VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Sakari Raatikainen

OpenVPN-etäyhteys

Liiketalous
2016

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Sakari Raatikainen
Opinnäytetyön nimi	OpenVPN-etäyhteys
Vuosi	2016
Kieli	suomi
Sivumäärä	48
Ohjaaja	Antti Mäkitalo

Tässä opinnäytetyössä tarkoitus on havainnollistaa kuinka OpenVPN-etäyhteys luodaan ja kuinka sitä käytetään. Työssä käydään läpi teoriaa sekä käytännön asennuksia. Teoriaosuus kertoo tarkemmin työn tärkeistä asioista ja käytännön asennukset antavat selvän kuvan kuinka asennukset suoritetaan onnistuneesti. Teoriaosuudessa käsitellään OSI-malli, VPN, OpenVPN, PfSense ja Wireshark.

Valitsin työssä käytettäväksi Virtuaalikoneeksi VirtualBoxin, koska se oli tuttu entuudestaan. Virtuaalikoneeseen asensin kaksi käyttöjärjestelmää sekä palomuurin. Työssä käytin lähteinä suomen- ja englanninkielisiä kirjoja sekä verkkomateriaalia.

Lopputuloksena luotiin toimiva OpenVPN-yhteys, joka kulkee palomuurin läpi.

Avainsanat VPN, OpenVPN, PfSense

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Sakari Raatikainen
Title	Remote Access with OpenVPN
Year	2016
Language	Finnish
Pages	48
Name of Supervisor	Antti Mäkitalo

This thesis studied how OpenVPN remote-access is created and how to use it. The project covers theory and practical installations. The theoretical study explains the important things of this project in more detail. The practical installation shows how to make installations successfully. The theoretical study explains OSI-model, VPN, OpenVPN, PfSense and Wireshark.

Virtualbox was chosen for the virtual machine because it was already familiar to me. I installed two operating systems and a firewall to the Virtualbox. In this project both Finnish and English books and online material were used as source material.

The result of this project was a successful OpenVPN remote access through PfSense firewall.

Keywords VPN, OpenVPN, PfSense

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

MÄÄRITELMÄT JA LYHENTEET

ARP	Address Resolution Protocol. Protokolla, joka selvittää IP-osoitteita vastaavat MAC-osoitteet.
Ekstranet	Yrityksen tai organisaation sisäinen suljettu verkkopalvelu, joka hyödyntää Internetiä.
GRE	Generic Routing Encapsulation. Cisco ip-tunnelointiprotokolla.
IP	Internet Protocol. Huolehtii tietoliikennepakettien perille toimittamisesta pakettikytkentäisissä verkoissa.
IPSec	IP Security. IETF:n standardoima tietoturvaprotokolla.
IPX	Internetwork Packet eXhange. Reititysprotokolla.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.
LLC	Logical Link Control. Osa siirtoyhteyskerrosta. Hallitsee lähiverkon toimintoja.
L2F	Layer 2 Forwarding. Tunnelointiprotokolla lähiverkkojen yhdistämiseen.
L2TP	Layer 2 Tunneling Protocol. Yhdistelmä L2F:stä ja PPTP:stä.
MAC	Media Access Control. Osajärjestelmä, joka hoitaa verkon varaamisen ja liikennöinnin.
PPP	Point-to-point Protocol. Muodostaa suoran yhteyden verkkolaitteiden välille.
PPTP	Point-to-point Tunneling Protocol. Suunniteltu modeemi-yhteyksille ja lankapuhelinverkossa kulkeville yhteyksille.

SSL	Secure Socket Layer. Tietoliikenteen salausprotokolla.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla yhteyksien muodostamiseen tietokoneiden välille.
UDP	User Datagram Protocol. yhteydetön protokolla.
VPN	Virtual Private Network. Virtuaalinen erillisverkko, muodostaa salatun yhteyden julkisen verkon yli.

1 JOHDANTO

VPN-tekniikka (Virtual Private Network) on hyvin suosittua ja tarpeellista nykypäivänä. Se mahdollistaa työasemien etäkäytön käytännössä mistä vaan. VPN-tekniikka on halpa vaihtoehto laajentaa yrityksen sisäistä verkkoa, koska tieto kulkee Internetin yli.

Tässä opinnäytetyössä ensiksi tutustutaan OSI-malliin. Sitten käydään läpi VPN-tekniikkaa sen yhteystapoja, tunnelointiprotokollia sekä hyötyjä. Teoriaosuudessa tutustutaan myös Wireshark verkkoanalysaattoriin, OpenVPN-ohjelmistoon sekä PfSense palomuuriin.

Työssä käytän ilmaista Virtualbox virtuaalikonetta, johon asennan käyttöjärjestelmät Windows 7 ja Ubuntu 14.04 LTS sekä PfSense-palomuurin. Windows koneelle asennan OpenVPN-clientin sekä Wireshark-ohjelman, jolla monitoroin koneiden välille luotua VPN-yhteyttä. Ubuntu koneelle asennan Apache2 HTTP-palvelimen. PfSense-palomuuriin asennan OpenVPN-ohjelman. VPN-yhteys kulkee Windows koneelta PfSense-palomuurin läpi Ubuntu koneelle.

Tämän työn on tarkoitus selvittää seuraavat tutkimuskysymykset

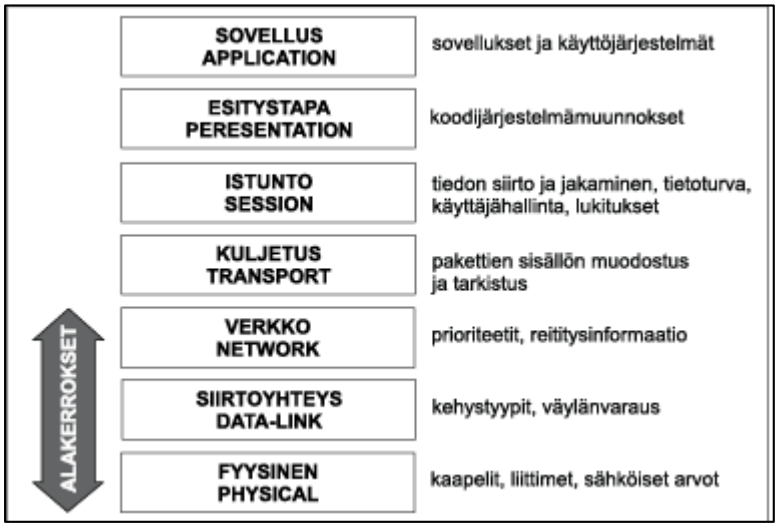
- Mitä on VPN-tekniikka ja mihin sitä käytetään?
- Kuinka OpenVPN-ohjelman asennus toteutetaan ja miten sitä käytetään?

Tavoitteet tässä opinnäytetyössä ovat opetella ja suorittaa OpenVPN:n asennus PfSense palomuuriin sekä suorittaa asennuksen testaus. Tavoitteena on myös kertoa työn kannalta tärkeää teoriaa.

2 OSI-MALLI

ISO:n (International Organization for Standardization) määrittelemä OSI-malli (Open Systems Interconnection Reference Model) on ehkä tärkein tietoliikenteen kuvauksissa käytettävä standardi. Tämä standardi oli tarkoitettu alun perin yhteensovittamaan eri valmistajien laitteet ja ohjelmistot. OSI-mallin mukaisia järjestelmiä ei kuitenkaan otettu laajamittaiseen käyttöön koska laitevalmistajien ja ohjelmiston toimittajien välinen kilpailu esti sen. Malli on kuitenkin käytössä tieto- ja tietoliikennejärjestelmien toiminnan kuvaamiseen. OSI-mallin tunteminen helpottaa hahmottamaan monimutkaisten järjestelmien eri osien yhteistoimintaa.

OSI-malli on jaettu seitsemään kerrokseen. Alemmat kerrokset (1-3) määrittelevät laitteistojen sekä niihin läheisesti liittyvien protokollien toiminnan. Kerroksia kutsutaan alakerroksiksi. Ylempiä kerroksia kutsutaan isäntäkerroksiksi ja ne määrittelevät asiakas- ja palvelinsovellusten ohjelmallisen toiminnan. (Hakala & Vainio 2005, 138.)



Kuvio 1. OSI-malli. (Hakala & Vainio 2005)

2.1 OSI-mallin kerrokset

OSI-mallin kerrokset ovat seuraavat alhaalta ylöspäin. (kuvio 1.)

2.1.1 Fyysinen kerros (kerros 1.)

Fyysinen kerros muuntaa siirrettävän datan bitti kerrallaan sähköimpulsseiksi, radiosignaaleiksi ja valoksi, tätä kutsutaan johtokoodaukseksi. Se määrittää myös yhteyden fyysiset ominaisuudet kuten kaapeloinnin ja liitännät. Fyysisen kerroksen aktiivilaitteisiin kuuluvat keskittimet, toistimet ja mediamuuntimet. (Beal 2015; Hakala & Vainio 2005, 139.)

2.1.2 Siirtoyhteyskerros (kerros 2.)

Siirtoyhteyskerros huolehtii siirtoprotokollan tiedoista sekä hallitsee ja korjaa fyysisellä kerroksella tapahtuvia virheitä.

Siirtoyhteyskerros jaetaan kahteen alempaan kerrokseen, jotka ovat The Media Access Control (MAC) kerros ja Logical Link Control (LLC) kerros. MAC kerros hallitsee sitä kuinka verkossa oleva tietokone saa yhteyden dataan sekä saa luvan lähettää sitä. LLC kerros hallitsee kehysten synkronoinnin, datan virtauksen hallinnan sekä virheentarkistuksen. (Beal 2015.)

2.1.3 Verkkokerros (kerros 3.)

Verkkokerros määrittelee tarvittavan reitityksen verkkojen väliseen tietoliikenteeseen sekä eri liikennemuotojen välisen tärkeysjärjestyksen. Lähiverkoissa käytetään tehtävien hoitamiseen yleisimmin IP-protokollaa (Internet Protocol) sekä Novellin IPX-protokollaa (Internetwork Packet eXhange). Verkkokerroksen keskeisin aktiivilaite on reititin. (Hakala & Vainio 2005, 139.)

2.1.4 Kuljetuskerros (kerros 4.)

Kuljetuskerroksen tehtävistä huolehtivat lähiverkoissa kuljetusprotokollat kuten TCP (Transmission Control Protocol), Novellin SPX (Sequential Packet Exchange) sekä NetBIOS-protokollat. Nämä protokollat huolehtivat sovellusten lähettämän datavirran segmentoinnista eli pilkkomisesta käsittelykokoisiin osiin. Yhteyden muodostaminen asiakas- ja palvelinohjelmistojen välillä on myös näiden kuljetusprotokollien tehtävänä. Ne varmistavat myös lähetetyn datan perille menon sopivalla kuittausmenetelmällä.

Vuono-ohjaus koostuu segmentoinnista, pakettikoon määrityksestä ja kuittauksesta. Jotkut kuljetusprotokollat ovat toisia kehittyneempiä ja ilmoittavat dataa lähettävälle laitteelle kuinka paljon tämä laite voi ottaa maksimissaan dataa vastaan. Nämä protokollat seuraavat laitteen kuormitustilannetta. Tällaisia protokollia kutsutaan yhteydelliseksi protokollaksi. Yhteydettömäksi protokollaksi kutsutaan sellaista protokollaa, joka huolehtii vain osasta vuono-ohjauksesta. Esimerkiksi TCP/IP-protokollaperheeseen kuuluva UDP-protokolla (User Datagram Protocol) huolehtii vain segmentoinnista, joten se on yhteydetön protokolla. (Hakala & Vainio 2005, 139-140.)

2.1.5 Istuntokerros (kerros 5.)

Käyttöoikeuksien tarkistaminen ja muut järjestelmien suojaukseen liittyvät kuuluvat istuntokerroksen tehtäviin. Sen ohjelmistot huolehtivat tiedosto-, tietue- ja kenttälukituksesta sekä tarjoavat tarvittavat kirjautumistavat ja salausmenetelmät. Keskusmuistialueiden suojaus kuuluu myös istuntokerroksen tehtäviin. Käyttöjärjestelmät vastaavat nykyisissä järjestelmissä useimmista tehtävistä. Tämän kerroksen ohjelmistoina toimivat myös osittain tietokantojen hallintajärjestelmät ja salausohjelmistot. (Hakala & Vainio 2005, 140.)

2.1.6 Esitystapakerros (kerros 6.)

Esitystapakerros määrittelee asiakkaan ja palvelimen välisen ns. sanomaliikenteen muodon. Näihin määrittelyihin kuuluvat erilaiset koodausjärjestelmät. Tiedonsiirto tapahtuu järjestelmien välillä binäärimerkkijonoina. Yhden tietotyypin siirrossa joudutaan määrittelemään sanomarakenteeseen, kuinka alkuperäiset tietotyypit koodataan binäärimerkkijonoiksi ja kuinka ne dekoodataan takaisin vastaanottavalle sovellukselle alkuperäiseen muotoon. (Hakala & Vainio 2005, 140.)

2.1.7 Sovelluskerros (kerros 7.)

Alemmista kerroksista ei ole määritelty kaikkia sovellusten ja käyttöjärjestelmien toiminnan osia. Sovelluskerros määrittelee ne osat. Sovellus-, esitystapa- ja istuntokerrosten erottaminen toisistaan ei ole mahdollista nykyisissä lähiverkkojen käyttöjärjestelmissä ja sovelluksissa. Näistä kolmesta muodostuu yksi ohjelmallinen kokonaisuus. (Hakala & Vainio 2005, 140-141.)

3 VPN

VPN (Virtual Private Network) kehitettiin helpottamaan etäyhteyksien luontia. Nykyään organisaatiot toimivat monimutkaisissa ja hajautetussa ympäristössä, jotka käsittävät monia toimipisteitä ympäri maailmaa. Useat näistä toimipisteistä tarvitsevat pääsyn organisaation keskitettyyn IT-ympäristöön sekä etäkäytön mahdollisuuden liikkuville työntekijöilleen. Ei ole kuitenkaan turvallista lähettää sisäverkon liikennettä sellaisenaan Internetin yli. Se on iso tietoturvariski. Julkisen verkon kautta voidaan rakentaa turvallinen tapa välittää tietoa ns. tunnelin läpi. Sitä kutsutaan VPN-yhteydeksi. Etäyhteyksistä on tullut tärkeä osa yritysmaailmaa. (Howath 2008; Hakala & Vainio 2005, 381.)

VPN on salattu etäyhteys kahden tai useamman yksityisen verkon välillä julkisen verkon kautta. VPN-yhteys luo ns. tunneliverkon jossa data liikkuu turvallisesti esimerkiksi yrityksen sisäisessä verkossa toimipisteestä toiseen tai työntekijän kotiin. (Gupta 2002, 4.) Turvallisuuden säilymiseksi täytyy tiedon muuttumattomuuden ja luottamuksellisuuden säilyä. Käyttäjien tunnistamisella ja heidän käyttöoikeuksien hallinnalla kasvatetaan turvallisuutta. (Kaario 2002, 314.)

Esimerkkejä VPN:n käytöstä

- Pääsy työpaikan verkkoon matkustaessa
    - VPN on käytössä paljon matkustavilla työntekijöillä. Heillä on pääsy yrityksen verkkoon ja kaikkiin resursseihin heidän ollessaan tien päällä.

- Pääsy kotiverkkoon matkustaessa
    - Voidaan asettaa myös oma VPN, jolla saadaan pääsy omaan kotiverkkoon ollessa matkoilla.

- Selaustoiminnan piilottaminen julkisessa verkossa

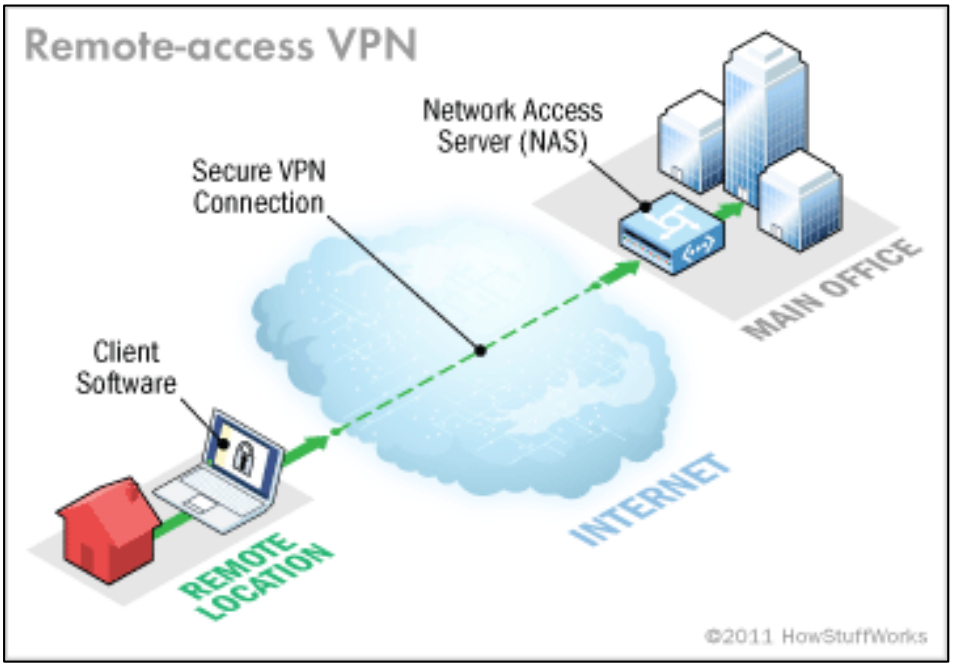
- Jos käyttää julkista Wi-Fi-yhteyttä selaustoiminta näkyy muille, jos ei surffaile HTTPS verkkosivuilla ja etsijät tietävät miten etsiä. Kun haluaa salata selaustoiminnan voi käyttää VPN:ää. (Hoffmann 2013.)

3.1 VPN yhteystavat

Kun data reititetään Internetin yli, se kulkee läpi erilaisten palveluntarjoajien verkkojen ja laitteiden. Palveluntarjoaja ei välttämättä tarjoa minkäänlaista turvallisuutta. Asiakkaat haluavat datansa kulkevan turvallisesti, eivätkä ehkä luota palveluntarjoajan verkkoon, joten he luovat virtuaalisen tunnelin saadakseen liikenteen turvallisesti perille. Tällaisissa tapauksissa palveluntarjoaja toimii vain IP-liikenteen kuljettajana. (Nayak & Rao 2014, 247.)

3.1.1 Etäyhteys (Host-to-site) VPN

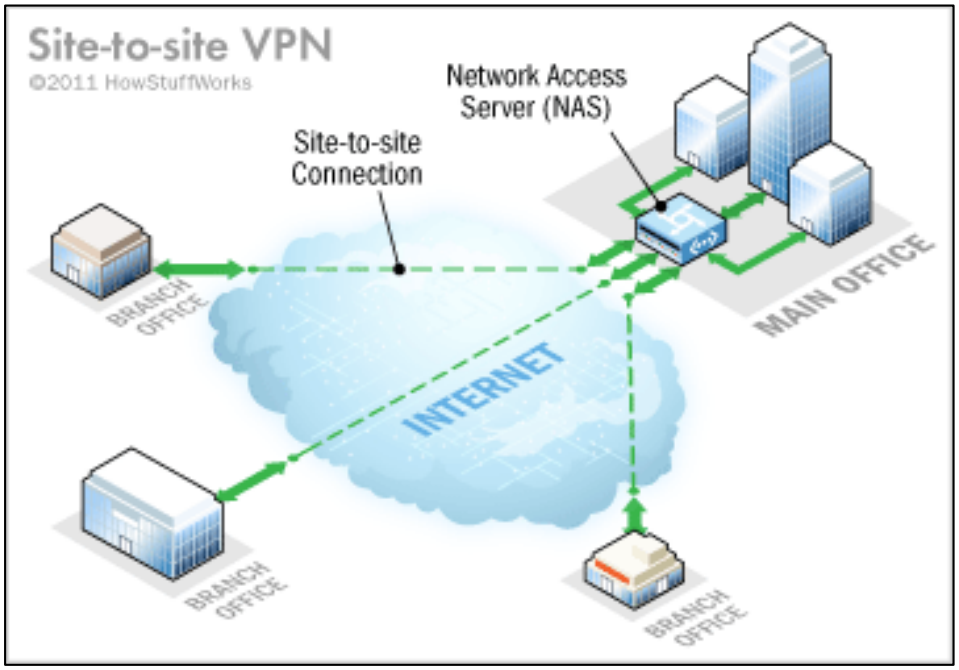
Etäyhteys VPN (kuvio 2.) yhdistää yksityisen käyttäjän laitteen ja yrityksen sisäverkon. Esimerkiksi matkustava työntekijä tarvitsee pääsyn yrityksen verkkoon turvallisesti yli internetin. Käyttäjä tarvitsee yhteyden luomiseen VPN-ohjelmiston. Yrityksen sisäverkon VPN-yhdyskäytävä huolehtii käyttäjän tunnistamisen ja luo salatun tunneliyhteyden. Kun salattu yhteys on luotu, käyttäjä voi turvallisesti siirtää dataa oman laitteen ja yrityksen verkon välillä. Tämän tyyppinen etäyhteys tarjoaa turvallista, salattua kommunikaatiota kahden osapuolen välillä, jotka ovat yhteydessä Internetiin. (Nayak & Rao 2014, 247.)



Kuvio 2. Host-to-site VPN-etäyhteys. (computer.howstuffworks.com)

3.1.2 Site-to-site VPN

Site-to-site VPN (kuvio 3.) yhdistää lähiverkon internetin yli toiseen lähiverkkoon, esimerkiksi yhdistäen organisaation toisen konttorin verkon pääkonttorin verkkoon. Tällaisessa tapauksessa VPN-tunneli on luotu kahden VPN-yhdyskäytävän väliin. Konttorin VPN-yhdyskäytävä neuvottelee pääkonttorin VPN-yhdyskäytävän kanssa ja muodostaa suojatun tunnelin. VPN-yhdyskäytävä on vastuussa tiedon salaamisesta, käyttäjien ja verkon tunnistamisesta sekä tiedon eheydestä. (Nayak & Rao 2014, 248.)



Kuvio 3. Site-to-site VPN-yhteys. (computer.howstuffworks.com)

3.1.3 Host-to-host VPN

Host-to-host VPN-yhteydessä kaksi konetta on yhteydessä toisiinsa salatun VPN tunnelin kautta. Ennen tiedonsiirtoa koneet tunnistavat käyttäjät ja salausavaimet vaihdetaan koneiden välillä. Tämän jälkeen tiedonsiirto voi alkaa. VPN-tunneli takaa tiedon aitouden, eheyden ja luottamuksellisuuden. (Nayak & Rao 2014, 248.)

3.2 VPN tunnelointiprotokollat

VPN yhteyden luomiseen tarvitaan jokin tunnelointiprotokolla. Seuraavassa esitellään muutamia tunnelointiprotokollia.

3.2.1 IPSec

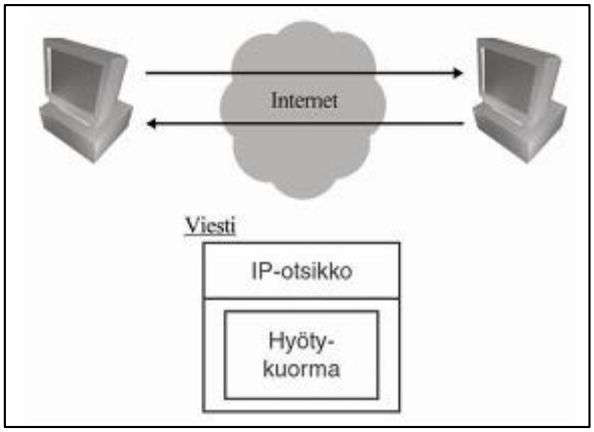
IPSecurity (IPSec) on IETF:n standardoima tietoturvaprotokolla. IPSec toimii OSI-mallin verkkokerroksella ja se sisältää IP-protokollan turvamekanismin sekä avaintenhallinta-protokollan. Koko verkko on suojattu, sillä jokaisen yhteyden täytyy kulkea verkkokerroksen läpi. Se on myös rakennettu IPV6-protokollalle. (Gupta 2002, 145-146.)

IPSec mahdollistaa viestien:

- eheyden varmistamisen
- lähettäjän varmistamisen
- toistamisen estämisen
- salakirjoittamisen.

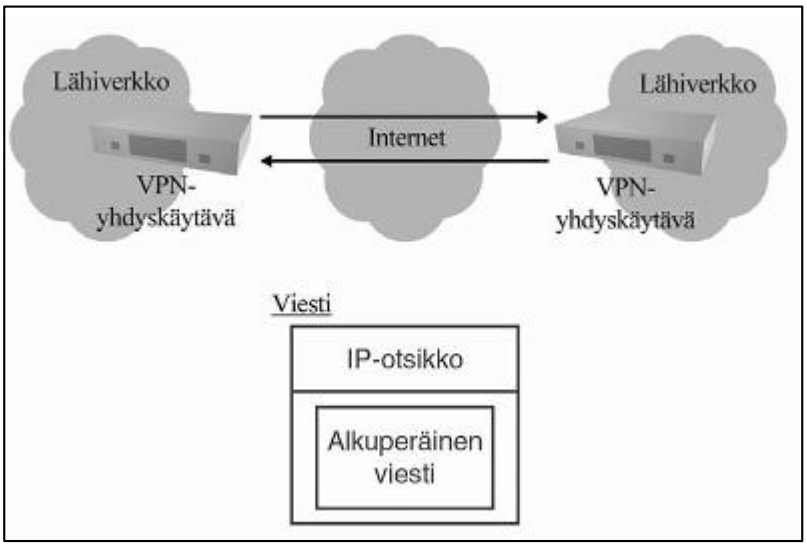
IPSec-protokollaa voidaan käyttää joko kuljetusmoodissa tai tunnelimoodissa.

Kuljetusmoodissa (kuvio 4.) IPSec-yhteys suojaa lähetettävän viestin sisällön sekä varmistaa IP-otsikon tietojen muuttumattomuuden saapuessa vastaanottajalle. Salakirjoitusta IP-otsikon tiedoille ei voida tehdä kuljetusmoodissa. (Ruohonen 2002, 291.)



Kuvio 4. Kuljetusmoodi. (Ruohonen 2002.)

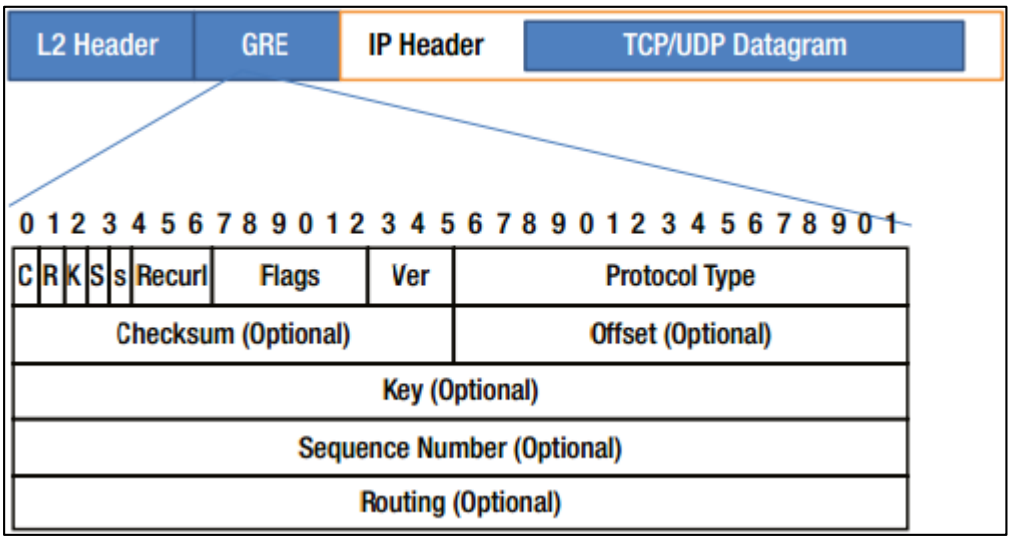
Tunnelimoodissa (kuvio 5.) IPSec-yhteydellä lähetettävät viestit asetetaan uuden viestin sisälle ja uusi viesti suojataan. Uuden viestin vastaanottaja purkaa siitä alkuperäisen viestin. Alkuperäinen viesti voidaan salakirjoittaa kokonaan tunnelimoodissa. (Ruohonen 2002, 291-292.)



Kuvio 5. Tunnelimoodi. (Ruohonen 2002.)

3.2.2 GRE

Generic Routing Encapsulation on tunnelointiprotokolla, joka tiivistää yhden IP-datagrammin toiseen IP-datagrammiin ja kuljettaa sen eteenpäin. Toisin sanoen GRE tiivistää yhden verkkokerroksen protokollan minkä tahansa toisen verkkokerroksen protokollan kanssa. (Nayak & Rao 2014, 253.)



Kuvio 6. Tyypillinen GRE-datagrammi. (Nayak & Rao 2014.)

Verkkokerrospaketti jota kutsutaan nimellä ”hyötykuorma” kapseloituu GRE pakettiin, joka voi sisältää kaikki hyötykuormapaketin verkon reititystiedot. Tuloksena GRE-paketti kapseloituu edelleen toiseen verkkokerroksen protokollaan nimeltä ”toimitusprotokolla” ja seuraavaksi se lähetetään VPN tunneliin. (Nayak & Rao 2014, 253.)

3.2.3 PPTP

PPTP (Point-to-point tunneling protocol) kehitettiin 1990-luvun puolivälissä mekanismiksi tunneloida PPP-paketteja läpi IP-verkon. PPTP takaa turvallisen tiedonsiirron etäkäyttäjältä nettipalvelimelle läpi IP-verkon, luoden VPN-yhteyden kahden päätepisteen väliin. Kun PPTP kehitettiin, internetyhteydet koostuivat modeemi-yhteyksistä eli lankapuhelinverkossa kulkevista yhteyksistä. Nykyään niitä ei ole käytössä lähes lainkaan. PPTP:n tietoturva on nykyään riittämätön, joten tätä protokollaa ei voida enää käyttää. (Held 2005, 90.)

3.2.4 L2F

L2F (Layer 2 Forwarding) on Ciscon oma tunnelointiprotokolla mitä käytetään vain Ciscon laitteissa. L2F-protokolla on hyvin samanlainen kuin PPTP-protokolla, se käyttää PPP (Point-to-point) protokollaa hyödyksi VPN-yhteyden luomiseksi. L2F:stä modernimpi versio L2TP on vaihtoehto L2F:n korvaajaksi. (Held 2005, 115; Gupta 2002, 115-116.)

3.2.5 L2TP

Layer 2 Tunneling Protocol toimii OSI-mallin toisella kerroksella eli siirtoyhteyskerroksella. Sitä käytetään PPP-kehysten siirtämiseen pakettikytkentäisissä verkoissa. Protokollan salaukseen käytetään IPSec-salausta.

L2TP-otsake ja UDP-otsake lisätään protokollan alkuperäiseen PPP-kehykseen. Paketti salataan IPSecillä ja siihen lisätään IPSec Encapsulating Security Payload -otsakkeet (IPSec ESP header ja IPSec ESP trailer) sekä IPSec Authentication trailer. IPSec Encapsulating Security Payload –otsakkeista IPSec ESP header on salaamaton ja IPSec ESP trailer salattu. IPSec Authentication trailer on salaamaton.

Näistä muodostunut salattu paketti sijoitetaan IP-datagrammin sisään. (Hakala & Vainio 2005, 383.)

3.2.6 SSL VPN

Nykypäivänä yleisimmin käytetyt VPN-yhteydet ovat SSL-pohjaisia. SSLVPN (Secure Sockets Layer Virtual Private Network) hyödyntää yhteyden salauksessa SSL/TSL-protokollaa. SSL VPN:ää voidaan käyttää joko selaimen kautta tai erillisellä asiakasohjelmistolla kuten Ciscon AnyConnect ja Microsoftin SSTP. Useimmat SSL-pohjaiset VPN-yhteydet käyttävät samaa verkkoprotokollaa kuin suojattu nettisivu (HTTPS). (Crist & Just Keijser 2015)

3.3 VPN:n hyödyt

- Halpa toteutus:

  VPN on huomattavasti halvempi vaihtoehto kuin perinteiset ratkaisut, jotka perustuvat kiinteisiin yhteyksiin, Frame Relay-, ATM- ja ISDN-teknologioihin. VPN poistaa pitkien matkojen kiinteiden yhteyksien tarpeen käyttämällä hyödyksi Internetiä.

- Helpompi yhteydenpito:

  VPN tarjoaa yrityksille helpomman yhteydenpidon yrityksen konttorien välillä. Koska Internettiin on pääsy maailmanlaajuisesti, VPN:n avulla voi yhdistää maailman toisella puolella sijaitsevan yrityksen konttorin samaan yrityksen sisäverkkoon. Työmatkalla oleva työntekijä pääsee käsiksi kannettavallaan tai älypuhelimellaan yrityksen sisäverkkoon.

- Turvallinen datan siirto:

  VPN käyttää salausta, todentamista ja valtuuttamista, taatakseen turvallisen, eheän ja luottamuksellisen tiedon siirron.

- Hyvä laajennettavuus:

  Internet pohjainen VPN mahdollistaa yrityksen sisäverkon kehityksen ja kasvamisen kun liiketoiminta tarvitsee muutosta, ilman suuria lisämenoja laitehankintoihin. Tämä tekee VPN pohjaisen sisäverkon hyvin laajennettavaksi ja mukautuvaksi ilman, että yritys laittaa paljon rahaa verkon rakentamiseen. (Gupta 2002, 8.)

- Ekstranet-verkko:

  Ekstranet-verkon avulla yritys voi nopeasti hoitaa asioita alihankkijoiden tai asiakkaiden kanssa, esimerkiksi lähettää ja vastaanottaa tilauksia. (Ruohonen 2002, 95.)

4 OPENVPN

OpenVPN Technologies perustettiin vuonna 2002 Kaliforniassa Pleasantonissa. Francis Dinha ja James Yohan perustivat yrityksen, kehitettyään OpenVPN-ohjelmiston OpenVPN-projektin tuloksena samaisena vuonna ja he halusivat, että OpenVPN-ohjelmiston kehitys jatkuisi edelleen. (openvpn.net, About US)

OpenVPN on GNU GPL – avoimen lisenssin alainen VPN-ohjelmisto. Se perustuu avoimeen lähdekoodiin ja on SSL VPN-pohjainen ratkaisu. OpenVPN pitää sisällään monia konfiguraatioita kuten etäyhteydet, Site-on-Site VPN yhteydet, Wi-Fi turvan ja yritystasolla etäratkaisut. OpenVPN tarjoaa kustannustehokkaan ja kevyen vaihtoehdon vastapainoksi muille VPN teknologioille, jotka ovat suunnattu yritysmarkkinoille.

OpenVPN:n turvallisuus perustuu SSL-protokollaan, joka on turvallinen tapa salata Internet yhteyksiä. OpenVPN käyttää OSI-mallin ensimmäistä tai toista kerrosta. Suojatakseen liikenteen se käyttää SSL/TLS-protokollaa. OpenVPN tukee käyttäjien monia todentamismenetelmiä kuten sertifikaatteja, älykortteja ja kaksivaiheista todentamista.

OpenVPN toimii Windows, Linux, Mac OS X, OpenBSD, FreeBSD, NetBSD ja Solaris käyttöjärjestelmillä. (openvpn.net, Overview)

OpenVPN:llä voi:

- Tunneloida minkä tahansa IP-aliverkon tai virtuaalisen Ethernet-sovittimen yli yhteen TCP- tai UDP-porttiin.

- Konfiguroida skaalautuvan VPN-serveri alustan käyttäen yhtä tai useampaa konetta, jotka voivat käsitellä VPN-clienteilta tulevia tuhansia dynaamisia yhteyksiä.

- Käyttää kaikkia salauksen, tunnistautumisen ja sertifioinnin OpenSLL-kirjaston ominaisuuksista, suojatakseen yksityistä verkkoa ja sen liikennettä Internetissä.

- Tunneloida verkot yli NAT:n

- Konfiguroida sitä käyttäen graafista käyttöliittymää GUI:tä (Graphical User Interface) Windowsilla tai Mac OS X:llä.
  (openvpn.net, WhatIsOpenVPN)

OpenVPN-ohjelman asennus PfSense-palomuuriin kuvataan myöhemmin Pfsense-kappaleessa.

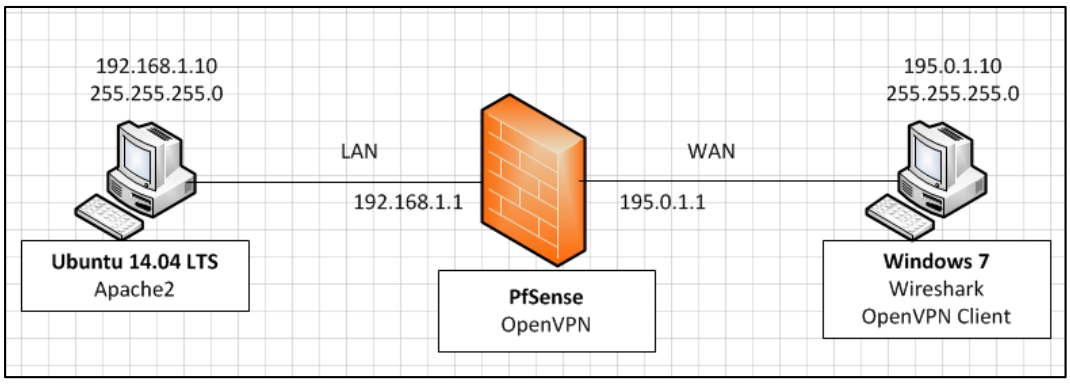
5 PFSENSE

PfSense projekti aloitettiin syyskuussa vuonna 2004. Sen aloittivat Chris Buechler ja Scott Ullrich apunaan kasvava kehitystiimi.

PfSense on ilmainen avoimen lähdekoodin ohjelma. Se on erityisesti räätälöity toimimaan palomuurina tai reitittimenä, jota voidaan kokonaisuudessaan hallita verkkokäyttöliittymän kautta. PfSense perustuu FreeBSD käyttöjärjestelmään. Lisäksi, että PfSense on voimakas ja muokkautuva palomuurin/reitittimen alusta. Se sisältää pitkän listan erilaisia ominaisuuksia. (pfsense.org/about-pfsense)

Latasin PfSense version 2.2.6-i386 osoitteesta pfsense.org/download ja asensin sen VirtualBox virtuaalikoneeseen.

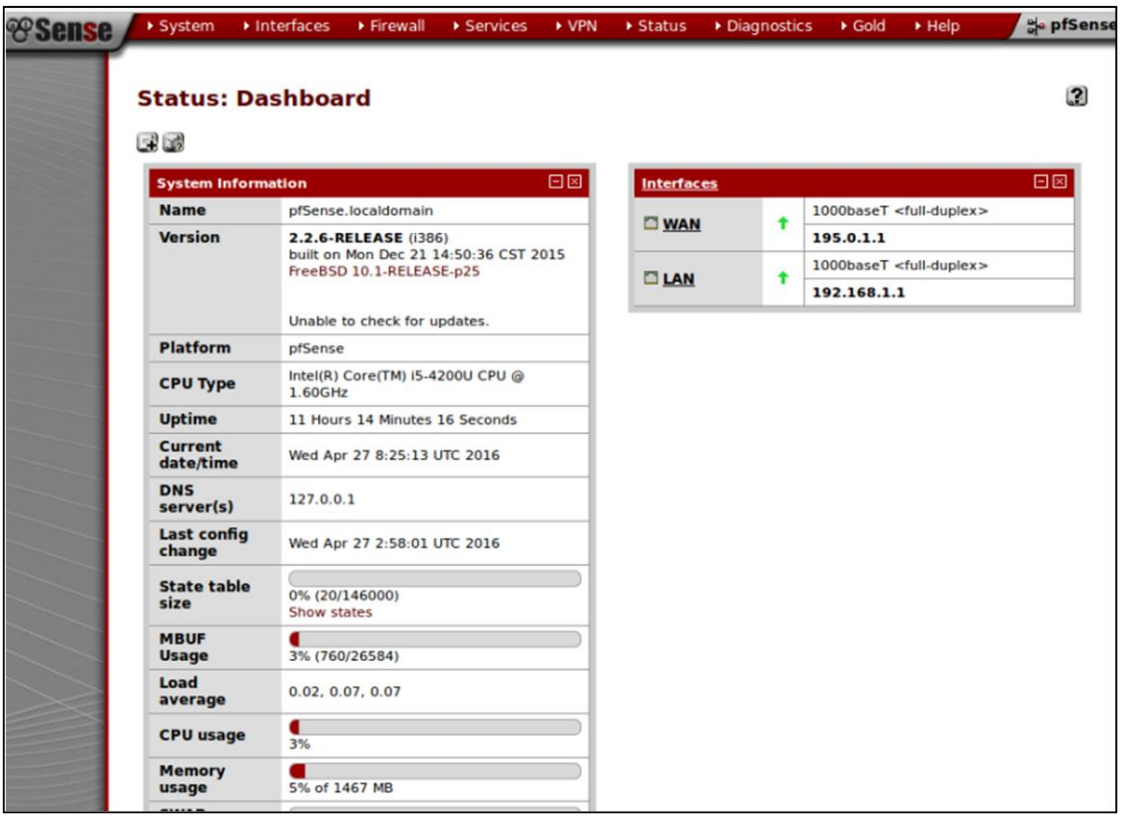
PfSenseen asetetaan Virtualboxissa kaksi verkkokorttia WAN ja LAN. Lan puolella on Ubuntu ja Wan puolella Windows.(kuvio 7.) PfSense verkkokäyttöliittymään (kuvio 9.) kirjaudutaan PfSensen LAN puolen IP-osoitteella. IP-osoite kirjoitetaan Ubuntu-koneen selaimeen, jotta päästään kirjautumaan PfSenseen.



Kuvio 7. Verkkokaavio.

PfSensen oletus käyttäjänimi on admin ja salasana on pfsense.(kuvio 8.)

Kuvio 8. PfSense kirjautuminen.



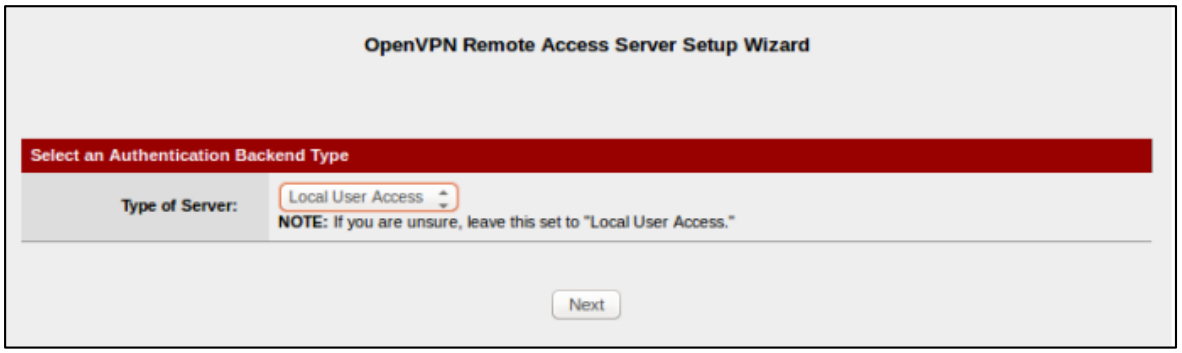
Kuvio 9. PfSense verkkokäyttöliittymän etusivu.

5.1 OpenVPN asennus

5.1.1 Authentication

Ensiksi navigoidaan PfSensen verkkokäyttöliittymässä kohtaan **VPN > OpenVPN** ja klikataan **wizard**.

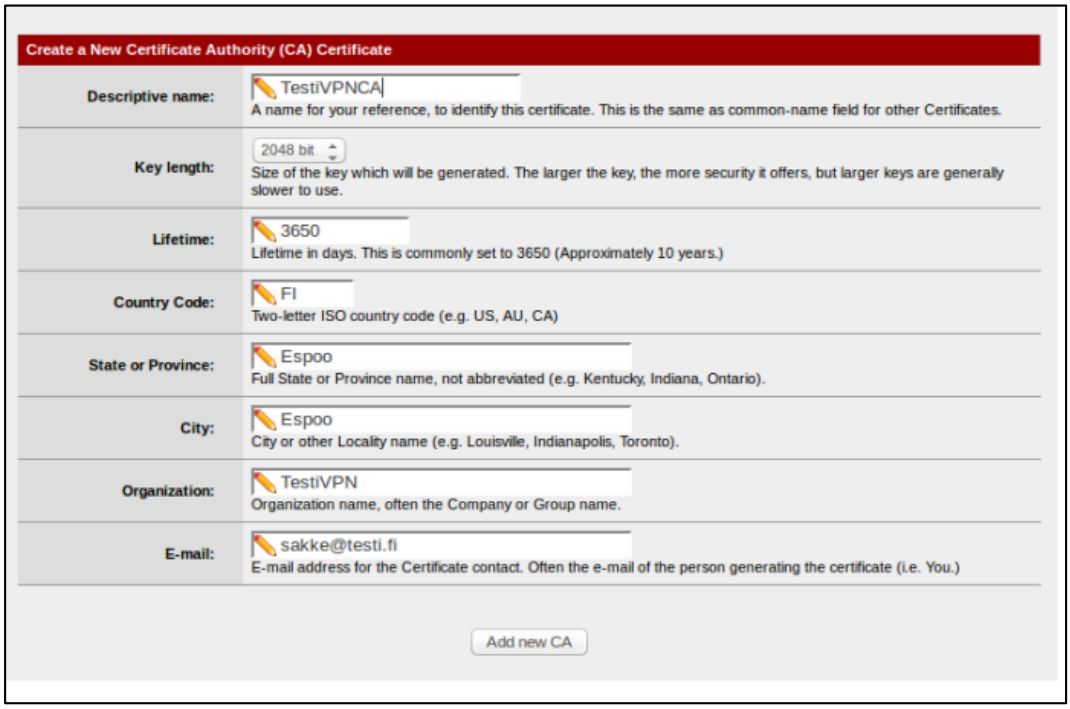
Seuraavaksi valitaan Authentication type. Valitaan **Local User Access** ja painetaan **next**.(kuvio 10.)



Kuvio 10. Authentication type.

5.1.2 Certificate Authority

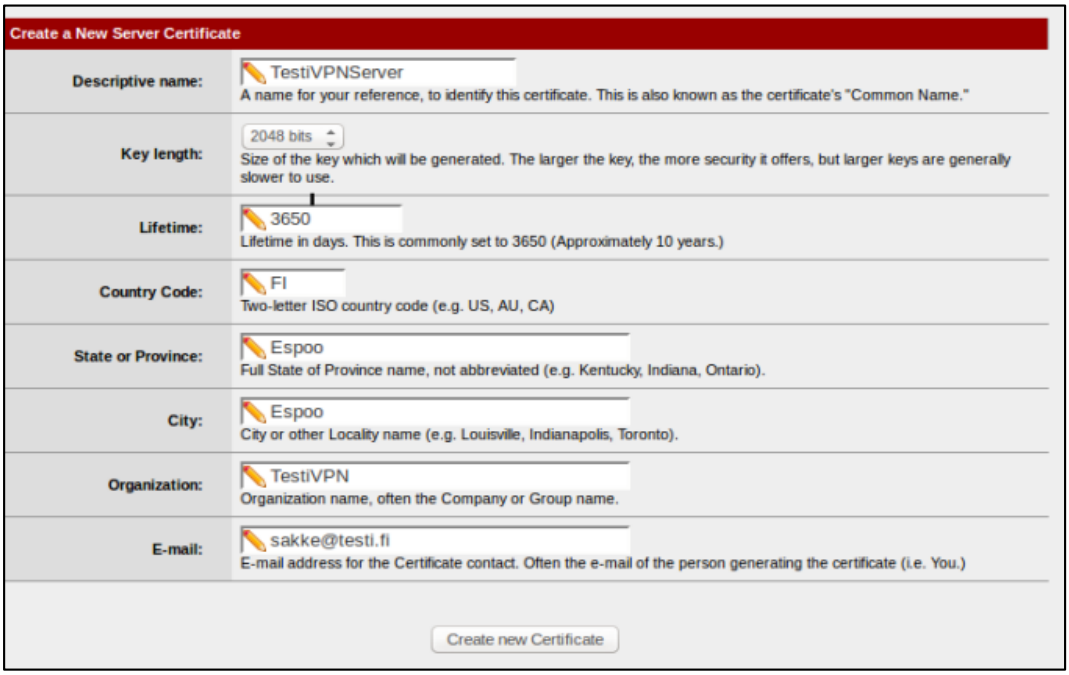
Seuraavassa vaiheessa luodaan uusi CA (Certificate Authority) eli varmennus. Tyhjät kohdat täytetään haluamilla tiedoilla. **Key length** sekä **lifetime** kohtiin voi jättää oletusarvot. Painetaan **Add new CA**.(kuvio 11.)



Kuvio 11. Uusi Certificate Authority.

5.1.3 Server Certificate

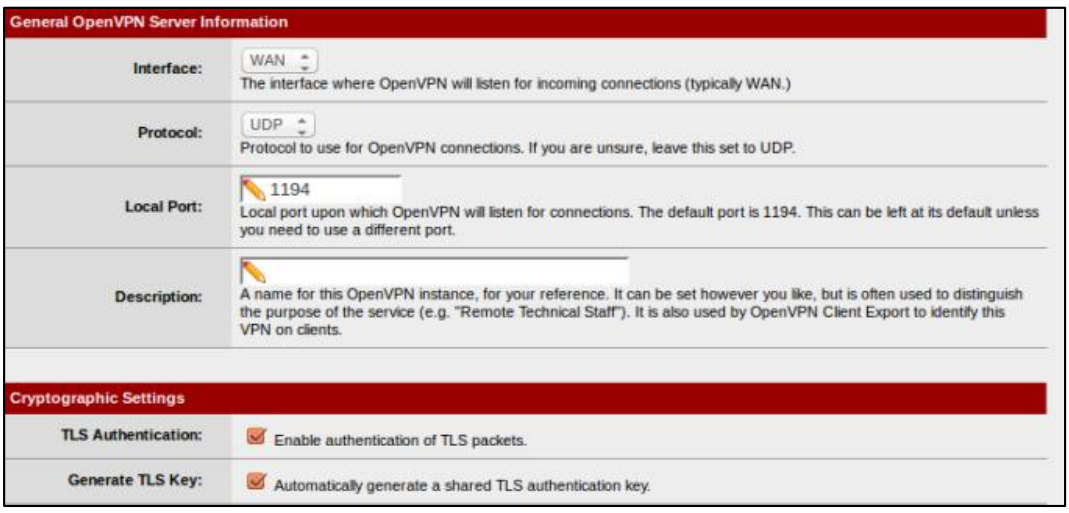
Seuraavaksi luodaan uusi **Server Certificate**. Samankaltainen ikkuna aukeaa kuin uuden CA:n luonnissa. Suurin osa kohdista on valmiiksi täytetty eikä niitä täydy vaihtaa. Vain **Descriptive name** on tyhjänä, joten täytetään se haluamalla nimellä. Klikataan **Create New Certificate**.(kuvio 12.)



Kuvio 12. Uusi Server Authority.

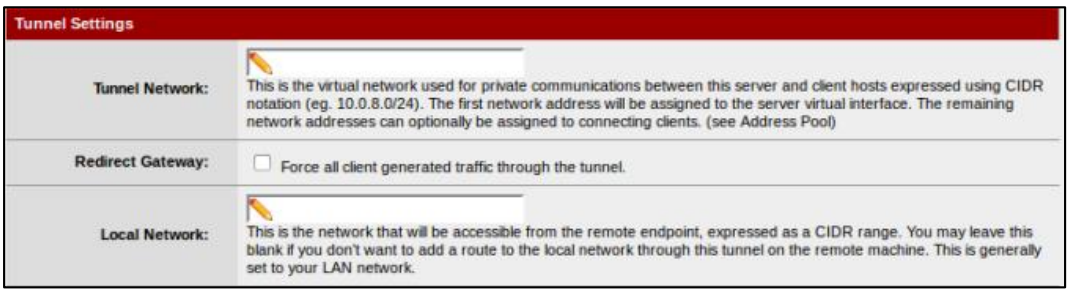
5.1.4 OpenVPN Server configuration

Seuraavaksi konfiguroidaan OpenVPN server. **TLS Authentication** ja **Generate TLS Key**-täpät jätetään.(kuvio 13.)



Kuvio 13. OpenVPN serverin konfigurointi.

Alempana asetaan **tunnel network** ja **local network** kohtiin haluamat IP-osoitteet ja painetaan **next**.(kuvio 14.) Käytin IP-osoitteita Tunnel Network: 192.168.2.0/24 ja Local Network: 192.168.1.0/24.



Kuvio 14. IP-osoitteiden lisääminen.

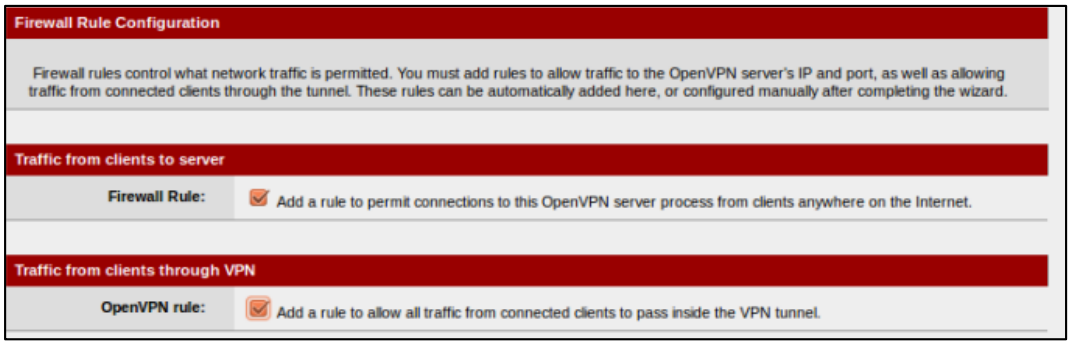
Tässä työssä käytetyt IP-osoitteet löytyvät alla olevasta taulukosta.(taulukko 1.)

Laite	IP	Mask	Gateway
Windows 7	195.0.1.10	255.255.255.0	195.0.1.1
pfSense / WAN	195.0.1.1	255.255.255.0	
pfSense / LAN	192.168.1.1	255.255.255.0	
Ubuntu 14.04 LTS	192.168.1.10	255.255.255.0	192.168.1.1

Taulukko 1. Työssä käytetyt IP-osoitteet.

5.1.5 Palomuurin säännöt

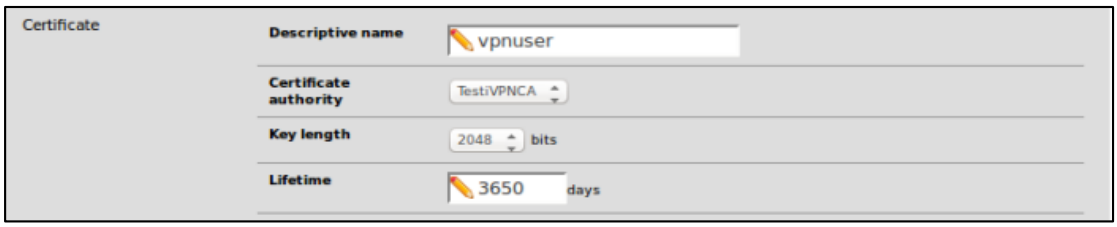
Palomuurin säännöt luodaan automaattisesti laittamalla täpät molempiin **Firewall Rule** ja **OpenVPN rule**.(kuvio 15.)



Kuvio 15. Palomuurin sääntö.

5.1.6 Käyttäjän luonti

Seuraavaksi luodaan käyttäjä. Navigoidaan **System > User Manager**. Painetaan + merkkiä oikealta **Add user**. Täytetään kohdat **Username, Password/confirmation**. Laitetaan täppä kohtaan **Click to create a user certificate**. Täytetään **Descriptive name** kohta käyttäjänimellä. **Key length-ja Lifetime** kohta menevät oletuksilla. Tallennetaan painamalla **save**.(kuvio16.)



Kuvio 16. Käyttäjän luonti.

5.1.7 OpenVPN client paketin tuonti

Seuraavaksi asennetaan OpenVPN Client export package. Tämän paketin asentamisen jälkeen voidaan ladata Windows-asennuspaketti, mikä sisältää konfiguraatiot client asennukseen.

Navigoidaan **System > Packages, Available Packages**

Etsitään listasta **OpenVPN Client export package** ja klikataan + merkkiä. Klikataan **Confim** ja paketti alkaa asentua.(kuvio 17.)

Name	Category	Version	Description
OpenVPN Client Export Utility	Security	1.3.0	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. No package info, check the forum

Kuvio 17. OpenVPN Client export package.

Konfiguraation vienti tapahtuu kohdasta **VPN > OpenVPN, Client Export** välilehti. Oletusasetukset ovat ok. Etsitään käyttäjälista lopusta ja valitaan sopiva konfiguraatiotyyppi joka halutaan asentaa Windowsille. (kuvio 18.) Valitsin x86-win6 Windows-asennuspaketin, mikä on 32-bittinen ja sopii Windows Vistalle ja sitä uudemmille Windowsille.

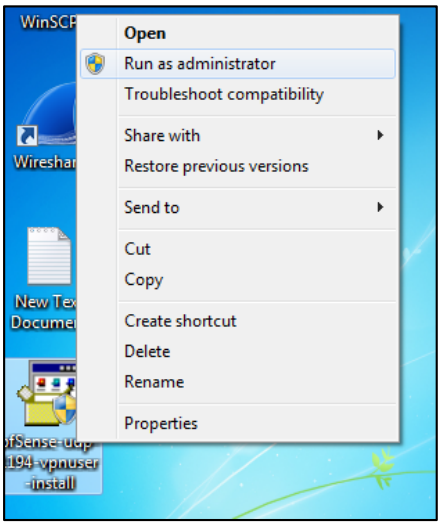
Client Install Packages

User	Certificate Name	Export
vpnuser	vpnuser	- Standard Configurations: Archive Config Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Windows Installers (2.3.8-Ix01): x86-xp x64-xp x86-win6 x64-win6 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

Kuvio 18. Windows-asennuspaketin lataus.

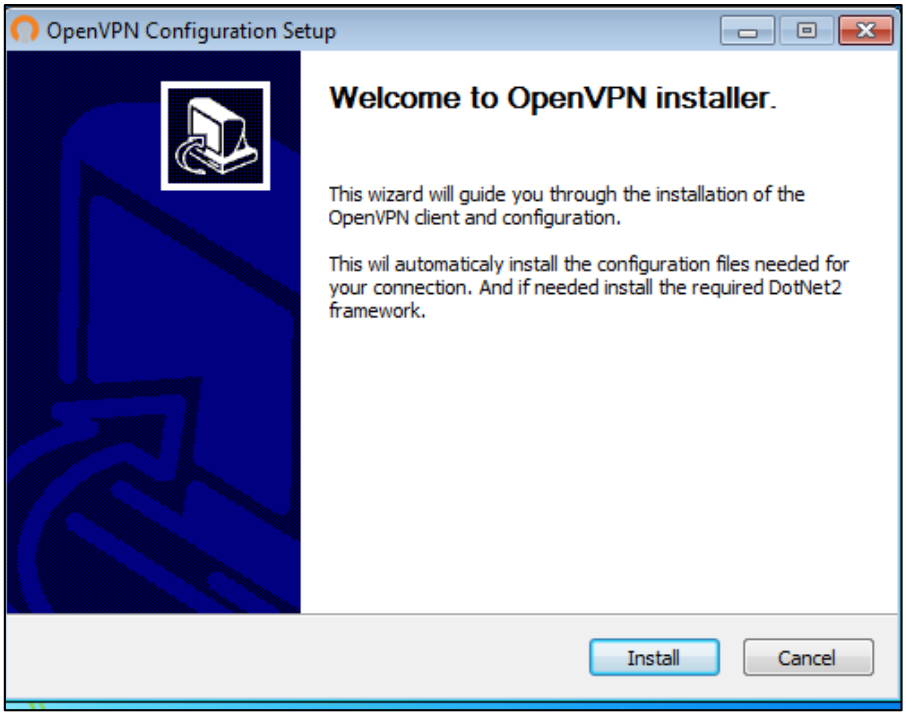
5.1.8 OpenVPN clientin asennus

OpenVPN-asennuspaketti siirretään Windows-koneelle. Suoritetaan asennuspaketti järjestelmänvalvojana. (kuvio 19.)



Kuvio 19. OpenVPN-asennuspaketti.

Aloitetaan asennus painamalla **install**.(kuvio 20.)



Kuvio 20. OpenVPN-asennus

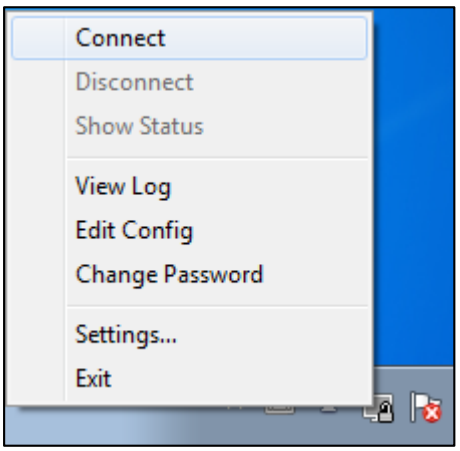
OpenVPN asennetaan painamalla oletuksilla eteenpäin. Kun asennus on valmis, painetaan **finish**.

6 OPENVPN-YHTEYDEN LUONTI

Käynnistetään OpenVPN GUI työpöydältä pikakuvakkeesta. Alapalkin oikeaan laitaan ilmestyy OpenVPN GUI kuvake. (kuvio 21.)

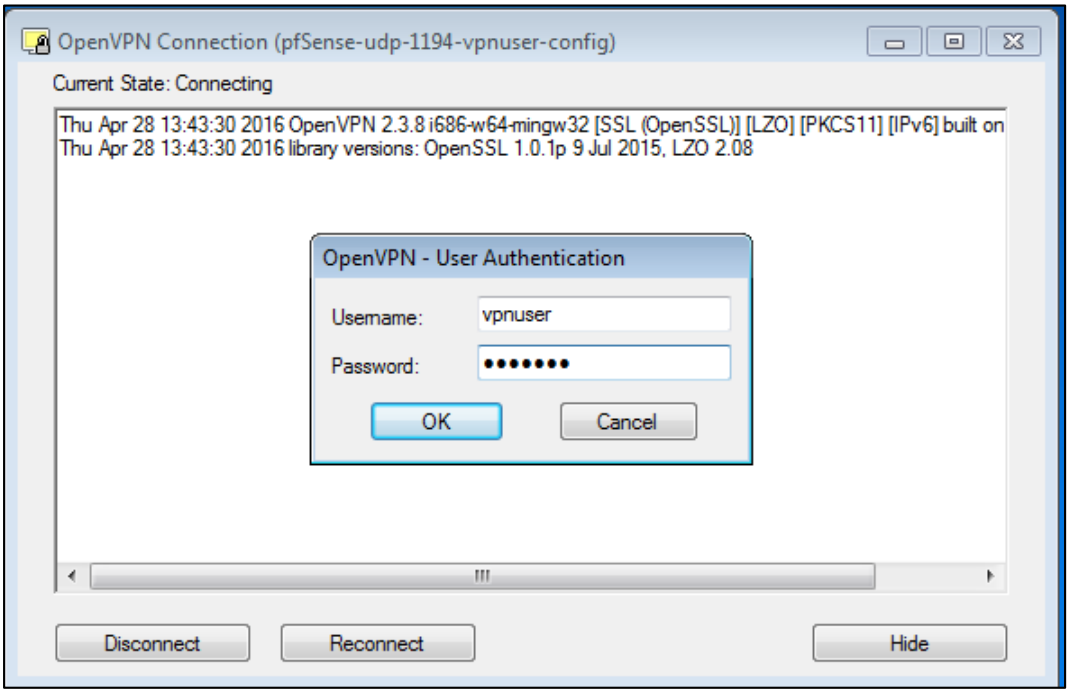
Kuvio 21. OpenVPN GUI.

Klikataan kuvaketta hiiren oikealla ja painetaan **Connect**. (kuvio 22.)



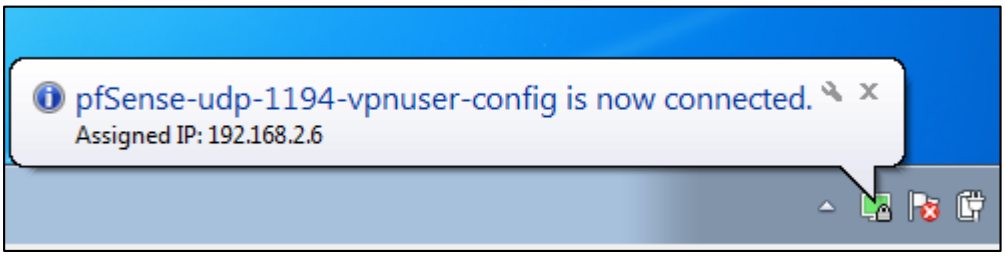
Kuvio 22. Yhteyden käynnistys.

OpenVPN – User Authentication avautuu. Kirjoitetaan **Username** ja **Password** (kuvio 23.), jotka ovat samat mitkä on asetettu aikaisemmin käyttäjää luodessa PfSense verkkokäyttöliittymällä.



Kuvio 23. OpenVPN – User Authentication.

Onnistuneesta OpenVPN-yhteyden luonnista tulee ilmoitus alareunaan. (kuvio 24.)



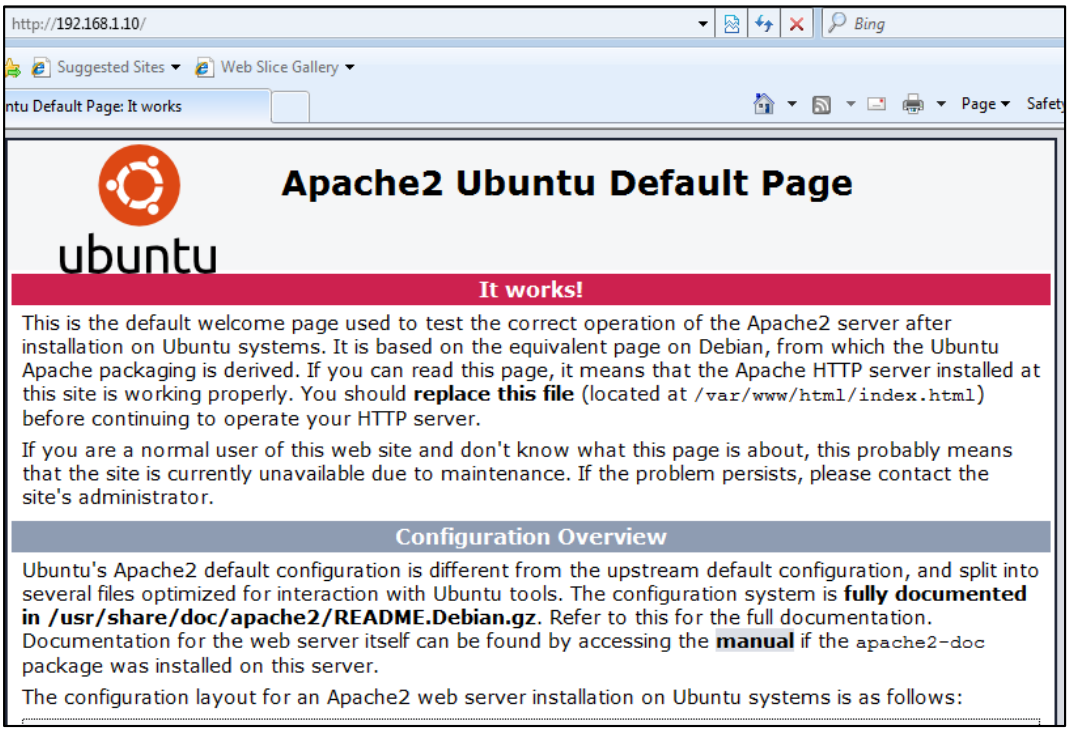
Kuvio 24. Onnistunut OpenVPN-yhteys.

6.1 OpenVPN-yhteyden testaus

Ubuntu-koneeseen asennetaan Apache2 HTTP-palvelin kirjoittamalla terminaaliin komento:

sudo apt install apache2

Testataan OpenVPN-yhteyden toimivuus kirjoittamalla Ubuntu-koneen IP-osoite Windows-koneen selaimeen. Selaimeen tulee **kuvion 25** mukainen ilmoitus yhteyden toimivuudesta.

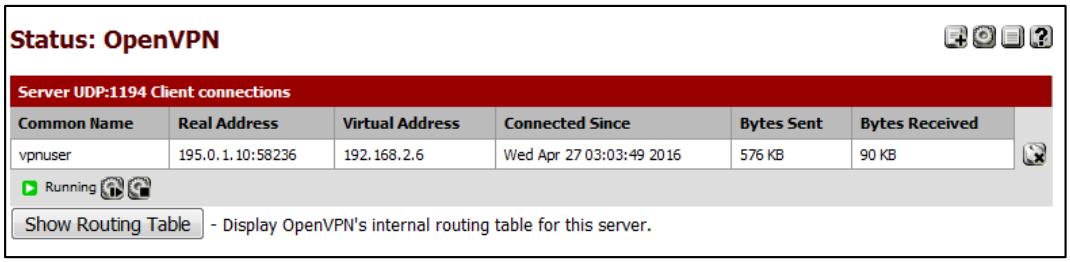


Kuvio 25. Apache2 HTTP-palvelin.

Testataan OpenVPN-yhteyden toimivuutta kirjoittamalla Windows-koneen selaimen osoiteriville PfSensen LAN puolen IP-osoite. Tällä IP-osoitteella pääsee käsiksi Ubuntu-koneella PfSensen verkkokäyttöliittymään. (kuvio 26.) Ilman luotua OpenVPN-yhteyttä Windows koneelta ei pääse PfSensen verkkokäyttöliittymään. Kun OpenVPN-yhteys on luotu, pääsee Windows koneeltakin kirjautumaan PfSensen verkkokäyttöliittymään.

Kuvio 26. PfSense kirjautuminen Windows koneelta.

PfSensen verkkokäyttöliittymästä navigoidaan **Status > OpenVPN** (kuvio 27.) ja huomataan, että vpnuser on yhteydessä virtuaalisella IP-osoitteella OpenVPN clientin kautta.



Kuvio 27. Yhteyden tarkistaminen.

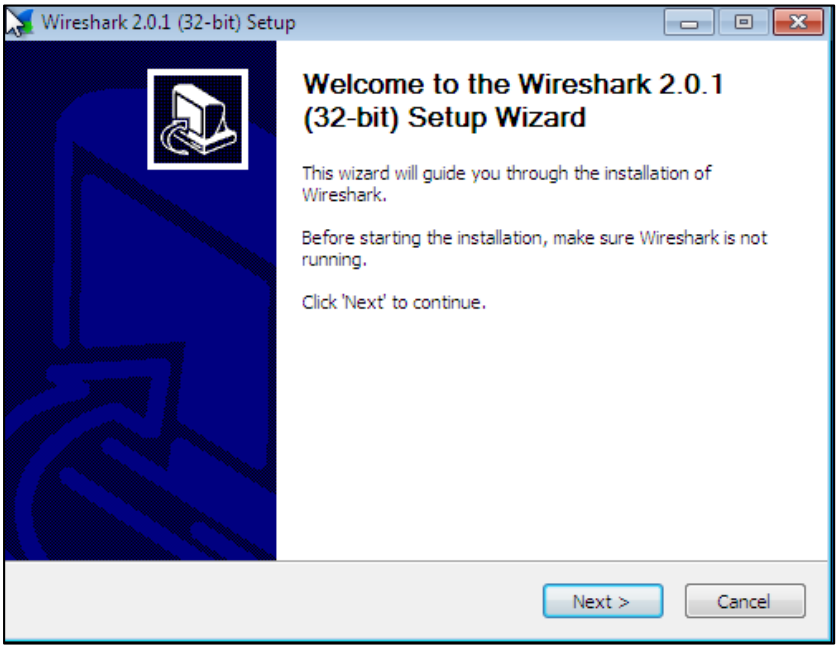
7 WIRESHARK

Wireshark on Gerald Combsin vuonna 1998 kehittämä ilmainen verkkoanalysaattori, jota käytetään verkon vianmääritykseen ja verkon analysointiin. Verkkoanalysaattori kaappaa verkon paketteja ja näyttää datan tarkasti. Wireshark on avoimeen lisenssiin (GNU General Public License) perustuva ohjelma.

Aikaisemmin Wiresharkin kaltaiset työkalut olivat kalliita tai yksinoikeudella valmistettuja. Kuitenkin kaikki muuttui kun Wireshark julkaistiin. Ennen nimenä oli Ethereal, Wiresharkiksi nimi vaihtui vuonna 2006. Vuonna 2015 julkaistiin versio 2.0, joka sisälsi uuden käyttöliittymän. Wiresharkia voi käyttää monella eri käyttöjärjestelmällä kuten Windows, Linux ja OS X. (wireshark.org, ABOUT)

Wireshark-ohjelman lataus osoitteesta wireshark.org/download. Latasin 32-bittisen Windows version 2.0.1.

Wireshark asennetaan painamalla oletuksilla eteenpäin. (kuvio 28.)



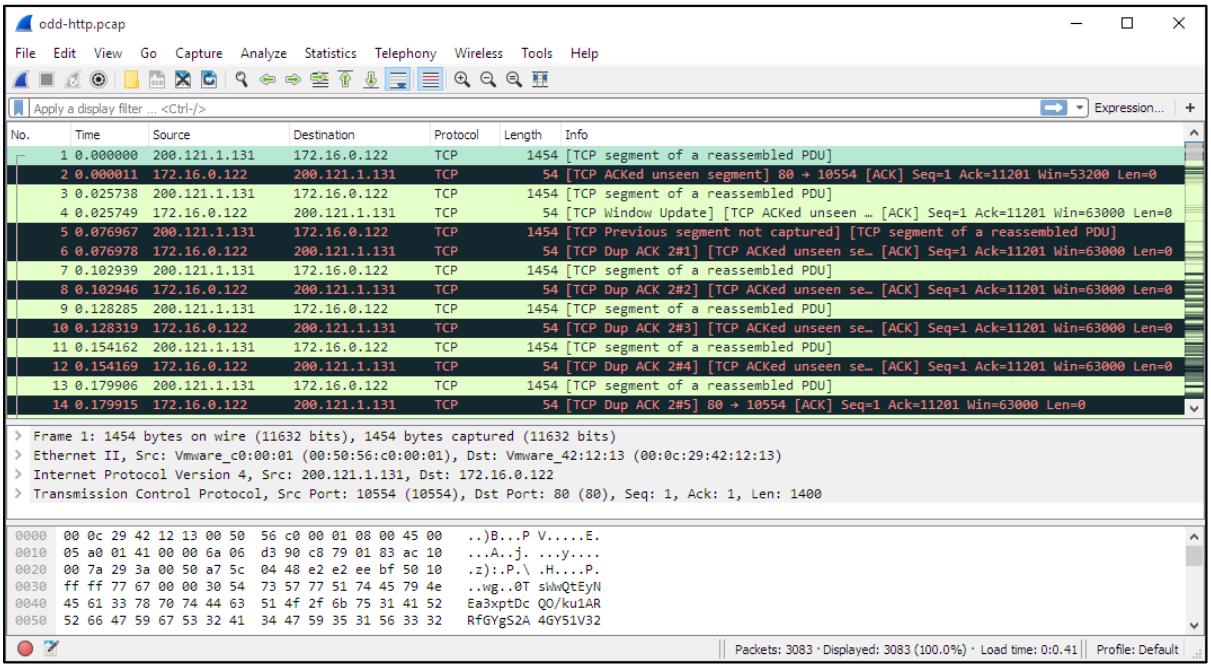
Kuvio 28. Wireshark-asennus.

7.1 Ominaisuudet

Wiresharkissa on paljon ominaisuuksia. Seuraavassa muutamia näistä ominaisuuksista.

- Perusteellinen tarkastus sadoille protokollille.
- Suora pakettidatan kaappaus ja offline analyysit.
- Monta alustaa se toimii mm. Windows, Linux, OS X, Solaris, FreeBSD, NetBSD ja monilla muilla käyttöjärjestelmillä.
- Näyttää pakettien protokollatietoja hyvin yksityiskohtaisesti.
- Pakettien haku ja suodatus monilla kriteereillä.

(wireshark.org/docs)



Kuvio 29. Esimerkki kaapatusta datasta Wiresharkilla. (blog.wireshark.org)

7.2 Käyttötarkoituksia

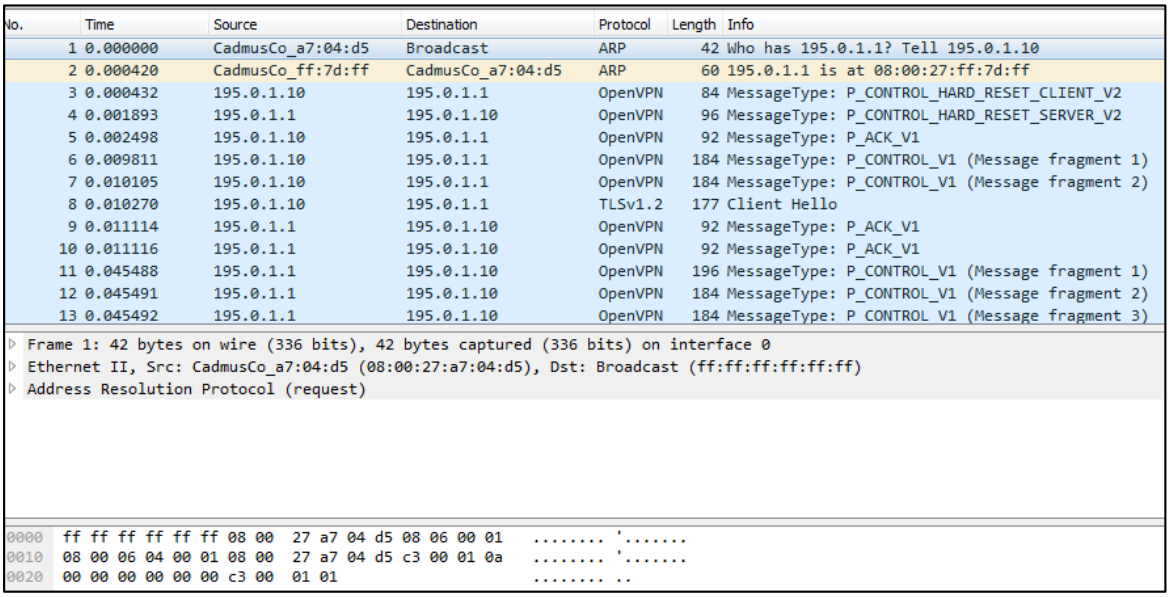
Tässä muutamia esimerkkejä mihin ihmiset käyttävät Wiresharkia:

- Verkon järjestelmänvalvojat käyttävät sitä verkon vianmääritykseen.
- Verkon turvallisuusvastaavat tarkastelevat sillä verkon turvallisuusongelmia.
- Suunnittelijat korjaavat virheitä protokollatoteutuksissa.

(wireshark.org/dogs)

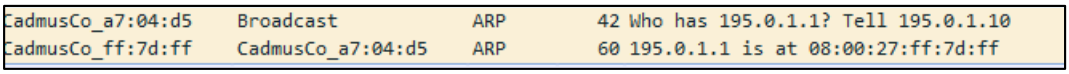
7.3 OpenVPN-yhteyden tarkastelu

Laitoin wireshark-ohjelman päälle kun muodostin OpenVPN-yhteyden Windows-koneesta Ubuntu-koneeseen. Wireshark keräsi paljon dataa yhteyden muodostamisesta. Kuviossa 30 näkyy kuinka ensiksi lähtee ARP- (Address Resolution Protocol) kysely, kenellä on IP-osoite 195.0.1.1 ja kerro 195.0.1.10 IP:lle.



Kuvio 30. Kaapattua dataa OpenVPN-yhteydestä.

ARP kysely (kuvio 31.), johon se liittää haluamansa IP-osoitteen lähtee jokaiselle verkossa olevalle koneelle. Se jolla on kyseinen IP-osoite lähettää ARP-vastausviestin, jossa on oma MAC-osoite. (Beal, Webopedia)



Kuvio 31. ARP kysely.

Wiresharkilla pystyy kaappaamaan suojattoman yhteyden käyttäjätunnuksia ja salasanoja. OpenVPN-yhteys on salattu, joten datasta ei löytynyt yhteydessä käytettyjä salasanoja eikä käyttäjätunnuksia.

8 YHTEENVETO

Tässä opinnäytetyössä oli tavoitteena vastata kysymyksiin

- Mitä on VPN-tekniikka ja mihin sitä käytetään?
- Kuinka OpenVPN-ohjelma asennetaan ja kuinka sitä käytetään?

Mielestäni työssä tulee selville mitä VPN-tekniikka on. Lukija saa käsityksen mitä sillä tehdään.

OpenVPN-ohjelman käytännön asennus onnistui hyvin muutamista ongelmista huolimatta. Onnistuin kuvaamaan asennuksen vaihe vaiheelta havainnollistavien kuvien kera. Ohjeitteni avulla käyttäjä pystyisi asentamaan OpenVPN-ohjelmiston PfSense palomuuriin.

Tavoitteena oli myös suorittaa OpenVPN-yhteyden testauksia. Ensin testattiin pääsy Windows koneelta PfSensen verkkokäyttöliittymään ja sitten yhteys Apache palvelimeen. Testaukset onnistuivat hyvin ja yhteys toimi haluamallani tavalla. Yhteys muodostui Windows koneelta läpi PfSense palomuurin Ubuntu koneelle.

Työn teoriaosuuden kirjoittaminen onnistui paremmin kuin mitä olin ajatellut ennen työn aloittamista. Lähteitä löytyi melko hyvin, enemmän englanniksi kuin suomeksi. Englanninkielisistä lähteistä oli haastavampaa tuottaa tekstiä kuin suomenkielisistä. Jotkut lähteet olivat vähän vanhempia kuin toiset mutta tiedot pitivät paikkaansa vanhemmissakin.

Virtualbox oli selvä valinta virtuaalikoneeksi tähän työhön, sillä minulla oli siitä aiempaa kokemusta. Oli helpompi lähteä työstämään tätä projektia kun ei tarvinnut käyttää aikaa uuden virtuaalikoneen käytön opetteluun.

Olen tyytyväinen opinnäytetyön lopputulokseen, sillä onnistuin hyvin tavoitteissani.

LÄHTEET

Beal, V. ARP - Address Resolution Protocol. Viitattu 16.5.2016. http://www.webopedia.com/TERM/A/ARP.html

Beal, V. 2015. The 7 Layers of the OSI Model. Viitattu 16.5.2016. http://www.webopedia.com/quick_ref/OSI_Layers.asp

Crist, E. F., Just Keijser, J. 2015. Mastering OpenVPN. Birmingham. Packt Publishing Ltd.

Gupta, M. 2012. Building a Virtual Private Network, Course Technology / Cengage Learning. Ohio.

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

Held, G. 2005. Virtual Private Networking : A Construction, Operation and Utilization Guide. England. John Wiley & Sons Ltd.

Hoffmann, C. 2013. HTG Explains: What is a VPN? (And Why You Might Want to Use One). Viitattu 19.5.2016. http://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

Howath, F. 2008. Evolution of the internet protocol virtual private network. Viitattu 5.2.2016. http://www.computerweekly.com/feature/Evolution-of-the-internet-protocol-virtual-private-network

Kaario, K. 2002. TCP/IP verkot. Porvoo. WS Bookwell.

OpenVPN, About Us. 6.2.2016. https://openvpn.net/index.php/about-menu/about-us.html

OpenVPN, HOWTO. Viitattu 3.2.2016. https://openvpn.net/index.php/open-source/documentation/howto.html

OpenVPN, Overview. Viitattu 17.5.2016 https://openvpn.net/index.php/open-source/245-community-open-source-software-overview.html

OpenVPN, What Is OpenVPN, Viitattu 10.4.2016. https://openvpn.net/index.php/open-source/333-what-is-openvpn.html

PFSENSE. Pfsense overview. Viitattu 22.4.2016. https://www.pfsense.org/about-pfsense/

Rao, U. H., Nayak, U. 2014. The InfoSec Handbook. US. Apress.

Ruohonen, M. Tietoturva Peruskirja. Porvoo. WS Bookwell.

WIRESHARK ABOUT, Viitattu 15.3.2016. https://www.wireshark.org/

WIRESHARK. Viitattu 20.2.2016. https://blog.wireshark.org/

WIRESHARK. Viitattu 20.2.2016.
https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html

WIRESHARK. Viitattu 20.2.2016.
https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#
ChIntroWhatIs