VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Ari Niemi

YRITYSVERKON KEHITTÄMINEN JA PÄIVITYS

Tekniikka ja Liikenne
2011

VAASAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Ari Niemi
Opinnäytetyön nimi	Yritysverkon kehittäminen ja päivitys
Vuosi	2011
Kieli	suomi
Sivumäärä	48
Ohjaaja	Antti Virtanen

Tämän opinnäytetyön tarkoituksena oli päivittää aiemmin Juho Latvan opinnäytetyönä tekemä pienen yrityksen testiverkko, joka oli toteutettu tietotekniikan osastolle opetuskäyttöön. Testiverkkoon kuului intraverkko ja DMZ-alue. Verkon toteutusta kehitettiin korvaamalla palomuurina toiminut Ipcop-kone Vyatta Core:lla. Domain-nimi ja julkiset IP-osoitteet päivitettiin Open IT Lab:n alaisuuteen ja sertifikaatit toteutettiin uuden domain-nimen mukaisesti. Etähallintaa kehitettiin jakamalla intraverkon ja DMZ-alueen etäyhteydet ja palvelut omien julkisten IP-osoitteiden taakse.

Opinnäytetyössä tutustutaan yritysverkon rakentamiseen ja käydään läpi keskeisimpiä palveluita. Työssä tutustutaan myös tietoturva-asioihin ja Windows-domainissa oleviin palveluihin. Opinnäytetyössä käytetään kahta Windows Server 2008 -palvelinta, Vyatta Core -palomuuria ja Zyxel-kytkintä intraverkossa. Verkossa toteutettiin Windows-palvelimien avulla WWW-, DNS-, levy ja sähköpostipalvelimet, Terminal Services sekä käyttäjien hallinta Windows Active Directory -domainissa. WWW-palvelin toteutettiin Windows IIS7:n avulla. Opinnäytetyön keskeisin asia on Vyatta Core -palomuuri, joka jakaa verkon kahteen osa-alueeseen, toimii DHCP-palvelimena ja tekee tarvittavat porttiohjaukset NAT-muunnoksen avulla.

Yritysverkkoa rakentaessa on hyvä panostaa verkon suunnitteluun, miettiä mitä palveluita todella tarvitaan ja minkä järjestelmien avulla ne kannattaa toteuttaa. Vaihtoehtoja on useita ja eri järjestelmien yhteensopivuuksiin kannattaa kiinnittää huomiota. Kehitettävää jäi vielä käyttäjäkohtaisissa levypalveluissa, joihin tulisi päästä kirjautumaan työasemasta riippumatta. Levypalvelut olisi myös hyvä toteuttaa sekä Windows- että Linux-palvelimien avulla. Työn suorituksessa oli ongelmia Windows-palvelimien käyttö-oikeuksissa, mistä johtuen ei pystytty määrittämään, mitkä käyttäjät pystyvät lisäämään koneen domainiin.

Avainsanat: Windows Server, Vyatta Core, Active Directory, DNS

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikan koulutusohjelma

ABSTRACT

Author	Ari Niemi
Title	Upgrading and Developing a Company Network
Year	2011
Language	Finnish
Pages	48
Name of Supervisor	Antti Virtanen

The purpose of this thesis was to upgrade earlier version of a small company network originally made by Juho Latva. The network was developed to IT department for teaching purposes. The test network included DMZ area and an intra network. Implementation of the network was developed by replacing the Ipcop firewall with Vyatta Core firewall. The new domain name and public IP addresses were received from Open IT Lab. The Certificates were updated according to the new domain name. The remote management was developed by giving the intra and DMZ networks separate public IP addresses.

This thesis introduces the construction and essential services of the corporate network. This thesis also includes data security and different services in Windows domain. The network was built with two Windows Server 2008 servers, Vyatta Core firewall and Zyxell switch. Windows servers were used for Web server, DNS server, File server, Terminal Services, mail server and user management in Windows Active Directory Domain Services. Web server was implemented with Windows IIS7. The most important part of the thesis is Vyatta Core firewall, which divides the network in two areas, works as DHCP server and makes all the necessary port forwarding with Network Address Translation.

Building of the company network design requires a proper planning. You need to know what services are really needed and by means of which systems they can be implemented. There are several options and compatibilities with different systems should be considered before using them. The implementation could be improved with proper user file services, which should be available to user regardless of the workstation used for login. File services would also be conveniently set up with Windows and Linux servers. Some problems occurred with user rights assignment in Windows server. Because of this it was not possible to determine which users are able to add a machine to the domain.

Keywords: Windows Server, Vyatta Core, Active Directory, DNS

LYHENNELUETTELO

AD	Active Directory Käyttäjätietokanta
AD DS	Active Directory Domain Services Käyttäjätietokannan domain-palvelut
DAP	Directory Access Protocol Hakemistopalvelujen verkkoprotokolla
DHCP	Dynamic Host Configuration Protocol IP-osoitteiden jakomenetelmä
DMZ	Demilitarized Zone Demilitarisoitu alue, eteisverkko
DNS	Domain Name Services Nimipalvelujärjestelmä
EPMAP	End Point Mapper Määrittää päätepisten RPC-yhteyksille
FTP	File Transfer Protocol Tiedonsiirtoprotokolla
HTTP	Hypertext Transfer Protocol Hypertekstin siirtoprotokolla
HTTPS	Hypertext Transfer Protocol Secure Salattu hypertekstin siirtoprotokolla
IIS	Internet Information Services Microsoftin WWW-palvelin
IMAP	Internet Message Access Protocol Sähköpostin lukemiseen tarkoitettu protokolla

IP	Internet Protocol Internetprotokolla
IPSEC	Internet Protocol Security Architecture Tietoliikenneprotokolla internetyhteyksien salaamiseen
IPsec	IP Security Architecture Tietoliikenneprotokolla yhteyden turvaamiseen
IPv4	Internet Protocol Version 4 internetprotokolla versio 4
IPv6	Internet Protocol Version 6 Internetprotokolla versio 6
LDAP	Lightweight Directory Access Protocol Hakemistopalvelujen verkkoprotokolla
LSA	Local Security Authority Protokolla paikallisten käyttöoikeuksien ylläpitämiseen
NAT	Network Address Translation Osoitteenmuutos
NETBIOS	Network Basic Input/Output System Verkkoprotokolla koneiden keskustelemiseen lähiverkossa
NFS	Network File System Verkkoprotokolla levyjakamiseen
OSI	Open Systems Interconnection Reference Model Tietoliikenteen käsitemalli
OU	Organizational Unit Hallintayksikkö
POP	Post Office Protocol

	Sähköpostin hakemiseen tarkoitettu protokolla
RDP	Remote Desktop Protocol Etäyhteysprotokolla
RPC	Remote Procedure Call Sovelluskerroksen kommunikointiprotokolla
SAM	Security Account Manager Tietokanta paikallisten käyttäjätietojen ylläpitämiseen
SMB	Server Message Block Verkkoprotokolla levyjakamiseen Microsoft-tuotteilla
SMTP	Simple Mail Transfer Protocol Protokolla sähköpostiviestien välittämiseen palvelimien välillä
SSL	Security Socket Layer Salausprotokolla
SSH	Secure Shell Salattu tietoliikenneprotokolla
TCP	Transmission Control Protocol Yhteydellinen kuljetusprotokolla
TS	Terminal Services Windowsin etäyhteys
UDP	User Datagram Protocol Yhteydetön tiedonsiirtoprotokolla
VPN	Virtual Private Network Virtuaalinen lähiverkko
WWW	World Wide Web Internet

SISÄLLYS

1 JOHDANTO

Tietoliikenneverkolla on keskeinen rooli yrityksen toiminnan ylläpitämisessä ja sen avulla voidaan hallinnoida tehokkaasti ja turvallisesti yrityksen tärkeitä asiakirjoja. Jokainen yritys on erilainen ja tarvitsee omanlaisensa palvelut verkkoonsa. Pienelläkin yrityksellä voi olla kattava verkkoratkaisu. Tärkeimmät toiminnot yritysverkossa ovat: tiedosto- ja tulostuspalvelut, käyttäjien hallinta, työpaikan sisäinen intraverkko ja toimintaa ylläpitävät järjestelmät. Suuressa verkossa käyttäjien ja käyttöoikeuksien hallinta pystytään toteuttamaan tehokkaasti ryhmien avulla, jolloin käyttäjät perivät valmiiksi määritellyt käyttöoikeudet eri ryhmistä. Levypalveluiden avulla käyttäjillä on samat resurssit käytettävissä riippumatta siitä, millä työasemalla järjestelmään on kirjauduttu.

Tässä opinnäytetyössä rakennetaan pienen yrityksen verkko, jossa vaaditaan seuraavat palvelut: käyttäjä- ja hakemistopalvelu, sähköpostipalvelin, WWW-palvelin, DNS-palvelin, DHCP-palvelin, NAT-porttiohjaukset, palomuuri ja levypalvelin. Opinnäytetyössä tutustutaan myös verkon eri osa-alueisiin. DMZ-alue (Demilitarized Zone) on tarkoitettu verkon julkisille palveluille, jotka ovat turvallisuussyistä erillään intraverkon palveluista. Intraverkko on yrityksen sisäinen verkko, jonne ei ulkoverkosta ole suoraa pääsyä. Intraverkkoon voidaan muodostaa salattu yhteys Terminal Services -palvelun avulla.

2 VERKKOTOPOLOGIA

2.1 Ongelman kuvaus

Vaasan ammattikorkeakoulun tietotekniikkaosastolle on aiemmin toteutettu pienyritysverkkoa vastaava verkkoratkaisu opetuskäyttöön. Tämä toteutus tehtiin opinnäytetyönä, jonka lopputulokseen jäi vielä kehitettävää. Verkon on tarkoitus vastata perusidealtansa koulun omaa verkkoa, mutta pienemmässä muodossa. Lisäksi verkkoon tulee olla mahdollisuus päästä käsiksi opetuskäyttöä varten. Aiemmassa työssä valittiin liian paljon asioita toteutettavaksi yhdelle henkilölle, ja tästä johtuen moni asia jäi keskeneräiseksi. Ongelmia ilmeni domain-nimien ristiriitaisuudessa koulun domain-nimien kanssa. Tästä johtuen sähköpostipalvelut eivät toimineet lähetettäessä sähköpostia koulun sähköpostiosoitteisiin. Sertifikaatin käyttäminen toteutettiin melko hankalasti, koska käyttäjän tuli tietää minne se asennetaan itse ilman erillistä ohjeistusta. Näiden ongelmien korjaamisen lisäksi verkkoratkaisu haluttiin toteuttaa vaihtamalla palomuurina toiminut Ipcop-kone Vyatta Core:n. Käytössä olleet tietokoneet korvattiin uusilla laitteilla, jotka sijoitettiin Open IT Lab:n palvelinhuoneeseen Vaasan ammattikorkeakoululle. Työhön käytettävät DNS- ja IP -osoitteet tulivat Open IT Lab:n kautta.

2.2 Vaatimusmäärittely

Opinnäyteyön aloittamista varten tehtiin vaatimusmäärittely. Tässä vaatimusmäärittelyssä listattiin keskeisimmät asiat työn suorittamista varten. Koska kyseessä on aiemman opinnäytetyön korjaaminen, mietittiin suurimmat ongelmakohdat ja tehtiin työn tavoitteet niiden mukaan. Vaatimusmäärittelyssä käydään seuraavat asiat:

Prioriteetti 1

- Uusi domain-nimi ja IP-osoitteet Open IT Lab:sta
- Sertifikaatit uuden domain-nimen mukaan
- Etähallinta ja toimiva käyttö sisä- ja ulkoverkosta
- Vyatta Core -palomuuri

- DMZ:n palvelut omalla julkisella IP-osoitteella
- Sisäverkon Domain Name Service ja Active Directory
- Tiedostopalvelut
- Uudet koneet ja siirto Open IT Lab:n palvelinhuoneeseen

Prioriteetti 2

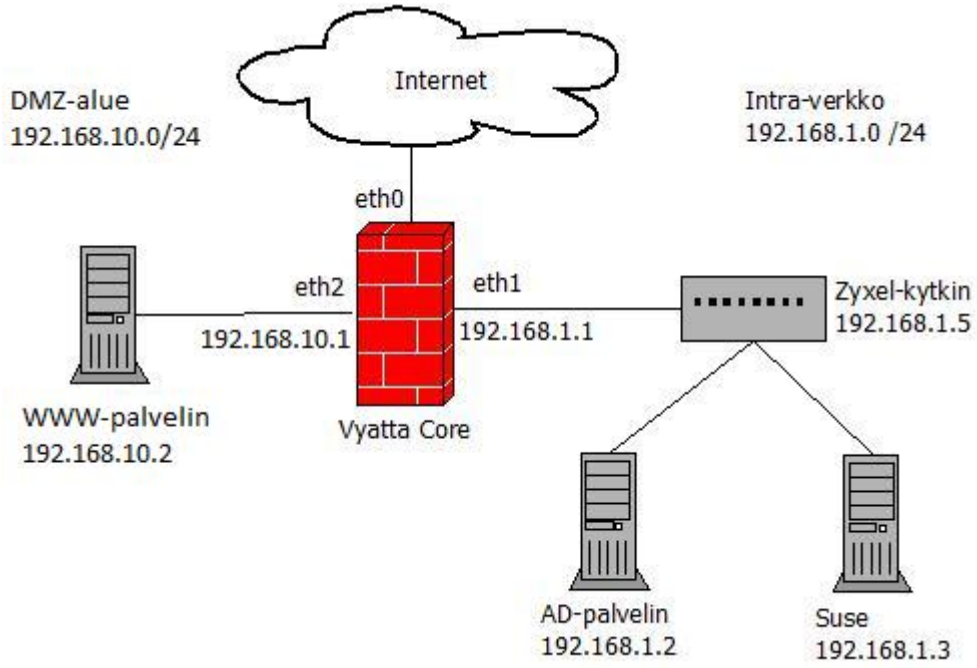
- VPN-yhteys
- LDAP
- Sähköpostipalvelu
- Verkonhallinta

Prioriteetti 3

- Terminal Services
- WWW-palvelu

2.3 Verkkokuvaus

Kuvassa 1 on esitetty suunnitellun verkon topologia ja laitteiden käyttämät IP-osoitteet. Vyatta Core -koneella verkko jaetaan kolmeen osa-alueeseen, jotka ovat: intra, DMZ ja public. DMZ-alueen tarkoitus on eristää verkon julkiset palvelut muusta verkosta turvallisuussyistä. Intraverkossa on toteutettu AD- ja levypalvelut. Public alueella tarkoitetaan verkon julkista osaa, johon internet on kytketty.



Kuva 1. Verkkotopologia.

Internetyhteys tulee Open IT Lab:n palomuurin kautta, joka tekee porttiohjauksen ulkoverkon osoitteista 85.134.47.40 ja 85.134.47.41 sisäverkon osoitteisiin 192.168.3.21 ja 192.168.3.22. Nämä sisäverkon osoitteet on asetettu Vyatta Core -koneen verkkokortille eth0. Ulkoverkon osoitteista 85.134.47.40 on ohjattu DMZ-alueella olevaan WWW-palvelimeen, joka vastaa mm. http-, sähköposti- ja etäyhteys-pyyntöihin. Toinen osoite on ohjattu suoraan intraverkon osoitteeseen 192.168.1.2, joka vastaa ainoastaan etäyhteyspyyntöön portissa 3389.

3 JÄRJESTELMÄT JA TEKNIIKAT

3.1 Vyatta lyhyesti

Vyatta Core on avoimen lähdekoodin Debian-pohjainen reititys- ja palomuuri -ohjelmisto. Core on Vyatta:n ilmainen versio, joka tarjoaa kattavat perusominaisuudet jo hieman vaativampaankin käyttöön. Vyatta Core:n on saatavilla kattava dokumentointi erilaisten asetuksien käyttöönottoa varten. Sen ominaisuuksiin kuuluu IPv4- ja IPv6 -reititykset, IPsec, SSL openvpn ja tilallinen palomuuri (statefull firewall). Vyatta Core on ollut saatavana vuodesta 2006 ja sen uusin versio on Vyatta Core 6.1. Vyatta Core:a tullaan tässä opinnäytetyössä käyttämään palomuurina, DHCP-palvelimena, jakamaan intraverkko ja DMZ-alue erilleen toisistaan sekä porttiohjaukseen käyttämällä NAT-muunnosta. /1/

3.2 Vyatta Core palomuurina

Vyatta Core:ssa on oletuksena kolme palomuuria jokaista verkkokorttia kohden, portille suoraan suunnattu liikenne, portille tuleva liikenne ja portilta lähtevä liikenne. Nämä suunnat on nimetty local, in ja out, katso taulukko1. Jokainen näistä palomuureista on oletuksena auki ja päästää kaiken liikenteen läpi. Tämä voidaan estää luomalla kullekin palomuurille yksi sääntö, jolloin automaattisesti kaikki muu liikenne on estetty. Tässä opinnäytetyössä on yhteensä 9 eri palomuuria, joten täytyi miettiä, mitkä palomuurit ovat oikeasti tarpeellisia ja mitkä voidaan jättää auki. Opinnäytetyössä asetettiin kolme eri palomuuria. Ensimmäisenä asetettiin palomuuri, joka vaikuttaa julkisesta verkosta sisään tulevaan liikenteeseen. Seuraavaksi asetettiin palomuuri, jolla sallittiin vain tarpeellinen pääsy DMZ-alueelta intraverkkoon. Kolmanneksi määriteltiin julkisesta verkosta suoraan Vyatta Core -koneen porttiin tuleva liikenne, jolla sallitaan SSH-yhteyden muodostaminen. Muut palomuurit voitiin jättää auki, koska ulkoverkkoon pääsyä ei tarvitse rajoittaa ja nämä palomuurit eivät vaikuta ulkoverkosta tulevaan liikenteeseen.

Palomuurille tulevaa liikennettä verrataan asetettuihin sääntöihin numerojärjestyksessä pienimmästä suurimpaan. Vertausta jatketaan kunnes löytyy jokin sopiva

sääntö, tai lista on käyty loppuun ja jäljellä on viimeinen sääntö, joka pudottaa paketin. Tässä opinnäytetyössä säännöt numeroitiin 10-numeron välein, jolloin voidaan myöhemmin tarvittaessa lisätä sääntö listan keskelle ilman, että koko numerointi menee uusiksi. Taulukossa 1 on esitetty Vyatta Core:n palomuurin toimintaperiaate. /2/

Taulukko1. Vyatta Core:n palomuurit.

Suunta	Selitys
local	Portille suoraan suunnattu liikenne
in	Porttiin tuleva liikenne, joka ohjataan palomuurin kautta eteenpäin
out	Palomuurin kautta tullut liikenne, joka ohjataan portista ulos

3.3 NAT

NAT tarkoittaa osoitteenmuunnosta yksityisestä osoitteesta julkiseksi osoitteeksi. Sen tarkoitus on säästää julkisia osoitteita, koska niitä on käytettävissä vain rajallinen määrä. Osoitteenmuunnosta voidaan käyttää myös muunnettaessa julkisesta osoitteesta yksityiseksi, jossain yhteyksissä tätä kutsutaan käänteiseksi muunnokseksi(reverse NAT). Vyatta Core:ssa on mahdollisuus käyttää source, destination, bidirectional tai masquerade -tyyppisiä verkkomuunnoksia. Tässä opinnäytetyössä tarvitaan masquerade-tyyppistä muunnosta sisäverkon osoitealueiden muuttamiseen julkiseksi osoitteeksi. Ilman tätä muunnosta ei sisäverkon koneilla olisi pääsyä internetiin. Opinnäytetyössä käytetään myös destination-muunnosta ulkoverkosta tuleville yhteyksille, jotka halutaan ohjata DMZ-alueella sijaitsevalle WWW-palvelimen sisäverkon osoitteeseen. /3/

3.4 DHCP-palvelin

Dynamic Host Configuration Protocol (DHCP) mahdollistaa automaattisen IP-osoitteiden määrittämisen verkkoon kytkettävälle työasemalle tai laitteelle. Palvelun avulla helpotetaan asetusten määrittämistä, koska käyttäjän ei tarvitse tietää oikeita IP-, gateway- tai DNS -osoitteita, riittää kun laite kytketään verkkoon ja kaikki tarvittavat osoitetiedot tulevat automaattisesti käyttöön. DHCP-palvelimen etuja ovat IP-osoitteiden uudelleen käytettävyys ja ylläpidon tehokkuus. Tässä

opinnäytetyössä DHCP-palvelin toteutetaan Vyatta Core:n avulla, joka jakaa asetukset automaattisesti Zyxel-kytkimen portteihin kytketyille laitteille. /4/

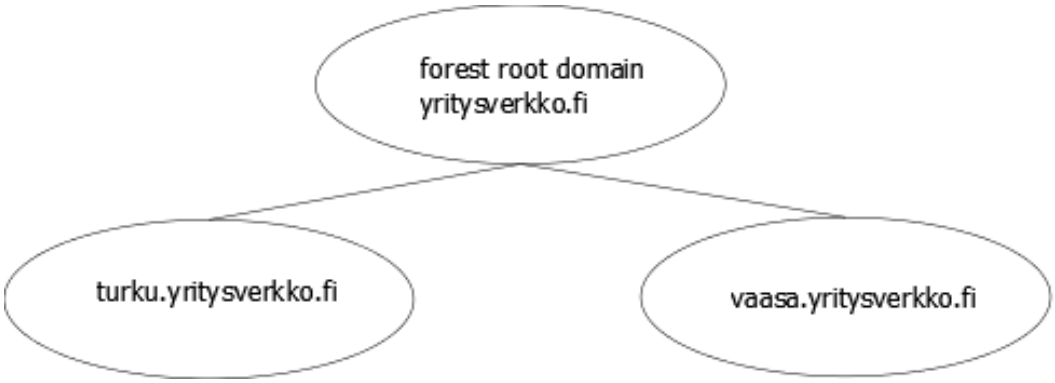
3.5 Windows Server 2008 lyhyesti

Windows Server 2008 on Windowsin uusin palvelinohjelmisto, jonka avulla voidaan helposti hallinnoida yrityksen verkkopalveluita. Windows Server 2008 tarjoaa muutamia uusia ominaisuuksia, ja on kehittänyt vanhoja palveluja Windows Server 2003:n verrattuna. Tässä opinnäytetyössä toteutetaan Windows Server 2008:n avulla sisäverkon AD, DNS, File Services ja käyttäjäryhmien hallinta. Lisäksi myös DMZ-alueen julkiset palvelut toteutetaan Windows Server 2008:n ja sen käyttämän IIS7:n avulla. Julkisia palveluja ovat Terminal Services, FTP- ja WWW -palvelin. /5/

3.6 Active Directory Domain Services

Active Directory Domain Services on käyttäjätietokanta ja hakemistopalvelu. Active Directory Domain Services tarjoaa turvallisen ja hierarkkisen ratkaisun käyttäjien ja resurssien hallintaan verkkoarkkitehtuurissa. Verkkoresursseja eli objekteja ovat tietokannat, tietokoneet, tulostimet ja muut verkossa olevat laitteet. Active Directory Domain Services on luokitteleva tietokanta, joka varastoi ja hallinnoi tietoja käyttäjistä ja laitteista.

Active Directory:n rakenne koostuu arkistohakemistosta ja metsästä. Jokaisessa metsässä voi olla yksi tai useampi domain ja jokaisella domainilla on oma hallintayksikkö(organizational units, OU), joiden tarkoitus on yksinkertaistaa käyttöoikeuksien jakaminen ja hallinta pienempiin yksiköihin. Metsä toimii yrityksen turvallisuusrajana ja määrää käyttöoikeudet ylläpitäjille. Metsä voidaan myös jakaa useimpiin domain-alueisiin, jolloin resurssien jakamista pystytään rajoittamaan paremmin. Esimerkiksi maantieteellisesti kaukana ja hitaamman yhteyden takana olevalle yksikölle voidaan luoda oma domain, joka pääsee käsiksi vain tiettyyn osaan datasta.



Kuva 2. Domain metsä.

Kuvassa 2 on esitetty metsä, jossa on kolme domainia. Tässä tapauksessa forest root domainilla on kaksi alidomainia, jotka sijaitsevat maantieteellisesti eri paikoissa. Turun ja Vaasan toimipisteet pääsevät käsiksi samoihin jaettuihin resursseihin kuin pääkonttorilla olevat käyttäjät. /6/

3.7 Domainin käyttämät palvelut ja portit

Tässä opinnäytetyössä halutaan sallia WWW-palvelimen kirjautuminen domain-alueeseen. Kirjautumista varten täytyy sallia domain-palvelun käyttämät portit eri protokollille ja palveluille. Useiden näiden protokollien merkitys tässä työssä on vähäinen, mutta niiden tarkoitus haluttiin selventää porttien avaamista varten. Suurimmaksi osaksi nämä palvelut liittyvät OSI-mallin eri kerroksiin, yhteyden muodostamiseen, koneiden keskustelemiseen lähiverkossa ja käyttäjien tunnistamiseen.

W32Time

W32Time on Windowsin käyttämä ajan synkronointipalvelu, joka hakee kellonajan ja päiväystiedot ulkoiselta palvelimelta. Windows domainiin kirjautuneiden koneiden kellonajat täytyy täsmätä, joten domainiin kirjautumista varten täytyy saada kellonaika synkronointi Domain Controller -koneelta. W32Time käyttää UDP-porttia 123.

RPC ja RPC-EPMAP

Remote Procedure Call (RPC) on sovelluskerroksen kommunikointiprotokolla, jonka avulla asiakaskone lähettää yhteyskutsun etäpalvelimelle, joka vastaa pyyntöön yhteyden muodostamiseksi. Se toimii vastaavasti kuten TCP-protokolla, mutta on tarkoitettu kevyemmille yhteystyypeille. Useat eri verkkoprotokollat käyttävät RPC:tä yhteydenmuodostukseen, esimerkiksi NFS-levyjako. EPMAP tulee sanoista end-point mapper, joka toimii palvelimella. Sen tarkoitus on kuunnella RPC-yhteyspyyntöjä UDP-portissa 135. RPC käyttää yhteyden muodostamiseen oletuksena palvelimen TCP-portteja 49152-65535. Tietoturvasyistä palomuurissa tulisi avata mahdollisimman vähän portteja. Windows-palvelimilla voidaan rajoittaa käytettävien porttien määrää komentokehotteen kautta komennolla **netsh int ipv4 set dynamicport tcp start=49152 num=255**. Tämä tarkoittaa sitä, että palvelin käyttää TCP/IP -yhteyksiin pienintä mahdollista porttimäärää (255kpl) alkaen portista 49152. Asetus täytyy määrittää molemmilla palvelimille tässä opinnäytetyössä. /7; 17/

NetBIOS

Network Basic Input/Output System eli NetBIOS on istuntokerroksen verkkoprotokolla, jonka avulla koneet voivat kommunikoida lähiverkon kautta. NetBIOS on alun perin IBM:n kehittämä protokolla, joka myöhemmin siirtyi Microsoftin omistukseen ja tuli sittemmin viralliseksi standardiksi. NetBIOS:n tärkeimmät toiminnot ovat nimen selvennyspalvelut ja istuntopalvelut yhteydellisiin ja yhteydettömiin tiedonsiirtoihin. NetBIOS:n käyttö uusimmissa verkkojärjestelmissä on vähentymässä, koska se on raskas ja kuormittaa turhaan verkkoa. Windows Server 2008:ssa NetBIOS hoitaa nimikyselyt esimerkiksi silloin, kun muodostetaan yhteyttä koneen nimellä \\AD, jolloin NetBIOS:n avulla koneen nimi yhdistetään IP-osoitteeseen. AD-verkon NetBIOS-nimeksi tullaan myöhemmin määrittelemään \\BOTNIA, jonka avulla voidaan myös muodostaa yhteys AD-palvelimelle. NetBIOS käyttää UDP-porttia 138. /8/

DNS

Domain Name Services eli DNS on palvelu, joka muuttaa verkkotunnuksia IP-osoitteiksi. DNS toimii kuljetuskerroksessa ja sen tehtävänä on tarjota käyttäjille nimenselvityspalveluita. DNS-palvelu helpottaa verkon käyttöä nimeämällä koneet helpommin muistettavilla verkkotunnuksilla, joilla on yhteinen verkon tunniste, kuten tässä työssä käytettävä botnia.openitlab.fi. Koneiden verkkotunnukset saadaan lisäämällä verkon yhteisen tunnisteen eteen koneen nimi, esimerkiksi AD -palvelimen verkkotunnus on AD.botnia.openitlab.fi. /9/

LDAP

Lightweight Directory Access Protocol (LDAP) on kevyempi versio x.500 -standardia käyttävävästä DAP:sta. LDAP on hakemistopalvelujen (kuten AD) käyttöön tarkoitettu protokolla, jonka yksi tärkeä tehtävä on käyttäjän ja käyttöoikeuksien tunnistaminen. LDAP toimii TCP/IP -kerroksen päällä. Sen avulla voidaan luoda yhteyksiä, tehdä hakuja ja muokata hakemistoissa olevia tietoja. LDAP pohjautuu Client/Server -malliin ja sen tärkein tehtävä on sallia yhteyksiä eri palveluihin. LDAP:n tieto- ja nimikannat ovat hyvin samankaltaisia kuin X.500 -hakemistopalvelussa, mutta sen tärkein eroavuus on alhaisemmat resurssivaatimukset. /10/

RDP

Remote Desktop Protocol (RDP) Microsoftin kehittämä graafinen käyttöliittymä, jonka avulla voidaan käyttää toista tietokonetta etäyhteyden kautta. Nykyään palvelimia hallitaan yhä useammissa verkoissa etäyhteyden avulla, jolloin palvelimelle päästään aina käsiksi vaikka käyttäjä sijaitsisi maantieteellisesti kaukana. Myös työasemia huolletaan vikatilanteissa etäyhteyden kautta. RDP käyttää yhteyden muodostamiseen TCP-porttia 3389.

Kerberos

Kerberos on käyttäjien tunnistuspalvelu, joka mahdollistaa käyttöoikeuksien hallinnan suojaamattomissa verkoissa. Windows Server 2008 AD käyttää kerberos 5

-versiota käyttäjien hallinnassa. Kerberos-protokollan avulla käyttäjä ja palvelin varmistavat toistensa identiteetit turvallisesti. Kerberos käyttää TCP- ja UDP -porttia 88.

SAM/LSA

Security Account manager (SAM) on tietokanta, joka säilyttää käyttäjätiedot kirjautumista varten paikallisille käyttäjille. Local Security Authority (LSA) on suojattu alijärjestelmä, joka autentikoi ja kirjaa käyttäjät paikalliseen järjestelmään. LSA ylläpitää tiedot kaikista paikallisista käyttöoikeuksista, jotka löytyy Windows Server 2008:sta nimellä Local Security Policy. /12/

3.8 Levypalvelut

Levypalveluiden avulla pystytään hallinnoimaan tehokasta ja tuvallista tiedostojen jakoa verkossa. Käyttäjien kansiot sijaitsevat työasemien sijaan verkkolevyillä, joihin pääsee käsiksi sijainnista ja työasemasta riippumatta. Levypalvelimella voidaan suorittaa tiedostojen automaattinen varmuuskopiointi tiedostojen turvaamiseksi. Samoihin kansioihin pääsee käsiksi Windows- ja Unix -käyttäjät SMB- ja NFS -protokollien avulla. SMB-protokollaa käytetään Windows-ympäristössä, mutta sitä pystytään käyttämään myös Linux-koneiden kanssa Samban avulla. NFS-protokollaa käytetään verkkojakamiseen jos verkossa on Unix-käyttäjiä, esimerkiksi Mac-koneet. Microsoft-levypalvelimella jaettavan kansion kapasiteettia voidaan rajoittaa QUOTA-palvelun avulla.

3.9 IIS7

Internet Information Services (IIS) on Microsoftin kehittämä palvelinohjelmistokokonaisuus, joka on tarkoitettu käytettäväksi Windows-pohjaisissa palvelimissa. IIS on kehitetty kaiken WEB-sisällön jakamiseen ja hallintaan. Sillä voidaan ylläpitää WWW-sivustoa, FTP-sivustoa, mediapalvelinta ja monia muita WEB-sovelluksia. IIS7:a voidaan pyörittää myös Windowsin desktop-tuotteiden kanssa. Tässä opinnäytetyössä käytetään Windows Server 2008:n mukana tulevaa IIS7 -versiota WEB- ja FTP -palvelimena. WEB-palvelimella ylläpidetään bot-

nia.openitlab.fi kotisivua, jonka kautta käyttäjät ohjataan verkon muihin palveluihin.

3.10 Terminal Services

Terminal Services (TS) on Microsoftin kehittämä etähallintasovellus Windows Server 2008:ssa. TS toimii tällä hetkellä ainoastaan Windows Explorer -selaimen kanssa. TS:n avulla voidaan jakaa palvelimen sovelluksia käytettäväksi selaimen kautta. Yhteys suojataan SSL-sertifikaatin avulla. TS:ssa voidaan jakaa muiden käytettäväksi sovellukset, jotka on asennettu palvelimelle. TS:a käytetään usein intraverkon yhteyden luomiseen, jolloin TS-yhteyden avulla voidaan käyttää esimerkiksi ainoastaan työpaikan sisäisessä verkossa olevia palveluita selaimen kautta. Tässä opinnäytetyössä TS:n tarkoitus on havainnollistaa yritysverkoissa hyvin yleistä palvelua ja sen avulla jaettiin Wireshark- ja Windows Explorer -ohjelmat. TS:n avulla voidaan myös muodostaa etäyhteys WWW-palvelimelle.

3.11 Sertifikaatti

Sertifikaatti on luotettavan kolmannen osapuolen digitaalisesti allekirjoittama todistus, jonka tarkoitus on osoittaa, että julkinen avain kuuluu tietylle avaimen käyttäjälle. Sertifikaatista selviää myös henkilön tai organisaation nimi, sertifikaatin myöntämispäivä ja sen päättymispäivä. Tässä opinnäytetyössä käytetään palvelinsertifikaattia, jonka avulla käyttäjä voi varmistua palvelimen todenperäisyydestä. Sertifikaatilla allekirjoitetaan yhteys käytettäessä Terminal Services -palvelua. /18/

3.12 Axigen Mail Server

Tässä työssä valittiin käytettäväksi sähköpostipalvelimena Axigen Mail Server, koska siihen saa ilmaisen kokeilulisenssin ja se tukee IMAP- ja SMTP -protokollia. Kokeilulisenssi on voimassa yhden vuoden seuraavilla rajoituksilla: käytettävissä yksi domain, 100 käyttäjää ja Antivirus- tai Antispam -palvelut eivät kuulu ilmaiseen versioon. Axigen Mail Server on helppokäyttöinen Windows -ohjelmisto, jossa on oma webmail. Axigen Mail Server asennetaan WWW-palvelimelle.

3.12.1 IMAP

Internet Message Access Protocol (IMAP) on sähköpostien lukemiseen tarkoitettu protokolla. IMAP säilyttää viestit palvelimella ja mahdollistaa käyttäjien pääsyn lukemaan viestejä useilta eri koneilta. IMAP tukee palvelimella olevia hakemistoja ja mahdollistaa viestien järjestelemisen eri kansioihin. IMAP luotiin vaihtoehtoiseksi protokollaksi korvaamaan vieläkin käytössä olevaa POP-protokollaa. Tällä hetkellä käytössä on RFC 3501 -dokumentin määrittelemä 4rev1-versio. IMAP toimii TCP/IP -yhteyden yli käyttäen porttia 143.

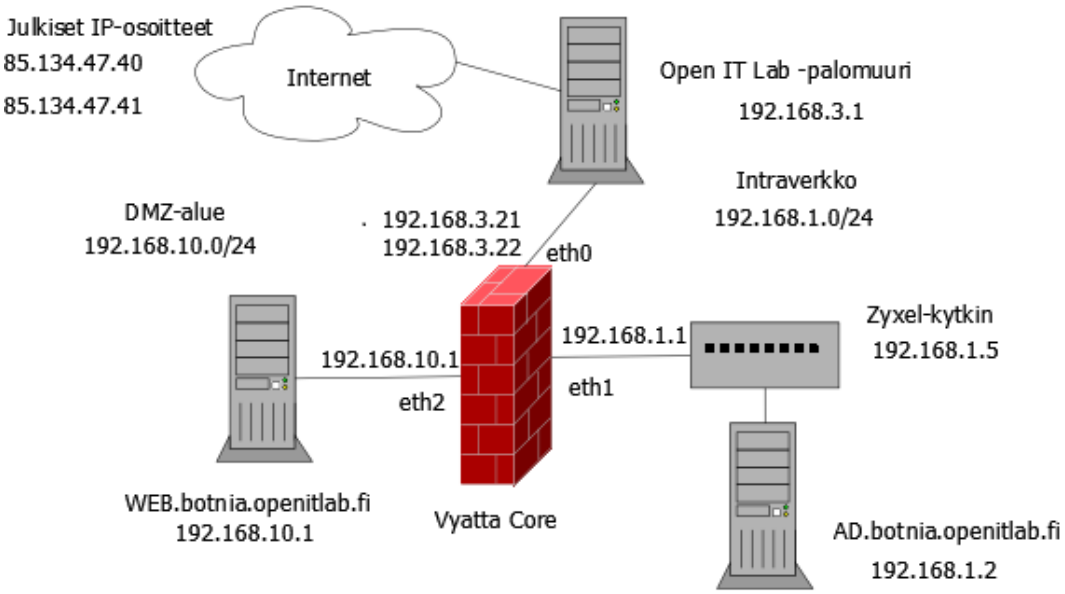
3.12.2 SMTP

Simple Mail Transfer Protocol (SMTP) on TCP-pohjainen protokolla, jota käytetään viestien välittämiseen sähköpostipalvelimien kesken. SMTP ei voi noutaa viestejä palvelimelta, joten se käyttää muita protokollia sitä varten, kuten IMAP ja POP. SMTP-protokolla käyttää viestin kuljettamiseen porttia 25.

4 TYÖN SUORITUS

4.1 Verkkotopologia

Työn lopullinen verkkotopologia on esitetty kuvassa 3. Ulkoiselle IP-osoitteelle 85.134.47.40 saatiin DNS-nimipalvelu, jolloin verkkoon voidaan muodostaa ulkoverkosta yhteys osoitteella http://botnia.openitlab.fi.



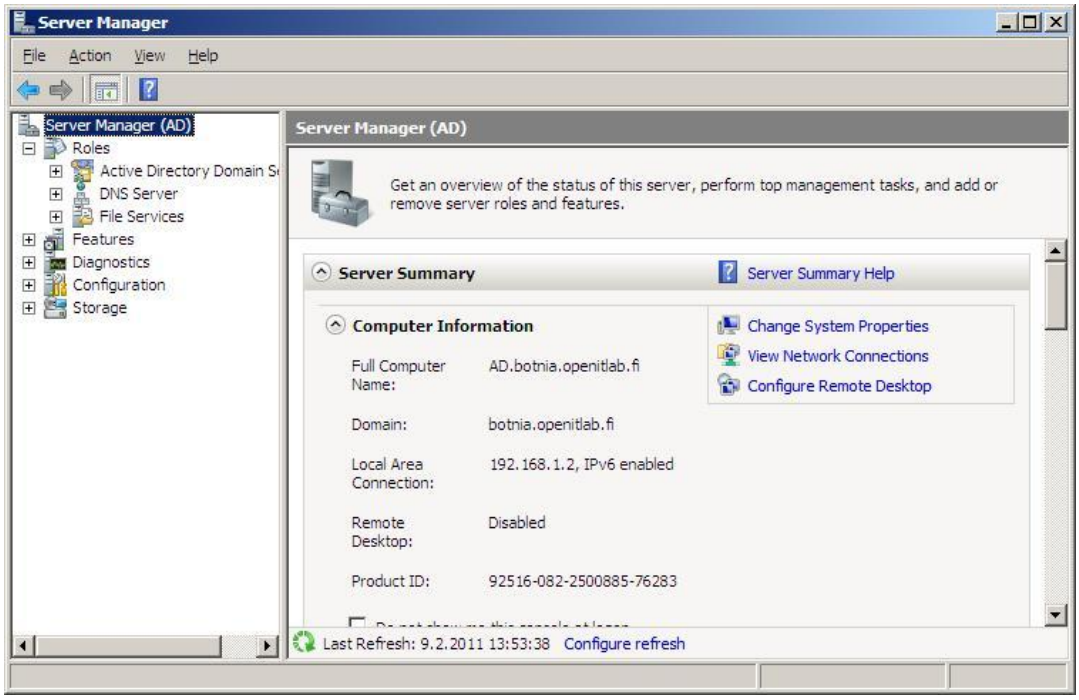
Kuva 3. Toteutunut verkkotopologia.

4.2 Windows Server 2008:n asennus

Windows Server 2008 asennetaan kuten muutkin Windowsin työasemat. Asennus käynnistetään DVD:ltä. Asennuksen aikana valitaan aikavyöhyke, mille osiolle asennus halutaan tehdä ja luodaan käyttäjänimi ja salasana. Tässä asennuksessa serverikonetta ei tarvita muuhun käyttöön, joten oletuksena valitaan käytettäväksi koko kiintolevy. Windows Server 2008:n asennuksessa voidaan valita eri asennusversioita, tässä opinnäytetyössä valittiin käytettäväksi Enterprise-versio ja full installation.

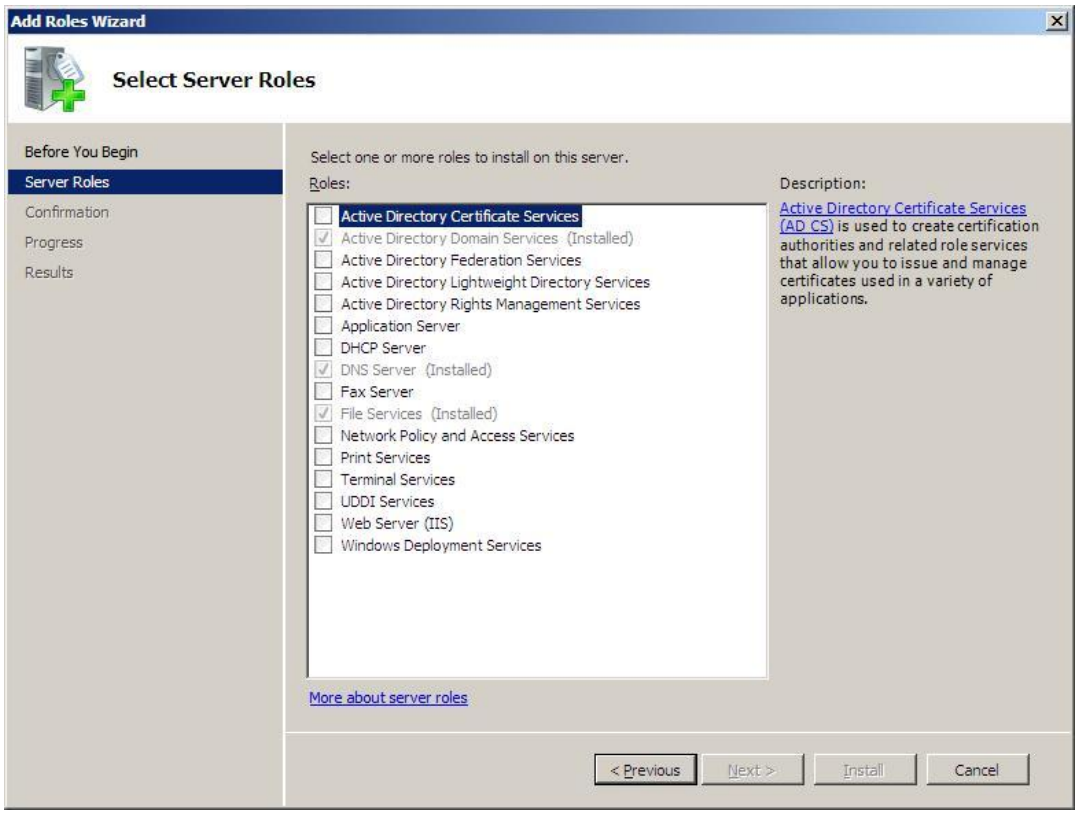
4.2.1 Server Manager

Server Manager on Windows Server 2008:n tehokas hallintakonsoli palvelimen roolien ja toimintojen hallinnointiin. Rooli kertoo palvelimen käyttötarkoituksesta. Palvelimella voi olla yksi tai useampi rooli ja jokaisella roolilla voi olla yksi tai useampi roolipalvelu (role services). Rooleja ja ominaisuuksia voi helposti lisätä tai poistaa Server Managerin snap in -valikosta. Kuvissa 4 ja 5 on esitetty roolien asentaminen Server Managerin avulla. /13/



Kuva 4. Server Manager.

Kuvassa 4 on esitetty Server Managerin oletusnäkymä. Vasemmalla snap in -valikossa näkyy asennetut roolit ja niiden ominaisuudet. Roolien alavalikoista päästään tarkastelemaan ja muokkaamaan palvelimen asetuksia.



Kuva 5. Roolien lisääminen.

Roolien asennus tapahtuu kuvan 5 osoittamalla tavalla. Valikosta valitaan halutut palvelut ja määritellään niille mahdolliset lisäasetukset.

4.2.2 Windows-palvelimien IP-asetukset

Palvelimet on hyvä asentaa kiinteiden IP-osoitteiden taakse. Molemmille Windows-palvelimille määritettiin omat IP- ja DNS -osoitteet sekä gateway-osoite, jonka kautta palvelimet muodostavat internetyhteyden. Palvelimille määritetyt osoitteet on esitetty taulukossa 2.

Taulukko2. Windows-palvelimien IP-asetukset.

Palvelin	AD	WWW
IP	192.168.1.2	192.168.10.2
Mask	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.10.1
DNS	192.168.1.2	192.168.1.2

4.3 AD-palvelimen asetukset

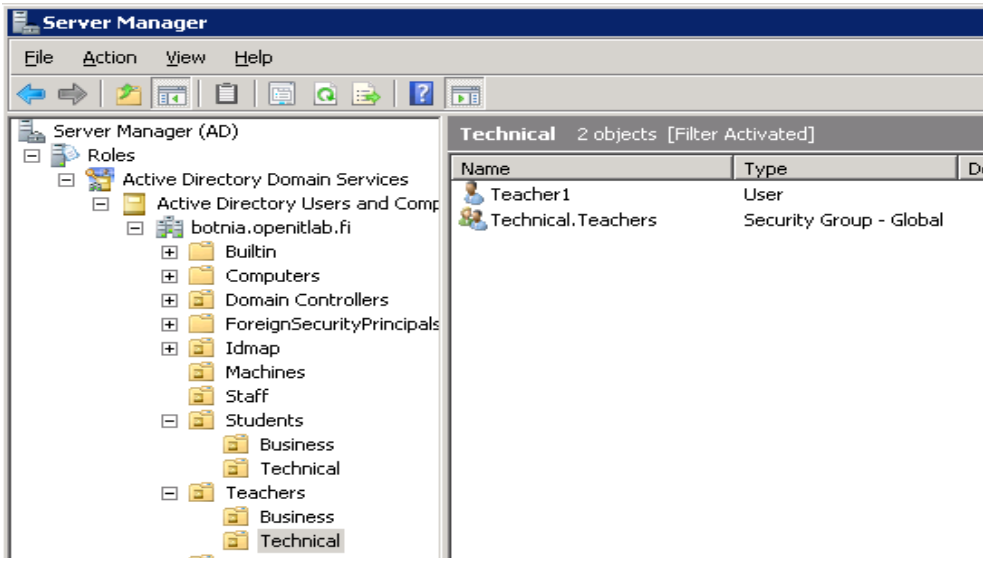
AD-palvelimen nimeksi määritettiin AD, jolloin koneen koko DNS suffix on AD.botnia.openitlab.fi ja IP-osoite 192.168.1.2. Muut koneet käyttävät AD-palvelimen IP-osoitetta DNS-osoitteena domainiin kirjautumista varten.

4.3.1 Active Directory Domain Services

Active directory Domain Services (AD DS) otetaan käyttöön joko lisäämällä rooli AD DS tai suorittamalla domainin asennusohjelma dcpromo.exe. Asennuksen alussa valitaan advanced tila, jotta saadaan paremmin puututtua asennuksen ominaisuuksiin. Asennus kysyy nimeä, joka on tässä työssä botnia.openitlab.fi. Tämän jälkeen asennus kysyy NetBIOS-nimeä, joka on BOTNIA.

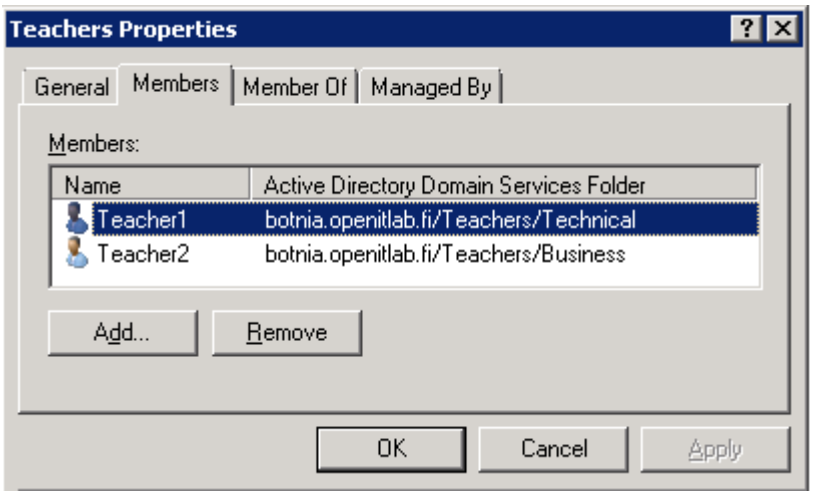
4.3.2 Käyttäjien ja ryhmien luominen

AD-verkon resurssien hallintaa varten voidaan luoda käyttäjiä ja käyttäjäryhmiä. Jokaiselle käyttäjälle voidaan erikseen määrittää käyttöoikeudet ja jaetut resurssit. Suurempia kokonaisuuksia hallittaessa on helpompi luoda ryhmiä, joille määritellään halutut ominaisuudet ja lisätään käyttäjät näiden ryhmien alle. Ryhmien ja käyttäjien lisääminen tapahtuu Server Manager -konsolista: valitaan rooli Active Directory Domain Services, avataan välilehti users ja valitaan new user. Tässä opinnäytetyössä luotiin kolme pääryhmää, joiden alle jaettiin käyttäjät kahteen eri yksikköön. Kuvassa 6 on esitetty käyttäjien ja ryhmien hierarkkinen jako. Ryhmät on jaettu kolmeen pääryhmään: Staff, Teachers ja Students. Ryhmien alle on jaettu käyttäjät yksiköittäin kahteen eri yksikköön business ja technical. Jokainen näistä eri ryhmistä on hallintayksikkö, jolle voi jakaa resurssien hallintaa tarvittaessa. Tässä opinnäytetyössä kuitenkin hallintayksiköiden käyttöä ei koettu tarpeelliseksi.



Kuva 6. Käyttäjät ja ryhmät.

Käyttäjät voidaan lisätä ryhmään kahdella eri tavalla. Ryhmän asetuksista voidaan lisätä ryhmälle käyttäjiä tai käyttäjän asetuksista voidaan lisätä käyttäjälle ryhmä tai useita ryhmiä. Myös ryhmiä voidaan lisätä toisen ryhmän alaisuuteen, näin saadaan helposti määriteltyä käyttöoikeuksia ryhmälle, katso kuva 7.

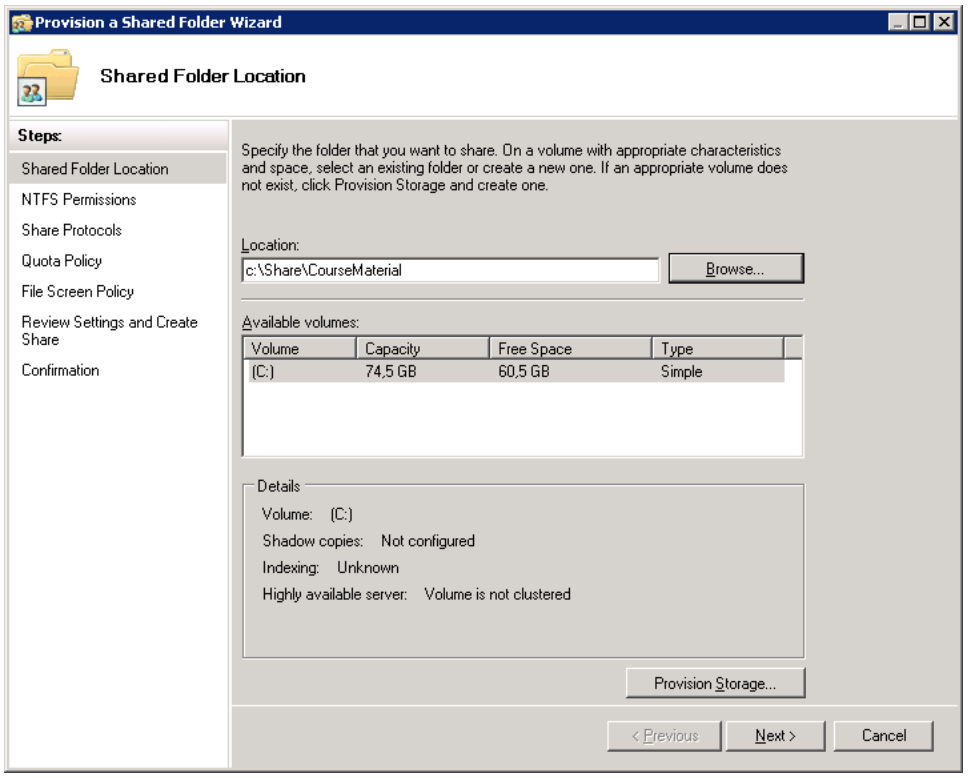


Kuva 7. Teachers-ryhmän jäsenet.

Kuvassa 7 nähdään Teachers-ryhmän jäsenet. Valitsemalla add voidaan lisätä ryhmälle lisää käyttäjiä. Kuvassa näkyy myös välilehti member of, jonka avulla ryhmä voidaan lisätä toisen ryhmän alaisuuteen.

4.3.3 Levyjaon käyttöönotto

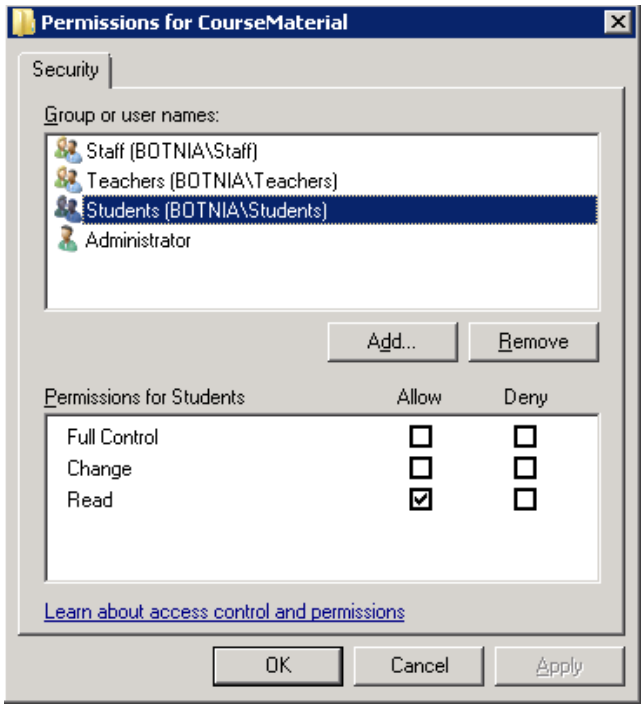
File Services asennetaan Windows Server Managerista lisäämällä rooli File Services. Jaettu kansio lisätään valitsemalla välilehti file services - share and storage management ja valitaan provision share. Jaettavaa kansiota luodessa valitaan sijainti, käytettävä protokolla ja käyttäjä- sekä ryhmäkohtaiset käyttöoikeudet kansiolle. Tässä opinnäytetyössä luotiin opettajille kansio kurssimateriaalien jakamista varten. Opettajat pääsevät muokkaamaan kansion sisältöä, johon opiskelijat saavat ainoastaan lukuoikeudet. Levyjaon luominen on esitetty kuvassa 8. /14/



Kuva 8. Levyjaon luominen.

Kuvassa 9 on esitetty levypalvelimen jakaman kansion käyttöoikeudet, eri mahdollisuuksia ovat: täysi hallinta, muutosoikeus ja vain lukuoikeus. Tämän lisäksi

luotiin myös muille ryhmille omat jaetut kansiot. Staff-ryhmän jäsenet ovat pääkäyttäjiä, jotka pääsevät muokkaamaan kaikkien jaettujen kansioiden sisältöjä.



Kuva 9. Levyjaon käyttöoikeudet.

4.3.4 TS Licensing

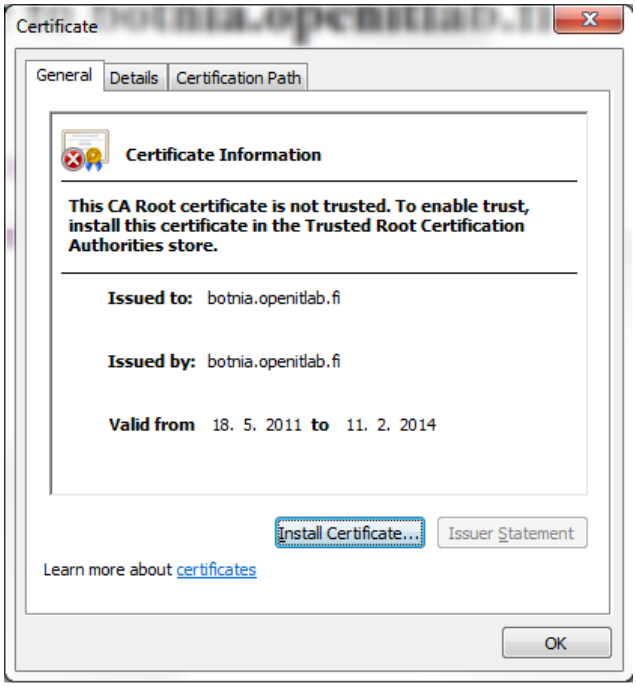
Terminal Services -palvelua käytettäessä tullaan sallimaan palveluun kirjautuminen botnia.openitlab.fi -domainin käyttäjille, mikä hyväksytään TS Licensing -roolin avulla. Terminal Services Licensing asennetaan lisäämällä rooli Terminal Services ja valitaan palveluista TS Licensing. Tämä palvelu asennetaan Domain Controller -koneelle. TS Licensing ei vaadi käyttöönoton jälkeen asetusten määrittelyä, vaan se hyväksyy automaattisesti verkossa olevat käyttö-oikeuspyynnöt TS-palvelimelta.

4.4 WWW-palvelimen asetukset

Koneen nimeksi määritettiin WEB, jolloin koneen koko DNS suffix on WEB.botnia.openitlab.fi ja IP-osoite 192.168.10.1.

4.4.1 Sertifikaatin luominen

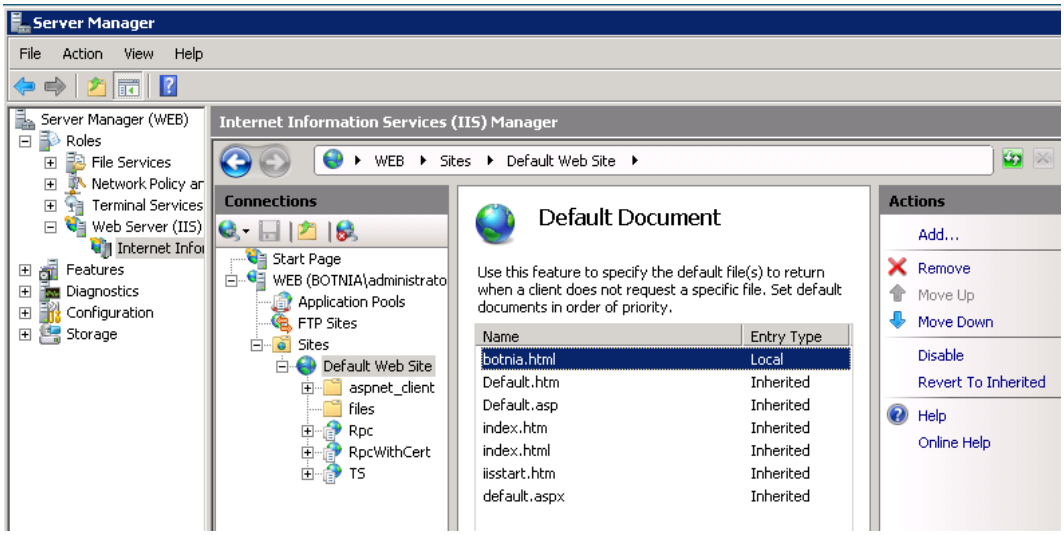
Sertifikaatin luomista kokeiltiin kahdella eri tavalla. Terminal Services -roolia lisättäessä voidaan luoda itse allekirjoitettu Sertifikaatti. IIS 7 käyttää Sertifikaatin luomisessa automaattisesti palvelimen nimeä Sertifikaatin tekijänä, joka ei aina välttämättä ole sama palvelimen DNS-osoitteen kanssa. Jos tekijän nimi ja DNS-osoite eroavat toisistaan, saadaan sertifikaattia käytettäessä virheilmoitus. Tämä ongelma voidaan korjata luomalla sertifikaatti käyttäen SELFSSL-ohjelmaa, joka tulee palvelimelle erikseen asennettavan IIS Resource Kit Tools -ohjelman mukana. Sertifikaatti luotiin opinnäytetyössä käytettävän domain-nimen botnia.openitlab.fi -mukaisesti. Koska luotettavan kolmannen osapuolen digitaalinen allekirjoitus sertifikaatille on kallis, päädyttiin sertifikaatti allekirjoittamaan itse. Käytettäessä täytyy sertifikaatti ensin ladata palvelimelta ja asentaa se itse Trusted Root Certification Authorities -kansioon. Asennuksen jälkeen sertifikaattia voidaan käyttää ilman virhesanomia. Sertifikaati on esitetty kuvassa 10.



Kuva 10. Sertifikaatti.

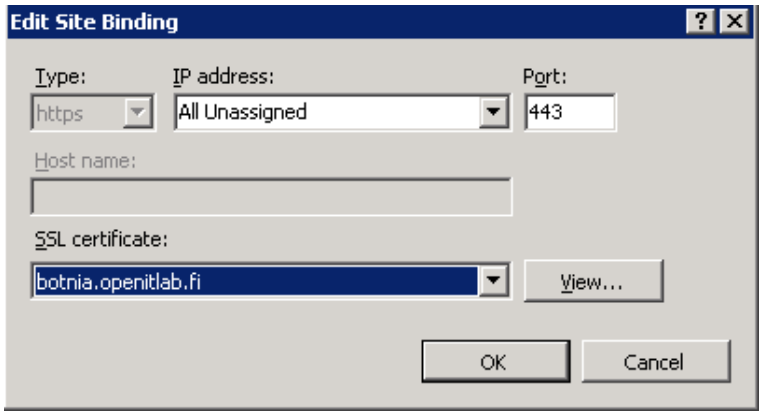
4.4.2 IIS7-asetukset

IIS7 otetaan käyttöön lisäämällä rooli Internet Information Services. Roolin lisäyksen jälkeen voidaan tarkastella sivunäkymää ottamalla selaimella yhteys http://localhost. IIS7:ssa on oletuksena oma aloitussivu, joka voidaan vaihtaa valitsemalla Server Manager:sta default document. Opinnäytetyötä varten luotiin oma kotisivu tiedostoon botnia.html, joka löytyy WWW-palvelimella kansiosta c:/inetpub/wwwroot. Seuraavaksi valitaan kuvan 11 mukaisesti käytettävä default document botnia.html:ksi.

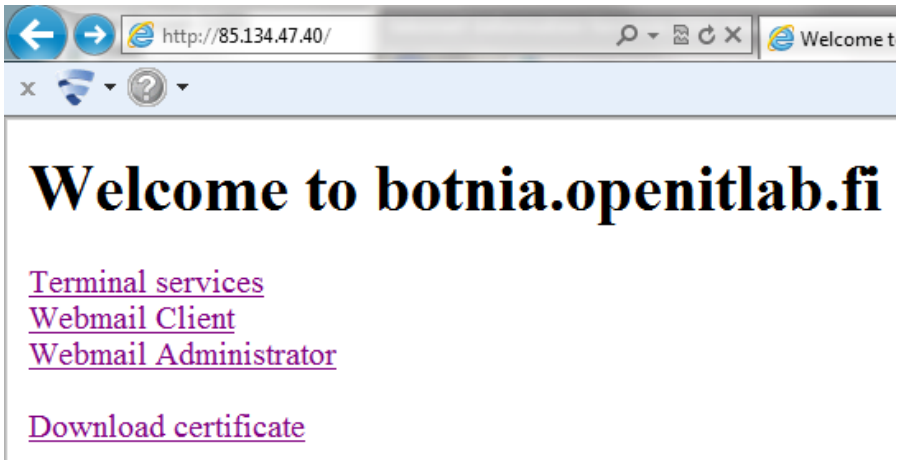


Kuva 11. IIS7 sivun hallinta.

Tämän jälkeen valitaan default web site, ja hiiren oikealla edit bindings. Tämä avaa kuvan 12 mukaisen näkymän, josta voidaan määrittää sivustolle IP-osoitteet ja käytettävät portit. IP-osoitetta ei tarvitse erikseen määrittää, joten valitaan kuvan 12 mukaisesti portti 443 ja valitaan yhteydelle käytettäväksi oma sertifikaatti. Nyt sivustoa voidaan käyttää joko suojaamattomalla yhteydellä portin 80 kautta, tai SSL-suojatulla yhteydellä portin 443 kautta. Kotisivuksi tehtiin oma sivunäkymä, johon lisättiin linkit työssä tehtyihin etäpalveluihin. WEB-sivustolla jaetaan myös sertifikaatti, jotta käyttäjät voivat ladata ja asentaa sertifikaatin. Jakaminen tehtiin lisäämällä tiedosto BotniaCert.crt suoraan WWW-palvelimen wwwroot-hakemiston alle, tällöin sertifikaatti voidaan ladata osoitteesta http://botnia.openitlab.fi/BotniaCer.crt. Kotisivu on esitetty kuvassa 13.



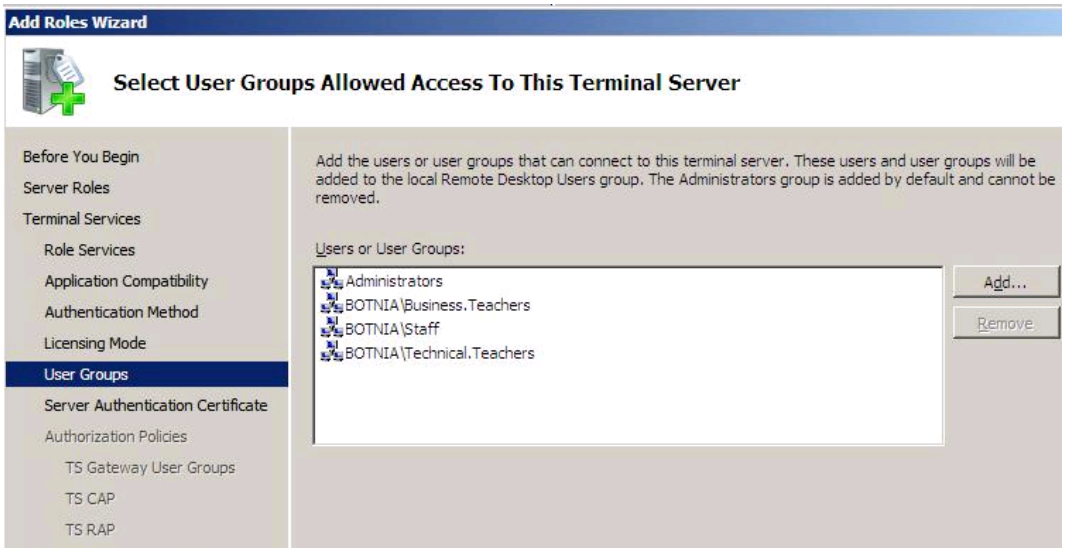
Kuva 12. Sertifikaatin ja portin valinta IIS7:ssa.



Kuva 13. Kotisivu.

4.4.3 Terminal Services asetusten määrittäminen

TS-rooli asennetaan kuten mikä tahansa muukin rooli Windows Server 2008:ssa, asennukseen valitaan seuraavat palvelut: Terminal Server, TS Gateway ja TS Web Acces. Roolia asennettaessa asennus käy läpi tarvittavat asetukset, kuten mitkä käyttäjät voivat kirjautua palveluun ja mitä sertifikaattia yhteyden varmentamiseen käytetään. Kuvassa 14 on esitetty TS-roolin lisääminen, kuvasta näkee, mitkä käyttäjäryhmät voivat kirjautua palveluun. Kuvasta 14 näkee myös vasemmalla olevasta valikosta asennuksen läpi käymät vaiheet. Tässä opinnäytetyössä tarvittiin määrittää vain sallitut käyttäjäryhmät ja valittiin käytettäväksi oma sertifikaatti BotniaCer.crt. AD-verkon käyttäjäryhmiä käytettäessä palvelu vaatii Domain Controller -koneelta varmistuksen ryhmien käyttöön. Tätä varten AD-koneelle asennettiin rooli TS Licensing.



Kuva 14. Terminal Service asetukset.

Asennuksen jälkeen palvelua voidaan käyttää osoitteesta https://botnia.openitlab.fi/ts. Sivulla näkyy vain oletusnäkymä ennen asetusten lopullista muokkaamista, joka tehdään Server Managerin avulla.

4.4.4 Sähköpostipalvelimen asennus

Axigen Mail Server asennetaan oman asennustiedoston avulla WWW-palvelimelle. Asennuksen jälkeen ohjelmisto kysyy automaattisesti yleiset käyttö-asetukset, jossa määritetään käytettäväksi domain-nimeksi botnia.openitlab.fi. Palvelimen hallintaan päästään ottamalla selaimella yhteys osoitteeseen http://botnia.openitlab.fi:8000. Palvelimelle määritettiin taulukossa 3 esitetyt asetukset.

Taulukko3. Sähköpostipalvelimen asetukset.

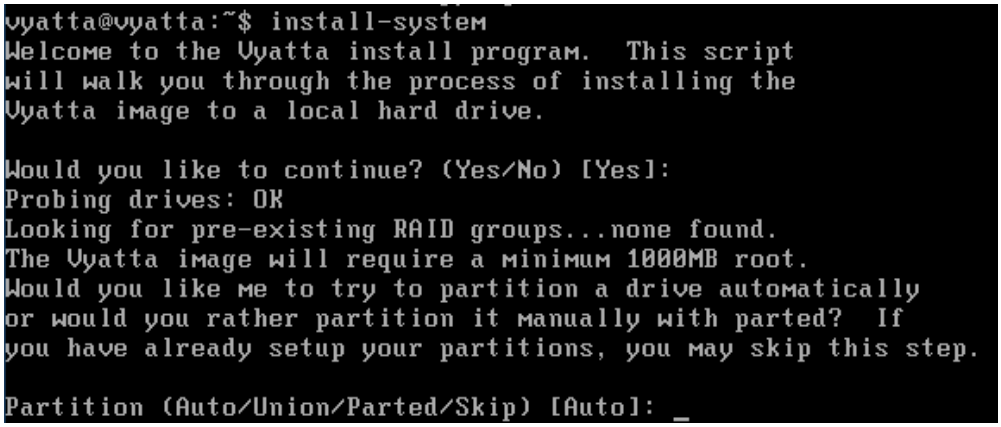
Palvelu	Asetus
Domain-nimi	85.134.47.40
IMAP-listener	0.0.0.0:143
SMTP-listener	0.0.0.0:25
Domain Name Resolver	192.168.3.1 62.80.132.128
Webadmin-portti	8000
Webmail-portti	7080

Domain Name Resolver selvittää lähtevien sähköpostiviestien DNS-nimen perusteella oikean IP-osoitteen, jonka avulla viesti saadaan toimitettua perille. Osoite 192.168.3.1 on Open IT Lab:n palomuurin paikallinen osoite, jonka kautta Vyatta Core -kone muodostaa internetyhteyden. Open IT Lab saa Julkiset IP-osoitteet ja DNS-nimipalvelut Multitronic-yritykseltä, jonka DNS-osoite on 62.80.132.128. Palvelimelle luotiin domain-käyttäjätilejä vastaavat sähköpostitunnukset, esimerkiksi Teacher1-käyttäjän sähköpostiosoite on Teacher1@botnia.openitlab.fi.

4.5 Vyatta Core:n asennus

Vyatta Core:n asentaminen tapahtuu vastaavasti kuten minkä tahansa muunkin Linux-jakelun asentaminen. Ensin ladataan asennuksen Image-tiedosto, joka poltetaan levylle. Tämän jälkeen käynnistetään tietokone CD-levy asemassa ja käynnistetään Live-CD. /15/

Vyatta Core asennetaan tekstipohjaisella käyttöliittymällä. Ensin täytyy syöttää käyttäjänimi ja salasana, molemmat ovat oletuksena vyatta. Seuraavaksi voidaan aloittaa asennus kahdella eri tapaa, joko kopioimalla CD:n image kovalevylle, tai asentamalla tiedostot kovalevylle. Tässä opinnäytetyössä valittiin tiedostojen asentaminen kovalevylle, joka tapahtui komennolla install-system. Tämän jälkeen asennus kysyy tarvittavia perustietoja. Vyatta Core:ssa tämä vaihe on tehty helpoksi syöttämällä oletusvaihtoehto automaattisesti valintakenttään, jolloin enteriä painamalla päästään eteenpäin seuraaviin vaiheisiin.



Kuva 15. Vyatta Core:n asentaminen.

Kuvassa 15 on esitetty Vyatta Core:n asentamimen. Asennus tutkii ensin kovalevyt ja kysyy sitten mille osiolle käyttäjä haluaa järjestelmän asentaa. Asennuksen annettiin tehdä osiointi automaattisesti valitsemalla hakasulkeissa esitetty suositeltu vaihtoehto painamalla enter. Tämän jälkeen asennus varmistaa vielä kuinka suuren osion käyttäjä haluaa luoda, tässä tapauksessa käyttöön otettiin koko 80 Gt:n kovalevy. Seuraavaksi asennus kopioi tarvittavat tiedostot ja kysyy sitten minkä asetustiedoston käyttäjä haluaa valita. Asennus ehdottaa oletuksena omaa tiedostoa, joka valittiin käytettäväksi. Tämän jälkeen syötetään pääkäyttäjän salasana ja valitaan oletuksena oleva kovalevy, jolle asennetaan bootloader. Nyt asennus on valmis ja järjestelmä täytyy uudelleenkäynnistää komennolla reboot.

4.5.1 Vyatta Core:n asetukset

Vyatta Core:sa määritettiin IP-osoitealueet kaikille kolmelle verkkokortille, osoitteet on esitetty kuvassa 16. Verkkokortille eth0 on määritetty kaksi eri IP-osoitetta, koska niiden kautta voidaan ohjata julkiset IP-osoitteet erikseen DMZ- ja intraverkon laitteille. Kuvauksesta selviää mille alueelle verkkokortti on kytketty. Local-zone tarkoittaa tässä työssä Vyatta Core:n omaa IP-osoitealuetta, jonka kautta ohjataan ulkoverkon yhteydet sisäverkkoon tai muodostetaan suoraan SSH-yhteys etähallintaa varten. Lisäksi Vyatta Core:n täytyy määrittää DNS- ja gateway -osoitteet internetyhteyttä varten. Vyatta Core sijaitsee Open It Lab:n palomuurin takana, joten se muodostaa kaikki yhteytensä ulkoverkkoon sen kautta. DNS- ja gateway -osoitteeksi määritettiin sisäverkon osoite 192.168.3.1.

```
vyatta@vyatta# run show interfaces
Interface    IP Address         State       Link   Description
eth0         192.168.3.21/24    up          up     local-zone
eth0         192.168.3.22/24    up          up     local-zone
eth1         192.168.1.1/24     up          up     Private-zone
eth2         192.168.10.1/24    up          up     DMZ-zone
lo           127.0.0.1/8        up          up
lo           ::1/128            up          up
```

Kuva 16. Vyatta Core:n IP-asetukset.

4.5.2 Palomuurin asetukset

Ulkoverkosta tulevaa liikennettä rajoitetaan sallimalla yhteydet, jotka on jo muodostettu tai liittyvät jo muodostettuun yhteyteen. Vyatta Core:ssa tämä määritellään asetuksilla stateful ja related, jotka vastaavat Linux-puolella yleisesti käytössä olevaa IP-tables palomuuriasetusta. Käytännössä tämä asetus sallii esimerkiksi internetsivuston vastaamisen omasta verkosta lähetettyyn pyyntöön. Tämän lisäksi ulkoverkosta täytyy päästä WWW-palvelimelle tiettyjä porttien kautta, jonka jälkeen NAT-muunnos hoitaa porttiohjauksen DMZ-alueella sijaitsevalle WWW-palvelimelle.

```
IPv4 Firewall "WAN_IN":

 Active on (eth0,IN)

(State Codes: E - Established, I - Invalid, N - New, R - Related)

rule  action  source           destination        proto     state
----  ------  ------           -----------        -----     -----
10    ACCEPT  0.0.0.0/0        0.0.0.0/0          all       E,R
20    ACCEPT  0.0.0.0/0        0.0.0.0/0          tcp       any
                               dst ports: 80,443,7080,143,25,8000,21,3389
10000 DROP    0.0.0.0/0        0.0.0.0/0          all       any
```

Kuva 17. Ulkoverkosta tulevan liikenteen palomuuri.

Kuvassa 17 on esitetty palomuuri WAN_IN, joka on aktiivisena verkkokortissa eth0 sisään tulevalle liikenteelle (in filter). Sääntö 10 sallii jo muodostetun tai siihen liittyvän yhteyden muodostamisen. Sääntö 20 sallii kuvassa esitetyille porteille tulevan liikenteen NAT-muunnosta varten. Porttien käyttötarkoitukset on esitetty taulukossa 4.

Taulukko4. WWW-palvelimelle ohjatut portit.

Portti	Protokolla	Palvelu
80	TCP	HTTP
443	TCP	HTTPS
21	TCP	FTP
25	TCP	SMTP-sähköposti
143	TCP	IMAP-sähköposti
3389	TCP	Remote Desktop
7080	TCP	Axigen webmail
8000	TCP	Axigen webmail admin

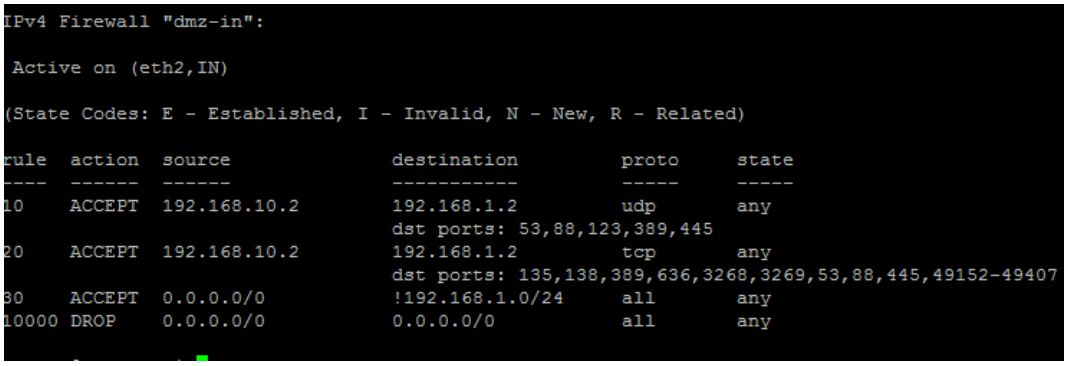
Taulukossa 4 on esitelty ulkoverkosta tulevalle liikenteelle sallitut portit, jotka ohjataan WWW-palvelimelle.

Tässä opinnäytetyössä haluttiin sallia WWW-palvelimelle pääsy DMZ-alueelta intraverkkoon AD-palvelimelle. Normaalisti tällaista pääsyä ei ole sallittu, mutta WWW-palvelimen täytyy päästä kirjautumaan domain-alueeseen käyttäjätietoja varten. Pääsyä varten luodaan palomuuri DMZ-alueelta lähtevälle liikenteelle (in filter), jolla sallitaan yhteys tietyille porteille (taulukko5). Käytännössä näiden porttien avaaminen luo pienen tietoturvariskin, mutta se ei ole tämän opinnäytetyön kannalta merkittävä, koska portit käyttävät vain tiettyjä protokollia.

Taulukko5. Domain-palvelimen käyttämät portit ja protokollat. /16/

Portti	Protokolla	Palvelu
123	UDP	W32Time
135	TCP	RCP-EPMAP
138	UDP	NetBIOS
49152 - 49407	TCP	RPC
389	TCP/UDP	LDAP
636	TCP	LDAP SSL
3268	TCP	LDAP GC
3269	TCP	LDAP GC SSL
53	TCP/UDP	DNS
88	TCP/UDP	Kerberos
445	TCP/UDP	SAM/LSA

Kuvasta 18 nähdään kuinka DMZ-alueelta lähtevään liikenteeseen vaikuttava palomuuri dmz-in on asetettu. Palomuuri on aktiivisena portissa eth2 ja se on liitetty sisään tulevaan liikenteeseen (in filter). Säännöt 10 ja 20 sallivat tarvittavat TCP- ja UDP -portit intraverkkoon pääsyä varten. Kun nämä säännöt ovat voimassa, kaikki muu liikenne on automaattisesti estettynä. WWW-palvelimelle täytyi mahdollistaa pääsy internetiin, joka toteutettiin säännöllä 30. Säännössä käytettiin negaatio-asetusta, eli kaikki muu liikenne DMZ-verkosta on sallittu, kunhan se ei ole osoitettu intraverkon osoitteisiin 192.168.1.0/24.



Kuva 18. DMZ-alueelta lähtevän liikenteen palomuuri.

SSH-yhteydellä päästään muokkaamaan Vyatta Core:n asetuksia ulkoverkosta. SSH käyttää porttia 22, jolle tuleva liikenne ulkoverkosta sallitaan, kaikki muu liikenne on estetty. Nämä asetukset on toteutettu palomuurilla vyatta-local, joka on aktiivisena verkkokortissa eth0, local filter.

4.5.3 NAT -asetukset

Sisäverkon koneiden ja laitteiden pääsy internetiin mahdollistetaan masquerade-tyyppisellä verkkomuunnoksella. Kuvassa 19 on esitetty verkkomuunnos intraverkon osoitealueelle 192.168.1.0/24.

```
vyatta@vyatta# show service nat
 rule 10 {
     description internet-acces-for-private-zone
     outbound-interface eth0
     source {
         address 192.168.1.0/24
     }
     type masquerade
```

Kuva 19. NAT-muunnos intraverkon osoitteille.

Tämä sääntö muuntaa kaikki intraverkon osoitealueella olevien koneiden osoitteet ulkoverkon osoitteeksi. Outbound-interface eth0 on ulkoverkkoon kytketty verkkokortti, jonka IP-osoitetta ei tarvitse erikseen määrittää, vaan sääntö muuntaa sisäverkon osoitteen ulos lähteväksi verkkokortin eth0 osoitteilla. Vastaava sääntö tehtiin myös DMZ-alueen osoitealueelle 192.168.10.0/24. Ulkoverkosta yhteyttä muodostettaessa täytyy yhteys ohjata ulkoverkon osoitteesta sisäverkon osoitteeksi. Tätä varten tehtiin kaksi eri sääntöä, joilla ohjataan taulukossa 3 esitettyihin portteihin muodostettu yhteys sisäverkkoon WWW-palvelimelle. Lisäksi intraverkossa olevalle AD-palvelimelle ohjataan etäyhteyden muodostus porttiin 3389 oman julkisen IP-osoitteen kautta. NAT-muunnos tehtiin kuvan 20 mukaisesti, jossa ohjataan osoitteeseen 192.168.3.21 tuleva liikenne osoitteeseen 192.168.10.2. Alun perin nämä yhteydet on muodostettu julkiseen IP-osoitteeseen 85.134.47.40, josta Open It Lab:n palomuuri ohjaa yhteyden eteenpäin. Etäyhteyden ohjaaminen AD-palvelimelle tapahtuu vastaavasti kuten kuvassa 20, mutta destination address on 192.168.3.22 ja inside address on 192.168.1.2. Nämä NAT-muunnokset tehtiin käyttämällä destination-tyyppistä muunnosta, jossa määritellään mistä verkkokortista yhteys tulee sisäänpäin (eth0), mihin osoitteeseen yhteys on muodostettu alun perin ja mihin osoitteeseen ja portteihin yhteys ohjataan.

```
vyatta@vyatta# show service nat rule 30
 description redirect-http-traffic-to-dmz
 destination {
     address 192.168.3.21
     port 80,443,7080,143,25,8000,21,3389
 }
 inbound-interface eth0
 inside-address {
     address 192.168.10.2
 }
 protocol tcp
 type destination
```

Kuva 20. WWW-palvelimelle ohjatut portit.

4.5.4 DHCP-asetukset

Kuvassa 21 on esitetty Vyatta Core:lle asennettu DHCP-palvelin, joka jakaa intraverkkoon liitetyille laitteille IP-osoitteet. Vyatta Core:ssa DHCP-palvelin liitetään haluttuun verkkokorttiin subnet-komennon avulla. Tässä tapauksessa subnet 192.168.1.0/24 on intraverkon osoitealue, joka on määritetty verkkokortille eth1. Default-router on eth1-portin osoite, jonka kautta intraverkon koneet muodostavat internet yhteyden. DNS-server on AD-koneen IP-osoite, joka täytyy määrittää domainiin kirjautumista varten. Kuvassa 21 on myös esitetty verkkokortin eth2 asetukset.

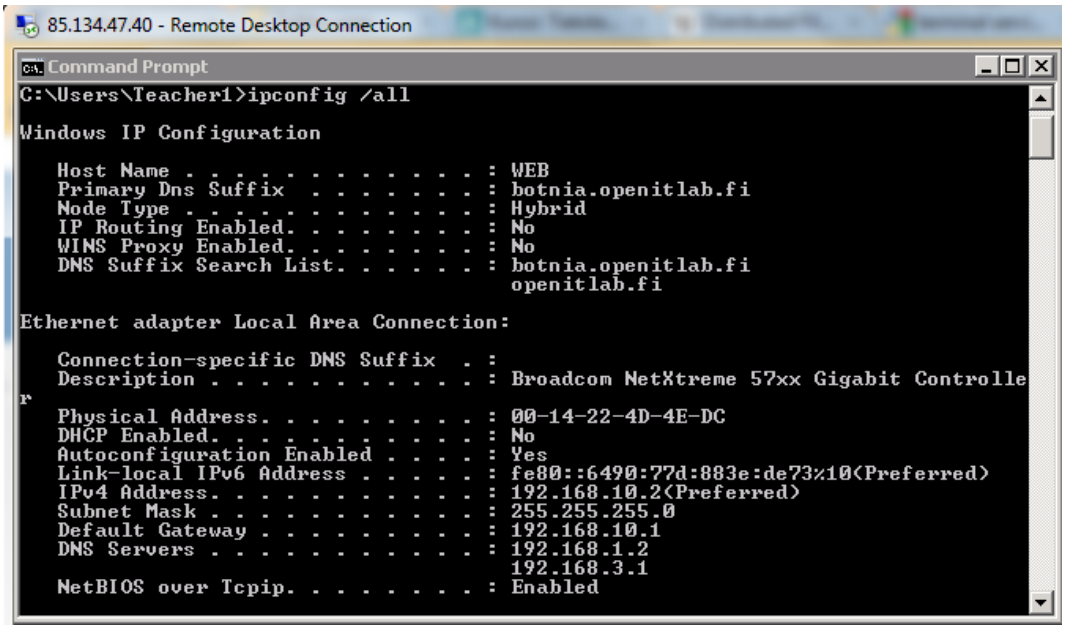
```
vyatta@vyatta# show interfaces ethernet eth2
 address 192.168.10.1/24
 description DMZ-zone
[edit]
vyatta@vyatta# show service dhcp-server
 disabled false
 shared-network-name POOL1_ETH1 {
     authoritative disable
     subnet 192.168.1.0/24 {
         default-router 192.168.1.1
         dns-server 192.168.1.2
         domain-name botnia.openitlab.fi
         start 192.168.1.20 {
             stop 192.168.1.30
```

Kuva 21. DHCP-palvelin ja eth2 asetukset.

5 TESTAUS

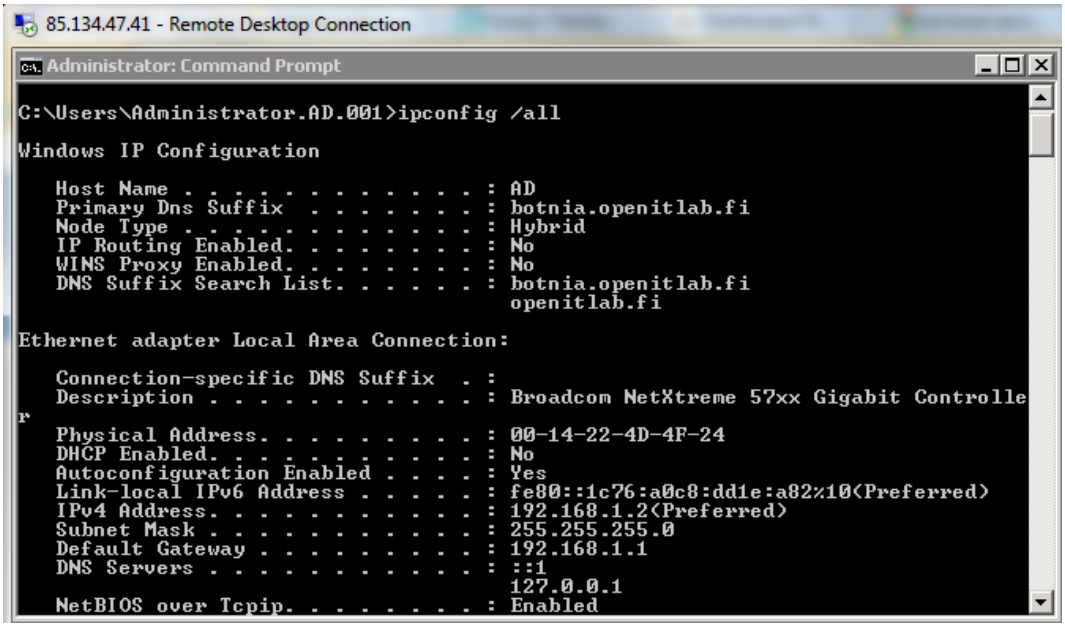
5.1 Etähallinta

Etähallintaa testattiin muodostamalla etäyhteys WWW- ja AD -palvelimille Windowsin Remote Desktop Connection -ohjelman avulla. Katso kuvat 22 ja 23.



Kuva 22. Etäyhteys WWW-palvelimelle.

Etäyhteys WWW-palvelimelle muodostettiin IP-osoitteen 85.134.47.40 kautta. Palvelimelle kirjauduttiin käyttäjän Teacher1 tunnuksilla. WWW-palvelimelle voi kirjautua etäyhteyden avulla käyttäen domainin käyttäjätunnuksia tai pääkäyttäjän tunnuksia.

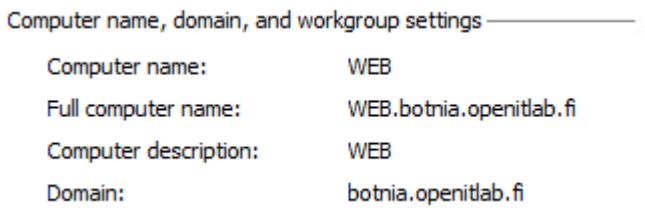


Kuva 23. Etäyhteys AD-palvelimelle.

Etäyhteyden muodostus AD-palvelimelle IP-osoitteen 85.134.47.41 kautta onnistui. Palvelimelle voi kirjautua etäyhteyden kautta ainoastaan pääkäyttäjän tunnuksilla.

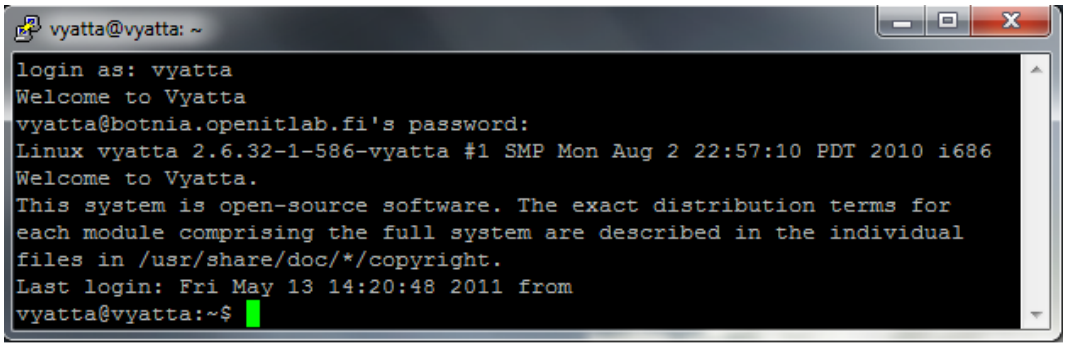
5.2 Palomuurin toimivuus

Palomuurin toimivuutta testattiin lisäämällä WWW -palvelin domain-alueeseen ja muodostamalla SSH-yhteys ulkoverkosta käyttäen Putty-ohjelmaa.



Kuva 24. WWW -palvelimen domain-tiedot.

WWW -palvelin lisättiin onnistuneesti domain-alueeseen.

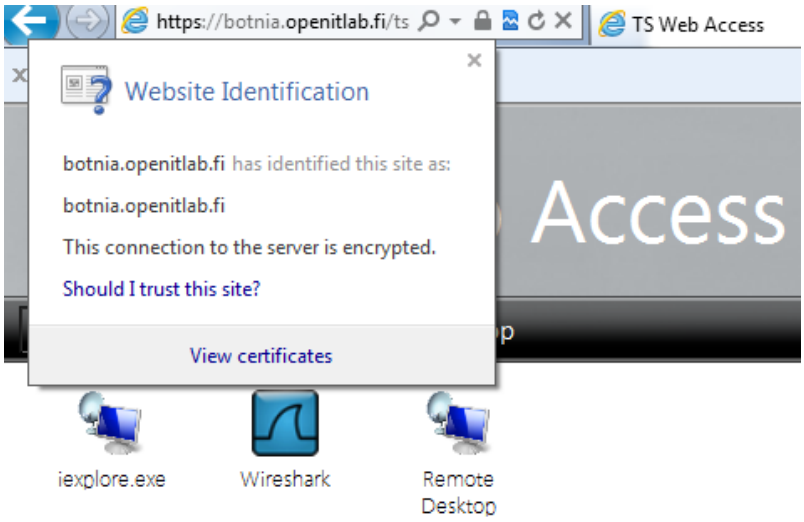


Kuva 25. SSH -yhteys ulkoverkosta.

Ulkoverkosta muodostettiin SSH-yhteys osoitteeseen 85.134.47.40 käyttäen porttia 22, yhteyden muodostus onnistui.

5.3 Sertifikaatti ja TS

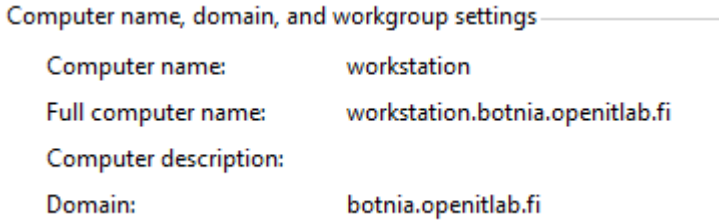
Sertifikaatin toimivuutta testattiin asentamalla se Trusted Root Certification Authorities -kansioon, jonka jälkeen muodostettiin yhteys osoitteeseen https://botnia.openitlab.fi/ts. Kuvasta 26 nähdään kuinka TS-sivusto on allekirjoitettu luotetulla sertifikaatilla.



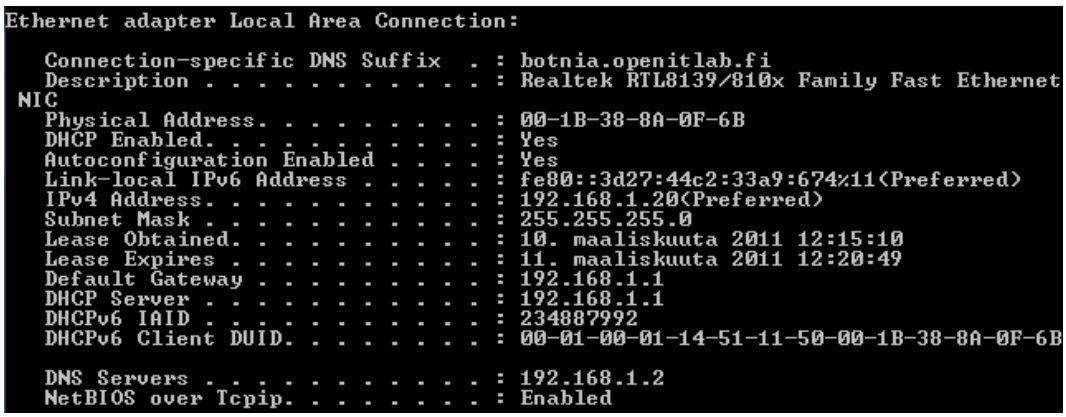
Kuva 26. Varmennettu TS-yhteys.

5.4 DHCP-palvelimen toimivuus

DHCP-palvelimen toimivuutta testattiin liittämällä työasema verkkoon ja botnia.openitlab.fi -domainiin.



Kuva 27. Työasema toimialueella.

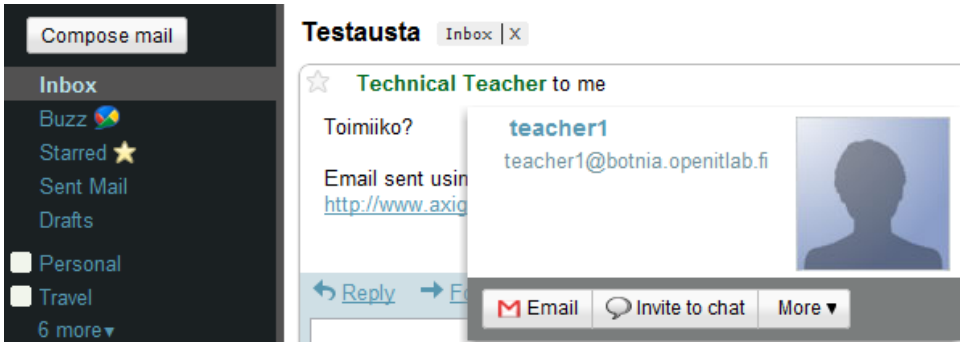


Kuva 28. Työasema DHCP -osoitteilla.

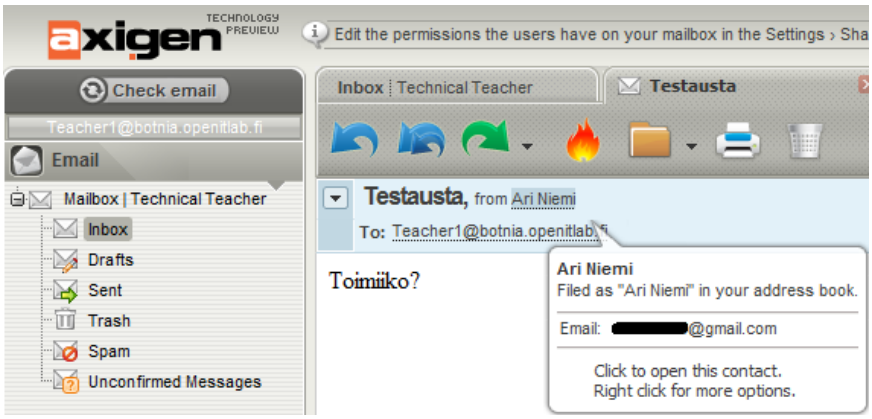
Työasema sai DHCP -palvelimelta oikeat osoitteet ja työaseman lisääminen domainiin onnistui, kuvat 27 ja 28.

5.5 Sähköpostipalvelimen testaaminen

Sähköpostipalvelimen toimivuutta testattiin lähettämällä ja vastaanottamalla sähköpostia Axigen webmailista, katso kuvat 29 ja 30.



Kuva 29. Sähköpostin lähettäminen.

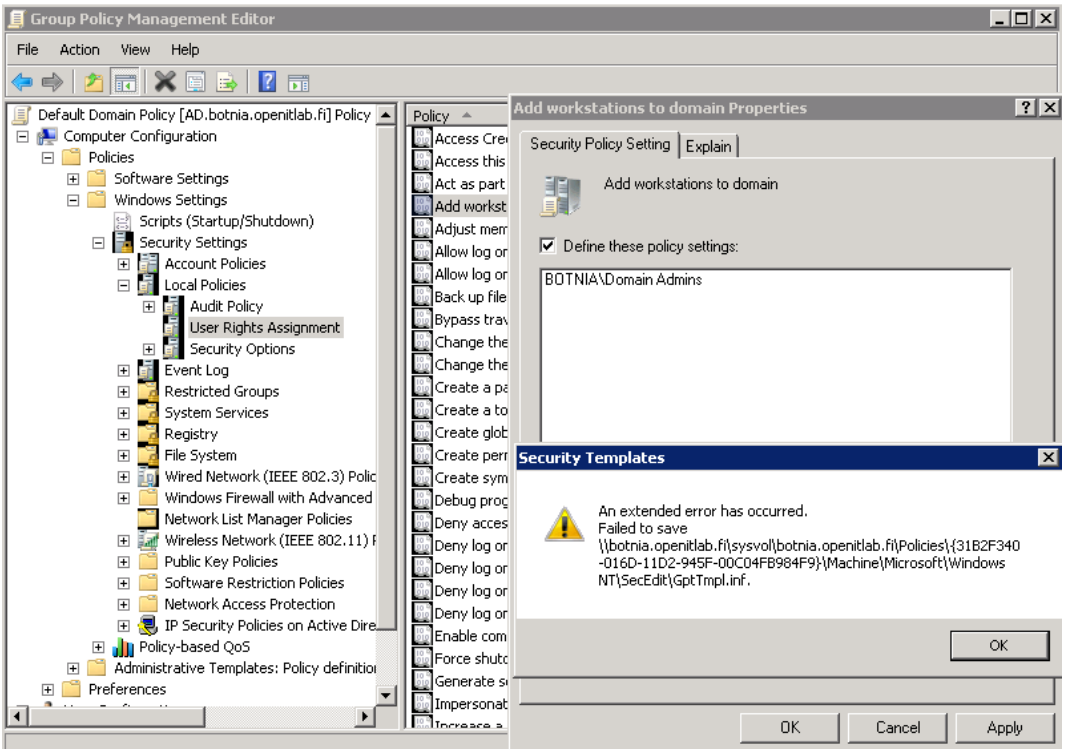


Kuva 30. Sähköpostin vastaanottaminen.

Sähköpostin lähettäminen ja vastaanottaminen onnistui.

5.6 Ongelmat Windows Server 2008:n kanssa

AD-palvelinta asennettaessa ei pystytty vaikuttamaan, mitkä käyttäjät voivat lisätä koneen domainiin. Windows Server 2008:ssa oletuksena kaikki kirjautuneet käyttäjät voivat lisätä työaseman tai laitteen Windows-domainiin. Tietoturvallisista syistä tämä oikeus tulisi sallia vain tietyille käyttäjille, joka voidaan tehdä Group Policy Management -valikon kautta kuvan 31 mukaisesti. Käyttöoikeuksia muokatessa saadaan virhesanoma ”An extended error has occured”, joka saattaa viitata käyttöoikeuksien puuttumiseen. Käyttöoikeudet tarkastettiin kuitenkin moneen kertaan, ja palvelimen pääkäyttäjällä pitäisi olla mahdollisuus muokata kaikkia toimintoja AD-palvelimessa. Ongelmaan ei kohtuullisen ajan puitteissa löydetty ratkaisua. Sama ongelma ilmeni myös hallintayksiköiden kanssa, jolloin ei pystytty verkon hallintaoikeuksia jakamaan eri hallintayksiköille tai lisäämään Logon Scriptia. Katso kuva 31.



Kuva 31. Extended error has occurred.

6 YHTEENVETO

Työn tavoitteissa onnistuttiin mielestäni melko hyvin, vaikka muutama asia jäikin toteuttamatta. Toteutuksesta jäi puuttumaan levypalvelimella sijaitsevat käyttäjien omat kansiot, joiden oli tarkoitus näkyä käyttäjille automaattisesti kirjautuessa. Logon Scriptin avulla käyttäjille voidaan määrittää kirjautumisasetukset, mutta AD-palvelimella oli ongelmia tiettyjen asetuksien määrittämisessä, joiden syyksi epäiltiin käyttöoikeuksien puuttumista, mutta lopullista ratkaisua tähän ei kuitenkaan saatu. Tästä johtuen ei hallintayksikön alle pystytty lisäämään Logon Scriptiä. Nämä palvelut oli tarkoitus toteuttaa myös Linux-palvelimella, jota ei kuitenkaan saatu kohtuullisessa ajassa toimimaan. Työssä suoritettiin onnistuneesti seuraavat asiat: WWW-palvelin, käyttäjien hallinta Windows Active Directory -domainissa, DNS-palvelin, DHCP-palvelin, palomuuri, NAT-osoitteenmuunnokset, Terminal Services -palvelut, sähköpostipalvelin, etähallinta, domain-nimi ja julkiset IP-osoitteet Open IT lab:n alaisuuteen ja sertifikaatit uuden domain-nimen mukaan.

Työn suorituksessa opin paljon uusia asioita, kuten eri tekniikoita ja protokollia, joita tarvitaan Windows-domainissa. Työssä käytetyt järjestelmät eivät olleet minulle tuttuja, joten opin paljon Windows-palvelinympäristöstä ja Vyatta Core:n tominnasta. Vyatta Core on mielestäni todella tehokas palomuuriohjelmisto, joka soveltuu varmasti suuremmankin verkkoratkaisun toteuttamiseen.

Sähköpostipalvelimen kanssa oli aluksi ongelmia lähetettäessä viestiä omalta palvelimelta toiselle palvelimelle. Ongelma saatiin korjattua oikeilla Domain Name Resolver -osoitteilla, joiden avulla sähköpostipalvelin selvittää ulkoverkkoon lähtevien viestien osoitetiedot. Microsoft IIS7 on monipuolinen WEB-sisällön hallintasovellus, jonka avulla pystytään omaa nettisivua ja verkon julkisia palveluita hallinnoimaan tehokkaasti. Ongelmia IIS7:n kanssa aiheutti FTP-palvelin, jonka pääsyn internetiin Windows-palvelimessa oletuksena oleva oma palomuuri esti. Ongelma voitiin korjata kytkemällä tämä palomuuri pois käytöstä, koska työssä asennettiin oma palomuurikone.

LÄHTEET

/1/ Vyatta.org – open network community. Vyatta Core:n kotisivu[online] [Viitattu 21.10.2010] Saatavilla WWW-muodossa: <URL:http://www.vyatta.org>.

/2/ Vyatta.org – open network community. Vyattan Core Firewall[online] [Viitattu 21.10.2010] Saatavilla WWW-muodossa: <http://www.vyatta.com/downloads/documentation/VC6.2/Vyatta_FirewallRef_R6.2_v01.pdf >.

/3/ Vyatta.org – open network community. Vyattan Core NAT[online] [Viitattu 21.10.2010] Saatavilla WWW-muodossa: <http://www.vyatta.com/downloads/documentation/VC6.2/Vyatta_NATRef_R6.2_v01.pdf >.

/4/ Vyatta.org – open network community. DHCP -palvelin[online] [viitattu 25.4.2011] Saatavilla WWW-muodossa: <URL:http://www.vyatta.com/downloads/documentation/VC6.2/Vyatta_ServicesRef_R6.2_v01.pdf>.

/5/ Microsoft corporation 2011. Windows server 2008[online] [viitattu 9.2.2011] Saatavilla WWW-muodossa: <URL: http://technet.microsoft.com/en-us/library/dd282984(WS.10).aspx>.

/6/ Microsoft corporation 2011. Active Directory[online] [viitattu 9.2.2011] Saatavilla WWW-muodossa: <URL:http://technet.microsoft.com/en-us/library/cc731053(WS.10).aspx>.

/7/ Microsoft corporation 2011. RPC[online] [viitattu 7.5.2011] Saatavilla WWW-muodossa: <URL: http://technet.microsoft.com/en-us/library/cc738291(WS.10).aspx>.

/8/ Microsoft corporation 2011. NetBIOS[online] [viitattu 7.5.2011] Saatavilla WWW-muodossa: <URL:http://technet.microsoft.com/en-us/library/bb727013.aspx>.

/9/ Microsoft corporation 2011. DNS[online] [viitattu 7.5.2011] Saatavilla WWW-muodossa: <URL: http://technet.microsoft.com/en-us/library/cc730921.aspx >.

/10/ Microsoft corporation 2011. LDAP[online] [viitattu 7.5.2011] Saatavilla WWW-muodossa: <URL: http://msdn.microsoft.com/en-us/library/aa367008(v=VS.85).aspx>.

/11/ Microsoft corporation 2011. Kerberos[online] [viitattu 7.5.2011] Saatavilla WWW-muodossa: <URL: http://technet.microsoft.com/en-us/library/bb742516.aspx>.

/12/ Microsoft corporation 2011. Kerberos[online]
[viitattu 7.5.2011] Saatavilla WWW-muodossa:
<URL: http://msdn.microsoft.com/en-us/library/ms721592(v=VS.85).aspx#_security_local_security_authority_gly>.

/13/ Microsoft corporation 2011. Server manager[online]
[viitattu 9.2.2011] Saatavilla WWW-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc732131(WS.10).aspx>.

/14/ Microsoft corporation 2011. File services[online]
[viitattu 13.2.2011] Saatavilla WWW-muodossa:
<URL: http://technet.microsoft.com/en-us/library/cc771548(WS.10).aspx>.

/15/ Vyatta.org – open network community. Vyattan asentaminen[online]
[Viitattu 21.10.2010] Saatavilla WWW-muodossa:
<URL:http://www.vyatta.com/products/training/free/installverify/VyattaInstallVerify.htm>.

/16/ Microsoft corporation 2011. How to configure a firewall for domains and trusts[online]
[viitattu 15.3.2011] Saatavilla WWW-muodossa:
<URL: http://support.microsoft.com/kb/179442>.

/17/ Microsoft corporation 2011. Default dynamic port range for TCP/IP[online]
[viitattu 14.5.2011] Saatavilla WWW-muodossa:
<URL: http://support.microsoft.com/kb/929851>.

/18/ Viestintävirasto 2011. Sertifikaatti[online]
[viitattu 14.5.2011] Saatavilla WWW-muodossa:
<URL:
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki/varmenne.html>.