterOS-a koju je moguće instalirati u virtualnom okruženju, kao uslugu u oblaku, na fizičkom poslužitelju ili na osobnom računalu. Funkcije CHR-a su slične klasičnom RouterOS-u iako postoje male razlike, poput nedostatka *Switch* postavki, pošto se RouterOS ne pokreće na uređaju koje sadrži više mrežnih sučelja,kao što je slučaj u fizičkom preklopniku. Licence CHR-a se razlikuju od licneci za RouterOS za fizičke uređaje. Razlike u licencama su u ograničenjima propusnosti po mrežnim sučeljima i ograničenjima ostalih mogućnosti.

U ovom radu, instalirati će se CHR posljednje verzije. Instalacija će se izvršiti na prethodno postavljenom privatnom poslužitelju te će ista biti detaljnije opisana u slijedećem poglavlju.

2.3. Operacijski sustav otvorenog koda

Operacijski sustavi otvorenog koda (open-source) su sustavi čiji je izvorni kod dostupan svima za distribuciju, upotrebu i izmjene. S financijskog gledišta, sustavi otvorenog koda su u većini slučajeva besplatni, iako određene tvrtke (npr. Red Hat) naplaćuju podršku ili prilagođene verzije samog sustava. Kada se govori o razvoju sustava, plan i financiranje razvoja određuje upravni odbor, pojedinci ili zajednica. Primjerice, sustavi otvorenog kuda su FreeBSD, Android, OpenSolaris, Linux.

Jedna od distribucija Linuxa je Debian što znači da u svojoj osnovi koristi Linux jezgru. Održava ga, usavršava i razvija Debian Project zajednica čiji je cilj pružiti besplatni operacijski sustav svim korisnicima, neovisno o potrebi, u svrhu korištenja, razvoja ili prilagodbe po želji. Debian strukturalno podsjeća na toranj, u temeljima se nalazi Linux jezgra, iznad nje se nalaze osnovni alati i instalirani programi, a na samom se vrhu nalazi Debian kao okruženje koji brine da sve komponente međusobno komuniciraju i rade na ispravan način. Nadalje, Debian omogućuje instalaciju oko 50,000 paketa što omogućuje prilagodbu ovog sustava gotovo svim potrebama. Kako je Debian distribucija koja je jako poznata i često korištena kao poslužiteljska okosnica u IT svijetu, autori aplikacija razvijaju iste upravo prilagođene za instalaciju na Debian sustavu. Jedna od takvih aplikacija će biti opisana u nastavku, Checkmk, koja ima podršku za instalaciju na nekoliko operacijski sustava i platformi uključujući i Debian odnosno njegove verzije 9 (Stretch) i 10 (Buster). U ovom završnom radu koristit će se Debian 9 verzija iz razloga što je stabilnija dok kod verzije 10 još postoje mogućnosti greški i ne mogućnosti instalacije potrebnih paketa.

2.4. Check_MK

Checkmk je sustav razvijen u Pythonu i C++ za nadzor IT infrastrukture. Koristi se za nadzor poslužitelja, aplikacija, mreža, cloud infrastrukture, kontejnera (eng. containers), sustava za pohranu, baza podataka i IoT uređaja.

Checkmk je dostupan u 3 verzije:

- verzija otvorenog koda (Checkmk Raw Edition – CRE),
- komercijalna verzija za tvrtke (Checkmk Enterprise Edition – CEE),

- komercijalna verzija za pružatelje nadzornih usluga (Checkmk Managed Services Edition – CME).

Ove verzije dostupne su za veliki broj platformi, posebno za razne verzije operacijskih sustava poput Debian-a, Ubuntu-a, SLES -a (SUSE Linux Enterprise Server) i Red Hat/CentOS-a. Checkmk je moguće implementirati i u Docker okruženju. Nadalje, Checkmk podržava široku paletu modela i vrsta uređaja koju može nadzirati u isto vrijeme, pružajući na taj način visoku razinu fleksibilnosti i skalabilnosti.

Prva inačica Checkmk sustava potječe iz 2008. godine kao zamjena za Inetd okruženje. Službeno je objavljen u travnju 2009. godine pod besplatnom GPL licencom. U početnim verzijama sustava, jezgra istog se temeljila na Nagios-u kao i njezini dodaci, dok se kod kasnijih verzija sustav razvijao bez korištenja postojećih modula već je svaka sastavnica razvijena kako bi odgovarala potrebama Checkmk sustava. Checkmk je razvila njemačka tvrtka tribe29 GmBH, koja ju i dalje razvija, usavršava i održava. Kako je već navedeno tribe29 nudi i plaćene komercijalne verzije za koje svojim kupcima pružaju podršku instalacije i konfiguracije.

Checkmk koristi tri vrste nadzora:

- statusni nadzor koji bilježi "zdravlje" uređaja ili aplikacije,
- metrični nadzor koji omogućuje snimanje i analizu grafova u određenom vremenskom periodu,
- nadzor temeljen na pohrani i pamćenju događaja koji se kasnije mogu analizirati i poduzeti odgovarajuće radnje.

Checkmk je relativno jednostavan za učenje i korištenje, ali dovoljno moćan za većinu složenih IT okruženja.

Korištenjem Checkmk sustava korisniku se nude brojne mogućnosti poput:

- Automatizacija – odnosi se na automatizirani nadzor kako bi se uštedilo na vremenu. Kod ove značajke omogućeno je jednostavnije dodavanje novih komponenti koristeći automatsku detekciju i konfiguraciju. Checkmk automatski prepoznaje vrstu uređaja i osigurava nadzor za sve relevantne komponente istog. Također je moguće integrirati

druge sustave koristeći snažne API-e kako bi se automatiziralo gotovo sve što možete zamisliti.

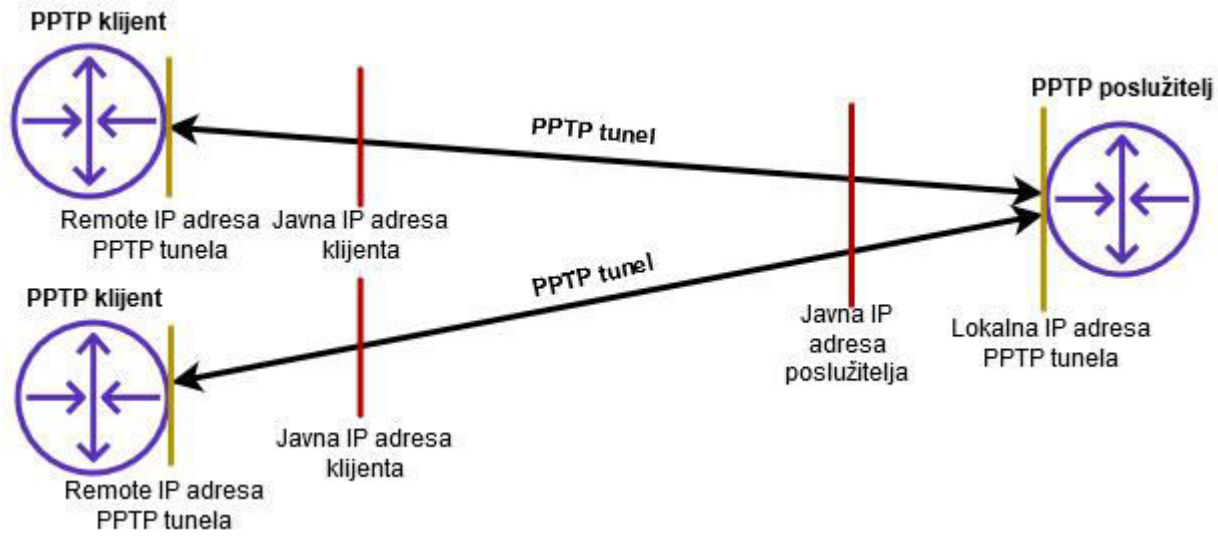
- Konfiguracija – Checkmk omogućava jednostavnu i brzu konfiguraciju. Također, ne trebate gubiti vrijeme na odabir parametara metrike treba jer Checkmk sam otkriva odgovarajuću metriku prema vrsti uređaja kojeg se želi nadzirati. Checkmk također brzo identificira probleme u IT okruženju preko jednostavnog sustava "stanja" (OK, WARN, CRIT) svake nadzirane komponente ili sustava.
- Softverski dodaci - Checkmk-ova kolekcija dodataka je jedinstvena, podržava približno 1900 dodataka. Ta usluga također omogućuje visoku razinu fleksibilnosti kada je potrebno nadzirati heterogene mreže koje sadrže veliki broj različitih vrsta uređaja i sustava. Isto tako, velikim brojem dodatka smanjuje se mogućnost korištenja dodataka iz nepoznatih izvora.
- Vizualizacija- omogućava vizualni pregled podataka koristeći poglede (eng.view) koji se mogu napraviti po želji ili odabrati već postojeće. Za vizualizaciju podataka Checkmk često koristi sustav grafova koji je integriran ili je moguće iste pregledavati putem Grafane, uz prethodnu integraciju iste.
- Upozoravanje - ova funkcija omogućava obavještavanje u realnom vremenu koristeći elektroničku poštu, SMS poruke i druge alate kao što su ServiceNow, Jira, Slack, PagerDuty i VictorOps.
- Nadzor unosa podataka u dnevnik - odnosi se na kombiniranje mjerenja i dnevničkih zapisa za brzo prepoznavanje problema i analizu uzroka. Kroz ovu funkciju mogu se filtrirati i prosljeđivati događaji, pokretati zapisi ili generirati obavijesti.
- Napredna analitika - omogućava proučavanje pohranjenih podataka nadziranja koji će pomoći u predviđanju budućih događaja i prema tome definiranje budućih radnji nad IT infrastrukturom.
- Izvještavanje - omogućava organizacijama i tvrtkama slanje automatski generiranih izvješća. Izvješća se generiraju u PDF formatu i sadrže sve odabrane stavke koje se žele provjeriti, bilo na zahtjev ili automatski u pravilnim vremenskim razmacima.

U praktičnom djelu ovog rada biti će instalirana najnovija, 2.0 verzija Checkmk sustava. Za razliku od prethodnih verzija ova verzija pruža bolje korisničko iskustvo i dodatne funkcionalnosti.

2.5. Point-to-Point Tunneling Protocol (PPTP)

Kako bi se omogućila veza između dvije točke, primjerice, između računala u kući i usmjernika u uredu firme, kreiraju se virtualne privatne mreže (VPN). Postoje veliki broj standarda pomoću kojih se može kreirati virtualna veza, jedan od njih je i protokol tuneliranja od točke do točke (eng. Point-to-Point Tunneling Protocol ili PPTP). PPTP protokol odnosi se na kreiranje virtualnog tunela od točke do točke koristeći enkapsulaciju unutar TCP/IP protokola, koji omogućava vezu prema Internetu. Na taj način, u isto vrijeme imamo vezu prema Internetu i sigurnost podataka koje omogućuje PPTP tunel.

PPTP standard temelji se na klijent-poslužitelj arhitekturi, drugim riječima, PPTP klijenti se spajaju na PPTP poslužitelj. Postoje dva načina uspostavljanja veze, dobrovoljni i prisilni. Dobrovoljno tuneliranje pokreće klijent dok prisilno tuneliranje je inicijalizirano od strane poslužitelja. Za uspostavljanje veze od strane klijenta potrebni su podaci profila (korisničko ime, lozinka, lokalna i udaljena adresa itd.) i javna IP adresa PPTP poslužitelja, po mogućnosti statička. Profil se kreira na poslužitelju, čime se omogućuje upravljanje spajanjem na poslužitelj, odnosno kreiranjem profila određuje se koji će klijenti imati dopuštenje za spajanje. Na PPTP klijentu se kreira profil za spajanje na PPTP poslužitelj, gdje se upisuju već navedeni podaci potrebni za inicijalizaciju veze prema poslužitelju. PPTP koristi TCP 1723 port i generički protokol za uvijanje usmjeravanja odnosno GRE (Generic Routing Encapsulation) preko IP porta 47. Kako bi se uspostavila veza, PPTP protokol koristi lokalne i udaljene adrese tunela (eng. local/remote address) (slika 4.), odnosno lokalna adresa je adresa na PPTP poslužitelju na koju se spajaju svi PPTP klijenti dok se Remote ili udaljena adresa odnosi na pojedine adrese PPTP klijenata. Kako je lokalna adresa privatna, ista nije vidljiva sa strane Interneta pa PPTP klijent ne može znati gdje se ona nalazi. Kako bi klijent znao gdje se upućuje poziv za uspostavljanje tunela, u klijentskoj strani profila potrebno je upisati javnu IP adresu PPTP poslužitelja. Na taj način dolazi do spajanja klijentske i poslužiteljske strane koristeći tunel, a komunikacija se odvija pomoću javnih adresa obiju strana.



Slika 3. Prikaz principa rada PPTP protokola

Razvijen 1999. godine u Microsoftu, PPTP je jedan od najstarijih VPN standarda koji se još uvijek koristi. Prednosti i nedostatci navedenog protokola su prikazani u tablici (Tablica 1.) ispod:

Tablica 2. Prikaz prednosti i nedostataka PPTP protokola

PREDNOSTI PPTP-a	NEDOSTATCI PPTP-a
Podržan na velikom broju operacijskih sustava i platformi	Podržava stari 128-bitni način enkripcije
Omogućava velike brzine	Lako je zaobići sigurnosni mehanizam
Ne zahtijeva velike resurse	Stabilnost veze ovisi o mreži
Lagan za postavljanje	Pružatelji internetskih usluga mogu lako blokirati priključke (eng. port) koje koristi,
	Nije predviđen za prijenos osjetljivih podataka

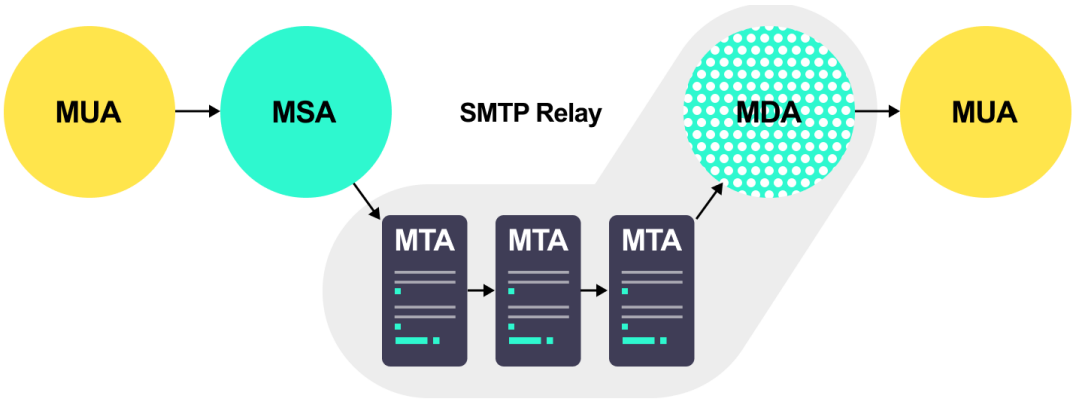
Iako PPTP ima dosta nedostataka, njegova upotreba ovisi o podacima koji se žele prenositi PPTP tunelom. U ovom završnom radu PPTP se koristi iz razloga što su podaci koji se šalju tunelom statusne i statističke prirode te je količina istih velika zbog stalnog osvježavanja

statusa uređaja na mreži, te će velika propusnost PPTP tunela omogućiti uredan rad sustava nadzora i kod sporih mreža.

2.6. Mail Transfer Agent (MTA)

Komuniciranje putem elektroničke pošte (eng. e-mail) postalo je jedan od glavnih načina komunikacije. Kako bi se elektronička pošta uspješno prenijela od jednog korisnika prema drugom korisniku, koristi se sustav prijenosa elektroničke pošte (slika 5.). Jedan od elemenata tog sustava je agent za prijenos poruka (eng. Mail Transfer Agent ili MTA). MTA je servis ili program koji ima ulogu mail poslužitelja, njegova glavna zadaća je upravljanje slanjem odlazne elektroničke pošte i primanje ili odbijanje dolazne elektroničke pošte. MTA servis prima elektroničku poštu od strane agenta za slanje poruka odnosno Mail Submission Agenta (MSA) koji istu nasljeđuje od Mail User Agenta (MUA). Drugim riječima, MUA agenti su u suštini klijentske aplikacije za upravljanje elektroničkom poštom, kao na primjer, Mozilla Thunderbird**,** Evolution**,** Microsoft Outlook**,** Apple Mail itd. Nakon što MTA dobije elektroničku poštu od MSA, on se ponaša kao posrednik koji provjerava da li se primatelj nalazi lokalno na domeni za koju je zadužen, u suprotnom elektroničku poštu pohranjuje i šalje do MTA poslužitelja u neposrednoj blizini, koji kada otkriju da je primatelj dodijeljen upravo njemu, šalju primljenu poštu prema agentu za dostavu poruka ili Mail Delivery Agentu (MDA) koji naposljetku šalje istu prema MUA primatelja, nakon čega primatelj vidi primljenu elektroničku poštu u svom poštanskom sandučiću.

Nerijetko se dogodi da primatelj nije u mogućnosti primiti elektroničku poštu, MTA istu zadrži i pokuša ponovno slanje u određenom periodu. Zbog ove mogućnosti MTA poslužitelj se još naziva i smart host, a kako za primanje i slanje elektroničke pošte koristi SMTP protokol, MTA je poznat i pod nazivom SMTP poslužitelj. Jednostavni protokol za prijenos pošte ili SMTP (Simple Message Transfer Protocol) je komunikacijski protokol koji omogućuje pouzdan i siguran prijenos elektroničke pošte. SMTP uz standard za proširenje funkcija elektronske pošte tj. MIME (Multi-purpose Internet Mail Extensions) omogućava dodavanje teksta bez ograničenja, obradu teksta, slanje svih vrsta podataka poput slike, videa, privitaka, binarnih datoteka itd. SMTP protkol koristi TCP port 25 i 587. Port 25, iako zastario, se koristi za komunikaciju između MTA poslužitelja dok se port 587 koristi za sve ostale vrste komunikacije između već spomenutih elemenata.



Slika 4. Prikaz rada MTA agenta [11]

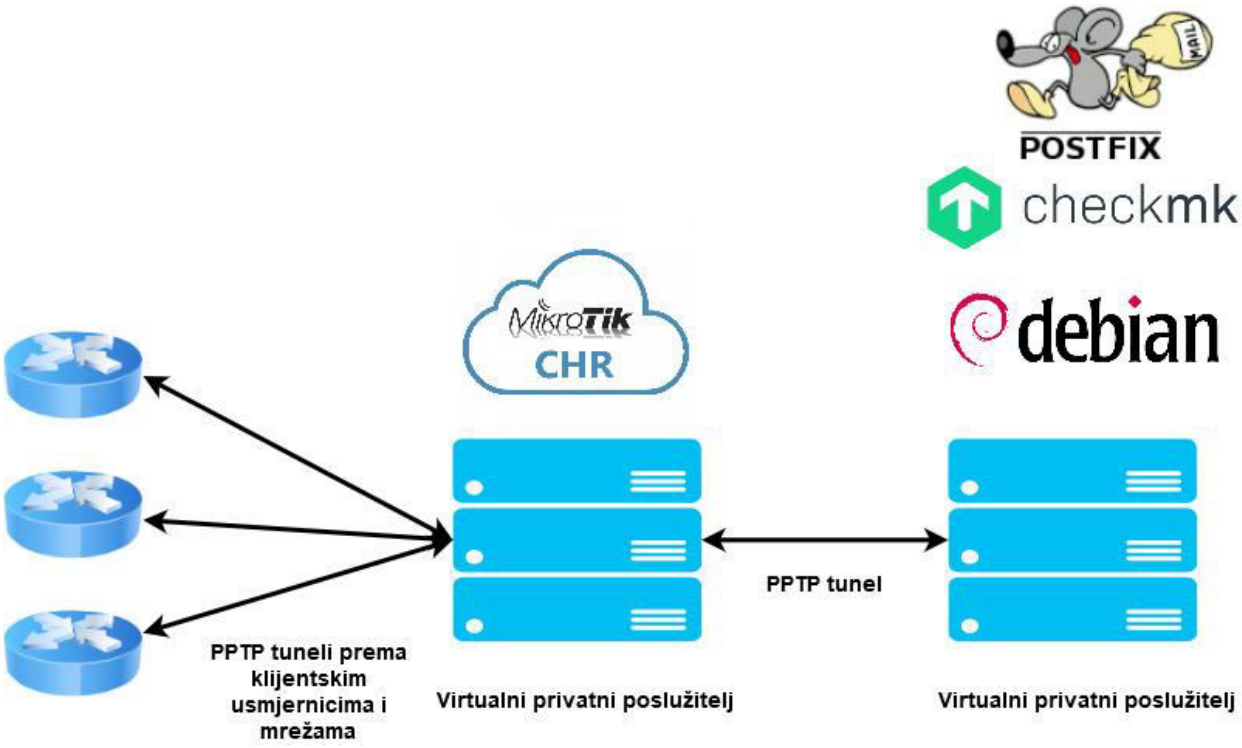
MTA agenti koji se najčešće koriste su Exim, Sendmail, Qmail, Mutt, Alpine, Microsoft Exchange itd. Jedna od njih je i Postfix, koji će biti implementiran za potrebe praktičnog dijela rada. Postfix je MTA agent koji razvijen od strane Wietse Zweitze Veneme, IBM-ova razvojnog inženjera, za potrebe mail poslužitelja u IBM-ovom razvojnom odjelu u kojem je radio. Iako je prvotno razvijen kao alternativa Sendmailu, Postfix je od istog naslijedio veliki broj funkcija, ali način rada je razvijen na potpuno drugačiji način. Postfix glasi kao jako brz po pitanju performansi te ga je lako konfigurirati i upravljati njegovim sigurnosnim mehanizmima. Postfix ima sljedeće mogućnosti:

- upravljanje neželjenom elektroničkom poštom (Filter sadržaja, Postscreen, SPF dodatak, Greylisting dodatak itd.),
- podrška za veliki broj protokola (IPv6, SASL i TLS autentikacija, Nginx, ETRN itd.),
- podrška za bazu podataka (MySQL, PostgreSQL, Berkley DB, SQLite, LDAP, CDB, LMDB itd.),
- podrška za poštanske sandučiće,
- podrška za upravljanje adresama (VERP, Postfix Address Rewriting itd.)

3. INSTALACIJA SASTAVNICA I IMPLEMENTACIJA SUSTAVA

3.1. Shematski prikaz povezivanja sastavnica

Kako je već navedeno u predstavljanju tehnologija, sustav se sastoji od nekoliko sastavnica (slika 6.). Glavne okosnice sustava čine virtualni privatni poslužitelji na kojima je instaliran MikroTik Cloud Router, softverska inačica usmjernika koju je moguće implementirati kao komponentu u oblaku te Checkmk, sustav nadzora udaljenih ili lokalnih mreža i ostale IT infrastrukture. Checkmk je strukturalno zamišljen kako aplikacija za čije je instaliranje potreban operacijski sustav, u ovom slučaju će se koristiti Debian 9. Kako sustav nadzora može potencijalno imati veliki broj uređaja koje nadgleda, radi lakšeg pregleda istih i dugoročnog zapisivanja statističkih informacija, implementirana je funkcija slanja informacija putem elektroničke pošte korištenjem Postfix agenta, koji za ove potrebe služi samo kao prijenosni medij između Checkmk sustava obavijesti i sandučića elektroničke pošte. Sva dodatna filtriranja i postavke obavijesti se odrađuju na Checkmk-u.

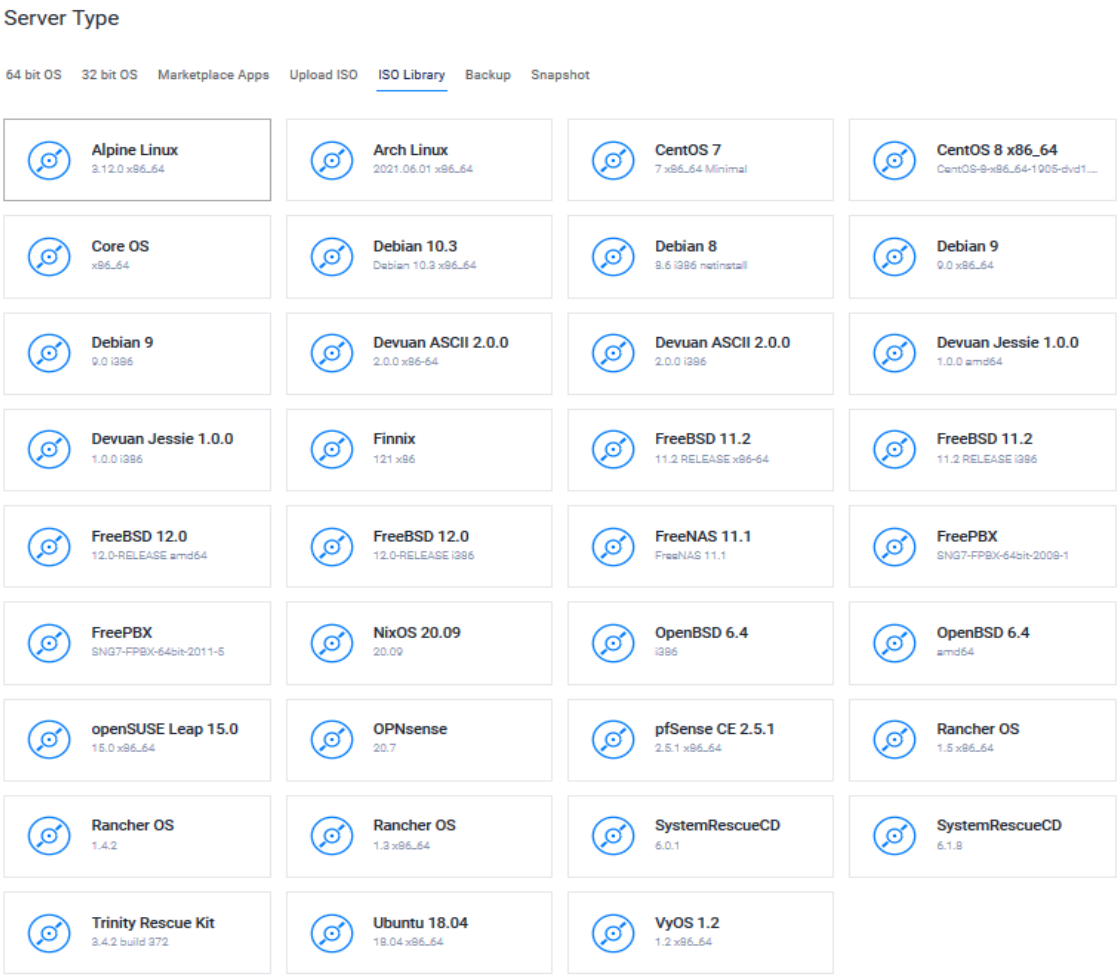


Slika 5. Shematski prikaz povezivanja sastavnica

3.2. Instalacija MikroTik CHR usmjernika

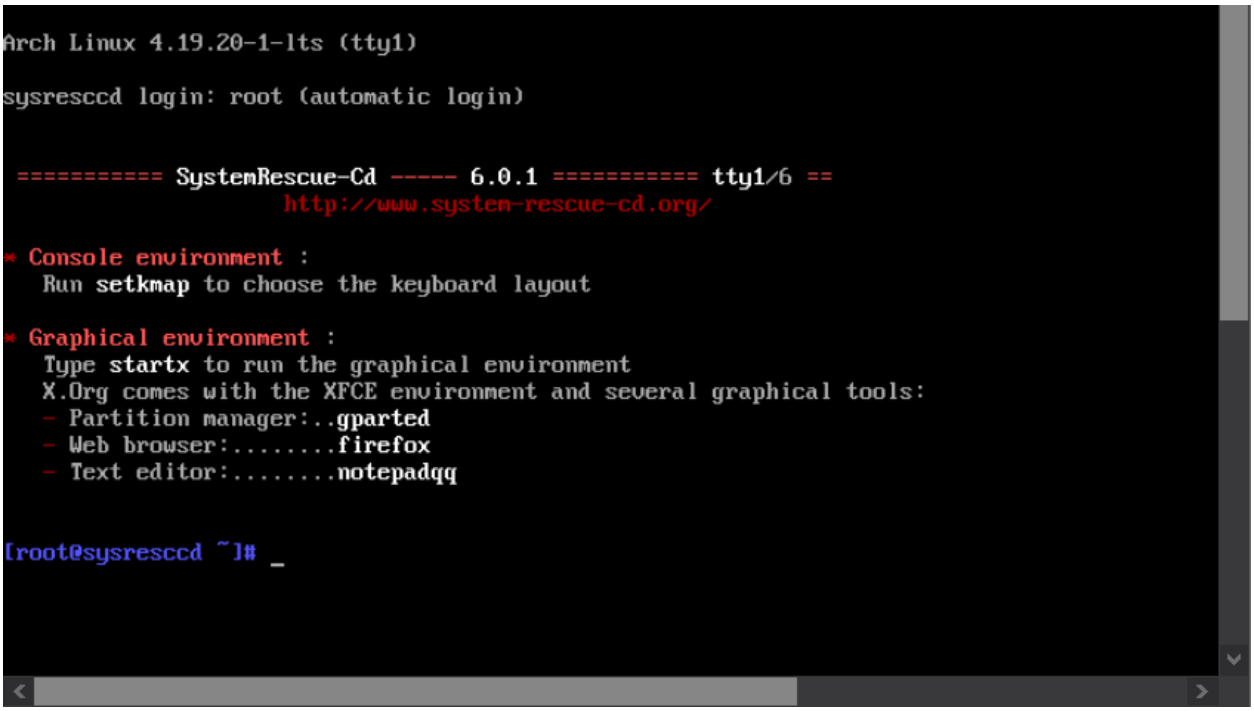
Pošto je MikroTik CHR sam po sebi operacijski sustav, njegova instalacija se provodi izravno na privatni poslužitelj, bez prethodno instaliranog drugog operacijskog sustava. Kako iznajmljeni privatni poslužitelj nema opciju instalacije MikroTik CHR-a, ista će se pokrenuti pomoću SystemRescueCD alata. SystemRescueCD je Linux-ov skup alata koji omogućuje popravak već instaliranog operacijskog sustava ili izvođenje dodatnih administratorskih naredbi, poput naredbi za preuzimanje i instalaciju MikroTik CHR usmjernika. U nastavku će biti prikazan postupak instalacije MikroTIk CHR sustava.

Prilikom kreiranja privatnog virtualnog poslužitelja kao vrstu operacijskog sustava potrebno je odabrati SystemRescueCD (slika 7.) unutar kartice ISO Library.



Slika 6. Prikaz opcija za odabir operacijskog sustava

Nakon odabranog SystemRescueCD-a i ostalih postavki, poslužitelj izvršava instalaciju i početne postavke. Nakon završetka instalacije, poslužitelju je moguće pristupiti preko VNC alata pružatelja poslužiteljskih usluga koji je implementiran na prikaznoj ploči poslužiteljske instance. Daljni pristup poslužitelju će biti omogućen preko javne IP adrese koja mu je dodijeljena putem SSH klijenata kao što je Putty-a, koji će se koristiti u ovom radu. Korisničko ime „root“ i slučajno generirana lozinka su dodijeljeni od strane pružatelja poslužiteljskih usluga. Nakon otvaranja VNC prozora, otvara se naredbeni redak (slika 8.) preko kojeg će se unositi naredbe za instalaciju MikroTik CHR sustava.



Slika 7. Prikaz naredbene linije putem VNC-a

Prva naredba koja će se izvesti je naredba za preuzimanje komprimirane .img slike sustava. .img će se koristiti pošto ne zahtijeva ni jednu virtualizacijsku platformu za instalaciju. Naredba se nalazi ispod.

wget https://download.mikrotik.com/routeros/6.48.3/chr-6.48.3.img.zip

Zatim se pomoću naredbe unzip dekomprimira slika sustava:

unzip chr-6.48.3.img.zip

Nakon završetka prethodne naredbe, koristeći dd naredbu zapisujemo .img sliku sustava na disk virtualnog poslužitelja. Na taj način se izvršava instalacija MikroTik CHR usmjernika na virtualni poslužitelja.

dd if=chr-6.48.3.img of=/dev/vda

Nakon ove naredbe, potrebno je ukloniti SystemRescueCD alat sa poslužitelja, nakon čega će se poslužitelj ponovno pokrenuti. Nakon ponovnog pokretanja, pristup naredbenog retku i grafičkom MikroTik CHR-a omogućen je putem javne IP adrese poslužitelja, što predstavlja jedan od sigurnosnih rizika.

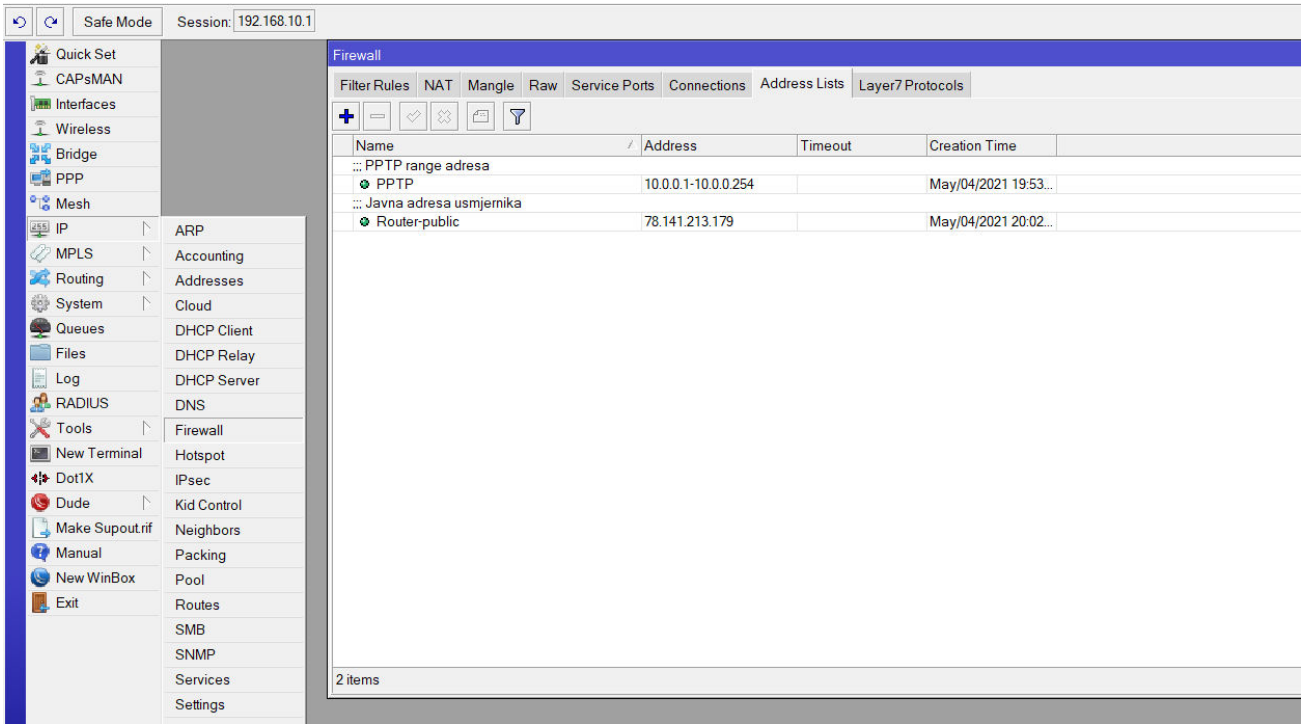
3.2.1. Pregled sigurnosnih rizika i zaštita usmjernika od neželjenog pristupa

Uvođenje sigurnosnih mehanizama mrežnih sustava je jedna od najvažnijih radnji i zadataka kada se govori o zaštiti mreže, jer je često jedna od najslabijih točaka iste. Sigurnosni mehanizmi mreže služe kako bi se kontrolirao pristup od strane korisnika, na svim razinama korištenja iste. Tako u slučaju izgradnje ovog sustava postoji nekoliko sigurnosnih rizika koji se često zanemaruju.

Prvi sigurnosni rizik je već naveden prethodno, a to je pristup usmjerniku preko javne IP adrese. Naime, kao što samo ime govori, javna IP adresa je vidljiva svima odnosno cijelom internetu, stoga je potrebno poduzeti sigurnosne korake kako bi se pristup ograničio na privatne adrese, dok bi se istovremeno odobrio pristup adresama i virtualnim priključcima (eng. port) koji se koriste za uspostavu PPTP tunela i prolazak prometa koji je neophodan za rad aplikacija sustava. Primjerice, potrebno je blokirati pristup putem SSH protokola, ali je korisno dopustiti HTTPS promet.

Kako bi se otklonio ovaj rizik, RouterOS omogućava kreiranje lista adresa pomoću kojih se može definirati skupovi adresa koje želimo zabraniti ili dopustiti. Liste adresa, nakon kreiranja, same po sebi ne dopuštaju niti blokiraju nikakav promet, ali se koriste za lakše kreiranje pravila vatrozida koja će provoditi zabranu odnosno dopuštenja na mreži. Prozor za

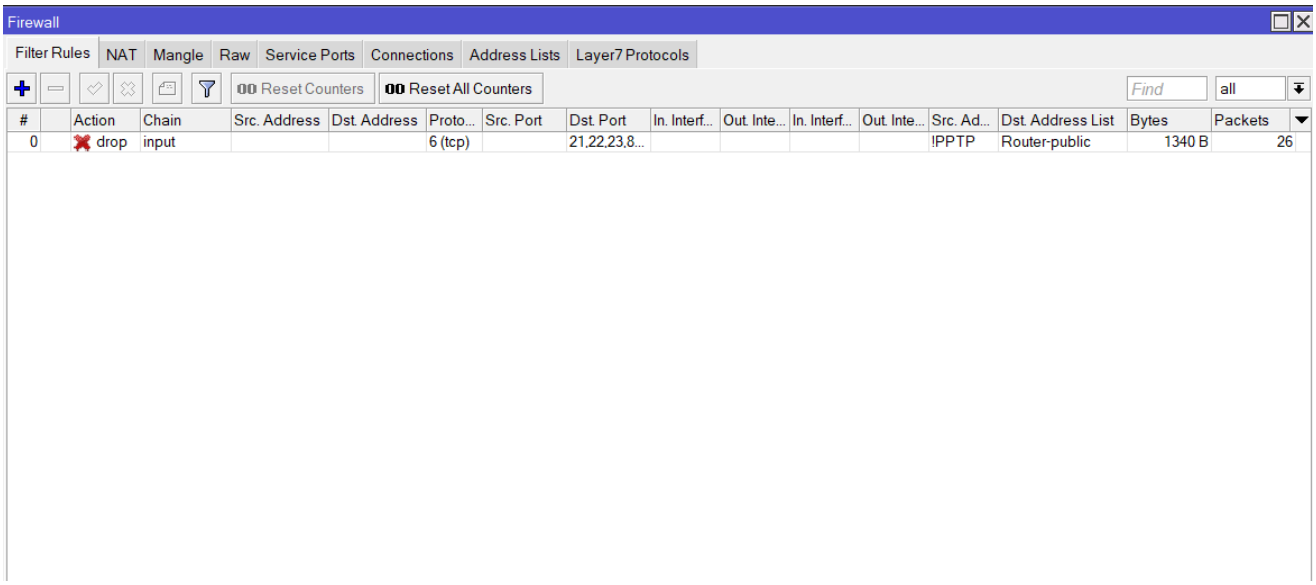
kreiranje lista adresa u RouterOS-u nalazi se na kartici Address Lists unutar podizbornika Firewall koji se nalazi u izborniku IP. Slika 9. prikazuje dvije kreirane adresne liste.



Slika 8. Prikaz kreiranih lista adresa

Prva lista adresa odnosi se na skup (eng. range) adresa koje će se koristiti za kreiranje PPTP tunela prema CheckMK sustavu i ostalim PPTP klijentima. Druga lista adresa označava javnu adresu usmjernika.

Nakon kreiranja lista adresa, potrebno je kreirati pravila filtriranja prometa na vatrozidu. Pravila vatrozida se kreiraju na kartici Filter Rules unutar podizbornika Firewall koji se nalazi u izborniku IP. Na slici ispod prikazano je pravilo kako bi se ograničio pristup preko javne IP adrese. Kreirano pravilo zabranjuje pristup usmjerniku za sve adrese koje se nalaze u adresnoj listi PPTP te također blokira sav promet koji se odvija na priključcima 21(ftp), 22(ssh), 23(telnet), 80 (http), 8291 (winbox). Nakon kreiranja ovog pravila, pristup usmjerniku je jedino moguć preko privatnih IP adresa putem PPTP tunela koji je kreiran kako VPN veza za proizvoljno spajanje na korisničkom uređaju.

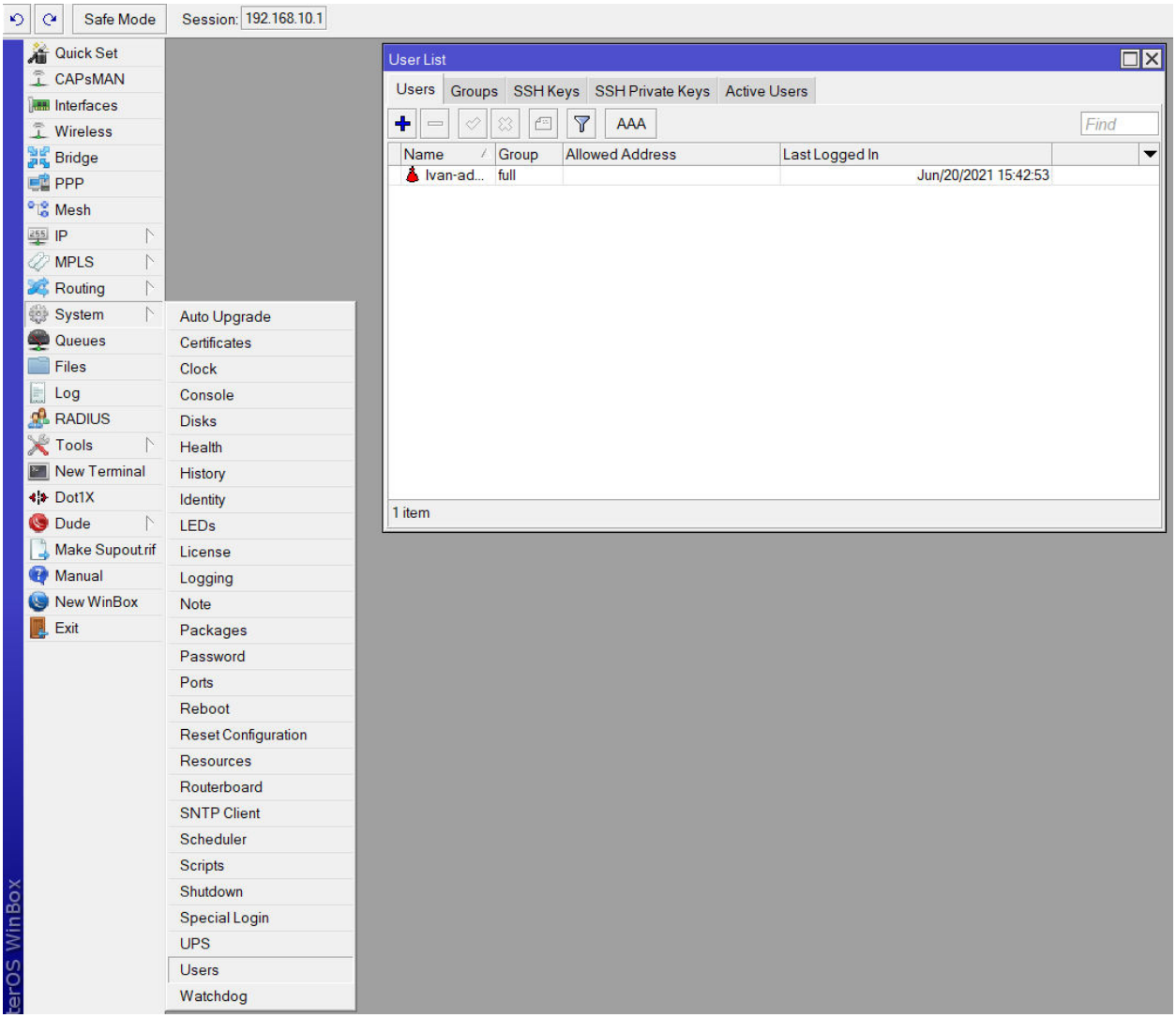


Slika 9. Prikaz kreiranog pravila u vatrozidu

Drugi sigurnosni rizik je korisničko ime i lozinka za prijavu u CHR. Naime, nakon prve instalacije CHR-a, inicijalno korisničko ime je „Admin“ dok lozinka nije definirana. Iako je prethodnim pravilima usmjernik zaštićen od vanjskog utjecaja, opasnost je još uvijek prisutna unutar mreže.

Drugim riječima, napadi se mogu dogoditi od strane računala ili korisnika, bilo namjerno ili nenamjerno. Bez obzira što se i ovakve situacije mogu staviti pod kontrolu kreiranjem pravila, dobra praksa je postaviti dovoljno složeno korisničko ime i lozinku kako bi se u slučaju napada na mrežu i dolaska napadača do usmjernika, onemogućio izravan pristup funkcijama istog.

U RouterOS-u, upravljanje korisničkim računima odvija se preko kartice Users (slika 11.) unutar podizbornika Users koji se nalazi u izborniku System. Nakon izrade novog korisnika sa svim ovlastima potrebno je zabraniti pristup (eng. Disable) starom korisniku ili ga u potpunosti izbrisati.



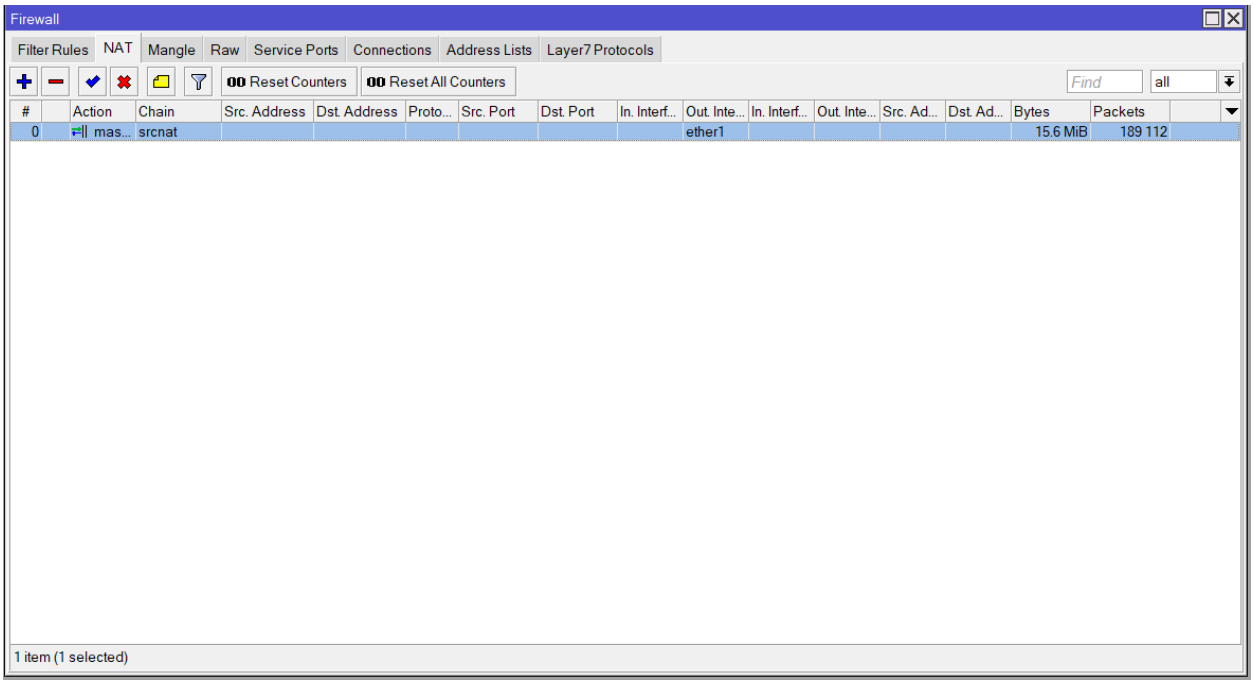
Slika 10. Prikaz postavki za korisničke račune

Navedene postavke ne rješavaju sve sigurnosne probleme, ali uklanjaju one koji su najčešći i koji svojom funkcijom izravno utječu na ispravan rad i učinkovitost usmjernika.

3.2.2. Postavljanje osnovnih postavki usmjernika

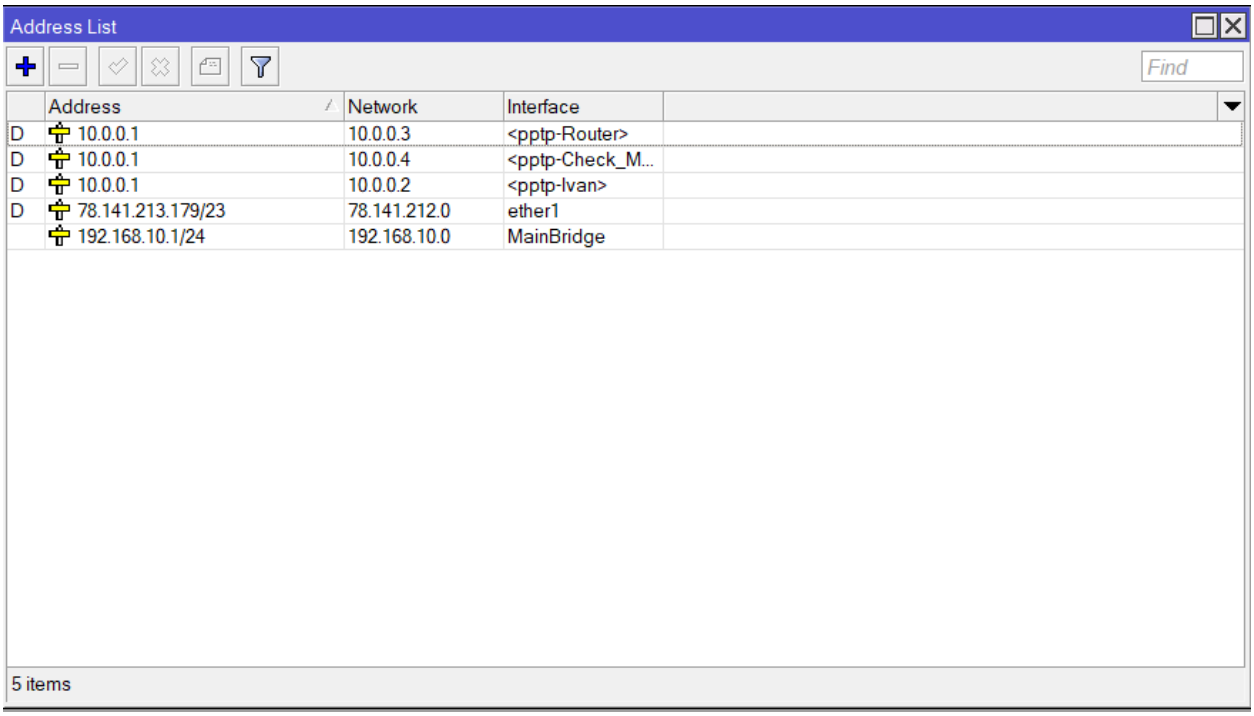
Kako bi CHR komponenta uspješno odrađivala svoju funkciju unutar sustava na nadzor udaljenih mreža, potrebno je omogućiti osnovne funkcije usmjernika. Prva od tih funkcija je NAT maskiranje, što u prijevodu omogućava pretvorbu privatnih adresa u privatne adrese usmjernika u mreži odnosno u javne adrese usmjernika koji šalje promet prema van, prema internetu. Maskiranje je u ovom radu važno za ispravan rad VPN konekcije prema CHR

usmjerniku. VPN konekcija sama po sebi omogućava spajanje na usmjernik, međutim, izlaz prema Internetu je u prolaznom (eng. pass-through) načinu rada, drugim riječima, ako NAT maskiranje nije uključeno, administrator spajanjem putem VPN-a na usmjernika gubi vezu na Internet, pa se tako i sama VPN veza prekida. NAT maskiranje na RouterOS-u se aktivira kroz prozor NAT unutar podizbornika Firewall koji se nalazi u izborniku IP. Slika 12. prikazuje NAT pravilo koje radi maskiranje adresa na prometu koji prolazi na ether1 mrežnom sučelju, odnosno sučelju koje povezuje usmjernik na Internet. U ovom slučaju ether1 sučelje je mrežna kartica poslužitelja.



Slika 11. Prikaz kreiranog NAT pravila

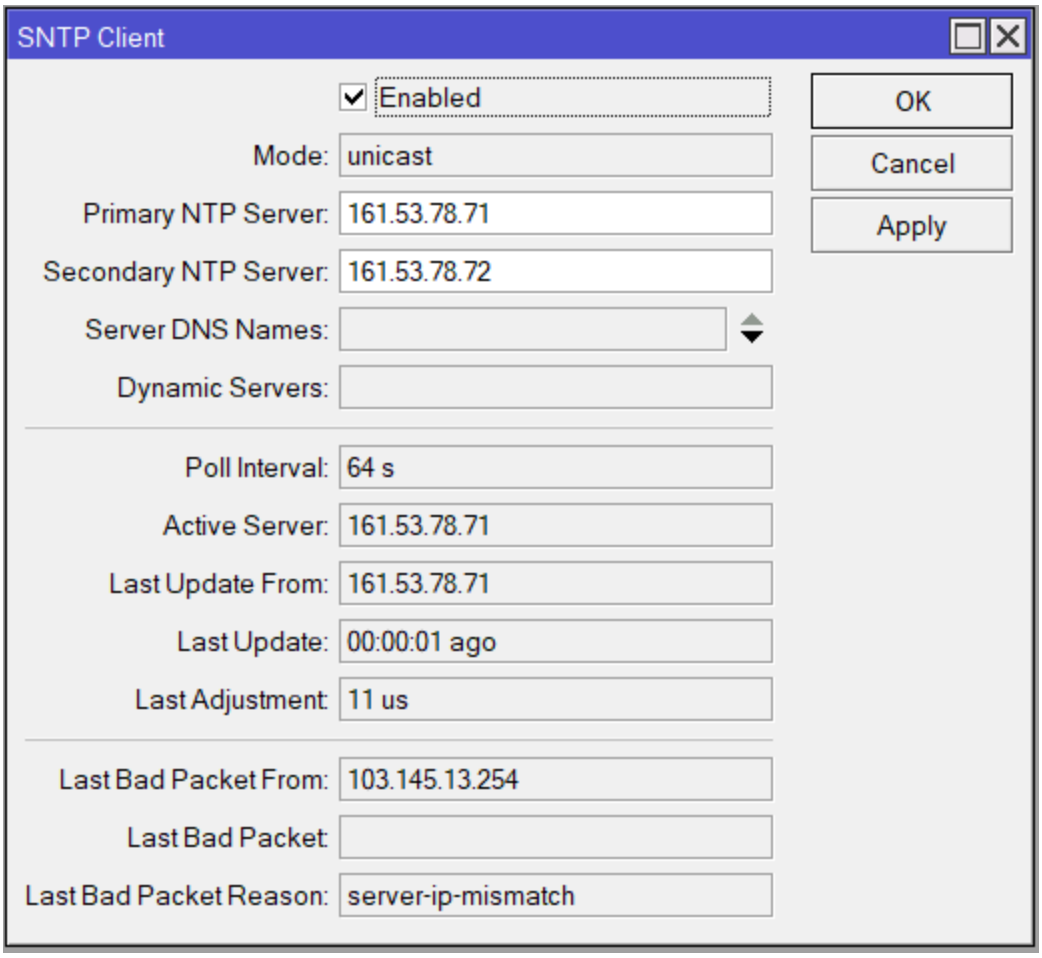
Druga bitna postavka usmjernika je kreiranje privatne mreže na usmjerniku. Privatna mreža će za ove potrebe služiti za nadzor samog usmjernika putem Checkmk-a te za pristup korisničkom sučelju, pošto je pristup preko javne adrese zabranjen. Privatna mreža se kreira u kartici Addresses (slika 13.) u izborniku IP.



Slika 12. Prikaz prozora za kreiranje mreža

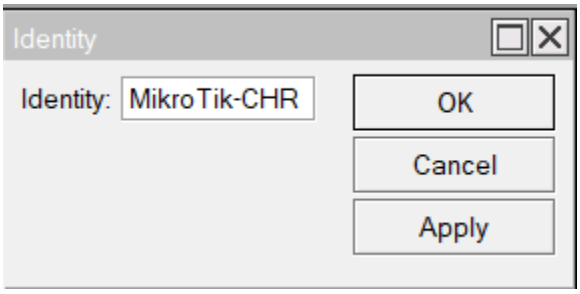
Za potrebe ovog rada, kreirana je privatna mreža 192.168.10.0/24. Prva adresa u mreži, 192.168.10.1., je adresa usmjernika dok se ostale adrese u mreži mogu koristiti za ostale namjene. Oznaka sučelja (eng. Interface) odnosi se na sučelje preko kojeg radi privatna mreža, a to može biti fizičko sučelje, VLAN, mrežni premosnik, VPN tuneli itd. Bitno je napomenuti da se na usmjerniku može kreirati više odvojenih mreža, ovisno o potrebama i namjenama. U slučaju da je potrebno dinamički dodijeliti adrese iz mreže, postavljanje se realizira u kraticama DHCP Server i Pool u istom izborniku. Kartica Addresses također prikazuje dinamički kreirane mreže od strane ostalih protokola, poput PPP protokola, kao što je vidljivo iz slike.

Vrijeme sustava nije najbitnija funkcija za ispravan rad usmjernika, ali je bitno za ispravan prikaz zapisa usmjernika, ispravan rad skripti koje se pokreću u određeno vrijeme, ispravno vrijeme kreiranja postavki, izrade sigurnosnih kopija itd. U slučaju kada se koristi fizički usmjernik, sinkronizacija vremena i datuma može se odraditi automatski, preko javne IP adrese, koristeći karticu Cloud u izborniku IP. U tom slučaju se informacije o vremenu i datum preuzimaju od NTP poslužitelja pružatelja internetskih usluga. Kada se usmjernik nalazi na udaljenom poslužitelju, isti se često nalazi na lokaciji koja nam je nepoznata, tada se koristi SNTP Client kartica koja se nalazi u izborniku System. Slika 14 prikazuje NTP postavke.



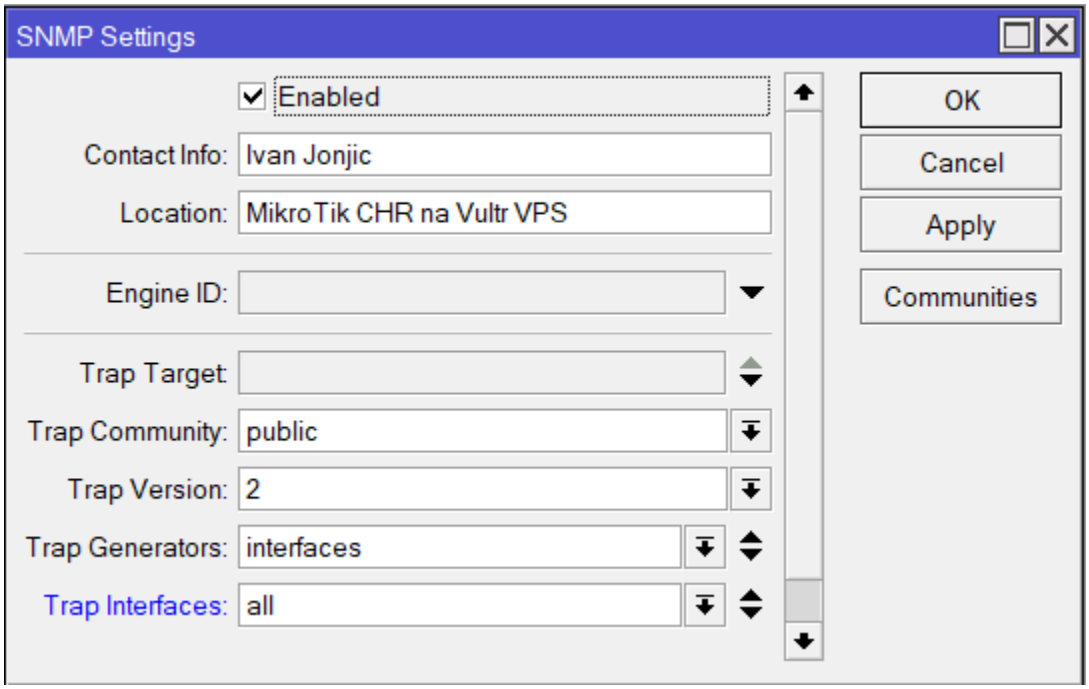
Slika 13. Prikaz NTP postavki

Za prikaz točnog vremena upisane su dvije javne adrese NTP poslužitelja koji se koriste u Republici Hrvatskoj. Naziv usmjernika je također bitan kako bi se lakše isti prepoznao na mreži. Naziv usmjernika se mijenja na kartici Identity (slika 15.) u izborniku System.



Slika 14. Prikaz prozora za promjenu naziva uređaja

Kako bi CheckMk mogao nadzirati mrežne uređaje poput usmjernika, preklopnika, poslužitelja, vatrozida itd. , koristi SNMP protokol. Na većini uređaja SNMP protokol nije uključen odnosno, uređaj ne može dati nikakve podatke sustavu za nadzor. Na RouterOS-u, SNMP se aktivira u kartici SNMP (slika 16.) u izborniku IP. Uz ostale informacije koje SNMP šalje, moguće je upisati kontakt i lokaciju uređaja koji je nadzire. Kartica SNMP također omogućava upravljanje postavkama poruka uzbune (trap poruke)koje su opisane u poglavlju tehnologija.



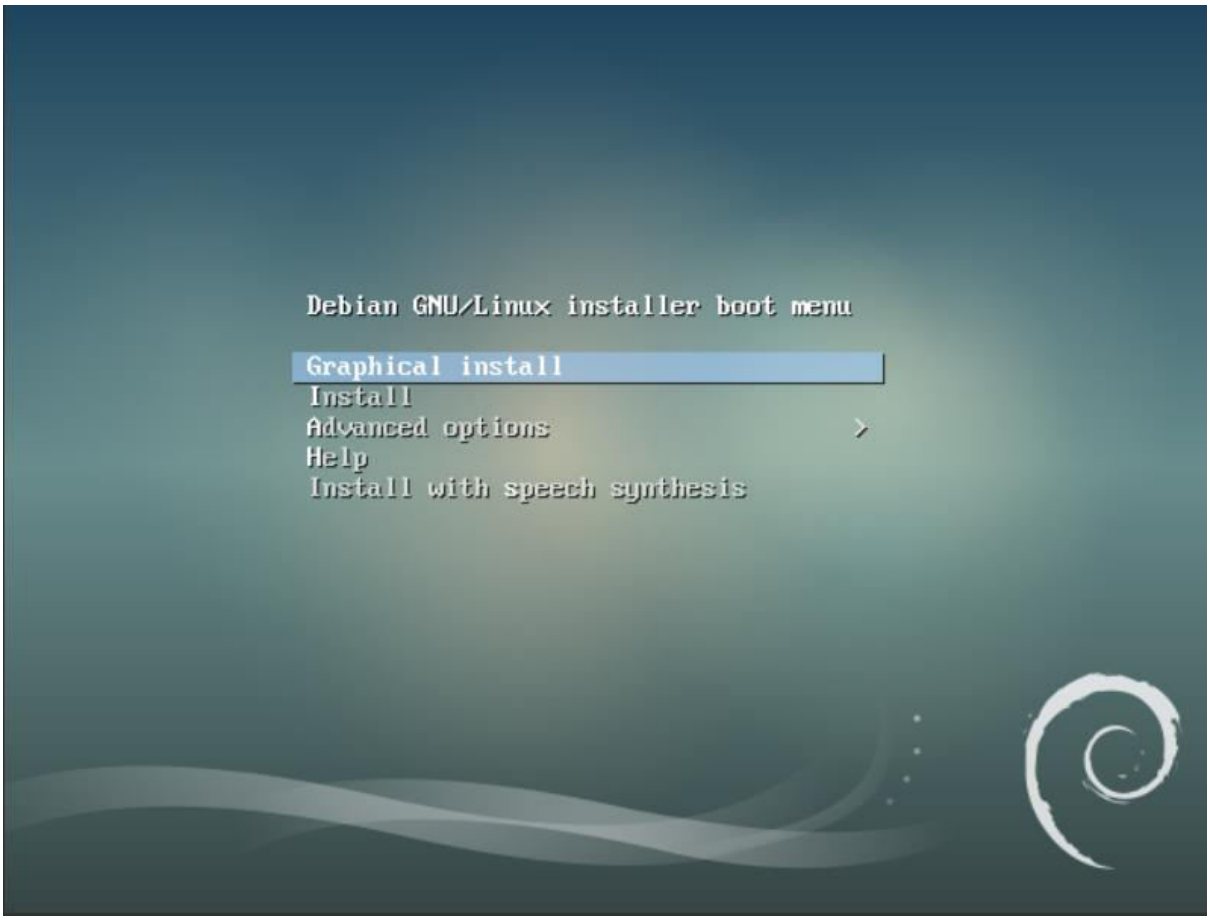
Slika 15. Prikaz SNMP postavki

3.3. Instalacija Debian 9 operacijskog sustava

Nakon instalacije i postavljanja MikroTik CHR usmjernika na jednom poslužitelju, na drugom virtualnom privatnom poslužitelju potrebno je instalirati Debian 9 operacijski sustav na kojem će se kasnije izvršiti instalacija CheckMk aplikacije i Postfix i PPTP paketa. U nastavku je opisan postupak minimalne instalacije (bez grafičkog sučelja i osnovnih alata) Debian-a 9.

Kao i kod instalacije MikroTik CHR-a, prilikom kreiranja poslužiteljske instance, odabire se operacijski sustav, ali u ovom slučaju to će biti Debian 9. Nakon odabira OS-a i ostalih podataka slijedi instalacija i početno postavljanje operacijskog sustava. Instalacija i početno

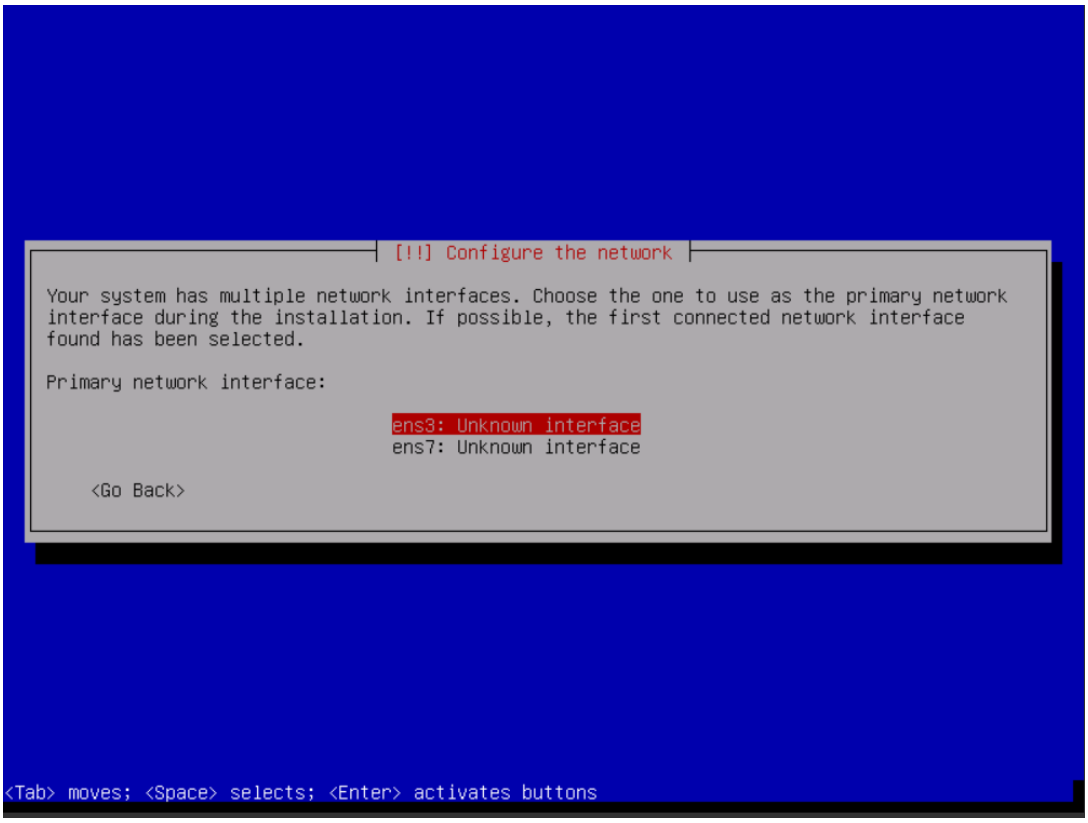
postavljanje odrađuje korisnik koristeći VNC terminal koji ima i mogućnost udaljenog prikaza grafičkog sučelja. Ulaskom na VNC terminal pojavljuje se početni prozor (slika 17.) za instalaciju.



Slika 16. Prikaz početnog prozora za instalaciju Debian-a

Odabirom opcije Install pojavljuju se okviri a kojima je potrebno za jezik sustava odabrati Engleski, a za lokaciju Hrvatska. Nakon odabira jezika sustava i lokacije potrebno je odabrati standardne postavke za lokaciju i jezik tipkovnice, u ovom slučaju to će biti en_US.UTF-8 i hrvatska tipkovnica.

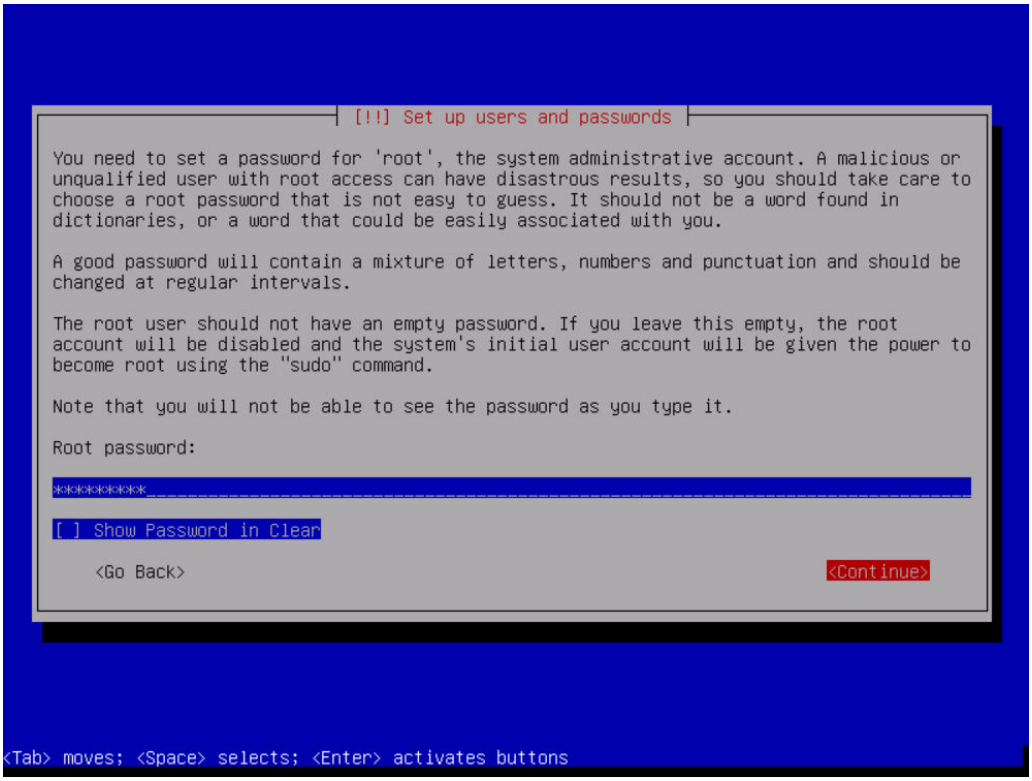
Nakon jezičnih postavki, slijede mrežne postavke. Prvi prozor, vidljiv na slici 18, omogućava odabir primarne fizičke mrežne kartice, pošto poslužitelj ima dvije. Odabrana je prva mrežna kartica.



Slika 17. Prikaz odabira fizičke mrežne kartice

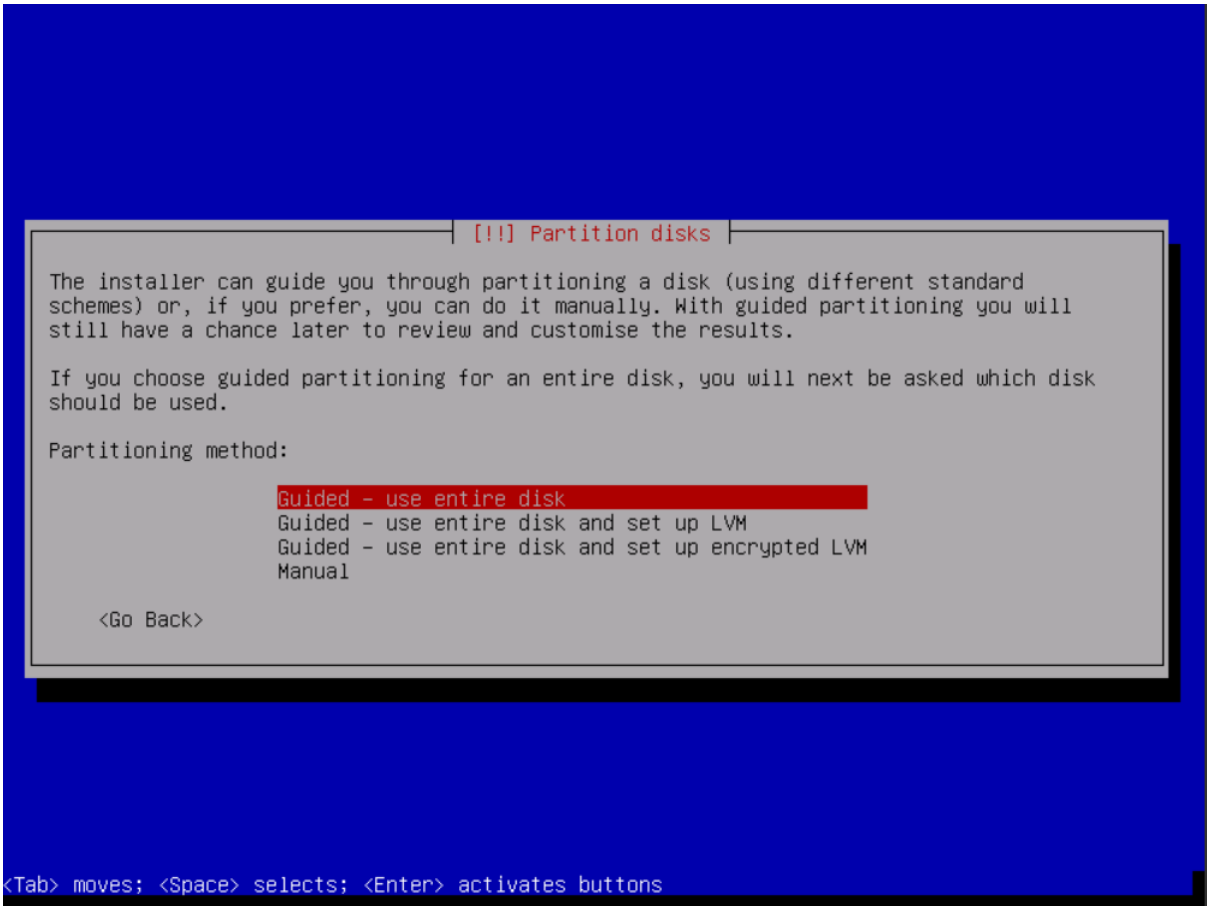
Sljedeći koraci je unos imena sustava (eng. hostname) i mrežne domene (eng. domain). Naziv sustava je proizvoljan, u ovom slučaju je to DebianCheckMK dok je se za domenu potrebno ostaviti već ponuđenu opciju.

Nakon mrežnih postavki, provode se koraci vezani za korisničke račune. Prvi od takvih koraka je unos lozinke za administratorski odnosno „root“ račun (slika 19.). Lozinka se unosi dva puta kako bi otklonile pogreške kod unosa. Isto tako, potrebno je kreirati račun uz pripadajuće korisničko ime i lozinku koji će se koristiti za neadministratorske aktivnosti. Lozinku je također potrebno unijeti dva puta.



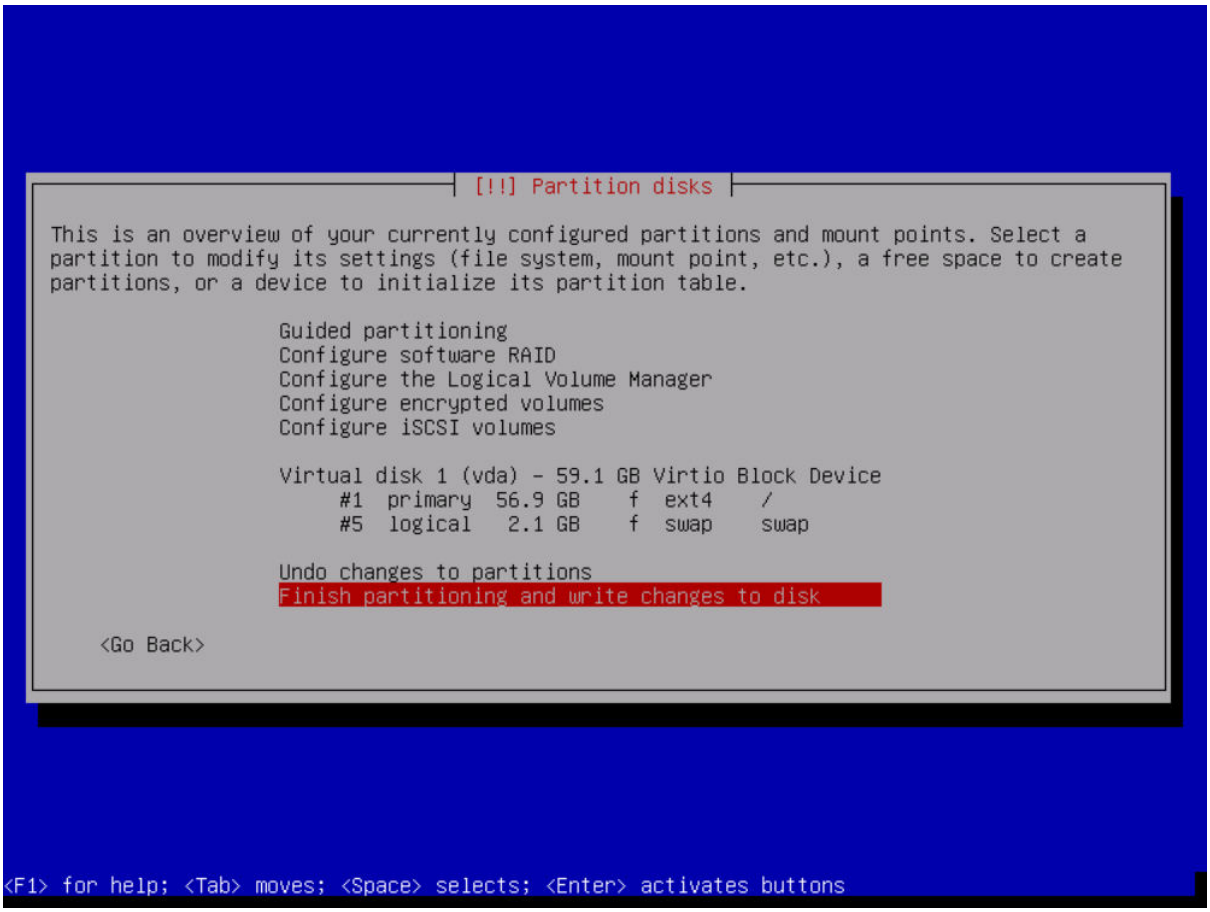
Slika 18. Prikaz unosa lozinka za "root" korisnika

Sljedeći koraci odnose se na izradu particija na fizičkom disku poslužitelja i odabir na kojoj će se particiji instalirati operacijski sustav. Prvi korak je odabir načina izrade particija, u ovom slučaju to će biti *Guided-Use entire disk* (slika 20.).



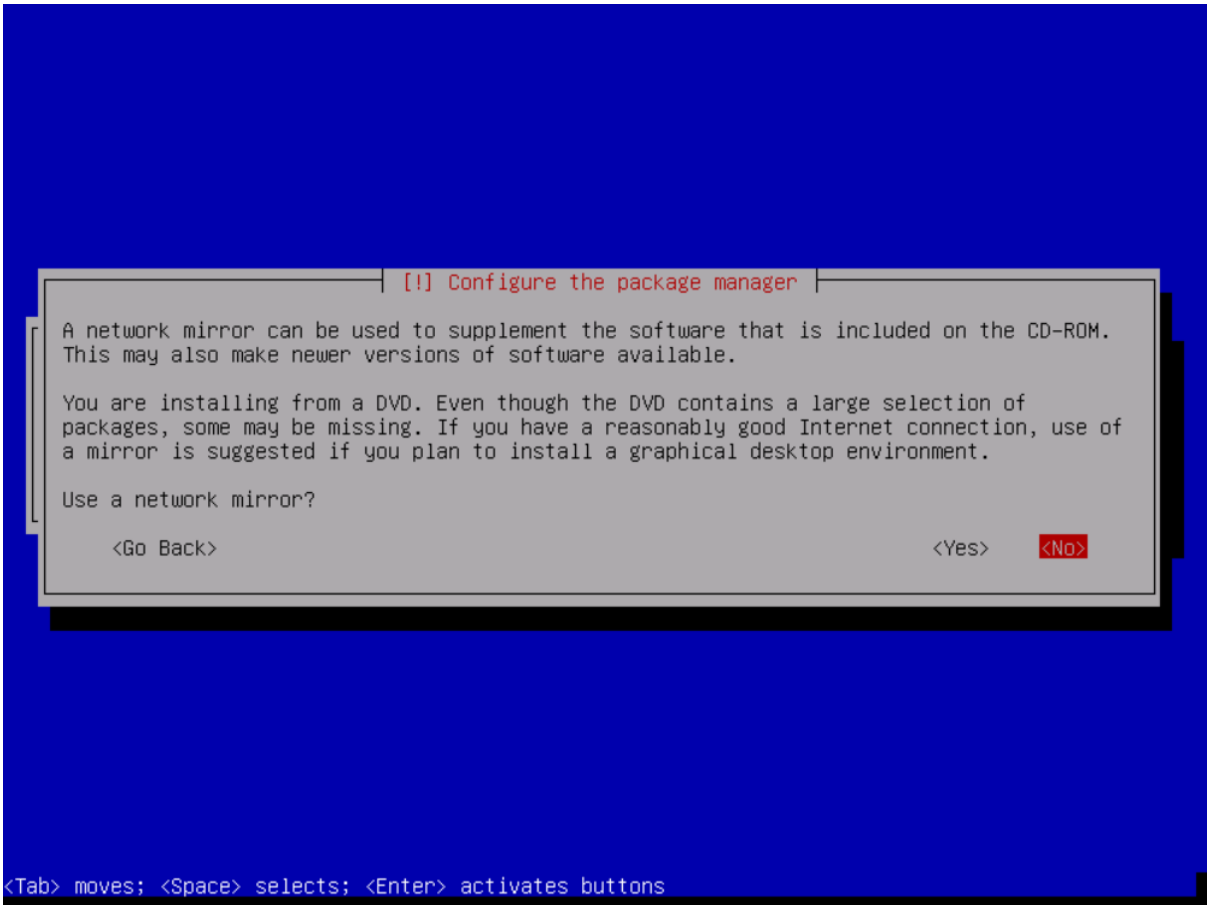
Slika 19. Prikaz odabira metode particioniranja

Nakon odabira metode particioniranja potrebno je odabrati shemu particioniranja. Za ove potrebe odabrana je shema smještanja svih datoteka na jednu particiju (eng. All files in one partition). Nakon odabrane sheme odabire se fizički disk na koji će se odnositi postavke nakon čega slijede završni koraci u kojima se omogućuju dodatno postavljanje poput iSCSI i RAID polja, LVM-a itd. U slučaju da dodatno postavljanje nije potrebno, odabire se završetak postavljanja i promjene se zapisuju (slika 21.).



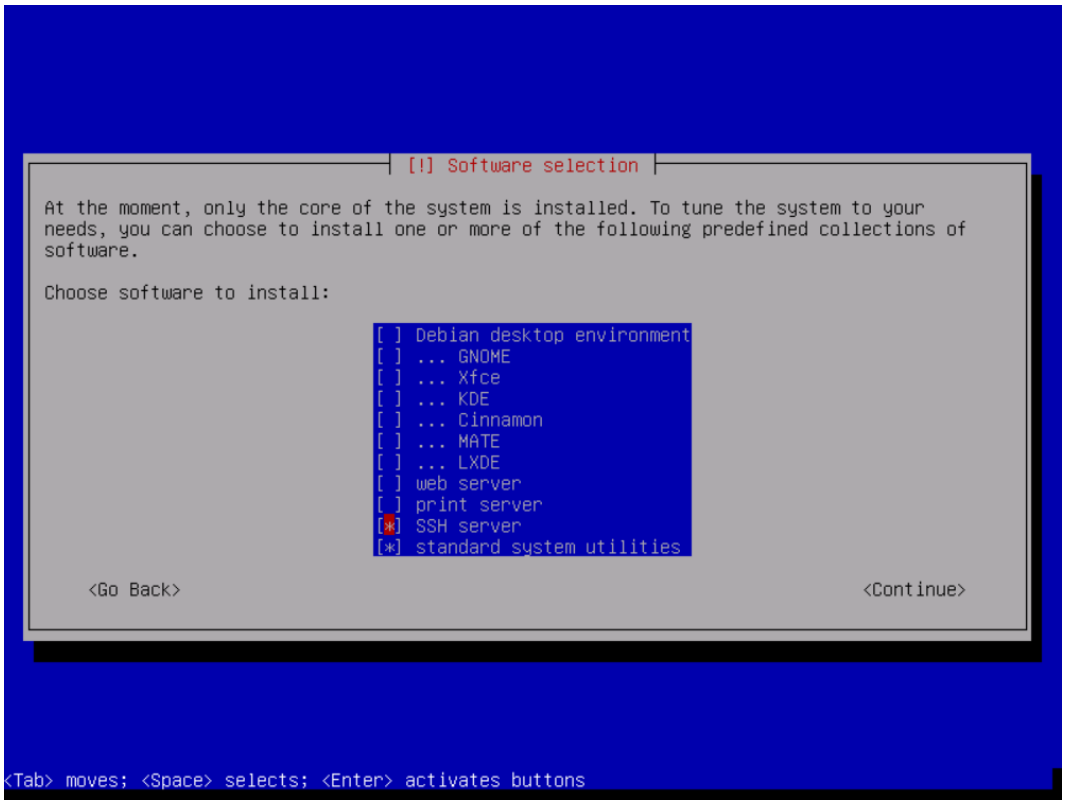
Slika 20. Prikaz završnog koraka konfiguracije particija

Nakon ovih koraka slijede završni koraci instalacije gdje je korisniku omogućeno skeniranje i korištenje dodatnih vanjskih medija. Također se korisniku omogućuje uključivanje mirror instalacije paketa (slika 22.) što svakako treba uključiti jer paketi koji će se kasnije instalirati na ovom sustavu možda neće postojati na izvornom repozitoriju već će se koristiti službeni Debian repozitorij za dohvaćanje istih.

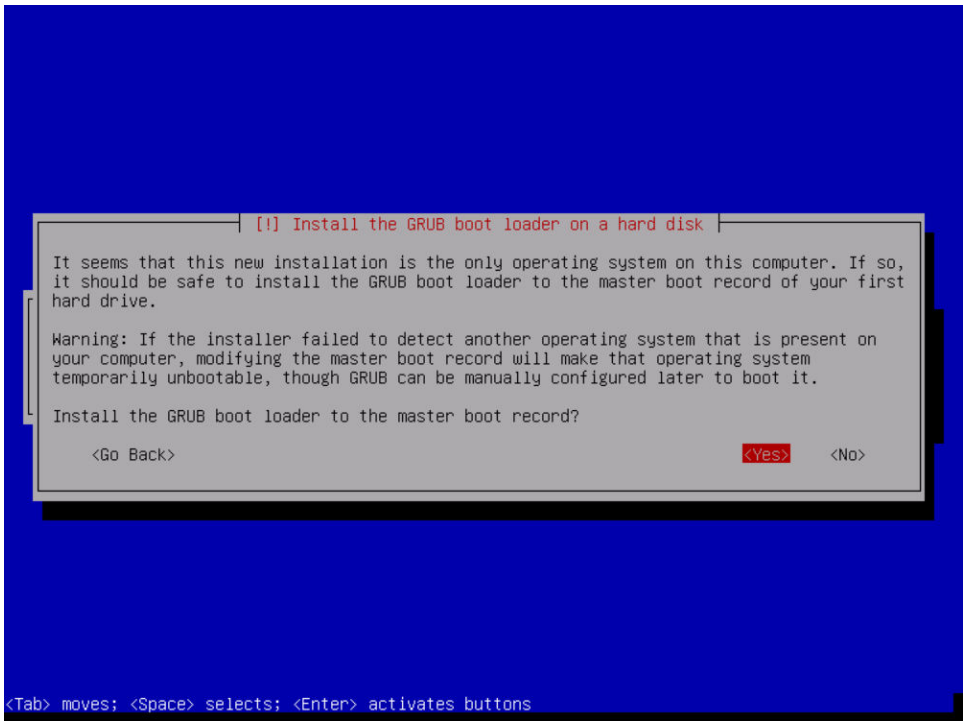


Slika 21. Prikaz uključivanja mirror instalacija

U sljedećim koracima potrebno je odabrati početne pakete koji će se instalirati (slika 23) i također je potrebno odobriti instalaciju GRUB pokretača operacijskog sustava (eng. boot loader) (slika 24.), nakon čega će se pojaviti prozor s porukom o uspješnoj instalaciji sustava.



Slika 22. Prikaz odabira instalacije programa



Slika 23. Prikaz instalacije GRUB boot loader-a

Nakon završne poruke, potrebno je ukloniti instalacijsku sliku koja je odabrana na početku instalacije i poslužitelj će se ponovno pokrenuti. Prilikom ponovnog pokretanja poslužitelj je spreman za daljnji rad, no u početnoj konfiguraciji onemogućen mu je pristup putem SSH klijenata. Kako bi se pristup odobrio potrebno se prijaviti u sustav sa administratorskim računom te se pozicionirati u mapu */etc/ssh/* i otvoriti datoteku *sshd_config* pomoću *nano* uređivača. Unutar *sshd_config* datoteke potrebno je promjeniti zapis *#PermitRootLogin without-password* u *PermitRootLogin yes* te spremiti promjene u datoteci. Nakon spremanja promjena potrebno je ponovno pokrenuti SSH servis pomoću naredbe:

/etc/init.d/ssh restart

3.3.1. Instalacija Postfix agenta

Prije samog početka instalacije Postfix servisa potrebno je provjeriti FQDN poslužitelja. Potpuno kvalificirani naziv domene ili FQDN (Fully Qalified Domain Name) je puni naziv poslužitelja koji se sastoji od naziva operacijskog sustava i domene. Provjera FQDN naziva je moguća pomoću naredbe:

hostname -f

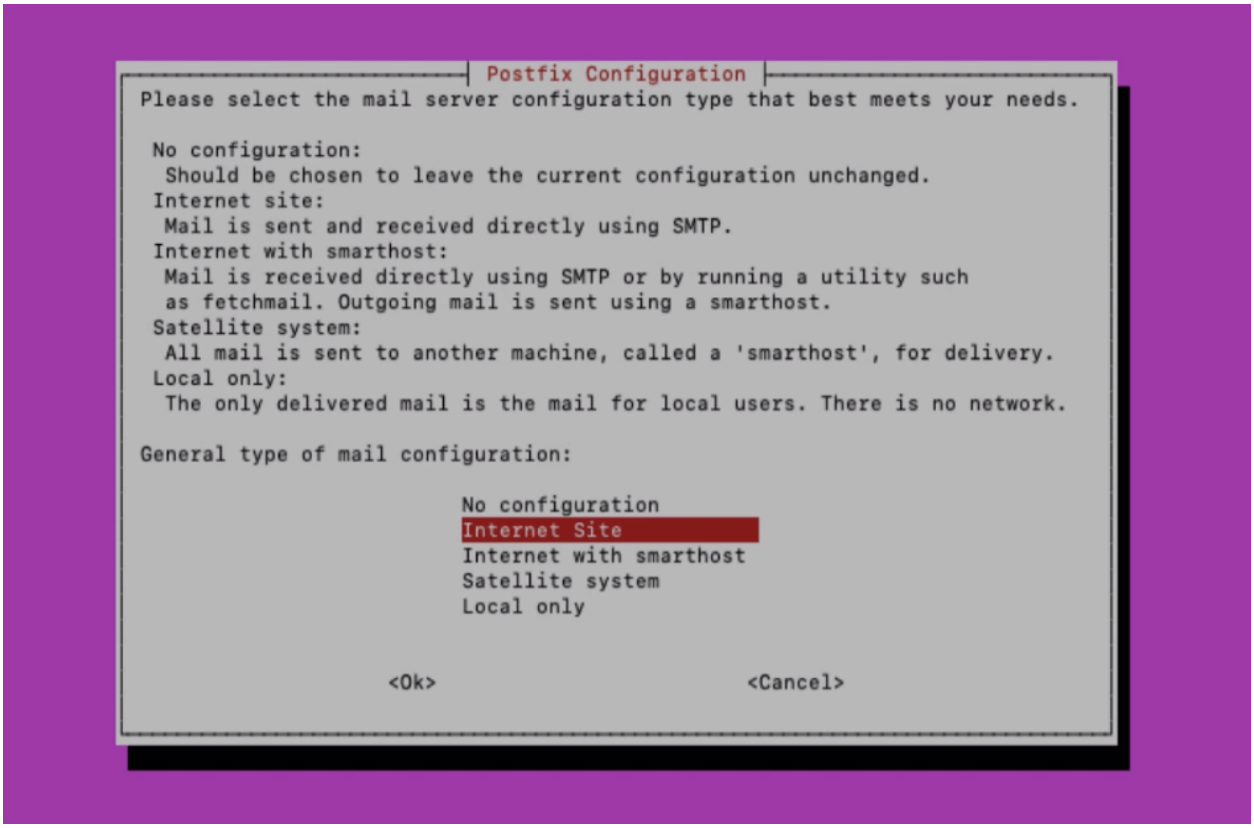
Rezultat pokrenute naredbe je *DebianCheckMK.179.138.158.vultr.com.* FQDN naziv će biti kasnije potreban za konfiguraciju Postfix-a. FQDN naziv je također potrebno unijeti kao pseudonim (eng. alias) u datoteku */etc/hosts*. Zapis u *hosts* datoteci je vidljiv ispod.

127.0.1.1 DebianCheckMK.179.138.158.vultr.com DebianCheckMK

Nakon napravljenih izmjena, potrebno je ponovno pokrenuti poslužitelj. Instalacija Postfix-a se pokreće pomoću sljedeće naredbe:

sudo apt-get install mailutils

Tijekom instaliranja *mailutils* paketa pojavit će se prozor kao na slici 25, na kojem treba odabrati odgovarajuće postavke mail poslužitelja. U ovom slučaju će biti odabrana Internet Site opcija koja omogućuje direktno slanje elektroničke pošte koristeći SMTP protokol. U sljedećem prozoru je potrebno upisati FQDN naziv i završiti postavljanje.



Slika 24. Prikaz odabira postavki mail poslužitelja

Kako će se za odredišnu mail adresu koristiti prethodno kreirani gmail račun, potrebno je dodatno izmijeniti postavke Postfix-a. Prvi dio izmjena se radi u datoteci */etc/postfix/main.cf.*

Unutar main.cf datotetke potrebno je napraviti sljedeće promjene:

- vrijednost varijable *Releyhost* postaviti u *[smtp.gmail.com]:587*
- u vrijednost varijable mydestination dodati *localhost.vultr.com* i *localhost. 179.138.158.vultr.com*

Također je potrebno provjeriti vrijednost varijable *hostname* i odgovara li vrijednosti FQDN naziva. Na kraju main.cf datoteke potrebno je unijeti sljedeće parametre:

- *smtp_sasl_auth_enable* = *yes* – omogućava SASL autentifikaciju za Postfix,
- *smtp_sasl_security_options* = noanonymous -zabranjuje anonimni način autentifikacije,
- *smtp_sasl_password_maps* = hash:/etc/postfix/sasl/sasl_passwd – označava lokaciju spremanja SASL loziniki,

- *smtp_tls_security_level = encrypt*- omogućava STARTTLS enkripciju za SMTP,
- *smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt* – označava lokaciju na kojoj je smješten TLS certifikat.

Nakon spremanja izmjena u main.cf datoteci nužno je napraviti izmjene u sasl_passwd datoteci. U spomenutu datoteku potrebno je dodati slijedeću liniju:

*[smtp.gmail.com]:587 checkmk0.moniotring@gmail.com:<<**Lozinka**>>*

Nakon dodavanje gore navedene linije, potrebno je spremiti promjene i pokrenuti slijedeću naredbu:

postmap /etc/postfix/sasl/sasl_passwd

Postmap naredba pretvara sasl_passwd datoteku u sasl_passwd.db tip datoteke i briše izvornu datoteku. Nad novo kreiranoj datoteci potrebno je izmijeniti prava pristupa pomoću naredbi:

chown root:root /etc/postfix/sasl/sasl_passwd.db

chmod 600 /etc/postfix/sasl/sasl_passwd.db

Na kraju, potrebno je ponovno pokrenuti Postfix servis koristeći slijedeću naredbu:

service postfix restart

Kao posljednji korak postavljanja sustava obavijesti, u postavkama Gmail računa potrebno odobriti autentifikaciju i slanje pošte putem SMTP protokola manje sigurnim aplikacijama.

Kako bi se provjerila uspješna konfiguracija Postfix-a može se poslati mail poruka putem komandne linije.

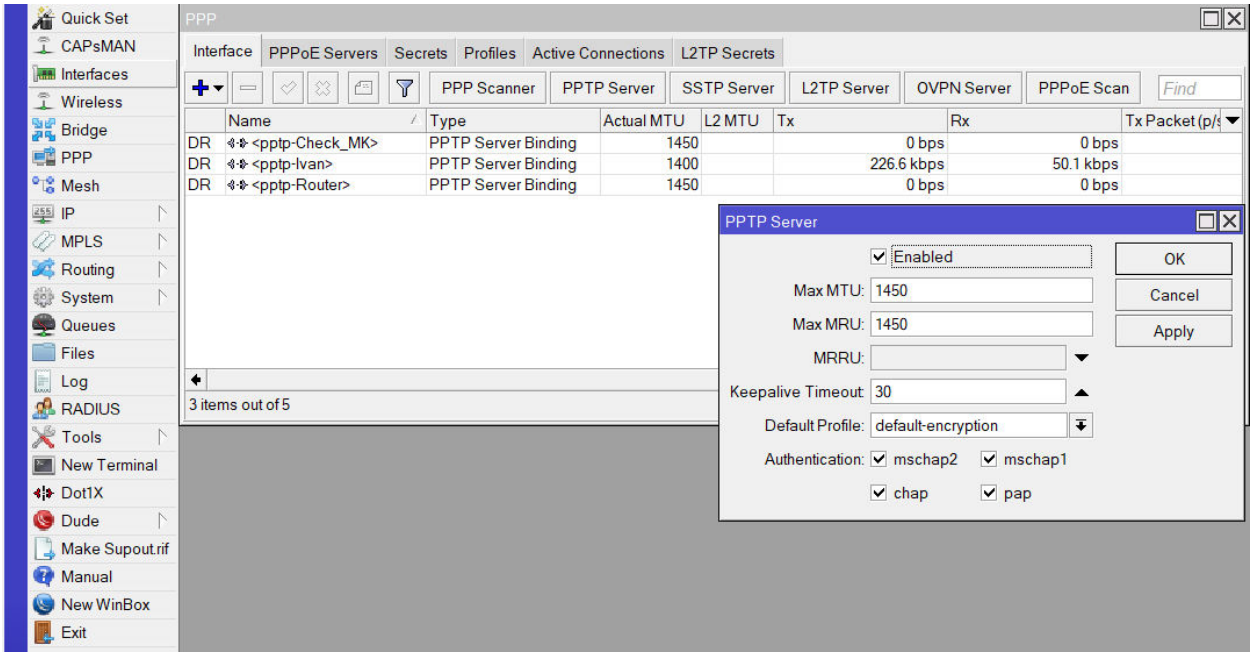
echo "Ovo je testni mail!" | mail -s "Testni mail!" checkmk0.monitoring@gmail.com

3.3.2. Instalacija i postavljanje PPTP servisa

U svrhu postavljanja PPTP tunela između dva VPS poslužitelja, ali i općenito između PPTP klijenta i PPTP poslužitelja, potrebno je kreirati PPTP profil za spajanje na obje strane.

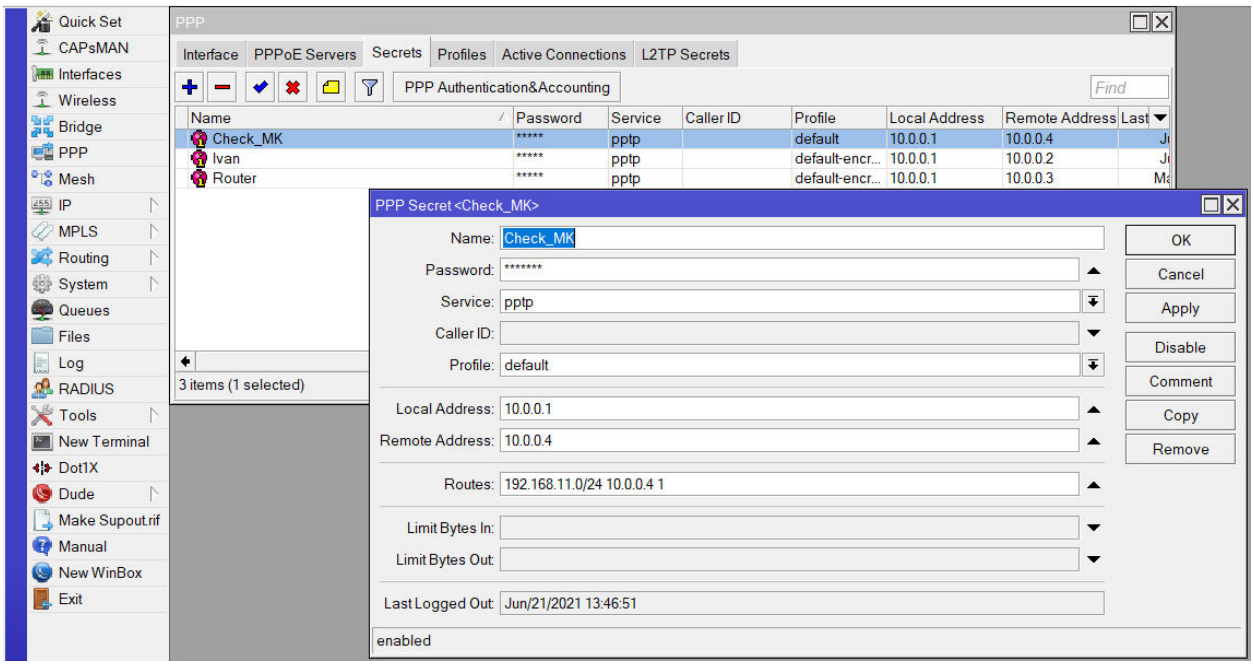
Profili za spajanje moraju sadržavati istu lozinku i korisničko ime kako bi spajanje proteklo uspješno.

Prvi korak je kreiranje profila na poslužiteljskoj strani. Kako bi RouterOS dopustio spajanje PPTP klijenata potrebno je omogućiti rad PPTP poslužitelja. PPTP poslužitelj se pokreće na kartici *PPTP Server* (slika 26.) u *PPP* izborniku.



Slika 25. Prikaz pokretanja PPTP poslužitelja

Nakon pokretanja PPTP poslužitelja, potrebno je kreirati profil. Kreiranje profila za spajanje na poslužiteljskoj strani omogućava upravljanje uspostavljanjem PPTP tunela prema klijentima inače bi se svaki klijent koji zatraži spajanje spojio bez ikakve provjere. Profil za spajanje se kreira na kartici *Secrets* (slika 27.) u *PPP* izborniku.



Slika 26. Prikaz kreiranja PPTP profila na PPTP poslužitelju

Prilikom kreiranja profila, od korisnika se traži unos sljedećih informacija:

- *Name* - korisničko ime
- *Password* - lozinka
- *Tip konekcije* - označava vrstu virtualnog tunela
- *Local Address* - odnosi se na lokalnu adresu PPTP tunela, najčešće se odabere prva adresa u odabranom skupu adresa. U ovom radu je odabran skup adresa 10.0.0.0/24. Local Address se može definirati kao adresa virtualnog usmjernika i za sve PPTP konekcije je preporučljivo koristiti istu.
- *Remote Address* - odnosi se na adresu koju će imati PPTP klijent.
- *Routes* - unosom ruta omogućuje se vidljivost odabrane privatne mreže preko PPTP tunela. Na ovaj način će CheckMk imati mogućnost nadzora svih uređaja koji imaju IP adresu iz navedene mreže. U ovom slučaju će biti dostupni svi uređaji koji se nalaze u mreži 192.168.11.0/24.

Nakon kreiranja profila na poslužitelju, slijedi kreiranje profila za spajanje na klijentskoj strani.

Instalacija PPTP klijenta na Debianu 9 pokreće se naredbom:

apt-get install pptp-linux

Nakon instalacije slijedi kreiranje klijentskog profila kojim će se poslužitelj spajati na MikroTik CHR.U ovom slučaju CHR ima ulogu PPTP poslužitelja na kojeg se spajaju svi PPTP klijenti, kao što je i prikazano na shemi na početku ovog poglavlja.

Za kreiranje klijentskog profila potrebna je izmjena dviju datoteka:

- */etc/ppp/chap-secrets* - koristi se za pohranu korisničkog imena i lozinke koje će PPTP konekcija koristiti prilikom autentikacije za vrijeme spajanja.
- */etc/ppp/peers/myvpn-name* – datoteka koja sadrži sve informacije o klijentskom profilu. Naziv datoteke je proizvoljan pošto svaka datoteka označava pojedini profil.

Podaci koji su potrebni za kreiranje profila su:

- adresa PPTP poslužitelja - odnosi se na javnu IP adresu MikroTik CHR-a,
- korisničko ime - proizvoljno korisničko ime koje mora biti isto kao i kod kreiranog profila na PPTP poslužitelju,
- lozinka - proizvoljna lozinka koja mora biti ista kao i kod kreiranog profila na PPTP poslužitelju,
- tip konekcije – PPTP,
- enkripcija - odnosi se na razinu enkripcije podataka, najčešće se odabire najviša moguća razina, a to je trenutačno MPPE 128-bitna enkripcija,
- dodatni parametar - proizvoljno ime konekcije koje može koristiti kod pokretanja, zaustavljanja i korištenja ostalih akcijama nad konekcijom.

Pohrana korisničkog imena i lozinke u chap-secrets datoteku izgleda ovako:

<<KorisničkoIme>> *PPTP* ***<<Lozinka>>*** ***

Nakon spremanja izmjena u *chap-secrets* datoteci, potrebno je dodati ostale informacije vezane za profil u prethodno kreiranu datoteku. Naziv datoteke se unosi po želji. Sadržaj datoteke se piše u slijedećem obliku:

pty "pptp ***<<adresa PPTP poslužitelja>>*** *--nolaunchpppd"*

name ***<<KorisničkoIme>>***

remotename PPTP

require-mppe-128

file /etc/ppp/options.pptp

ipparam ***<<NazivKonekcije>>***

Linija *file /etc/ppp/options.pptp* označava putanju prema datoteci iz koje će se povlačiti postavke nakon uspostave konekcije.

Povezivanja na PPTP poslužitelj pokreće se slijedećom naredbom:

pppd call ***<<NazivKonekcije>>***

Pokretanjem prethodne naredbe, životni vijek PPTP tunela će trajati do sljedećeg ponovnog pokretanja poslužitelja. Kako bi se postiglo automatsko pokretanje nakon svakog podizanja sustava, potrebno je dodati sljedeće izmjene u datoteku */etc/network/interfaces*:

auto tunnel

iface tunnel inet ppp

provider ***<<NazivKonekcije>>***

Ako je povezivanje proteklo uspješno, pozivanjem slijedeće naredbe mogu se vidjeti poruke koje prikazuju uspješno spajanje na PPTP poslužitelj.

tail -f /var/log/messages

Za sva spajanja budućih klijenata potrebno je na poslužiteljskoj strani kreirati profil za novog klijenta, dok konfiguracija na strani klijenta ovisi o vrsti uređaja ili sustava prema kojem želimo uspostaviti PPTP tunel. Primjerice, ako je PPTP klijent fizički MikroTik usmjernik, potrebno je u istom izborniku kreirati PPTP klijentski profil. Ovaj primjer će biti opisan u sljedećem poglavlju.

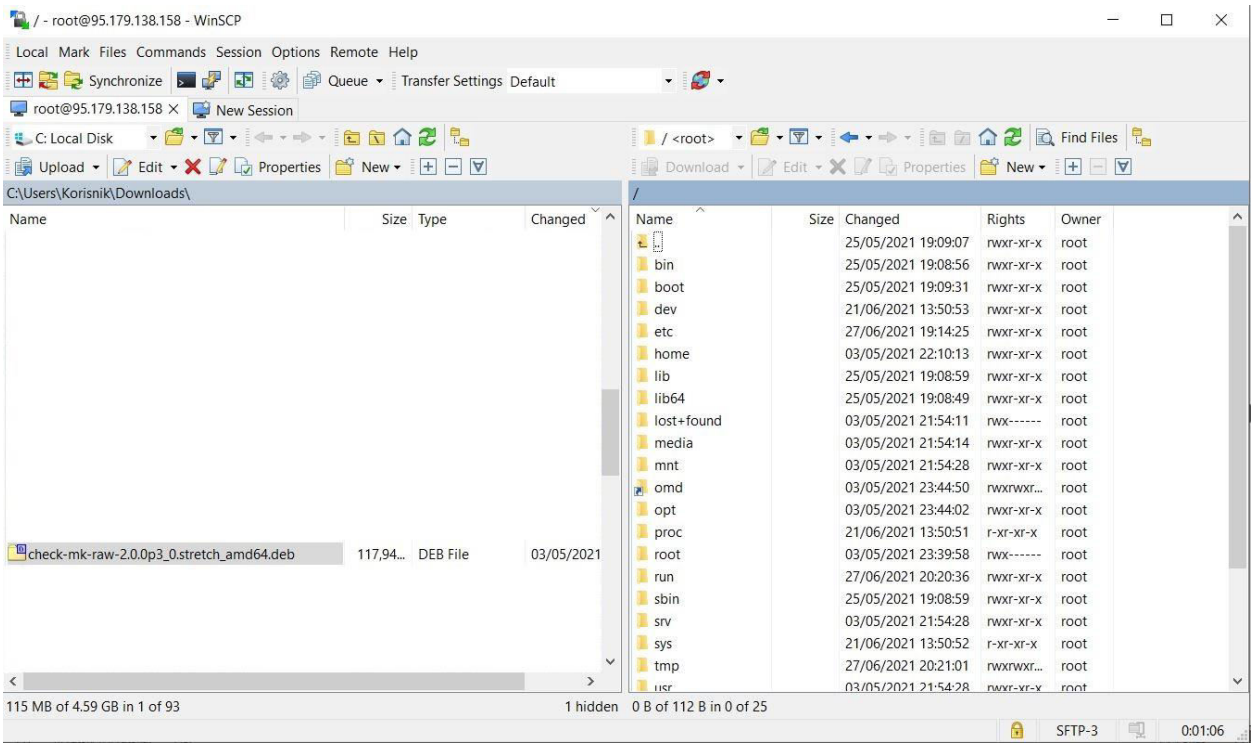
3.4. Instalacija CheckMk sustava

Prije same instalacije potrebno je preuzeti instalacijski paket sa službenih stranica. U ovom završnom radu korištena je besplatna raw verzija Checkmk sustava. Nakon preuzimanja instalacije, istu je potrebno kopirati na poslužitelj. Kopiranje se obavlja putem Protokola

sigurnog kopiranja ili SCP (Secure Copy Protocol) protokola koji koristi sigurnosni mehanizam SSH protkola kako bi se podaci prenijeli na siguran način. SCP se može omogućiti instalacijom openssh-server paketa nakon kojeg je kopiranje moguće obaviti pomoću slijedeće naredbe:

scp check-mk-raw-2.0.0p3_0.stretch_amd64.deb root@DebianCheckMK:/

Alternativa je korištenje jednog od besplatnih SCP klijenta, poput WinSCP programa. SCP klijenti omogućuju lakše kopiranje datoteka na odredište putem grafičkog sučelja. Prije samog prebacivanja prijaviti se u odredišni sustav istim pristupnim podacima kao i kod SSH pristupa. Slika broj 28 prikazuje WinSCP klijent. Akcija kopiranja se izvršava povlačenjem i puštanjem (eng. drag and drop) datoteke sa izvorišnog mjesta na željeno odredišno mjesto.



Slika 27. Prikaz kopiranja instalacijskog paketa na poslužitelj

Nakon kopiranja se provode naredbe za provjeru valjanosti instalacijskog paketa. Naredbe su:

apt install dpkg-sig

wget https://download.checkmk.com/checkmk/Check_MK-pubkey.gpg

apt-key add Check_MK-pubkey.gpg

dpkg-sig --verify check-mk-raw-2.0.0p3_0.focal_amd64.deb

Prvom naredbom se instalira paket koji omogućuje provjeru Checkmk instalacije. Drugom naredbom se preuzima javni ključ sa službenih stranica. Trećom naredbom se prethodno preuzeti javni ključ uvrštava u popis vjerodajnica, dok posljednja naredba omogućuje provjeru samog instalacijskog paketa.

Nakon uspješne provjere pokreće se naredba za instalaciju Checkmk sustava na poslužitelj.

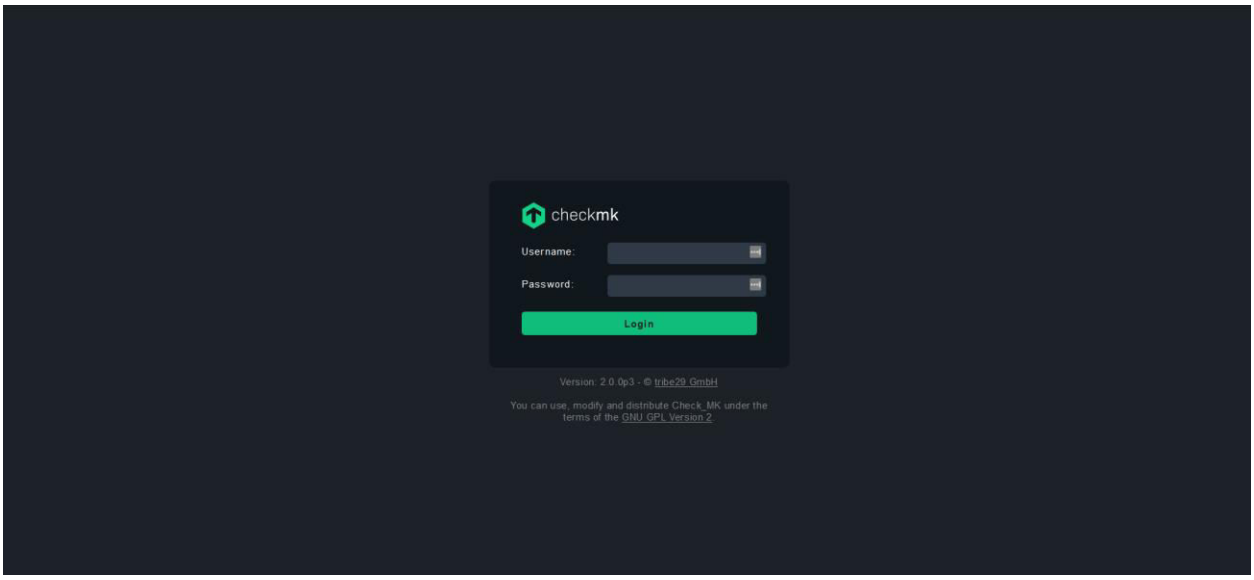
apt install /check-mk-raw-2.0.0p3_0.stretch_amd64.deb

Nakon završene instalacije kreira se i pokreće Checkmk instanca pomoću slijedećih naredbi:

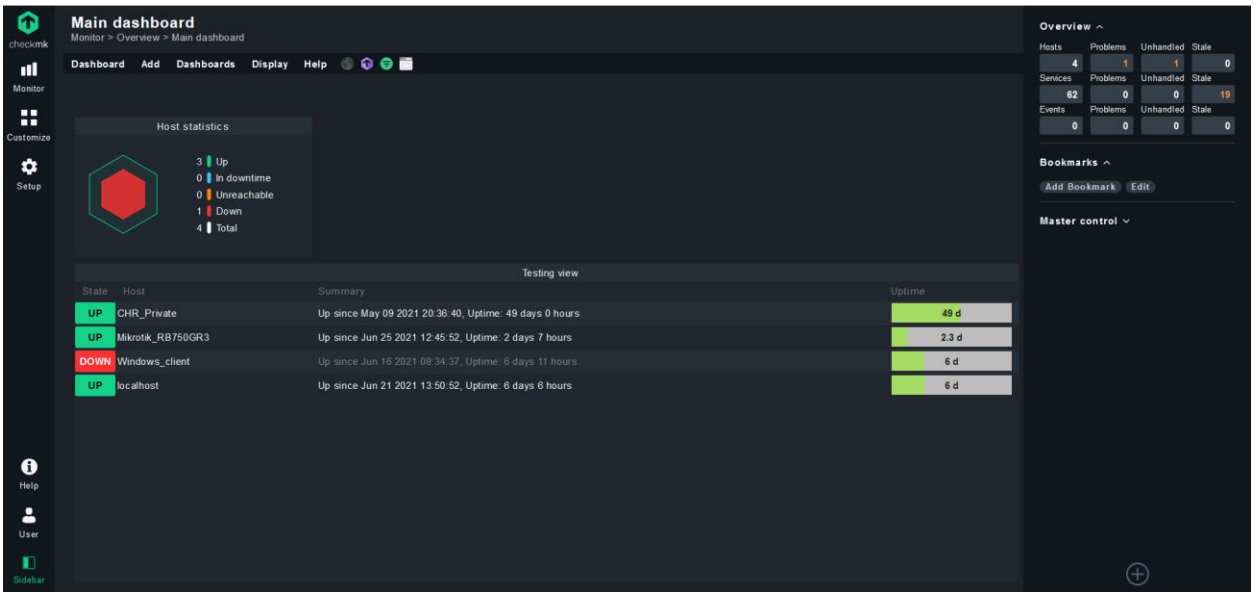
omd create checkmkmonitor

omd start checkmkmonitor

Instanca koja je kreirana naziva se checkmkmonitor. Naziv instance je proizvoljan i instanci se može kreirati više, ovisno o potrebama. Nakon kreiranja instance pojavljuje se poruka koja prikazuje korisničko ime (cmkadmin) i slučajno kreiranu lozinku koja služi za inicijalnu prijavu u sustav. Sustavu se pristupa putem internet pretraživača preko adrese *http://95.179.138.158/checkmkmonitor* (slika 29.). Nakon prijave u sustav potrebno je napraviti novi administratorski račun ili barem promijeniti lozinku cmkadmin računa. Slika 30. prikazuje korisničko sučelje Checkmk sustava.



Slika 28. Prikaz prozora za prijavu

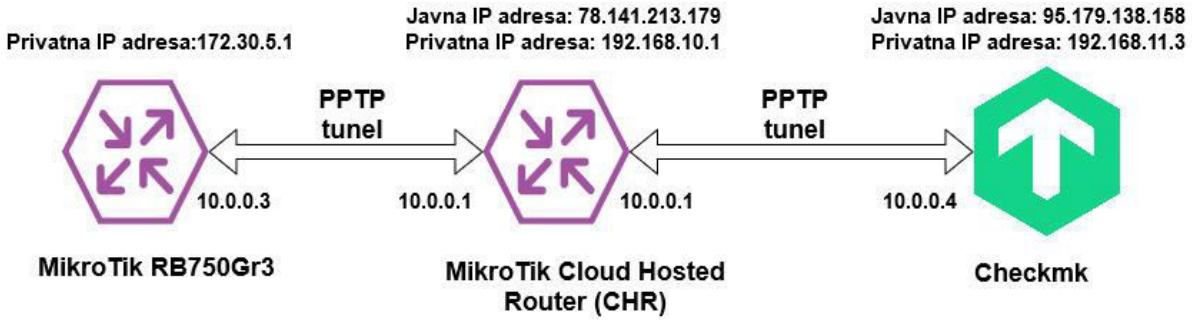


Slika 29. Prikaz korisničkog sučelja Checkmk sustava

3.5. Primjer konfiguracije nadzora i omogućavanje pristupa udaljenim mrežama

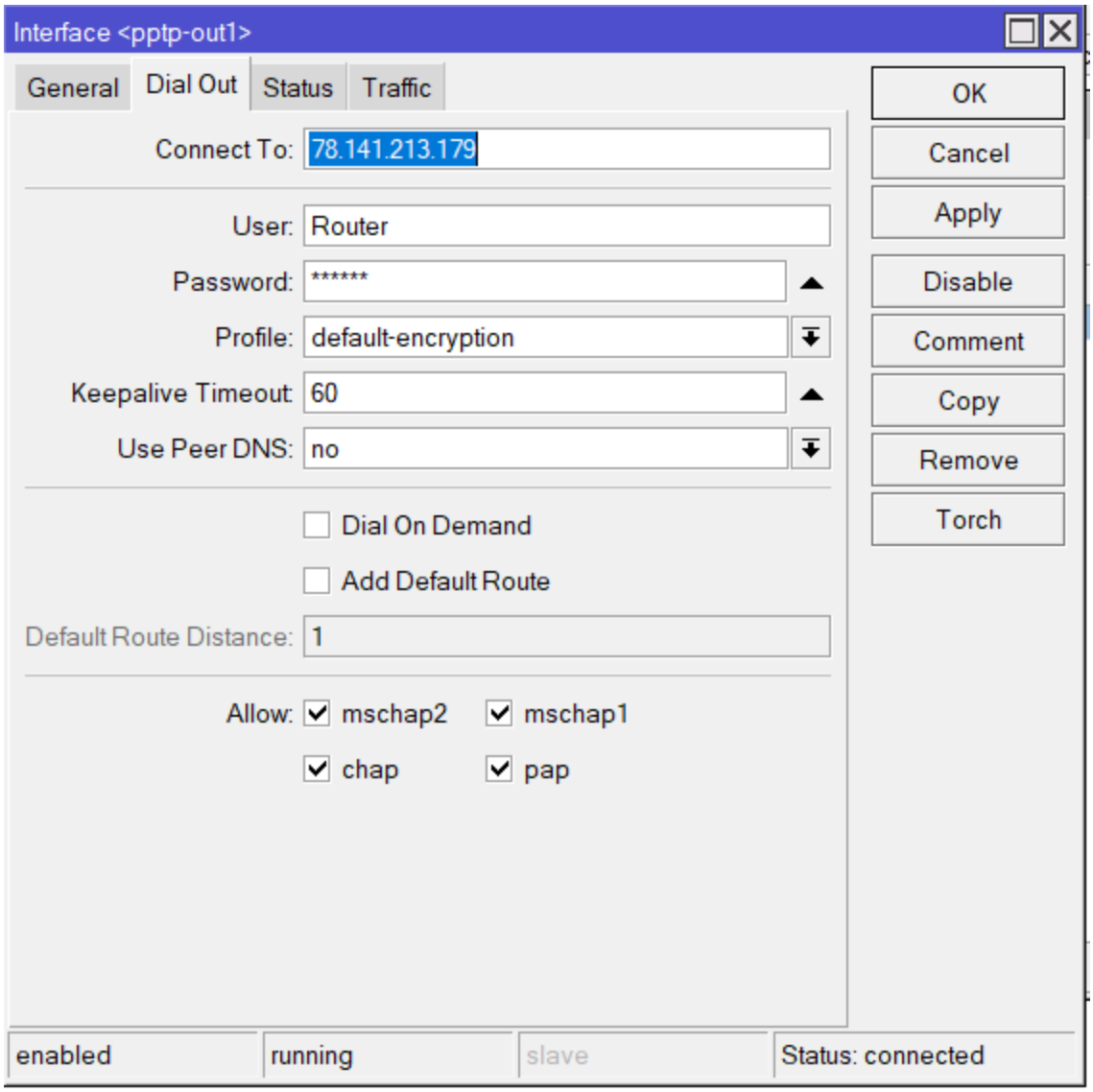
Kao praktični primjer kojim će se pokazati funkcije sustava obavit će se konfiguracija za nadzor i pristup fizičkom usmjerniku MikroTik RB750Gr3. Fizički usmjernik je priključen u udaljenu privatnu mrežu. IP adresa usmjernika je postavljenja proizvoljno i u ovom slučaju je to 172.30.5.1. Ovim primjerom, cilj je omogućiti udaljeni pristup usmjerniku na adresi 172.30.5.1 i

svim uređajima koje se nalaze u istoj mreži (172.30.5.0/24). Slika 31. prikazuje načelnu shemu kako sustav nadzora i pristupa funkcionira.



Slika 30. Prikaz sheme za konfiguraciju fizičkog usmjernika iz primjera

U prethodnim poglavljima opisan je način spajanja PPTP klijenta i poslužitelja (CHR-a i Debian-a), a na isti način se povezuje CHR (PPTP poslužitelja) sa fizičkim usmjernikom (PPTP klijent). Jedina razlika je u polju za unos udaljene adrese (eng. remote address) polju koje mora biti različito za svakog PPTP klijenta. Slika 32 prikazuje kreiranje klijentskog PPTP profila na fizičkom usmjerniku uz prethodno kreiranje profila na poslužiteljskoj strani.



Slika 31. Prikaz kreiranja klijentskog PPTP profila

Nakon kreiranja promjena, PPTP tunel se automatski uspostavlja, ako su uneseni podaci točni. U ovom trenutku Checkmk i fizički usmjernik su spojeni PPTP tunelima na CHR, međutim, još uvijek nije moguće nadzirati fizički usmjernik na Checkmk-u. Kako bi nadzor bio moguć, potrebno je napraviti mrežne pravce na obje strane, na CHR-u i na Checkmk-u, kako bi se fizički usmjernik i Checkmk međusobno vidjeli. Na CHR strani je potrebno u PPTP profilu unijeti slijedeću rutu:

172.30.5.0/24 10.0.0.3 1

Unesena ruta povezuje PPTP tunel i privatnu mrežu usmjernika. Oznaka 1 predstavlja broj skokova u ruti. U ovom trenutku nije omogućen nadzor, ali je moguće pristupiti fizičkom usmjerniku na adresi 172.30.5.1. S druge strane, na Debian-u, potrebno je također unijeti statičke rute prema odredišnim uređajima. Kako bi rute ostale i nakon ponovnog pokretanja sustava, potrebno je napraviti skriptu koja će se pokrenuti nakon podizanja operacijskog sustava. Skriptu sa proizvoljnim imenom je potrebno kreirati na putanji */etc/ppp/ip-up.d.* Sadržaj skripte je sljedeći:

#!/bin/bash

ip route add 10.0.0.0/24 via 10.0.0.4 dev ppp0

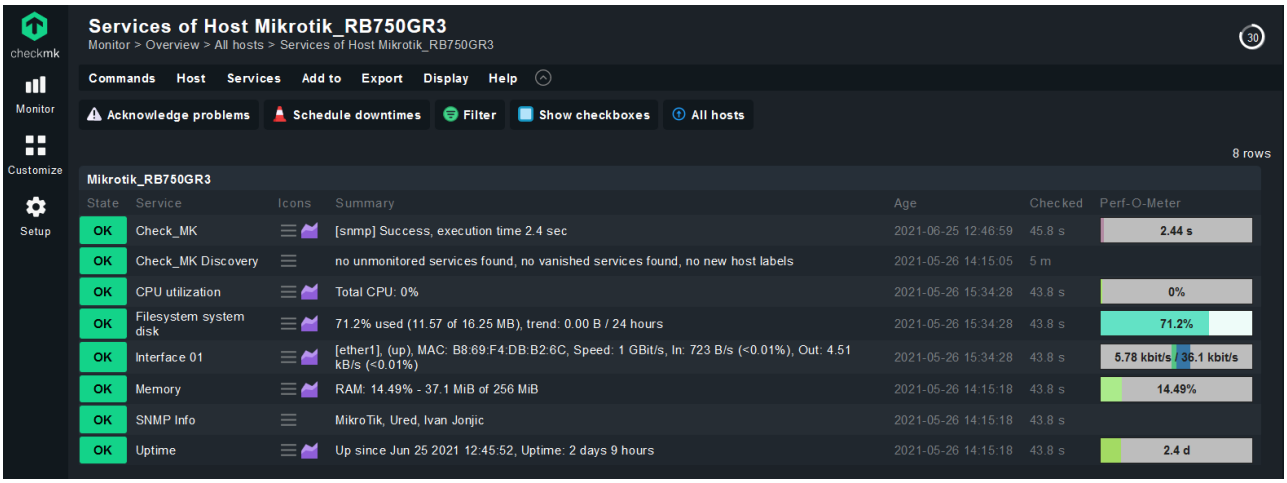
ip route add 192.168.10.0/24 via 10.0.0.4 dev ppp0

ip route add 172.30.5.0/24 via 10.0.0.4 dev ppp0

Prva ruta omogućava Debian poslužitelju, pa samim time i Checkmk sustavu vidljivost svih PPTP klijenata i poslužitelja u 10.0.0.0/24 mreži. Druga ruta omogućava vidljivost privatne mreže CHR usmernika, dok treća ruta omogućava vidljivost privatne mreže fizičkom usmjerniku. Kako bi fizički usmjernik mogao vidjeti Checkmk i CHR privatne mreže, potrebno je na njemu kreirati rute na isti način.

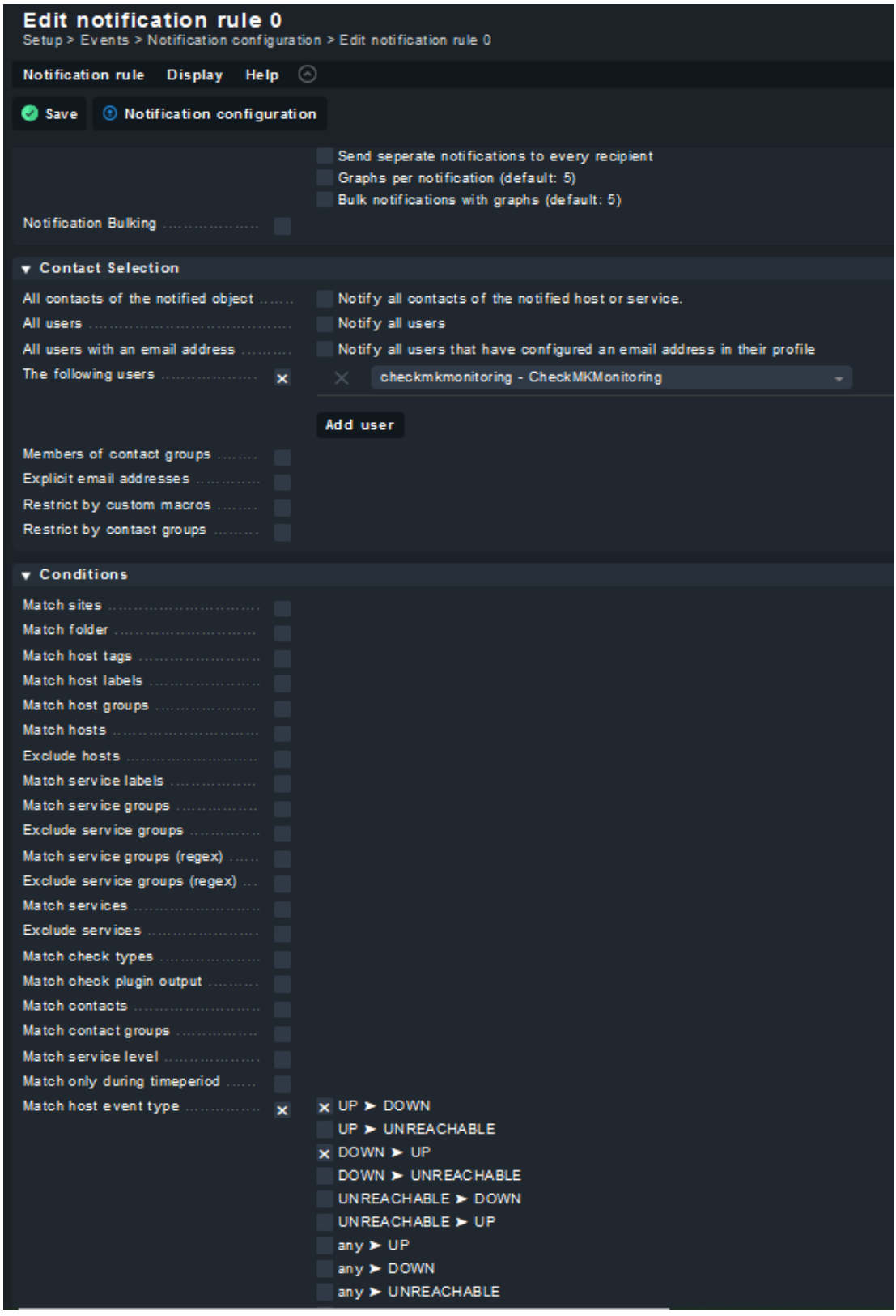
Nakon postavljenih ruta, slijedi dodavanje uređaja na Checkmk sustav. Uređaji se dodaju putem Setup izbornika korištenjem Hosts prozora. U Hosts prozoru se nalazi opcija za dodavanje novog uređaja kojeg se želi nadzirati. Klikom na dugme, otvara se okvir u kojem je potrebno unijeti informacije o uređaju. Najvažnije informacije su naziv uređaja, IP adresa ili DNS naziv i agent za nadzor. Agent za nadzor označava način nadziranja. Kako se radi o usmjerniku, u ovom slučaju je potrebno odabrati SNMP agenta. Na fizičkom usmjerniku je također potrebno omogućiti pružanje SNMP informacija. Ako se između uređaja i Checkmk sustava, u mreži nalaze i drugi uređaji korisno je dodati roditelj (eng. parents) i dijete (eng. childs) parametre. U ovom slučaju je potrebno dodati CHR kao roditelja.

Nakon unošenja svih potrebnih podataka, Checkmk automatski skenira uređaj i prikazuje sve servise i informacije koje može prikazivati i nadzirati. Administrator sam odabire što želi nadzirati. Slika 33. prikazuje informacije o fizičkom usmjerniku.



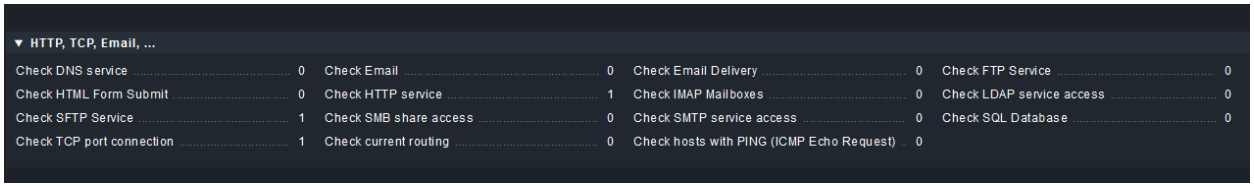
Slika 32. Prikaz nadziranih parametara fizičkog usmjernika

Prethodnom konfiguracijom postignut je nadzor i udaljeni pristup fizičkog usmjernika. Sada je potrebno dodati uređaj u sustav obavijesti. U ovom primjeru Checkmk će slati obavijesti samo kada fizički usmjernik ne bude dostupan i kada se vrati u dostupno stanje (UP-DOWN i DOWN-UP stanja). Konfiguracija obavijesti se obavlja u Events dijelu Setup izbornika. Potrebno je kliknuti na Notifications opciju koja će prikazati prozor za kreiranje pravila za obavijesti. Kao i kod dodavanja uređaja, klikom na dugme Add rule otvara se prozor koji omogućuje konfiguraciju pravila prema potrebama. Potrebno je unijeti naziv, odnosno kratki opis pravila, način obavještavanja (elektronička pošta), filtrirati za koje uređaje želimo slati obavijesti i kakve će se informacije slati u obavijestima. Slika 34 prikazuje pravilo za sve uređaje koji se nadziru. Obavijest će biti poslana samo ako uređaji promjene stanje u DOWN i obrnuto, iz stanja DOWN u stanje UP.



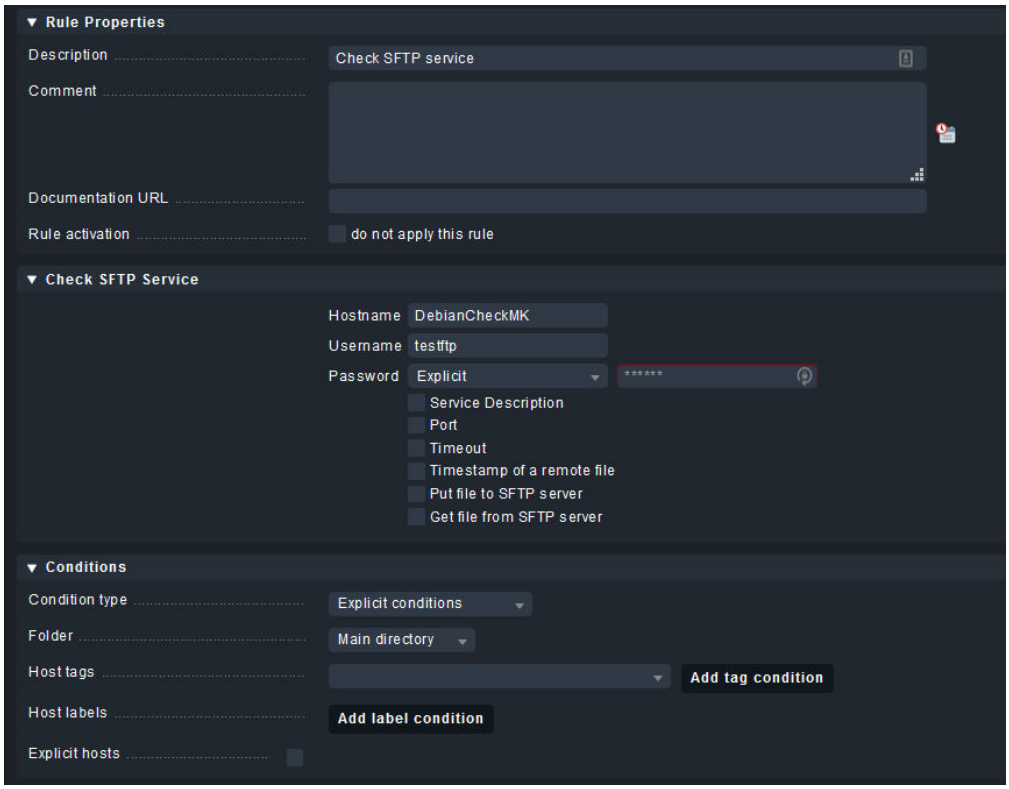
Slika 33. Prikaz postavki za slanje obavijesti

Kao dodatni primjer koji pokazuje širinu mogućnosti Checkmk sustava nadzora, na virtualni stroj instalirana su dva servisa, SFTP i Apache servis. Kako bi Checkmk mogao nadzirati stanje spomenutih servisa potrebno je kreirati pravila koja omogućuju aktivnu provjeru stanja spomenutih servisa. Pravila aktivne provjere servisa kreiraju se unutar *Setup* kartice klikom na *HTTP,TCP,Email…* poveznicu koja se nalazi u *Services* odjeljku. Slika 35 prikazuje popis servisa za koje je moguće kreirati pravila za aktivnu provjeru.



Slika 34. Prikaz servisa

Za nadzor SFTP i Apache servisa potrebno je napraviti pravila na poveznicama *Check SFTP Service* i *Check HTTP service.* Na *Check SFTP Service* je kreirano pravilo (slika 36) koje provjerava uspješnu prijavu SFTP korisnika na SFTP poslužitelj.

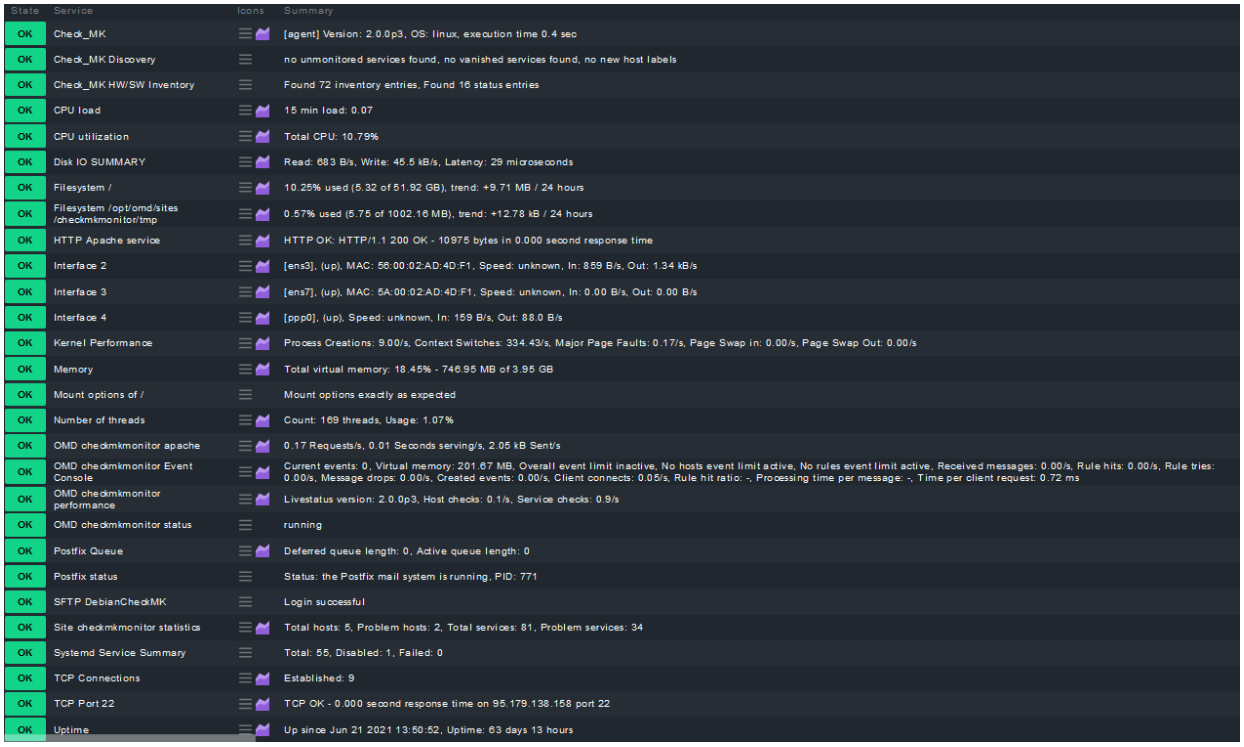


Slika 35. Postavke pravila za aktivnu provjeru SFTP servisa

Za provjeru Apache servisa odabrana je provjera HTTP poslužitelja. Kroz pravilo (slika 37.) je definirana provjera javne IP adrese 95.179.138.158 na priključku 80 kojeg HTTP servis koristi za komunikaciju.

Slika 36. Postavke pravila za aktivnu provjeru Apache/HTTP servisa

Kreirana pravila će se propagirati do svih dostupnih uređaja na mreži bez obzira na vrstu i funkciju. Kako bi se primjena pravila ograničila na željene resurse, u postavkama pravila potrebno je odabrati uređaje, u ovom slučaju to će biti poslužitelj na kojem su instalirani servisi. Nakon primijenjenih postavki, aktivne provjere za instalirane servise će se pojaviti na pregledu parametara koji nadziru na navedenom poslužitelju (slika 38).



State	Service	Icons	Summary
OK	Check_MK		[agent] Version: 2.0.0p3, OS: linux, execution time 0.4 sec
OK	Check_MK Discovery		no unmonitored services found, no vanished services found, no new host labels
OK	Check_MK HW/SW Inventory		Found 72 inventory entries, Found 16 status entries
OK	CPU load		15 min load: 0.07
OK	CPU utilization		Total CPU: 10.79%
OK	Disk IO SUMMARY		Read: 683 B/s, Write: 45.5 kB/s, Latency: 29 microseconds
OK	Filesystem /		10.25% used (5.32 of 51.92 GB), trend: +9.71 MB / 24 hours
OK	Filesystem /opt/omd/sites /checkmkmonitor/tmp		0.57% used (5.75 of 1002.16 MB), trend: +12.78 kB / 24 hours
OK	HTTP Apache service		HTTP OK: HTTP/1.1 200 OK - 10975 bytes in 0.000 second response time
OK	Interface 2		[ens3], (up), MAC: 56:00:02:AD:4D:F1, Speed: unknown, In: 859 B/s, Out: 1.34 kB/s
OK	Interface 3		[ens7], (up), MAC: 5A:00:02:AD:4D:F1, Speed: unknown, In: 0.00 B/s, Out: 0.00 B/s
OK	Interface 4		[ppp0], (up), Speed: unknown, In: 159 B/s, Out: 88.0 B/s
OK	Kernel Performance		Process Creations: 9.00/s, Context Switches: 334.43/s, Major Page Faults: 0.17/s, Page Swap in: 0.00/s, Page Swap Out: 0.00/s
OK	Memory		Total virtual memory: 18.45% - 746.95 MB of 3.95 GB
OK	Mount options of /		Mount options exactly as expected
OK	Number of threads		Count: 169 threads, Usage: 1.07%
OK	OMD checkmkmonitor apache		0.17 Requests/s, 0.01 Seconds serving/s, 2.05 kB Sent/s
OK	OMD checkmkmonitor Event Console		Current events: 0, Virtual memory: 201.67 MB, Overall event limit inactive, No hosts event limit active, No rules event limit active, Received messages: 0.00/s, Rule hits: 0.00/s, Rule tries: 0.00/s, Message drops: 0.00/s, Created events: 0.00/s, Client connects: 0.05/s, Rule hit ratio: -, Processing time per message: -, Time per client request: 0.72 ms
OK	OMD checkmkmonitor performance		Livestatus version: 2.0.0p3, Host checks: 0.1/s, Service checks: 0.9/s
OK	OMD checkmkmonitor status		running
OK	Postfix Queue		Deferred queue length: 0, Active queue length: 0
OK	Postfix status		Status: the Postfix mail system is running, PID: 771
OK	SFTP DebianCheckMK		Login successful
OK	Site checkmkmonitor statistics		Total hosts: 5, Problem hosts: 2, Total services: 81, Problem services: 34
OK	Systemd Service Summary		Total: 55, Disabled: 1, Failed: 0
OK	TCP Connections		Established: 9
OK	TCP Port 22		TCP OK - 0.000 second response time on 95.179.138.158 port 22
OK	Uptime		Up since Jun 21 2021 13:50:52, Uptime: 63 days 13 hours

Slika 37. Prikaz parametara koji se nadziru na virtualnom stroju

4. ZAKLJUČAK

Nije nepoznanica da sve veći broj tvrtki i organizacija koristi IT infrastrukturu u svom poslovanju, u većoj ili manjoj mjeri. S vremenom, broj mrežnih uređaja o kojem ovisi dio poslovanja ili koji služe kao okosnica cijelog informacijskog sustava postaje sve veća. Za ispravan i dugotrajan rad cijele mreže i svih njezinih uređaja potrebna je stalna kontrola i provjera njezinih parametara, pogotovo u okruženjima čije se poslovanje potpuno oslanja na IT rješenja. Administriranje već spomenutih uređaja iz jedne točke, bez fizičkog pristupa istom, još je jedna funkcionalnost koja se mora planirati kod povećanja opsega i lokacija mreže.

Kako bi se ispunili ovi zahtjevi, u ovom završnom radu je opisana implementacija sustava za upravljanje i nadzor udaljenih mreža koja pruža rješenja za gore opisane zahtjeve na puno isplativiji i jednostavniji način. Checkmk sustav za nadzor IT infrastrukture i MikroTik CHR, softverski usmjernik, čine okosnicu ovog sustava. Korištenjem PPTP tunela prema CHR-u i ostalim udaljenim mrežama, Checkmk ima mogućnost nadzora nad usmjernicima i ostalim uređajima u istoj mreži koristeći SNMP protokol ili pridruženi klijent koji je posebno razvijen za određene uređaje. Radi obavještavanja u realnom vremenu, implementiran je sustav obavijesti koji koristi Checkmk modul za obavijesti i Postfix mail agent. Prije, tijekom i nakon izrade ovog rada zaključeno je da ovakvi sustavi:

- omogućavaju bolje i preciznije korištenje mrežnih uređaja,
- omogućavaju osobama zaduženim za nadzor da na vrijeme primijete i otklone probleme,
- poboljšavaju razinu profesionalnosti i kvalitetu korisničke podrške.

Također je važno napomenuti da sustavi ovog tipa u većini slučajeva nisu jednokratni kada se govori o implementaciji i održavanju istog, kao i svakom sustavu potrebno mu je stalno održavanje, unaprjeđivanje, revizija i testiranje njegovih funkcionalnosti. Zaključno, korištenje sustava za pristup i nadzor mreža, pa tako i ovog, isplatjivo je ukoliko nadzire sve uređaje na mreži, što znači da se za vrijeme planiranja implementacije treba uzeti u obzir njegova razina fleksibilnosti i težina adaptacije na nove vrste i modele uređaja na mreži. Isto tako, informacije o mreži koje pruža sustav zahtijeva znanje analize istih od strane osoba koje su zadužene za nadzor jer u konačnici, bez informacija koje su razumljive i koje dolaze u pravo vrijeme, sustav nadzora nema svrhu u okruženju koje nadzire.

LITERATURA

[1] https://mikrotik.com/ (posjećeno 28.05.2021.)

[2] https://wiki.mikrotik.com/wiki/Main_Page (posjećeno 28.05.2021.)

[3] https://help.mikrotik.com/docs/ (posjećeno 28.05.2021.)

[4] VPS - Što je to i trebate li ga i zašto, https://mydataknox.hr/blog/vps/vps-sto-je-to-trebate-li-ga-i-zasto.html (posjećeno 29.05.2021.)

[5] RouterOS , http://www.mikrotik-routeros.net/routeros.aspx (posjećeno 29.05.2021.)

[6] What is MikroTik RouterOS- Part One, https://www.broadbandbuyer.com/advice/2163-what-is-mikrotik-routeros-part-one/ (posjećeno 29.05.2021.)

[7] What is MikroTik RouterOS- Part Two, https://www.broadbandbuyer.com/advice/2164-what-is-mikrotik-routeros-part-two/ (posjećeno 29.05.2021.)

[8] 6 Best Mail Transfer Agents (MTA's) for Linux, https://www.tecmint.com/best-mail-transfer-agents-mta-for-linux/ (posjećeno 29.05.2021.)

[9] Message Transfer Agent (MTA), https://www.techopedia.com/definition/1691/message-transfer-agent-mta (posjećeno 29.05.2021.)

[10] Which SMTP Port Should I Use? Understanding Ports 25, 465, & 587 , https://www.mailgun.com/blog/which-smtp-port-understanding-ports-25-465-587/ (posjećeno 29.05.2021.)

[11] What is an MTA? , https://mailtrap.io/blog/mail-transfer-agent/ (posjećeno 29.05.2021.)

[12] An Introduction to Internet E-Mail, http://wooledge.org/~greg/mail.html (posjećeno 29.05.2021.)

[13] What is a Tunneling Protocol?, https://www.kaspersky.com/resource-center/definitions/tunneling-protocol (posjećeno 30.05.2021.)

[14] VPN Tunnels explained: what are they and how can they keep your internet data secure , https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure (posjećeno 30.05.2021.)

[15] PPTP , https://techterms.com/definition/pptp (posjećeno 01.06.2021.)

[16] What Is PPTP? (Everything You Need to Know) , https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp/#pptp-definition (posjećeno 01.06.2021.)

[17] Light at the end of the tunnel: Answers to all your PPTP questions , https://techgenix.com/pptp-point-to-point-tunneling-protocol-questions-answered/ (posjećeno 01.06.2021.)

[18] Open vs Closed- source operating system, https://hr.computersm.com/16-open-vs-closed-source-operating-system-45730 (posjećeno 02.06.2021.)

[19] Debian Stretch, https://wiki.debian.org/DebianStretch (posjećeno 02.06.2021.)

[20] RouterOS, https://rickfreyconsulting.com/resources/ (posjećeno 05.06.2021.)

[21] Checkmk features, https://checkmk.com/product/features (posjećeno 20.06.2021.)