TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Daniel Geller 206771IAAB

Kõrgkäideldava mitmepoolse VPN-teenuse rakendamine seadmeid ja tarkvara tarniva ettevõtte näitel

Bakalaureusetöö

Juhendaja: Kristiina Hakk
PhD

Tallinn 2023

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Daniel Geller

24.04.2023

Annotatsioon

Lõputöö eesmärk on välja töötada ja rakendada kõrgkäideldav mitmepoolne VPN-teenus seadmeid ja tarkvara tarniva ettevõtte näitel.

Bakalaurusetöö teoreetiline osa koosneb ülesande püstitamisest ja projekti eesmärkide seadmisest, samuti esitatakse tingimused, millele projekt peab vastama. Lisaks viiakse läbi VPN-protokollide analüüs ja valitakse töös kasutatava ühenduse tüüp.

Praktilises kirjeldatakse samm-sammult lahenduse loomist. Lõpuks esitatakse infrastruktuuri testimise tulemused ja hinnang lahenduse usaldusväärsusele.

Lõputöö on kirjutanud eesti keeles ning sisaldav teksti 31 leheküljel, 6 peatükki, 31 joonist, 3 tabelit.

Abstract

Implementation of High Availability Multi-Site VPN Service on Behalf of Equipment and Software Supplier Company

The aim of this project is to create the Implementation of High Availability Multi-Site VPN Service on behalf of Equipment and Software Supplier Company.

The theoretical part of the thesis consists of defining the problem and setting the goals of the project, as well as presenting the conditions that the project must ultimately meet. In addition, an analysis and selection of VPN protocols and the type of connection used in the work is performed.

In the practical part, the essence of the solution is unfolded step by step and detailed explanations of why each step is taken are provided. Finally, the results of the infrastructure testing and the overall reliability of the solution are presented.

The thesis is written in Estonian and contains text on 31 pages, 6 chapters, 31 figures, and 3 tables.

Lühendite ja mõistete sõnastik

CA	*Certificate Authority*, sertifitseerimisasutus
CARP	*Common Address Redundancy Protocol*, ühine aadressi koondamise protokoll
DHCP	*Dynamic Host Configuration Protocol*, dünaamiline hostikonfiguratsiooni protokoll
DNS	*Domain Name System*, domeeninimide süsteem
GUI	*Graphical User Interface*, graafiline kasutajaliides
HA	*High Availability*, kõrgkäideldavus
IP	*Internet Protocol*, internetiprotokoll
IPSec	*Internet Protocol Security*, internetiprotokolli turvalisus
L2TP	*Layer 2 Tunneling Protocol*, kiht 2 tunneliprotokoll
LAN	*Local Area Network*, lokaalne võrk
NAT	*Network Address Translation*, võrguaadresside teisendus
PPTP	*Point-to-Point Tunneling Protocol*, punkt-punkti tunneldamise protokoll
RDP	*Remote Desktop Protocol*, kaugtöölaua protokoll
SNMP	*Simple Network Management Protocol*, lihtne võrguhalduse protokoll
SSL	*Secure Sockets Layer*, turvasoklite kiht
TCP	*Transmission Control Protocol*, edastusjuhtimisprotokoll
TLS	*Transport Layer Security*, transpordikihi turvalisus
UDP	*User Datagram Protocol*, kasutajadatagrammi protokoll
WAN	*Wide Area Network*, laivõrk
VPN	*Virtual Private Network*, virtuaalne privaatvõrk
XML	*Extensible Markup Language*, laiendatav märgistuskeel
XMLRPC	*XML Remote Procedure Call*, kaugprotseduuri kutsung

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Kaasaegses maailmas, kus äri muutub üha globaliseeritumaks ja organisatsioonid laiendavad oma tegevust rahvusvahelisel tasandil, tekib vajadus integreerida kaugkontorid ja keskne kontor ühtsesse võrgu infrastruktuuri. See muutub eriti oluliseks olukordades, kus kaugtöö laieneb ja on palju geograafiliselt hajutatud töötajaid. Andmete edastamise turvalisuse, võrgu usaldusväärsuse ja kõrgkäideldavuse tagamine on kriitiliselt olulised ülesanded organisatsiooni katkematu ja efektiivse toimimise jaoks.

Käesoleva töö eesmärk on välja töötada ja rakendada kõrgkäideldav mitmepoolne VPN (*Virtual Private Network*)-teenus seadmeid ja tarkvara tarniva ettevõtte näitel. Loodud lahendus peab tagama turvalise ja usaldusväärse ühenduse kaugkontorite ja keskse kontori vahel. See aitab suurendada andmete turvalisust ning tagada äriprotsesside sujuv toimimine.

Töö on jaotatud kuueks peatükiks. Teises peatükis kirjeldatakse lahendatavat probleemi ja projekti eesmärki ning antakse ülevaade olemasolevatest lahendustest. Kolmandas peatükis viiakse läbi olemasolevate tehnoloogiate analüüs ning hinnatakse nõudeid lahendustele ja tutvustatakse valitud tehnoloogiaid. Neljandas peatükis kirjeldatakse tulemuste realiseerimise protsessi, sh serveri ja klientide seadistamist ning testimist. Viiendas peatükis esitatakse saavutatud tulemused ja käsitletakse edasiarenduse võimalusi.

2 Ülesande püstitus ja projekti eesmärk

Käesolevas peatükis esitatakse ülesande püstitus ja lähtetingimused. Seejuures kirjeldatakse kaugkontorite ja keskse kontori vahelise ühenduse tagamise probleemi, hinnatakse projekti olukorda ja võimalikke piiranguid.

2.1 Ülesande püstitus

Laialt tuntud fakt on, et tänapäeva äri toetub üha enam IT-infrastruktuurile, mis omakorda loob vajaduse tagada turvaline ja usaldusväärne juurdepääs ettevõtte ressurssidele, kaugtöötajatele ja kaugkontoritele. Selle kontekstis on kõrgkäideldavad mitmepoolsed VPN-teenused eduka organisatsiooni töö jaoks võtmeteguriks.

Virtuaalne privaatvõrk on tehnoloogia, mis loob turvalise ja krüpteeritud ühenduse avaliku interneti kaudu, võimaldades andmete turvalist edastamist ja ligipääsu ressurssidele. VPN-teenuse abil saavad ettevõtted oma töötajatele pakkuda turvalist juurdepääsu ettevõtte võrgule ning jagada andmeid ja ressursse erinevate asukohtade vahel. See on eriti oluline tänapäeva üha kasvava mobiilse tööjõu jaoks, kus töötajad peavad sageli töötama väljaspool kontorit ja kaugtöökohti. [1]

Kõrgekäideldavus on süsteemide, rakenduste ja teenuste disaini põhimõte, mille eesmärk on tagada, et need oleksid võimalikult pikka aega kasutatavad ja töökorras, minimeerides katkestusi ja tõrkeid. Kõrgkättesaadavuse tagamine on kriitilise tähtsusega ettevõtetele, kes sõltuvad oma IT-süsteemide ja teenuste pidevast töökindlusest. Kõrgkäideldavuse lahendused hõlmavad tavaliselt selliseid tehnikaid nagu klasterdamine, varundamine, koormuse jaotamine ja redundantsus, et tagada süsteemi töökindlus ja vastupidavus erinevatele tõrgetele ja riketele. [2] Probleemid, mida tuleb lahendada eduka kõrgkäideldava mitmepoolse VPN-teenuse rakendamiseks ja tagamiseks, hõlmavad järgmisi olulisi aspekte [1], [3] - [6]:

- Usaldusväärse ja turvalise VPN-lahenduse valimine on oluline ülesanne, mille puhul tuleb valida VPN-tehnoloogia, mis tagab andmete privaatsuse, konfidentsiaalsuse ja terviklikkuse kaugasuvate saitide vahel.

- VPN-teenuse kõrgkäideldavuse tagamine on kriitiline, kuna VPN-teenuse vastupidavus ja katkematu töö on selle eduka rakendamise kriitilised näitajad. On vaja välja töötada selline arhitektuur, mis minimeerib seisakute arvu ja taastab kiiresti töö pärast võimalikke rikkeid.
- Skaleeritavus ja paindlikkus on olulised, kuna VPN-teenus peab olema skaleeritav ja paindlik, et kohaneda organisatsiooni muutuvate vajadustega, kasutajate ja saitide arvu kasvuga ning tehnoloogiate arenguga.
- Integreerimine olemasoleva IT-infrastruktuuriga on hädavajalik, kuna VPN-teenuse rakendamine peab hõlmama integreerimist olemasolevate süsteemide ja võrguseadmetega, tagades maksimaalse ühilduvuse ja minimaalsed hooldus- ja toe kulud.
- Turvalisus ja juurdepääsukontrol, on kriitilised , kuna VPN-teenuse rakendamine peab tagama range juurdepääsukontrolli ettevõtte ressurssidele, lähtudes turvapoliitikatest ja kasutajate õiguste eraldamisest. Lahendus peab sisaldama autentimist, autoriseerimist ja kasutajate tegevuste jälgimist turvalisuse ja vastavuse tagamiseks regulatiivsetele nõuetele.

Nimetatud probleemide lahendamine võimaldab edukalt rakendada kõrgkäideldavat mitmepoolset VPN-teenust, mis tagab turvalise ja katkematu juurdepääsu ettevõtte ressurssidele kaugtöötajatele ja kontoritele, suurendab organisatsiooni operatiivsust ja tõhusust ning üldiselt vähendab IT-infrastruktuuri hooldus- ja toetusmakseid. [3]

Praegu annab seadmeid ja tarkvara tarniv ettevõtte rendile seadmeid, millega on probleeme välitöödelt saadud andmete töötlemise ja serverisse saatmisega. Nende seadmete eesmärk on muuta töö efektiivsemaks ja vähendada aega, mis kulub andmete kogumisele ja analüüsimisele. Samuti on oluline, et renditud seadmete hooldamine ei nõua igale seadmele füüsilist juurdepääsu, vaid võimaldab ühenduda mis tahes seadmega võrgus ühest punktist. See peaks lihtsustama hooldustöid ja vähendama sellega seotud logistilisi probleeme.

Ettevõttes, kus lõputöö autor töötab, kasutatakse hetkel lahendusena käsitsi andmete (mõõtmistulemusi, asukohta, tööaega ja muid olulisi tööparameetreid) sisestamist ja serveriga RDP (*Remote Desktop Protocol*) kaudu ühendamist, mis aeglustab tööd. Tarkvara võimaldab seda kõike teha automaatselt, kuid vastav lahendus senini puudub. See tekitab töötajatele lisakoormust ja suurendab vigade tekkimise tõenäosust andmete

sisestamisel. Lisaks tuleb seadmete hooldamiseks külastada igat asukohta või ühenduda samas võrgus asuva rendiseadmega arvuti kaudu, kasutades kaugtööd võimaldavat tarkvara. Selline lähenemine on aeganõudev ja kulukas, eriti kui arvestada transpordikulusid ja tööjõukulusid.

Peamine eesmärk on automatiseerida andmete edastamise ja seadmete hoolduse protsess, et suurendada töö efektiivsust, vähendada vigade tõenäosust ja säästa aega ning ressursse. Valmis lahendus peaks tagama kõigi seadmete kättesaadavuse ühest kohast (serveriruumis või VPN-iga ühendatud võrkudes) ja stabiilse VPN-võrgu töö. Automaatse lahenduse abil saavad töötajad keskenduda teistele olulistele tööülesannetele, samal ajal kui süsteem tegeleb andmete kogumise, edastamise ja seadmete hooldamisega. Lisaks aitab see vähendada transpordi- ja tööjõukulusid, kuna töötajad ei pea iga seadme juurde füüsiliselt kohale minema ega käsitsi andmeid sisestama.

2.2 Lähtetingimused

Selles töös tuleb järgida teatud üldisi kriteeriume, et tagada projekti edukas elluviimine vastavalt seda tüüpi tööle esitatavatele nõuetele ja ootustele. [1]

1. Olemasoleva võrguinfrastruktuuri ja seadmete arvesse võtmine on väga oluline VPN-teenuse nõuete määramisel ning selle integreerimisel juba olemasolevatesse süsteemidesse. See hõlmab võrguprotokollide, topoloogia, läbilaskevõime ja teiste parameetrite analüüsi, mis võivad mõjutada VPN-ühenduste jõudlust ja stabiilsust.
2. Tuleb kindlaks määrata VPN-teenuse minimaalselt lubatav kättesaadavuse tase, samuti nõuded tõrkekindlusele, taastumisele pärast rikkeid ja intsidentide reageerimisajale.
3. Kättesaadavate eelarveliste vahendite ja ressursside määramine VPN-teenuse edukaks rakendamiseks ja toetamiseks on oluline tegur, mis mõjutab seadmete, tarkvara ja kõrgkäideldavuse tagamise valikut.
4. Personal, kes vastutab VPN-teenuse haldamise ja toetamise eest, mõjutab samuti valitud lahendust ja lähenemisi rakendamisel. On oluline arvestada töötajate praegust teadmiste taset ja vajadust täiendava koolituse või konsultatsioonide järele.

3 Analüüs

Käesolevas peatükis esitatakse erinevate VPN-tehnoloogiate ja protokollide analüüs ja võrdlus, vaadeldakse nende erinevusi ning eeliseid. Hinnatakse tehnoloogiate vastavust projekti nõudmistele ning võrreldakse nende toimivust, turvalisust ja stabiilsust ning vaadeldakse juba turul olevaid võimalusi, mis võivad aidata probleemi lahendada. Järgnevalt räägitakse klientide poolt esitatud nõuetest.

Lõpuks tutvustatakse kasutatavaid tehnoloogiaid, mis on valitud selle projekti jaoks. Selgitatakse, miks need tehnoloogiad on valitud, kuidas nad vastavad klientide nõuetele ja kuidas nad aitavad saavutada projekti eesmärke. Samuti selgitatakse, kuidas neid saab kasutada tõhusa ja turvalise VPN-lahenduse loomiseks.

3.1 Olemasolevate tehnoloogiate võrdlus

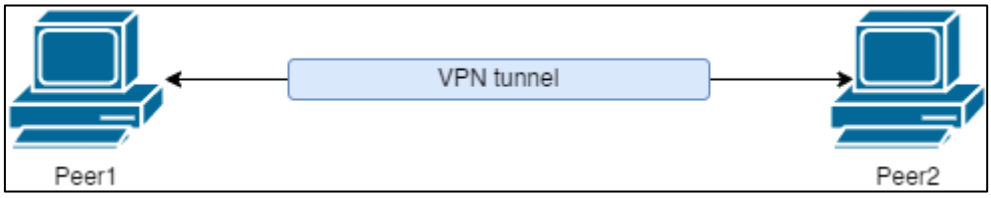
Selles alapeatükis vaatleme mõningaid levinumaid VPN-ühenduste loomise lahendusi ja nendega seotud omadusi. Olemasolevate lahenduste uurimine võimaldab meil teha põhjendatud otsuse tehnoloogia valiku kohta kõrgkäideldava mitmepoolse VPN-teenuse rakendamiseks ning tuvastada võimalikud probleemid ja piirangud, mis võivad tekkida süsteemi arendamise ja kasutuselevõtu protsessis. See tagab sujuvama ja edukama lahenduse arendamise ja rakendamise protsessi ning lahenduse vastavuse organisatsiooni nõuetele ja turvastandarditele.

3.1.1 Tehnoloogiate võrdlus

Käesolevas alapeatükis võrreldakse erinevaid VPN-tehnoloogiaid, et leida projekti jaoks sobivaim lahendus. VPN-tehnoloogiad jagataksed tavaliselt neljaks peamiseks kategooriaks: võrdõigusvõrk (*peer-to-peer),* saidilt saidile (*site-to-site),* kaugjuurdepääs (*remote access)* ja mitmepoolne (*multisite)*. Allpool võrreldakse iga kategooria omadusi, eeliseid ja puudusi.

Võrdõigusvõrk VPN

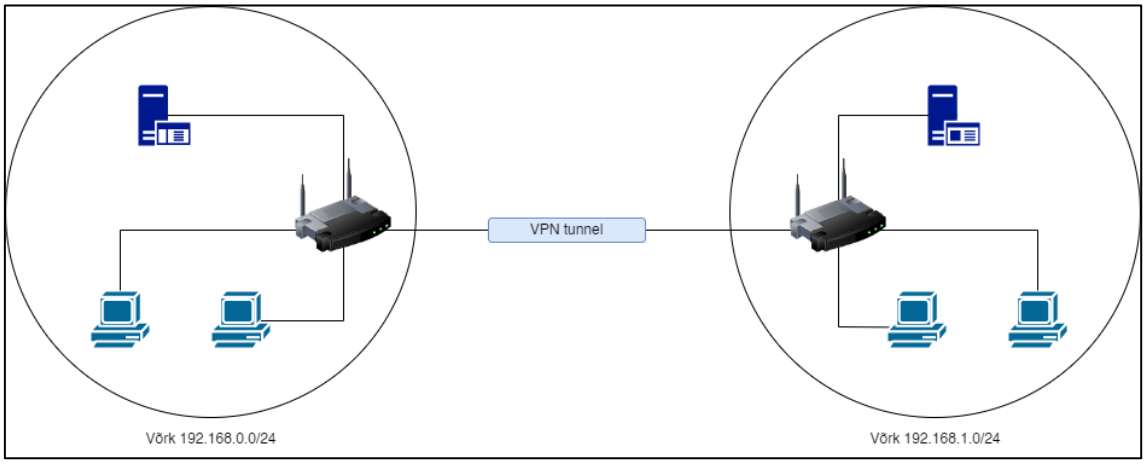
Võrdõigusvõrk või *P2P* tüüp VPN-ühendust hõlmab ühendust kahe seadme vahel, tavaliselt serveri ja kliendi vahel. Sel juhul luuakse VPN-tunnel otse kahe seadme vahel ja kõik edastatavad andmed on kaitstud volitamata juurdepääsu eest [4]. Selle ühenduse skeem on esitatud järgneval joonisel (vt Joonis 1. Võrdõigusvõrk VPN ühendus.



Joonis 1. Võrdõigusvõrk VPN ühendus.

Saidilt saidile VPN

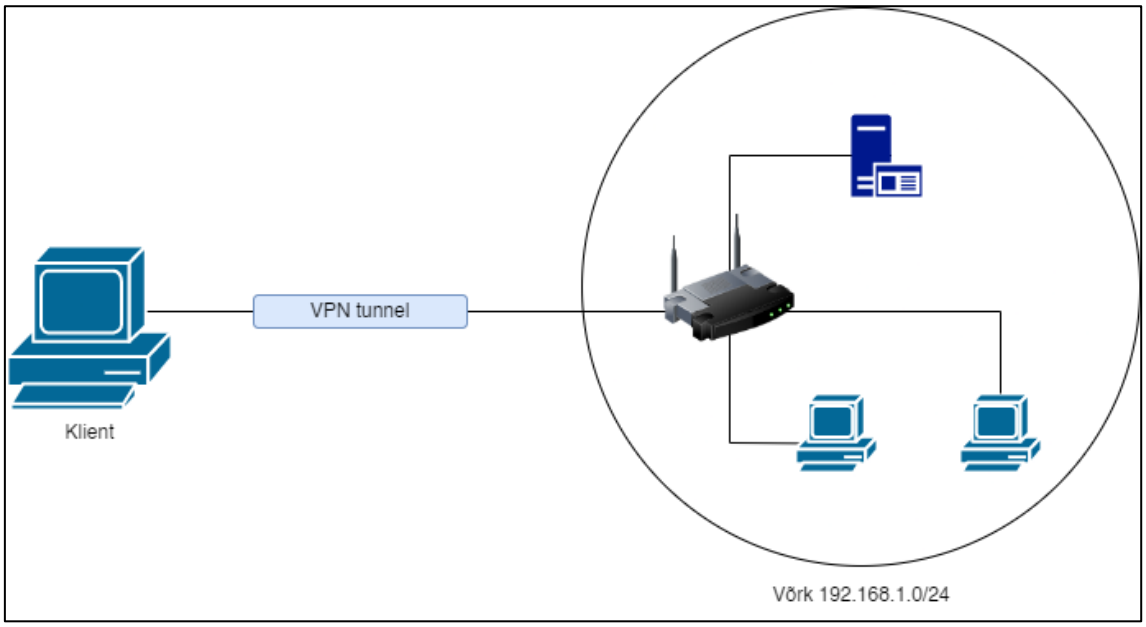
Saidilt saidile või *S2S* VPN-ühenduse tüüp on mõeldud kahe või enama kaugvõrgu ühendamiseks, näiteks keskse kontori ja harukontorite vahel. Sellisel juhul luuakse VPN-tunnel võrgu lüüside (ruuterite või tulemüüride) vahel iga võrgu jaoks, mitte eraldi seadmete vahel. See võimaldab mõlema võrgu kasutajatel lihtsalt ja kiiresti andmeid vahetada ning kasutada teise võrgu võrguressursse, nagu oleksid nad samas kohalikus võrgus. [5] Selle ühenduse skeem on esitatud järgneval joonisel (vt Joonis 2).



Joonis 2. Saidilt saidile VPN ühendus.

Kaugjuurdepääs VPN

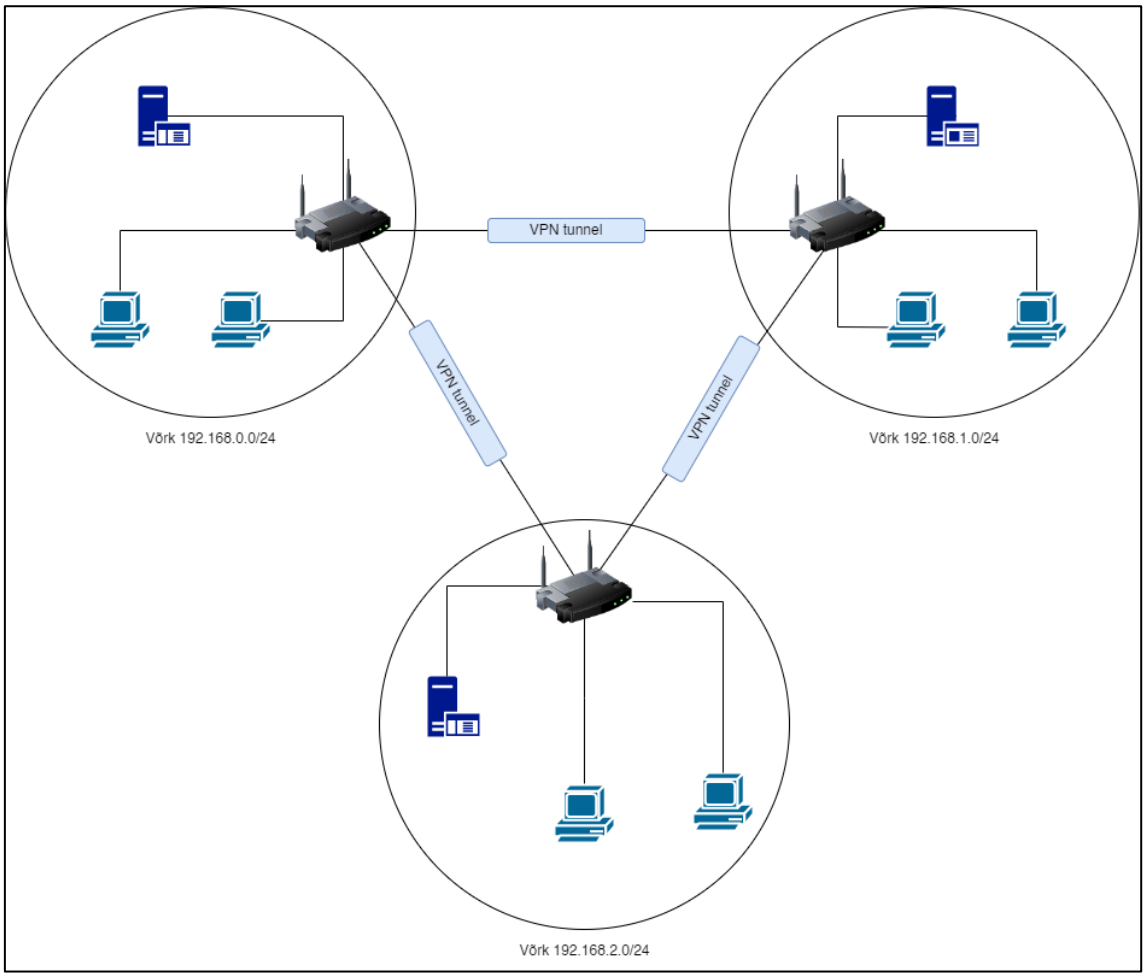
Kaugjuurdepääsu VPN-ühendus luuakse kaugkasutaja (näiteks kodust töötava töötaja) ja organisatsiooni võrgu lüüsi (VPN-serveri) vahel. See võimaldab kaugkasutajal turvaliselt ühenduda ettevõtte võrguga ja pääseda ligi kõigile selle ressurssidele, nagu oleksid nad kontoris. [6] Selle ühenduse skeem on esitatud järgneval joonisel (vt Joonis 3).



Joonis 3. Kaugjuurdepääs VPN ühendus.

Mitmepoolne VPN

Mitmpoolne VPN-teenus ühendab mitmeid erinevaid ühendusi (näiteks saidilt saidile ja kaugjuurdepääs), et tagada turvaline ja usaldusväärne ühendus kaugemate kontorite, keskse kontori ja individuaalsete kaugjuurdepääsukasutajate vahel. Sel juhul võimaldab mitmepoolne VPN integreerida erinevad asukohad ja kaugjuurdepääsukasutajad ühtsesse turvalisse võrguinfrastruktuuri, mis hõlbustab andmevahetust ja võrguressursside haldamist [7]. Selle ühenduse skeem on esitatud järgneval joonisel (vt Joonis 4).



Joonis 4. Mitmepoolne VPN ühendus.

3.1.2 Protokollide võrdlus

OpenVPN

OpenVPN on üks populaarsemaid ja turvalisemaid avatud lähtekoodiga lahendusi VPN-ühenduste loomiseks. See toetab mitmesuguseid krüptograafilisi algoritme, omab paindlikku konfiguratsioonisüsteemi ja seda saab kasutada erinevatel platvormidel. Siiski on oluline teada, et OpenVPN võib vajada täiendavaid teadmisi ja kogemusi seadistamiseks ja hooldamiseks. [8]

OpenVPN pakub kõrgetasemelist turvalisust ja privaatsust. See kasutab liikluse krüpteerimiseks SSL (*Secure Sockets Layer*)/TLS-i (*Transport Layer Security*) ning toetab mitmeid krüpteerimis- ja autentimisalgoritme. OpenVPN võib töötada erinevate portide ja protokollidega, sealhulgas TCP (*Transmission Control Protocol*) ja UDP (*User Datagram Protocol*). [9]

See protokoll toetab erinevaid konfiguratsioone ja laiendusi, võimaldades rakendada erinevaid tööstsenaariume, sealhulgas kõrgkäideldavat ja mitmepoolset arhitektuuri.

Lisaks on OpenVPN ühilduv enamiku platvormide ja operatsioonisüsteemidega, mis lihtsustab selle integreerimist olemasoleva IT-infrastruktuuriga. [10]

IPsec/L2TP

IPsec (*Internet Protocol Security*) ja L2TP (*Layer 2 Tunneling Protocol*) on standardprotokollid turvaliste VPN-ühenduste loomiseks. Need pakuvad kõrget turvalisuse taset ja ühilduvust erinevate seadmete ja operatsioonisüsteemidega. Siiski võib IPsec/L2TP seadistamine ja hooldamine olla keeruline ning võib tekkida probleeme läbipääsu korral läbi NAT-i (*Network Addressing Translation*) ja tulemüüride. [11]

IPsec ja L2TP pakuvad usaldusväärset andmekaitset tänu tugevatele krüptograafilistele algoritmidele. IPsec/L2TP sobib suurte VPN-võrkude loomiseks, mis hõlmavad mitmeid seadmeid ja võrke. [12]

IPSec/L2TP ei ole siiski kõige turvalisem VPN-protokoll, kuna L2TP kasutab täiendava turvalisuse tagamiseks IPSeci, mis pakub suuremat andmekaitset kui mõned teised protokollid. [13]

PPTP

PPTP (*Point-to-Point Tunneling Protocol*) on vana ja kiire VPN-protokoll. See on lihtne seadistada ja ühildub enamiku operatsioonisüsteemide ja seadmetega, võimaldades kiiresti ja lihtsalt luua VPN-ühendust. Siiski peetakse PPTP-d praegu aegunuks ja ebaturvaliseks protokolli haavatavuste tõttu ning selle kasutamine konfidentsiaalsete andmete korral ei ole soovitatav. [14]

PPTP tagab kiire ühenduse tänu oma lihtsale arhitektuurile ja minimaalsetele lisakuludele [15]. Selle protokolli puudused seisnevad selles, et see on nõrgalt krüpteeritud ja seda võivad turvalünkude kaudu ära kasutada nii luureasutused kui ka kvalifitseeritud ründajad. [16]

WireGuard

WireGuard on kaasaegne ja kõrge jõudlusega avatud lähtekoodiga VPN-protokoll. See pakub lihtsat ja kasutajasõbralikku arhitektuuri, kõrget ühenduse kiirust ja usaldusväärset turvalisust. Siiski on WireGuard endiselt aktiivses arendusetapis ning mõned funktsioonid võivad olla kättesaamatud või ebastabiilsed, mis lisab riskielemendi, millega tuleb arvestada. [17]

Tänu kaasaegsele arhitektuurile ja optimeerimisele tagab WireGuard kõrge ühenduse kiiruse ja madala latentsuse. [18]

Tabel 1 toob välja OpenVPN-i eelised võrreldes teiste VPN-protokollidega. Seejuures paistab silma OpenVPN-i kõrge turvalisus, paindlikkus ja suurepärane ühilduvus erinevate seadmetega, mis teeb sellest sobiva valiku meie mitmepoolse VPN-teenuse rakendamiseks.

Tabel 1. Erinevate VPN-protokollide võrdlustabel. [19]

Protokoll	**Turvalisus**	**Jõudlus**	**Ühilduvus seadmetega**	**Seadistus**	**Mitmepoolse VPN-i tugi**
OpenVPN	Kõrge	Kõrge	Suurepärane	Keskmine	Kõrge
PPTP	Madal	Kõrge	Suurepärane	Lihtne	Madal
IPsec/L2TP	Keskmine	Keskmine	Suurepärane	Keeruline	Keskmine
Wireguard	Kõrge	Kõrge	Hea	Lihtne	Keskmine

OpenVPN eelised, mis mõjutavad selle valikut [20] [21]:

- Kõrge turvalisustase: OpenVPN kasutab kaasaegseid krüptograafilisi algoritme ja toetab autentimist sertifikaatide abil, mis tagab andmete ja konfidentsiaalsuse kõrge kaitsetaseme. See võimaldab organisatsioonidel usaldada OpenVPN-i nende tundlike, oluliste ja konfidentsiaalsete andmete ning ettevõtte võrgu kaitseks.
- Paindlikkus ja skaleeritavus: OpenVPN pakub laialdasi kohandamisvõimalusi ja toetab erinevaid tööstsenaariume, sealhulgas kõrgkäideldavuse, mitmepoolse arhitektuuri ja koormuse tasakaalustamist. See võimaldab lahendust lihtsalt ja kiiresti kohandada organisatsiooni spetsiifiliste vajaduste järgi ning tagada paindlikkus võrguinfrastruktuuri laiendamisel või muutmisel.
- Ühilduvus: OpenVPN on ühilduv enamiku operatsioonisüsteemide ja seadmetega, mis lihtsustab selle integreerimist olemasoleva IT-infrastruktuuriga ning võimaldab erinevate seadmete ühendamist VPN-võrku ilma ühilduvusprobleemideta.

3.2 Nõuded lahendustele

Antud peatükis esitatakse lahenduse peamised nõuded. Nõuete väljaselgitamiseks viidi läbi intervjuu kliendipoolse projektijuhiga. Nõuded tulenevad kliendi äriprotsesside ja tehniliste vajaduste analüüsist, tagades lahenduse tõhususe ja turvalisuse.

- Serveriseadmete eelarve: mitte rohkem kui 1000 eurot.
- Kliendiseadmed: Teltonika 4G ruuterid.
- Server peab olema kergesti skaleeritav uute klientide lisamiseks.
- VPN-serveri konfigureeritav ühenduste piirang.
- Sertifikaatidega autentimine.
- Sertifikaatide haldus ja uuendamine.
- Automaatne seadistuste sünkroniseerimine kahe tulemüüri vahel.
- VPN-teenus peab töötama 24 tundi ööpäevas.

Nõue serveriseadmete eelarvele on maksimaalselt 1000 (üks tuhat) eurot. See tähendab, et serveri riistvara ja selle komponentide valik tuleb optimeerida maksumuse seisukohast, säilitades samas VPN-serveri kvaliteedi, jõudluse ja usaldusväärsuse. Võib-olla tuleb teha kompromisse, arvestades eelarvelisi piiranguid, kuid valik tuleb teha, võttes arvesse VPN-serveri funktsionaalsuse ja stabiilsuse tagamist. See eelarvepiirang tuleneb asjaolust, et tegemist on testimisetapiga, mistõttu on ajutiselt kärbitud eelarvet. Mainitud eelarve hõlmab ainult seadmete maksumust, mitte tööjõukulusid.

Kliendiseadmeteks on Teltonika 4G ruuterid. See valik on tingitud asjaolust, et VPN-kliendiseadmed paigaldatakse välitingimustesse, kus Teltonika ruuterid sobivad tänu oma vastupidavatele omadustele. See eeldab, et valitud VPN-serveri protokoll peab olema kooskõlas nende ruuteritega ja suutma nendega luua stabiilse ja turvalise VPN-ühenduse. Samuti tuleb pöörata tähelepanu VPN-i integreerimisele Teltonika 4G ruuteritega, kontrollida ühilduvust ja seadistada vastav konfiguratsioon, et tagada korrektne töö.

Nõue serveri skaleeritavusele eeldab, et valitud lahendus peab olema paindlik ja suutma kohanduda muutustega, nagu klientide arvu kasv ja nende vajaduste muutused. VPN-server peab olema konfigureeritud selliselt, et uute klientide lisamine või nende konfiguratsiooni muutmine oleks lihtne ega tekitaks probleeme süsteemi jõudluse, turvalisuse või stabiilsuse osas. Lisaks, kui projekt osutub edukaks, on plaanis lisada uusi

ühenduspunkte, mida tuleb VPN-serveriga ühendada, nõudes seeläbi veelgi suuremat paindlikkust ja skaaleritavust.

VPN-server peab võimaldama administraatoril seadistada ühenduste arvu piirangu, et kontrollida samaaegseid kasutajaid ja vältida ülekoormust. See on vajalik, et tagada kindla arvu VPN-klientide üheaegne töö ning vältida ebasoovitavate ja volitamata kasutajate pääs süsteemi, mis võib kahjustada võrgu turvalisust ja jõudlust.

VPN-lahendus peaks toetama sertifikaatidega autentimist, mis tagab suurema turvalisuse ja usaldusväärsuse, võrreldes traditsiooniliste kasutajanimede ja paroolidega. Lisaks sellele peab VPN-server võimaldama lihtsat sertifikaatide haldust, sealhulgas sertifikaatide genereerimine, uuendamine ja tühistamine, et säilitada süsteemi turvalisus ja usaldusväärsus.

Süsteemis peaks olema seadistatud automaatne seadistuste sünkroniseerimine kahe tulemüüri vahel, et tagada nende konfiguratsioonide järjepidevus ja võimaldada sujuvat üleminekut rikke korral. See omakorda aitab vähendada aega ja vaeva, kuna pole vajadust teha samu seadistusi mõlemal seadmel eraldi, vaid kõik muudatused kanduvad automaatselt ühelt seadmele teisele.

VPN-teenus peab töötama 24 tundi ööpäevas. See tähendab, et VPN-ühendus peab olema alati kättesaadav ettevõtte pideva andmevahetuse ja äriprotsesside toetamiseks, sõltumata kellaajast või nädalapäevast. Selles kontekstis on kõrgekäideldavuse tagamine kriitilise tähtsusega, kuna see aitab vältida töökatkestusi ja tagab süsteemi usaldusväärsuse isegi suurenenud koormuse.

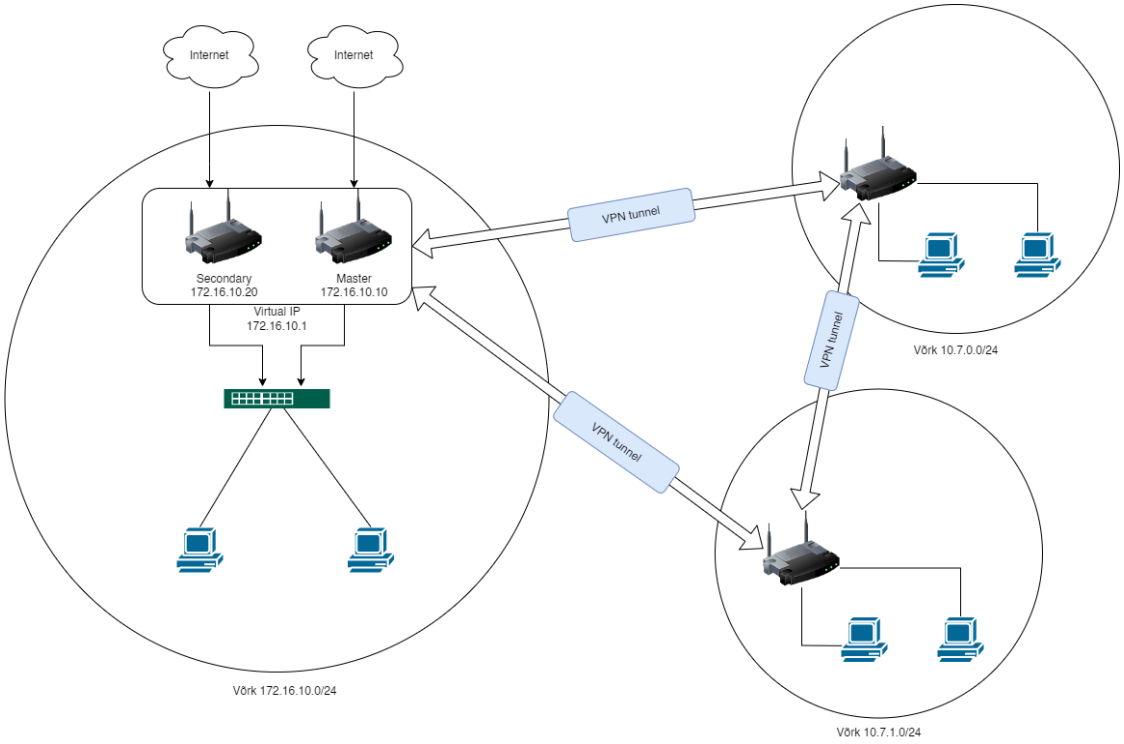
Üldiselt määratlevad nõuded lahenduse arendamise ja rakendamise vajaduse VPN-süsteemi loomiseks, mis vastab eelarvelistele piirangutele, on ühilduv klientseadmetega ning on skaleeritav, võttes arvesse organisatsiooni kasvu ja muutusi.

3.3 Kasutatavad tehnoloogiad

Selles peatükis antakse ülevaade peamistest tehnoloogiatest, mida kasutatakse kõrgkäideldava mitmepoolse VPN-teenuse projekti elluviimisel.

- Virtuaalne IP (*Internet Protocol*)-tehnoloogia kahe pfSense seadme klasterdamiseks.

Kõrgkäideldavuse seadistamiseks projektis kasutatakse virtuaalse IP-tehnoloogiat, mis võimaldab luua klasterduse kahe pfSense seadme vahel. See tagab automaatse ülemineku seadmete vahel rikke korral, tagades VPN-teenuse katkematu töö. Lahenduses kasutatakse ka CARP (*Common Address Redundancy Protocol*) protokolli, mis võimaldab virtuaalse IP-aadressi ühist kasutamist kahe pfSense seadme vahel. [22]
Võrgu topoloogia illustratsioon on esitatud allpool (vt Joonis 5).



Joonis 5. Topoloogia.

- Virtuaalse privaatvõrgu tehnoloogia rakendamine OpenVPN abil.

OpenVPN kasutatakse selle projekti raames põhivõrguühenduse (VPN) protokollina. OpenVPN on võimas ja paindlik avatud lähtekoodiga VPN-tehnoloogia, mis võimaldab luua turvalisi ja usaldusväärseid VPN-ühendusi. Oluliseks eeliseks OpenVPN-i puhul on selle ühilduvus erinevate platvormide ja seadmetega, mis lihtsustab integreerimist Teltonika 4G ruuterite ja teiste kliendiseadmetega [23].

- Serverite jälgimis- ja haldussüsteem.

Ettevõttesisest serverite jälgimis- ja haldussüsteemi kasutatakse VPN-serveri ja pfSense-seadmete töö jälgimiseks. See võimaldab SNMP (*Simple Network Management Protocol*) protokolli abil jälgida serveri jõudlust, koormust ja muid serveri parameetreid reaalajas. Anomaaliatest või võimalikest probleemidest teavitamine võimaldab kiiret reageerimist intsidentidele ja tagab VPN-teenuse kõrgkäideldavuse. Tõhusa jälgimissüsteemi kasutamine aitab õigeaegselt tuvastada ja lahendada probleeme, mis omakorda tagab VPN-serverite usaldusväärsuse ja stabiilsuse. [24]

- Andmete varundamine ja taastamine.

Andmete usaldusväärsuse ja kättesaadavuse tagamiseks soovitatakse kasutada andmete varundamise ja taastamise süsteeme, et minimiseerida andmete kadumise või kahjustamise riski. See võib hõlmata serveri konfiguratsioonifailide, sertifikaatide, turvavõtmete ja muude kriitiliste andmete regulaarset varundamist. Häirete korral või andmete kaotuse korral võimaldab see kiiresti taastada VPN-teenuse toimimise. [25]

- OpenVPN-i haldus- ja konfiguratsioonivahendid.

OpenVPNi haldamise ja seadistamise lihtsustamiseks võib kasutada spetsiaaliseid tööriistu ja platvorme nagu pfSense-si OpenVPN Server GUI (*Graphical User Interface*). See pakub graafilist kasutajaliidest ja integreeritud tööriistu serveri seadistamiseks, kasutajate haldamiseks, monitoorimiseks jne. [26]

- Mitmepoolse tehnoloogia OpenVPNi seadistamiseks.

Mitmepoolse tehnoloogia valik sellele projektile põhineb andmete turvalisuse tagamisel krüpteeritud tunnelite kaudu, võimalusel seadmete omavaheliseks suhtlemiseks klientide võrkudes ressursside tõhusaks kasutamiseks, ühilduvusel Teltonika ruuteritega, toel OpenVPNile ning võrgu mastaapsusel [27]. See teeb lahenduse veelgi paindlikumaks, kohanduvamaks ja vastavaks võrgu infrastruktuuri, OpenVPN-i serverite ja klientseadmete nõuetele.

Samuti on oluline kavandada IP-aadresside jaotust kogu projekti raames. Tabel 2 sisaldab näidet erinevate seadmete ja võrgusegmentide jaoks kasutatavatest IP-aadressidest. Selle

teabe põhjal saab kavandada ja seadistada VPN-ühendusi serverite ja klientide vahel ning tagada korrektne liikluse marsuutimine.

Tabel 3 sisaldab hindu seadmete ja teenuste kohta, mis on vajalikud selle töö teostamiseks.

Tabel 2. Seadme teave: nimi, tüüp, IP-aadress ja võrguaadress.

Nimi	**Klass**	**IP**	**Võrgu aadress**
pfsense_main	IP	172.16.10.10 (LAN (*Local Area Network*))	
	IP	192.168.1.2 (SYNC)	
pfsense_secondary	IP	172.16.10.20 (LAN)	
	IP	192.168.1.3 (SYNC)	
pfsense_cluster	IP	172.16.10.1 (LAN)	
pfsense_network	Võrk		172.16.10.0/24 (LAN)
	Võrk		192.168.1.0/24 (SYNC)
client_1_network	Võrk		10.7.0.0/24
client_2_network	Võrk		10.7.1.0/24
vpn_tunnel_network	Võrk		192.168.23.0/24

Tabel 3. Eelarve: seade nimi, arv, hind.

Nimi	**Arv**	**Hind (EUR)**
Netgate 1100 (pfSense)	2	240+KM (Käibemaks)
Teltonika RUT240	2	170+KM
	Hind kokku	820+KM

4 Lahenduse loomine

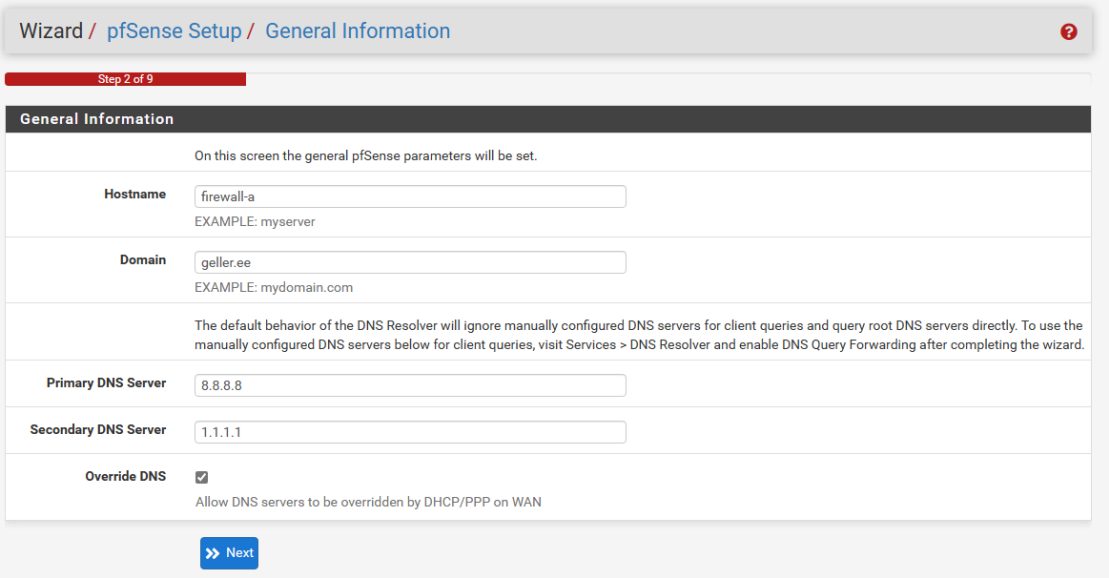
Käesoleva peatükis annab autor ülevaate lahenduse loomisest rakendades probleemi analüüsil saadud tulemusi. Peatükis käsitletakse serveri seadistamist ja sellele järgnevat testimist.

4.1 Serveri seadistamine

Serveri seadistamine algab eelseadistustega, kus käsitletakse vajalikke protsesse ja samme, mis tuleb enne serveri põhiseadistamist teha. Seejärel keskendutakse kõrgkäideldavuse seadistamisele, mis on oluline meie mitmepoolse VPN-teenuse jaoks. Järgnevalt kirjeldatakse VPN serveri seadistamist, esitades detailsed juhised serveri VPN-funktsioonide seadistamiseks. Viimasena kirjeldatakse logide kogunemise seadistamist, mille eesmärk on aidata haldamisel ja tõrkeotsingul.

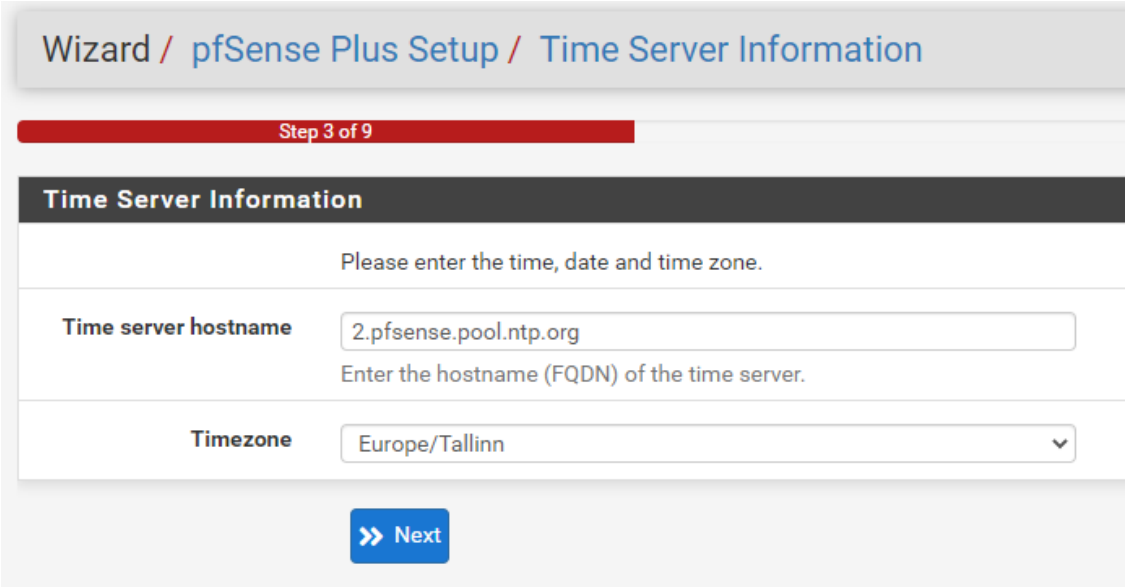
4.1.1 Eelseadistused

Joonis 6 illustreerib tulemüüri esialgset seadistamist, kus esimeses etapis on esitatud ruuteri hostinimi (*firewall-a*), domeen ning DNS (*Domain Name System*)-serverid. Valitud DNS-aadressid 8.8.8.8 (*Google*'i avalik DNS-server) ja 1.1.1.1 (*Cloudflare*'i avalik DNS-server) tagavad kiire ja turvalise domeeninimede lahendamise teenuse. DNS serverite ümberkirjutamine on lubatud, et võimaldada kasutajatel muuta ruuteri vaike-DNS-servereid vastavalt oma vajadustele, näiteks turvalisuse suurendamiseks.



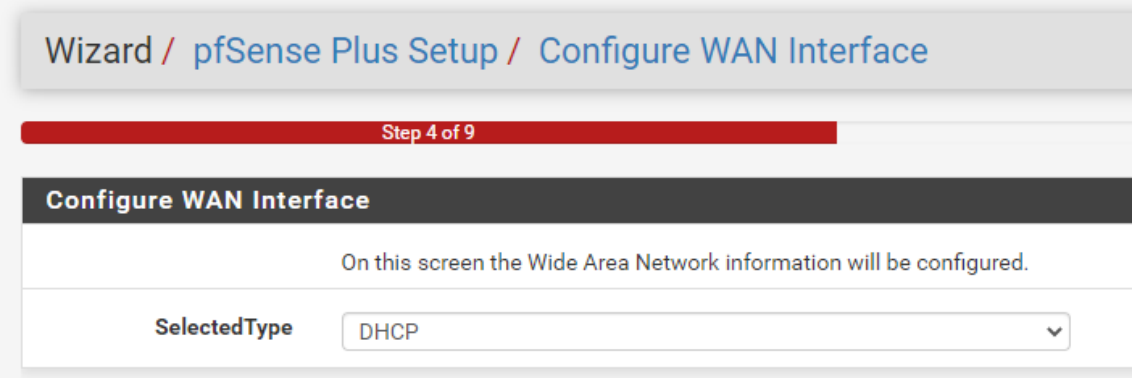
Joonis 6. Ruuteri konfigureerimine: Põhi informatsiooni täitmine.

Joonis 7 kujutab järgmise sammuna tulemüüri eelseadistamisel ajaserveri seadistamist. Ajaserver on oluline tulevaste SNMP rakenduste jaoks, et näha täpset aega, millal ilmnevad vead või probleemid võrgus. Selle abil saab tagada parema võrgu monitoorimise ja haldamise, samuti võimaldab ajaserver kiiret ja täpset reageerimist võrguprobleemidele.



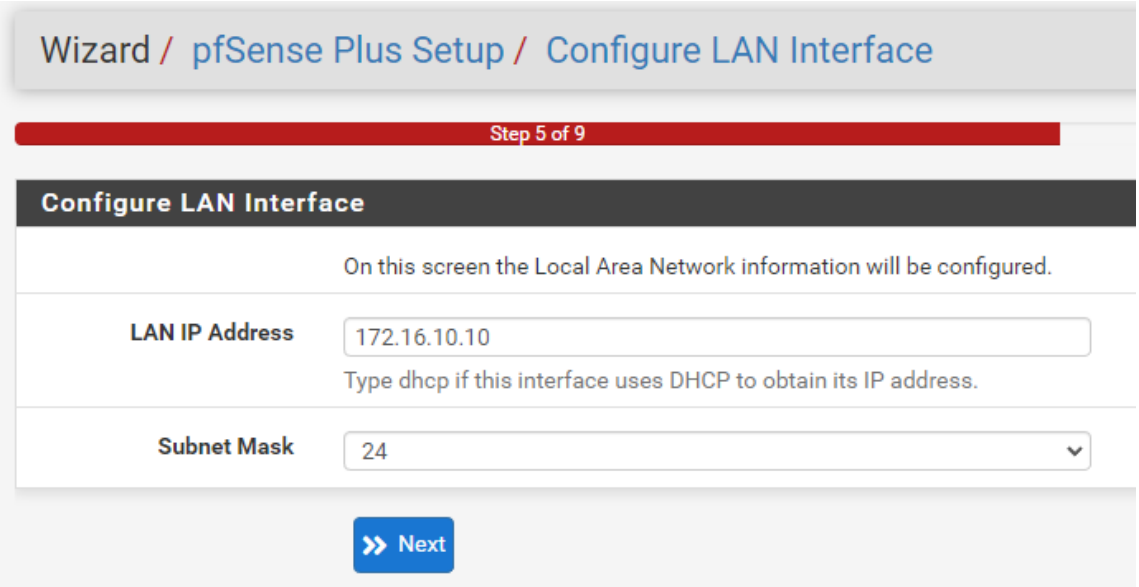
Joonis 7. Ruuteri konfigureerimine: Ajaserveri määramine.

Joonis 8 kujutab tulemüüri eelseadistamise protsessis WAN (*Wide Area Network*)-ühenduse seadistamist. DHCP (*Dynamic Host Configuration Protocol*) seadistuse abil saab tulemüür automaatselt IP-aadressi, alamvõrgu maski, võrguvärava ja DNS-serveri teabe Telia poolt, tagades sujuva ja stabiilse Interneti-ühenduse.



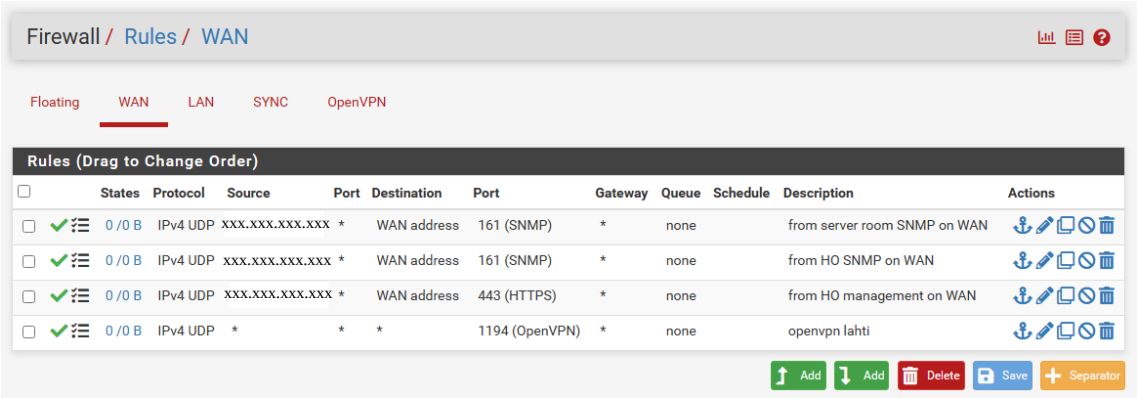
Joonis 8. Ruuteri konfigureerimine: WAN-ühenduse seadistamine.

Joonis 9 kujutab tulemüüri eelseadistamise protsessis LAN-ühenduse seadistamist. Sarnaselt on konfiguratsioon läbi viidud teises ruuteris, kus on määratud IP aadressiks 172.16.10.20, kasutades sama alavõrgu maski (/24).



Joonis 9. Ruuteri konfigureerimine: LAN-ühenduse seadistamine.

Joonis 10 kujutab tulemüüri seadistamise protsessis määratud turvareeglite ülevaadet WAN-pordi jaoks. Vajalikud on kaks eraldi reeglit, et tagada juurdepääs SNMP-logidele, kaugjuurdepääs WEB GUI-le ja OpenVPN-i kasutamine.

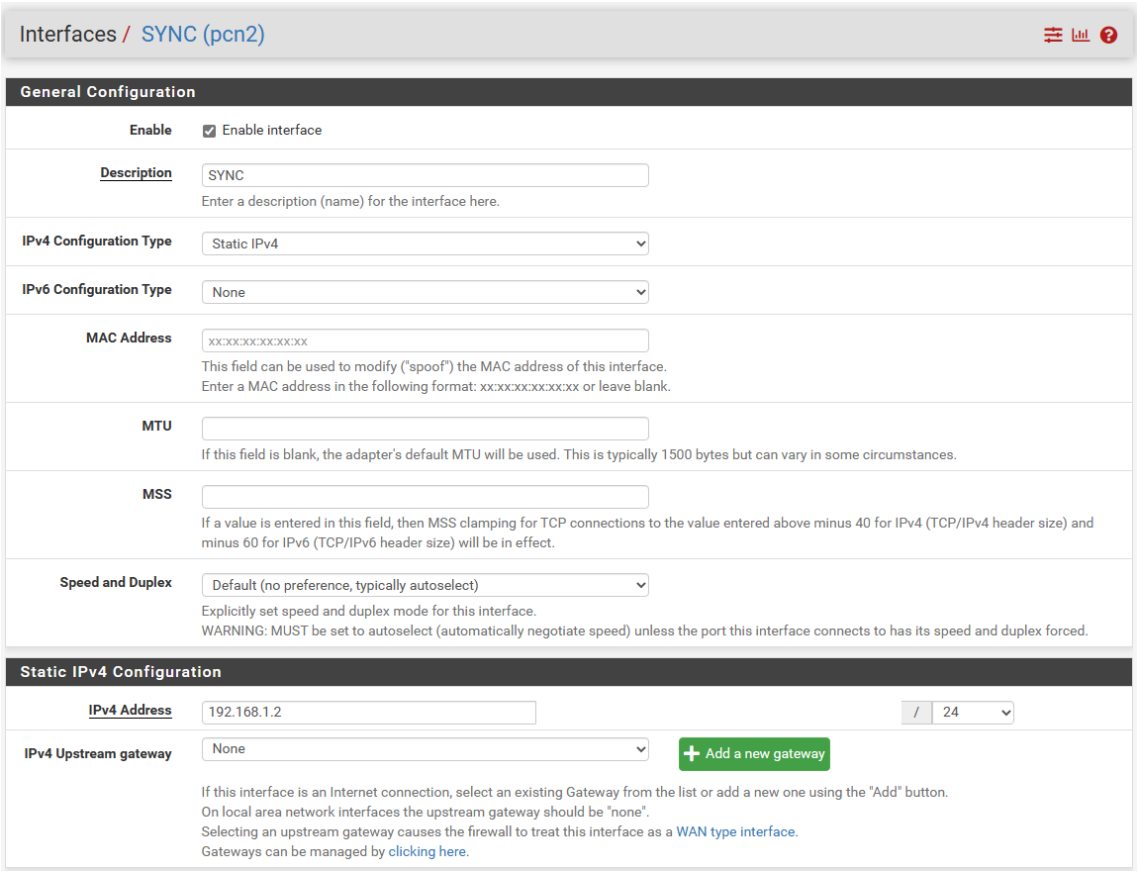


Joonis 10. Tulemüüri WAN reeglid.

4.1.2 Kõrgkäideldavuse seadistamine

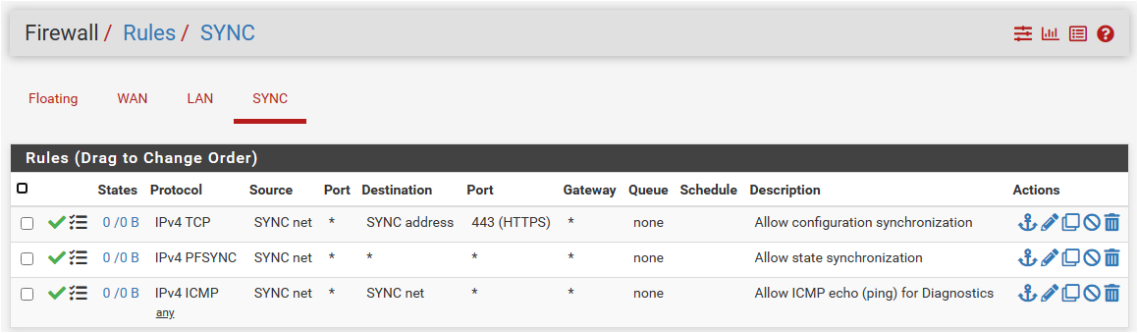
Joonis 11 kujutab protsessi, kus aktiveeritakse SYNC-port ja määratakse sellele IP-aadress. Teisele ruuterile määratakse selle SYNC-pordi jaoks IP-aadress 192.168.1.3.

SYNC-pordi konfigureerimine võimaldab ruuteritel seadistusi omavahel sünkroniseerida.



Joonis 11. SYNC pordi sisse lülitamine ja aadressi seadistamine.

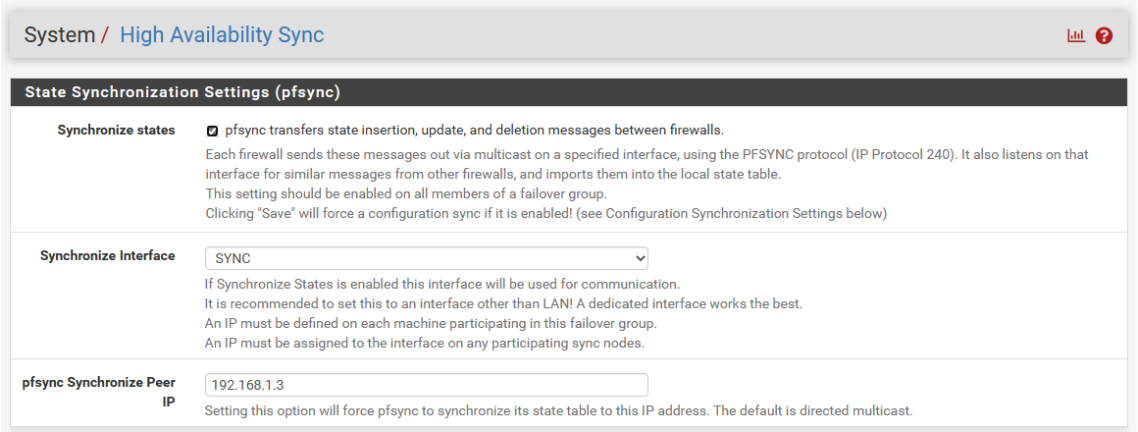
Joonis 12 kujutab SYNC-pordi jaoks seadistatud turvareeglite ülevaadet, mis on vajalikud kahe tulemüüri vahelise sünkroniseerimise toimimise tagamiseks. Nende turvareeglite abil lubatakse sünkroniseerimisliiklus kahe ruuteri vahel.



Joonis 12. SYNC pordi reeglid.

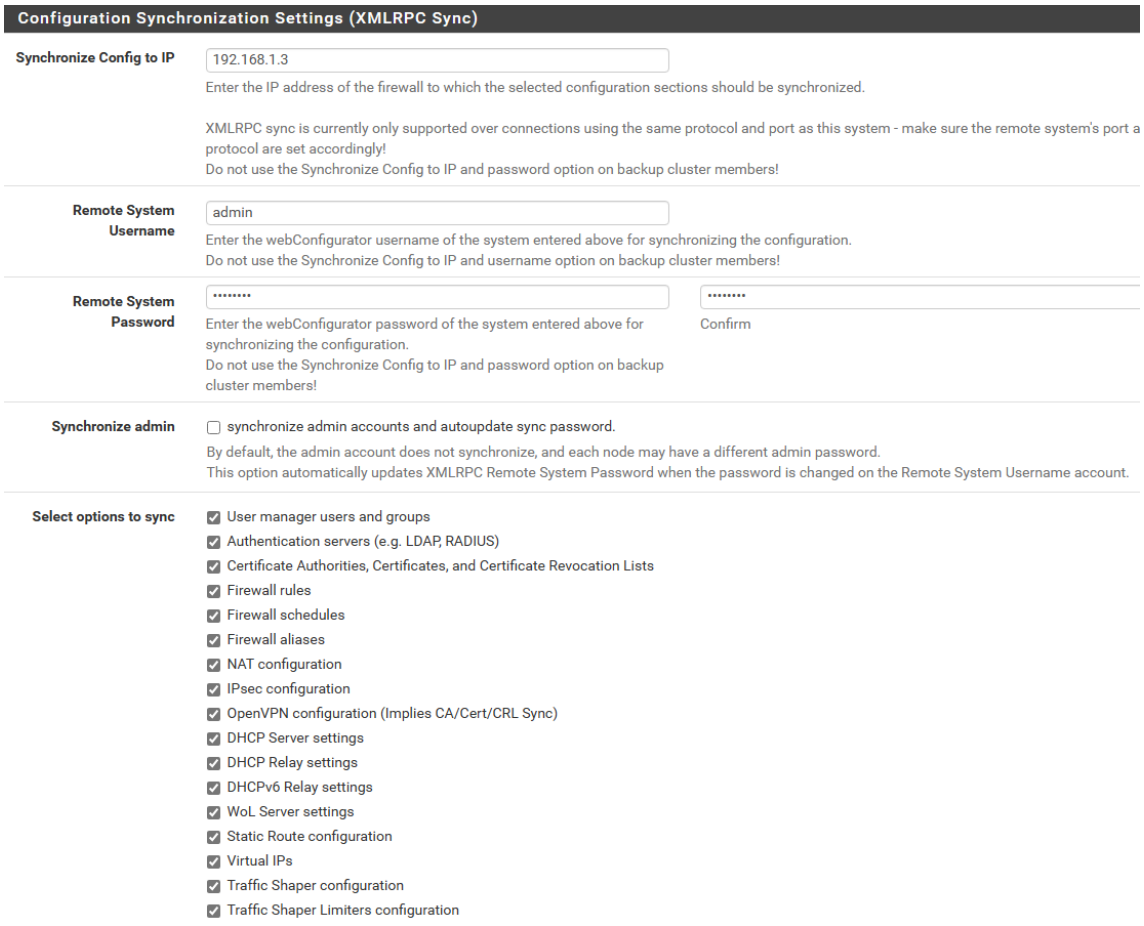
Joonis 13 kujutab HA (*High Availability*) sünkroniseerimise aktiveerimise seadistamist, kus määratakse port, mille kaudu sünkroniseerimine toimub (SYNC port projekti olukorras) ja teise tulemüüri SYNC IP-aadress. HA sünkroniseerimise seadistamine võimaldab tagada ruuterite töökindluse ja katkematu võrguteenuse pakkumise, kuna ühe ruuteri rikke korral võtab teine ruuter automaatselt üle võrgu haldamise ja töö.

Sama seadistus on tehtud ka teises tulemüüris.



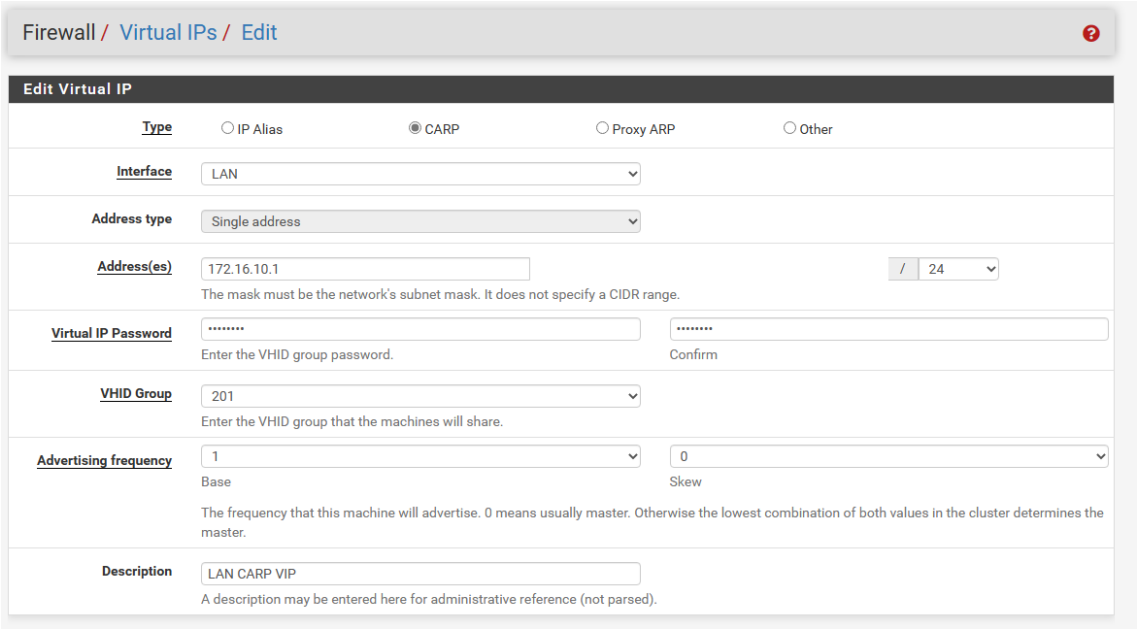
Joonis 13. HA seadistamine.

Joonis 14 kujutab XMLRPC (*XML* (*Extensible Markup Language*) *Remote procedure call*) sünkroniseerimise seadistamist. Seda seadistust on vaja ainult peamise tulemüüri jaoks. Määratakse seadme aadress, millega peamise seadme konfiguratsioon sünkroniseeritakse, kasutaja, kelle kaudu ühendus toimub, ning sünkroniseeritavad seadistused.



Joonis 14. XMLRPC süngi seadistamine.

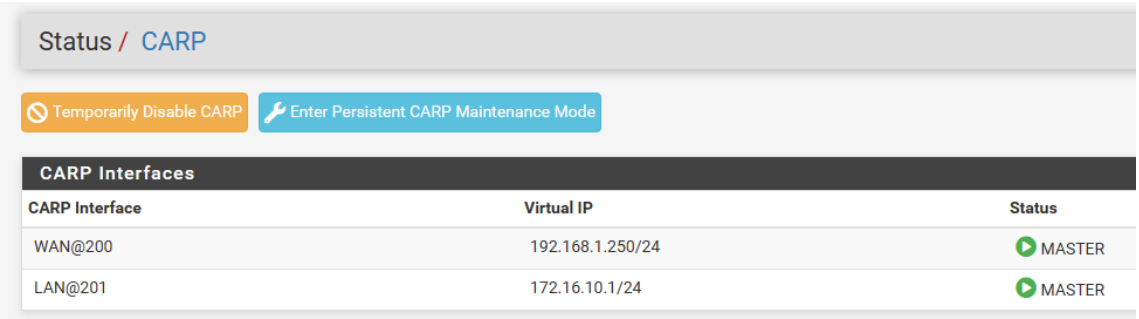
Joonis 15 kujutab CARP (*Common Address Redundancy Protocol*) tüüpi virtuaalse IP-aadressi seadistamist LAN võrgu jaoks. CARP võimaldab mitmel ruuteril jagada ühist IP-aadressi, et tagada ühtlane koormuse jaotamine ja kõrgkäideldavus.



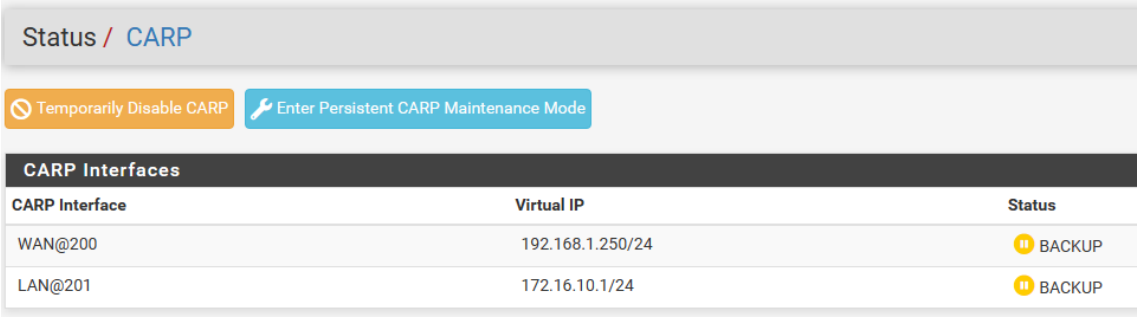
Joonis 15. Virtuaal IP seadistamine klastri jaoks.

Joonis 16 kujutab peamise pfSense ruuteri staatust, samas kui Joonis 17 näitab teise ruuteri staatust. Nendelt ekraanipiltidelt on näha, et peamine ruuter on määratud kui "*MASTER*" ja teisejärguline ruuter kui "*BACKUP*".

See konfiguratsioon tagab, et kui peamine ruuter peaks ebaõnnestuma, siis teine ruuter võtab automaatselt töö üle ja hoiab võrguühenduse stabiilsena.



Joonis 16. CARP staatus peatulemüüris.



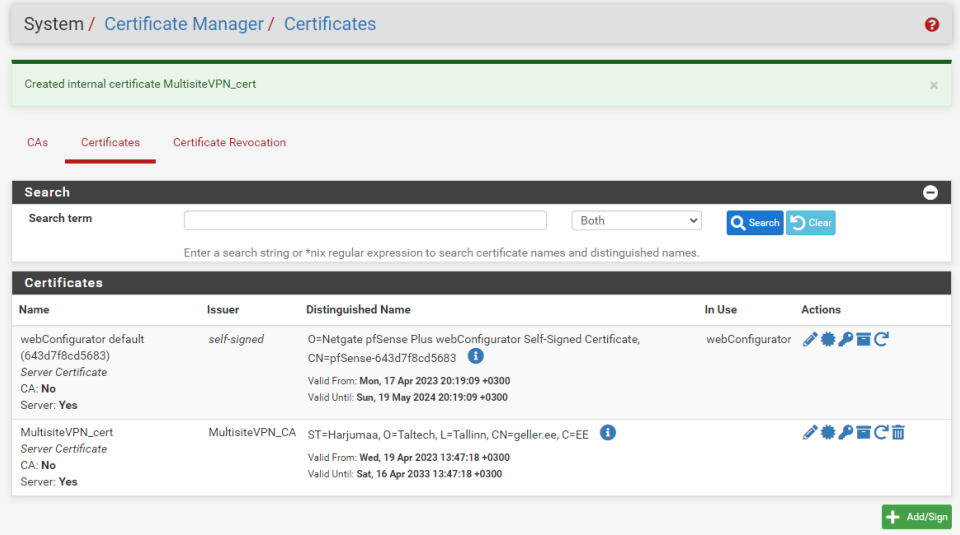
Joonis 17. CARP staatus teises tulemüüruis.

4.1.3 VPN serveri seadistamine

Joonis 18 kujutab loodud CA (*Certificate Authority*) sertifikaati, mis on vajalik OpenVPN-serveri seadistamiseks. CA-sertifikaat võimaldab luua turvalise krüpteeritud ühenduse serveri ja klientide vahel, tagades andmete privaatsuse turvalisuse VPN-ühenduse kaudu.

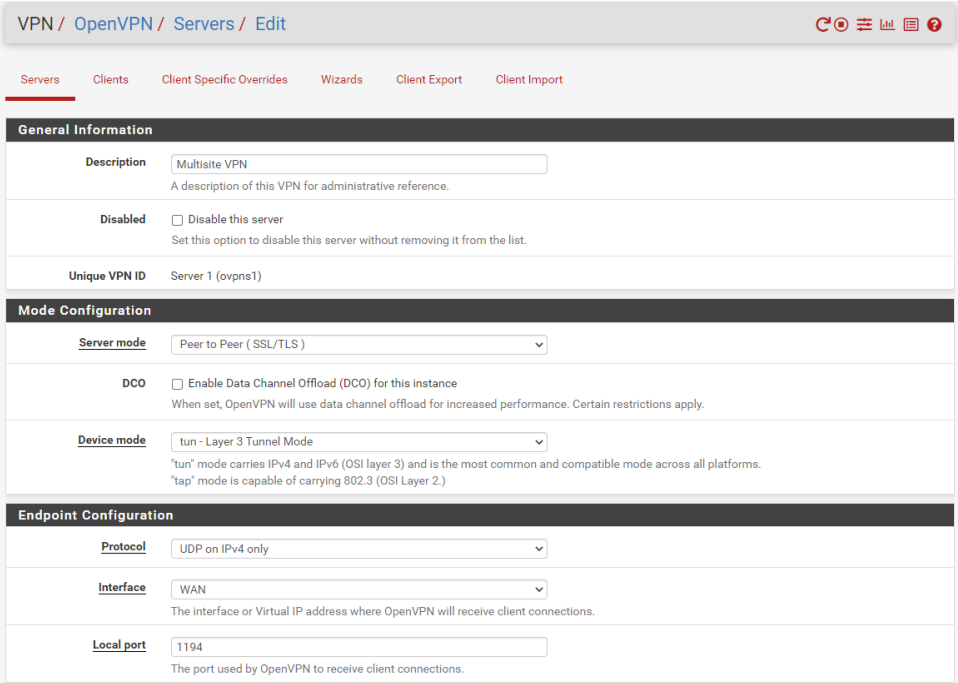
Joonis 18. OpenVPN serveri seadistamine: Sertifitseerimisasutuse loomine.

Joonis 19 kujutab loodud serveri sertifikaati, mis on samuti vajalik OpenVPN-serveri seadistamiseks. Serveri sertifikaat on oluline komponent turvalise krüpteeritud ühenduse loomisel klientide ja VPN-serveri vahel.



Joonis 19. OpenVPN serveri seadistamine: Serveri sertifikaadi loomine.

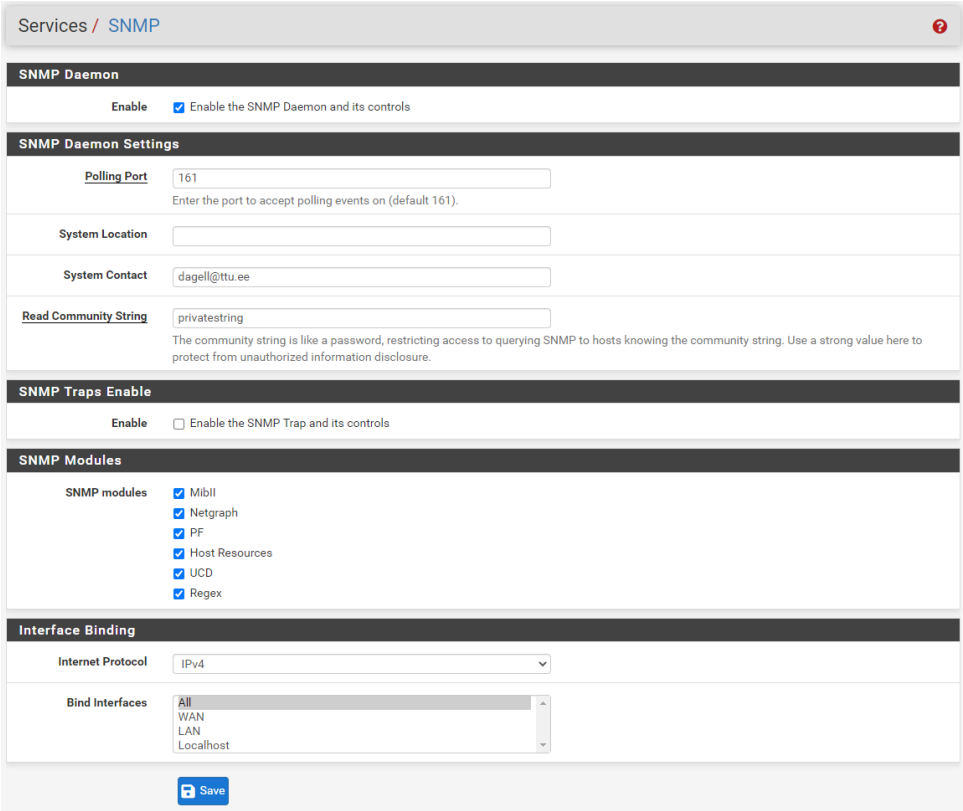
Joonis 20 ja lisas 2 toodud joonised kujutavad kõik OpenVPN-serveri seadistusi. Serverile on antud kirjeldus, määratud on serveri tüüp (*peer-to-peer* (SSL/TLS)), mis on vajalik ühendamiseks kaugruuteritega, mis toimivad klientidena. Samuti on määratud CA ja serveri sertifikaadid, VPN-tunneli jaoks eraldatud võrgu aadress, kohalik võrk, millele VPN-kliendid ligi pääsevad ja kaugvõrgud, millele on samuti juurdepääs olemas. VPN-klientide vaheline suhtlus on lubatud. Valiku *Advanced settings* alt on lisatud käsk "push "route 10.7.0.0 255.255.0.0", mis määrab marsruudi VPN-klientidele, et tagada võrguside kohalike ja kaugvõrkude vahel.



Joonis 20. OpenVPN serveri seadistamine: üldine informatsioon, režiimi määramine, lõpp-punkti konfiguratsioon.

4.1.4 Logide kogunemise seadistamine

Joonis 21 kujutab SNMP seadistusi, mille puhul on kasutusel SNMPv2. Kuigi SNMPv3 pakub täiustatud turvaomadusi, on selles kontekstis valitud kasutada SNMPv2 versiooni. Selle põhjuseks on asjaolu, et juurdepääs toimub ainult serveriruumist ja peakontorist, mis piirab oluliselt võimalikke turvariske. Lisaks on projekt ajutine, mistõttu on piisav muuta ainult *Read Community String*-i standardseadistust.



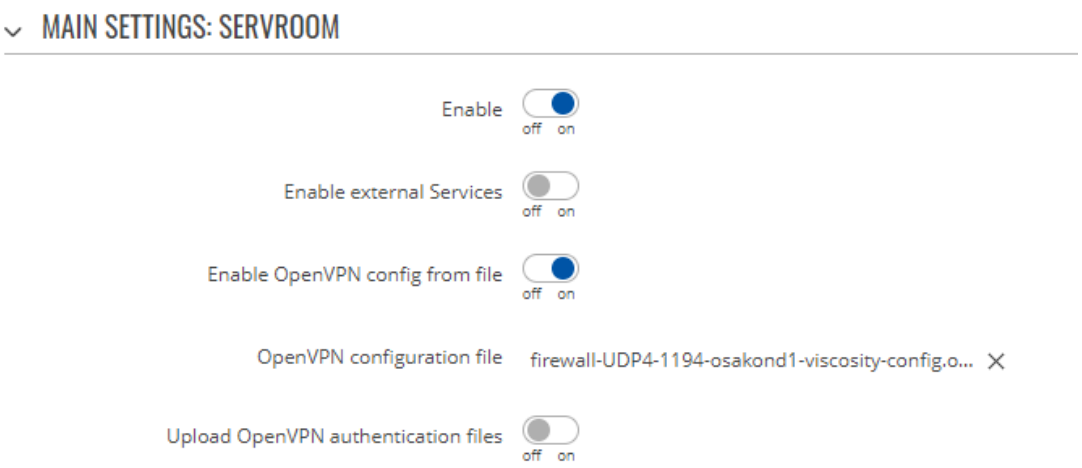
Joonis 21. SNMP seadistus.

4.2 Testimine

Käesolev alapeatükk hõlmab OpenVPN-i ja kõrgkäideldavuse testimist. OpenVPN-i testimise eesmärk on veenduda, et kõik tehtud seadistused on korrektselt paigas ja toimivad ettenähtud viisil. Kõrgkäideldavuse testimise eesmärk on kontrollida süsteemi võimet toime tulla erinevate olukordadega, tagades samal ajal teenuse järjepidevuse.

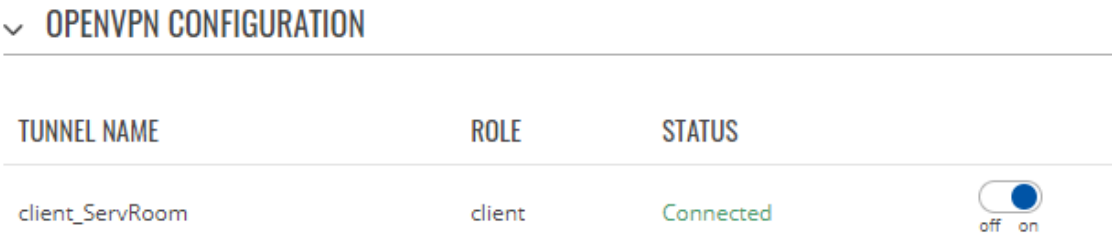
4.2.1 OpenVPN-i testimine

Joonis 22 näitab, kuidas toimub OpenVPN-kliendi seadistamine Teltonika RUT240 4G ruuteril. Selles etapis on konfigureeritud vajalikud parameetrid, et luua ühendus OpenVPN-serveriga.



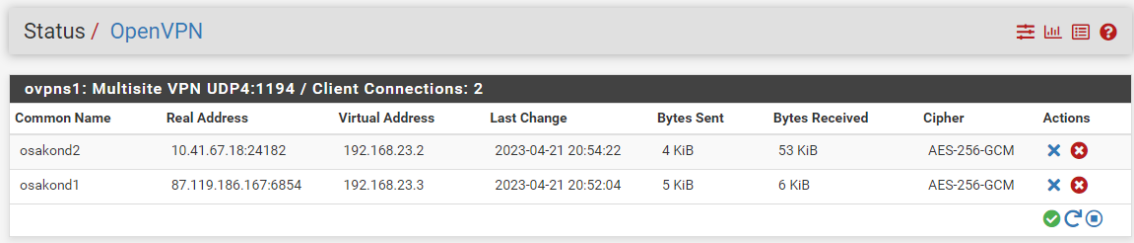
Joonis 22. Kliendi poolt VPN ühenduse seadistamine.

Joonis 23 kujutab Teltonika RUT240 4G ruuterit, mis on edukalt ühendatud VPN-serveriga. Ekraanipilt näitab ruuteri olekut ja teavet, mis kinnitab, et VPN-ühendus on loodud ja töötab nõuetekohaselt.



Joonis 23. Klient ühendatud VPN serverile.

Joonis 24 kujutab OpenVPN-serveri staatust, mis näitab, et mõlemad kliendid on edukalt ühendatud.



Joonis 24. OpenVPN status serveris.

Joonis 25 ja Joonis 26 näitavad, et ping päringud serveri lokaalsest võrgust jõuavad edukalt VPN-klientide kohalike võrkudeni.

```
C:\Users\server>ping 10.7.0.102

Pinging 10.7.0.102 with 32 bytes of data:
Reply from 10.7.0.102: bytes=32 time=5ms TTL=127
Reply from 10.7.0.102: bytes=32 time=5ms TTL=127
Reply from 10.7.0.102: bytes=32 time=6ms TTL=127
Reply from 10.7.0.102: bytes=32 time=7ms TTL=127

Ping statistics for 10.7.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 5ms
```

Joonis 25. Ping päring serveri ruumist 1 osakonnale tulemus.

```
C:\Users\server>ping 10.7.1.1

Pinging 10.7.1.1 with 32 bytes of data:
Reply from 10.7.1.1: bytes=32 time=6ms TTL=127
Reply from 10.7.1.1: bytes=32 time=6ms TTL=127
Reply from 10.7.1.1: bytes=32 time=5ms TTL=127
Reply from 10.7.1.1: bytes=32 time=12ms TTL=127

Ping statistics for 10.7.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 12ms, Average = 7ms
```

Joonis 26. Ping päring serveri ruumist 2 osakonnale tulemus.

Joonis 27 ja Joonis 28 näitavad, et ühe VPN-kliendi lokaalsest võrgust saadetud ping päringud jõuavad edukalt nii VPN-serveri lokaalse võrku kui ka teise VPN-kliendi lokaalse võrku.

```
C:\Users\daniel>ping 10.7.1.1

Pinging 10.7.1.1 with 32 bytes of data:
Reply from 10.7.1.1: bytes=32 time=8ms TTL=127
Reply from 10.7.1.1: bytes=32 time=6ms TTL=127
Reply from 10.7.1.1: bytes=32 time=5ms TTL=127
Reply from 10.7.1.1: bytes=32 time=7ms TTL=127

Ping statistics for 10.7.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 8ms, Average = 6ms
```

Joonis 27. Ping päring 1 osakonnast 2 osakonnale tulemus.

```
C:\Users\daniel>ping 172.16.10.50

Pinging 172.16.10.50 with 32 bytes of data:
Reply from 172.16.10.50: bytes=32 time=6ms TTL=127
Reply from 172.16.10.50: bytes=32 time=9ms TTL=127
Reply from 172.16.10.50: bytes=32 time=11ms TTL=127
Reply from 172.16.10.50: bytes=32 time=5ms TTL=127

Ping statistics for 172.16.10.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 11ms, Average = 7ms
```

Joonis 28. Ping päring 1 osakonnast serveri ruumile tulemus.

Joonis 29 ja Joonis 30 näitavad, et teise VPN-kliendi lokaalsest võrgust saadetud ping päringud jõuavad edukalt nii VPN-serveri lokaalsesse võrku kui ka esimese VPN-kliendi lokaalsesse võrku.

```
C:\Users\daniel>ping 10.7.0.102
Pinging 10.7.0.102 with 32 bytes of data:
Reply from 10.7.0.102: bytes=32 time=6ms TTL=127
Reply from 10.7.0.102: bytes=32 time=10ms TTL=127
Reply from 10.7.0.102: bytes=32 time=7ms TTL=127
Reply from 10.7.0.102: bytes=32 time=6ms TTL=127

Ping statistics for 10.7.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 10ms, Average = 7ms
```

Joonis 29. Ping päring 2 osakonnast 1 osakonnale tulemus.

```
C:\Users\daniel>ping 172.16.10.50
Pinging 172.16.10.50 with 32 bytes of data:
Reply from 172.16.10.50: bytes=32 time=6ms TTL=127
Reply from 172.16.10.50: bytes=32 time=8ms TTL=127
Reply from 172.16.10.50: bytes=32 time=7ms TTL=127
Reply from 172.16.10.50: bytes=32 time=7ms TTL=127

Ping statistics for 172.16.10.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 8ms, Average = 7ms
```

Joonis 30. Ping päring 2 osakonnast serveri ruumile tulemus.

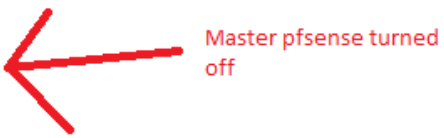
4.2.2 Kõrgkäideldavuse testimine

Joonis 31 kujutab kõrgkäideldavuse testimist. Alustuseks tehti ping päring klastri IP-aadressile. Mõne aja pärast lülitati pearuuter välja, mille järel mõned sekundit hiljem hakkas teine ruuter tööle kui *MASTER*.

```
C:\Users\server>ping 172.16.10.1 -t

Pinging 172.16.10.1 with 32 bytes of data:
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time=2ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Reply from 172.16.10.1: bytes=32 time=2ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time=1ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64
Reply from 172.16.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.10.1:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
Control-C
^C
```



Joonis 31. HA testimine. Ping päring klastrile.

5 Tulemused ja edasiarenduse võimalused

Käesoleva töö raames on rakendatud kõrgkäideldav mitmepoolne VPN-teenus seadmeid ja tarkvara tarniva ettevõtte näitel, mis tagab turvalise ja usaldusväärse võrguühenduse erinevate asukohtade vahel ning aitab kaasa süsteemi stabiilsusele ja töökindlusele.

Edasiarenduse võimalused võivad hõlmata kõrgkäideldavusega klastri paigutamist erinevatesse geograafilistesse asukohtadesse. Sellise klastri loomine erinevates asukohtades võib tagada suurema töökindluse ja vähendada katkestuste mõju ettevõtte igapäevasele tegevusele.

Lisaks võib kaaluda täiendavate turvameetmete rakendamist VPN-teenuse jaoks, nagu näiteks tugevamad krüpteerimisalgoritmid, juurdepääsu kontrollimine või täiendavate autentimismeetodite kasutamine, et saavutada veelgi suuremat turvalisust, paindlikkust ja skaleeruvust.

6 Kokkuvõte

Käesoleva töö eesmärk oli välja töötada ja rakendada kõrgkäideldava mitmepoolse VPN-teenuse projekt seadmeid ja tarkvara tarniva ettevõtte näitel, et tagada turvaline ja usaldusväärne ühendus kaugkontorite ja keskse kontori vahel.

Selle eesmärgi saavutamiseks viidi läbi olemasolevate tehnoloogiate analüüs ning valiti projekti põhitehnoloogiateks OpenVPN ja pfSense, kasutades virtuaal-IP-d CARP protokolliga kõrgkäideldavuse klastri loomiseks. Töö käigus käsitleti erinevaid projekti aspekte, nagu nõuete analüüs, tehnoloogiate valik, serveri- ja kliendiinfrastruktuuri rakendamine, süsteemi seadistamine ja testimine. Samuti uuriti võimalusi integreerimiseks täiendavate tehnoloogiate ja teenustega, nagu jälgimissüsteemid.

Töö tulemusena saavutati kõik seatud eesmärgid ning rakendati edukalt kõrgkäideldav mitmepoolne VPN-teenus. Saadud tulemused ja rakenduskogemus võivad olla kasulikud ettevõtetele ja võrgutehnoloogia valdkonna spetsialistidele, kes planeerivad võrguinfrastruktuuri rakendamist või moderniseerimist, samuti VPN-teenuste ja võrguturbega tegelevatele võrguarendajatele ja administraatoritele.

Kasutatud kirjandus

[1] Tele2, „Mis on VPN ja millega seda süüakse?,“ Tele2, 20 February 2017. [Võrgumaterjal]. Available: https://tele2.ee/blogi/teletarkus/vpn. [Kasutatud 15 February 2023].

[2] „What Is High Availability?,“ Cisco, [Võrgumaterjal]. Available: https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-high-availability.html#~high-availability-clusters-explained. [Kasutatud 15 April 2023].

[3] R. Araiza, „What is a VPN and why do organizations use them?,“ Digital Guardian, 15 June 2022. [Võrgumaterjal]. Available: https://www.digitalguardian.com/blog/5-virtual-private-network-vpn-best-practices-2022. [Kasutatud 15 April 2023].

[4] C. McGuire, A. Zaman, D. Coulter ja J. Martinez, „Remote work using Azure VPN Gateway Point-to-site,“ Microsoft, 14 February 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/azure/vpn-gateway/work-remotely-support. [Kasutatud 18 April 2023].

[5] N. Drake, „What is a site-to-site VPN?,“ techradar, [Võrgumaterjal]. Available: https://www.techradar.com/vpn/what-is-a-site-to-site-vpn. [Kasutatud 18 April 2023].

[6] M. Higgins, „What is a remote access VPN and how does it work?,“ NordVPN, 6 October 2022. [Võrgumaterjal]. Available: https://nordvpn.com/ru/blog/remote-access-vpn/. [Kasutatud 18 April 2023].

[7] „Introducing Multi-Site and Site-to-Site VPN,“ Meraki, 11 July 2022. [Võrgumaterjal]. Available: https://blog.meraki-go.com/2022/11/07/introducing-multi-site-and-site-to-site-vpn/. [Kasutatud 19 April 2023].

[8] Cloud Timeweb, „Что такое OpenVPN и для чего он нужен?,“ Timeweb Cloud, 9 February 2022. [Võrgumaterjal]. Available: https://timeweb.cloud/blog/chto-takoe-openvpn-i-dlya-chego-on-nuzhen. [Kasutatud 14 April 2023].

[9] „What is OpenVPN?,“ OpenVPN, [Võrgumaterjal]. Available: https://openvpn.net/faq/what-is-openvpn/. [Kasutatud 10 April 2023].

[10] S. Mash, „OpenVPN VPN Protocol,“ PrivacyHQ, [Võrgumaterjal]. Available: https://privacyhq.com/documentation/openvpn-vpn-protocol/. [Kasutatud 12 April 2023].

[11] „What is L2TP/IPsec?,“ ExpressVPN, [Võrgumaterjal]. Available: https://www.expressvpn.com/what-is-vpn/protocols/l2tp. [Kasutatud 10 April 2023].

[12] D. Crawford, „OpenVPN vs IKEv2 vs PPTP vs L2TP/IPSec vs SSTP - Ultimate Guide to VPN Encryption,“ ProPrivacy, 30 June 2020. [Võrgumaterjal]. Available: https://proprivacy.com/vpn/guides/vpn-encryption-the-complete-guide. [Kasutatud 21 April 2023].

[13] S. Mash, „L2TP VPN Protocol,“ PrivacyHQ, [Võrgumaterjal]. Available: https://privacyhq.com/documentation/l2tp-vpn-protocol/. [Kasutatud 12 April 2023].

[14] „What is PPTP?,“ ExpressVPN, [Võrgumaterjal]. Available: https://www.expressvpn.com/what-is-vpn/protocols/pptp. [Kasutatud 14 April 2023].

[15] F. S. Perez, "A Framework for the Performance Analysis and," 01 June 2018. [Online]. Available: https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=7867&context=etd. [Accessed 21 April 2023].

[16] S. Mash, „PPTP VPN Protocol,“ PrivacyHQ, [Võrgumaterjal]. Available: https://privacyhq.com/documentation/pptp-vpn-protocol/. [Kasutatud 12 April 2023].

[17] „What is WireGuard?,“ [Võrgumaterjal]. Available: https://www.websiterating.com/vpn/glossary/what-is-wireguard/. [Kasutatud 14 April 2023].

[18] S. Mash, „Wireguard VPN Protocol,“ PrivacyHQ, [Võrgumaterjal]. Available: https://privacyhq.com/documentation/wireguard-vpn-protocol/. [Kasutatud 12 April 2023].

[19] P. Bischoff, „VPN protocols explained and compared,“ comparitech, 25 August 2021. [Võrgumaterjal]. Available: https://www.comparitech.com/vpn/protocols/. [Kasutatud 5 May 2023].

[20] D. Fincher, „The Advantages and Disadvantages of OpenVPN,“ SAP, 24 April 2019. [Võrgumaterjal]. Available: https://blogs.sap.com/2019/04/24/the-advantages-and-disadvantages-of-openvpn/. [Kasutatud 12 April 2023].

[21] „OpenVPN – Pros and Cons,“ bobcares, 8 February 2019. [Võrgumaterjal]. Available: https://bobcares.com/blog/openvpn-pros-and-cons/. [Kasutatud 13 April 2023].

[22] Netgate Docs, „Virtual IP Addresses,“ Netgate, 29 June 2022. [Võrgumaterjal]. Available: https://docs.netgate.com/pfsense/en/latest/firewall/virtual-ip-addresses.html. [Kasutatud 17 April 2023].

[23] „OpenVPN Compatibility,“ OpenVPN, [Võrgumaterjal]. Available: https://openvpn.net/faq/openvpn-compatibility/. [Kasutatud 23 April 2023].

[24] J. Ellingwood, „An Introduction to SNMP (Simple Network Management Protocol),“ DigitalOcean, 18 August 2014. [Võrgumaterjal]. Available: https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol. [Kasutatud 14 April 2023].

[25] A. Thapa, „Why Should I Backup Data? What’s The Importance,“ TechNewsToday, 10 August 2022. [Võrgumaterjal]. Available: https://www.technewstoday.com/why-should-you-backup-data/. [Kasutatud 15 April 2023].

[26] „OpenVPN,“ Netgate, 2 August 2022. [Võrgumaterjal]. Available: https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html. [Kasutatud 22 April 2023].

[27] „OpenVPN Site-to-Site Configuration Example with SSL/TLS,“ Netgate, 30 January 2023. [Võrgumaterjal]. Available: https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-s2s-tls.html. [Kasutatud 20 April 2023].

[28] M. Eddy, „PCMag,“ 21 February 2023. [Võrgumaterjal]. Available: https://www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one. [Kasutatud 15 April 2023].

[29] R. Joyce, „How to best implement a VPN solution,“ itbusiness, 31 July 2002. [Võrgumaterjal]. Available: https://www.itbusiness.ca/news/how-to-best-implement-a-vpn-solution/4391. [Kasutatud 15 April 2023].

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Daniel Geller

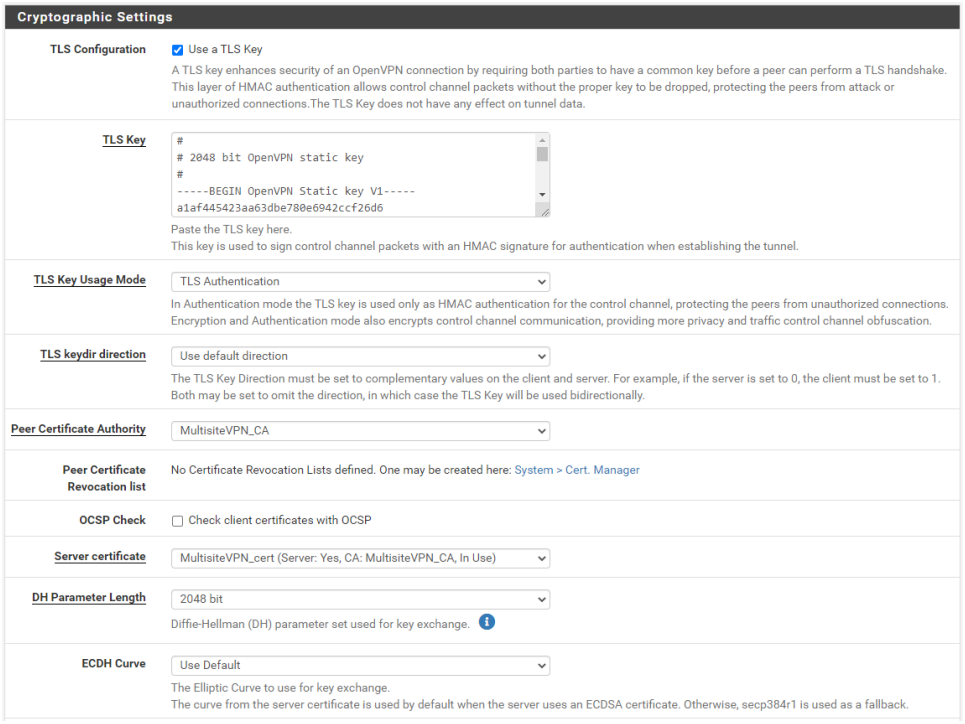
1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Kõrgkäideldava mitmepoolse VPN-teenuse rakendamine seadmeid ja tarkvara tarniva ettevõtte näitel", mille juhendaja on Kristiina Hakk
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

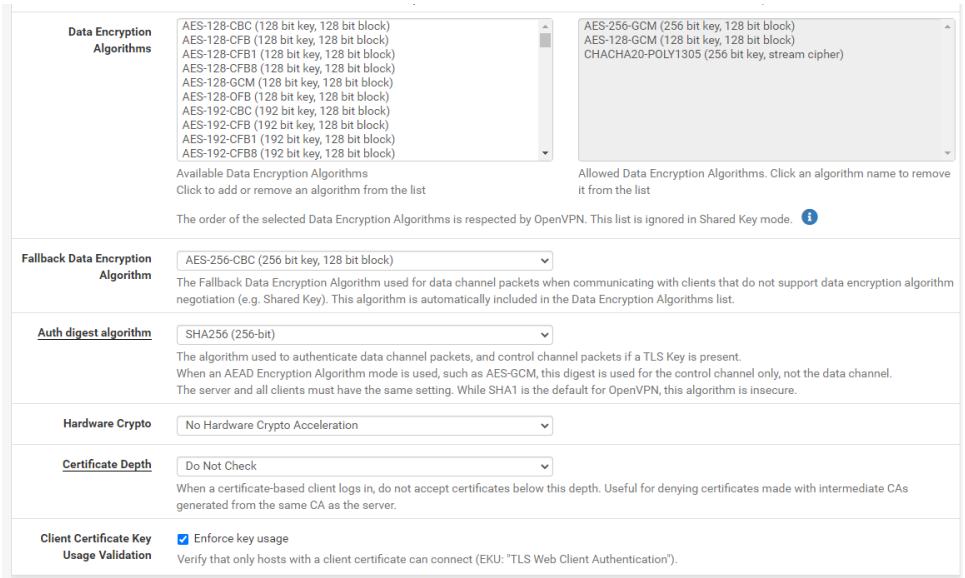
24.04.2023

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – OpenVPN serveri sätted

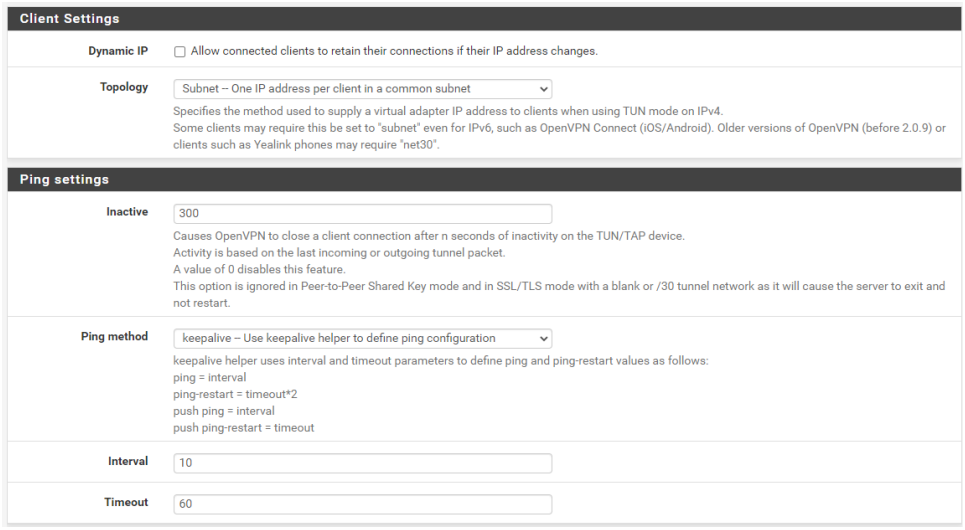
OpenVPN serveri seadistamine: krüptograafilised sätted.





OpenVPN serveri seadistamine: tunneli sätted.

OpenVPN serveri seadistamine: kliendi sätted, ping sätted.



OpenVPN serveri seadistamine: täiustatud konfiguratsioon.