LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Yrityksen tietoverkon parantaminen ja demonstraatiotilan toteuttaminen

Case: Ictum Oy

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2016
Sami Kemppinen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KEMPPINEN, SAMI:

Yrityksen tietoverkon parantaminen ja demonstraatiotilan toteuttaminen
Case: Ictum Oy

Tietoliikennetekniikan opinnäytetyö, 49 sivua

Kevät 2016

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli parantaa Ictum Oy:n tietoverkkoa demonstraatiotilan rakentamista varten. Ictum Oy tarvitsi myynnin edistämiseksi demonstraatiotilan, jossa he voivat esitellä asiakkaille tulevia ratkaisuja.

VPN ja virtualisointi ovat nykypäivänä monelle yrityksille tärkeitä osa-alueita. Suurin osa yrityksistä, joilla on monta toimipistettä, käyttävät VPN-tekniikkaa yrityksen sisäverkkojen yhdistämiseksi. Virtualisointi on myös yleistynyt yrityksissä, koska sen tuomat edut ovat suuria. Virtualisointi tarjoaa yritykselle kustannustehokasta ja joustavaa ratkaisua palvelintarpeisiin, ja todennäköisesti virtualisoinnin käyttö tulee lisääntymään huomattavasti.

Tietoverkon keskeisiä osa-alueita ovat VPN-tekniikat sekä virtualisointi. Käytännön työssä toteutus aloitettiin kartoittamalla yrityksen nykyinen tilanne. Kartoituksen perusteella yritykselle luotiin uusi ratkaisumalli. Ratkaisumallissa vertailtiin myös AC-standardin tukiasemia, tyypin 2 virtualisointialustoja, VPN Client -ohjelmia sekä IPSec VPN ja SSL VPN -protokollien eroja toimipisteiden yhdistämistä varten.

Ratkaisumallin perusteella Lahden ja Vantaan toimipisteiden välille luotiin IPSec VPN-yhteys kahta Netgear FVS336Gv2 VPN-palomuuria hyödyntäen, jotta saatiin toimipisteiden aliverkot yhdistettyä. Vantaan toimipisteelle konfiguroitiin uusi AC-standardin WLAN-tukiasema nopeampia langattomia yhteyksiä varten. Lopuksi Vantaan toimipisteelle asennettiin tyypin 2 virtualisointialusta VMware Workstation, johon lisättiin kaksi valmista virtuaalipalvelinta. Lopputuloksena Ictum Oy sai toimivan demonstraatiotilan myynnin edistämistä varten.

Asiasanat: tietoverkko, VPN, virtualisointi

Lahti University of Applied Sciences
Faculty of Technology

KEMPPINEN, SAMI:

Improving a company network and building a demo space
Case: Ictum Oy

Bachelor's Thesis in Telecommunications, 49 pages

Spring 2016

ABSTRACT

In this thesis the purpose was to improve the company network of Ictum Oy and build them a new demo space. Ictum Oy needed demo space for promoting their upcoming solutions for customers.

VPN and virtualization are important for many companies nowadays. Most companies that have multiple offices are using VPN techniques for connecting their local area networks between offices. Virtualization has become more common, because of its big benefits. Virtualization also brings cost-effective and flexible solutions for server requirements and the use of virtualization is likely going to expand considerably.

The key components for network are VPN techniques and virtualization. The practical implementation started by surveying the company's current situation and the plan for the new solution was based on this survey. The plan also included comparition of AC standard WLAN access points, type 2 virtualization platforms, VPN client software and the differences between the IPSec VPN or SSL VPN protocols for connecting different offices.

Based on the plan, an IPSec VPN connection was created between the Lahti and Vantaa offices, using two Netgear FVS336Gv2 VPN firewalls so local area networks could be connected.A new AC standard WLAN access point was configured to the Vantaa office for faster wireless connections. Also, a type 2 virtualization platform VMWare Workstation was installed, and two preinstalled virtual servers were added to it. As the end result, Ictum Oy got a working demo space for promoting upcoming solutions for customers.

Keywords: network, VPN, virtualization

SISÄLLYS

LYHENNELUETTELO

CHAP	Challenge Handshake Authentication Protocol. Autentikointi-menetelmä.
CMS	Content Management System. Ohjelmisto digitaalisen sisällön syöttämiseen.
DHCP	Dynamic Host Configuration Protocol. Protokolla, jonka yleisin tehtävä on jakaa IP-osoitteita laitteille.
DNS	Domain Name System. Nimipalvelujärjestelmä.
DSM	Digital Signage Manager. Ohjelmisto digitaalisen sisällön valvontaan.
ESP	Encapsulating Security Payload. Pakettivirtojen turvaamiseen tarkoitettu protokolla.
FQDN	Fully Qualified Domain Name. Absoluuttinen verkkotunnuksen nimi.
GRE	Generic Routing Encapsulation. Tunnelointi -protokolla.
IKE	Internet Key Exchange. Avaimenvaihto -protokolla.
IP	Internet Protocol. TCP/IP-mallin Internet-kerroksen -protokolla.
IPv4	Internet Protocol version 4. Internet protokollan 4. versio.
IPv6	Internet Protocol version 6. Internet protokollan 6. versio.
IPSec	IP Security. Joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen.

ISO	International organization for standardization, kansainvälinen organisaatio, joka asettaa standardeja.
ISP	Internet Service Provider. Internet-palveluntarjoaja, joka tarjoaa asiakkaalleen internet-yhteyden.
L2TP	Layer 2 Tunneling Protocol. Tunnelointi -protokolla.
LAN	Local Area Network. Lähiverkko.
MAC	Media Access Control. Verkkosovittimen ethernet-verkossa yksilöivä osoite.
NAT	Network Address Translation. Osoitteenmuunnos.
PAP	Password Authentication Protocol. Salasanan autentikointi -protokolla.
PPP	Point-to-Point Protocol. Tiedonsiirtoon käytetty protokolla, jota käytetään suoraan yhteyteen.
PPTP	Point-to-Point Tunneling Protocol. Tiedonsiirtoon käytetty tunnelointi -protokolla, jota käytetään suoraan yhteyteen.
PSK	Pre-Shared Key. Etukäteen jaettu kryptausavain.
RAM	Random-Access Memory. Keskusmuisti.
RAS	Remote Access Service. Kryptausmenetelmä.
SSL	Secure Sockets Layer. Salausprotokolla.
TCP	Transmission Control Protocol. Protokolla, jota käytetään luomaan yhteyksiä tietokoneiden välille.
USB	Universal Serial Bus. Yleisesti käytössä oleva sarjaväyläarkkitehtuuri.
VPN	Virtual Private Network. Virtuaalinen lähiverkko.

WAN	Wide Area Network. Ulkoverkko.
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 JOHDANTO

Ictum Oy on digitaaliseen esitys- ja audiovisuaaliseen tekniikkaan erikoistunut yritys, joka on perustettu vuonna 2005. Toimipisteet sijaitsevat Lahdessa ja Vantaalla, mutta tarvittaessa palvelevat asiakkaita ympäri Suomea. (Ictum Oy 2016.)

Opinnäytetyön tavoitteena on rakentaa toimiva demonstraatiotila yrityksen kahden toimipisteen välille myynnin edistämiseksi. Demonstraatiotilan toimimista varten täytyy olla yhteys kahden toimipisteen välillä, jota ei tällä hetkellä ole. Muina vaatimuksina demonstraatiotilalle on nopea langaton internetyhteys langatonta esitystekniikkaa varten sekä VMware virtualisointialusta digitaalisen infosisällön esittämistä varten.

Opinnäytetyön teoriaosuudessa käydään läpi yleisesti tietoverkkoja, tutkitaan eri VPN-tekniikoita (Virtual Private Network) ja protokollia. Lopuksi tutustutaan yleisellä tasolla virtualisointiin.

Käytännönosuudessa toteutetaan yrityksen tietoverkon parantaminen. Ensimmäisenä kartoitetaan yrityksen tämänhetkinen tilanne. Kartoituksen pohjalta vertaillaan eri laitteita sekä ohjelmistoja ja luodaan yritykselle ratkaisumalli, jonka jälkeen ratkaisumalli toteutetaan.

2 TIETOVERKKO

2.1 Yleistä tietoverkoista

Tietoverkot alkoivat yleistyä 1950-luvulla. Siihen aikaan tietoliikenne koostui reikäkorteista, joita käytettiin suurtietokoneissa. Virkailijat kantoivat reikäkortteja suurtietokoneelta toiselle. Ensimmäisenä korjauksena yritettiin pidentää suurtietokoneelta päätteeseen vievää kaapelia ja näin vähentää konkreettista kantomatkaa. Käytännössä asia ei toiminut ja keksittiin kytkeä suurtietokoneeseen useampia päätteitä ja siitä syntyi tietoverkko. (Koulutus & Konsultointi 2016a.)

Tietoverkon tärkein tehtävä on siirtää dataa tietoverkon välillä. Data kulkee yleensä joko lanka- tai kuparikaapelia pitkin, mutta nykyään myös optiset kuidut ja langattomat verkot ovat yleistyneet. Siirtolinja, jota pitkin data kulkee, on tärkeässä asemassa tietoverkon nopeuteen ja tiedonsiirtokapasiteettiin nähden, eli oikean siirtolinjan valitsimen on otettava huomioon tietoverkkoa rakentaessa. (Koulutus & Konsultointi 2016b.)

OSI-malli (Open Systems Interconnection) on ISO:n (International Organization for Standardization) määrittelemä kansainvälinen standardi. OSI-mallilla on seitsemän kerrosta, joista monella on merkittävä rooli tietoverkoissa. OSI-mallin kerrosten ideana on, että ylempi kerros käyttää aina hyväkseen alempia kerroksia (kuvio 1). (Microsoft 2016a.)

KUVIO 1. OSI-malli (Wikipedia 2016c)

Fyysisen kerroksen tehtävänä on datan siirtäminen lähettäjän ja vastaanottajan välillä sähköisesti, optisesti tai radiosignaaleina. Kerros muuttaa bitit eli 1:t ja 0:t tarvittavaan muotoon. (Microsoft 2016a.)

Siirtokerros huolehtii päätepisteiden välisestä yhteydestä, eli siirtokerroksessa luodaan ja puretaan yhteydet. Siirtokerros myös kehystää ylempien kerrosten paketteja fyysiseen kerrokseen siirtoa varten. Kytkimet toimivat usein siirtokerroksessa. (Microsoft 2016a.)

Verkkokerros hoitaa reitityksen, jotta paketit löytäisivät parhaan mahdollisen reitin päämäärään. Verkkokerros myös tarjoaa ylemmille kerroksille yhteyden, joka ei ota kantaa verkon rakenteeseen. Reitittimet toimivat verkkokerroksessa. (Microsoft 2016a.)

Kuljetuskerros tarjoaa tietoliikenneyhteyden tietoverkkoa varten. Kuljetuskerros myös varmistaa, että datan mukana ei tule virheitä tai puutteita ja muuttaa datan oikeanlaiseen muotoon. (Microsoft 2016a.)

Istuntokerros avaa yhteyden viestintää varten, jotta kaksi ohjelmaa voi kommunikoida sekä käyttää yhteyttä keskenään. Istuntokerros hoitaa myös tunnistautumisen, koska jotkut sovellukset vaativat tunnistautumista ennen istunnon avaamista. (Microsoft 2016a.)

Erityistapakerros muokkaa datan oikeaan muotoon sovelluskerrosta ja kuljetuskerrosta varten. Erityistapakerroksen avulla esimerkiksi kuvat ja

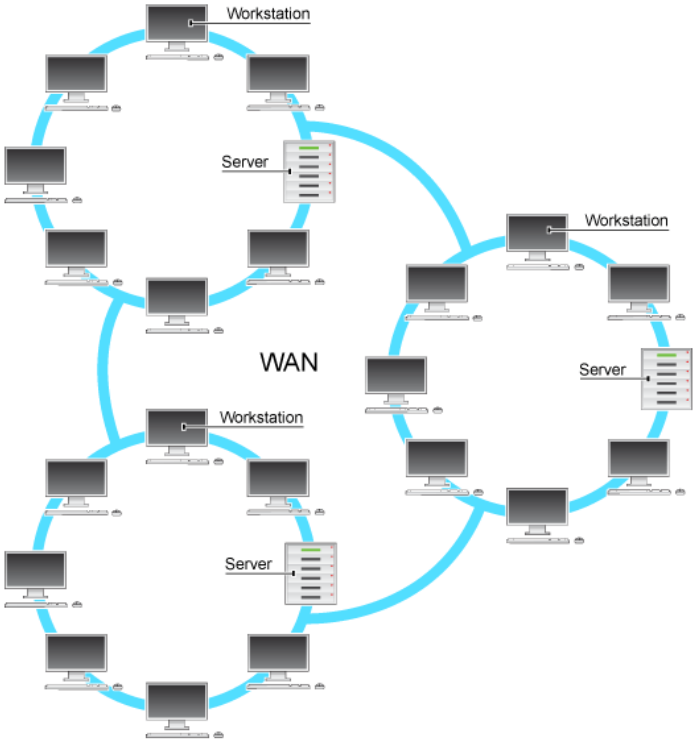
sähköpostit näkyvät oikein kaikilla käyttäjillä. (Microsoft 2016a.)

Sovelluskerros toimii linkkinä sovelluksen ja käyttäjän välillä. Sovelluskerroksessa toimii kaikki eri ohjelmat, kuten internet-selain. (Microsoft 2016a.)

2.2 Ulkoverkko

Ulkoverkko eli WAN (Wide Area Network) on verkko, joka yleensä yhdistää koneita laajalta alueelta. Ulkoverkkoa voidaan käyttää yhdistämään esimerkiksi kaupunkeja tai maita. Ulkoverkko toimi lähes samalla tavalla sisäverkon kanssa, mutta käytännössä ulkoverkko on toteutettu eri tekniikalla. Ulkoverkon käyttäjä ei yleensä omista yhteyttä vaan käyttäjä ostaa ulkoverkon palveluntarjoajalta, minkä jälkeen käyttäjä voi yhdistää oman sisäverkon ulkoverkkoon. Ulkoverkko ei käytännössä yhdistä laitteita vaan ulkoverkko yhdistää sisäverkkoja, jotka taas yhdistävät laitteita (kuvio 2). (Gale 2007.)

Ulkoverkko voi käyttää joko point-to-point -yhteyttä eli suoraa yhteyttä kahden pisteen välillä. Nykyisin ulkoverkoissa käytetään pääsääntöisesti paketinvaihtoyhteyttä, jossa viesti pilkotaan paketeiksi ja paketit voivat siirtyä eri reittejä haluttuun määränpäähän, paketinvaihto yhteys on tästä syystä myös nopeampi protokolla kuin point-to-point. Kun paketit ovat saapuneet määränpäähän, paketit yhdistetään alkuperäiseksi viestiksi. (Gale 2007.)



KUVIO 2. Esimerkki ulkoverkosta (BBC 2014)

2.3 Lähiverkko

Lähiverkko eli LAN (Local Area Network) on nopea verkko, joka on maantieteellisesti rajatun alueen sisäinen tietoliikenteen toteuttava verkko. Lähiverkko on tavallisesti ulkoverkosta poiketen organisaation tai yksityisen henkilön hallinnassa. Lähiverkko koostuu kaapeleista, työasemista, palvelimista sekä palveluista. Lähiverkkoihin käytetään pääsääntöisesti Ethernet- tai WLAN-tekniikkaa (Wireless Local Area Network). (The Gale Group 2002.)

Lähiverkkoa voidaan myös pilkkoa pienempiin osiin (kuvio 3). Pilkkomista kutsutaan aliverkottamiseksi. Aliverkotus on mahdollista käyttäen hyväksi aliverkon peitettä, jolla on samanlainen hierarkia kuin IPv4-osoitteella (Internet Protocol versio 4) (taulukko 1). Aliverkotusta hyödynnetään myös, jos esimerkiksi yrityksellä olisi kaksi osastoa, joista toisella osastolla olisi arkaluontoista sisältöä, jotta he eivät pääsisi toistensa aliverkkoihin käsiksi (taulukko 2). (Mitchell 2015.)

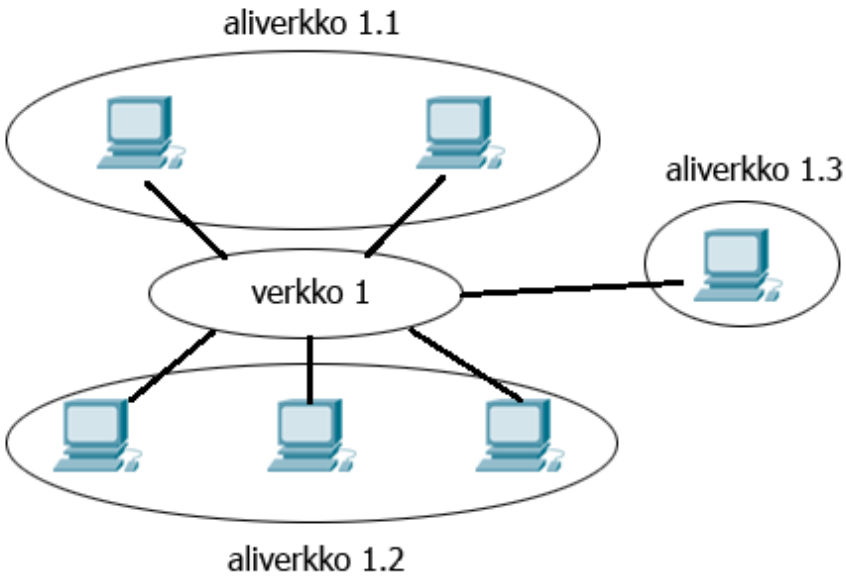
TAULUKKO 1. C-luokan aliverkon peitteet

C	Aliverkon peite	Aliverkkojen määrä	Osoitteita	Työasemia
/24	255.255.255.0	1	256	254
/25	255.255.255.128	2	128	126
/26	255.255.255.192	4	64	62
/27	255.255.255.224	8	32	30
/28	255.255.255.240	16	16	14
/29	255.255.255.248	32	8	6
/30	255.255.255.252	64	4	2

Esimerkkinä aliverkotetaan pienyrityksen eli taulukon 2 verkko kolmeen C-luokan aliverkkoon. Ensimmäisenä kannattaa muistaa, että C-luokan aliverkkoja voi olla (2,) 4, 8, 16, 32 64 … kappaletta. Taulukon 1 mukaan voidaan miettiä, mikä olisi yrityksen kannalta järkevin vaihtoehto aliverkkojen ja työasemien kannalta. Oletetaan, että myöhemmin tarvitaan laajennusta, joten valitaan /28 peitteen aliverkko, eli 255.255.255.240, jossa aliverkkoja on 16 ja osoitteita 16. Näistä osoitteista ensimmäinen on varattu verkon osoitteelle ja viimeinen mainostukselle, joten käytössä on 14 osoitetta jokaista aliverkkoa kohti. (Puska 2000, 149 – 151.)

TAULUKKO 2. C-luokan aliverkotus

Verkko	Ensimmäinen IP	Viimeinen IP	Käyttö
.0	192.168.1.0	192.168.1.15	Aliverkko 1.1
.16	192.168.1.16	192.168.1.31	Aliverkko 1.2
.32	192.168.1.32	192.168.1.47	Aliverkko 1.3
.48	192.168.1.48	192.168.1.63	Varalla
.64	192.168.1.64	192.168.1.79	Varalla



KUVIO 3. Aliverkon periaate

2.4 IP-osoitteet

IPv4-osoite on 32-bittinen osoite, joten osoitteiden määrä on rajattu maailmassa 4 294 2967 296 (2^{32}) osoitteeseen. Rajallisten osoitteiden määrän takia yleisesti käytetään osoitteenmuunnosta tai porttimuunnosta osoitteiden lisäämiseksi.

IPv4-osoite koostuu neljästä kahdeksan bitin oktetista, joka on luettavuuden kannalta muunnettu desimaalimuotoon esimerkkinä osoite 175.14.200.15. Taulukon 3 ensimmäisessä kentässä on IP-osoitteen desimaalimuoto ja toisessa kentässä havainnollistettu bitti muoto kyseiselle osoitteelle.

TAULUKKO 3. IPv4-osoite

175 . 14 . 200 . 15
10101111 . 00001110 . 11001000 . 00001111
4 x 8 bitin lohkoa

Koko IPv4-osoiteavaruus on jaettu viiteen eri luokkaan A-E, jotka käsittävät eri osoitealueet, jotka määräävät koneiden määrän tai tarkoituksen (taulukko 4). Kyseisistä luokista voidaan tunnistaa taulukon 5 avulla, miten osoitteen luokat ja kentät liittyvät toisiinsa (taulukko 5). (Hakala & Vainio 2005, 192.)

TAULUKKO 4. Osoiteluokat

Luokka	Osoitealue	Koneiden määrä tai tarkoitus
A	000.000.000.000 - 127.255.255.255	16 000 000
B	128.000.000.000 - 191.255.255.255	65 534
C	192.000.000.000 - 223.255.255.255	254
D	224.000.000.000 - 239.255.255.255	Multicast
E	240.000.000.000 - 255.255.255.255	Kokeilut

TAULUKKO 5. Luokkien tunnistus

	1. Oktetti	2. Oktetti	3. Oktetti	4. Oktetti
A	verkko	kone	kone	kone
B	verkko	verkko	kone	kone
C	verkko	verkko	verkko	kone

IPv6 on uusin versio Internet Protokollasta, joka vahvistettiin vuonna 1995. Kyseinen protokolla kehitettiin vastaamaan IPv4-osoitteiden loppumista varten sekä laajentamaan osoitteistusmahdollisuuksia. 32-bittisestä koosta 128-bittiseen kokoon siirtyminen tarkoittaa, että osoitteita on käytännössä loputon määrä, kun taas IPv4-osoitteita on vain noin 4,3 miljardia. (RFC 2460, 1998.)

IPv6:n merkittävimpiä eroja ovat, että IPv6-osoitteet ovat luokattomia, mutta niissä on hierarkia, josta selviää, mille operaattorille kyseinen osoite kuuluu sekä missä se maantieteellisesti sijaitsee. Toisaalta IPv6:n

mahdollistavien runkoreitittimien uusiminen sekä osoitteenmuunnos on mahdollistanut laajenevan IPv4-osoitteiden käytön ilman osoitteiden loppumisen vaaraa. Lisäksi reititysongelmat ovat siirtäneet IPv6-standardiin siirtymistä vuosilla eteenpäin. Uusien koneiden sekä langattomien laitteiden määrän arvioidaan kuitenkin kasvavan koko ajan nopeammin, joten on vain ajan kysymys koska varsinainen siirtymä IPv6-standardiin toteutuu. (Hakala & Vainio 2005, 216.)

IPv6:ssa ei käytetä IPv4:n tapaan broadcast-osoitteita, vaan niiden sijasta käytetään multicast-osoitteita, jotka jakavat laitteet multicast-ryhmiin. Verkon kaikki koneet muodostavat ryhmiä ja paketit lähetetään muodostetuille ryhmille. IPv4:n broadcastilla paketit lähetetään verkon jokaiselle koneelle. Näin säästetään verkon kuormitusta. IPv6:n mukana tuli myös uusi osoitemuoto anycast. Anycastin avulla on mahdollista tarjota palveluita monesta eri lähteestä yhdellä osoitteella. (Hakala & Vainio, 216.)

IPv6-osoite koostuu kahdeksasta kahdeksan bitin oktetista, joka on muunnettu heksadesimaalimuotoon ja eroteltu kaksoispistein. IPv6-osoitteessa nollat voidaan korvata kahdella kaksoispisteellä ”::” tai yhdellä nollalla, josta esimerkkinä:

2001:cdaa:9d38:0000:0000:0000:3255:7242

2001:cdaa:9d38:0:0:0:3255:7242

2001:cdaa:9d38::3255:7242

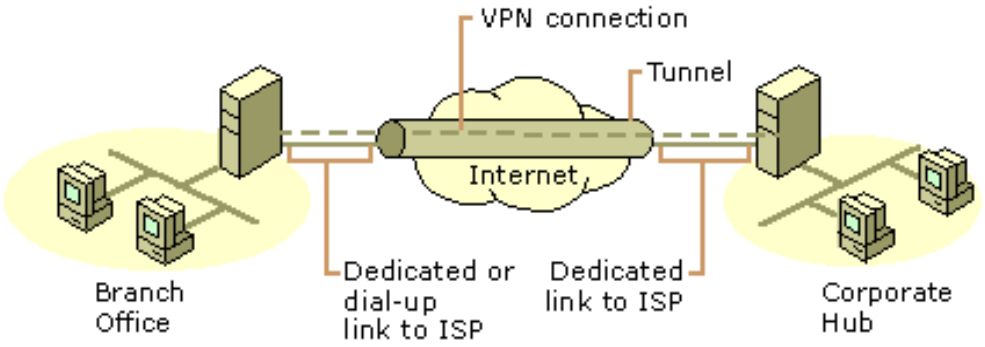
(Das 2008.)

3 VPN

3.1 Yleistä VPN:stä

VPN kehitettiin vastamaan yritysten tietoturvan parantamista. Yritykset tarvitsivat tavan, jolla voidaan olla yhteydessä luotettavasti, nopeasti ja tietoturvallisesti muihin yritysten toimipisteisiin. (Cisco 2008b.)

VPN on virtuaalinen yksityinen verkko, jolla voidaan yhdistää kaksi tai useampia yksityisiä verkkoja yhteen julkista verkkoa käyttäen. VPN käyttää virtuaalista reititystä julkisen internetin läpi ja luo tunnelin kahden VPN kohteen välille (kuvio 4). (Cisco 2008b.)

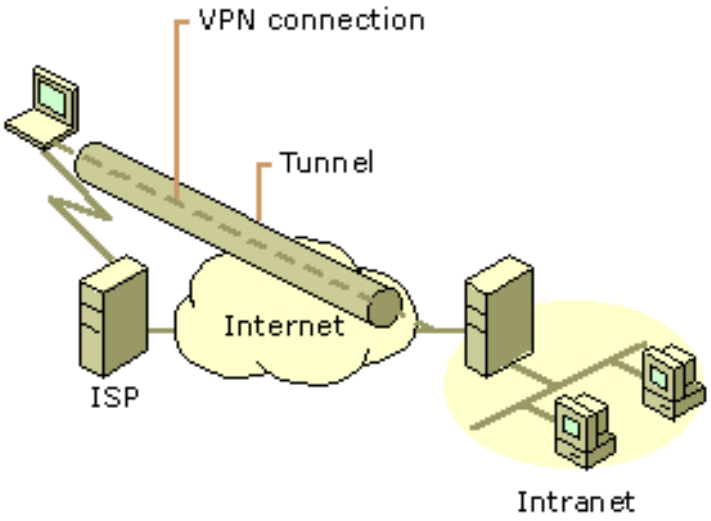


KUVIO 4. VPN Site-to-Site kahden toimipisteen välillä (Microsoft 2001c)

Tunnelin luomisen lisäksi pitää ottaa huomioon tunnelin tietoturva. Tämä edellyttää salaustekniikoita sekä käyttäjien tunnistautumista. Yleensä VPN-yhteys muodostetaan kahden VPN-laitteen välille, joihin konfiguroidaan tunneli. VPN -yhteyttä voidaan myös käyttää etäohjelmiston avulla yhden ihmisen tarpeisiin esimerkiksi työskennellessä kotoa käsin. (Hakala & Vainio 2005, 381-382.)

Käytössä on siis yleisesti kaksi erilaista VPN-tekniikkaa. Ensimmäinen tekniikka on Remote-Access VPN eli VPN-yhteys yhden käyttäjän koneelta esimerkiksi yrityksen lähiverkkoon VPN Client -ohjelmaa hyödyntäen (kuvio 5). Esimerkki Remote-Access VPN tarpeesta voisi olla yritys, jonka käytössä olevat materiaalit sijaitsevat palvelimella, jonne ei

ole pääsyä ulkoverkosta mutta työntekijä haluaa työskennellä etänä. (Cisco 2008b.)



KUVIO 5. Remote-Access VPN (Microsoft 2001c)

Toinen tekniikka on Site-to-Site VPN eli VPN yhteys kahden toimipisteen välille. Site-to-Site VPN mahdollistaa yrityksen sisäverkon laajentamisen kaikkien toimipisteiden välille julkista internetiä hyödyntäen. Site-to-Site VPN:llä on kaksi eri variaatiota. Ensimmäinen variaatio on intranet VPN, joka on yrityksen sisäinen VPN-yhteys. Toinen variaatio on ekstranet VPN, joka on kahden yrityksen sisäverkon yhdistämiseen tarkoitettu VPN-yhteys, extranet VPN auttaa kahta tai useampaa yritystä työskentelemään helpommin yhteistyössä, kun käytössä on turvallinen jaettu sisäverkko. (Cisco 2008b.)

3.2 VPN protokollat

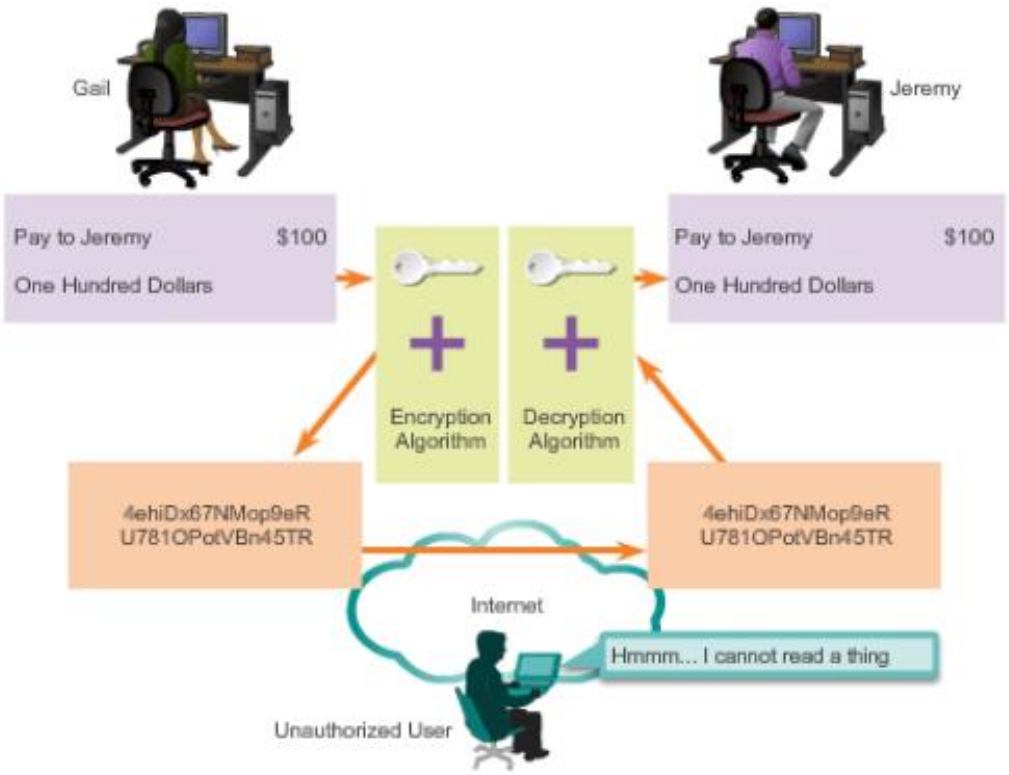
VPN yhteyksiä on mahdollista toteuttaa monella eri protokollalla. Hyvä VPN yhteys käyttää useampia protokollia samaan aikaan. VPN:n yksi tärkeimmistä tehtävistä on salata dataa, koska välttämättä ei haluta, että ulkopuoliset pääsevät dataan käsiksi esimerkiksi yrityksen toimipisteiden välillä. Yleisimpiä VPN protokollia ovat PPTP, L2TP, IPSec sekä GRE. (Cisco 2008b.)

PPTP (Point-to-Point Tunneling Protocol) on Microsoftin kehittämä tunnelointi protokolla. PPTP kehitettiin PPP (Point-to-Point Protocol) protokollaan lisukkeeksi tuomaan tietoturvallisempaa ratkaisua. Protokollaa käytetään Remote-Access VPN yhteyksissä eli etäkäyttäjä on yhteydessä yrityksen sisäverkkoon VPN tunnelin avulla. PPTP enkapsuloi PPP paketit ja siirtää siirtää ne TCP/IP:n yli. (Transmission Control Protocol) Datan salaukseen PPTP käyttää RAS (Remote Access Service) kryptausta jossa molemmat päät saavat salausavaimen. Lopullinen tunnistus tapahtuu CHAP:n (Challenge Handshake Authentication Protocol) tai PAP:n (Password Authentication Protocol) avulla. (Microsoft 2016b.)

L2TP (Layer 2 Tunneling Protocol) on Ciscon ja Microsoftin kehittämä tunnelointi protokolla. L2TP toimii nimensä mukaisesti OSI -mallin toisessa kerroksessa. L2TP ei itse tarjoa salausta liikenteelle, eli L2TP protokollaa käytetään usein IPSec (Internet Protocol Security) protokollan kanssa, jotta data saadaan salattua. Koska L2TP käyttää IPSec protokollaa hyödyksi, käytettävän VPN Clientin / VPN serverin on tuettava molempaa protokollaa. (Microsoft 2015b.)

GRE (Generic Routing Encapsulation) on salaamaton tunnelointi protokolla ja GRE:n tehtävä on enkapsuloida datapaketteja ja siirtää paketit laitteeseen joka dekapsuloi paketit ja lähettää paketit eteenpäin. Tämä mahdollistaa virtuaalisen point-to-point yhteyden, jonka avulla voidaan kuljettaa eri protokollia laitteiden välillä. (Juniper 2015.)

IPSec on avoimen standardin protokolla, joka ei ole sidottu mihinkään enkryptaus tai autentikointi menetelmään, eli voidaan käyttää useita eri enkryptaus tai autentikointi menetelmiä. IPSec toimii OSI -mallin kolmannessa kerroksessa. Salaus vaatii tiedon käytettävistä salaus menetelmistä, jotka se saa IKE:ltä (Internet Key Exchange) ja ESP (Encapsulating Security Payload) protokolla hoitaa datan salaamisen ennen datan lähettämistä. Jotta salaus toimii, molemmilla päillä täytyy olla oikeat salaus avaimet (kuvio 6). (Cisco 2008a.).



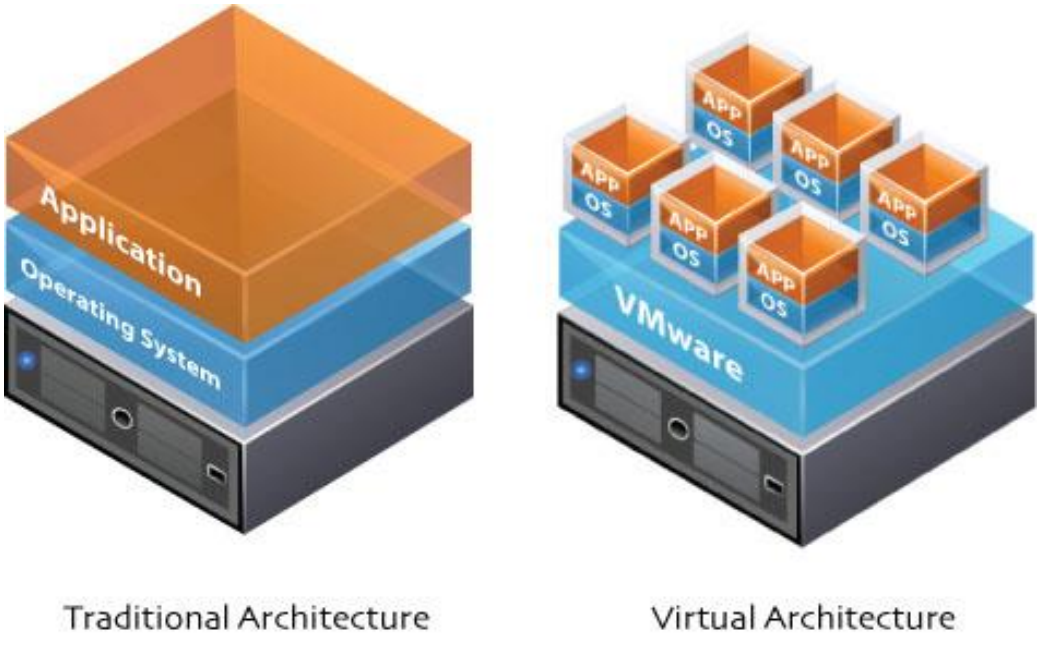
KUVIO 6. IPSec datan salaaminen (Cisco 2008a)

4 VIRTUALISOINTI

4.1 Yleistä virtualisoinnista

Virtualisointi on fyysisten prosessien sijasta virtuaalisten prosessien luontia. Virtualisointia voi liittyä lähes jokaisen tietotekniikan osa-alueeseen esimerkiksi tietokoneisiin, käyttöjärjestelmiin tai tietoverkkoihin. Pääosin virtualisointia kuitenkin käytetään palvelinten virtualisointiin. (VMware 2016b.)

Ennen tarvittiin isoja tiloja palvelinsalien pyörittämiseen, koska jokainen käyttöjärjestelmä tarvitsi oman palvelimen. Nykyään palvelinsalit voivat olla jopa 85 - 95% pienempiä, koska on siirrytty pääosin kokonaan palvelinten virtualisointiin. Yhdellä palvelimella voi olla jokin virtualisointi alusta ja virtualisointi alustan päällä useita virtuaalikoneita ja käyttöjärjestelmiä palvelimen raudasta riippuen (KUVIO 7). (VMware 2016b.)



KUVIO 7. Virtualisoidun ympäristön ero ei virtualisoituun (VMware 2016b)

4.2 Virtualisoinnin hyödyt ja haitat

Virtualisoinnilla on lukuisia hyötyä, mutta myös muutamia haittoja. Virtualisoinnin yksiä merkittävimpiä etuja on laitteiston väheneminen ja tätä kautta parempi hyödyntäminen. Laitteiston väheneminen tarkoittaa kustannusten pienenemistä yrityksillä sekä laitteiston kustannusten pienenemistä. Lisäksi laitteistolle tarvitaan vähemmän tilaa kuin aikaisemmin. Kustannusten pienenemisen lisäksi virtualisointi on paljon ekologisempi ratkaisu sähkön kulutuksen sekä laitekannan uusimisesta syntyvän elektroniikkaromun kannalta. (Angeles 2014.)

VMwaren vanhempi tuotemarkkinoinnin johtaja Julia Lee on jakanut virtualisoinnin kustannussäästöt kolmeen kategoriaan: investoinninsäästöt, käyttökustannussäästöt ja energiansäästöt. Investointien kohdalla yritykset voivat säästää, kun voidaan ajaa montaa palvelinta yhdeltä virtualisointi alustalta. Käyttökustannussäästöjen kohdalla valmiit virtualisoidut palvelimet voidaan käytännössä automatisoida, joka vähentää IT henkilöstön työtä palvelinten hallintaan. Energiansäästöjen kohdalla virtualisointi voi tarkoittaa huomattavia säästöjä yrityksen koosta riippuen. (Angeles 2014.)

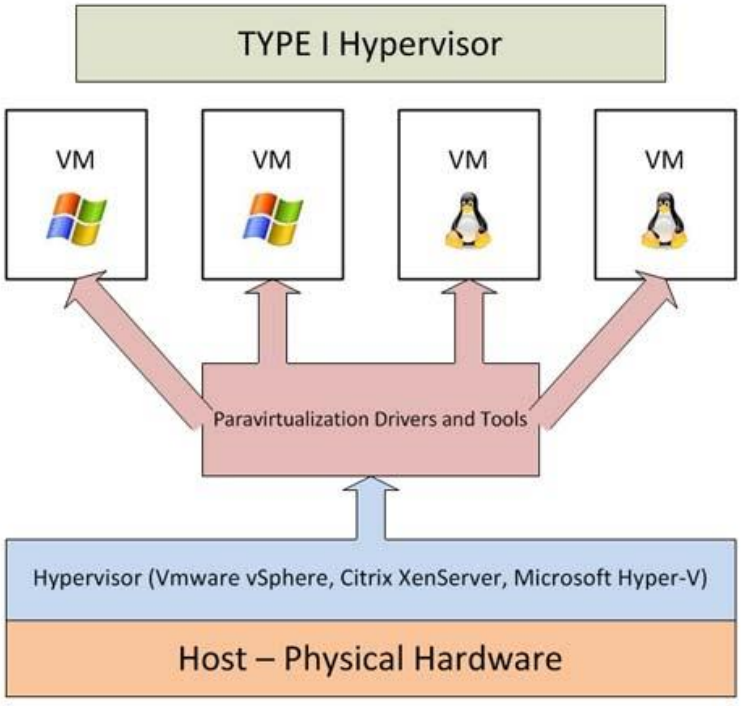
Virtualisointi myös helpottaa IT-infran hallinnoimista ja tekee hallinnoimisesta nopeampaa. Virtuaalipalvelimia yleensä hallitaan yhden hallintaohjelman tai etäyhteyden avulla. Tarvittaessa voidaan myös nopeasti luoda uusia virtuaalikoneita, koska ei tarvita uutta laitteistoa. Lisäksi kaikista virtuaalikoneista voidaan tarvittaessa ottaa varmuuskopioita tai hallintaohjelma voidaan määritellä ottamaan varmuuskopiot automaattisesti tietyin väliajoin esimerkiksi verkkolevylle. Näin voidaan taata tietojen säilyminen, jos esimerkiksi fyysinen rauta hajoaa. (Angeles 2014.)

Vaikka virtualisointi pienentää kustannuksia, virtualisointi voi myös vaatia aluksi isompaa investointia kuin ei virtualisoitu palvelin. Lisäksi kaikki yritykset eivät välttämättä tarvitse kuin yhden palvelimen. Nykyään kuitenkin on paljon palveluntarjoajia joilta voi halutessaan hankkia

yksittäisiä virtuaalipalvelimia. Yleisesti virtualisointia kannattaa miettiä pitkän tähtäimen hankintana, jota voi hyödyntää myöhemmin. (Angeles 2014.)

4.3 Virtualisointialustat

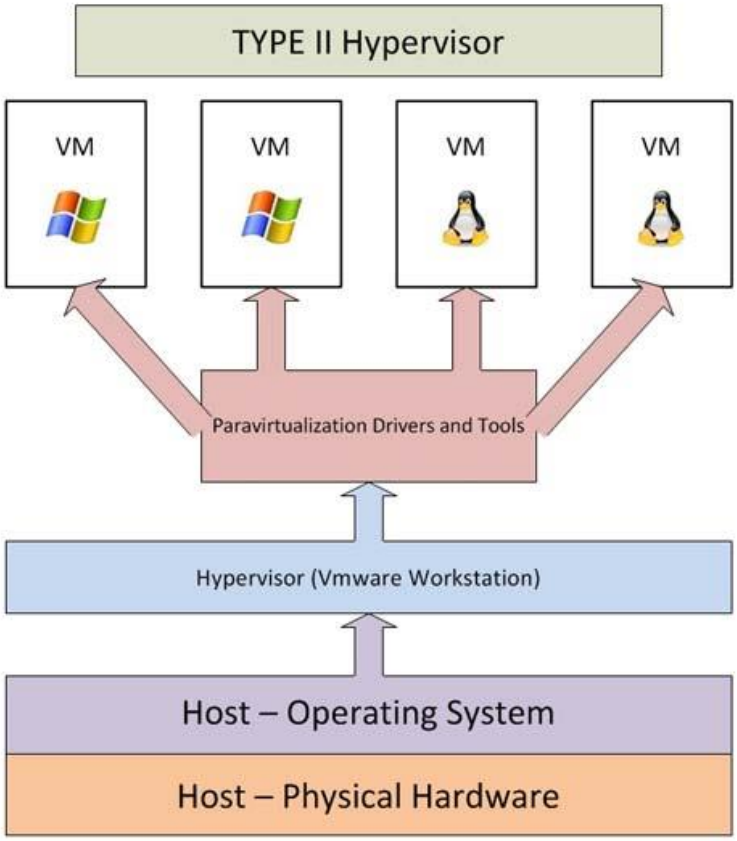
Virtualisointialustoja on kahta eri päätyyppiä. Ensimmäinen tyyppi on TYPE 1 Hypervisor eli ensimmäisen tyypin virtualisointialusta ja toinen tyyppi, on TYPE 2 Hypervisor eli toisen tyypin virtualisointialusta. Tyypin 1 virtualisointialustat asennetaan ”Bare-metal” tyylisesti, eli suoraan fyysisen laitteiston päälle (kuvio 8). Tämän ansiosta tyypin 1 virtualisointialustat voivat jakaa kaikkia fyysisiä resursseja tuleville virtuaalikoneille. Tällä tyypillä on myös huomattavasti parempi suorituskyky, koska käyttöjärjestelmä ei syö yhtään tehoa virtualisointialustalta. (Kleyman 2012.)



KUVIO 8. Tyypin 1 virtualisointialusta (Kleyman 2012.)

Tyypin 2 virtualisointualustat ovat hostattuja virtualisointialustoja, eli alustoja ei asenneta tyypin 1 tapaisesti ”Bare-metal” asennuksena vaan virtualisointialustat asennetaan käyttöjärjestelmän päälle.

Käyttöjärjestelmänä voi toimia esimerkiksi Windows Server 2012 R2, jonka päälle asennetaan jokin 2 tyypin virtualisointialusta (kuvio 9). Lähtökotaisesti tyypin 2 virtualisointialustoja on kaikille yleisimmille käyttöjärjestelmille. Tyypin 2 virtualisointialustoissa isäntäkone huolehtii laitteiston hallinnasta ja tästä syystä tyypin 2 virtualisointialustoille ei voida määritellä ulkoisia verkkokortteja vaan ne käyttävät virtualisoidun verkkokortin. (Kleyman 2012.)



KUVIO 9. Tyypin 2 virtualisointialusta (Kleyman 2012)

Virtualisointimarkkinoilla on monta eri toimitsijaa. Tärkein ja tunnetuin on VMware ja vSphere tuoteperhe. VMware on tunnetuin virtualisointialusta maailmalla, kun tullaan palvelinvirtualisointiin. Yhtenä heikkoutena VMware:lla on lisenssien määrä. VMware:lla on jokaiselle eri tuotteelle monta erityyppistä lisenssiä ja asiakkaan pitäisi osata valita oikea lisenssi. Toinen tärkeä toimija on Hyper-V. Hyper-V:stä usein luullaan, että kyseessä on tyypin 2 virtualisointialusta, koska Hyper-V tavallaan pyörii käyttöjärjestelmän päällä (kuvio 9). Hyper-V on kuitenkin rakennettu

käyttöjärjestelmän sisään, joten Hyper-V voi hyödyntää kaikkea fyysistä laitteistoa, eli tästä syystä Hyper-V on tyypin 1 virtualisointialusta (kuvio 8). Kolmantena tulee Citrix XenServer. (Kleyman 2012.)

VMware on vuonna 1998 perustettu pilvipalveluihin sekä virtualisointiin perustuva yritys. VMware on ensimmäinen yhtiö, joka on virtualisoinut x86 arkkitehtuuria kaupalliseen käyttöön. Yhtiön pääkonttori sijaitsee Palo Altossa Piilaaksossa. VMwarella on useita tuotteita virtualisointiin liittyen. (VMware 2016a.)

Palvelinpuolen ohjelmistoista löytyy kaksi 1 tyypin virtualisointipalvelinta: VMware ESXi ja VMware Server, joista ESXi versio on uudempi ja käytetympi. Työpöytä ohjelmistoista löytyy kolme tyypin 2 virtualisointipalvelinta: VMware Workstation, joka on VMwaren vanhin virtualisointiohjelma, VMware Player, joka on karsittu ilmainen henkilökohtaiseen käyttöön tarkoitettu versio VMware Workstationista. Viimeisenä on VMware Fusion, joka on Mac käyttöjärjestelmälle tarkoitettu versio VMware Workstationista. VMware Fusionia voidaan käyttää, jos työntekijä haluaa käyttää esimerkiksi Apple MacBookia, mutta osa yrityksen ohjelmistoista on vain Windows käyttöön tarkoitettuja. 2016 vuoden tammikuussa VMware ilmoitti, että he eivät enään jatka VMware työpöytä versioiden kehittämistä ja irtisanoi kaikki osaston työntekijät. Tästä voidaan tehdä johtopäätös, että VMware aikoo keskittyä entistä enemmän palvelinpuolen virtualisointiin. (Wikipedia 2016d.)

Hyper-V on Microsoftin kehittämä virtualisointialusta. Ennen Hyper-V:tä Microsoftilla oli Windows Server Virtualization, johon Hyper-V perustuu. Ensimmäisen kerran Hyper-V tuli Windows Server 2008 käyttöjärjestelmään päivityksen muodossa. Nykyisin Hyper-V:llä on kaksi eri versiota: Windows Server käyttöjärjestelmään liitetty versio sekä toinen erillinen ohjelmisto Microsoft Hyper-V Server. (Wikipedia 2016b.)

Hyper-V:n käyttöönotossa tulee ottaa huomioon käyttötarpeet, koska Microsoftilla on useita eri versioita Windows käyttöjärjestelmistä (taulukko 6). Jos halutaan käyttää käyttää useampaa kuin kahta virtuaalikonetta

vaihtoehtona on ainoastaan Windows Server 2012 R2 Datacenter, joka tukee rajoittamattomasti virtuaalikoneita. Windows Server 2012 Essentials versiota ei suositella virtualisointiin, koska käytössä on maksimissaan 2 ydintä. (Wikipedia 2016b)

TAULUKKO 6. Windows Server 2012 R2 erot (Microsoft 2016.)

Ominaisuudet	**Essentials**	**Standard**	**Datacenter**
Maksimi ytimet	2	64	64
Maksimi muisti	64 GB	4 TB	4 TB
Lisenssit	1 / palvelin	1 / CPU + CAL	1 / CPU + CAL
Virtualisointi	1 VM / fyysinen	2 VM	Rajoittamaton

Citrix on 1989 perustettu virtualisointia ja pilvipalveluita toteuttava yritys. Citrixin pääkonttori sijaitsee Floridan Fort Lauderdalessa. Citrix tekee laajaa yhteistyötä Microsoftin kanssa joka alkoi samana vuonna 1989, kun Citrix perustettiin ja Citrix lisensoi OS/2:n lähdekoodin. Yhtön perusti vanha IBM:n työntekijä Ed Lacobucci. Suurin osa Citrixin alkuperäisistä työntekijöistä on tullut Citrixille IBM:n OS/2 –projektin kautta.2000 –luvun puolivälissä Citrix alkoi siirtymään palvelin ja työpöytä virtualisointiin, josta syntyi tunnettu 1 tason virtualisointialusta XenServer sekä 2 tason virtualisointialusta XenDesktop. (Wikipedia 2016a.)

XenServerin käyttö ja ominaisuudet vastaavat käytännössä enemmän VMware ESXi:tä kuin Microsoft Hyper-V:tä. XenServer tosin soveltuu yhdelle käyttäjälle paremmin kuin VMware sekä on näistä edullisempi vaihtoehto. (Wikipedia 2016a.)

5 TIETOVERKON PARANTAMINEN

5.1 Tietoverkon lähtötilanne

Ictum Oy tarvitsee tulevaa demonstraatiotilaa varten palvelimen, johon asennetaan kaksi virtuaalipalvelinta. Vaatimuksena verkolle oli, että he eivät halua palvelimille pääsyä ulkoverkosta käsin, mutta verkkoon pitäisi päästä myös Lahden toimistolta käsiksi. Lisätarpeena oli AC-standardin tukiasema langattomien audiovisuaalisten demonstraatiolaitteiden toimintaa varten.

Opinnäytetyön tarkoituksena on kartoittaa tämänhetkisen tietoverkon lähtötilanne ja miettiä tarvittavat muutokset, jotta haluttu tulos saavutettaisiin. On myös otettava huomioon tulevat tarpeet päätavoitteen ohella. Lisäksi toteutettiin VPN Client-yhteys, etätöiden mahdollistamiseksi.

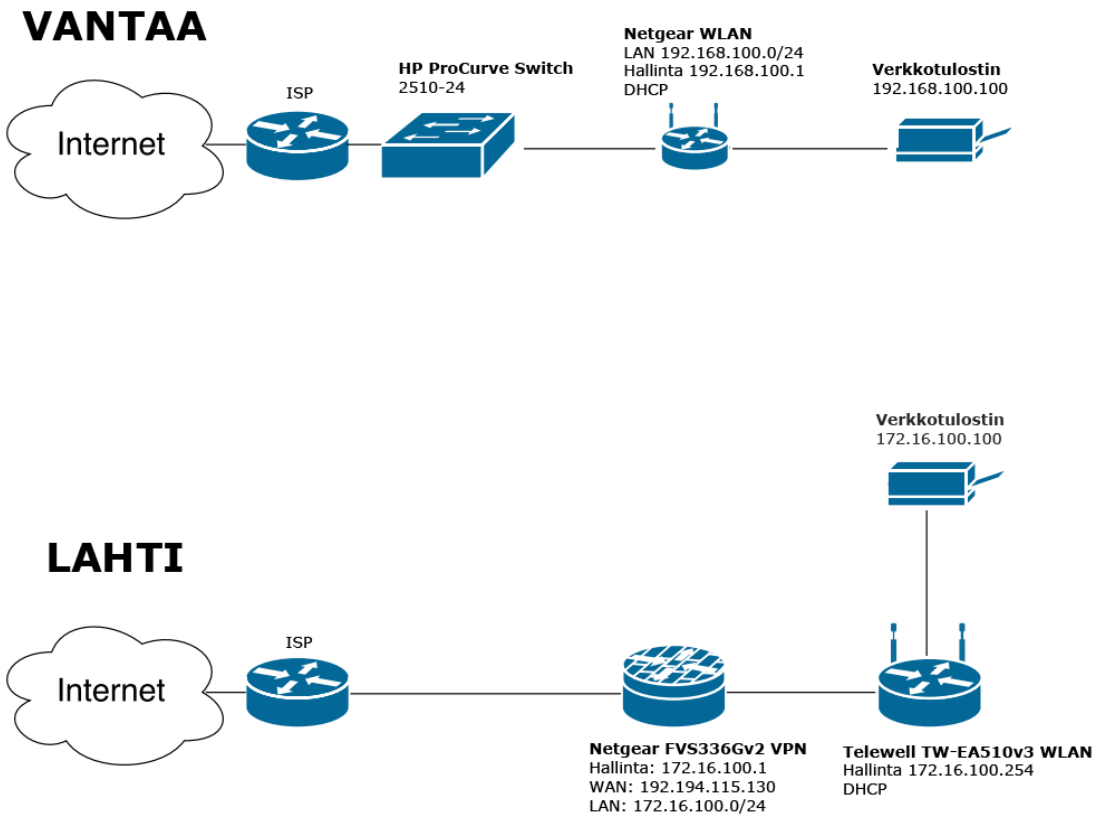
5.2 Tietoverkon kartoitus

Kartoitus aloitettiin käymällä läpi kummankin toimipisteen laitteet sekä tarvittavat IP-osoitteet. Laitteiden ja IP-osoitteiden perusteella tehtiin niistä verkkokuva (kuvio 10).

Lahden toimiston verkossa oli kytkettynä Netgear FVS336Gv2 VPN-palomuuri jossa oli kiinni Telewell TW-EA510v3 ADSL / WLAN-reititin, jota käytetään toimiston langattomaan yhteyteen. Lisäksi toimistolla oli verkkotulostin, sekä hyllyssä ylimääräinen Netgear FVS336Gv2 VPN-palomuuri joka on ollut käytössä vanhassa toimipisteessä Imatralla (kuvio 10).

Vantaan toimistolla oli HP ProCurve Switch 2510-24, joka on palveluntarjoajan omaisuutta ja yrityksen oma HP ProCurve Switch 1700-24, joka ei ollut käytössä. Kytkimestä lähti ristikytkennän kautta työasemapisteisiin verkkoyhteys, sekä yhteen työasemapisteeseen oli laitettu kiinni Netgear WLAN-reititin, josta saatiin langaton yhteys

toimistolle (kuvio 10). Samassa Netgear WLAN-reitittimessä oli kiinni verkkotulostin. Vantaalla on myös ylimääräinen pöytäkone, jossa on Windows Server 2012 R2.



KUVIO 10. Tietoverkon lähtötilanne

5.3 Netgear FVS336Gv2 SSL:n ja IPSec VPN:n vertailu

IPSec VPN toimii OSI – mallin kolmannessa kerroksessa, eli verkkokerroksessa. IPSec salaa kaiken datan joka liikkuu kahden pisteen välillä ilman ylimääräisiä ohjelmia. SSL VPN (Secure Sockets Layer) toimii OSI – mallin seitsemännessä kerroksessa, eli sovelluskerroksessa. SSL käyttää internet-pohjaista yhteyttä ja salaus kulkee selaimen kautta. SSL salaa jokaisen ohjelman erikseen. (Saxena 2013.)

IPSec VPN-yhteyden vahvuus SSL VPN-yhteyteen nähden on jatkuva yhteys kahden pisteen välillä. Toimiminen OSI – mallin kolmannessa kerroksessa myös mahdollistaa, että IPSec VPN:n läpi voidaan tunneloida kaikkia IP protokollia. IPSec VPN:n heikkous on sen sisäinen tietoturva. Kun IPSec VPN-tunneli on luotu, kaikki tunnelin käyttäjät ovat tavallaan yhteydessä koko tunneloituun lähiverkkoon. SSL VPN:ää käytetään lähinnä silloin, kun halutaan luoda etäyhteys päätepisteeseen mistä tahansa. SSL VPN ei tarvitse mitään ohjelmistoa, kun sitä halutaan käyttää. SSL VPN voidaan konfiguroida siten, että selaimen kautta voidaan ottaa VPN yhteys päätepisteeseen. (Saxena 2013.)

Kummallekin VPN protokollalle löytyy omat käyttötarpeet ja ideaalissa tilanteessa molempia protokollia käytetään täydentämään toisiaan. Pääsääntöisesti kuitenkin IPSec VPN:ää käytetään, kun halutaan jatkuvasti päällä oleva VPN yhteys ja SSL VPN:ää käytetään, kun halutaan ottaa etäyhteys päätepisteeseen. (Saxena 2013.)

5.4 VPN Client ohjelmistojen vertailu

VPN Clientin valintaan otettiin muutama esimerkki ohjelmisto. Netgear ProSafe on Netgearin oma VPN Client -ohjelma joka ei ole universaali. Netgear ProSafesta löytyy myös IPv6 sekä SSL tuki. Sen avulla voidaan myös hyödyntää USB Tokenia tai SmartCardia tunnistautumiseen. Haittapuolena on ohjelman maksullisuus, koska jokainen erillinen lisenssi maksaa (taulukko 7). (Netgear 2016.)

Toisena ohjelmana oli GreenBow. Ohjelmana GreenBow on Netgearin ProSafen kanssa ominaisuuksiltaan samanlainen, mutta kalliimpi. GreenBowista löytyy myös IPv6 sekä SSL tuki. Lisäksi siitä löytyy myös USB Token sekä SmartCard tuki tunnistautumiselle. GreenBowin hyvä puoli on, että se on universaali eli sitä voidaan käyttää myös muiden valmistajien VPN pääpisteiden kanssa. Lisäksi ohjelman saa suomenkielisenä (taulukko 7). (The Green Bow 2016.)

Shrew Soft on VPN Client -ohjelmista karsituin. Siinä ei ole IPv6 eikä SSL tukea. Käyttökielenä on englanti. Tunnistautuminen onnistuu vain salasanalla. Hyvänä puolena ohjelma on universaali sekä ilmainen (taulukko 7). (Shrew Soft 2010.)

TAULUKKO 7. VPN Client -ohjelmien vertailu

Ohjelma	**Netgear ProSafe**	**GreenBow**	**Shrew Soft**
IPv4 / IPv6	IPv4 / IPv6	IPv4 / IPv6	IPv4
SSL	X	X	
IPSec	X	X	X
Käyttökieli	Englanti	Suomi	Englanti
USB Token / SmartCard	X	X	
Maksullinen	X	X	
Universaali		X	X

Yritykselle valittiin käyttöön Shrew Soft. Perusteluina oli ohjelmiston kustannukset, ja Shrew Soft oli ohjelmistoista ainoa ilmainen. Myös käyttötarpeet otettiin huomioon, eli ei tarvittu IPv6 tai SSL tukea. Lisäksi käyttökieli oli englanti, joka vaikutti myös päätökseen.

5.5 VMware tyypin 2 virtualisointialustojen vertailu

Tyypin 2 virtualisointialustat ovat käyttöjärjestelmän päälle asennettavia virtualisointialustoja. VMware:lla on neljä tyypin 2 virtualisointialustaa: VMware Workstation Player, VMware Workstation Pro, VMware Fusion ja VMware Fusion Pro. Workstation Player sekä Workstation Pro on Windows käyttöjärjestelmälle asennettavia virtualisointialustoja. Fusion sekä Fusion Pro ovat Mac käyttöjärjestelmälle asennettavia virtualisointialustoja.

Workstation Player on karsittu versio Workstation Pro:sta. Workstation Playerin ominaisuuksiin virtuaalikoneen suorittamisen lisäksi kuuluu virtuaalikoneiden luonti. Workstation Playerillä ei esimerkiksi onnistu varmuuskopiot, eikä sitä voida yhdistää VMware vSphereen. Workstation Playerin hyviä puolia on, että se on ilmainen henkilökohtaiseen käyttöön, eli se kilpailee lähinnä muiden ilmaisten virtualisointialustojen kanssa. Workstation Pro:lla pystytään Workstation Playerin tavoin luomaan ja käyttämään virtuaalikoneita. Lisäksi Workstation Pro:lla pystytään kloonaamaan virtuaalikoneita, ottamaan varmuuskopioita tai automatisoimaan varmuuskopiot otettavaksi tietyin väliajoin. Workstation Pro:lla pystytään käyttämään virtuaali levyjä sekä liittämään virtuaalikoneita vSphereen (taulukko 8). (VMware 2016d.)

Fusion ja Fusion Pro on Mac käyttöjärjestelmälle tarkoitettu virtualisointialusta. Yleisin käyttötarkoitus Fusionilla on Windows käyttöjärjestelmän käyttö Mac käyttöjärjestelmän päällä. Fusion on rajallinen versio Fusion Prosta, eli Fusionilla voidaan pelkästään luoda ja ajaa virtuaalikoneita, mutta Fusionilla voidaan lisäksi ottaa varmuuskopioita. Fusion Pro tuo lisänä varmuuskopioiden automatisoinnin, virtuaalikoneiden kloonausta sekä virtuaalikoneiden yhdistämisen vSphereen (taulukko 8). (VMware 2016c.)

TAULUKKO 8. VMware tyypin 2 virtualisointialustojen vertailu

VMware	**Workstation Player**	**Workstation Pro**	**Fusion**	**Fusion Pro**
Virtuaalikoneiden luonti	X	X	X	X
Virtuaalikoneiden kloonaus		X		X
Varmuuskopiot		X	X	X
Automatisoidut varmuuskopiot		X		X
Virtuaalilevyt		X		X
vSphere yhteys		X		X

Virtualisointialustoista käyttöön valittiin Workstation Pro. Tärkeimpiä ominaisuuksia valinnoille olivat automatisoidut varmuuskopiot ja alustan saatavuus Windows työasemakoneelle. Workstation Pro osoittautui ainoaksi vaihtoehdoksi, joka täytti kyseiset kriteerit.

5.6 AC-standardin WLAN-tukiasemien vertailu

Vaatimuksina AC-standardin WLAN-tukiasemalle oli, että WLAN-tukiaseman hintataso pysyy maltillisena, mutta on myös tarpeeksi tehokas. Yhtenä valinnaisena kriteerinä oli USB (Universal Serial Bus) portti, jota voitaisiin hyödyntää kevyessä tiedoston jakamisessa vieraille kytkemällä siihen esimerkiksi USB kovalevyn tai muistitikun. Edellä mainitusta tilanteesta ja käyttäjien vähyydestä johtuen otin vertailuun kuluttajapuolen AC-standardin WLAN-tukiasemia ja jätin yrityskäyttöön tarkoitetut AC-standardin WLAN-tukiasemat pois vertailusta.

Vertailuun otettiin kolme eri hintaluokan AC-standardin WLAN-tukiasemaa. Ensimmäinen vertailun tukiasema oli Asus RV-AC87U AC2400 Dual-Band WLAN-tukiasema, joka oli vertailun kallein. Toisena tukiasemana oli TP-Link Archer C9 Dual-Band WLAN-tukiasema, joka sijoittui hinnoittelussa vertailun keskiluokkaan. Viimeisenä tukiasemana vertailussa oli TP-Link Archer C50 Dual-Band WLAN-tukiasema, joka oli vertailun halvin. (Jimm’s 2015.)

TAULUKKO 9. Tukiasemien vertailu

Laite	Asus TV-AC87U	TP-Link Archer C9	TP-Link Archer C50
WAN nopeus	1000 Mbps	1000 Mbps	100 Mbps
LAN nopeus	1000 Mbps	1000 Mbps	100 Mbps
2,4GHz nopeus	600 Mbps	600Mbps	300 Mbps
5,GHz nopeus	1734 Mbps	1300Mbps	867 Mbps

USB	1x USB 2.0 1x USB 3.0	1x USB 2.0 1x USB 3.0	1x USB 2.0
Hinta	189,92 €	113,92 €	37,92 €

TP-Link Archer C50:n, rajoitteena on WAN/LAN nopeus joka jäi maksimissaan 100 Mbps. 2,4GHz taajuuden ja 5GHz taajuuden nopeudet ovat reilusti pienempiä, kuin esimerkiksi Asus TV-AC87U:ssa (taulukko 9).

Asus TV-AC87U:n ja TP-Link Archer C9:n 1000 Mbps WAN/LAN nopeus on riittävä ja molemmista tukiasemista löytyy USB 3.0 portti. Asus TV-AC87U:n 5GHz taajuuden nopeus on 1734 Mbps ja TP-Link Archer C9:n 5GHz taajuuden nopeus on 1300 Mbps (taulukko 9). Lopulta päädyttiin TP-Link Archer C9:ään, koska kyseinen laite oli kustannustehokkaampi yrityksen käyttötarkoitukseen nähden.

5.7 Tietoverkon ratkaisu

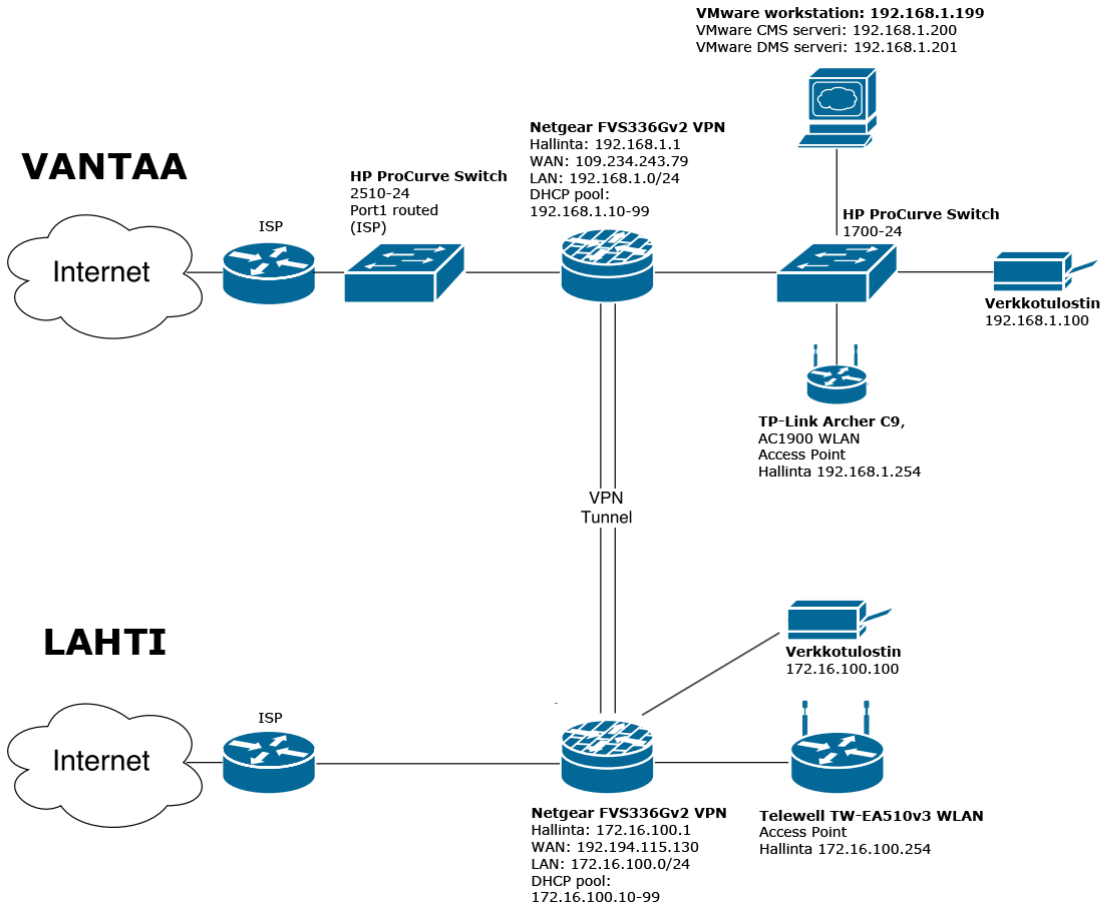
Lähtökohtana käytetään olemassa olevia laitteita niiltä osin, kun pystytään. Vantaalle hankitaan AC-standardin WLAN-tukiasema. Palvelimena hyödynnetään Vantaalla olevaa pöytäkonetta, johon hankitaan VMware Workstation lisenssi virtuaalipalvelimia varten. Lisänä ratkaisuun tulee IPSec VPN Client valmius, jotta voidaan tarvittaessa päästä yrityksen sisäverkkoon käsiksi VPN Clientin avulla.

Lahden toimistolla työskentelee kolme ihmistä ja käyttö rajoittuu suurimmaksi osaksi internetin käyttöön, sekä tulevaisuudessa demonstraatio virtuaalipalvelimen käyttöön. Lisäksi toimitilan koko on vain noin 20 neliömetriä. Tällä hetkellä ratkaisu on pysyä samassa laitteistossa, mutta pienin muutoksin laitteiston konfiguraatioon liittyen.

Vantaan toimistolla työskentelee kuusi ihmistä ja rekrytointi on käynnissä, sekä tilat ovat isommat kuin Lahden toimistolla. Vantaalla on tarve siirtää isompia tiedostoja virtuaalipalvelimelle, sekä demonstroida langattomia

audiovisuaalisia ratkaisuja asiakkaille, sisältyy isojen videotiedostojen siirtelyä virtuaalipalvelimelle. Vantaalle ratkaisu on tuoda Lahdesta hyllyssä oleva Netgear FVS336Gv2 VPN palomuuri IPSec VPN-yhteyttä varten. Vantaalle hankitaan uusi langaton AC-standardin tukiasema TP-Link Archer C9 AC1900 parempia sisäverkon nopeuksia varten. Vantaalla otetaan myös käyttöön käytöstä poissaoleva HP ProCurve 1700-24 kytkin, koska HP ProCurve 2510-24 kytkimeen tulee valokuitu, ja Netgear FVS336Gv2 VPN-palomuurissa on vain 4 porttia ja kyseistä VPN-palomuuria on tarkoitus käyttää DHCP-palvelimena.

Valmiista ratkaisusta tehtiin uusi verkkokuva (kuvio 11), johon on mietitty IP-osoitteistus valmiiksi esimerkiksi DHCP-poolien sekä kiinteiden laitteiden osalta.



KUVIO 11. Verkkokuva valmiista ratkaisusta

5.7.1 Lahden konfiguraatio

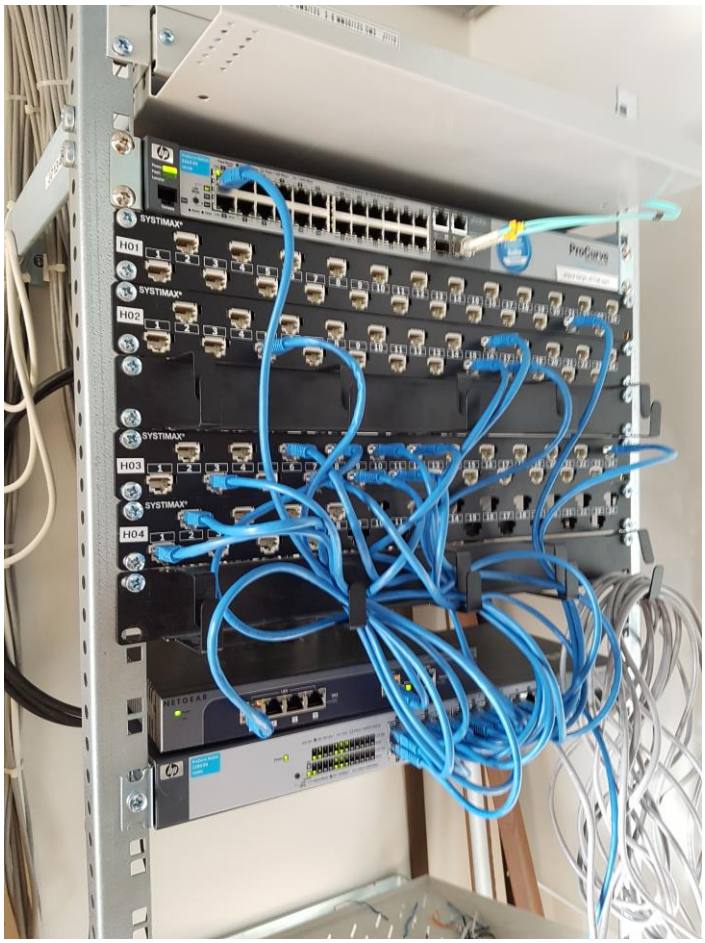
Sekä Lahden Netgear FVS336Gv2 VPN-palomuuriin, että Telewell-EA510v3 WLAN-reitittimen oli konfiguroitu DHCP-palvelu päälle. Verkkotulostin oli liitetty Telewell reitittimeen. Telewell reititin vaihdettiin Access Point tilaan, ja Netgear VPN-palomuurin DHCP-palvelin jätettiin päälle, sekä tulostin kytkettiin suoraan Netgear VPN-palomuuriin.

Lahden Netgear VPN-palomuuriin konfiguroitiin uusi IPSec VPN-yhteys Vantaan Netgear VPN-palomuuriin, että saadaan toteutettua kahden toimipaikan välinen sisäverkkoyhteys. Lisäksi konfiguroitiin IPSec VPN Client valmius ja luotiin jokaiselle käyttäjälle omat tunnukset, jotta voidaan tarvittaessa käyttää yrityksen sisäverkkoa muualta, kuin yritykseltä käsin.

5.7.2 Vantaan konfiguraatio

HP ProCurve 2510-24 oli palveluntarjoajan toimesta NAT:n (Network Address Translate) takana ja tästä syystä VPN-yhteys ei todennäköisesti tulisi toimimaan, ellei hankittaisi dynaamista DNS (Domain Name System) palvelua yritykselle, joka taas on kuukausimaksullinen palvelu. Palveluntarjoaja muutti portin 1 reitittävään tilaan, jotta yritys saisi julkisen IP-osoitteen suoraan Netgear FVS336Gv2 VPN-palomuurin, joka on kytkettynä HP ProCurve 2510-24 porttiin 1. Tämä mahdollistaa VPN-yhteyden toimimsen ilman dynaamista DNS-palvelua, koska FVS336Gv2 VPN-palomuurille tulee julkinen eikä yksityinen IP-osoite.

HP ProCurve 2510-24 kytkimen ja ristikytkentäpaneelin väliset kytkennät irroitettiin. Netgear FVS336Gv2 VPN-palomuurin WAN1 portti kytkettiin palveluntarjoajan HP ProCurve 2510-24 kytkimen porttiin 1. Tämän jälkeen otettiin käyttöön yrityksen HP ProCurve 1700-24 kytkin. Netgear FVS336Gv2 VPN-palomuuri kytkettiin LAN1 portista HP ProCurve 1700-24 kytkimen porttiin 1. Lopuksi kytkettiin ristikytkennät HP ProCurve 1700-24 kytkimestä työasemapisteille (kuvio 12).



KUVIO 12. Ristikytkennät

Seuraavaksi konfiguroitiin Netgear FVS336Gv2 VPN-palomuurille tarvittavat asetukset. WAN asetuksiin määriteltiin ISP:n antamat julkiset IP-osoitteet sekä valittiin reititystavaksi NAT. LAN asetuksista määriteltiin IP-osoitteeksi 192.168.1.1/24 ja laitettiin DHCP-palvelin päälle ja annettiin Netgear FVS336Gv2 VPN-palomuurille DHCP-pooliksi 192.168.1.10-99, sekä ISP:n DNS-palvelimen IP-osoitteet. VPN asetuksista konfiguroitiin IPSec VPN-yhteyden asetukset Vantaan toimiston ja Lahden toimiston välille. Lisäksi konfiguroitiin IPSec VPN Client valmius ja luotiin jokaiselle käyttäjälle omat tunnukset, kuten Lahden Netgear VPN-palomuurissa, jotta voidaan tarvittaessa käyttää yrityksen sisäverkkoa muualta, kuin yritykseltä käsin.

TP-Link Archer C9 WLAN-tukiasema konfiguroitiin Access Point tilaan ja sille konfiguroitiin 2,4GHz ja 5,0GHz yhteydet sisäiseen käyttöön, sekä 2,4GHz WLAN vierasverkko vieraita varten. WiFi Analyzerillä tutkittiin

vapaat kanavat ja 2,4GHz taajuus asetettiin kanavalle 8, sekä 5GHz taajuus asetettiin kanavalle 40 kanavan vähäisen käytön vuoksi. WLAN-tukiasema sijoitettiin välikattoon keskeiselle paikalle ja tarkastettiin WiFi Analyzerillä, että yhteys on vakaa ja toimiva yrityksen jokaisessa paikassa (kuvio 13).

KUVIO 13. WLAN 2,4GHz ja 5,0GHz kanavat

Tulostin kytkettiin myös ristikytkennän kautta suoraan HP ProCurve 1700-24 kytkimeen. Aikaisemmin tulostin oli kytketty WLAN-tukiaseman kautta ja tulostinta ei voitu käyttää langallisesta verkosta.

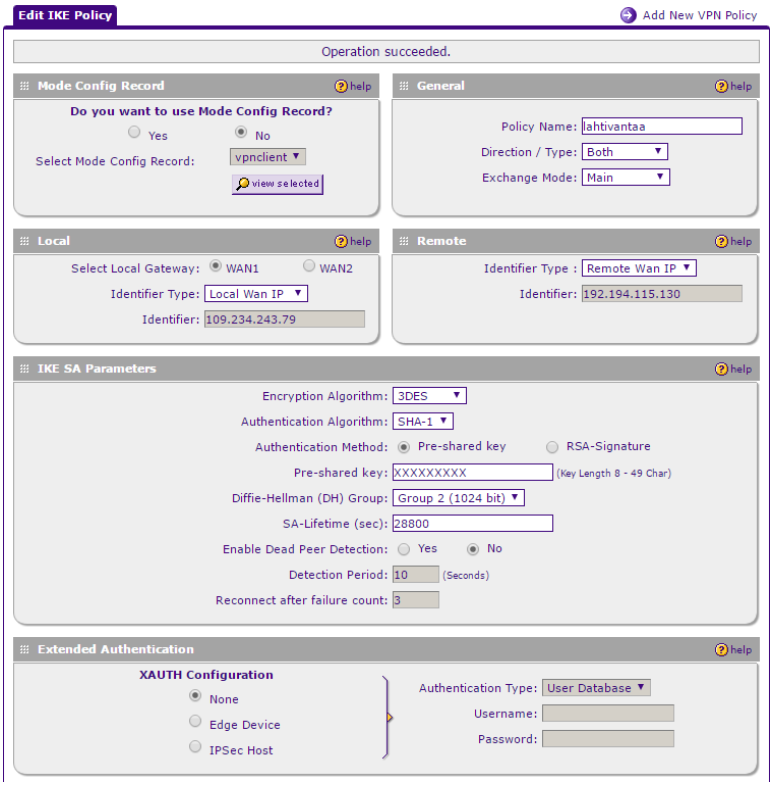
Palvelimeksi otettiin käyttöön pöytäkone, johon on asennettuna Windows Server 2012 R2. Windows Server 2012 R2:lle ostettiin VMware Workstation lisenssi, kahta virtuaalipalvelinta varten. Virtuaalipalvelimien valmistajan tuen alla oli ainoastaan VMware, ja tästä syystä päädyttiin käyttämään toimittajana VMwarea. VMware Workstationista tehtiin Windows Server 2012 R2:n päälle perusasennus. Kun VMware asennus

oli valmis, lisättiin siihen kyseiset kaksi valmista virtuaalipalvelinta, sekä ajastettiin VMware ottamaan varmuuskopioita halutun kaavan mukaan.

5.8 IPSec VPN tunnelin luominen

Netgear FVS336Gv2 VPN-palomuurin konfigurointi tapahtuu netgearin hallintapaneelista. Ensimmäisenä valitaan haluttu protokolla, joka luodaan. Aiemman vertailun perusteella käytettäväksi protokollaksi valittiin IPSec VPN.

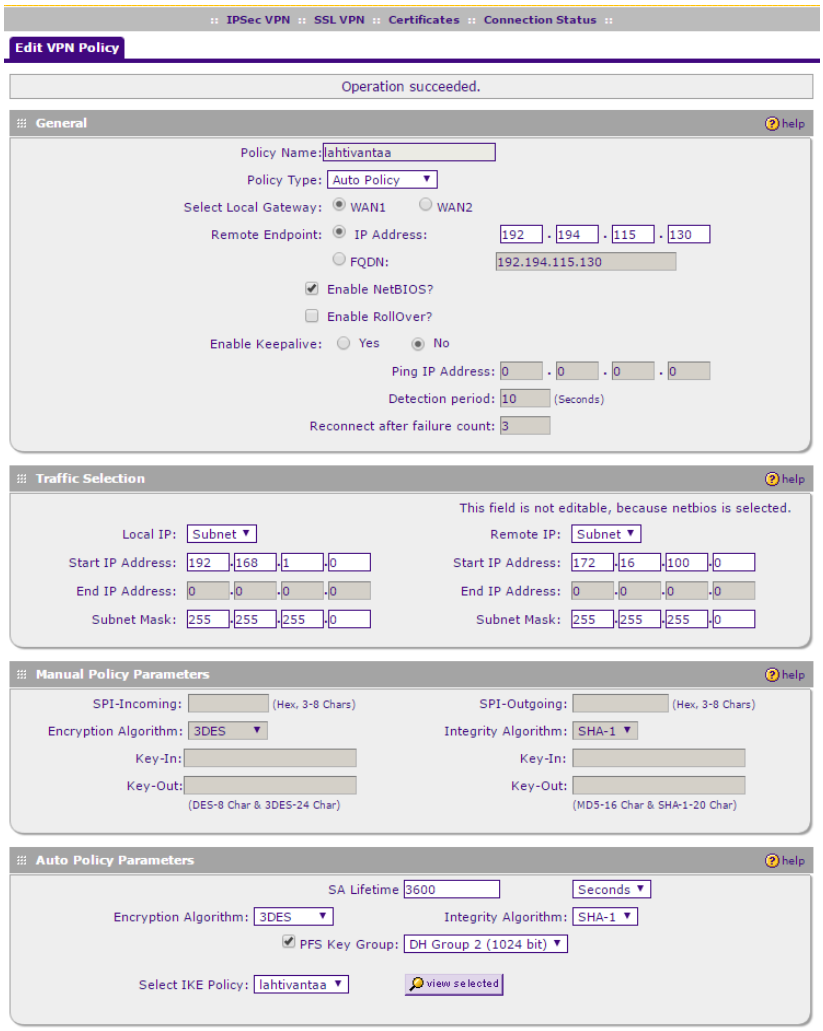
Luodaan IKE policy, joka hoitaa kahden laitteen välillä neuvottelun salausavainten jaosta. Policylle annetaan nimi, suunta/tyyppi joka määrittelee, onko sallittuna ulos- ja sisäänpäin liikenne. IKE:lle pitää myös antaa avaimen vaihtotila, jota se käyttää avainten vaihtoon. Vaihtotiloina on joko agressiivinentila tai päätila. Agressiivinentila on nopeampi, mutta ei niin tietoturvallinen, kun taas päätila päinvastoin hitaampi, mutta turvallisempi. Seuraavaksi määritellään mitä yhdyskäytävää IKE käyttää paikalliseen ja etäkäyttöön. Lopuksi IKE policylle valitaan halutut enkryptaus algoritmit, sekä autentikointi algoritmit ja asetetaan tälle haluttu PSK-avain (Pre-Shared Key). Lopuksi määritellään haluttu Diffie-Hellman ryhmä, jota IKE policy käyttää (kuvio 14).



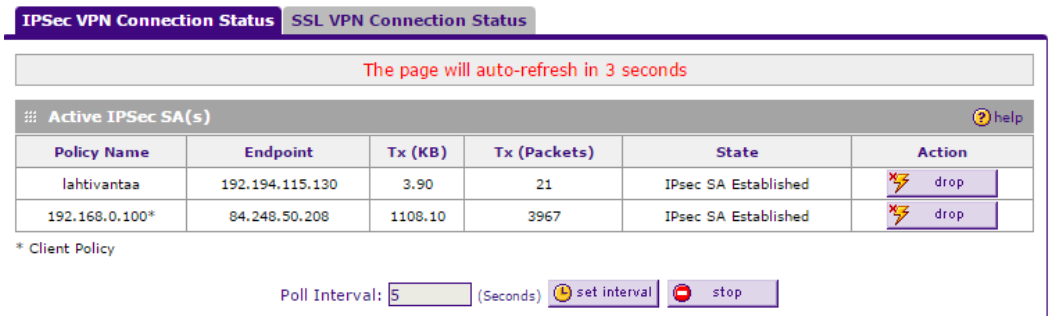
KUVIO 14. IKE Policy IPSec VPN yhteydelle

IKE policyn jälkeen luodaan VPN policy. VPN policylle annetaan nimi sekä paikallinen yhdyskäytävä ja annetaan sille IP-osoite, johon VPN-tunneli halutaan luoda. Lisäksi annetaan lokaalin sisäverkon IP-osoite avaruus, sekä kyseisen sisäverkon IP-osoite avaruus johon VPN-tunneli luodaan. Lopuksi määritellään haluttu enkryptaus- ja yhtenäisyysalgoritmi. Tämän jälkeen valitaan aiemmin luotu IKE policy käytettäväksi (kuvio 15).

Sama konfiguraatio toistetaan toisen pään päätelaitteelle vastapuolen IP-osoitteilla. Tämän jälkeen käytössä tulisi olla toimiva IPSec VPN-yhteys. Yhteys voidaan vielä todentaa toimivaksi Netgearin asetuksista (kuvio 16).



KUVIO 15. VPN Policy IPSec VPN yhteydelle

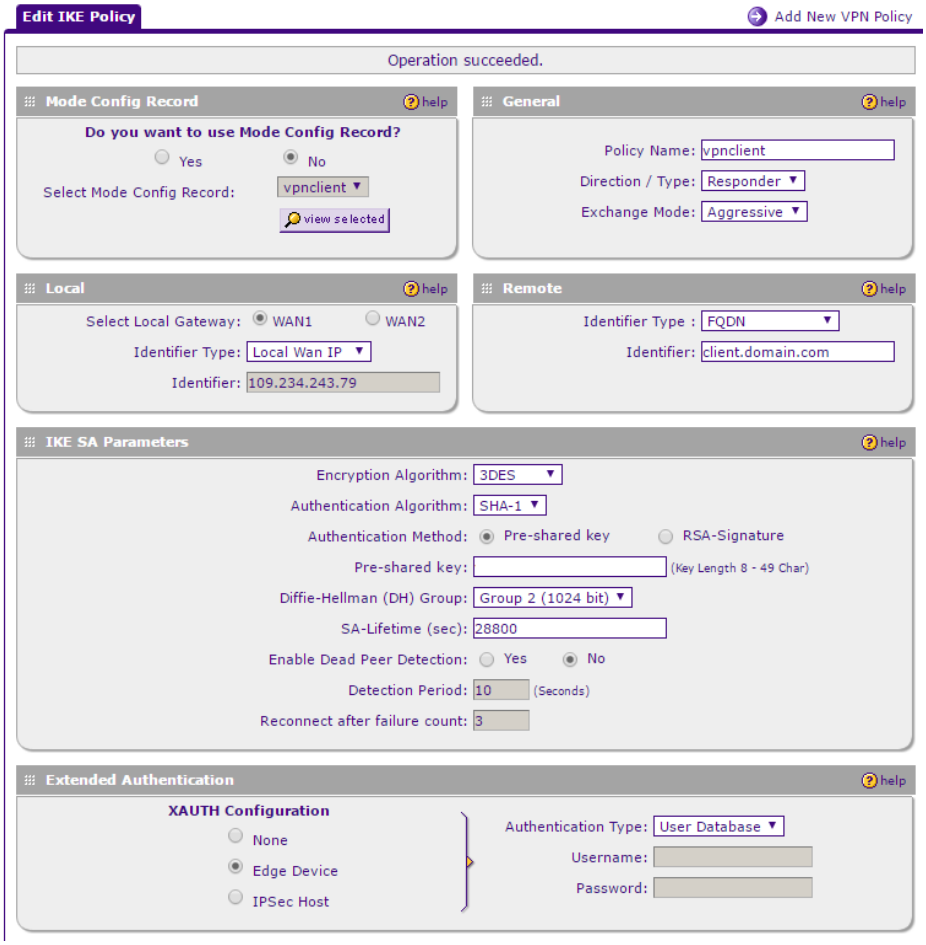


KUVIO 16. Yhteyden toimivuuden todennus

5.9 IPSec VPN Client valmiuden luominen

IPSec VPN Client valmiutta varten luodaan IKE policy lähes samalla kaavalla kuin IPSec VPN. Ensimmäisenä annetaan IKE policylle nimi,

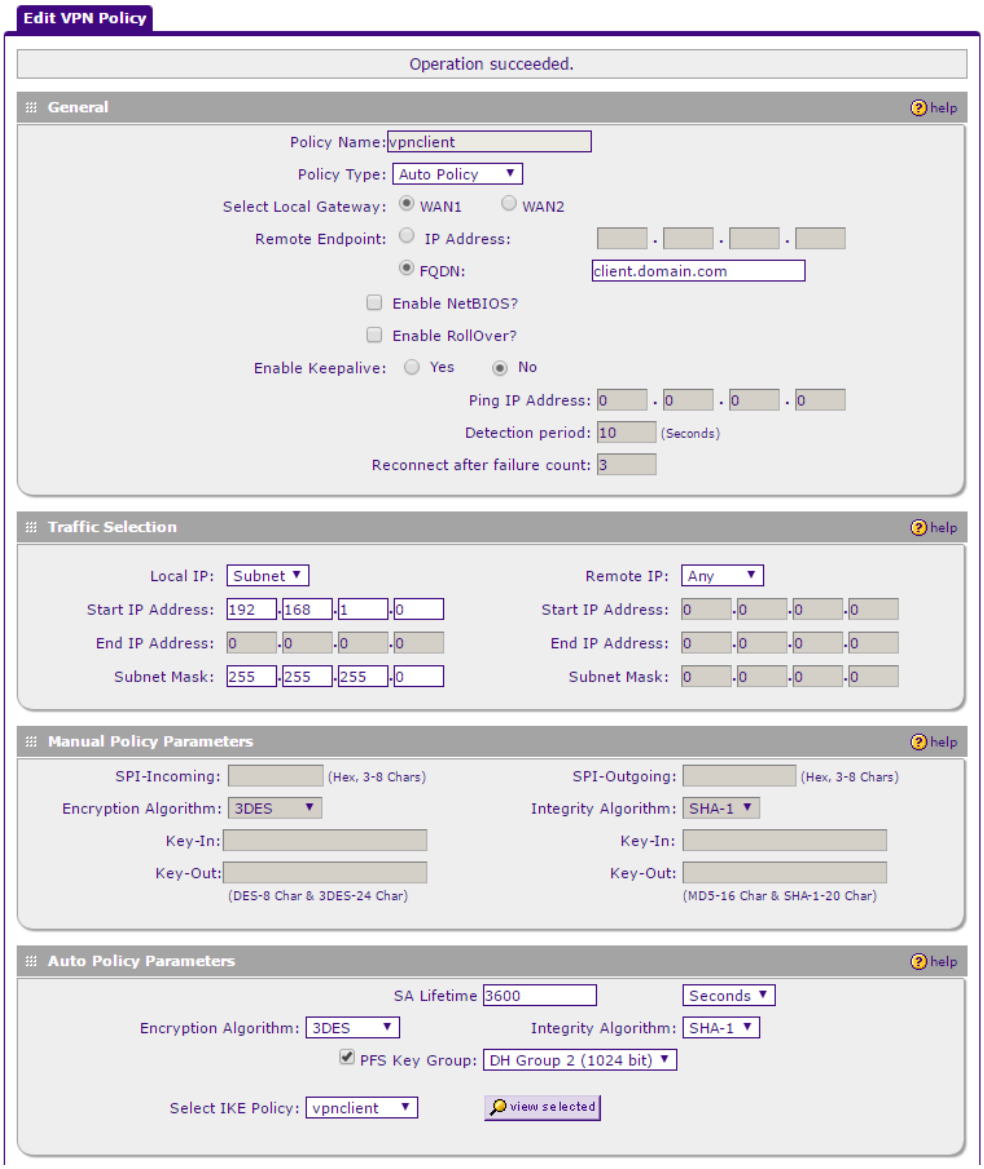
määritellään liikenteen suunta, mikä on tässä tapauksessa vain vastaanottava, koska kyseessä on yhdensuuntainen yhteys johon VPN Client ottaa yhteyden. Pääasetuksista määritellään lisäksi avaimenvaihtotyyppi. Lisäksi määritellään lokaali yhdyskäytävä, sekä etäkäyttöä varten FQDN (Fully Qualified Domain Name), eli täysi domainnimi tunnisteeksi. Seuraavaksi määritellään halutut salaus ja autentikointi algoritmit sekä haluttu PSK-avain ja Diffie-Hellman ryhmä. Lopuksi määritellään käyttöön reunalaite autentikointi ja autentikoinnin tyypiksi käyttäjä tietokanta, jotta vain luodut käyttäjät voivat ottaa IPSec VPN Client-yhteyden (kuvio 17).



KUVIO 17. IKE Policy IPSec VPN Client valmiudelle

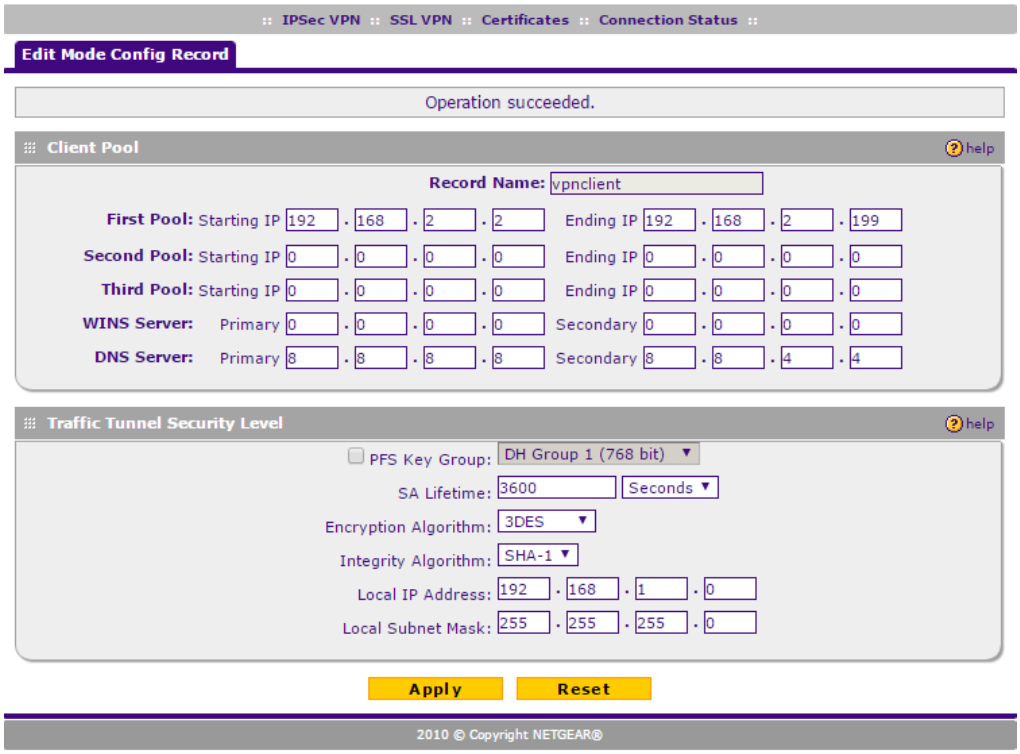
IPSec VPN Client valmiudelle pitää myös luoda VPN policy. Kyseisessä VPN Policyssä määritellään policylle nimi sekä aiemmin IKE policyssä määritelty paikallinen yhdyskäytävä sekä etäkäytön täysi domainnimi. Seuraavaksi määritellään sisäverkko johon etäyhteys clientillä hautaan,

sekä IP-osoitteet joista halutaan pääsy kyseiseen sisäverkkoon. Lopuksi määritellään halutut enkryptaus- ja tunnistealgoritmit, sekä aiemmin luotu IKE policy (kuvio 18).



KUVIO 18. VPN Policy IPSec VPN Client valmiudelle.

IPSec VPN client yhteyttä varten täytyy luoda oma IP-osoite alue, jota Netgear FVS336Gv2 VPN-palomuuri jakaa uusille IPSec VPN client-yhteyksille. IP-osoite alueen tulee olla eri kuin sisäverkon IP-osoite alue. (kuvio 19).



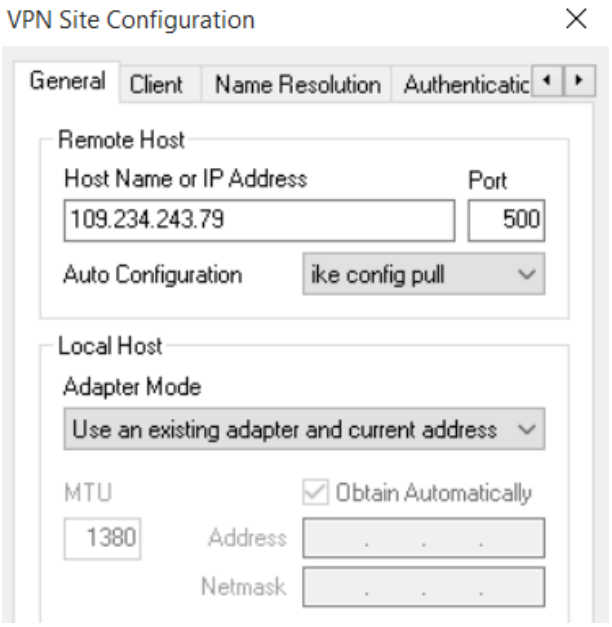
KUVIO 19. IP-osoite alue IPSec VPN client-yhteyksiä varten.

Yrityksen työntekijöille luodaan tunnukset IPSec VPN client-yhteyttä varten. Käyttäjille määritellään halutut tunnukset sekä yhteyden tyypiksi IPSec VPN yhteys.

5.10 VPN Client

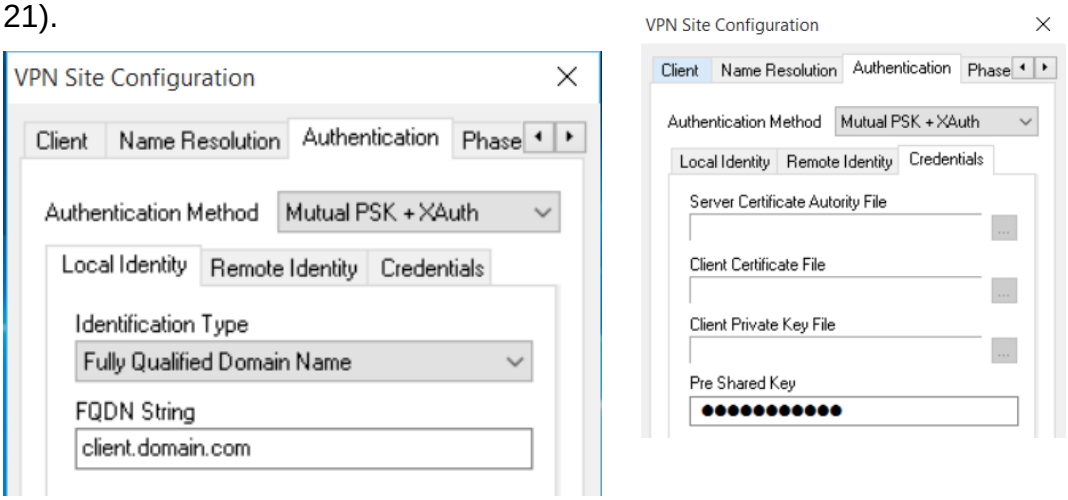
VPN Clienttinä käytettiin Shrew Soft VPN Clienttiä aiemman vertailun perusteella. Shew Soft osottautui hyvin helppokäyttöiseksi VPN Client ohjelmaksi. Shrew Soft oli vertailluista ohjelmista ainoa ilmainen.

Ensimmäisenä ryhdyttiin luomaan uutta VPN-yhteyttä ja nimettiin yhteys toimipaikan mukaan. Seuraavaksi määriteltiin kohteen pääasetukset eli Vantaan toimipisteen IP-osoite, sekä mitä verkkosovitinta käytetään (kuvio 20).



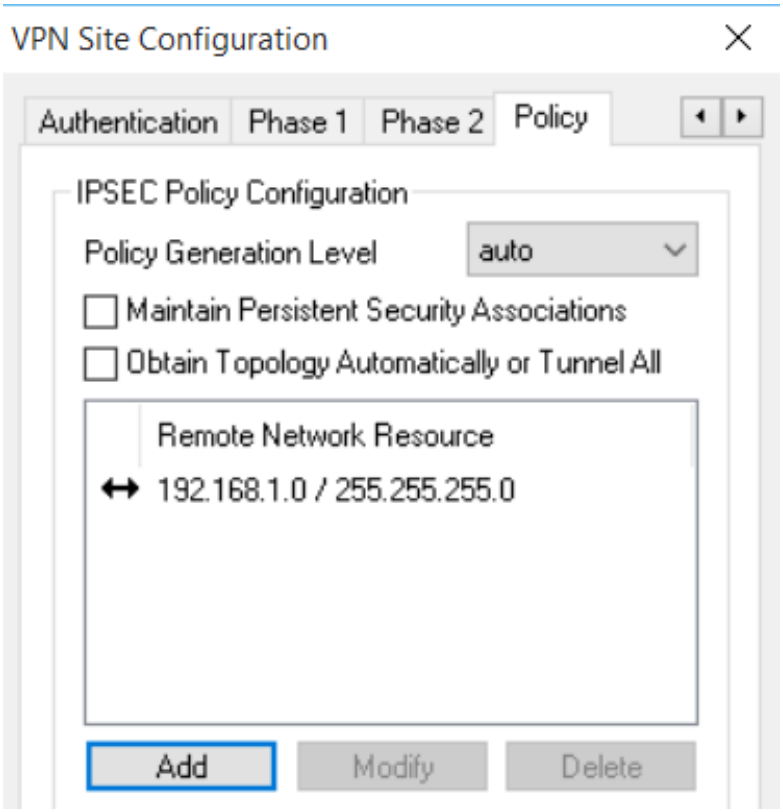
KUVIO 20. VPN Clientin pääasetukset

Autentikointi menetelmäksi valittiin Mutual PSK + XAuth vastaamaan aiemmin Netgear FVS336Gv2 VPN-palomuuriin määritettyä autentikointi asetusta. Paikalliseksi tunnisteeksi määriteltiin *client.domain.com* (kuvio 21).



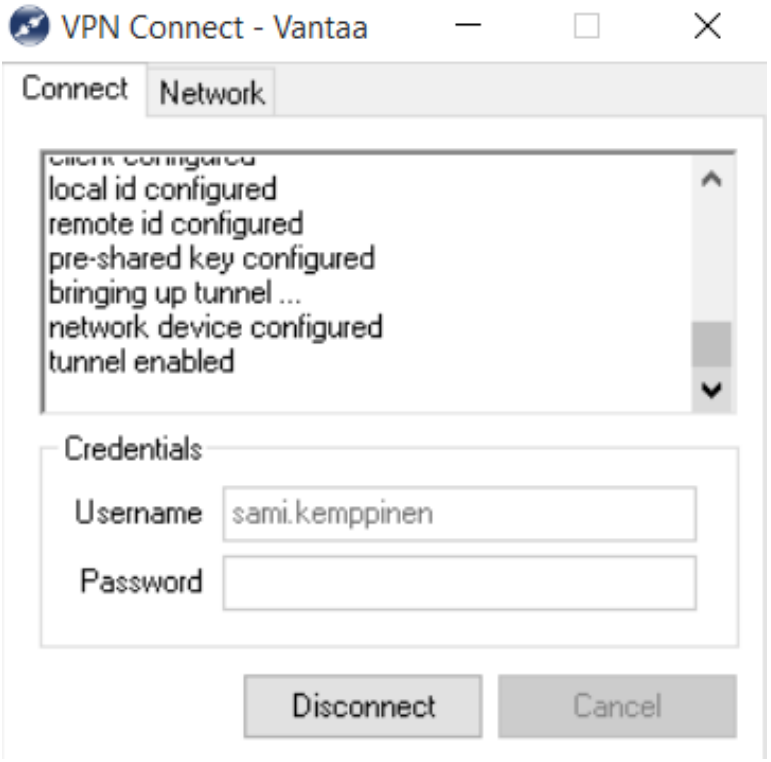
KUVIO 21. VPN Clientin autentikointiasetukset

Policy asetuksista otettiin pois päältä automaattinen topologian hakeminen. Lisäksi määriteltiin etäkäytettävän sisäverkon IP-osoiteavaruus (kuvio 22).



KUVIO 22. VPN Client Policy asetukset

Lopuksi todennettiin VPN Clientin toimivuus yhdistämällä VPN-tunneliin. Kun konfiguraatio oli todettu toimivaksi, vietiin kyseinen konfiguraatio omaksi tiedostoksi, jotta yrityksen työntekijän tarvitsee vain ladata kyseinen konfiguraatio tiedosto ja tuoda se omaan Shrew Softin VPN Clienttiin (kuvio 23).

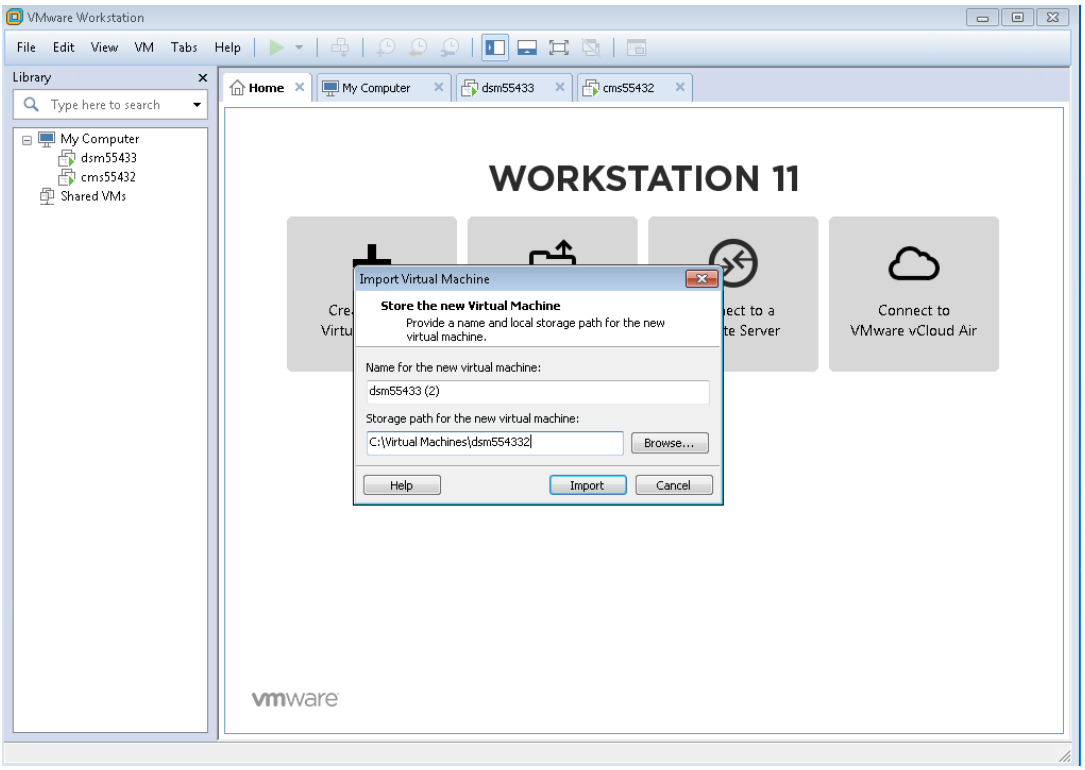


KUVIO 23. VPN Clientin toimivuuden todennus

5.11 VMware Workstationin asennus ja konfigurointi

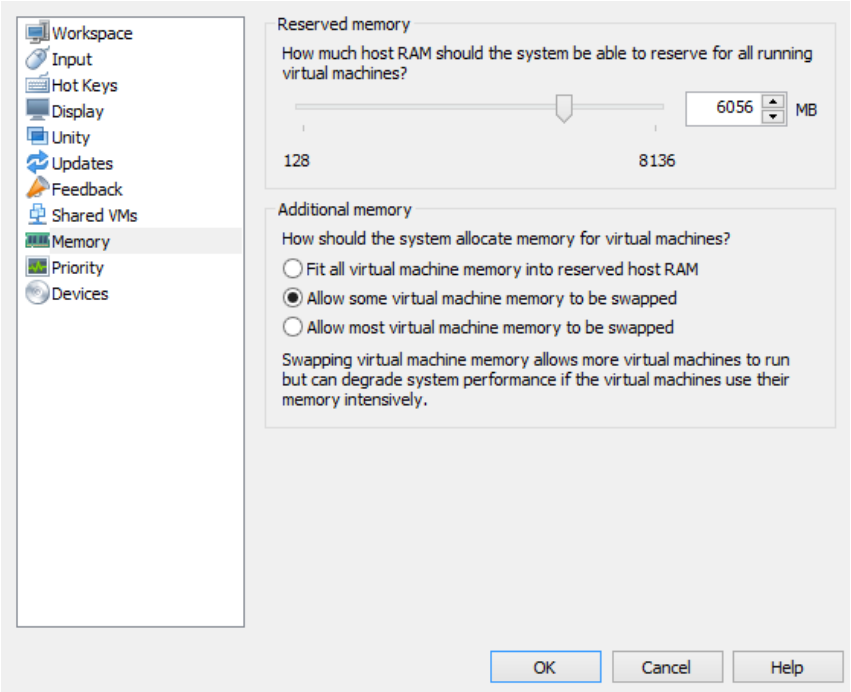
Windows Server 2012 R2:n päälle asennettiin VMware Workstation 11.0 perusasennuksena. Tämän jälkeen VMware määriteltiin käynnistymään automaattisesti Windowsin uudelleenkäynnistyksen yhteydessä, jotta virtuaalipalvelimia ei tarvitse itse käynnistää uudelleen, jos Windows Server 2012 R2 jostain syystä käynnistyy uudelleen.

VMware Workstation ohjelman asennuksen jälkeen ohjelmaan lisättiin kaksi virtuaalipalvelinta (kuvio 24). Virtuaalipalvelimet olivat valmiiksi asennettuja Linux-pohjaisia virtuaalipalvelimia, joita käytetään erinäisten palveluiden demonstroimiseen asiakkaille. Toinen palvelimista oli CMS (Content Management System), jonka tarkoituksena on tuoda digitaalista sisältöä näyttöihin. Toinen palvelin oli DSM (Digital Signage Manager), jolla valvotaan digitaalista sisältöä, jota tuodaan näytöille CMS:n kautta.

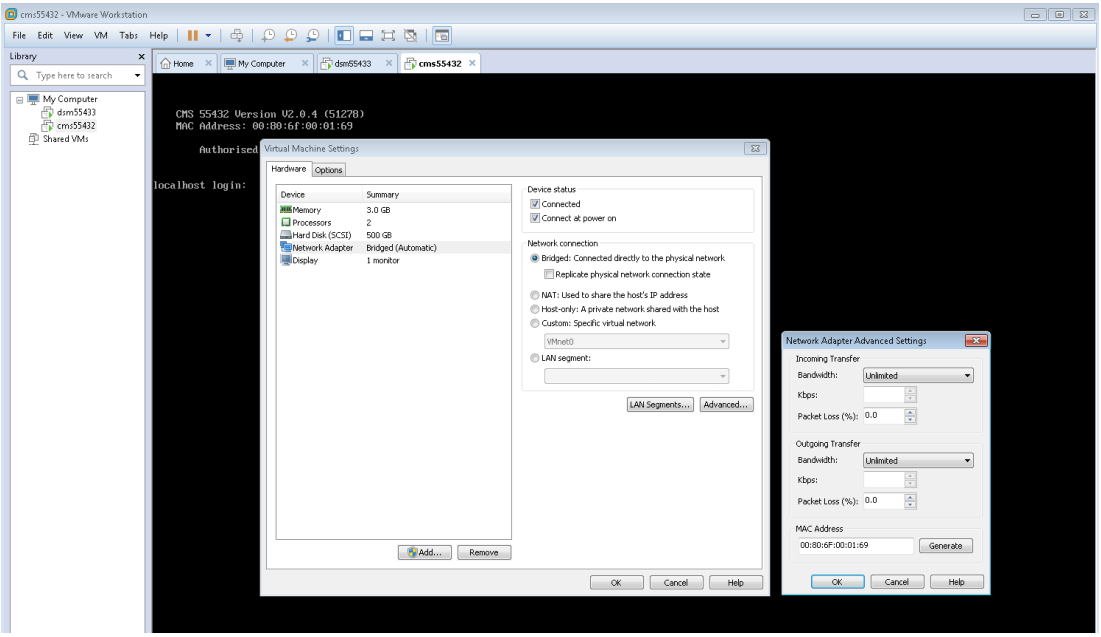


KUVIO 24. Valmiin koneen importtaaminen VMware Workstationiin

Seuraavaksi VMware Workstationin asetuksista määriteltiin kuinka paljon RAM (Random-access memory) muistia järjestelmä saa varata käyttöön käynnissä oleville virtuaalikoneille (kuvio 25). Myös valmiille virtuaalikoneille määriteltiin asetukset. RAM muistin määräksi asetettiin 3.0GB ja prosessorien ytimien määräksi 2 kappaletta. Lopuksi vaihdettiin asetuksista MAC-osoite (Media Access Control) vastaamaan valmiin virtuaalikoneen osoitetta (kuvio 26).



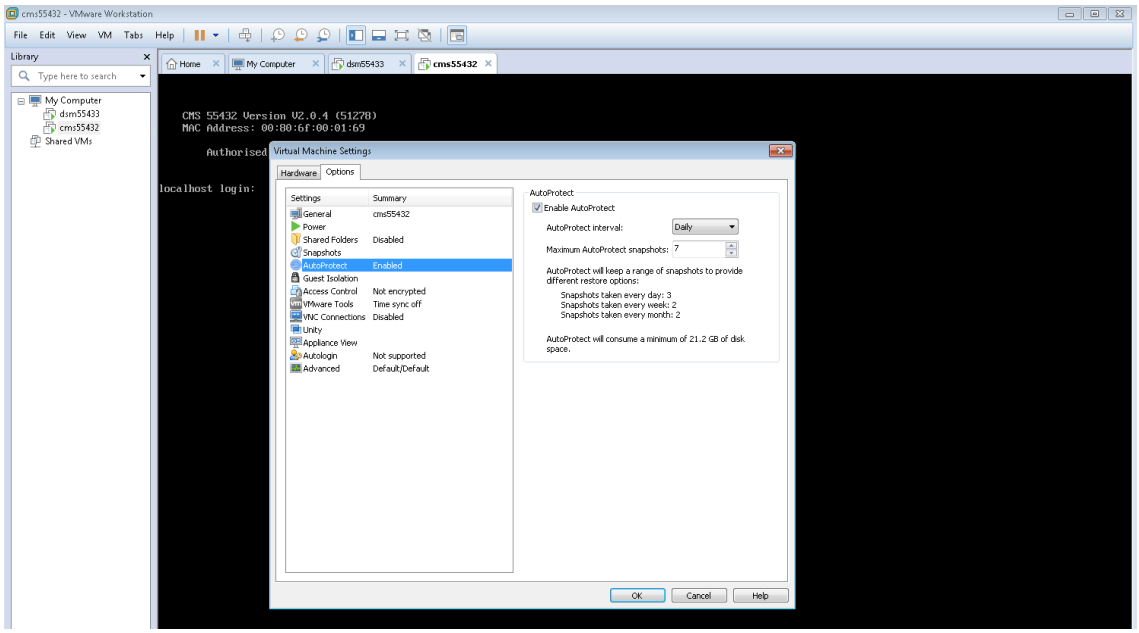
KUVIO 25. Muistin varaaminen VMware Workstationille



KUVIO 26. VMware virtuaalikoneen asetukset

VMware workstationille konfiguroitiin AutoProtect käyttöön, jotta saadaan automatisoitua varmuuskopiot. AutoProtectin tehtävänä on ottaa varmuuskopioita virtuaalikoneista tietyin aikavälein. Normaali asetuksilla AutoProtect säilyttää 7 uusinta varmuuskopiota. 3 näistä varmuuskopioista on 1-3 päivää vanhoja, 2 seuraavaa varmuuskopiota on 1:n ja 2 viikon

takaiset varmuuskopiot, sekä 2 viimeistä varmuuskopiota on 1:n ja 2 kuukauden takaiset varmuuskopiot. AutoProtectin avulla voidaan palata vaikka kuukauden tai viikon takaiseen varmuuskopioon tarvittaessa (kuvio 27).



KUVIO 27. VMware AutoProtectin konfigurointi

5.12 Lopputulos

Lopputuloksena vertailtiin yrityksen tietoverkkoa ennen ja jälkeen muutosten (taulukko 10). Toimipisteiden välille luotiin IPSec VPN-yhteys. Työntekijöiden etäyhteyttä varten luotiin IPSec VPN -ohjelmisto mahdollisuus. Virtualisoitiin yritykselle palvelin. Määriteltiin palvelimelle automaattiset varmuuskopiot. Korjattiin huono WLAN konfiguroimalla ja asentamalla uusi WLAN-tukiasema.

Lopputuloksessa todettiin, että kaikkiin kohtiin löydettiin ratkaisu ja parannukset olivat onnistuneita. Tietoverkkoa on myös mahdollista parantaa jatkossa hankkimalla toinen internet yhteys nykyisen rinnalle ja luoda yhteyksien välille kahdennus.

TAULUKKO 10. Lopputulosten vertailu.

Toimimattomuus	**Uudistus**
Yhteys toimipisteitten välillä	IPSec VPN-yhteys
Etäyhteys verkkoon	IPSec VPN -ohjelmisto
Virtualisointi	VMware Workstation Pro
Varmuuskopiot	Workstation Pro automatisoidut varmuuskopiot
Huono WLAN	Uusi AC-luokan tukiasema

6 YHTEENVETO

VPN ja virtualisointi ovat nykypäivänä monelle yrityksille tärkeitä osa-alueita. Suurin osa yrityksistä, joilla on monta toimipistettä, käyttävät VPN-tekniikkaa yrityksen sisäverkkojen yhdistämiseksi. Virtualisointi on myös yleistynyt yrityksissä, koska sen tuomat edut ovat suuria. Virtualisointi tarjoaa yritykselle kustannustehokasta ja joustavaa ratkaisua palvelintarpeisiin, ja todennäköisesti sen käyttö tulee lisääntymään huomattavasti.

Työn tavoitteena oli perehtyä yrityksen tietoverkon nykyiseen tilaan, ja kartoittaa millaisia muutoksia yrityksen tietoverkkoon tarvitsee tehdä, jotta yritykselle saadaan rakennettua toimiva demonstraatiotila myynnin kehittämistä varten. Toisena tavoitteena oli luoda kartoituksesta ratkaisumalli ja toteuttaa se yritykselle. Työn teoriaosuudessa käytiin läpi käytäntöön liittyviä osa-alueita, kuten tietoverkkoja, VPN-tekniikkaa sekä virtualisointia.

Työn tavoite täyttyi, kun yrityksen kaksi toimipistettä oli yhdistetty IPSec VPN-tekniikalla ja toiselle toimipisteelle asennettu virtualisointialusta, ja virtualisointialustalle kaksi toimivaa virtuaalipalvelinta. Lisäksi IPSec VPN Client-yhteys saatiin toimimaan ja osa yrityksen työntekijöistä on ottanut sen jo käyttöön.

Yrityksen tietoverkkoa on mahdollista parantaa myöhemmin hankkimalla toinen internet-yhteys kahdentamista varten, koska Netgear FVS336Gv2 VPN-palomuurissa on kaksi WAN-porttia ja kuormantasauspalvelun mahdollisuus. Lisäksi Lahteen olisi hyvä hankkia parempi AC-standardin WLAN-tukiasema vanhan ADSL WLAN-reitittimien tilalle.

Tietoverkkojen parantaminen ja uudistaminen tulee olemaan tärkeässä asemassa aina. Tulevaisuus tuo tullessaan uusia laitteita, haavoittuvuuksia, uhkia sekä mahdollisuuksia. Uhkilta ei voida välttyä, jos jätetään yritysten tietoverkkojen uudistaminen ja keskitytään vain tähän hetkeen. Myös mahdollisuudet jäävät käyttämättä, jos ei katsota tulevaisuuteen. Tietoliikenne on radikaalisti muuttuva ala, jonka

muutoksien perässä on pysyttävä, jos halutaan välttyä isoilta harmeilta mutta myös pysyä kehityksen perässä.

LÄHTEET

Angeles, S. 2014. The Pros and Cons of Virtualization [viitattu 28.3.2016]. Saatavissa: http://www.businessnewsdaily.com/6014-pros-cons-virtualization.html

BBC 2014. What is a Network? [viitattu 17.4.2016]. Saatavissa: http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/2networksrev1.shtml

Chenley. 2011. Hypervisors [viitattu 29.3.2016]. Saatavissa: https://blogs.technet.microsoft.com/chenley/2011/02/09/hypervisors/

Cisco 2008a CCNA4, Chapter 7: Securing Site-to-Site Connectivity [viitattu 2.4.2016]. Saatavissa: http://reppu.lamk.fi/pluginfile.php/777102/mod_folder/content/0/CCNA4_Chapter7.pdf

Cisco 2008b How Virtual Private Networks Work [viitattu 2.4.2016]. Saatavissa: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Das, K. 2008. IPv6 Addressing [viitattu 15.4.2016]. Saatavissa: http://www.ipv6.com/articles/general/IPv6-Addressing.htm

Gale, T. 2007. Wide Area Networks (WANs) [viitattu 17.4.2016]. Saatavissa: http://www.encyclopedia.com/topic/wide_area_network.aspx

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen Porvoo: WS Bookwell.

Ictum Oy 2016. [viitattu 02.03.2016]. Saatavissa: http://www.ictum.fi

Jimm’s 2015. [viitattu 08.09.2015]. Saatavissa: http://www.jimms.fi

Juniper 2015. Understanding Generic Routing Encapsulation [viitattu 2.4.2016]. Saatavissa:

http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/gre-tunnel-services.html

Kleyman, B. 2012. Hypervisor 101: Understanding the Virtualization Market [viitattu 30.3.2016]. Saatavissa: http://www.datacenterknowledge.com/archives/2012/08/01/hypervisor-101-a-look-hypervisor-market/

Koulutus & konsultointi 2016a. Tietoverkkojen historiasta [viitattu 17.4.2016]. Saatavissa: http://www.2kmediat.com/tietoverkot/historiaa.asp

Koulutus & konsultointi 2016b. Tietoverkon fyysiset osatekijät [viitattu 17.4.2016]. Saatavissa: http://www.2kmediat.com/tietoverkot/tekijat1.asp

Microsoft 2016a. The OSI Model's Seven Layers Defined and Functions Explained [viitattu 12.4.2016]. Saatavissa: https://support.microsoft.com/en-us/kb/103884

Microsoft 2016b Understanding PPTP [viitattu 1.4.2016]. Saatavissa: https://technet.microsoft.com/library/cc768084.aspx

Microsoft 2009c. Virtual Private Networking: An Overview [viitattu 27.03.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/bb742566.aspx

Mitchell, B. 2015. IP Tutorial, Subnet Masks and Subnetting [viitattu 16.4.2016]. Saatavissa: http://compnetworking.about.com/od/workingwithipaddresses/l/aa043000b.htm

Netgear 2016. VPN Client Professional Software [viitattu 17.4.2016]. Saatavissa: http://www.netgear.com/business/products/security/vpn-software.aspx

Puska, M. 2000 Lähiverkkojen tekniikka, Pro training. Jyväskylä: Gummerus

RFC 2460 1998. Internet Protocol, Version 6 (IPv6) Specification [viitattu 15.4.2016]. Saatavissa: http://tools.ietf.org/html/rfc2460

Saxena, A. 2013. Quick overview of IPSEC and SSL VPN technologies [viitattu 18.4.2016]. Saatavissa: https://supportforums.cisco.com/document/113896/quick-overview-ipsec-and-ssl-vpn-technologies

Shrew Soft 2010. Shrew Soft VPN Client: Administrators Guide [viitattu 17.4.2016]. Saatavissa: https://www.shrew.net/static/help-2.1.x/vpnhelp.htm

The Gale Group 2002. Local Area Network (LAN) [viitattu 17.4.2016]. Saatavissa: http://www.encyclopedia.com/topic/local_area_network.aspx#1

The Green Bow 2016. TheGreenBow VPN Client [viitattu 17.4.2016]. Saatavissa: http://www.thegreenbow.com/vpn_client.html

Wikipedia 2016a. Citrix_Systems [viitattu 4.4.2016]. Saatavissa: https://en.wikipedia.org/wiki/Citrix_Systems

Wikipedia 2016b. Hyper-V [viitattu 4.4.2016]. Saatavissa: https://en.wikipedia.org/wiki/Hyper-V

Wikipedia 2016c OSI-malli [viitattu 12.4.2016]. Saatavissa: https://fi.wikipedia.org/wiki/OSI-malli

Wikipedia 2016d. VMware [viitattu 4.4.2016]. Saatavissa: https://en.wikipedia.org/wiki/VMware

VMware 2016a. Company [viitattu 4.4.2016]. Saatavissa: http://www.vmware.com/company/

VMware 2016b. Virtualization [viitattu 28.3.2016]. Saatavissa: https://www.vmware.com/virtualization/how-it-works.html

VMware 2016c. VMware Fusion [viitattu 13.4.2016]. Saatavissa: http://www.vmware.com/products/fusion/compare.html

VMware 2016d. VMware Workstation [viitattu 13.4.2016]. Saatavissa: http://www.vmware.com/products/workstation/compare.html