TALLINNA TEHNIKAÜLIKOOL
INSENERITEADUSKOND
Virumaa kolledž

Ettevõtte IT-süsteemi renoveerimine VMware tõrkekindla klastri tehnoloogiaga

Renovation of company's IT system with VMware failover cluster technology

TELEMAATIKA JA ARUKAD SÜSTEEMID

Üliõpilane: Eduard Mazur
Üliõpilaskood: 183327
Juhendaja: Oleg Shvets, lektor

Kohtla-Järve, 2022

AUTORIDEKLARATSIOON

Olen koostanud lõputöö iseseisvalt.

Lõputöö alusel ei ole varem kutse- või teaduskraadi või inseneridiplomit taotletud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

"...." ..... 20.....

Autor: .....
/ allkiri /

Töö vastab rakenduskõrgharidusõppe lõputööle/magistritööle esitatud nõuetele
"...." ..... 20.....

Juhendaja: .....
/ allkiri /

Kaitsmisele lubatud
"...." ..... 20.....

Kaitsmiskomisjoni esimees .....
/ nimi ja allkiri /

LIHTLITSENTS LÕPUTÖÖ ÜLDSUSELE KÄTTESAADAVAKS TEGEMISEKS JA REPRODUTSEERIMISEKS

Mina Eduard Mazur (sünnikuupäev: 15.09.1966)

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

lõputöö "Ettevõtte IT-süsteemi renoveerimine VMware tõrkekindla klastri tehnoloogiaga", mille juhendaja on Oleg Shvets,

1.1. reprodutseerimiseks säilitamise ja elektroonilise avaldamise eesmärgil, sealhulgas 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 punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta kolmandate isikute intellektuaalomandi ega isikuandmete kaitse seadusest ja teistest õigusaktidest tulenevaid õigusi.

TalTech Inseneriteaduskond Virumaa kolledž
LÕPUTÖÖ ÜLESANNE

Üliõpilane: Eduard Mazur, 183327

Õppekava, peaeriala: EDTR17/18 – Telemaatika ja arukad süsteemid

Juhendaja(d): Lektor, Oleg Shvets, oleg.shvets@taltech.ee

Konsultant: nimi, amet

ettevõte, telefon, e-post

Lõputöö teema:

(eesti keeles) *Ettevõtte IT-süsteemi renoveerimine VMware tõrkekindla klastri tehnoloogiaga*

(inglise keeles) Renovation of company's IT system with VMware failover cluster technology

Lõputöö põhieesmärgid:

Lõputöö peamine eesmärk on luua väikese ettevõtte IT-süsteemi renoveerimise projekt koos tõrkekindla klastri loomisega.

1. Domeenivõrgu kujundamine koos VMware virtuaalsete masinate tõrkekindla klastri loomisega.
2. Ruuteri konfigureerimine arvutivõrgu VLAN-segmenteerimiseks, võttes arvesse turvanõudeid.
3. Andmete tervikliku arhiveerimise ja turvalise tootmisesisese infoedastuse tagamine.

Lõputöö etapid ja ajakava:

Nr	Ülesande kirjeldus	Tähtaeg
1.	Lõputöö teema valik	01.09.22
2.	Infosüsteemi kujundamise põhisuundade valik	08.09.22

3.	Otsida ettevõtte kohtvõrku sobivat renoveerimisprojekti	12.09.22
4.	Reaalobjekti valitud tehnilise projekti mõõdistuse analüüs	18.09.22
5.	Eesmärkide selgitamine ja lõputöö etappide moodustamine	25.09.22
6.	Lõputöö etappide teostamise ajakava koostamine.	28.09.22
7.	IT tehnoloogiate ja meetodite valimine töö tegemiseks	02.10.22
8.	Soodsa varustuse ja tarkvara erinevate võimaluste analüüs	07.10.22
9.	Selleks, et töötada välja tõrkekindla süsteemi tehnoloogia, valmistada ette labori stend	10.10.22
10.	Valmistada ette täielik käskude loend VLAN-ide konfigureerimiseks Mikrotik ruuteris	15.10.22
11.	Reaalobjektil sekundaarne tööde teostamine	21.10.22
12.	Töötage välja tehnoloogia tõrkesiirde klastri loomiseks ettevõtte kohalikus võrgus	22.11.22
13.	Stendil põhiülesannete osas tehtud tööde põhjal koostada reaalse objekti tööplaan.	01.12.22
14.	Lõputöö esitamine	12.12.22

Töö keel: Eesti..... **Lõputöö esitamise tähtaeg:** "....."..... 20.....a

Üliõpilane: ..... "....."..... 20.....a
/allkiri/

Juhendaja: ..... "....."..... 20.....a
/allkiri/

Konsultant: ..... "....."..... 20.....a
/allkiri/

Programmijuht: ..... "....."..... 20.....a
/allkiri/

SISUKORD

EESSÕNA

"Ettevõtte IT-süsteemi renoveerimine VMware tõrkekindla klastri tehnoloogiaga"-teema valik tuleneb sellest, et autor osales IT-süsteemi uuendamise projektis Ida-Virumaa väiketööstusettevõttes. Huvipakkuvaimaks ülesandeks oli luua süsteem uue tehnoloogiaprogrammi pidevaks toimimiseks, milleks sobib hästi käesolevas töös uuritav VMware hüperviisoril põhinev virtuaalmasinate tõrkeklastri tehnoloogia.

Teiseks väljakutset pakkuvaks ülesandeks oli olemasoleva MikroTiki ruuteri ettevalmistamine kohtvõrgu segmenteerimiseks (VLAN-ide loomine). Kuna selles odavas ruuteris ei ole riistvaralist kommutaatorit, ei tööta tavaline konfiguratsioon õigesti. Autor usub, et selle töö tulemusena loodud ruuterikäskude täielik loend on kasulik selle ettevõtte kohaliku võrgu edasiseks moderniseerimiseks. See hõlmab käske, et tagada kaitse väliste ohtude vastu (tulemüüri), luua VLAN-e, ning tagada kaugtöö puhul (VPN ühendus) turvalise kanali.

Täiendavalt tuli uurida võimalust teabe ohutuks edastamiseks tootmise juhtimise kontrolleritest tehnoloogide ja laborantide kontorisse. Uuringu tulemusena õnnestus leida turvaline ja soodne lahendus.

Autor tänab kõiki, kes aitasid kaasa antud töö valmimisele!

Märksõnad: MikroTik, MS Server, VPN, Veeam Backup, PRTG Monitor, VLAN, GPO, VMware ESXi, Failover cluster, Modbus Gateway.

LÜHENDITE JA TÄHISTE LOETELU

- VLAN - loogiliselt kokkukuuluv võrgustatud olemite kogum. ISO/IEC 27033: loogiliselt struktuurilt sõltumatu võrk füüsilises võrgus
- ROUTING - marsruutimine
- VPN - virtuaalne privaatvõrk
- L2TP - Layer 2 Tunneling Protocol, "kihi 2 tunnelduspротokoll"
- GPO - rühmapoliitika objekt - MS Serveris
- DHCP - hosti dünaamilise konfigureerimise protokoll
- DNS – Domain Name System
- Gateway - funktsionaalüksus, mis ühendab kaht arhitektuurilt üksteisest erinevat arvutivõrku
- Firewall – tulemüür, läbistuskindel komponendikogum kahe võrgu vahel, juhib kogu võrguliiklust mõlemas suunas, laseb läbi ainult kohaliku turvapoliitikaga lubatava liikluse
- Winbox – MikroTik'i konfiguratsioonitarkvara
- RouterOS - MikroTik'i WiFi ruuteri OS
- PharOS – TP-Link'i WiFi ruuteri OS
- F_1 - esimene Fersnel tsoon
- Ping Watch Dog - WiFi-ühenduse kontrollimine
- VMware - platvorm virtuaalmasinate loomiseks ja hooldamiseks
- VM – virtuaalmasin

SISSEJUHATUS

Esitletava töö eesmärgiks on väiketööstusettevõtte IT-süsteemi renoveerimine. Tavaliselt hõlmab renoveerimine vanade seadmete ja arvutite väljavahetamist, uue turvalisema võrgu loomist välisohtude eest kaitseks ning andmete turvalise kasutamise ja säilitamise tagamist.

Pärast uue serveri installimist tuleks juurutada kaks Windows Serveriga virtuaalmasinat. Üks Active Directory DC-i ja teine failiserveri (FS) jaoks.

Virtuaalsete masinate jaoks mõeldud kaasaegse tõrkekindla klastrite tehnoloogia tundmaõppimine peaks tagama, et vajalikud rakendused töötavad jätkusuutlikult. Antud töös on kasutatud kaasaegseid tarkvaralahendusi tuntud virtuaalsete IT-süsteemide arendajalt - VMware. Nende tehnoloogiate valik tuleneb sellest, et autor omab väga head mitmeaastast kogemust VMware tarkvaratoodetega.

Kahtlemata on turvalise, usaldusväärse ja kollisioonikindla kohtvõrgu loomine üsna raske ülesanne ja nõuab eelnevaid kogemusi sarnaste projektidega.

Ettevõtte arvutivõrgu väliste ohtude kaitsmiseks on süsteemi kõige olulisem komponent ruuteri tulemüür. Käesoleval ajal kasutab ettevõte MikroTik ruuterit, mis on odav, kuid usaldusväärne ja tõestatud.

Arvutivõrkude turvalisuse üheks oluliseks komponendiks on ka võrgu segmenteerimine eraldi osadeks - VLAN. Praktikas hõlbustab segmenteeritud võrgumudeli loomine Cisco Packet Traceris võrgu struktuuri mõistmist.

Virtuaalsete masinate tõrgeteta töö tagamise probleemi lahendamiseks selles ettevõttes on vaja luua eraldi laboristend. Nii on võimalik turvaliselt uurida keerulisi tehnoloogiaid, ja seejärel kasutada parimaid lahendusi praktikas.

Enne IT-süsteemi uuendamise projektiga alustamist uuriti selle tegelikku seisu:

- kolmekorruselises kontoris kasutatakse 15 arvutit, 1 failiserver, 3 haldamata kommutaatorit ja mitu võrguprinterit;
- internetiühenduse tagab MikroTik ruuter;
- tööstuslikud kontrollerid ja juhtimissüsteem on isoleeritud Internetist ja kontorist (SCADA);
- WiFi AP kaudu on kontoriga ühendatud 2 kaugobjekti;
- registripidajaga on ühendatud mitu IP videovalve kaamerat.

Käesoleva töö struktuuri loomisel otsustati IT-süsteemi vaadeldavad funktsioonid jagada kolmeks põhiosaks:

- ***serveri funktsioonid***;
- ***ruuteri funktsioonid***;
- ***teised üksikud funktsioonid***, mis kuuluvad samuti ettevõtte IT-süsteemi ja kasutavad IT-tehnoloogiaid.

Töös kasutatakse tuntud programme, teenuseid ja seadmeid, nagu: MS Server Standard, Domain AD, Group Policies (GPO), server DELL PowerEdge R440, VMware vSphere ESXi, router MikroTik L3 RB750gr3, WSUS, Veeam Backuper, PRTG Monitor, WiFi ruuterid TP-link ja Mikrotik, hallatavad kommutaatorid L2+.

1 SERVERI FUNKTSIOONID

1.1 Uue projekti analüüsi osa

Projekti töö algfaasis viidi läbi süsteemi hetkeseisu audit. Auditi aruanne esitati ettevõtte juhtkonnale, seal kajastusid võrgu struktuuris ilmsed ja võimalikud puudused ning riskid turvasüsteemis. Ettevõtte võrgu renoveerimiseks koostati nimekiri soovitustest.

Peamised soovitused on:

- Asendada vanad võrgukaablid uutega vastu vastavalt standardile CAT6e;
- Hallatavad kommutaatorid tuleb täiendada varutoiteallikaga (UPS), ja paigutada võtmega lukustatavatesse väikestesse serverikappidesse;
- Seadistada ruuter ümber VLAN-ide loomiseks ja paremaks kaitseks;
- Backup server ei tohiks asuda serveriruumis ning peab olema tagatud samasugune kaitse sissetungimise eest - alarm, valvekaamera, väga piiratud juurdepääs;
- Valmistada uues serveris ette 2 virtuaalmasinat MS Windows operatsioonisüsteemiga;
- Valmistada ette 3 „VMware" serverit (hostit) ja luua „ESXi 7.0.3" baasil virtuaalmasinate tõrkekindel klaster;
- Andmete ja virtuaalmasinate arhiveerimiseks paigaldada ja konfigureerida tarkvara „Veeam Backup & Replication Community Edition";
- Paigaldada tarkvara „PRTG monitori" võrgu ja arvutite oleku jälgimiseks ja analüüsimiseks.

1.2 Seadmete valik

IT-süsteemi uuendamise eesmärgil käsitletakse antud alateemas arvutite, võrguseadmete ja tarkvara uuendamise võimalusi. Pakutavad varustuse valikud peavad olema ühelt poolt piisavalt tõhusad ja teisest küljest mõistliku maksumusega.

Koostati hinnapakkumised, osa neilt oli praktikas rakendatud ja seadmed on juba töös (vt lisa 1).

1.2.1 Põhiserveri valik

Põhiserveri eeldatavad töövaldkonnad on:

- Domeenikontroller;
- DNS server;

- Failiserver;
- Raamatupidamise tarkvara server;
- WSUS-i värskenduste server.

Oli võrreldud serverid järgmistest tootjatelt: Dell, HP, Lenovo ja Fujitsu. Oli otsustatud, et kõige otstarbekaim on kasutada Dell R440. See on tavaline, üsna odav server. See sobib peaaegu igasse serveri rolli jaoks. Serveri, kasutajalitsentside, VMware tarkvarapaketi täishinnapakkumine on esitatud seadmete tabelis (vt lisa 1).[1]

Joonis 1.1. Dell Server R440

1.3 Domeenivõrgu Active Directory

Domeenivõrgus on alati olemas põhiserver – domeenikontroller. Domeenikontroller vastutab failidele ja teistele ressurssidele juurdepääsuõiguste eest.[2]

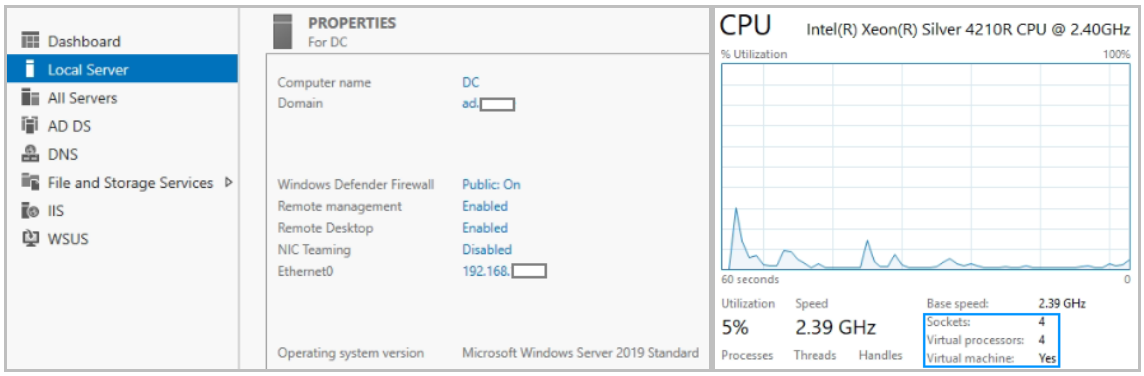
1.3.1 Vajadus domeenivõrgu järele

Domeenivõrgule tuleks mõelda, kui vähemalt üks väide on tõene:

- Kontoris on üle 15 arvuti ja nende arv kasvab;
- Arvutivõrgus on failiserver;
- Vajalik on arvutiseadmete ühtsus – sama tarkvara, võrguprinterite kasutamine, samad turvaseaded;
- Ettevõttes on personali voolavus (töötajad tihti tulevad juurde või lahkuvad);
- Töötajad töötavad vahetustega sama arvuti taga;
- Sama töötaja töötab mitmes arvutis;
- On vaja teada, kes ja millal failidega töötas. Nt. keegi võiks mõne olulise dokumendi kustutada või viirust sisse tuua;
- On vajadus kontrollida juurdepääsu Internetile. Nt. lülitada sotsiaalvõrgudele liigipäsu välja või lubada juurdepääsu ainult ettevõtte veebilehele.

Pärast uue serverikapi vastuvõtmist ja kokkupanemist, paigaldati sellesse uus „*rackmount server*". Windows Server 2019 litsents võimaldab kasutada ainult kahte VM-i ja mitte rohkem kui 16 protsessorituuma. Seetõttu installiti üks VMware ECX 7.0 VM domeenikontrolleri jaoks (DC, 4 vCPU-d) ja teine failiserveri jaoks (FS, 12 vCPU-

d). Vastavalt ülesandele tõsteti DC, DNS, FS, WSUS ja IIS rollid. Samuti oli installitud seadmete kasutajalitsentsid (20 CALs for devices). Samuti installeeriti seadmete kasutajalitsentsid (20 CALs for devices). Arvutid ja kasutajad sisestati domeeni ning andmed viidi uude serverisse.



Joonis 1.2. VM Windows Server 2019 DC, DNS, FS, IIS ja WSUS-i rolliga

1.3.2 Rühmapoliitikate seadistamine

Rühmapoliitika on MS Windows Active Directory lisa, mis võimaldab kasutajate ja arvutite kontode täiendavat kontrolli. See võimaldab kasutaja arvutit keskselt hallata ja seadistada, andes sellega lisaturbe võimaluse. Rühmapoliitika iseenesest on hulk süsteemiadministraatorite loodud seadistusi, mis on seotud Active Directory konteineriga (domeenid, veebilehküljed, OUd).

Lisaks on administraatoritele Group Policy Analyser. Haldusvahend on mõeldud GPOde omavaheliseks võrdlemiseks ja tööjaamade seadistuste auditeerimiseks rühmapoliitikate vastu. Rühmapoliitika objektid protsessitakse loogilises järjekorras:

- Kohalik poliitika
- Veebilehe poliitika
- Domeeni poliitika
- OUde poliitika – rakendub ka hierarhiliselt.

See jaotis sisaldab mõningaid rühmapoliitika reegleid ja nõuanned rühmapoliitika haldamiseks. Domeeni konfigureerimise rakendati mõned mainitud reeglid.[3]

Reegel 1. Kasutada minimaalselt Default Policy muudatusi.

Active Directory sisaldab kahte vaikepoliitikat: „Default Domain Policy" ja „Default Domain Controllers Policy".

Default Domain Policy peaks määrama ainult järgmiste:

- Salasõna poliitika
- Domeenikonto lukustamise eeskirjad

- Domeeni Kerberose poliitika

Default Domain Controllers Policy peaks määrama ainult järgmised parameetrid:

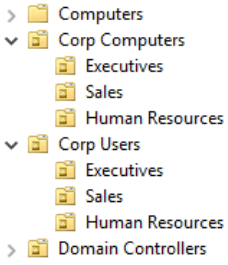
- Kasutajaõiguste määramise poliitika
- Auditipoliitika

Reegel 2. Kasutada minimaalselt GPO-d juurdomeeni tasemel.

Peaks minimeerima kõik muud juurdomeeni tasemel lingitud GPO-d, kuna need eeskirjad kehtivad kõigile domeeni kasutajatele ja arvutitele.

Reegel 3. Korraldada oma OU struktuuri.

Hea organisatsiooniüksuse struktuur muudab mitme rühmapoliitika haldamise ja tõrkeotsingu lihtsamaks.



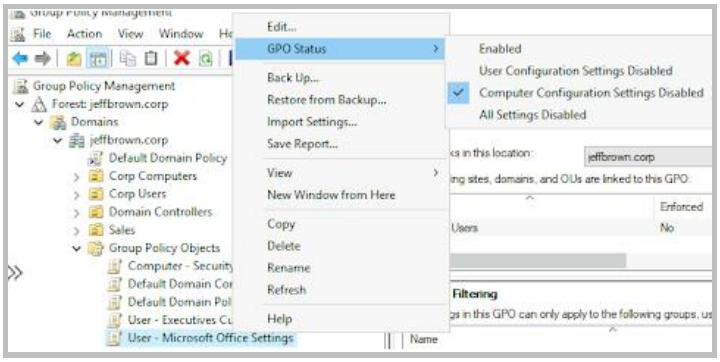
Joonis 1.3. Struktuur, mis sisaldab konkreetsete osakondade OU-sid

Reegel 4. Vältida poliitika pärimise ja poliitika jõustamise blokeerimist.

GPO pärimise blokeerimine OU tasemel takistab kõrgema taseme poliitikate rakendamist, näiteks ülem-OU-lt või juurdomeenilt.

Reegel 5. Kasutada kirjeldavaid nimesid, et saaksite kiiresti tuvastada GPO eesmärgi.

Reegel 6. Kasutamata arvuti ja kasutaja konfiguratsioonid tuleb keelata.



Joonis 1.4. Arvuti konfiguratsiooniseaded on kasutajate jaoks keelatud – Microsoft Office'i seadete GPO

Reegel 7. Lihtsustage haldust väiksemate GPO-dega.

GPO-d sihivad konkreetseid sätteid, nagu Microsoft Office või arvutiturve. Mõned teised ideed väiksemate poliitikate jaoks on järgmised: Windowsi värskendus, brauseri seaded, võrgusätted, Bitlocker, Applocker, tulemüüri reeglid.

Reegel 8. Rühmapoliitika varundamine.

Rühmapoliitikad on oluline osa Active Directory infrastruktuurist ja seetõttu tuleb poliitikat regulaarselt reserveerida. Saab kasutada kolmanda osapoole tööriistu või luua PowerShelli kohandatud skripti, kasutades käsku Backup-GPO.

Renoveeritud ettevõtte IT-süsteemi Active Directory turvasüsteemi seadistamine sisaldab muu hulgas järgmisi seadistusi:

- Kohaliku tööjaama salasõnade vahemälu seadistamine;
- Windows Defender Application Control: AppLocker ja Device Guard on Windows Defenderi üks osa;
- Edge, Chrome'i ja Firefoxi vaikebrauseri seadistamine;
- Tarkvara paigaldamine rühmapoliitika abil;
- OneDrive'i keelamine, kuna ettevõte seda ei kasuta;
- Remote Desktopi seadistamine: GPO-de kasutamine RDP kaudu;
- Vaikekeele muutmine sisselogimiskuval;
- Failide ja kaustade jagamist Interneti kaudu keelamine;
- Pikkade failiteede kasutamine;
- Kasutaja kausta ümbersuunamine;
- Otselink loomine töölaual;
- Mõnede Windowsi rakenduste käivitamise takistamine;
- Irdketaste ja mälupulkade kasutamise keeld;
- Värskenduste hankimine WSUS-i kaudu;
- Arvuti lukustamine tegevusetuse ajal.

Seadete salvestamise näide on toodud lisas 2 olevas tabelis.

1.4 Failiserver

Failiserverid muudavad failide salvestamise, turvamise ja jagamise organisatsioonis lihtsamaks. Failiserverid on häkkerite ja lunavara levinud sihtmärk, seega tuleb erilist tähelepanu pöörata nende kaitsmisele rünnakute eest.

Failiserverid sisaldavad tavaliselt lisafunktsioone, mis võimaldavad mitmel kasutajal neile samaaegselt juurde pääseda.

- Lubade haldust kasutatakse selleks, et määrata, kes pääseb juurde millistele failidele ja kellel on õigused faile redigeerida või kustutada.
- Failide lukustamine takistab mitmel kasutajal sama faili samaaegset redigeerimist.
- Redigeerimisel konfliktide lahendamine säilitab andmete terviklikkuse ka failide ülekirjutamise korral.
- Hajutatud failisüsteem võib muuta andmed üleliigseks ja väga kättesaadavaks, kopeerides need mitmesse serverisse erinevates kohtades. [4]

Kohaliku failiserveri plussid ja miinused

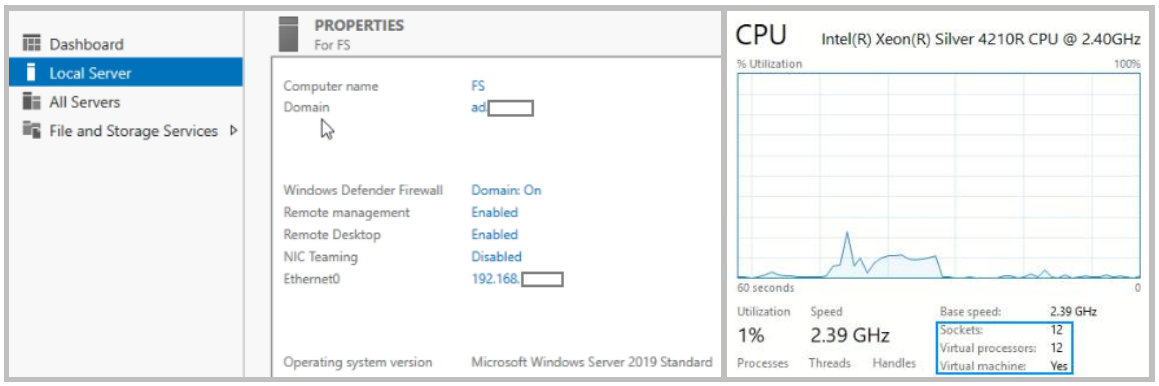
Plussid	Miinused
Suhteliselt madal hind	Nõuab administreerimist
Kergesti rakendatav ja konfigureeritav	Vajab andmekaitset
Suure andmemahu	Sisaldab piiratud metaandmeid
Kiire juurdepääs andmetele	Vaja on planeerida võimsuse laiendamist

Tabel 1.1. Kohaliku failiserveri plussid ja miinused

Failiserveri valimisel tuleb analüüsida, kui suur andmemaht on juba olemas, kuidas andmemaht ketastel tulevikus kasvab, milliste uute programmide jaoks failiserverit hakatakse kasutama. Näiteks meiliserver ja WSUS-i värskendusserver võivad salvestada üsna palju andmeid.

Andmete salvestamise kindluse tagamiseks kasutatakse sageli RAID funktsiooni ja selleks on vaja kahte või enamat identset ketast. Seda tuleb serveri komplekteerimisel arvestada.

Peale SQL tabelite üleviimist vanast serverist paigaldati uues failiserveris VM-ile SAF 7.0 raamatupidamisprogramm koos MS SQL Serveriga.



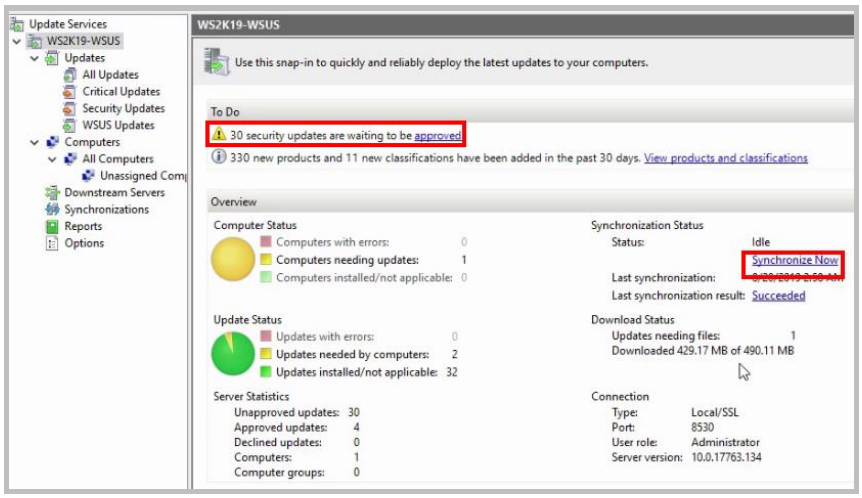
Joonis 1.5. VM Windows Server 2019 FS rolliga

1.5 WSUS-i värskendusserveri konfigureerimine

Windows Server Update Services (WSUS) võimaldab administraatoritel juurutada uusimad Microsofti tootevärskendused. WSUS on Windows Serveri serveri roll ja selle installimisel saate värskendusi tõhusalt hallata ja juurutada.

Süsteemiadministraatorite üks olulisemaid ülesandeid on hoida klient- ja serveriarvuteid värskeimate tarkvarapaikade ja turvavärskendustega kursis. Ilma Windows Serveri värskendusteenusteta (WSUS) oleks värskenduste juurutamist tõesti raske hallata.

Selle asemel, et lasta mitmel arvutil värskendusi otse Internetist alla laadida, on võimalik seadistada WSUS-i serveri ja suunata kliente kõiki värskendusi WSUS-serverist alla laadima. Sellega säästate oma Interneti läbilaskevõime ja kiirendate ka Windowsi värskendusprotsessi. Selle serverirolli installimise protsessi on hästi kirjeldatud ühes paljudest Windows Server 2019 juhenditest (vt link [5]). Vaatamata Interneti läbilaskevõime suurendamisele meie aja, on see funktsioon endiselt väga kasulik, kui ettevõttes on rohkem kui 8-10 arvutit.



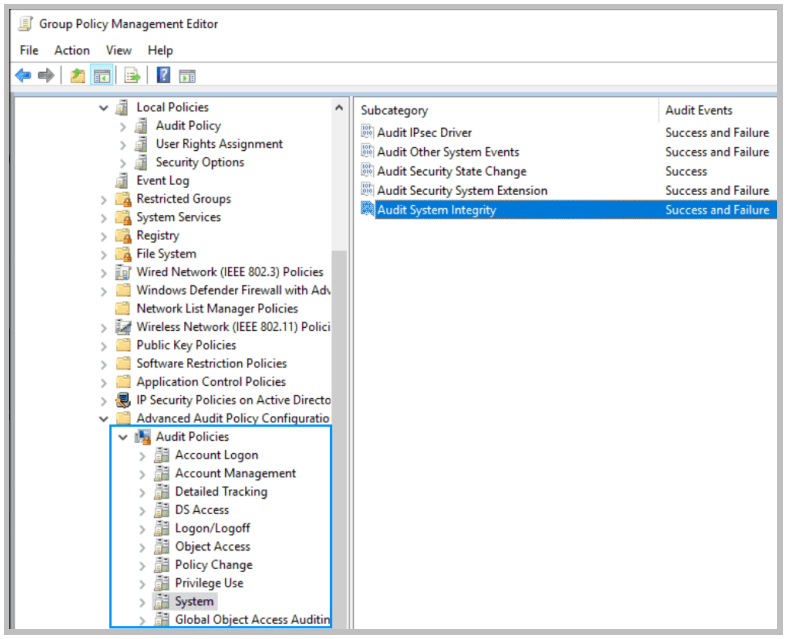
Joonis 1.6. WSUS-i staatus

1.6 Failiserveri audit

Turvaintsidentide avastamisel ja uurimisel on oluline oskus auditeerida sündmusi. Pahatahtliku tegevuse korral aitavad korralikud turvalogid tuvastada tegevust ja selle allika. Ilma logideta ei saa tõenäoliselt kunagi teada, et midagi juhtus, või avastatakse seda siis, kui on liiga hilja.

Näiteks on töötaja, kes kopeerib ettevõtte tundlikke andmeid USB-mälupulgale ja annab need konkurendile, kui toimingut ei logita ega peata andmekao vältimise süsteem (DLP) puudub, siis puudub ka võimalus selle kasutaja tuvastada ning üldse tõestada, et juhtum toimus. Kuid kui on salvestatud õige sündmus koos kasutajanime ja failinimedega, on tulevikus lihtne tõestada kasutaja tegevusi.

Microsoft on aastate jooksul integreerinud Windows Serveri süsteemidesse tõeliselt võimsad auditeerimisvõimalused. Auditeerida on võimalik peaaegu kõike.[6]



Joonis 1.7. Auditi seadistus tehakse MS Windows Serveri GPO-s

Tuleb tähele panna, et nagu alati turvalisuse puhul, peab leidma oma keskkonna jaoks toimiva tasakaalu.

Pärast selle rühmapoliitika rakendamist, kasutajad ei märganud failiserveriga töötamisel kiiruse vähenemist. Kuigi aktiivses igapäevatöös on auditi võimalikku mõju võrgu kiirusele väga raske mõõta.

1.7 Võrgu konfiguratsiooni ja seadmete seadistuste salvestamine

Projekteerimisdokumentatsioonis tuleks kirjeldada kõiki ettevõtte IT-süsteemi komponente, arvutivõrgu konfiguratsiooni, seadmete sätteid. Samuti on seal mugav

salvestada infot arvutikasutajate, gruppide, meilikontode, võrguressurssidele juurdepääsu ja muude oluliste andmete kohta. Kui puudub selleks ettenähtud tarkvara, võib kasutada MS Excelit. Üks võimalikest valikutest on toodud tabelites näitena (vt lisa 2).

1.8 Tõrkekindel klastri loomine

Viimastel aastatel on IT-valdkonnas üha enam kasutatud pilvetehnoloogiaid ja virtuaalmasinaid. Kõige laialdasemalt kasutatavad kõrgtehnoloogilised lahendused, mis põhinevad Microsofti Hyper-V-l ja VMware VSphere'il. Need virtualiseerimissüsteemid loovad seadme jaoks usaldusväärse, skaleeritava ja kiire virtuaalse keskkonna.

Selles lõputöös käsitletakse tõrketaluva virtuaalmasina süsteemi loomist, mis põhineb kaasaegsel ja töökindlal VMware tehnoloogial.

VMware vSphere sisaldab järgmisi komponente:

- VMware ESXi: tüüpi hüperviisor, mis vastutab protsessorite, mälu, salvestusruumi ja muude ressursside koondamise eest mitmesse virtuaalmasinasse (VM)
- VMware vCenter Server on haldustööriist, mis pakub ESXi hostide jaoks ühte klaaspaneeli
- VMware vSphere Client on uus HTML5-põhine haldusliides, mis võimaldab kasutajatel vCenter Serveriga kaugühenduse luua
- VMware Virtual Machine File System (VMFS): suure jõudlusega klastri failisüsteem ESXi VM-ide jaoks
- VMotion: funktsioon, mis võimaldab reaalajas migratsiooni sisselülitatud VM-idele samas andmekeskuses
- Storage vMotion: sarnaselt tavalisele vMotion-ile võimaldab see virtuaalsete ketaste või konfiguratsioonifailide reaalajas migratsiooni uude andmesalve virtuaalse masina töötamise ajal
- VSphere High Availability (HA): see utiliit taaskäivitab ebaõnnestunud VM-id teistes saadaolevates serverites
- VMware Distributed Resource Scheduler (DRS): utiliit, mis jagab ja tasakaalustab dünaamiliselt VM-ide arvutusvõimsust riistvararessursside kogumite vahel

- Storage DRS: sarnaselt VMware DRS-iga tasakaalustab see utiliit dünaamiliselt koormust salvestusmahtu ja sisend- ja väljundvõimsust andmesalvede kogumite lõikes
- Tõrketaluvus: funktsioon, mis loob klastri erinevas hostiserveris valitud töökoormuse duplikaadi, et tagada pidev kättesaadavus.[7]

Klaster on hostide rühm, mis jagavad ressursse ja haldusliidest. Kui lisate klastrisse hosti, muutuvad hosti ressursid osaks klastri ressurssidest. Klaster haldab kõigi selles sisalduvate hostide ressursse.

Klastrid võimaldavad lahendusi vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA) ja vSphere Fault Tolerance (FT) lahendusi.

VMware High Availability (HA-d) kasutatakse sageli töökindluse parandamiseks, seisakuaja vähendamiseks virtuaalsetes keskkondades ja avariitaaste/tegevuse järjepidevuse parandamiseks.

HA võeti kasutusele selleks, et kaitsta hosti tõrgete eest, kuid see põhjustas virtuaalse masina lühikese aja seiskamise, kuni see teises hostis taaskäivitati. Fault Tolerance (FT) viib selle järgmisele tasemele ja garanteerib, et VM töötab hosti rikke ajal, hoides selle teisese koopia teises hostiserveris töötamas. Esmane ja sekundaarne VM jäävad üksteisega sünkroonis, kasutades tehnoloogiat nimega Record/Replay. Salvestamine/taasesitus toimib arvuti täitmise VM-is salvestamise ja selle logifaili salvestamise teel; seejärel võib see võtta selle salvestatud teabe ja taasesitada seda mõnes teises virtuaalses masinas, et saada koopia, mis on algse VM-i duplikaat.[8]

1.8.1 Laboristendi ettevalmistus

Selle töö üks eesmärke on luua juhend virtuaalmasinate tõrkeotsingu klastri ehitamiseks. Üsna keeruliste VMware virtualiseerimistehnoloogiate uurimiseks ja rakendamiseks otsustati ehitada laboristend. Arvutitele ja võrguseadmetele esitatavad nõuded on täidetud. Näiteks virtuaalmasinate migreerimiseks ESXi hostide vahel peavad protsessorid olema sarnased – kõik Intel või kõik AMD, andmeedastusaeg üle arvutivõrgu ei tohiks olla pikem kui 10 ms ja igal arvuti peab olema 3 või rohkem võrguadaptereid. VMware vCenter Server Appliance vajab tööks vähemalt 2 vCPU-d ja 12 GB mälu.

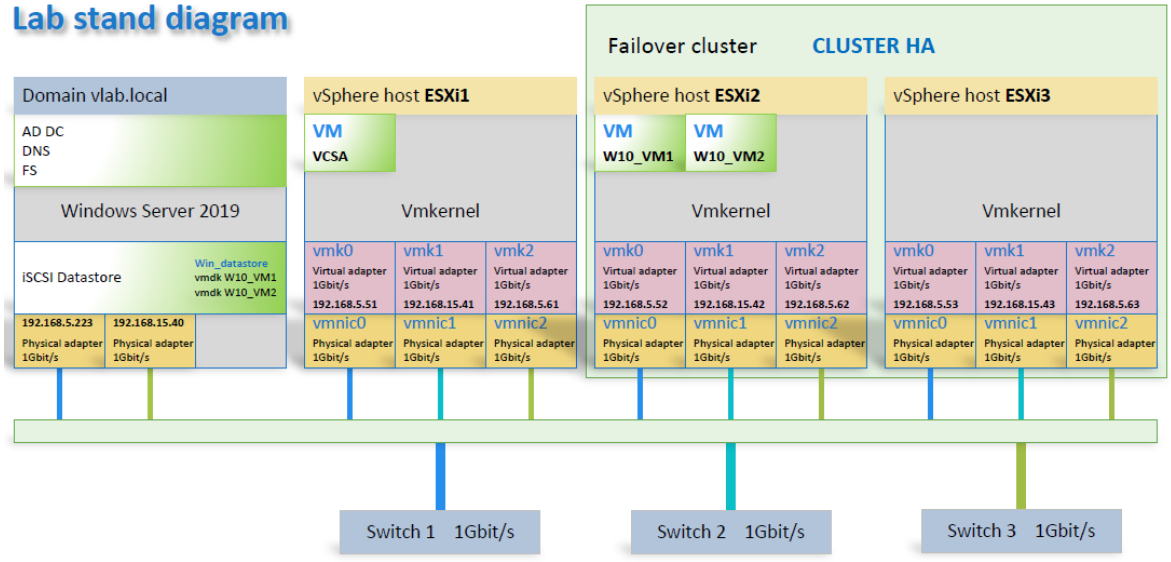
Laboristendil on: 4 arvutit Intel i5 protsessori ja 3 võrguadapteriga, 3 1Gb hallatud kommutaatorit, võrgu NAS ja 3 monitori.

Arvutite funktsioonid:

- AD DC iSCSI kettaga (MS Server 2019);
- ESXi1 – Linux VM vCenter Server Appliance-ga;

- ESXi2 - W10_VM1 ja W10_VM2 virtuaalmasinatega;
- ESXi3 - DRS, HA ja FT-ks.

Joonis 1.9. Laboristend



Joonis 1.10. Laboristendi skeem

1.8.2 Arvutid tõrkekindla klastri jaoks

Tõrkekindel klaster peab tagama SQL-serveriga töötava tarkvara pideva toimimise. Need on: uus tehnoloogiline programm ja pidevalt töötav raamatupidamis tarkvara. 3 füüsilist arvutit tuleb osta virtuaalmasinate tõrkekindla klastri ehitamiseks.

VMware soovitab kasutada serveriklassi arvuteid. Tegelikult piisab ESXi hüperviisori installimiseks suhteliselt uutest tuntava arvutitest "tööjaamade" seeriast. See

tähendab, et neis peab olema serveriklassi emaplaat. Sekretäri või mängu arvuti ei läbi programmi installimisel VMware kontrolli. Peab selgitada, et igale neist tuleb lisada kolme või enama pordiga võrgukaardid.

SQL-serveri puhul ei pea teatavasti kasutama MS Server 2019 või 2022. See töötab hästi W10 või W11-s.

Domeeniga liitumiseks on soovitatav osta Windows Pro litsentsiga arvutid. Näiteks Dell Vostro 3910 i5-12400 Midi Tower või HP ProDesk 400 G7 i5-10500 Micro Tower (vt. tabel L1.1).

1.8.3 VMware tarkvara valimine

VMware virtuaalmasinate tõrkesiirdeklastri loomiseks soovitab autor osta tarkvarapaketi VMware vSphere Standard. See valik sisaldab kõiki vajalikke funktsioone.[9]

Business continuity

Product features	VMware vSphere Standard	VMware vSphere Enterprise Plus	VMware vSphere with VMware Tanzu[1]	VMware vSphere+
vSphere Hypervisor Provides a robust, production-proven, high-performance virtualization layer.	✓	✓	✓	✓
vMotion Enables live migration of virtual machines with no disruption to users or loss of service, eliminating the need to schedule application downtime for planned server maintenance. The recent enhancements in vMotion logic provides non-disruptive operations, irrespective of the size of VMs, specifically for large and mission critical workloads.	✓	✓	✓	✓
vCenter® Hybrid Linked Mode Enables unified visibility and management across on-premises vCenter and vCenter on a vSphere enabled cloud such as VMware Cloud on AWS.	Requires vCenter Server STD	Requires vCenter Server STD	Requires vCenter Server STD	✓
vSMP Virtual symmetric multiprocessing (SMP) enables virtual machines to have multiple virtual CPUs.	✓	✓	✓	✓
High Availability (HA) Automatically restarts your VMs following physical machine failure.	✓	✓	✓	✓
Storage vMotion Avoids application downtime for planned storage maintenance by migrating live virtual machine disk files across storage arrays.	✓	✓	✓	✓
Fault Tolerance Provides continuous availability of any application in the event of a hardware failure — with no data loss or downtime. For workloads up to 4-vCPU.	2-vCPU	8-vCPU	8-vCPU	8-vCPU
vShield Endpoint™ Secures virtual machines with offloaded anti-virus and anti-malware solutions, without the need for agents inside the virtual machine.	✓	✓	✓	✓

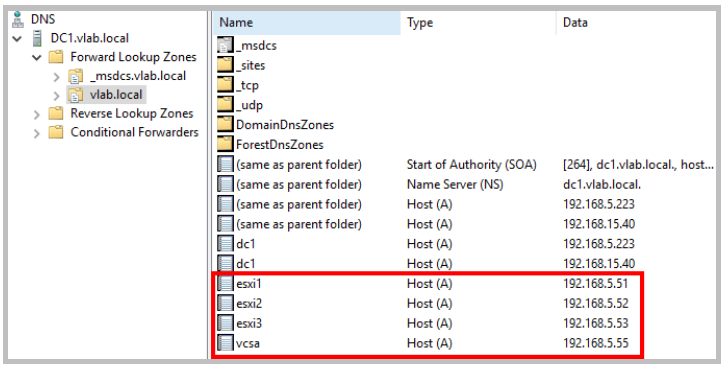
Tabel 1.2. Vajalikud funktsioonid sisalduvad VMware Standardis

1.8.4 Tarkvara installimine

MS Server 2019 installiti ühte arvutisse DC, DNS, FS ja iSCSI serveri rollidega.

Peale VMware.com veebilehel registreerumist ja tarkvara ostmist saab sealt ka vajalikud komponendid alla laadida ja VMware serveritesse installida. Paigaldamine toimub tavapäraselt – järgige paigaldaja juhiseid. Stendi jaoks kasutati vSphere'i ja vMotioni prooviversiooni.[10]

Süsteem ESXi vSphere Hypervisor ja vMotion plugin oli installitud standardrežiimis igale kolmele hostile mälupulgalt. Laboristendis – ESXi1, ESXi2 ja ESXi3-le. Kõik haldusvõrgus (Management Network) olevad võrguadapterid on saadud staatilised aadressid võrgust 192.168.5.0/24. Kõik kolm ESX-i hosti olid ühendatud uue *vlab.local* domeeniga ja oli täiendavalt eraldi käsitsi lisama ESXi1, ESXi2 ja ESXi3 DNS-serveri A-tsooni.



Joonis 1.11. VM-ide lisamine käsitsi

Pärast seda oli paigaldatud väga oluline tarkvara komponent – eelkonfigureeritud Linuxi versioon, mida nimetatakse vCenter Server Appliance-ks (VCSA) ainult ESXi1 hostile. vCenter Server on vajalik mõne vSphere'i täiustatud funktsiooni jaoks, nagu vSphere High Availability, vSphere Fault Tolerance ja vSphere vMotion.

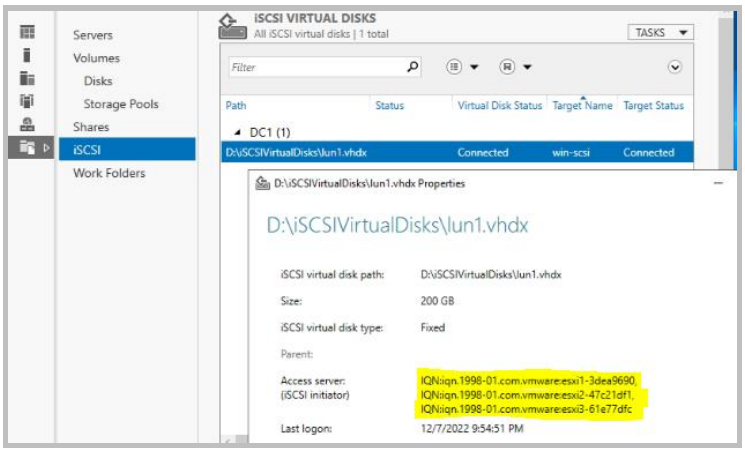
VCenter Server koosneb järgmistest komponentidest:

- vSphere Web Clienti saab kasutada teie vCenter Serveri haldamiseks.
- vCenter Serveri andmebaas – talletab laoartiklid, turberollid, ressursside kogumid, jõudlusandmed ja muu teave.
- vCenter Single Sign-On (SSO) – võimaldab autentida mitme kasutaja hoidla, näiteks Active Directory kaudu.
- Hallatud hostid – ESXi hostid ja nende vastavad virtuaalmasinad.

Tuleb meeles pidada, et selle serveri installimise ajal peate sisestama salasõna, mis aegub 90 päeva pärast. Pärast installimist tuleb selle VCSA-serveri seadetes muuta salasõna aegumiskuupäev *piiramatuks*. Vastasel juhul tekib probleeme lisaprogrammide installimise ja konfiguratsiooni muutmisega.

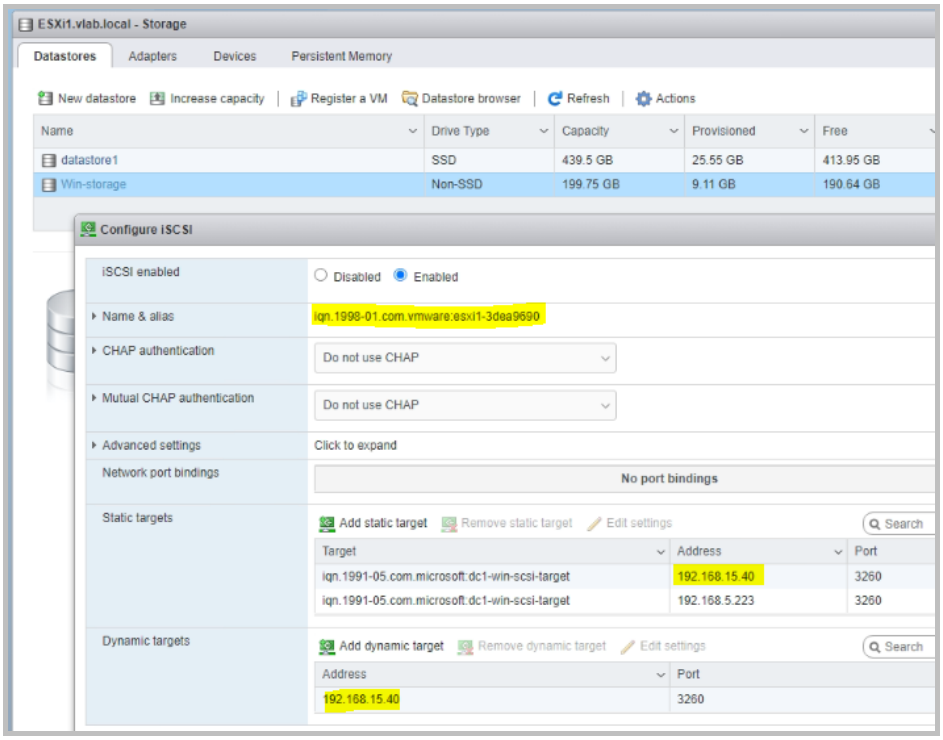
1.8.5 Uue datastore iSCSI loomine

Jagatud andmete salvestamiseks ja tõrketaluvate tehnoloogiatega töötamiseks on soovitatav kasutada välist datastore. Sellesse stendi installiti Windows Server 2019 Target iSCSI andmesalvestusfunktsioon. Kõik kolm ESXi-i hosti määrati algatajateks.



Joonis 1.12. Selle Windowsi Serveri *Target disk* jaoks on registreeritud 3 hosti ESXi-id

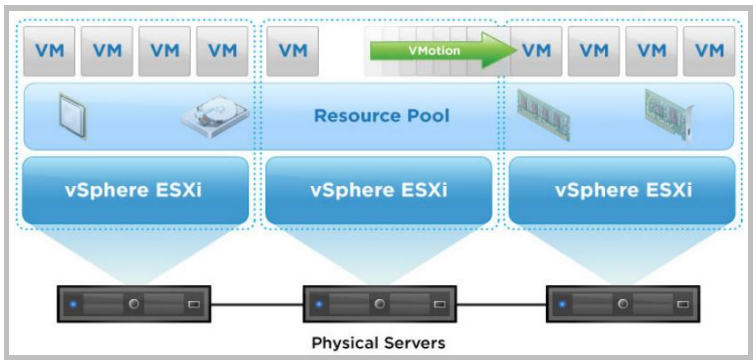
Nende IP-aadressid on juba teada ja nende iSCSI ID-d genereeritakse hostides, kui lisatakse uus datastore iSCSI. Eraldi tuleb märkida, et andmete vahetamiseks iSCSI-kettaga kasutatakse eraldi võrku 192.168.15.0/24, millel on oma kommutaator. Liikluse eraldamine virtuaalmasinate ja võrgu iSCSI-kettaga vahel tagab töökindluse ja suure andmeedastuskiiruse.[11]



Joonis 1.13. iSCSI ühenduse parameetrid: ID, serveri IP-aadressid virtuaalmasina võrgus (192.168.5.223) ja iSCSI võrgus (192.168.15.40)

1.8.6 vMotion-i konfigureerimine

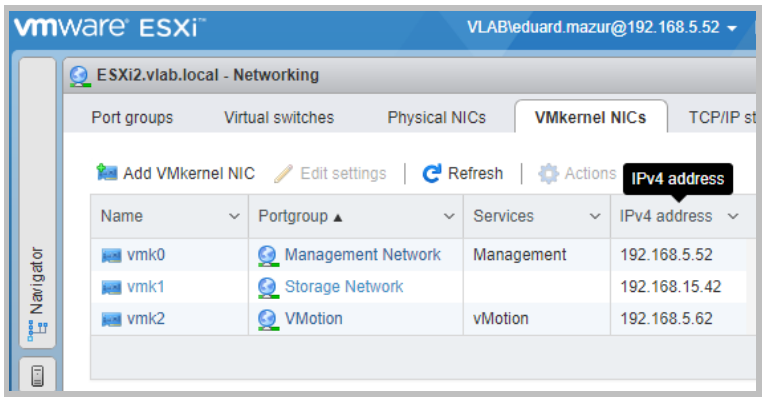
VMware täiustatud funktsioonide töötamiseks ja virtuaalmasinate hostide vahel migreerimiseks peab installima vMotion-i komponendi. Näiteks peab tegema tööd füüsilise ESXi serveriga hoolduseks.



Joonis 1.14. vMotion-i skeem

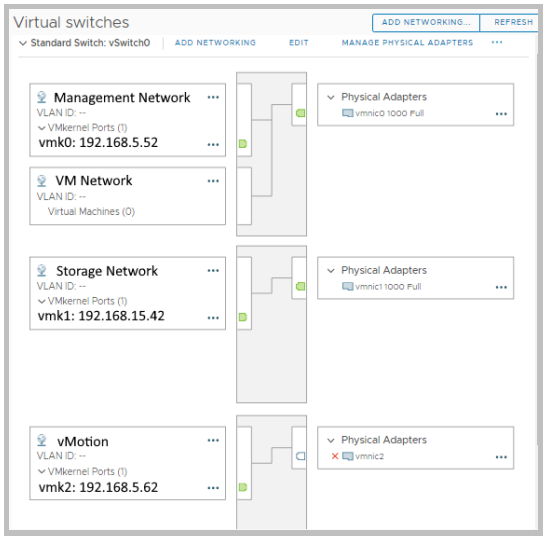
Selle teenuse toimimiseks peab lisama VMkerneli virtuaalse võrguadapteri ja määrama sellele eraldi IP-aadressi.

Siis on igal hostil 3 adapterit. Selles näites - vmk0, vmk1 ja vmk2.



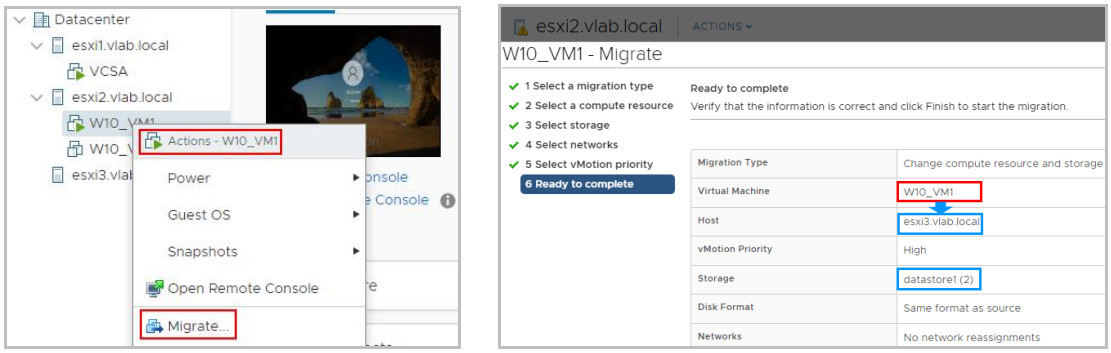
Joonis 1.15. Võrgukonfiguratsioon

Samuti on vaja luua täiendavaid virtuaalseid kommutaatori haldusvõrke ja virtuaalmasina võrke, iSCSI võrku ühendamiseks läbi eraldi füüsilise kommutaatori ning migratsioonivõrgude jaoks.



Joonis 1.16. 3 füüsilised võrguadapterid ja 4 virtuaalkommutaatorid

Migreerimisfunktsiooni testimiseks migreeriti virtuaalmasin *W10_VM1* hostist *esxi2* hostile *esxi3*. Valiti täielik migratsioonirežiim – nii virtuaalmasina enda (vmdk) ressursid kui ka failid. Tuleb meeles pidada, et selliste tõsiste režiimide kasutamiseks peab failistruktuur olema staatiline – *Thick provisioning* . See tähendab, et vmdk-faili suurus ei muutu. Migratsiooniprotsessi alustamiseks peab kasutama vCenter-st. Web vSphere Client-i abil valiti soovitud virtuaalmasina menüüst üksus *Migrate* ning seadistati migratsiooniparameetrid mida, kuhu ja kuidas migreerida.

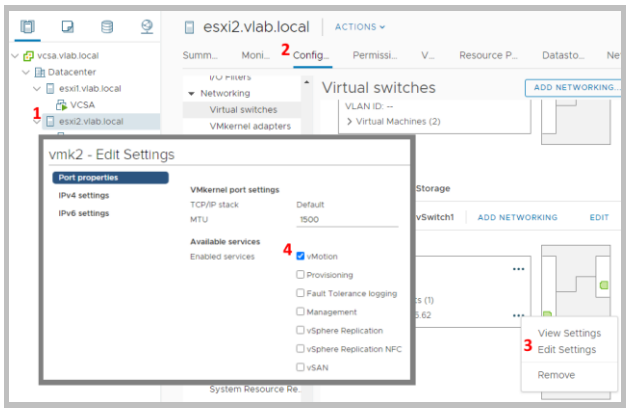


Joonis 1.17. Kõik on *W10_VM1* migratsiooniks valmis

Sellise toimingu kestus sõltub eelkõige virtuaalmasina suurusest, kettasüsteemi ja arvutivõrgu kiirusest. Selles näites kulus selleks 22 minutit.

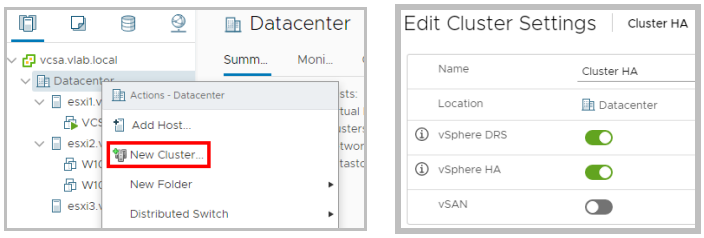
1.8.7 ESXi-i klastri loomine

Funktsioonide DRS, HA ja FT kasutamiseks vajab ESXi serverite klastrit. Kõigi serverite arvutusvõimsus on ühendatud loogiliseks kogumiks. Kõigepealt peab VM-i migratsioonifunktsioonidele seotud virtuaalse kommutaatori sätetes lubama service vMotion.



Joonis 1.18. vMotion on lubatud

Järgmise sammuna tuleb luua uus klaster *Cluster HA*, lisada hostid *ESXi2* ja *ESXi3*, samuti VM-id *W10_VM1* ja *W10_VM2*.

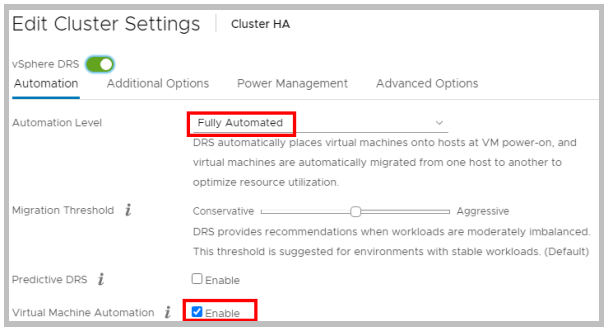


Joonis 1.19. Klaster loodud

Sel juhul tuleb failid üle kanda iSCSI datastore-sse *Win_storage*. On vaja *Change storage only*-režiimis funktsiooni *Migrate*. Kui kuvatakse viga "Disk 2000 is not moving…", peab VM-i atribuutides valima CD/DVD – *Client Device*.

1.8.8 Distributed Resource Scheduler (DRS)

Pärast klastri loomist sai kättesaadavaks funktsioon "Distributed Resource Scheduler™" (DRS). Aeg-ajalt võivad VM-ide töökoormused muutuda ja paljude muutuva töökoormusega VM-ide puhul võib klastris esineda tasakaalustamatust. DRS lahendab need probleemid, jälgides vaikimisi klastri tasakaalu olekut iga viie minuti järel. DRS määrab automaatselt kindlaks, millistele virtuaalsetele masinatele teisele hostile kolimisest kasu oleks, ja reaalajas migreerib VM-i vMotioni abil uude hosti. Nii tagab DRS igale klastri virtuaalsele masinale vajalikud hostressursid (nt mälu ja protsessor).

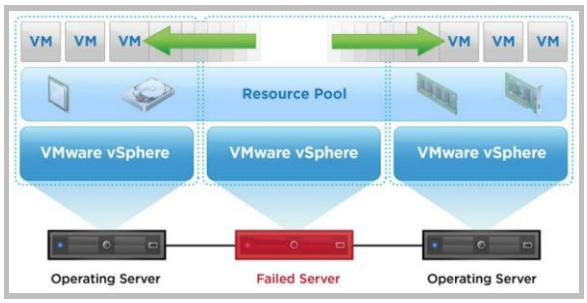


Joonis 1.20. DRS-i funktsiooni seadistus

Režiimis *Manual* pakub süsteem VM-i üleviimist teise hosti. *Migration Treshold* reguleerimisega määrake mälu ja protsessori koormuse väärtus, mille ületamine põhjustab virtuaalse masina migreerumise teise ESXi-serverisse. Kuna praeguses renoveerimisprojektis peaks klastri jaoks kasutama üsna võimsaid arvuteid, siis DRS-funktsiooni ei kasutata.

1.8.9 VMware vSphere High Availability (HA)

vSphere HA pakub virtuaalsete masinate jaoks kõrget kättesaadavust, koondades virtuaalsed masinad ja nendes asuvad hostid klastrisse. Klastris olevaid hoste jälgitakse ja tõrke korral taaskäivitatakse ebaõnnestunud hostis olevad virtuaalmasinad alternatiivsetel hostidel.[12] See on kaitse põhitase.

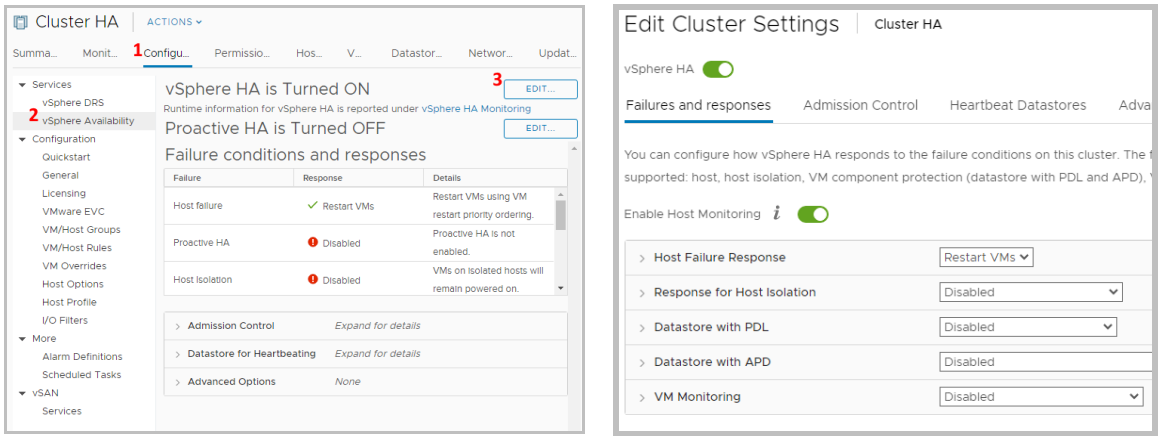


Joonis 1.21. High Availability (HA) klasterdiagramm toimivas stendis

Tegelikult on virtuaalmasina keskkonnas tõrgete ilmnemiseks viis võimalust: ESXi-serveris (hostis), rakendustes, VM operatsioonisüsteemis, datastores või arvutivõrgus.

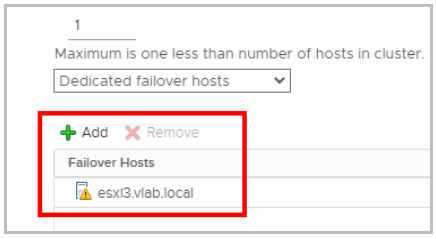
- HA funktsiooni kasutatakse sageli plaanilise hostihoolduse puhul. VM taaskäivitatakse teises klastri hostis, kuid side võrguteenustega, andmebaasi tehingud ja muud andmevahetus katkeb. HA teeb *Haldusvõrku* pingi abil enesediagnostikat – kas see on hosti probleem või see töötab, aga on võrgust isoleeritud.
- Külalisoperatsioonisüsteemi (nt Windows) probleemide korral määrab HA probleemi VM-i installitud *VMTools* jaoks spetsiaalsete teadete abil. Pärast seda taaskäivitatakse VM samas hostis.
- Kui VM-i komponendikaitseprogramm (VMCP) on installitud, saab kontrollida datastore saadavust (vt joonis 1.18). Näiteks seadetes on VM-iga seotud probleemile reageerimiseks konservatiivne valik – HA otsib probleemse VM-i jaoks saadaolevaid ressursse teistes hostides. Kui leiab, siis käivitab seal VM-i, kui ei leia, siis ei käivita. Agressiivses režiimis proovib HA niikuinii käivitada VM-i teises hostis.

Seega seadistatakse *vSphere Availability* menüüs toimingud probleemide korral.



Joonis 1.22. vSphere Availability seaded

Menüüs *Admission Control* on vaikimisi valitud *Cluster resource Persentage*. Siin saab määrata, kui palju protsessori- ja mäluressursse tõrkekindelklastri loomiseks reserveerida. Laboristendi jaoks valiti aga viimane variant – spetsiaalne tõrketaluvusega host (*Dedicated failover hosts)*: *ESXi3* server.

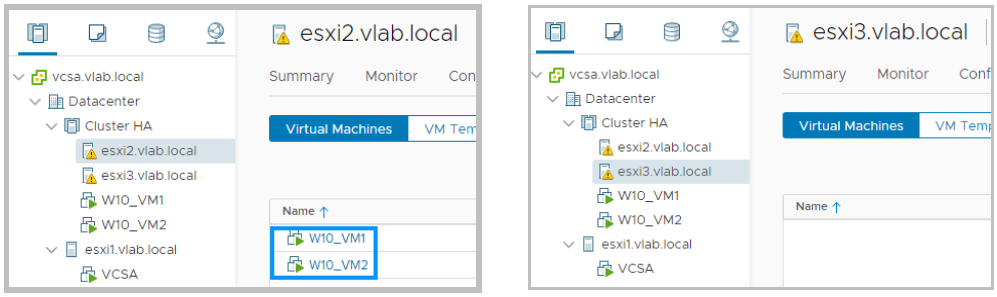


Joonis 1.23. *Dedicated failover host* on lisatud

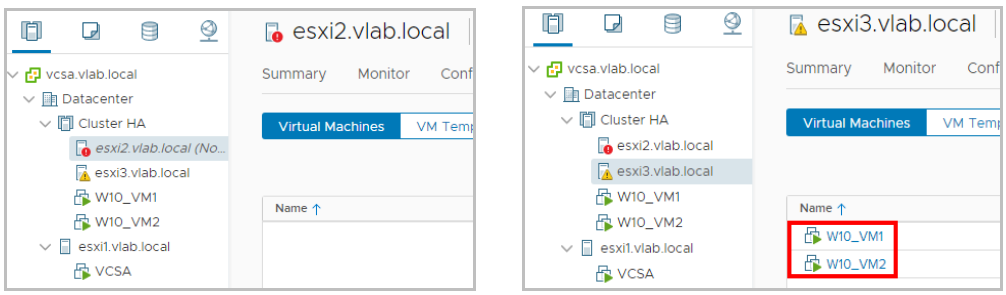
Väga oluline on tagada *Haldusvõrku* toimimist, et selle signaalid jõuaksid alati hostidele. Selleks peab oma IP-aadressiga looma teine *Virtuaalne kommutaator* ja lisama sellele *Haldusvõrk*. *ESXi2* ja *ESXi3* hostidel asuvas laboristendis loodi vmk2 *Virtuaalne kommutaator* ja lisati *Haldusvõrku* funktsioon. Ühe virtuaalse võrguga seotud probleemide korral saab alamhost suhelda põhihostiga ja uurida ressursside saadavust.

Kui klastri konfigureerimine on lõpule viidud, tuleb selle kontekstimenüüs iga klastri virtuaalse masina jaoks käivitama käsku *Reconfigure for vSphere HA*.

Nüüd kontrollime HA funktsiooni tööd – ***taaskäivitada ESXi2*** serveri kahe VM-iga.



Joonis 1.24. Serverite seisukord klastris ***enne*** testimist



Joonis 1.25. Serverite seisukord klastris ***pärast*** testimist

See migratsiooniprotsess võttis aega umbes kolm minutit – põhimõtteliselt kulus aega Windowsi käivitamiseks VM-idel.

Testi tulemus kinnitab vSphere High Availability (HA) funktsiooni edukat toimimist.

1.8.10 VMware vSphere Fault Tolerance (FT)

VMware vSphere Fault Tolerance (FT) pakub rakendustele pidevat kättesaadavust, luues virtuaalmasina reaalajas varieksemplari, mis peegeldab esmast virtuaalmasinat. Riistvara rike korral käivitab vSphere FT automaatselt tõrkesiirde, et kõrvaldada seisakud ja vältida andmete kadumist. Pärast tõrkesiiret loob vSphere FT automaatselt uue sekundaarse virtuaalmasina, et pakkuda rakendusele pidevat kaitset.[13]

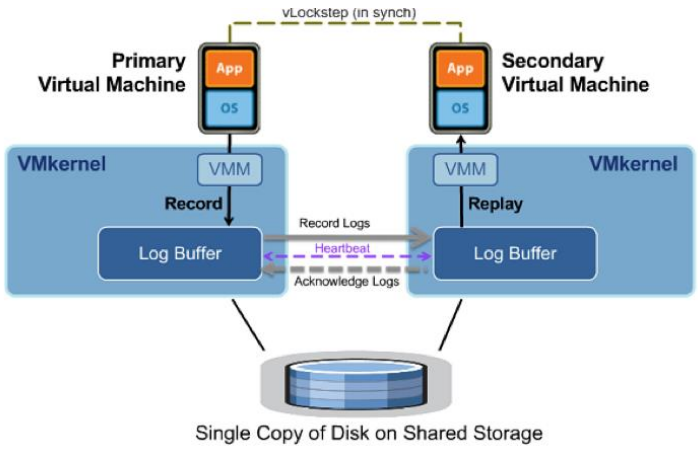
VMware vSphere Fault Tolerance toetab virtuaalmasinaid, mis on konfigureeritud mitte rohkem kui 4 vCPU ja 64 GB muutmäluga, maksimaalselt 4 tõrketaluvusega virtuaalmasinat, mis töötavad ühes ESXi hostis.

Nii esmasel kui ka sekundaarsel virtuaalmasinal on oma virtuaalmasinafailide komplekt (sh VMX- ja VMDK-failid), mida hoitakse sünkroonis.

Lisaks virtuaalmasina failidele on veel kaks faili, mida peetakse oluliseks VMware vSphere Fault Tolerance`i töötamisel, st *share.vmft*, mida tuntakse ka metaandmete failina, mis vastutab UUID-i säilitamise eest nii esmasel kui ka sekundaarsel failil ning *.ftgeneration* vastutab vältides jagatud aju stsenaariumi, mis võib ilmneda hosti isoleerimisel, tagab *.ftgeneration* **ainult üks** virtuaalmasin (esmane/sekundaarne) saab lugeda ja kirjutada virtuaalmasina ketastele.

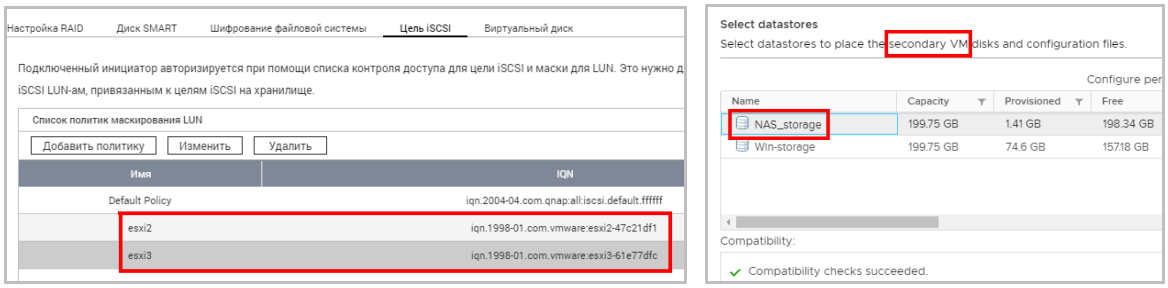
Kui on lubatud virtuaalmasinas VMware vSphere'i Fault Tolerance`i, toimub esmane täielik sünkroonimine kahe VMDK-faili vahel VMware Storage vMotioni abil, tagades, et esmasel ja teisesel virtuaalmasinal on täpselt sama ketta olek.

Kui esialgne täielik sünkroonimine on tehtud, hakkab VMware vSphere Fault Tolerance peegeldama VMDK kirjutamistoiminguid primaarse ja sekundaarse vahel FT logimisvõrgu kaudu, et tagada koopiate identne salvestamine.



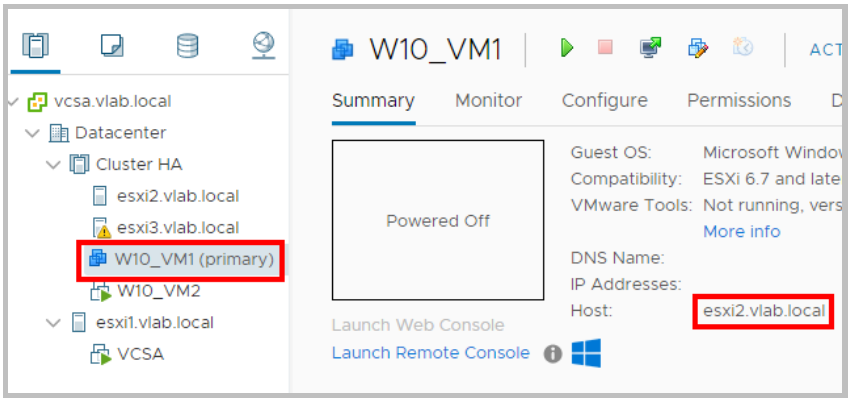
Joonis 1.26. Fault Tolerance (FT) klasterdiagramm. Teine masin saab kõik andmed esimeselt ja on passiivses sünkroonimisrežiimis

Veataluvuse funktsiooni lubamine toimub valitud virtuaalmasina kontekstimenüüs. Seejärel peab määrama primaarse ja teisese VM-i sünkroonimisfailide asukoha, samuti selle, millisesse andmesalve primaarse masina koopia luuakse. Süsteem nõuab, et esmase ja teisese maailma masinate wmdk-failid asuksid erinevates füüsilistes seadmetes. Seetõttu tuli laboristendile lisada teine datastore iSCSI. Selleks kasutati tuntud tootja QNAP NAS-i.



Joonis 1.27. Teisese VM-i (klooni) põhifailide salvestamiseks määrab uue datastore iSCSI NAS_storage

Pärast teisese VM-i ettevalmistamist teises hostis on süsteem sünkrooninud virtuaalse masina praeguse oleku, mille olek on nüüd kaitstud. Nüüd saab selle VM-i käivitada. Sellel puhul asub esmane VM ESXi2 hostis ja sekundaarne VM ESXi3 hostis.



Joonis 1.28. Fault Tolerance klastri funktsiooni ettevalmistamine on lõpetatud

Kontrollimiseks taaskäivitati esmane VM. Kaitstud W10_VM1 töö ei katkenud. Teisesele VM-ile ülemineku ajal läks kaduma vaid 2 pingi paketi.

Loomulikult on see virtuaalmasina tõrkekindla klastri kõige huvitavam funktsioon. Aga ka kõige nõudlikum. Kõik komponendid peavad olema dubleeritud: võrguadapterid, kommutaatorid, sünkroonimisfailide datastore ja virtuaalmasin ise. Lisaks on väga oluline kasutada kaasaegseid komponente. Näiteks kasutati selles protsessis NAS-i suurte ketastega, kuid väikese kiirusega (mitte SSD-ga).

2 RUUTERI FUNKTSIOONID

Kaasaegse võrguandmetöötluse põhiline tööriist on ruuter, mis töötab nii kohalike kui ka Interneti võrkudega, kus toimub peaaegu iga oluline äritegevus. Ilma ruuteriteta ei saaks Internetti kasutada koostööks, suhtlemiseks ega teabe kogumiseks ja õppimiseks.

Turvalisust võivad tagada ka ruuterid. Sisseehitatud tulemüür ja sisu filtreerimise tarkvara pakuvad täiendavat kaitset soovimatu sisu ja pahatahtlike veebisaitide eest, ilma et see mõjutaks teie võrgukogemust.

Ruuter pole siiski mõeldud ainult andmeedastuseks või Interneti-ühenduste loomiseks.

Väikeettevõtete jaoks ja piiratud eelarvega saab ruutereid edukalt kasutada kohaliku võrgu väiksemateks võrkudeks jagamiseks - VLAN-ide korraldamiseks.

LAN-keskkonnas jagavad VLAN-id leviedomeene. Kui ühes VLAN-is olev host peab suhtlema teise VLAN-i hostiga, tuleb liiklus nende vahel suunata.

Kõrgete võrgukoormuste korral on soovitatav kasutada selleks otstarbeks suure jõudlusega kolmanda kihi kommutaatorite või tulemüüre. Fakt on see, et sildistatud liikluse töötlemine võtab teatud aja ja sellega saavad paremini hakkama spetsiaalsed kiibid, mis on integreeritud sellistesse tõhusatesse võrguseadmetesse.

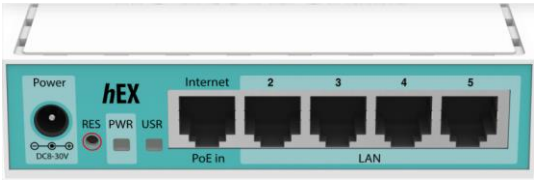
Aga kolmanda kihi kommutaatorite hind on üsna suur. Seejuures ei ole väiksematel ettevõtetel tavaliselt suurt võrgukoormust. Ja võrgu fragmenteerumise funktsiooni võib täita suhteliselt odav ruuter.

Kuna antud töös on kasutusel tööprojekt olemasoleva võrgu kaasajastamiseks, siis oli üheks oluliseks tehnilise töö punktiks odavate komponentide kasutamine, tingimusel, et tagatakse vajalik kaitsetase ja funktsionaalsus.

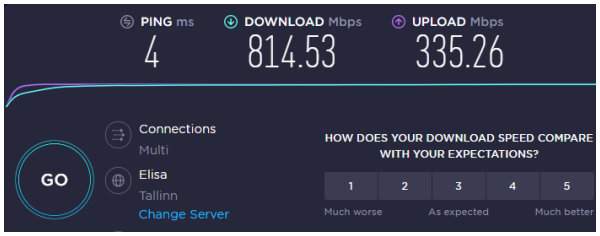
2.1 VPN ruuteri spetsifikatsioonid

Objektil on juba mitu aastat töötanud väga soodne, kuid üsna tõhus VPN ruuter MikroTik RB750Gr3 võimsa RouterOS-iga. See mudel on erakordselt tugev variant hinnaga 65 eurot. Sellel on kahetuumaline 880 MHz protsessor, 256 MB muutmälu ja 16 GB välkmälu, mida saab laiendada microSD-kaardi pesa kaudu, mida saab kasutada võrgutuvastusutiliidi Dude jaoks.

Selge eelis Mikrotik hEX RB750Gr3 on selle haldustööriistad. Näiteks saab selle haldamiseks koos teiste Mikrotiku seadmetega kasutada Windows WinBoxi utiliiti.



Joonis 2.1. VPN-i ruuter MikroTik RB750Gr3



Joonis 2.2. Speedtest ruuteriga RB750Gr3

Selle odava ruuteri kiirusest piisab 50-70 kasutaja kontoritööks. Praktikas töötas selline ruuter edukalt kontoris, kus oli L2TP VPN-i kaudu korraga 65 kohalikku ja 25 kaugarvutit, üsna hea kiirusega. (vt joonis 2.2).

2.2 Tulemüüri seadistamine

IT-infoturbe tagamine, eriti pärast kaugtöö massilist kasutuselevõttu, on muutunud ettevõtluse oluliseks atribuudiks. Tõepoolest, küberkuritegevuse juhtumid on viimastel aastatel sagenenud. Ründajad kasutavad infoturbe auke, et varastada ettevõtete konfidentsiaalseid andmeid või kuidagi kahjustada nende tegevust. Tavaliselt juhtub see väljapressimise eesmärgil.

Tõrjumata küberrünnak või loomulik küberoht (nt inimlik eksitus, litsentsimata tarkvara) toob kaasa maine- ja rahalise kahju. Mõnel juhul viivad küberrünnakud isegi ettevõtte sulgemiseni. Seetõttu investeerivad maailmatasemel kaubamärgid küberturvalisusesse miljardeid dollareid, sest ebapiisav küberturvalisus põhjustab rohkem kahju.

Traditsiooniliselt vastutab tulemüür välispiiride turvamise ning ettevõttesisese stabiilse, tõrketaluvuse ja tõhusa töö tagamise eest. Kaasaegsete turvastandardite järgi loodud süsteem ei saa mitte ainult ära hoida häkkereid, viirusi ega vähendada DDoS-i rünnakutest tulenevaid kadusid, vaid ka suurendada võrgu jõudlust, tasakaalustada kohalike võrgusegmentide koormust ja oluliselt vähendada olulise teabe varastamise võimalust.

Viimastel aastatel on koroonaviiruse pandeemia tõttu kaugtööliste arv hüppeliselt kasvanud. See suundumus kasvab pidevalt, kuigi nagu igal teisel kaasaegsel inimtegevuse korraldusel, on sellel positiivseid ja negatiivseid külgi. Näiteks haridusvaldkonnas on hariduse kvaliteet märgatavalt langemas ning ettevõtte

töötajate töö efektiivsus sisemiste ressurssidega kaugühendusel on pidevalt kahtluse all. Kuid pikaajaliste piirangute kontekstis ei saa seda võimalust üle hinnata.

Hästi valitud ja hästi konfigureeritud tulemüürid aitavad ära hoida ründeid IT-ressursside vastu, pakuvad ettevõtte töötajatele turvalist juurdepääsu välisvõrkudele ja volitatud kaugkasutajatele ettevõtte ressurssidele.

Varasema põlvkonna tulemüürid, mis blokeerisid ainult võrgupordid ning IP- ja MAC-aadressid, asendatakse uuemate süsteemidega, millel on rakenduste tasemel turvafunktsioonid, kus praegu toimub enamik ründeid.

2.2.1 Kaitsetasemed ja -objektid

Selles töös käsitletakse üksikasjalikult välisohtude eest kaitsmise meetodeid MikroTik ruuterite operatsioonisüsteemi RouterOS näitel. Sellel süsteemil on palju funktsioone ja peenhäälestust, kuid algajale spetsialistile, kellel pole üksikasjalikku juhendit, võib see tunduda keeruline.[14]

Ruuteri turvalisus		
Kaitse L2	**Kaitse L3/L4**	**Kaitse - teised**
1.Pub/Local interface 2.MAC-Address 3.MAC-Telnet 4.MAC-Winbox 5.RoMon 6.ARP-tables 7.Use VLANs for management	1.Pub/Local networks list 2.Neighbor list 3.Trusted address list 4.Firewall 5.Port change 6.NO simple port mapping	1.Strong password 2.Encrypted communication 3.Routing protocol proper config 4.SNMP ACLs and communities 5.L7 filters 6.Log analyze

Tabel 2.1. Kaitsetasemed

2.2.2 Turvalisus L2 ja MAC

1. Peida marsruutimisseadme tüüp
2. Peida hankijapõhine teave. Mudel, püsivara versioon, tootmiskuupäev jne.
3. Peida tarkvara teave: OS-i versioon, järgu number, töötavate teenuste ja rakenduste versioonid.

MAC-aadress sisaldab teavet tuntud tootja seadmete kohta. Seda on vaja muuta. Peab olema ettevaatlik, et vältida MAC-aadresside konflikti!

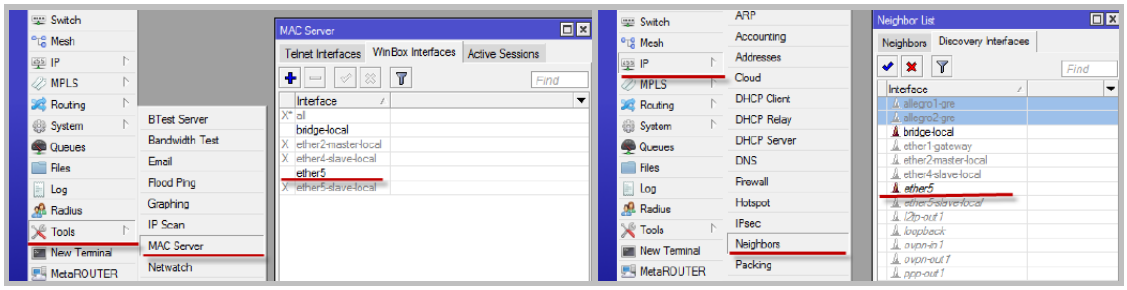
/interface ethernet set ether1 mac-address=0a:0b:0c:0d:0e:0f.

Alustuseks peab keelama juurdepääsu igast küljest. Luba ainult Winboxi.

```
Then, in order to improve safety, we disable all unused services, leave only Winbox:
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
```

Joonis 2.3. Vajadus vältida tarbetu juurdepääsu ruuterile

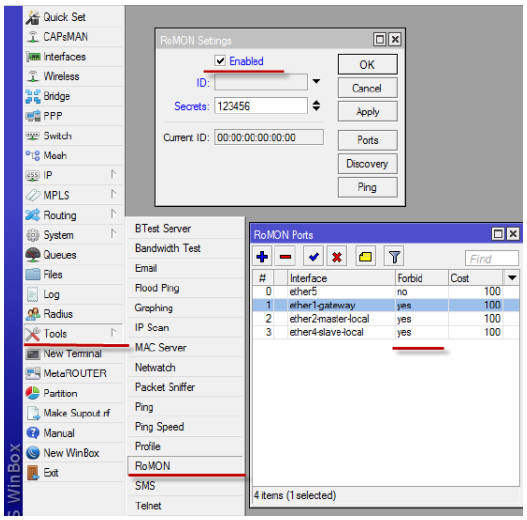
Vaikimisi on Discovery igal uuel liidesel SEES:



Joonis 2.4. MAC-services ja Discovery-services

Neighbor service levitab infot - teave seadme mudeli, operatsioonisüsteemi versiooni, MAC- ja IP-aadresside ja UpTime, IPv6 saadavuse kohta.

Peab lülitama RoMoni teenus välistel liidestel välja:



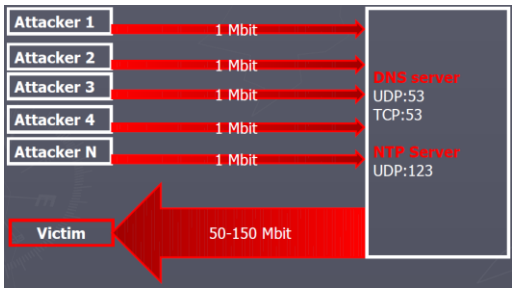
Joonis 2.5. RoMON service töötab. On vaja lülitada seda välja

2.2.3 Turvalisus L3. Võrguressursid

- Peab veenduma, et väliste liideste kaudu ei pääse sild usaldusväärsete haldusliidestele (haldusvõrk).
- Peab kontrollima tulemüüri seadeid, et nad ei piira liiklust haldusvõrgus.

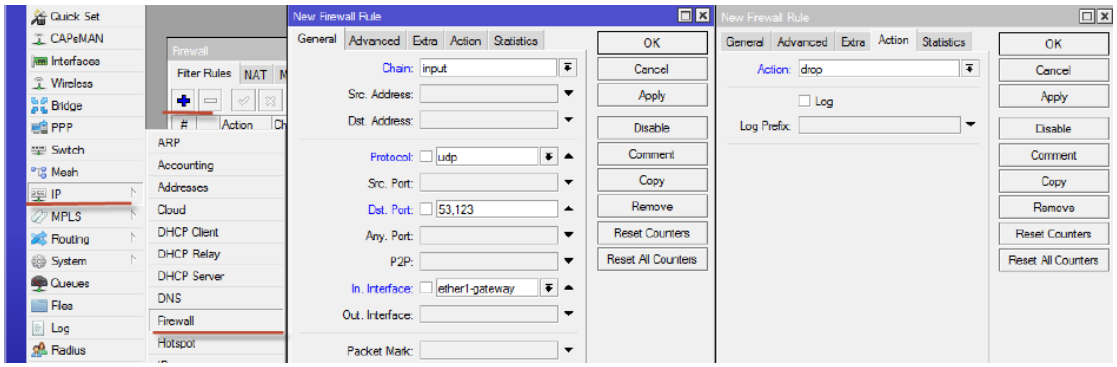
2.2.3.1 UDP-uputusrünnaku kaitse

1. Kurjategija saadab UDP päringu ohvri SRC IP-aadressiga
2. DNS/NTP server vastab suure UDP paketiga ohver
3. Ohver langeb DDoS rünnaku alla suure UDP paketid MikroTik serverist, pordist 53 või 123



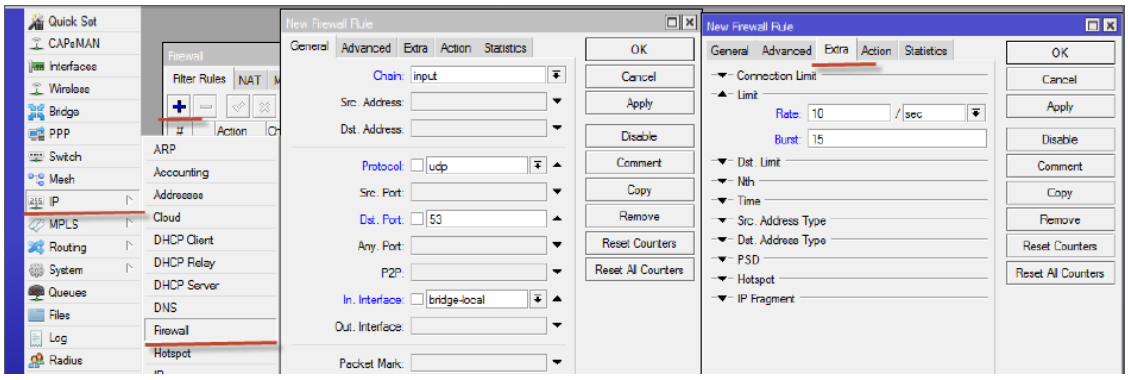
Joonis 2.6. UDP-uputusrünnak

Lahendus: sulgemine Internetist pordid 123 udp, 53 tcp ja udp:



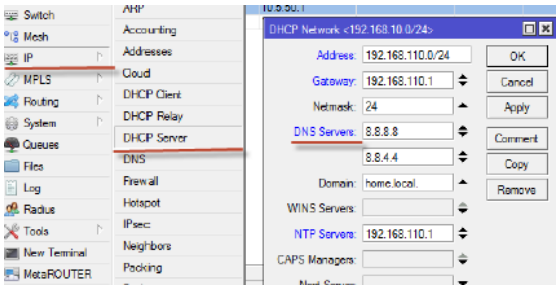
Joonis 2.7. Peab pordid 123 udp, 53 tcp ja udp sulgema

Samuti piirata liiklust udp:53 udp:123 tulemüüriga:



Joonis 2.8. On vaja piirata liiklust udp:53 udp:123 tulemüüriga

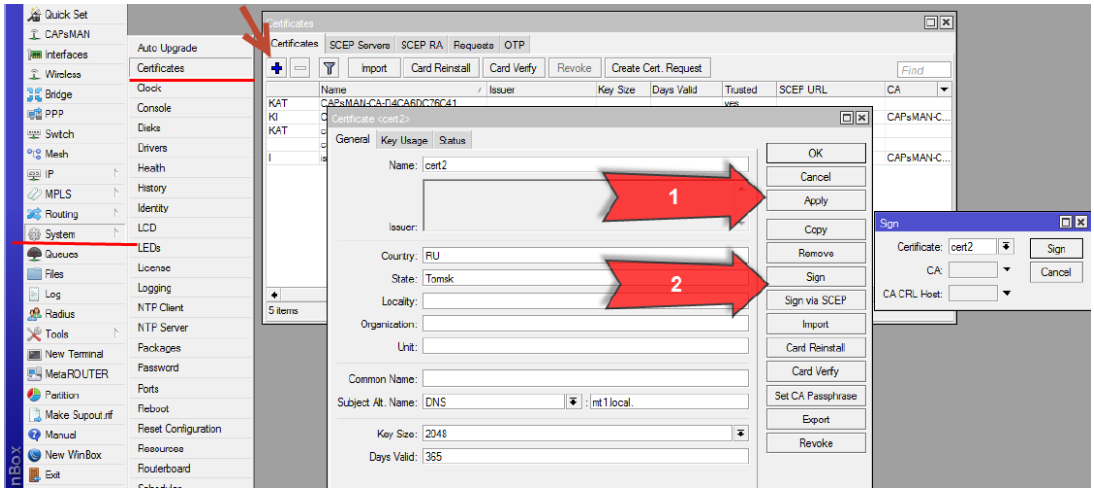
- Luba DNS-ile juurde pääseda ainult usaldusväärsetel hostidel
- Kasutada väliseid DNS-servereid (nt google DNS)



Joonis 2.9. On vaja kasutada väliseid DNS-servereid

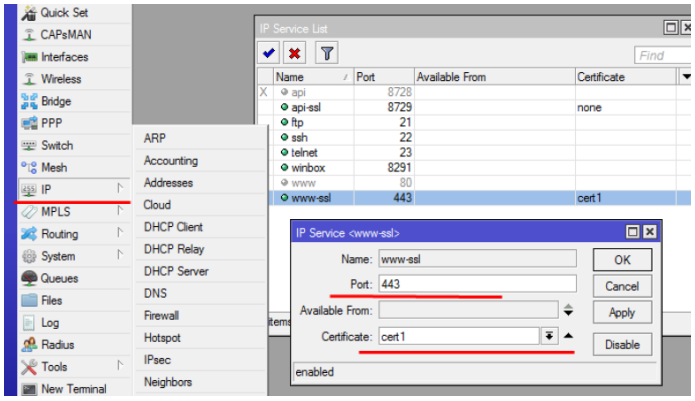
2.2.3.2 WebFigi ja API-de kaitse

- HTTP edastab andmeid lihttekstis
- HTTPS ei ole vaikimisi sees
- HTTPS vajab töötamiseks sertifikaati. Ükskõik millist



Joonis 2.10. Sertifikaati loomine

Tuleb installida sertifikaat teenusesse, muuta porti:



Joonis 2.11. Teenuse sertifikaat tuleb paigaldada

2.2.3.3 Tulemüür – trap port

Kasutamata tuntud teenindusport põhjustab ühenduse loomisel keelu.

Connect to TCP 3389 ? > Blacklist

Peab sisestama Src-IP aadressi loendisse "Blacklist". Kohaloleku aja peab valima enda järgi turvapoliitika.

/ip firewall filter add action=add-src-to-address-list address-list=blacklist address-list-timeout=0s chain=input protocol=tcp dst-port=3389 comment="RDP cracker"

2.3 Võrgu segmenteerimine

Kohtvõrgu segmenterimine (VLANid) võimaldab efektiivselt liiklust eraldada, võrku paremini ära kasutada ning vähendada võrguseadmete koormusi. Sideprotokoll IEEE 802.1Q liidab mehhanisme, mis võimaldab LAN liiklusel kanda VLAN identifikaatoreid ja selle järgi liiklust segmenteerida. VLANid võimaldavad efektiivselt liiklust eraldada, võrku paremini ära kasutada ning vähendada võrguseadmete koormusi.

Lähtudes lähteülesannetest töötati välja skeem uue võrgu jagamiseks 7 alamvõrkudeks (VLAN-id): videovalveseadmed, kaubandusosakond, laboratoorium, finantsosakond ja juhid, serverid, välised Wi-Fi-seadmed ja IT juhtimine.

192.168.1.0/24

# hosts		65536	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	2^N
Σ bits		128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	2^N
# hosts		65534	32766	16386	8190	4094	2046	1022	510	254	126	62	30	14	6	2	0	2^N
# bit		16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	N bit
192	168	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	1	
192	168	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	0	1	0	1	1	1	1	1	
192	168	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	1	
192	168	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	1	0	0	1	1	1	1	1	
192	168	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	1	0	1	1	1	1	1	1	
192	168	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	1	1	0	1	1	1	1	1	
192	168	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	
192	168	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	

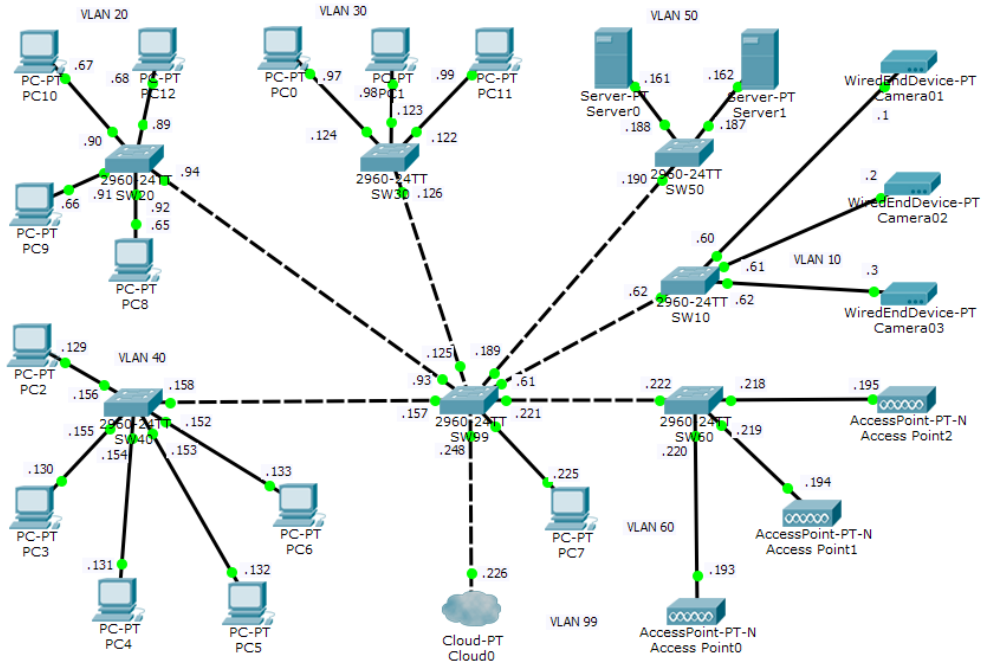
Tabel 2.2. IP-aadressi bittide tabel

Hosts	Network	First IP Host	Last IP Host	Broadcast
Subnet 10 - 62 hosts	192.168.1.0/26	192.168.1.1/26	192.168.1.62/26	192.168.1.63/26
				255.255.255.192
Subnet 20 - 30 hosts	192.168.1.64/27	192.168.1.65/27	192.168.1.94/27	192.168.1.95/27
				255.255.255.224
Subnet 30 - 30 hosts	192.168.1.96/27	192.168.1.97/27	192.168.1.126/27	192.168.1.127/27
				255.255.255.224
Subnet 40 - 30 hosts	192.168.1.128/27	192.168.1.129/27	192.168.1.158/27	192.168.1.159/27
				255.255.255.224
Subnet 50 - 30 hosts	192.168.1.160/27	192.168.1.161/27	192.168.1.190/27	192.168.1.191/27
				255.255.255.224
Subnet 60 - 30 hosts	192.168.1.192/27	192.168.1.193/27	192.168.1.222/27	192.168.1.223/27
				255.255.255.224
Subnet 100 - 30 hosts	192.168.1.224/27	192.168.1.225/27	192.168.1.254/27	192.168.1.255/27
				255.255.255.224

Tabel 2.3. Alamvõrgu piiride tabel

Paindlikuma ja tõhusama disaini jaoks loodi võrguemulaatoris uue süsteemi mudel – Cisco Packet Tracer.[15]

Selles töö etapis pakuti välja ka optimaalsem, turvalisem ja töökindlam kommutaatorite ja juhtmega ühenduste paigutus. Kommutaatorid pidid olema paigutatud eraldi võtmega lukustatavatesse kappidesse koos varutoiteseadmetega (UPS).



NVR VLAN
VLAN 10 | 192.168.1.0/26
Commerce VLAN
VLAN 20 | 192.168.1.64/27
Lab VLAN
VLAN 30 | 192.168.1.96/27
Finance VLAN
VLAN 40 | 192.168.1.128/27
Server VLAN
VLAN 50 | 192.168.1.160/27
AP VLAN
VLAN 60 |192.168.1.192/27
IT VLAN
VLAN 99 | 192.168.1.224/27

Passwords		
# SW	CLI	Telnet
SW10	SW10vlan10	Vlan1@
SW20	SW20vlan20	Vlan2@
SW30	SW30vlan30	Vlan3@
SW40	SW40vlan40	Vlan4@
SW50	SW50vlan50	Vlan5@
SW60	SW60vlan60	Vlan6@
SW99	SW99vlan99	Vlan9@

Subnetting IPv4		
# VLAN	Network	Broadcast
VLAN 10	192.168.1.0/26	192.168.1.63/26
VLAN 20	192.168.1.64/27	192.168.1.95/27
VLAN 30	192.168.1.96/27	192.168.1.127/27
VLAN 40	192.168.1.128/27	192.168.1.159/27
VLAN 50	192.168.1.160/27	192.168.1.191/27
VLAN 60	192.168.1.192/27	192.168.1.223/27
VLAN 100	192.168.1.224/27	192.168.1.255/27

Joonis 2.12. Uue kohtvõrgu mudel Cisco emulaatoris

ROUTER R1 MikroTik RB750Gr3 - configuration
Clear configuration (better through menu):
/system reset-configuration no-defaults=yes skip-backup-yes
We name the router:
/system identity
set name "R1"
Then, in order to improve safety, we disable all unused services, leave only Winbox:
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
For convenience, we rename the network interfaces and add comments:
/interface ethernet
set [find default-name=ether1] comment="WAN" name=ether1-wan
set [find default-name=ether2] comment="TRUNK 1" name=ether2-trunk
set [find default-name=ether3] comment="TRUNK 2" name=ether3-trunk
set [find default-name=ether4] comment="TRUNK 3" name=ether4-trunk
set [find default-name=ether5] comment="IT MGMT" name=ether1-it

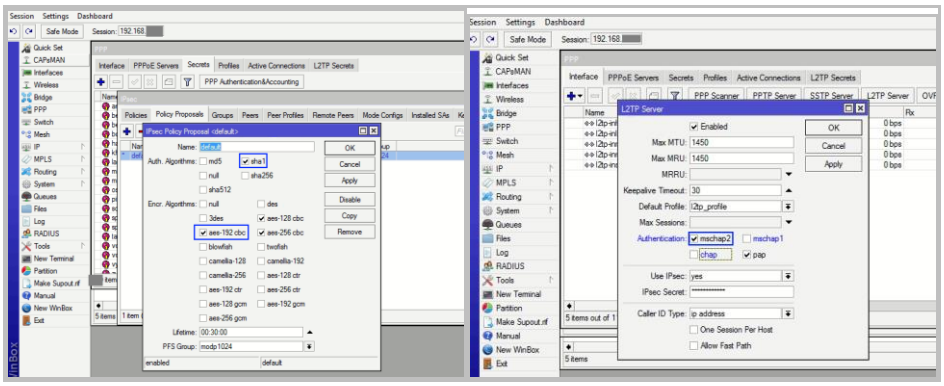
The interfaces ether2 and ether3 need to be turned into trancks by giving the right vlan to each port:
/interface vlan
add interface=ether2-trunk name=vlan10-trunk-to-uby vlan-id=10
add interface=ether2-trunk name=vlan20-trunk-to-uby vlan-id=20
add interface=ether2-trunk name=vlan30-trunk-to-uby vlan-id=30
add interface=ether2-trunk name=vlan70-trunk-to-uby vlan-id=70
add interface=ether3-trunk name=vlan40-trunk-to-tplink vlan-id=40
add interface=ether3-trunk name=vlan60-trunk-to-tplink vlan-id=60
add interface=ether4-trunk name=vlan50-trunk-to-vmware vlan-id=50
VLAN's been created, but ports other2 and other3 are still unlinked.
With the help of the bridge, we combine each vlan into our bridge, and we also place the corresponding ports of access:
/interface bridge port
add bridge=bridge-vlan10-nvr comment="VLAN10" interface=vlan10-trunk-to-uby
add bridge=bridge-vlan20-commerce comment="VLAN20" interface=vlan20-trunk-to-uby
add bridge=bridge-vlan30-lab comment="VLAN30" interface=vlan30-trunk-to-uby
add bridge=bridge-vlan70-top comment="VLAN70" interface=vlan70-trunk-to-uby
add bridge=bridge-vlan40-finance comment="VLAN40" interface=vlan40-trunk-to-tplink
add bridge=bridge-vlan60-ap comment="VLAN60" interface=vlan60-trunk-to-tplink
add bridge=bridge-vlan50-server comment="VLAN50" interface=vlan50-trunk-to-vmware
add bridge=bridge-vlan99-it-mgmt comment="VLAN99" interface=ether5

Tabel 2.4. Terminali kasutamine käskude sisestamiseks

2.4 VPN-ühenduste konfigureerimine

VPN on Interneti kasutamise viis, andes kasutajatele või kaugrühmale juurdepääsu organisatsioonivõrgule kaitstud keskkonnas. Windows 10 on konfigureeritud kasutama protokollide komplekti, mis pakuvad enda ja VPN-lüüsi vahel virtuaalset privaatvõrguühendust (VPN), lisaks kaitstud side kaudu HTTPS-i kaudu. Windows rakendab IPseci, et pakkuda kahe peerarvutiga kaitstud, autentiseeritud, konfidentsiaalset ja turvamärkevõrgustikku.

RouterOS-i operatsioonisüsteemil MikroTikis on palju erinevaid seadistusi VPN-ühenduste jaoks. Neid saab valida menüü kaudu või sisestada terminalis käske.

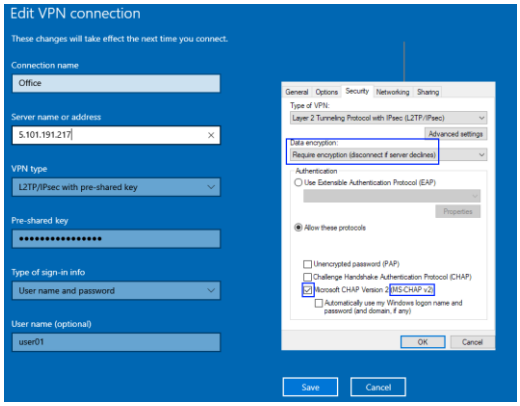


Joonis 2.13. WinBoxi utiliidi kasutamine tunnelite sisendi seadistamiseks

```
Setup of VPN L2TP+Ipsec
Adding a new subnet:
/ip pool add name=vpnpool ranges=192.168.111.100-192.168.111.199

First you need to set network parameters for VPN clients:
/ppp profile
add change-tcp-mss=yes dns-server=192.168.111.1 local-address=192.168.111.1 name=l2tp remote-address=pool-1 use-encryption=yes

Activation of the VPN server (only mschap2):
/interface l2tp-server server
set authentication=mschap2 default-profile=l2tp enabled=yes ipsec-secret=edruzam@Tulemyyrit#2022 use-ipsec=required

Creation of a VPN account for a client:
/ppp secret
add name=user1 password=user1 profile=l2tp
add name=user2 password=user2 profile=l2tp

Firewall for the client's VPN permits:
/ip firewall filter
add action=accept chain=input comment="Port Access" dst-port=500,1701,4500 in-interface=WAN protocol=udp
add action=accept chain=input comment="Ipsec-esp" protocol=ipsec-esp
add action=accept chain=forward comment="vpn-to-vlan50" src-address=192.168.111.0/24 in-interface=!ether1-wan out-i

IPsec setting:
```

Joonis 2.14. Terminali kasutamine käskude sisestamiseks

Üks populaarsemaid VPN kliente on oma Windows-i 10 ja 11 „IPsec VPN klient". Järgnevalt on toodud seadistuste näited kaitstud ühenduse loomiseks L2TP-protokollis, mis on krüpteeritud IPsec AES 192 bitti MS-CHAP2 algoritmiga.



Joonis 2.15. Windowsi VPN-kliendi seadistamise näide

3 TEISED ÜKSIKUD FUNKTSIOONID

3.1 Arhiveerimissüsteemi loomine

Varundamise eesmärk on luua koopia andmetest, mida saab taastada esmase andmetõrke korral. Esmased andmetõrked võivad tuleneda riist- või tarkvararikkest, andmelaostust või inimese põhjustatud sündmusest, näiteks pahatahtlikust rünnakust (viirus või pahavara) või andmete juhuslikust kustutamisest. Varukoopiad võimaldavad andmeid taastada varasemast ajahetkest, et aidata ettevõttel plaanivälisest sündmusest taastuda.

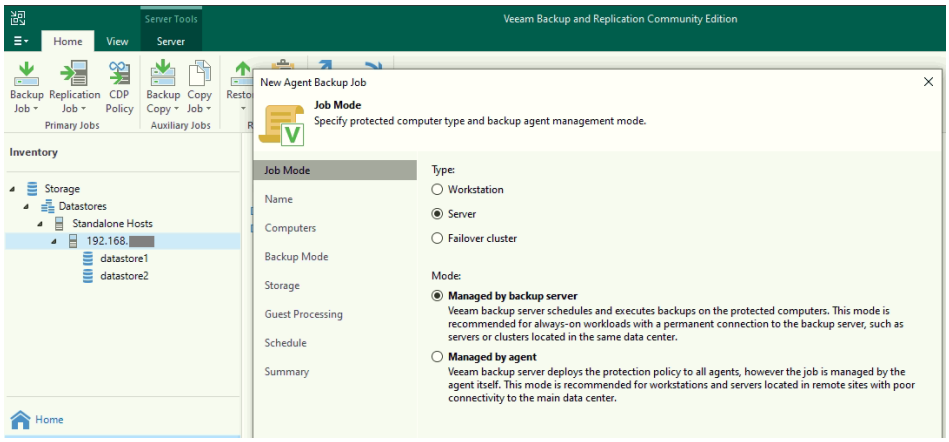
Andmete koopia salvestamine eraldi andmekandjale on kriitilise tähtsusega, et kaitsta andmete kaotsimineku või korruptsiooni eest. See täiendav andmekandja võib olla sama lihtne kui väline ketas või USB-pulk või midagi olulisemat, näiteks ketta salvestussüsteem või pilvesalvestuskonteiner. Alternatiivne andmekandja võib olla lähteandmetega samas kohas või kauges kohas.[16]

Autor on kasutanud oma kogemusi erinevate andmete arhiveerimise tarkvara rakendamisel. Oli paigaldatud usaldusväärse ja mugava arhiveerimissüsteemi loomiseks kahte tarkvarat, et salvestada andmete koopiat serverist ja virtuaalsetest masinatest - Veeam Backup & Replication Community Edition ja Iperius Backup free edition.

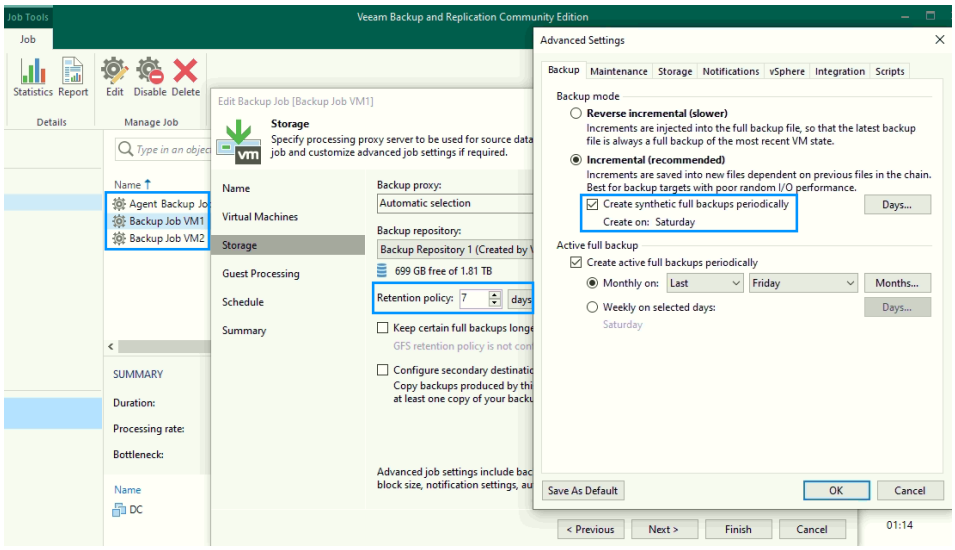
3.1.1 Veeam Backup & Replication

Selles peatükis on toodud näiteid selle tarkvara rakendamisest tööobjektil.

Tarkvara võimaldab salvestada andmeid nii füüsilistelt masinatelt kui ka virtuaalsetelt VMwaradelt ja Hyper-V-delt. Füüsiliste objektidega tegelemiseks paigaldab tarkvara objektile oma arhiiviagendi. Andmeallikaks võib olla arvuti, server või isegi tõrkekindel klaster.[17]



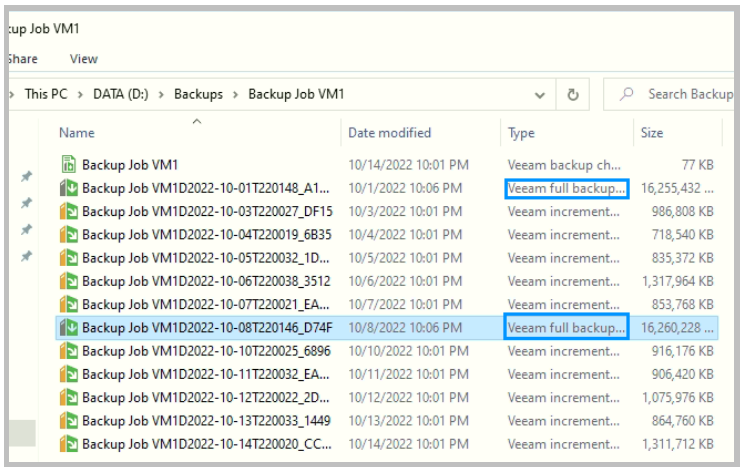
Joonis 3.1. Uue ülesande loomine arhiveerimiseks füüsilisest serverist



Joonis 3.2. Arhiveerimise algoritmi muutmine

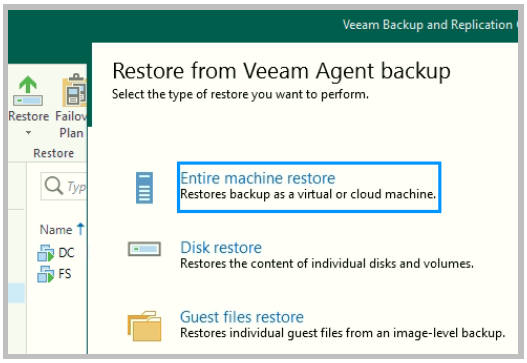
Joonisel 3.2 on näha uue serveri ühe virtuaalmasina varundusseaded. Tööpäevadel luuakse virtuaalmasinast „incremental" koopia - ainult sel päeval muudetud andmeid kopeeritakse. Laupäeval valmib täielik koopia. Pildil on märgitud sünteetilise režiimi variant - täielik koopia luuakse ilma faile ümber kirjutamata, kui neid ei muudeta. See suurendab kopeerimiskiirust.

Reaalsel näitel on näha arhiveerimisülesande tulemusi - 2 täisnädalast arhiivi ja mõned „incremental" (väikesed).



Joonis 3.3. Arhiveerimisülesande tulemused

Sellel programmil on veel üks väga kasulik funktsioon - füüsilise masina täielikust koopiast saab luua identse virtuaalse masina!

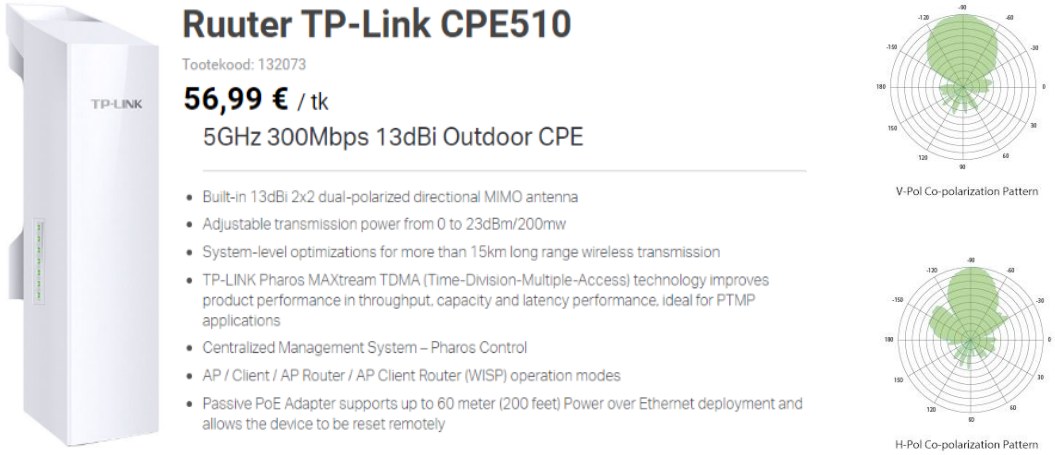


Joonis 3.4. Füüsilise masina konverteerimine virtuaalseks

3.2 WiFi AP-i paigaldamine ja seadistamine

Vastavalt tehnilisele ülesandele tuleb luua tootmiskontrollerite vaheline võrguühendus kontoriga. Objekti uurimisel selgus, et kõige efektiivsem ja tasuvam oleks WiFi AP paigaldus tootmise poolt. Seda enam, et 3 sellist seadet on juba pikka aega töötanud. Peamoodul on AP, mis on paigaldatud kontori katusele ja kaks KLIENTI ettevõtte territooriumile. Mitmepunktiühendus on loodud TP-Link CPE510 ruuterite abil. Mudel on odav, kuid tõhusa varustusega.

Selle seadme praktiline kasutamine näitas selle suurt töökindlust, head kiirust, suurt sidekaugust ja laia suunadiagrammi (vt joonis L1.7). Mitme sellise kliendi ühendus (kolme praktikas) toimib stabiilselt ja võimaldab ühendada kaugeid objekte näiteks kontoriga.

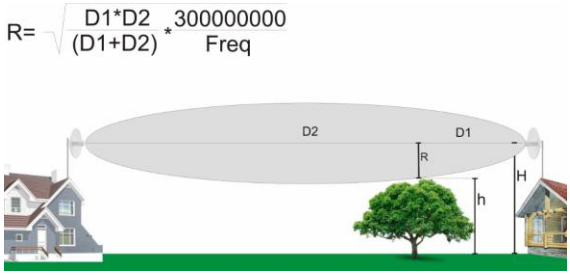


Joonis 3.5. WiFi ruuter TP-Link CPE510 ja tema antenni suunadiagramm

Tööstuspiirkonnas on üsna palju raadiohäireid. Sellel soodsal mudelil on sisseehitatud häirete analüsaator:

Joonis 3.6. Saab valida kõige puhtama kanali

Otsustati paigaldada veel üks KLIENT tootmishoone juurde. Kaugus AP-st on umbes 600 meetrit. Kuid väga halb otsenähtavus häirib torusid ja tehnoloogilisi seadmeid. Nagu on teada, tuleb Fresneli seaduse kohaselt ühenduse hea kvaliteedi tagamiseks tagada puhas nähtavust, mille raadius on väiksem kui kaugus kiire keskmest takistuseni.

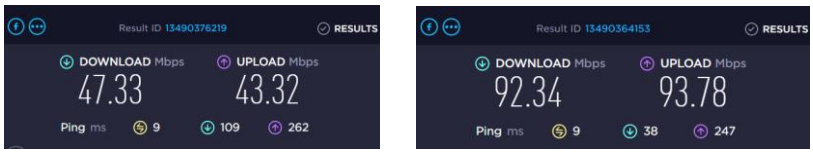


Joonis 3.7. Fresneli tzoon[18]

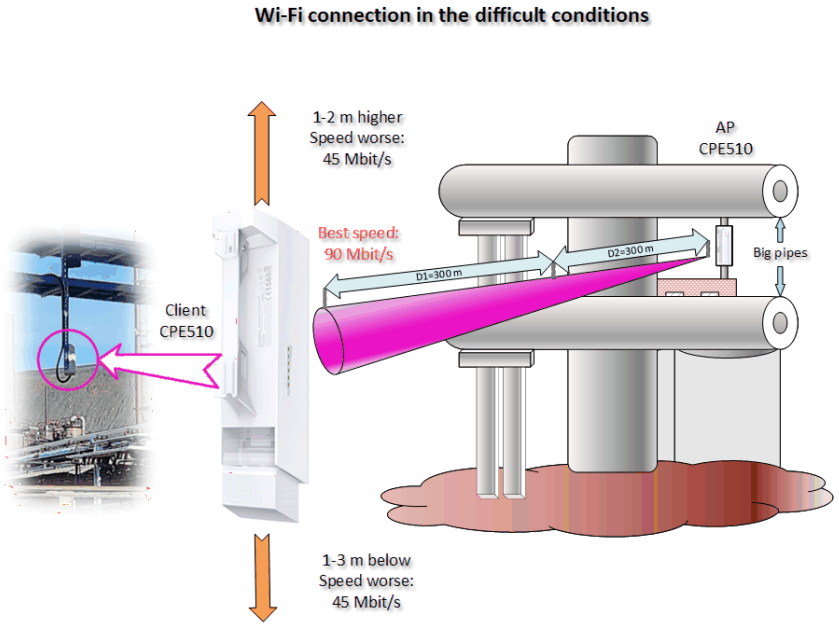
Praktiliste rakenduste jaoks on sageli kasulik teada esimese Fresneli tsooni maksimaalset raadiust F1 (n=1). Arvutamiseks rakendati valemit [18]:

- $F_1[\mathrm{m}] = 8.656\sqrt{\frac{D[\mathrm{km}]}{f[\mathrm{GHz}]}}$, sisestasid D=0,6km ja f=5. Siis F1=2.998m

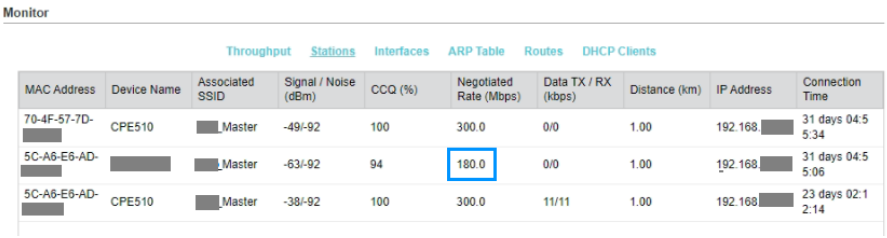
Probleem oli selles, et umbes keskel on 2 horisontaalset torustikku suurte torudega. Õnnestus leida punkt, millest oli näha pearuuter kontori katusel. Signaali sirge joon kulges just torude vahel. Täpselt sellesse kohta paigaldati ruuter ja saadi maksimaalseks kiiruseks 93 Mbps.



Joonis 3.8. Speedtest. Vasakul - 1 m madalamal ja paremal - parim paigalduskoht



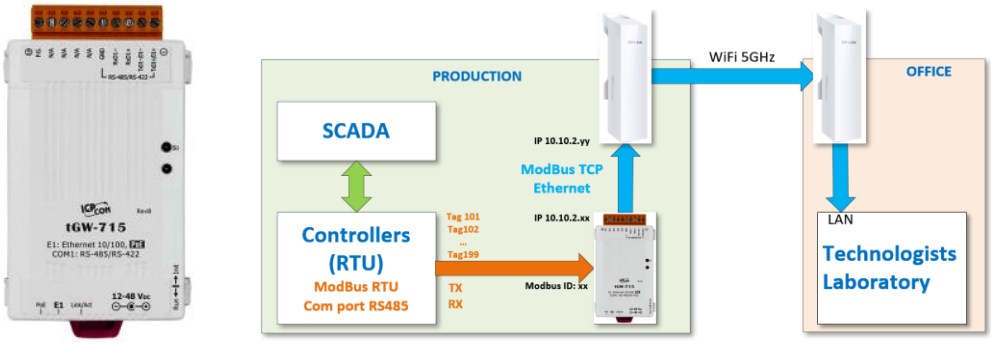
Joonis 3.9. Parim paigalduskoht – parim kiirus



Joonis 3.10. Pearuuteri ühenduste tabel (AP)

3.3 Andmete vastuvõtmine SCADA-st

Ülesanne lahendamiseks valiti välisohtude seisukohalt turvaline tehnoloogia. Oli kasutatud andmeedastusmuundur ModBus RTU standardist (serial RS-485) ModBus TCP-ks (ethernet). Valiti ja konfigureeriti odav moodul ModBus Gateway tGW-715:



Joonis 3.11. tGW-715 ja andmeedastustehnoloogia skeem SCADA-st kontorisse

Turvanõuete kohaselt tuleks automaatjuhtimissüsteem (APCS) eraldada Internetist ja ettevõtte muudest IT-allsüsteemidest. Tavaliselt on see autonoomne isemajandav süsteem. Kuid mõnikord on vaja teostada andmevahetust kontoriga. Näiteks

tehnoloogidele või laboritele. Sellistel juhtudel saab edastuskanalis kasutada vaheandmete teisendust. See sulgeb võimaluse siseneda juhtimissüsteemi.

Pärast selle seadme paigaldamist saavad tehnoloogid juhtimissüsteemist mitmeid protsessiandmeid.

3.4 4G ruuteri paigaldamine ja seadistamine

Mõnel juhul on nõutav juurdepääs tööstusseadmetele kaugemal asuvas kohas. Selleks kasutatakse nüüd 4G mobiilitehnoloogiat. Turul on palju üsna kalleid suurepäraste funktsioonidega 4G ruutereid. Kuid kui on vaja kaugobjekti väikese raha eest Internetiga ühendada, saab osta tuntud tootja MikroTik usaldusväärse ja tõestatud seadmeid: antenn + 4G modemikomplekti. Antenni tüüp on SXT R (10,5 dBi 60 kraadi LTE antenn, millel on 2x Etherneti porti koos PoE-ga). Modem võib olla kas P11-LTE või P11-LTE6. Kogu SXT R + R11e-LTE komplekt maksab 170 eurot. R11e-LTE modem toetab 4. kategooria 4G-d (150Mbps Downlink, 50Mbps Uplink).[19]

Kuna antennis töötab operatsioonisüsteem RouterOS, saab leida selle seadistamise soovitused selle töö jaotisest *Ruuteri funktsioonid*. See odav komplekt on kohapeal testitud. See tagab hea andmeedastuskiiruse ja stabiilse töö isegi rasketes ilmastikutingimustes. Täpselt sama komplekt paigaldati ka uuele ettevõtte pakendamismasinale.

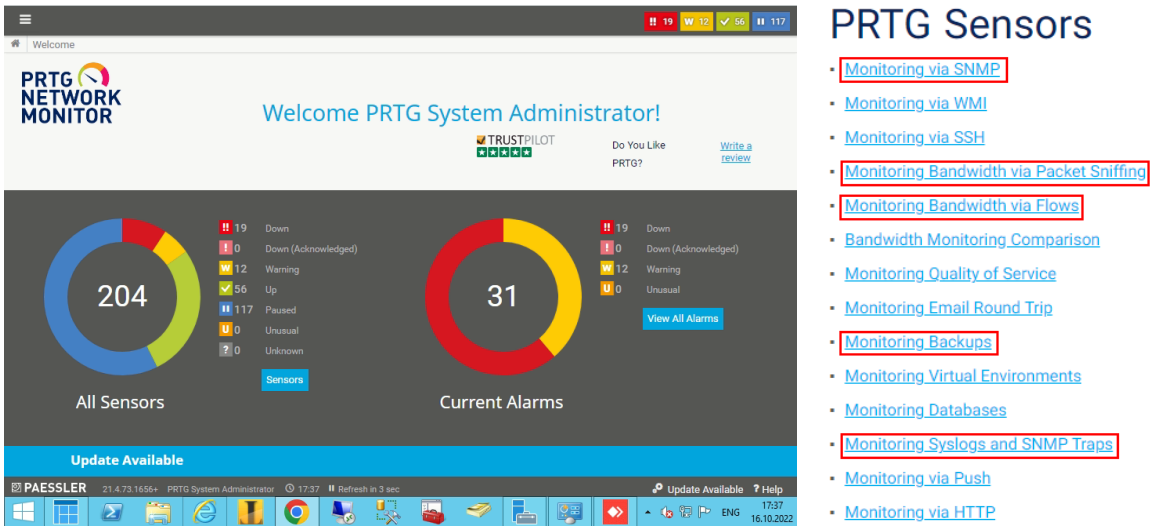
Joonis 3.12. MikroTik-i 4G ruuter ja LTE modem

3.5 Võrgu ja arvutite jälgimine

3.5.1 PRTG Network Monitor-i konfigureerimine

Igas arvutisüsteemis on võimalus võrguseade välja lülitada või selle parameetreid kriitiliselt muuta. On mitmeid programme, mis kontrollivad etteantud arvutivõrgu punkte ja hoiatavad IT-teenistust või administraatorit probleemi eest.

On olemas üsna võimas ja populaarne - PRTG Network monitor. Kasutatud oli tasuta versioon.



Joonis 3.13. PRTG Network Monitor ja andurid

Iga litsents, isegi vabavara väljaanne, pakub täielikku valikut funktsioone. Tasuta tarkvara 100-sensoriga väljaanne, mis on rakendatud tervikliku seirelahendusena, on piisav väikese ettevõtte võrgu või suure koduvõrgu jaoks. Tasuta versiooni jaoks peab valima kõige vajalikumad andurid (vt. joonis 3.11).[20]

Näiteks saab SNMP-ga koguda võrgu läbilaskevõimest kasutusandmeid väga lihtsal viisil.

Ühes hostis või serveris on selle konkreetse seadme kasutatava läbilaskevõimest mõõtmiseks parim viis SNMP-andur.

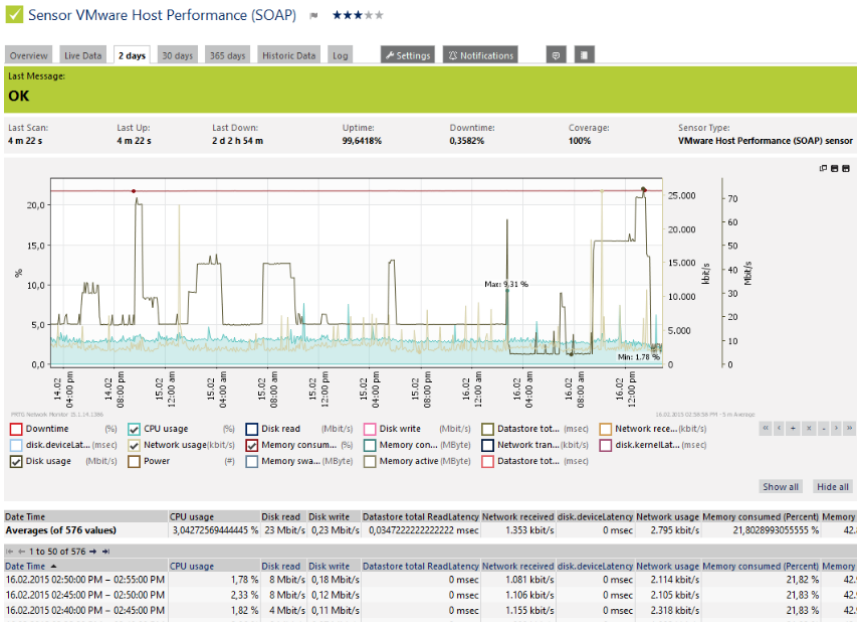
Kommutaatoris või ruuteris näitavad SNMP andurid läbilaskevõimest kasutamist konkreetses pordis. Iga pordi kohta on vaja seadistada üks andur.

Flow tehnoloogiad (NetFlow, IPFIX, jFlow, sFlow) sobivad kõige paremini Cisco, Juniperi, HPE ja muude ettevõtte tasemel ruuterite ja kommutaatorite jaoks. Need protokollid peavad olema seadmes sisse lülitatud. Voo jälgimine võimaldab tuvastada kitsaskohti ja tarbimist IP-aadressi järgi, et tuvastada läbilaskevõimest probleemi algpõhjust.

Kui teil on vaja teada ainult praeguse ja hiljutise liikluse kohta protokolli või IP-aadressi järgi, saab lisada ka ainult ühe vooluanduri ja lubada funktsiooni Toplist. Näiteks saab NetFlow v9 anduri abil jälgida kommutaatori või ruuteri aktiivsemad kasutajaid, protokolle ja ühendusi.

Veel üks kasulik andur - VMware hosti jälgimine. Sarnaselt vooseirega nõuab VMware keskkondade jälgimine tavaliselt kalleid erilahendusi või lisandmooduleid. Ja nagu vooluandurid, kuuluvad VMware andurid PRTG funktsioonide hulka.

Freeware Editioni saab kasutada VMware integreeritud jälgimise täiendamiseks häire- ja aruandlustööriistaga. VMware jaoks spetsiaalsete hostandurite abil võimaldab see PRTG-l lugeda ja töödelda põhjalikke jõudlusandmeid. Lisaks saab PRTG jälgida ka riistvara, millel VMware host töötab.[21]



Joonis 3.14. VMware hosti jälgimine

KOKKUVÕTE

Lõputöö teema "Ettevõtte IT-süsteemi renoveerimine VMware tõrkekindla klastri tehnoloogiaga" on seotud tööstusettevõtte IT-süsteemi rekonstrueerimise projektiga sobiva infrastruktuuriga Ida-Virumaa tööstuspiirkonnas selle aasta septembris. Tõsine argument selle otsuse kasuks oli kliendi nõue mitte ainult uuendada olemasolevat IT-süsteemi, vaid tagada ka VMware vSphere platvormil virtuaalmasinaid kasutava spetsiaalse tehnoloogilise programmi pidev töö. Nii õnnestus autoril uurida huvitavaid, kaasaegseid, kuid üsna keerukaid HA ja FT funktsioone. Selleks oli vaja välja töötada oma laboristendi, paigaldada VMware ESXi operatsioonisüsteemid, seadistada Active Directory domeen ning läbi viia vajalikud uuringud.

Lõputöö teiseks põhiülesandeks oli erinevate ohtude eest kaitstud ettevõtte domeeniarvutivõrgu 15-20 arvutiga loomine madalate finantskuludega. Kuna selles ettevõttes on juba mitu aastat töötanud odav ja end tõestanud ruuter Mikrotik RB750gr3, otsustati seda mitte muuta. Sellele oli vaja lisada kaitsefunktsioonid ja VLAN-süsteem. Lisaks loodi Cisco Packet Tracer emulaatori abil 7 VLAN-ist süsteemi töömudel koos üksikasjaliku võrgu diagrammiga. Lisas 3 on täielik loetelu ruuteri seadistamise käskudest, mis on juba reaalselt kasutusel töötavas ettevõtte IT-süsteemis.

Kolmanda ülesande eesmärk oli näidata madala hinnaga lahendust eraldiseisvate tehnilistele küsimustele. Sealhulgas kaugobjektidega suhtlemise korraldamine Wi-Fi tehnoloogiate ja 4G mobiilside abil. Andmete automaatse arhiveerimise tagamine usaldusväärse ja multifunktsionaalse programmi Veeam Backuper Community kasutamisel. Selle kasutamine on Windowsi serverite tasuta, ning VMware hostide jaoks tasuta, eeldusel, et sellesse on installitud mis tahes tasuline vSphere ESXi-i versioon. Samal ajal võimaldab võimsa võrgujälgimisprogrammi PRTG Monitor tasuta versiooni kasutamine tuvastada ja analüüsida probleeme arvutitega või arvutivõrguga.

Autori töö kinnitab võimalust kasutada selliseid seadmeid ja tarkvara, mis ühelt poolt suudavad tagada vajaliku funktsionaalsuse ja töökindluse ning teiselt poolt ei nõua liigseid investeeringuid.

Lõputöö lisas on soovitatavate seadmete loetelu ja hinnapakkumised kehtivate hindadega. Suurem osa nendest seadmetest juba töötab tööstusobjekti renoveeritud IT-süsteemis vastavalt tehnilisele projektile.

Lisa sisaldab ka MikroTik ruuteri konfigureerimise käskude täielikku loendit, mis põhineb selliste seadmetega saadud kogemustel ja kaasaegsete võrguturbelahenduste uurimisel.

Selgitused läbiviidud tööde kohta lõputöö käigus:

- oli määratletud väikeettevõtte IT-süsteemi funktsioonid;
- oli iga funktsiooni jaoks pakutud välja renoveerimise eesmärkidele vastavad seadmed;
- olid käsitletud üksikasjalikult ohud ettevõtte võrgu turvalisusele ja pakutud välja MikroTik ruuteritel põhinevad kaitsemeetodid;
- oli ehitatud ettevõtte arvutivõrgu mudel, milles oli jagatud 7 märgistatud alamvõrkku (VLAN);
- selle mudeli ja võrgu turvanõuete põhjal oli loodud ruuteri MikroTik RB750gr3 konfiguratsioon;
- oli esitatud täielik käskude loend selle seeria ruuterite nullist konfigureerimiseks (lisa 3);
- oli valmistatud laboristend VMware virtuaalmasinate kaitsmise üsna keerukate ja asjakohaste tehnoloogiate uurimiseks - Distributed Resource Scheduler (DRS), vSphere High Availability (HA) ja vSphere Fault Tolerance (FT);
- oli läbi viidud edukad katsed tõrketaluva virtuaalmasinate klastri loomiseks vSphere ESXi ja koostatud plaan nende kaasaegsete tehnoloogiate juurutamiseks ühes tööstusettevõttes 2023. aasta alguseks.

VMware virtuaalmasinate tõrkekindla klastri laboratooriumis testimise tulemuse tunnistas ettevõtte juhtkond edukaks ja aktsepteeriti tõrkekindla klastri loomisega seotud tööd ettevõtte reaalses IT-süsteemis. Need tööd peaksid algama 2023. aasta jaanuaris. Oluline on märkida, et selles lõputöös välja toodud virtuaalmasinate tõrkesiirde klastrite põhimõtted aitavad vältida vigu ja mõistavad neid tõhusaid tehnoloogiaid paremini. Kuna praegu kasutatakse IT-süsteemides palju virtuaalmasinaid, tulevad praktilised kogemused autorile edaspidises töös kindlasti kasuks.

Läbiviidud uurimistöö ja praktilise töö tulemusena saavutati edukalt kõik lõputöö püstitatud eesmärgid. Autor näitas oma oskust lahendada üsna keerulisi tehnilisi küsimusi, kasutada efektiivselt dokumentatsiooni ja internetti, analüüsida tekkivaid ebastandardseid olukordi ning rakendada Virumaa Kolledžis omandatud teadmisi praktikas.

SUMMARY

The subject of the graduation work "Renovation of company's IT system with VMware failover cluster technology" is related to an IT system reconstruction project of an industrial company with suitable infrastructure in the industrial region of Ida-Virumaa in September 2022. A serious argument in favor of this decision was the client's requirement not only to update the existing IT system, but also to ensure the continuous operation of a specific technological program using virtual machines on the VMware vSphere platform. Thus, the author managed to study interesting, modern, but rather complex functions of HA and FT. In order to do so, it was required to build an own laboratory, install VMware ESXi operating systems, connect them to Active Directory and conduct the necessary research.

The second main task of the thesis was to create a low-cost corporate domain computer network with 15-20 computers protected against various threats. Since the inexpensive and proven Mikrotik RB750gr3 router has been working in this company for several years, it was decided not to change it. It was necessary to add protection functions and a VLAN system. Additionally, a working model of the 7 VLAN system with a detailed network diagram was created using the Cisco Packet Tracer emulator. Appendix 3 provides a complete list of router configuration commands that are already in use in a live corporate IT system.

The purpose of the third task was to show a budget solution to more narrow technical issues. Including the organization of communication with remote objects using Wi-Fi technologies and 4G mobile communications. The automatic data archiving is based on the use of the reliable and multifunctional program Veeam Backuper Community. It is free to use for Windows servers, as it is free for VMware hosts, provided that any paid version of vSphere ESXi is installed. At the same time, using the free version of the powerful network monitoring program PRTG Monitor allows to identify and analyze problems with computers or a computer network. This graduation work confirms the possibility of using such devices and software, which, on the one hand, can provide the necessary functionality and reliability, and, on the other hand, do not require excessive investment.

The appendix of the thesis contains a list of recommended equipment and price offers with current prices. Most of these devices are already working in the renovated IT system of the industrial facility in accordance with the technical project.

The appendix also contains a complete list of MikroTik router configuration commands based on experience with such devices and research into modern network security solutions.

Explanations for the work performed during the thesis:

- the functions of the IT system of a small company were defined;
- for each function, equipment corresponding to the objectives of the renovation was proposed;
- threats to the security of the company's network were discussed in detail and protection methods based on MikroTik routers were proposed;
- a model of the company's computer network, divided into 7 subnets (VLANs), was built;
- the MikroTik RB750gr3 router configuration was created based on this model and network security requirements;
- a complete list of commands for configuring routers of this series from scratch was provided (Appendix 3);
- a laboratory stand was prepared to study quite complex and relevant technologies for protecting VMware virtual machines - Distributed Resource Scheduler (DRS), vSphere High Availability (HA) and vSphere Fault Tolerance (FT);
- successful experiments to create a fault-tolerant cluster of virtual machines for vSphere ESXi were conducted, and a plan to implement these modern technologies in an industrial enterprise in early 2023 was prepared.

The result of testing the failover cluster of VMware virtual machines in the laboratory was recognized as successful by the company's management, and the work related to the creation of a failover cluster in the real IT system of the company was accepted. These works should start in January 2023. It is important to note that the principles of virtual machine failover clustering outlined in this thesis will help to avoid mistakes and better understand these effective technologies. Since many virtual machines are currently used in IT systems, practical experience will certainly be useful to the author in his future work.

As a result of the research and practical work performed, all the stated goals of the final work were successfully achieved. The author showed his ability to solve rather complex technical issues, use documentation and the Internet effectively, analyze emerging non-standard situations and apply the knowledge gained at Virumaa College in practice.

KASUTATUD KIRJANDUSE LOETELU

1. Dell support. [Online] 12.10.22 https://www.dell.com/support/home/en-ee/product-support/product/poweredge-t40/docs
2. Benefits of Active Directory (Pros and Cons). [Online] 10.10.22 https://cloudinfrastructureservices.co.uk/benefits-of-active-directory/
3. 12 Group Policy Best Practices: Settings and Tips for Admins [Online] 01.12.22 https://www.varonis.com/blog/group-policy-best-practices
4. What is a file server? [Online] 01.12.22 https://www.techtarget.com/searchnetworking/definition/file-server
5. Install and Configure WSUS on Windows Server 2019 [Online] 01.12.22 https://www.prajwaldesai.com/install-configure-wsus-on-windows-server-2019/
6. Windows Server 2016/2019 auditi poliitika parim tava [Online] 12.10.22 https://4sysops.com/archives/windows-server-2016-2019-audit-policy-best-practice/
7. VMware vSphere [Online] 01.12.22 https://www.techtarget.com/searchvmware/definition/VMware-vSphere
8. VMware availability guidelines and VMware HA best practices [Online] 01.12.22 https://www.techtarget.com/searchdisasterrecovery/High-availability-guidelines-and-VMware-HA-best-practices
9. VMware vSphere Standard [Online] 01.12.22 https://store-us.vmware.com/products/data-center-virtualization-cloud-infrastructure.html
10. Product Evaluation Center for VMware vSphere Hypervisor [Online] 01.12.22 https://customerconnect.vmware.com/en/evalcenter?p=free-esxi8
11. VMware iSCSI Initiators [Online] 01.12.22 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-7A4E3767-CB54-4E88-9BA8-298876119465.html
12. How vSphere HA works [Online] 12.10.22 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc
13. vSphere Fault Tolerance [Online] 12.10.22 https://www.vmware.com/products/vsphere/fault-tolerance.html
14. MikroTik RouterOS. Documentation [Online] 01.12.22 https://help.mikrotik.com/docs/display/ROS/RouterOS
15. Cisco Packet Traser – Tutorial For Beginners [Online] 01.12.22 https://topologynetwork.com/cisco-packet-tracer-tutorial-beginners/

16. Why Backup and Recovery is important. [Online] 12.10.22 https://www.netapp.com/cyber-resilience/data-protection/data-backup-recovery/what-is-backup-recovery/
17. Powerful VMware Backup and Recovery [Online] 01.12.22 https://www.veeam.com/vmware-esx-backup.html
18. Fresnel zone [Online] 12.10.22 https://en.wikipedia.org/wiki/Fresnel_zone
19. MikroTik Routers and Wireless [Online] 01.12.22 https://mikrotik.com/product/sxt_r#fndtn-gallery
20. Free network monitoring with PRTG [Online] 01.12.22 https://www.paessler.com/howto-free-network-monitoring
21. How to set up bandwidth monitooring in PRTG in 4 steps [Online] 01.12.22 https://www.paessler.com/support/how-to/bandwidth-monitoring

LISA 1 HINNAPAKKUMISED UUTELE SEADMETELE

Objekti renoveerimise kulude kalkuleerimiseks tuleb teada projekteerimise maksumust, projektis ettenähtud töid ning loomulikult riistvara ja tarkvara maksumust.

Tabelis on toodud antud lõputöös kirjeldatud võrguseadmete hinnad, serveriprogrammid ja mõnede tööde maksumus.

	Uus server			
	Nimetus	**Kogus**	**Ühiku hind**	**Summa**
1	Dell Server R440 CPU 4214SILV 12C/24T,	1	1645.00	1645.00
	Raid H730P, Power Supply 550W			
2	RAM 32 GB, DDR4, Registered, ECC	2	196.00	392.00
3	Micron 5300 PRO SSD 960 GB, SATA 2.5"	4	174.00	696.00
4	MS Windows Server 2019 Standard, 16 cores	1	752.00	752.00
5	MS Windows Server 2019 Standard, 5 User OEM CAL	4	179.00	716.00
6	Vmware vSphere Standard	1	1322.00	1322.00
			Kokku KM-ga	**5523.00**

	Arvutid VMware serverite jaoks			
	Nimetus	**Kogus**	**Ühiku hind**	**Summa**
1	DELL Vostro 3910 i5-12400, 32GB, 512GB NVMe, W11 Pro	1	775.00	775.00
2	HP ProDesk 400 G7 i5-10500, 16GB, 256GB SSD, W11 Pro	2	660.00	660.00
			Kokku KM-ga	**1435.00**

	Võrguseadmed			
	Nimetus	**Kogus**	**Ühiku hind**	**Summa**
1	VPN Router MikroTik RB750Gr3	1	65.00	65.00
2	WiFi Router/AP TP-Link CPE510	4	57.00	228.00
3	Modbus RTU/ASCII Gateway	1	85.00	85.00
2	TP-LINK TL-SG1016PE Managed switch, POE+ , 16 ports	2	188.00	376.00
3	QNAP 4-Bay QTS NAS TS-431K, Hot-Swap, 2x1GbE	1	347.00	347.00
4	Router MikroTik SXT R, 10,5dBi w.o. LTE modem	1	85.00	85.00
5	Modem R11e-LTE	1	85.00	85.00
6	27U Põranda Kapp 19" 600X800 H=1380mm Klaasuksega	1	305.00	305.00
7	Samsung SSD PM893 960 GB for NAS	2	236.00	472.00
			Kokku KM-ga	**2048.00**

Tabel L1.1 hinnapakkumised uutele arvutivõrgu seadmetele

LISA 2 IT-SÜSTEEMI PARAMEETRITE TABEL. NÄITED

Layout of VLANs

Vlan number	Vlan name	Zone	Network	Gateway	DNS
Vlan10	NVR	SW1 NVR	192.168.1.0/24	192.168.1.1	192.168.5.221
Vlan20	FLOOR1	SW2, floor 1	192.168.2.0/24	192.168.2.1	192.168.5.221
Vlan30	FLOOR2	SW3, floor 2	192.168.3.0/24	192.168.3.1	192.168.5.221
Vlan40	FLOOR3	SW4, SW5 floor 3	192.168.4.0/24	192.168.4.1	192.168.5.221
Vlan50	SERVER	Server Lan1	192.168.5.0/24	192.168.5.1	192.168.5.221
Vlan60	AP-OUTDOOR	APs Mechanics, Shower room	192.168.6.0/24	192.168.6.1	192.168.5.221
Vlan70			192.168.7.0/24	192.168.7.1	192.168.5.221
Vlan99	IT-MGMT	IT Management	192.168.99.0/24	192.168.99.1	192.168.5.221

Interfaces of MikroTik R1		
	from SW	Vlans
ether1	WAN	
ether2	SW3 eth1 TP-Link floor 2	Vlan10, Vlan20, Vlan30, Vlan70
ether3	SW4 eth1 TP-Link floor 3	Vlan40, Vlan60
ether4	Server	Vlan50
ether5	IT admin PC	Vlan99

Interfaces of TP-Link SW4		
	from SW	Vlans
ether1	MikroTik R1 ether3, trunk	Vlan40, Vlan60

... | PCs | Users on FS on 09.12.2022 | Network devices | Wi-Fi AP | Switches | VLANs | VPN | MikroTik

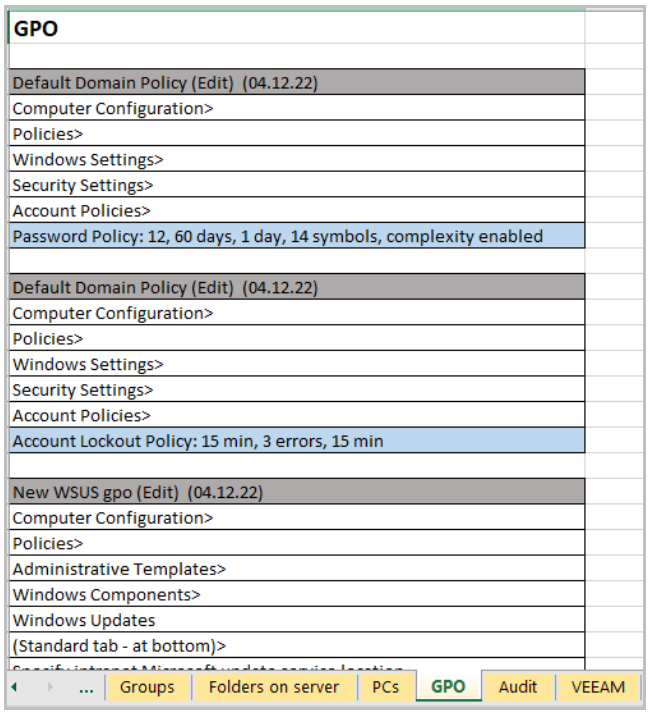
Tabel L2.1 VLAN konfiguratsioon renoveeritud IT süsteemis

Network devices

Device name	Room	IP	MAC address	VLAN	Switch	Interface
TP-Link CPE510 Cam	Box 3rd floor	192.168.1.	30:B5:C2:86:55:	Vlan10	SW3	17
TP-Link CPE510 Cam		192.168.1.	60:E3:27:72:3B:	Vlan10	SW3	17
TP-Link CPE510 Cam		192.168.1.	C4:E9:84:F5:47:	Vlan10	SW3	17
Dahua AP (Main)	Box 3rd floor	192.168.6.	38:AF:29:DE:83:	Vlan60	SW4	18
Dahua AP (Rail)	Rail	192.168.6.	38:AF:29:DE:8B	Vlan60	SW4	18
Ubiquiti AP (Main)	Box 3rd floor	192.168.6.	00:27:22:2E:60:	Vlan60	SW4	19
Ubiquiti AP (Shower room)	Shower room	192.168.6.	00:27:22:CC:C5:	Vlan60	SW4	19
MikroTik AP	3rd floor Conference	192.168.4.	B8:69:F4:34:D3:	Vlan40	SW4	7
MikroTik AP	3rd floor	192.168.4.	B8:69:F4:34:D3:	Vlan40	SW4	8
Canon MF240	Commerce	192.168.2.	84:BA:3B:96:7A	Vlan20	SW2	4
Canon MF240	Pearaamat	192.168.3.	9C:32:CE:54:F7:	Vlan30	SW3	8
Canon MF230	Finance	192.168.3.	74:BF:C0:24:1B:	Vlan30	SW3	11
Canon MF260	Lab	192.168.3.	74:BF:C0:8A:F6:	Vlan30	SW3	14
Canon MF445dw	Lab	192.168.3.	74:38:B7:FB:6D:	Vlan30	SW3	13
Edimax	AP	192.168.3.	74:DA:38:C9:FE	Vlan30	SW3	10
Canon MF440	Commerce	192.168.2.	00:BB:C1:76:DB	Vlan20	SW2	5
TP-Link CPE510 AP (Main)	Box 3rd floor	192.168.6.	70:4F:57:7D:57:	Vlan60	SW4	21
TP-Link CPE510 AP (Mechanics)	Mechanic`s service	192.168.6.	70:4F:57:7D:72:	Vlan60	SW4	21
TP-Link CPE510 AP (Ladu)	Ladu	192.168.6.	5C:A6:E6:AD:A9	Vlan60	SW4	21
TP-Link CPE510 AP (ASUTP)	ASUTP	192.168.6.	5C:A6:E6:AD:A7	Vlan60	SW4	21

Server | VM DC | VM FS | Network devices | Wi-Fi AP | Switches | VLANs | VPN | MikroTik | Use ...

Tabel L2.2 Arvutivõrgus olevate seadmete loend. Ilma arvutite ja IP-telefonideta



GPO
Default Domain Policy (Edit) (04.12.22)
Computer Configuration>
Policies>
Windows Settings>
Security Settings>
Account Policies>
Password Policy: 12, 60 days, 1 day, 14 symbols, complexity enabled
Default Domain Policy (Edit) (04.12.22)
Computer Configuration>
Policies>
Windows Settings>
Security Settings>
Account Policies>
Account Lockout Policy: 15 min, 3 errors, 15 min
New WSUS gpo (Edit) (04.12.22)
Computer Configuration>
Policies>
Administrative Templates>
Windows Components>
Windows Updates
(Standard tab - at bottom)>

... Groups | Folders on server | PCs | GPO | Audit | VEEAM

Tabel L2.3 Tabelis on näidatud iga kasutatud GPO konfigureerimise täielik tee

LISA 3 RUUTERIMEESKONDADE NIMEKIRI MIKROTIK RB750GR3

/system reset-configuration no-defaults=yes skip-backup-yes
Name of the router:
/system identity
set name "R1"
Then, in order to improve safety, need to disable all unused services, leave only Winbox:
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
For convenience, will be renamed the network interfaces and added comments:
/interface ethernet
set [find default-name=ether1] comment="WAN" name=ether1-wan
set [find default-name=ether2] comment="TRUNK 1" name=ether2-trunk
set [find default-name=ether3] comment="TRUNK 2" name=ether3-trunk
set [find default-name=ether4] comment="TRUNK 3" name=ether4-trunk
set [find default-name=ether5] comment="IT MGMT" name=ether1-it
Set the dynamic IP (from DHCP-server):
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=ether1-wan
The VLAN access ports layout uses bridges in RouterOS.
/interface bridge
add comment=NVR fast-forward=no name=bridge-vlan10-nvr
add comment=COMMERCE fast-forward=no name=bridge-vlan20-commerce
add comment=LAB fast-forward=no name=bridge-vlan30-lab
add comment=FINANCE fast-forward=no name=bridge-vlan40-finance
add comment=SERVER fast-forward=no name=bridge-vlan50-server
add comment=AP fast-forward=no name=bridge-vlan60-ap
add comment=TOP fast-forward=no name=bridge-vlan70-top
add comment=IT_MGMT fast-forward=no name=bridge-vlan99-it-mgmt
Prior to the setting of the DHCP, a pool of addresses must be created for each enumeration:
/ip pool
add comment=NVR name=pool-vlan10-nvr ranges=192.168.1.100-192.168.1.199
add comment=COMMERCE name=pool-vlan20-commerce ranges=192.168.2.100-192.168.2.199
add comment=LAB name=pool-vlan30-lab ranges=192.168.3.100-192.168.3.199
add comment=FINANCE name=pool-vlan40-finance ranges=192.168.4.100-192.168.4.199
add comment=SERVER name=pool-vlan50-server ranges=192.168.5.100-192.168.5.199
add comment=AP name=pool-vlan60-ap ranges=192.168.6.100-192.168.6.199
add comment=TOP name=pool-vlan70-top ranges=192.168.7.100-192.168.7.199

add comment=IT_MGMT name=pool-vlan99-it-mgmt ranges=192.168.99.100-192.168.99.199
Will assign all the IPs with DHCP servers. Each server will issue an IP from its own pool:
/ip dhcp-server
add address-pool=pool-vlan10-nvr disabled=no interface=bridge-vlan10-nvr name=dhcp-vlan10-nvr
add address-pool=pool-vlan20-commerce disabled=no interface=bridge-vlan20-commerce name=dhcp-vlan20-commerce
add address-pool=pool-vlan30-lab disabled=no interface=bridge-vlan30-lab name=dhcp-vlan30-lab
add address-pool=pool-vlan40-finance disabled=no interface=bridge-vlan40-finance name=dhcp-vlan40-finance
add address-pool=pool-vlan50-server disabled=no interface=bridge-vlan50-server name=dhcp-vlan50-server
add address-pool=pool-vlan60-ap disabled=no interface=bridge-vlan60-ap name=dhcp-vlan60-ap
add address-pool=pool-vlan70-top disabled=no interface=bridge-vlan70-top name=dhcp-vlan70-top
add address-pool=pool-vlan99-it-mgmt disabled=no interface=bridge-vlan99-it-mgmt name=dhcp-vlan99-it-mgmt
In each subnet, will be assigned own IP to the router:
/ip address
add address=192.168.1.254/24 comment=NVR interface=bridge-vlan10-nvr
add address=192.168.2.254/24 comment=COMMERCE interface=bridge-vlan20-commerce
add address=192.168.3.254/24 comment=LAB interface=bridge-vlan30-lab
add address=192.168.4.254/24 comment=FINANCE interface=bridge-vlan40-finance
add address=192.168.5.254/24 comment=SERVER interface=bridge-vlan50-server
add address=192.168.6.254/24 comment=AP interface=bridge-vlan60-ap
add address=192.168.7.254/24 comment=TOP interface=bridge-vlan70-top
add address=192.168.99.254/24 comment=IT_MGMT interface=bridge-vlan99-it-mgmt
Then, for each subnet, indicate the DNS and the locks used by default:
/ip dhcp-server network
add address=192.168.1.0/24 comment=NVR dns-server=192.168.5.223 gateway=192.168.1.254 netmask=24
add address=192.168.2.0/24 comment=COMMERCE dns-server=192.168.5.223 gateway=192.168.2.254 netmask=24
add address=192.168.3.0/24 comment=LAB dns-server=192.168.5.223 gateway=192.168.3.254 netmask=24
add address=192.168.4.0/24 comment=FINANCE dns-server=192.168.5.223 gateway=192.168.4.254 netmask=24
add address=192.168.5.0/24 comment=SERVER dns-server=192.168.5.223 gateway=192.168.5.254 netmask=24
add address=192.168.6.0/24 comment=AP dns-server=192.168.5.223 gateway=192.168.6.254 netmask=24
add address=192.168.7.0/24 comment=TOP dns-server=192.168.5.223 gateway=192.168.7.254 netmask=24
add address=192.168.99.0/24 comment=IT_MGMT dns-server=192.168.5.223 gateway=192.168.99.254 netmask=24
The interfaces ether2 and ether3 need to be turned into trunks by giving the right vlan to each port:
/interface vlan
add interface=ether2-trunk name=vlan10-trunk-to-uby vlan-id=10
add interface=ether2-trunk name=vlan20-trunk-to-uby vlan-id=20
add interface=ether2-trunk name=vlan30-trunk-to-uby vlan-id=30
add interface=ether2-trunk name=vlan70-trunk-to-uby vlan-id=70

add interface=ether3-trunk name=vlan40-trunk-to-tplink vlan-id=40
add interface=ether3-trunk name=vlan60-trunk-to-tplink vlan-id=60
add interface=ether4-trunk name=vlan50-trunk-to-vmware vlan-id=50
VLAN's been created, but ports other2 and other3 are still unlinked.
With the help of the bridge, should be combined each vlan into bridge, and also placed the corresponding ports of access:
/interface bridge port
add bridge=bridge-vlan10-nvr comment="VLAN10" interface=vlan10-trunk-to-uby
add bridge=bridge-vlan20-commerce comment="VLAN20" interface=vlan20-trunk-to-uby
add bridge=bridge-vlan30-lab comment="VLAN30" interface=vlan30-trunk-to-uby
add bridge=bridge-vlan70-top comment="VLAN70" interface=vlan70-trunk-to-uby
add bridge=bridge-vlan40-finance comment="VLAN40" interface=vlan40-trunk-to-tplink
add bridge=bridge-vlan60-ap comment="VLAN60" interface=vlan60-trunk-to-tplink
add bridge=bridge-vlan50-server comment="VLAN50" interface=vlan50-trunk-to-vmware
add bridge=bridge-vlan99-it-mgmt comment="VLAN99" interface=ether5
VLAN's part on the R1 is all set. For ease of operation with Firewall, filters and limitations, need to be created two lists of interfaces:
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
Then the interfaces will be divided into groups:
/interface list member
add interface=ether1-wan list=WAN
add interface=bridge-vlan10-nvr list=LAN
add interface=bridge-vlan20-commerce list=LAN
add interface=bridge-vlan30-lab list=LAN
add interface=bridge-vlan40-finance list=LAN
add interface=bridge-vlan50-server list=LAN
add interface=bridge-vlan60-ap list=LAN
add interface=bridge-vlan70-top list=LAN
add interface=bridge-vlan99-it-mgmt list=LAN
If will be used PPPOE, WAN should also be added ether1 and pope-client. So is VPN.
Bridge-vlan99-it-mgmt is added to the list of LAN-interfaces.
First, access to the Internet is needed in this network.
Secondly, need to keep Mikrotik in control from this network.
So that Mikrotik doesn't show up in Winbox Neighbor, should be imposed restrictions, indicating access to the LAN group:
/ip neighbor discovery-settings
set discovery-interface-list=LAN
Additionally, limit the connection to Mikrotik by MAC:
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox
set allowed-interface-list=LAN
Connections will only be allowed from LAN-group interfaces.

In order for users of all networks to be able to access the Internet, requests for the DNS server must be approved and the masquerading set up:
/ip dns
set allow-remote-requests=yes
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" ipsec-policy=out,none out-interface-list=WAN
If any VLAN is banned, then in the src.address, we clearly indicate only authorized networks: 192.168.2.0/24, etc.
The rules must be given before the following:
/ip firewall filter
add action=accept chain=input comment="defconf: accept established,related,untracked" connection-state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec policy" ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec policy" ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" connection-state=established,related
add action=accept chain=forward comment="defconf: accept established,related, untracked" connection-state=established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" connection-state=invalid
add action=drop chain=forward comment="defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat connection-state=new in-interface-list=WAN
There are nuances that are not mentioned in many instructions. The fact is, the Layer 2, VLANs are completely isolated among themselves.
But with Layer 3, it's not that simple.
The router knows all the addresses and subnets, so sometimes the devices from one VLAN can see the devices from another VLAN.
Could be wrote a disabling rule on Firewall for a chain forward.
But better will be implement this more aesthetically - through the rules of routing:
/ip routes rule
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.2.0/24
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.3.0/24
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.4.0/24
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.5.0/24
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.6.0/24
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.7.0/24
add action=unreachable dst-address=192.168.1.0/24 src-address=192.168.99.0/24
add action=unreachable dst-address=192.168.2.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.2.0/24 src-address=192.168.3.0/24
add action=unreachable dst-address=192.168.2.0/24 src-address=192.168.4.0/24
add action=unreachable dst-address=192.168.2.0/24 src-address=192.168.6.0/24
add action=unreachable dst-address=192.168.2.0/24 src-address=192.168.7.0/24
add action=unreachable dst-address=192.168.2.0/24 src-address=192.168.99.0/24

add action=unreachable dst-address=192.168.3.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.3.0/24 src-address=192.168.2.0/24
add action=unreachable dst-address=192.168.3.0/24 src-address=192.168.4.0/24
add action=unreachable dst-address=192.168.3.0/24 src-address=192.168.6.0/24
add action=unreachable dst-address=192.168.3.0/24 src-address=192.168.7.0/24
add action=unreachable dst-address=192.168.3.0/24 src-address=192.168.99.0/24
add action=unreachable dst-address=192.168.4.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.4.0/24 src-address=192.168.2.0/24
add action=unreachable dst-address=192.168.4.0/24 src-address=192.168.3.0/24
add action=unreachable dst-address=192.168.4.0/24 src-address=192.168.6.0/24
add action=unreachable dst-address=192.168.4.0/24 src-address=192.168.7.0/24
add action=unreachable dst-address=192.168.4.0/24 src-address=192.168.99.0/24
add action=unreachable dst-address=192.168.5.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.6.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.6.0/24 src-address=192.168.2.0/24
add action=unreachable dst-address=192.168.6.0/24 src-address=192.168.3.0/24
add action=unreachable dst-address=192.168.6.0/24 src-address=192.168.4.0/24
add action=unreachable dst-address=192.168.6.0/24 src-address=192.168.7.0/24
add action=unreachable dst-address=192.168.6.0/24 src-address=192.168.99.0/24
add action=unreachable dst-address=192.168.7.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.7.0/24 src-address=192.168.2.0/24
add action=unreachable dst-address=192.168.7.0/24 src-address=192.168.3.0/24
add action=unreachable dst-address=192.168.7.0/24 src-address=192.168.4.0/24
add action=unreachable dst-address=192.168.7.0/24 src-address=192.168.6.0/24
add action=unreachable dst-address=192.168.7.0/24 src-address=192.168.99.0/24
add action=unreachable dst-address=192.168.99.0/24 src-address=192.168.1.0/24
add action=unreachable dst-address=192.168.99.0/24 src-address=192.168.2.0/24
add action=unreachable dst-address=192.168.99.0/24 src-address=192.168.3.0/24
add action=unreachable dst-address=192.168.99.0/24 src-address=192.168.4.0/24
add action=unreachable dst-address=192.168.99.0/24 src-address=192.168.6.0/24
add action=unreachable dst-address=192.168.99.0/24 src-address=192.168.7.0/24
Setup of VPN L2TP+Ipsec
Adding a new subnet:
/ip pool add name=vpnpool ranges=192.168.111.100-192.168.111.199
First you need to set network parameters for VPN clients:
/ppp profile
add change-tcp-mss=yes dns-server=192.168.111.1 local-address= 192.168.111.1 name=l2tp remote-address=pool-1 use-encryption=yes
Activation of the VPN server **(only mschap2)**:

/interface l2tp-server server
set authentication=mschap2 default-profile=l2tp enabled=yes ipsec-secret=edruzam@Tulemyyr#2022 use-ipsec=required
Creation of a VPN account for a client:
/ppp secret
add name=user1 password=user1 profile=l2tp
add name=user2 password=user2 profile=l2tp
Firewall for the client's VPN permits:
/ip firewall filter
add action=accept chain=input comment="Port Access" dst-port=500,1701,4500 in-interface=WAN protocol=udp
add action=accept chain=input comment="Ipsec-esp" protocol=ipsec-esp
add action=accept chain=forward comment="vpn-to-vlan50" src-address=192.168.111.0/24 in-interface=!ether1-wan out-interface=bridge-vlan50-server
IPsec setting:
/ip ipsec proposal
add auth-algorithms=sha1 enc-algorithms=aes-128-cbc,aes-192-cbc lifetime=8h name=Proposal-IpSec
or add **aes-128 cbc** to the "default" proposal (if encryption is required in the Windows VPN client).

Tabel L3.1. RB750gr3 ruuteri konfigureerimine