SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

VPN-YHTEYDEN TOTEUTUS-TAVAT

TEKIJÄ/T: Kim Ruuskanen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Kim Ruuskanen	
Työn nimi VPN-yhteyden toteutustavat	
Päiväys 27.5.2015	Sivumäärä/Liitteet 30/0
Ohjaaja(t) lehtori Veijo Pitkänen / Savonia-ammattikorkeakoulu	
Toimeksiantaja/Yhteistyökumppani(t) Pieksämäen kaupunki / tietohallinto / IT-pääsuunnittelija Tommi Tikkanen	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia VPN-tunnelin eri toteutustapoja. Työssä valittiin yksi toteutustapa, jonka pohjalta suunniteltiin VPN-tunnelin esimerkkiratkaisu. Valittavassa toteutustavassa tuli ottaa huomioon tietoturva sekä jo olemassa olevat laitteet.

Opinnäytetyön ensimmäisessä vaiheessa käytiin läpi eri tunnelointiprotokollia sekä salausprotokollia. Näistä tuotiin esille perusasiat, esiteltiin tunnelointiprotokollien rakennekuvat sekä millä tavalla ne toimivat. Toisessa vaiheessa käsiteltiin VPN-yhteyden vaatimia rooleja sekä tietoturvaa. Viimeisenä tässä opinnäytetyössä vertailtiin eri toteutustapoja ja suunniteltiin niiden pohjalta yksi toteutusmalli joka voidaan jatkossa toteuttaa.

Esimerkkisuunnitelmassa valittiin käytettäväksi Ciscon ASA-5505 – palomuuria, johtuen sen helppokäyttöisyydestä sekä laitteen hyvästä skaalautuvuudesta muutosten edessä. Yhtenä perustana valintaa tehdessä oli myös se, että työn tilaajalla oli ennestään olemassa Ciscon ASA-5505 – palomuureja.

Tämän opinnäytetyön tuloksien avulla Pieksämäen kaupungin tietohallinto pystyy toteuttamaan VPN-yhteyden tarvitsemiinsa kohteisiin.

Avainsanat
VPN, protokolla, tietoturva, Cisco

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Kim Ruuskanen			
Title of Thesis Methods of Implementing VPN Connection			
Date	27 May 2015	Pages/Appendices	30/0
Supervisor(s) Mr. Veijo Pitkänen, Principal Lecturer/ Savonia University of Applied Sciences			
Client Organisation /Partners Pieksämäki city / Information Management / Mr. Tommi Tikkanen, It-Lead Designer			

Abstract

The purpose of this thesis was to examine the different methods of implementing a VPN connection. One implemtation method was chosen, based on which an example VPN tunnel solution was designed. On the chosen implementation method, security and already existing devices needed to be taken into consideration.

The work was started by acquiring the literature and web-based materials required for the work. Next the different tunneling protocols and encryption protocols were studied. Then the roles and the security measures needed for the VPN connection were presented. Lastly, the different implementing methods were compared, and based on the comparison one implementation model was designed which could be implemented later on.

In the implementation model of this thesis, a Cisco ASA-5505 series firewall was used because of its user-friendly interface and scalability and because the commissioner of the thesis already has those devices.

As a result of the thesis, the information management of the city of Pieksämäki will be able to implement a VPN connection to the locations where needed.

Keywords
VPN, protocol, security, Cisco

SISÄLTÖ

LYHENTEET JA TERMIT 6
1 JOHDANTO 8
2 VIRTUAL PRIVATE NETWORK 9
2.1 Toimintaperiaate 9
2.2 Edut ja haitat 9
3 VPN-TUNNELOINTIPROTOKOLLAT 10
3.1 Point to Point Tunneling Protocol 10
3.2 Layer 2 Tunneling Protocol 10
3.3 Secure Socekt Tunneling Protocol 11
3.4 Generic Routing Protocol 11
3.5 IP Security 12
3.5.1 Kuljetusmoodi 14
3.5.2 Tunnelimoodi 14
3.5.3 IPSec-yhdyskäytävä 14
4 SALAUSPROTOKOLLAT 15
4.1 Secure Sockets Layer 15
4.2 Secure Sockets Layer Virtual Private Network 15
4.3 Secure Shell 16
4.3.1 Secure Shell siirtokerroksessa 16
4.3.2 Secure Shell käyttäjätunnistuskerroksessa 16
4.3.3 Secure Shell yhteyskerroksessa 17
5 VPN-YHTEYDEN ROOLIT 18
5.1 Active Directory Certificate Services 18
5.2 Dynamic Host Configuration Protocol 18
5.3 Domain Name System 18
6 TIETOTURVA 19
7 TOTEUTUSTAVAT 20
7.1 Ohjelmapohjainen ratkaisu 20
7.1.1 OpenVPN 20
7.1.2 AnyConnect VPN 21
7.2 Laitepohjainen ratkaisu 21

7.2.1 Linux VPN -palvelin 21
7.2.2 Cisco ASA 5505-Firewall 22
8 VALITTU TOTEUTUSTAPA 23
8.1 VPN-tunnelin toteutus Cisco ASA-5505 -palomuurilla 23
9 YHTEENVETO 28
LÄHTEET JA TUOTETUT AINEISTOT 29

LYHENTEET JA TERMIT

AD	*Active Directory.* Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu
AD CS	*Active Directory Certificate Services.* Tunnistus sekä pääsyn valvonta jolla luodaan sekä hallitaan julkisia avaimia.
AES	*Advanced Encryption Standard.* Lohkosalausmenetelmä, jota käytetään tietotekniikassa.
AH	*Authentication Header.* Toinen IPsecin suojausprotokollista, joka autentikoi datan.
ASA	*Adaptive Security Appliance.* Ciscon suunnittelema tietoturvalaite.
DH	*Diffie-Hellman.* Avainten vaihto algoritmi.
DES	*Data Encryption Standard.* Salausmenetelmä, jota on käytetty laajasti ympäri maailmaa.
3DES	*Triple Data Encryption Standard.* Yleisimmin käytetty DES-salauksen muoto.
DHCP	*Dynamic Host Configuration Services.* IP-osoitteiden jakoon tarkoitettu protokolla.
DNS	*Domain Name System.* Nimipalvelu, joka muuntaa verkko-osoitteita IP-osoitteiksi.
EAP	*Extensible Authentication Protocol*. Käyttäjien tunnistusprotokolla.
ESP	*Encapsulation Security Payload.* Toinen IPsecin suojausprotokollista, joka salaa datan ja autentikoi sen.
FTP	*File Transport Protocol.* Tiedonsiirtomenetelmä, jonka avulla voidaan siirtää tietoja kahden tietokoneen välillä.
GRE	*Generic Routing Encapsulation.* Ciscon kehittämä tunnelointiprotokolla.
HTTP	*Hypertext Transfer Protocol.* Hypertekstin siirtoprotokolla.
HTTPS	*Hypertext Transfer Protocol Secure.* Suojattu Hypertekstin siirtoprotokolla.
IKE	*Internet Key Exchange.* Internet salausavaimien jakeluun tarkoitettu protokolla.
IPSec	*IP Security Architecture.* Laajennettu IP-protokolla, jonka avulla todennetaan ja salataan jokainen IP-paketti istunnon aikana.
L2TP	*Layer 2 Tunneling Protocol.* Microsoftin ja Ciscon kehittämä VPN-tunnelointiprotokolla.
MD5	*Message-Digest.* Tuottaa tuloksenaan 128-bittisen tiivisteen, joka tyypillisesti esitetään 32-merkkisenä heksakoodatussa muodossa
MPPE	*Microsoft Point-to-Point Encryption.* VPN-yhteyksissä käytettävä tiedonsalausmenetelmä.
MS-CHAP	*Microsoft Challenge Handshake Authentication Protocol.* Salasanasuojattu todennusprotokolla.
OSI	*Open System Interconnection Reference Model.* Tiedonsiirtoprotokollien yhdistelmä.
PPP	*Point-to-Point Protocol.* Digitaalisessa tiedonsiirrossa käytetty protokolla

PPTP	*Point-to-Point Tunneling Protocol.* VPN-tunnelointiprotokolla, joka pohjautuu PPP-protokollaan.
PSK	*Pre-Shared Key.* Etukäteen jaettu salausavain, jonka avulla osapuolet todennetaan.
RSA	*Rivest, Shamir & adleman.* Digitaalisissa allekirjoituksissa ja salaisten avainten salauksessa käytetty algoritmi.
SHA	*Secure Hash Algorithm.* MD5 ns. korvaaja, jonka tuottama tiiviste on 160 bittiä pitkä.
SSH	*Secure Shell.* Etäyhteyden tietoliikenteen salaamiseen tarkoitettu protokolla.
SSL	*Secure Sockets Layer.* Internet-sovellusten tietoliikenteen salaamiseen tarkoitettu protokolla.
SSL VPN	*Secure Sockets Layer Virtual Private Network.* Tekniikka, jossa otetaan VPN-yhteys SSL-yhteyden yli suljettuun verkkoon etätyöasemalta tai yhdistetään kaksi suljettua verkkoa keskenään
SSTP	*Secure Socket Tunneling Protocol.* VPN-tunnelointiprotokolla jossa verkkoliikenteen salaukseen on käytetty SSL-salausta.
TLS	*Transport Layer Security.* salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli
VPN	*Virtual Private Network.* Virtuaalinen erillisverkko, yhdistetään useampia verkkoja julkisen verkon yli.

1 JOHDANTO

Opinnäytetyö tehdään toimeksiantona, joka on saatu Pieksämäen kaupungin tietohallinnon IT-pääsuunnittelija Tommi Tikkaselta syksyllä 2014. Opinnäytetyön tavoitteena on tutkia eri toteutustapoja VPN-tunnelin luomiselle.

Työssä tutkitaan, kuinka VPN-yhteys voidaan rakentaa sekä, mitä laitehankintoja tarvitaan vai voiko yhteyden toteuttaa ainakin osittain ohjelmallisesti. Lisäksi käsitellään VPN-yhteyttä myös yleisellä tasolla sekä tehdään Pieksämäen kaupungille esimerkkisuunnitelma, jonka mukaan VPN-tunneli voidaan toteuttaa.

Pääasiallinen tavoite on tutkia eri toteutustapoja VPN-yhteydellä sekä tehdä esimerkkisuunnitelma Pieksämäen kaupungille VPN-tunnelin rakentamisesta. Suunnitelman avulla Pieksämäen kaupunki voi myöhemmin rakentaa VPN-tunnelin Pieksämäen kyliltä kaupunkiin. VPN-tunnelin avulla verkon hallittavuus, valvonta ja etäyhteydet parantuvat eikä tietoliikenne pääse harhautumaan. Kokonaisuutena VPN-tunneli tuo Pieksämäen kaupungin ja sen kylien väliseen tietoliikenneyhteyteen lisää tietoturvaa sekä yksinkertaistaa verkkoarkkitehtuuria. Pieksämäen kaupungille suunnitellaan yhteys jossa on parhain tietoturvaratkaisu. Kuvassa 1 nähdään maantieteellinen aluekuvaus kohteesta, johon esimerkkiratkaisu suunnitellaan.

KUVA 1. Esimerkki suunnitelman maantieteellinen aluekuvaus (Ruuskanen 2015-14-4.)

2 VIRTUAL PRIVATE NETWORK

Lyhenne VPN tulee sanoista Virtual Private Network eli virtuaalinen yksityisverkko. VPN-yhteys on keino, jolla voidaan muodostaa suojattu yhteys kahden suljetun verkon välille julkisen verkon yli. VPN-yhteys on aina salattu ja yleisin käytetty salausmenetelmä on SSL (Secure Socekts Layer). Salauksena voidaan käyttää myös SSH:ta (Secure Shell), mutta se ei ole tietoturvan kannalta yhtä hyvä ratkaisu kuin SSL-salausmenetelmä. Nykysin salauksena käytetään paljon myös IPsec:iä.

2.1 Toimintaperiaate

Yleisimmin VPN-yhteyksiä luodaan eri toimipaikkojen reitittimien välille. Kun yhteys luodaan reitittimien välille, ei työasemille tarvitse asentaa ja määritellä erillisiä VPN-asiakasohjelmistoja. Etuna tässä on myös se, että työntekijältä ei vaadita toimenpiteitä muodostaakseen VPN-yhteyden. VPN-yhteyksiä voidaan rakentaa myös Point-To-Point-tyyppisesti, jolloin käyttäjän on itse muodostettava VPN-yhteys.

VPN-tunneli mahdollistaa intra-osoitteita käyttävien laitteiden liikennöinnin Internetin läpi ilman suojausta. Vaikka liikennettä ei ole suojattu, on tunnelissa kulkeva data turvassa, koska VPN-yhteydet käyttävät vahvaa salausta ja käyttäjien tunnistusta. (Hakala ja Vainio 2005, 382.)

Perusajatuksena VPN-yhteydessä on siis tiedonsiirron ja sen sisältämän datan yksityisyys. Yksityisyyden saavuttamiseen vaaditaan, että tieto salataan ulkopuolisilta ja varmistutaan tiedon aitoudesta. Tämä saavutetaan tunnelointiprotokollia hyödyntäen. Tunnelointiprotokollia käsitellään tarkemmin luvussa 3.

VPN-tunneli luo julkisen verkon sisälle eristetyn tunnelin, jonka sisällä kulkeva liikenne on suojattu ulkopuolisilta (2kmediat 2014). Useimmiten VPN-tunneliin ohjataan vain etälaitteen ja yrityksen sisäverkon välinen liikenne; muu liikenne ohjataan suoraan ulos VPN-tunnelin ohi.

2.2 Edut ja haitat

VPN-yhteyden etuja ovat tiedon saatavuus paikasta riippumatta sekä se, että VPN on hyvin skaalautuva muutosten edessä. VPN-yhteyden avulla saadaan helposti myös salattua arkaluontoisia asioita julkiselta liikenteeltä.

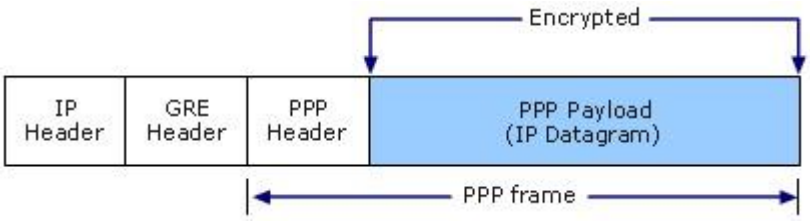
VPN-yhteyksien rakentaminen vaati kuitenkin asiantuntemusta ja VPN-tunnelin suorituskyky riippuu täysin julkisen verkon suorituskyvystä. VPN-yhteyden suorituskyky ei siis ole lainkaan käyttäjän tai ylläpitäjän hallittavissa. VPN vaatii myös syvällistä asiantuntemusta tietoliikenteen tietoturvasta.

3 VPN-TUNNELOINTIPROTOKOLLAT

VPN-tunneli voidaan rakentaa käyttämällä eri tunnelointiprotokollia. Käytettävä tunnelointiprotokolla valitaan sen mukaan, minkälaiseen käyttöön VPN-tunneli tulee sekä käytettävistä laitteista, eli palvelimista, palomuureista tai reitittimistä. Yleisimpinä käytössä olevia protokollia ovat L2TP ja GRE ja kaikista yleisin on IPsec. Näiden yhdistelmistä yleisin käytössä oleva on GRE – IPsec yhdistelmä. Tässä luvussa esitellään näiden lisäksi myös PPTP ja SSTP -protokollat.

3.1 Point to Point Tunneling Protocol

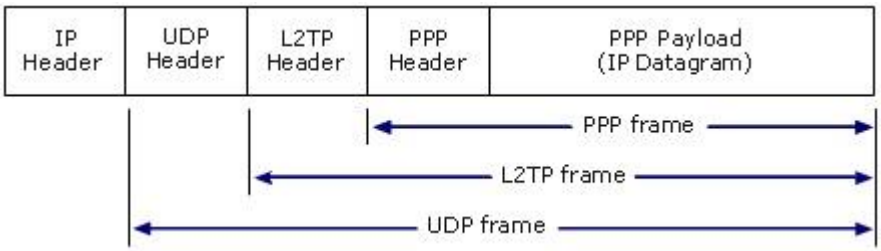
Point to Point Tunneling Protocol (PPTP) periaatteena on, että se kapseloi PPP-kehykset IP-datagrammeiksi. Tämän avulla PPP-kehykset voidaan lähettää verkon yli. PPTP-protokolla käyttää TCP- ja GRE-protokollia. TCP-protokollaa käytetään tunnelin hallinnoimiseen ja GRE-protokollan laajennettua versiota PPP-paketin kuljetukseen verkossa. PPTP-tekniikka soveltuu käytettäväksi sekä yksittäisten käyttäjien että reitittimien välisiin yhteyksiin. (Microsoft Corporation 2014.)



KUVA 2. PPTP-paketin rakenne (Microsoft Corporation 2012.)

3.2 Layer 2 Tunneling Protocol

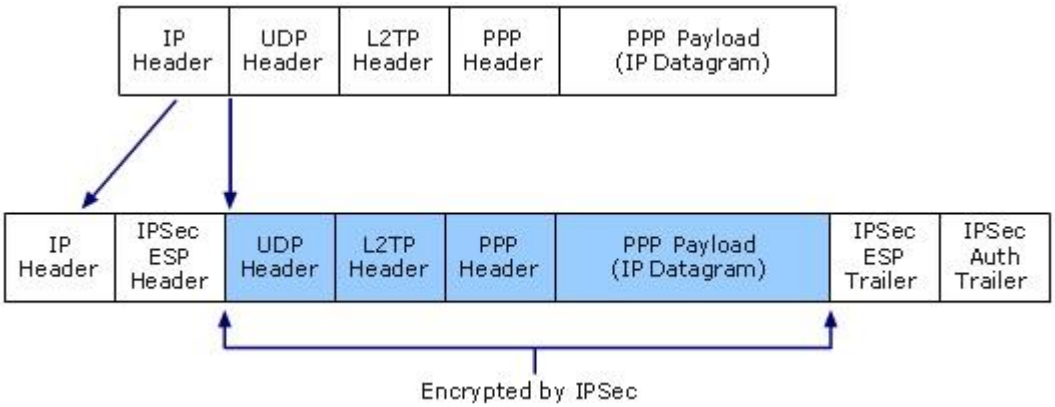
Layer 2 Tunneling Protocol (L2TP) sopii kaikkiin OSI-mallin 2. kerroksella eli siirtokehyskerroksella toimivien yhteyksien hyödyntämiseen, mutta L2TP:n rakenne on paljon monimutkaisempi kuin PPTP-protokollan. Yleisimmin L2TP:tä käytetään PPP-kehysten siirtämiseen internetissä. Salauksena L2TP.ssä käytetään IPSec:ä.



KUVA 3. L2TP-paketin rakenne (Microsoft Corporation 2012.)

L2TP-protokollassa alkuperäiseen PPP-kehykseen lisätään L2TP-otsake ja lisäksi vielä UDP-otsake. Jotta paketista saataisiin salattu, salataan se vielä IPSec:llä lisäämällä pakettiin IPSec Encapsulation Security Payload -otsakkeet sekä IPSec Authentication trailer. Alkuun sijoitetaan salaamaton IPSec ESP header ja loppuun salattu IPSec ESP trailer. Lopuksi kun paketti on koottu ja salattu, sijoitetaan

salattu paketti vielä IP-datagrammin sisään. Kuvassa 4 on kuvattu, miten IPSec-salausmenetelmä vaikuttaa L2TP-paketin rakenteeseen. (Hakala, Vainio ja Vuorinen 2006, 287.)



KUVA 4. L2TP-paketin rakenne kun se on salattu käyttäen IPSec-salausta (Microsoft Corporation 2012.)

3.3 Secure Socekt Tunneling Protocol

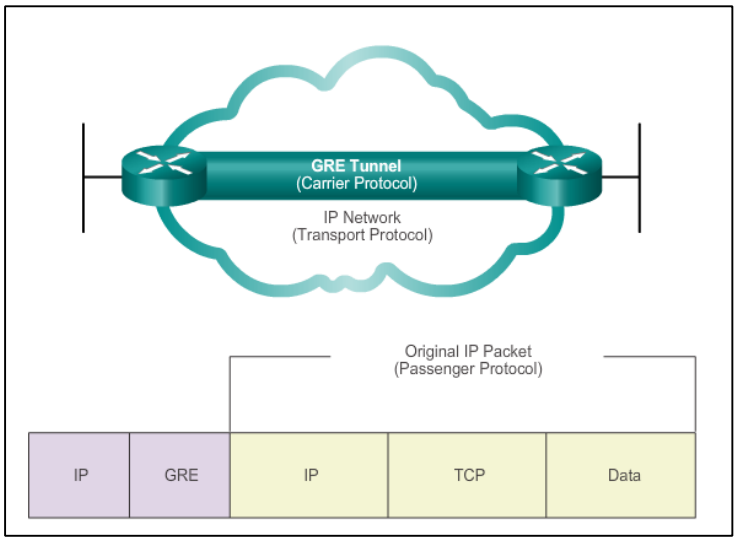
Secure Socket Tunneling Protocol (SSTP) on VPN-tekniikoista uusin ja se on ollut saatavilla Windows Vistan SP1 -versiosta lähtien. SSTP on standardisoitu protokolla, ja sen on kehittänyt Microsoft. (Crawford 2014.)

SSTP mahdollistaa PPP- ja L2TP-pakettien lähettämisen SSL 3.0 -kanavan kautta. Kun L2TP- ja IP-Sec-liikenne yleisimmin torjutaan palomuurissa, SSTP mahdollistaa verkkoliikenteen pääsyn palomuurin läpi. Yhteys palvelimen ja asiakkaan välille muodostetaan TCP-portin 443 kautta, koska SSTP hyödyntää HTTPS-protokollaa. (Crawford 2014.)

SSTP ei sovellu Site-To-Site-yhteyksiin, vaan se on luotu käytettäväksi ainoastaan asiakasyhteyksiin, eli Point-To-Point. (Crawford 2014.)

3.4 Generic Routing Protocol

Generic Routing Encapsulation (GRE) on IETF määrittelemä standardi, ja se käyttää IP-protokolla 47 GRE-pakettien tunnistamiseen (Cisco Systems b). GRE on IP-protokollan otsikkotietojen avulla muodostettava yksinkertainen, salaamaton yhteys. (Hakala ja Vainio 2005, 382) Kuvassa 5 on esitelty GRE-paketin rakenne.



KUVA 5. GRE-paketin rakenne (Cisco Systems.)

Pitkänen (2015-1-26) painotti ”Vaikka GRE on jo itsessään tunneli, niin sitä ei voi sellaisenaan käyttää turvallisen yhteyden luomiseen, koska siinä ei ole mitään salausta. GRE-tunneli on aina ”pusketttava” esim. IPSec-tunnelin sisään. Pelkkä GRE-tunneli ilman salausta on ns. VN-tunneli (Virtual Network), mutta kun se ajetaan IPSec-tunnelin sisään, saadaan siitä muodostettua varsinainen VPN-tunneli.”

3.5 IP Security

IPsec (IP Security) on IETF:n kehittämä protokolla. IPsec on itse asiassa joukko protokollia, joilla mahdollistetaan turvallinen pakettien siirto verkossa. IPsec toimii IP-protokollan päällä, joten IPsec:ä voidaan käyttää minkä tahansa protokollan turvaamiseen, joka toimii IP-protokollan päällä. (Hakala, Vainio ja Vuorinen 2006, 393.) IPSec:n protokollat mahdollistavat turvallisen menetelmän avaintenvaihtoon joka yleisimmin tapahtuu IKE-menetelmää (Internet Key Exchange) käyttäen. (Hussain 2006).

IPSec-protokolla muodostuu kahdesta eri osasta, ESP-protokollasta (Encapsultaion Security Payload) ja AH-protokollasta (Authentication Header). Nämä ovat IPsec:n kaksi suojausprotokollaa.

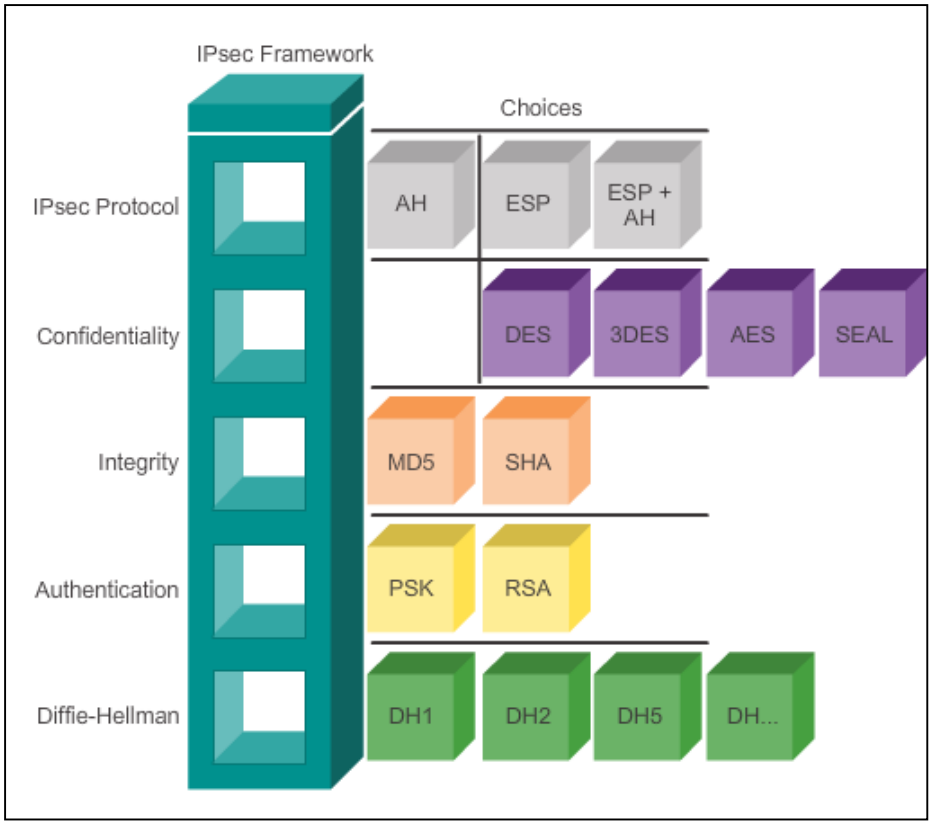
Näiden protokollien avulla IPsec mahdollistaa viestien

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

(Hakala, Vainio ja Vuorinen 2006, 393.)

AH:lla todennetaan osapuolet ja varmistetaan tiedonsiirron eheys. Tiedonsiirron eheydellä tarkoitetaan, että varmistetaan viestin alkuperä ja siirrettyjen tietojen muuttumattomuus tiedonsiirron aikana. (Hussain 2006.)

Kuvassa 6 on esitetty IPsec:n rakennekuva, jossa ESP hoitaa varsinaisen salauksen ja IP-paketin aitouden todentamisen, joka on kapseloitu IPsec-paketin sisään. ESP:n yleisimmin käytetyt variaatiot ovat ESP tai ESP+AH. Käyttämällä pelkästään ESP:tä saadaan tiedonsiirto salattua, kun taas käyttämällä ESP+AH:ta saadaan salauksen lisäksi myös todennettua osapuolet. Luottamuksellisuuden varmistamiseen käytetään yleisimmin AES (Advanced Encryption Standard) -menetelmää. Käyttämällä MD5:tä (Message Digest) tai SHA:ta (Secure Hash Algorithm), varmistetaan, että sisältöä ei ole muutettu matkalla. VPN-tunnelin molempien päiden todentamiseen käytetään joko PSK (PreShared Key)- tai RSA (Rivest, Shamir & adleman)- menetelmää. Viimeisenä IPsec-rakenteessa valitaan käytettävä DH-ryhmä (Diffie-Hellman group). DH-ryhmä on avainten vaihto algoritmi. Jos salaukseen ja todentamiseen on käytetty 128bit. avainta, käytetään DH-ryhmiä 5, 14, 19, 20 tai 24. Mikäli salaus ja todennus on suojattu 256bit. salauksella käytetään DH-ryhmiä 21 tai 24. Mitä isompi DH-ryhmä on käytössä, sitä turvallisempi avaintenvaihto prosessi, mutta mitä suurempaan DH-ryhmään mennään sitä raskaampi ja hitaampi avainten vaihto prosessi on. DH-ryhmän valinnassa joudutaan siis tekemään kompromisseja tietoturvallisuuden ja VPN-yhteyden nopeuden kanssa. Pienin DH-ryhmä on 1 joka on 768-bit. (Cisco Systems c.)



KUVA 6. IPSec rakennekuva (Cisco Systems c.)

IPSec:ä voidaan käyttää kahdella eri tavalla, joko kahden tavallisen osapuolen välisen yhteyden turvaamiseen (kuljetusmoodi) tai luomaan osapuolien välille suojattu tunneli (tunnelimoodi) (Hakala, Vainio ja Vuorinen 2006, 393).

3.5.1 Kuljetusmoodi

Kuljetusmoodissa käytettynä IPsec suojaa lähetettävän viestin sisällön ja IP-otsakkeen uuden IP-paketin sisään. Mikään viestin alkuperäisestä osasta ei ole muutettavissa eikä näkyvissä sinä aikana kun pakettia siirretään verkon yli. (Hakala, Vainio ja Vuorinen 2006, 393.)

3.5.2 Tunnelimoodi

Tunnelimoodissa IPSec-yhteyden osapuolina voivat olla joko tavallinen tietokone tai IPSec-yhdyskäytävä. IPSec-yhdyskäytävänä voi toimia joko palomuuri tai reititin. IPSec-yhdyskäytävät käyttävät viestien lähettämiseen aina tunnelimoodia, kun taas tietokoneet voivat avata toistensa välille IPSec-yhteyden joko kuljetus- tai tunnelimoodissa. (Hakala, Vainio ja Vuorinen 2006, 393.)

3.5.3 IPSec-yhdyskäytävä

Avattaessa yhteyttä toiseen verkkoon käyttäen IPsec-yhdyskäytävää, avaa yhdyskäytävä tunnelimoodiyhteyden kohdeverkon IPsec-yhdyskäytävään. Kaikki viestit jotka ohjataan yhdyskäytävään, suojataan yhdyskäytävän välisen yhteyden ajaksi verkkojen välille luodulla IPSec-yhteydellä. Yhdyskäytävään voidaan lähettää mitä tahansa viestejä, oli ne sitten ennestään suojattuja tai suojaamattomia. (Hakala, Vainio ja Vuorinen 2006, 393.)

4 SALAUSPROTOKOLLAT

Puhuttaessa tietoverkkojen tietoturvallisuudesta ei niiden salauksen merkitystä voida vähätellä, koska liikenteen salaaminen on internetin tietoturvan perusta. VPN lukeutuu niihin joiden salaus tulee olla erityisen vahva. (Hakala ja Vainio 2005, 382).

Yksi tärkeimmistä periaatteista suojatussa liikenteessä on, että käytetään mahdollisimman monta erityyppistä salausalgoritmia. Tämä estää sen, ettei hyökkääjä ensimmäisen salauksen purettuaan pysty purkamaan toista samalla menetelmällä kuin aiemman.

4.1 Secure Sockets Layer

Secure Sockets Layer (SSL) ei vaadi käyttäjältä erikseen sen kytkemistä päälle vaan se kytkeytyy itsestään päälle kun avataan SSL-yhteyttä käyttävä sivusto tai yhteys. Edellytyksenä, että SSL-yhteyttä voidaan käytää, tulee palveluntarjoajan olla hankkinut tarvittavat varmenteet ja ohjelmat. Palveluntarjoaja joutuu erikseen ostamaan SSL-varmenteen esimerkiksi Verisign:lta. (Hakala, Vainio ja Vuorinen 2006, 391.)

SSL luo vahvan salauksen käyttäjän ja www-palvelimen välille. Salauksen etuna on, että ulkopuolinen ”hyökkääjä” ei liikennettä seuraamalla saa käsiinsä luottamuksellisia tietoja. SSL ei ainoastaan salaa liikennettä vaan se tarjoaa myös vahvan todentamisen varmenteiden avulla. Varmenne on erikseen asennettu palvelimelle ja tämän perusteella voidaan varmistua oikeasta palvelusta. (Hakala, Vainio ja Vuorinen 2006, 391.) SSL salaa tiedon OSI-mallin sovelluskerroksilla eli kerroksilla viisi ja kuusi.

SSL:stä on olemassa useita verisoita. SSL:n luoman salauksen vahvuus selviää sen nimen perässä olevasta luvusta. Usein käytetty on SSL128, jolloin salaus avain on 128bit pitkä joka on huomattavan vaikea murtaa johtuen sen pituudesta ja monimutkaisuudesta. (If 2015.)

4.2 Secure Sockets Layer Virtual Private Network

Secure Sockets Layer Virtual Private Network (SSL VPN) on tekniikkaa, jossa VPN-yhteys otetaan SSL-yhteyden yli suljettuun verkkoon etälaitteelta tai yhdistetään kaksi erillistä suljettua verkkoa keskenään. SSL VPN ero perinteiseen VPN-yhteyteen on se, että SSL VPN on toteutettu ylemmillä OSI-mallin kerroksilla (4-7), kun esimerkiksi IPSec, jota on paljon käytetty VPN-yhteyksissä, toteutetaan OSI-mallin kerroksella 3. SSL VPN ei ole standardisoitu ja tästä johtuen se ei välttämättä toimi kaikkien järjestelmien kanssa keskenään. (SSL VPN Wikipedia 2013.)

Tavallinen VPN-yhteys tarvitsee aina erillisen VPN-client ohjelman, kun taas SSL VPN-yhteys voidaan avata millä tahansa internet-selaimella. (Helppari Oy 2014.)

4.3 Secure Shell

Secure Shell (SSH) on salattuun tietoliikenteeseen tarkoitettu protokolla. Yleisin tapa käyttää SSH:ta on, että SSH-asiakasohjelmalla otetaan yhteys SSH-palvelimeen, jota kautta päästään käyttämään etäpalveluita. (SSH Wikipedia 2015.)

Kun tunnelointiin käytetään SSH:ta, tulee huomioida, että palvelimelle voidaan avata yhteyksiä jotka normaalisti estettäisiin palomuurissa. Myöskään virustorjuntaohjelmat eivät pysty tutkimaan SSH-yhteyksiä, koska SSH-yhteydet ovat salakirjoitettuja. (Hakala, Vainio ja Vuorinen 2006, 388.)

4.3.1 Secure Shell siirtokerroksessa

Siirtokerros eli siirtoprotokolla huolehtii työaseman ja palvelimen tunnistamisesta, viestin eheydestä ja salakirjoittamisesta. Siirtoprotokolla toimii TCP-protokollan päällä.

SSH-yhteyttä käyttävät osapuolet sopivat viestinnässä käytettävästä

- pakkausmenetelmästä
- tiivistefunktiosta jolla viestien eheys varmistetaan
- istuntoavaimesta
- palvelimen tunnistamisesta
- salakirjoitusmenetelmästä

Vaikka edellä mainitut asiat on sovittu yhteyden muodostus vaiheessa, voi kumpi tahansa osapuoli koska vain vaatia viestinnässä käytettävien menetelmien uusimista. Kun menetelmistä on sovittu uudestaan, yhteys jatkuu normaalisti. (Hakala, Vainio ja Vuorinen 2006, 389.)

4.3.2 Secure Shell käyttäjätunnistuskerroksessa

Käyttäjätunnistuskerros eli käyttäjätunnistusprotokolla toimii siirtoprotokollan päällä ja sen tehtäviin lukeutuu tunnistaa suojatun yhteyden käyttäjät. Tähän on olemassa esimerkiksi seuravia tapoja:

- käyttäjänimen ja salasanan perusteella
- käyttäjänimen ja julkisen avaimen perusteella
- käyttäjänimen ja työaseman perusteella

Kun tunnistamiseen käytetään käyttäjänimeä ja salasanaa, työasema lähettää kyseiset tiedot siirtoprotokollaa käyttäen palvelimelle selkokielisenä, jossa ne tarkistetaan ja päätetään sallitaanko yhteyden luominen. Vaikka käyttäjänimi ja salasana lähtevätkin selväkielisenä siirtoprotokollalle, niin eivät ne kuitenkaan kulje verkossa selväkielisenä, koska siirtoprotokolla salakirjoittaa kaiken mitä se kuljettaa. (Hakala, Vainio ja Vuorinen 2006, 389.)

Jos tunnistaminen tapahtuu käyttämällä käyttäjänimeä ja julkista avainta, työaseman julkinen avain tarkistetaan käyttäjän avainparin salaisella avaimella. Tästä syntyy niin sanottu digitaalinen allekirjoi-

tus joka koostuu yhteyttä koskevista tiedoista. Näitä tietoja ovat mm. käyttäjänimi ja julkisen avaimen algoritmin nimi siirtoyhteyskerrosyhteydellä. (Hakala, Vainio ja Vuorinen 2006, 389.)

4.3.3 Secure Shell yhteyskerroksessa

Yhteyskerros eli yhteysprotokolla toimii siirtokerroksen ja käyttäjätunistuskerroksen päällä. Tämän avulla voidaan avata useita kanavia siirtoprotokollan sisälle. Näitä kanavia voidaan käyttää kuin erillistä yhteyttä pääteyhteyteen tai yhteyden välittämiseen. Voidaan siis todeta, että SSH-yhteyden osapuolten välillä on yksi siirtoprotokollan yhteys, jonka kaikki kanavat on tunneloitu sen yhteyden kautta. (Hakala, Vainio ja Vuorinen 2006, 390.)

Erona SSH:lla ja SSL:llä on se, että SSH toimii OSI-mallin sovelluskerroksella kun taas SSL toimii kerroksilla neljä - seitsemän.

5 VPN-YHTEYDEN ROOLIT

Jotta VPN-yhteys voidaan toteuttaa, tulee yrityksellä olla asennettuna palvelimella tiettyjä rooleja mitä VPN-yhteys tarvitsee. Näistä välttämättömimmät ovat AD CS, DHCP ja DNS joista kerrotaan tässä luvussa tarkemmin.

5.1 Active Directory Certificate Services

Active Directory Certificate Services (AD CS) on Active Directoryn (AD) työkalu, jonka avulla järjestelmien ylläpitäjät voivat hallinnoida ja myöntää varmenteita eri palveluille. VPN-yhteyksien lisäksi näihin palveluihin lukeutuvat mm. Internet Protocol Security (IPSec), Secure Sockets Layer (SSL) ja Transport Layer Security (TLS).

5.2 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol:in (DHCP) tyypillisin tehtävä on jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille. Osoiteavaruus, jolta DHCP jakaa IP-osoitteita on ylläpitäjän ennalta määräämä, esim. 192.168.1.51–192.168.1.66, tällöin jaossa on 15 IP-osoitetta. Mikäli laitteita kytkeytyy lähiverkkoon enemmän kuin IP-osoitteita on jaossa, ei osoiteavaruuden ylimeneville laitteille anneta IP-osoitetta, ennen kuin niitä taas vapautuu.

DHCP ei jaa asiakkaille pelkkiä IP-osoitteita, vaan se voi jakaa myös oletusyhdyskäytävän ja nimipalvelimen. DHCP:n kautta voidaan jakaa myös monia muita verkon asetuksia.

5.3 Domain Name System

Domain Name System (DNS) on nimipalvelujärjestelmä, joka muuntaa IP-osoitteet verkkotunnuksiksi ja päinvastoin. (Kaario 2002, 75 -78). Yhdistettäessä tietokonetta DNS:n avulla esimerkiksi internetsivustoon tai verkkolevyyn, voidaan käyttää numeerisen osoitteen tilalla sitä vastaavaa nimeä, eli esimerkiksi selaimen osoitekenttään voidaan kirjoittaa suoraan www.savonia.fi sen sijaan, että syötettäisiin numeerinen osoite, joka tässä tapauksessa olisi 193.167.78.120.

6 TIETOTURVA

On huomattava, että VPN-yhteyden molemmissa päissä tulee olla palomuuri. Vaikka liikenne olisi salattu, ilman palomuuria tunnelin pää olisi kuitenkin täysin avoin. Näin ollen esimerkiksi L2TP tai GRE-tunnelin käyttö pelkästään ei riitä, vaan tunneli on suojattava vielä vaikka IPsec-tunelilla, jonka sisään GRE tai L2TP-paketti ajetaan.

PPTP-protokollaa käytettäessä salaus toteutetaan Microsoft Point-To-Point Encryption -salauksella (MPPE). MPPE:ssä salausavaimet generoidaan käyttäjätunnistus prosessin yhteydessä, näitä ovat mm. Microsoft Challenge Handshaking Authentication Protocol (MS-CHAP) tai Extensible Authentication Protocol Transport Level Security (EAP-TSL). (Hakala, Vainio ja Vuorinen 2006, 288.)

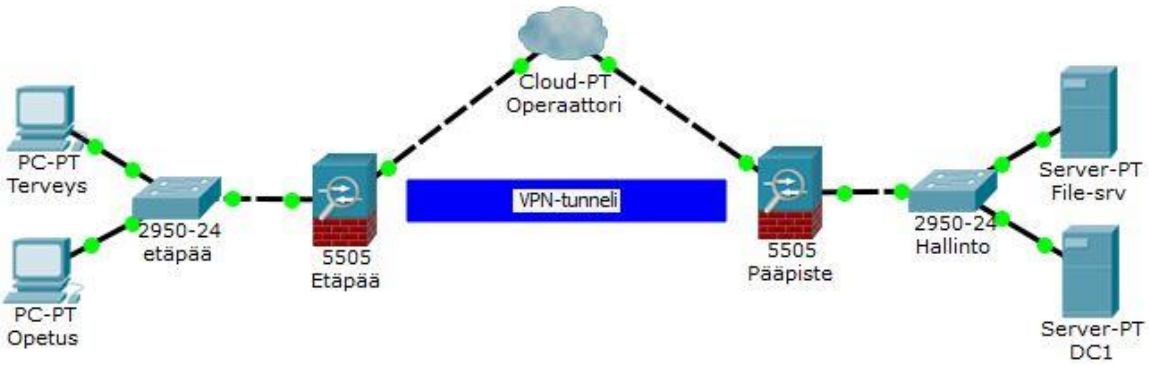
Jos yhteyttä muodostava laite käyttää MS-CHAP-protokollaa, lähetetään yhteyttä muodostavalla laitteelle satunnainen viesti salattavaksi. Yhteyttä muodostava laite lähettää saamansa viestin salakielisenä takaisin yhdessä yhteystunnisteen ja salasanan kanssa. Alkuperäisen viestin lähettänyt etäkäyttöpalvelin tai IAS-palvelin (Internet Authentication Server) purkaa saamansa salatun viestin ja mikäli se vastaa palvelimen lähettämää viestiä – voidaan yhteys muodostaa. (Hakala, Vainio ja Vuorinen 2006, 288.)

Mikäli tarvitaan laajempaa käyttäjän tunnistusta, käytetään salaukseen EAP-TSL-protokollaa. EAP-TSL soveltuu hyvin käytettäväksi liikkuvien etäkäyttäjien tunnistamiseen, koska siinä käytetään julkisen avaimen salaukseen liittyviä sertifikaatteja. Tämä puolestaan mahdollistaa vaihtuvien tunnuslukujen tai älykorttien käytön VPN-asiakkaan tunnistamiseen. (Hakala, Vainio ja Vuorinen 2006, 289.)

IPSec-protokolla vastaa salauksesta silloin, kun käytetään L2PT-protokollaa. Viesti salataan DES (Data Encryption Standard) -ja 3DES (Triple DES) -salauksella. L2PT-protokollan käytön edellytys on se, että tunnelin molemmissa päissä oleville laitteille on jaettu etukäteen ns. aloitusavain. (Hakala, Vainio ja Vuorinen 2006, 289.)

7 TOTEUTUSTAVAT

VPN-yhteyksien toteutustapoja on monia; tavat riippuvat käytetyistä protokollista, käyttötarkoituksista sekä käytettävissä olevista resursseista. Kyse on siis tavasta, jolla yhteys tunneloidaan ja muodostetaan kahden reitittimen välille. Yleisimpiä tapoja muodostaa yhteys on käyttää L2TP-protkollaa sekä GRE- ja PPTP-protokollaa. Myös IPSec-protokolla on yleinen käytössä oleva toteutusmuoto. Kuvassa 7 on esitetty VPN-tunnelin rakennekuva Site-To-Site yhteydessä kun käytetään Ciscon ASA-5505 -palomuuria. Tässä luvussa käydään läpi laitepohjainen ja ohjelmapohjainen ratkaisutapa läpi ja esitellään molemmista tavoista kaksi eri tapaa toteuttaa VPN-yhteys.



KUVA 7. Site-To-Site VPN -tunnelin rakenne (Ruuskanen 2015-4-4.)

7.1 Ohjelmapohjainen ratkaisu

Ohjelmapohjainen VPN-yhteys sopii hyvin etä- ja matkatyötä tekevälle henkilölle, jonka on tarve päästä käsiksi yrityksen tietoihin ja palveluihin. Ohjelmistopohjainen VPN tarvitsee aina käyttäjän toimia yhteyden muodostukseen. Tämä tarkoittaa lähinnä sitä, että käyttäjä muodostaa itse VPN-yhteyden avaamalla käytössä olevan VPN-ohjelman ja syöttää tunnuksen ja salasanan muodostaakseen yhteyden.

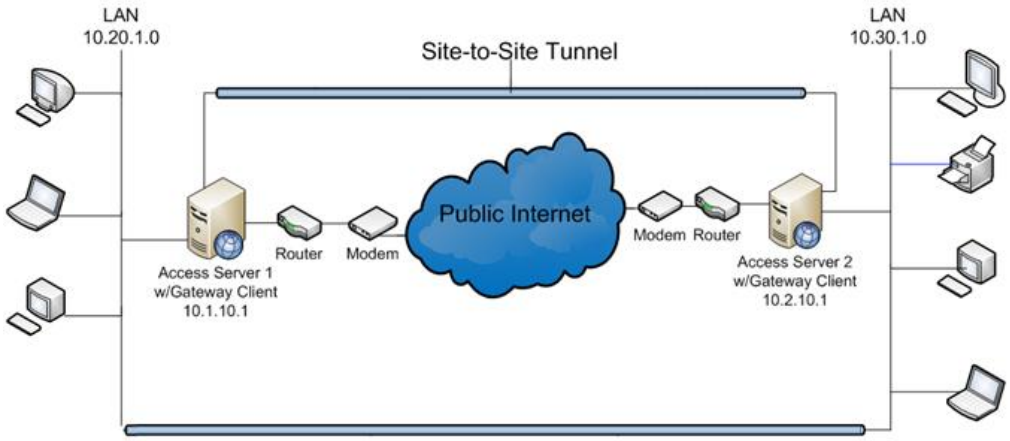
7.1.1 OpenVPN

Yleisin käytössä oleva ohjelmapohjainen ratkaisu on OpenVPN. OpenVPN on asiakas-palvelin, eli Point-To-Point-tyyppinen ratkaisu. OpenVPN:a voidaan käyttää myös Site-To-Site-yhteyksiin, mutta se vaatii enemmän palvelinmäärityksiä. (OpenVPN Technologies.)

OpenVPN on avoimeen lähdekoodiin perustuva SSL/TLS-pohjainen ratkaisu, joka toimii OSI-mallin kerroksilla 2 ja 3. OpenVPN:stä on omat versionsa palvelimelle ja etätietokoneelle. Tietoliikenteen salauksessa on mahdollista käyttää joko symmetristä tai epäsymmetristä salausta. (OpenVPN Technologies.)

Mikäli halutaan luoda Site-To-Site-tyyppinen tunneli käyttämällä OpenVPN-ohjelmaa, tarvitsee tunnelin molempiin päihin asentaa palvelin, joista toinen toimii niin sanottuna Access- eli yhdyskäytävä-

palvelimena. Access-palvelimella tarkoitettaan sitä, että se toimii yhteyden yhdyskäytävänä, joka hoitaa VPN-yhteyden liikenteen. Tunneli luodaan siis palvelimien välille. Kuvassa 8 on esitetty verkon rakennekuva silloin, kun käytetään OpenVPN Site-To-Site-tyyppisellä yhteydellä. (OpenVPN Technologies.)



KUVA 8. OpenVPN Site-To-Site verkon rakennekuva (OpenVPN Technologies.)

OpenVPN:ssä liikenne kulkee aina yksittäisen UDP- tai TCP-portin kautta eikä näin ollen käytä esimerkiksi IPsec-protokollaa. (OpenVPN Technologies).

7.1.2 AnyConnect VPN

Yksi vaihtoehto ohjelmapohjaiseen VPN-yhteyden toteutukseen on käyttää Ciscon AnyConnect VPN-ohjelmaa. AnyConnect VPN käyttää uudempia protokollia kuin jo ehkä hieman vanhentunut IPSec VPN-asiakasohjelma. AnyConnect VPN tukee SSL-protokollaa sekä uudempaa IKEv2 (Internet Key Exchange) –protokollaa. (Cisco Systems e.)

AnyConnect VPN -menetelmä on hyvä siksi, että se käyttää IPSec-protokollaa, eli se toimii jokaisen sellaisen ohjelman kanssa, joka toimii IP-osoitteen pohjalla. AnyConnect VPN:n etu on myös, että se käyttää SSL-protokollaa, jolla on myös selaintuki. Tällöin FTP-, HTTPS- ja HTTP-ohjelmat ovat myös käytettävissä. (Cisco Systems e.)

7.2 Laitepohjainen ratkaisu

Laitepohjaisessa toteutuksessa käyttäjältä ei vaadita toimenpiteitä yhteyden muodostamiseen vaan yhteys on valmiiksi muodostettu reitittimellä. Laitepohjainen yhteys on yleensä aina Site-To-Site tyyppinen ja ohjelmistopohjaisissa ratkaisuissa käytetään useimmiten Point-To-Point-yhteyksiä.

7.2.1 Linux VPN -palvelin

Laitepohjaisia ratkaisuja on monia. Yhtenä ratkaisuna voidaan asentaa VPN-tunnelin toiseen päähän Linux-pohjainen VPN-palvelin, joka hoitaa kaiken tarvittavan, kuten liikenteen salauksen ja kapseloinnin sekä käyttäjän todentamisen. Tämä vaihtoehto on kustannuksiltaan edullinen ja hyvä ratkai-

su pienten toimipisteiden välille. Tätä toteutustapaa käyttäessä olisi parempi käyttää Point-To-Point-yhteyksiä.

Erillisen VPN-palvelimen kanssa toteuttava yhteys vaatii aina enemmän konfigurointia ja määrityksiä riippuen käytettävästä protokollasta ja salausmenetelmästä.

7.2.2 Cisco ASA 5505-Firewall

Yhtenä hyvänä vaihtoehtona Site-To-Site-yhteyksiin olisi näkemykseni mukaan hyvä käyttää Ciscon ASA 5505 -palomuuria yhteyden toteuttamiseen. Ciscon ASA 5505 -palomuuria käytettäessä voidaan VPN-yhteys muodostaa käyttäen IPSec:ä tai SSL:ää. ASA-palomuuriin voidaan suoraan määritellä eri VLAN:eja sekä voidaan määrittää, käytetäänkö salaukseen IPSec:ä vai SSL:ää.

Kuvassa 9 nähdään SSL:n ja IPsec:n vertailu taulukko. Taulukosta käy ilmi, että IPsec mahdollistaa kaikkien niiden ohjelmien käytön, jotka toimivat IP-pohjaisesti, ja sen autentikointiin käytetään kaksisuuntaista todennusta käyttäen joko esijaettua salausavainta tai digitaalista varmennetta, kun taas SSL:ää käytettäessä autentikointi on joko yksisuuntainen tai kaksisuuntainen. IPsec:ä käytettäessä ainoastaan erikseen määritellyt ja konfiguroidut laitteet voivat muodostaa yhteyden. SSL:ä käytettäessä kaikki laitteet voivat muodostaa yhteyden.

Ciscon ASA 5505 –palomuurin käyttö ei ole niin edullinen kuin edellä mainittu Linux-pohjainen ratkaisu. Tämän toteutustavan kustannukset riippuvat siitä kuinka laajaan ympäristöön laitteet tulisivat eli kuinka monta käyttäjää (yhteyksiä) ja VLAN:a kohteessa tarvitaan.

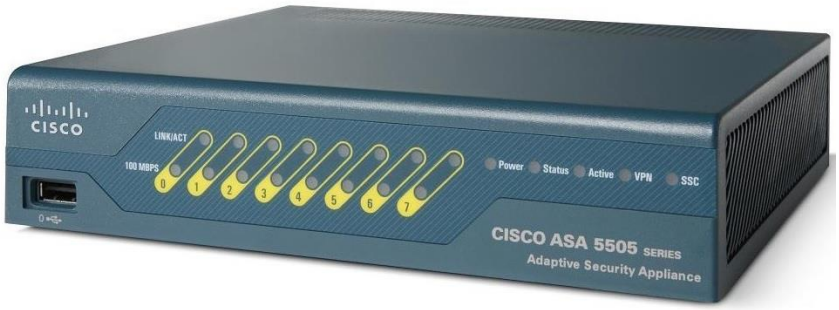
	SSL	IPsec
Applications	Web-enabled applications, file sharing, Email	All IP-based applications
Encryption	**Moderate to Strong** Key lengths from 40 bits to 256 bits	**Strong** Key lengths from 56 bits to 256 bits
Authentication	**Moderate** One-way or two-way authentication	**Strong** Two-way authentication using shared secrets or digital certificates
Connection Complexity	**Low** Requires only a web browser	**Medium** Can be challenging to nontechnical users
Connection Options	Any device can connect	Only specific devices with specific configurations can connect

KUVA 9. SSL:n ja IPSec:n vertailutaulukko (Cisco Systems a.)

8 VALITTU TOTEUTUSTAPA

Kohteet joihin VPN-yhteys Pieksämäen kaupungilla tulisi rakentumaan, käsittävät kaikki useita VLAN:eja mm. oppilaitos, terveydenhuolto ja hallinto. Ciscon ASA-palomuuria käyttämällä, ei käyttäjän tarvitse itse muodostaa VPN-yhteyttä vaan yhteys on valmiiksi jo olemassa.

Parhaimmaksi ratkaisuksi esimerkkikohteeseen valittiin käyttää Ciscon ASA-5505 palomuuria, kuva 10. Valinta perustuu yhteystyyppiin (Site-To-Site) ja siihen, että Ciscon ASA-palomuurissa on hyvä mahdollisuus eri VLAN:lle. Perus lisenssiin kuuluu kolme (3) VLAN:nia, jotka ovat lisälisenssillä laajennettavissa 20kpl:seen, lisäksi Pieksämäen kaupungilla on ennestään jo käytössä kyseisiä laitteita.



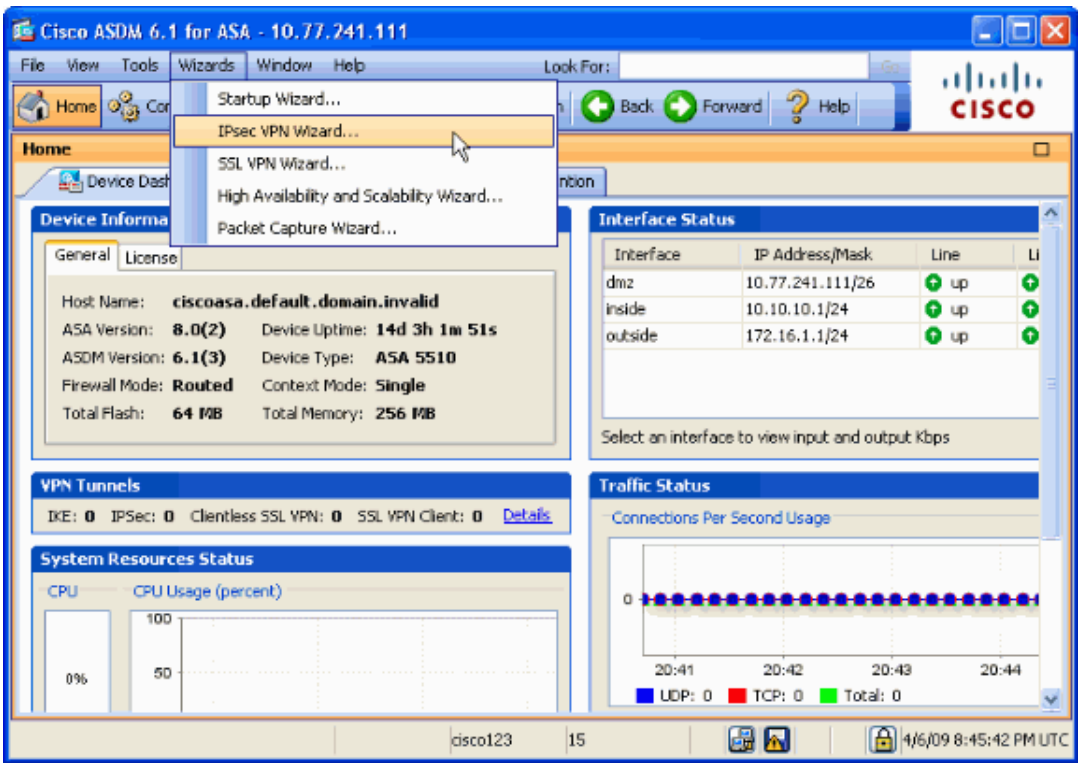
KUVA 10. Cisco ASA-5505 (Cisco Systems.)

8.1 VPN-tunnelin toteutus Cisco ASA-5505 -palomuurilla

VPN-tunnelin rakentaminen aloitetaan ottamalla yhteys laitteeseen IP-osoitteen perusteella. Yhteyden ottamiseen käytetään Cisco ASDM Launcher -ohjelmaa. Mikäli laitetta ei ole vielä konfiguroitu millään tavalla, ei sillä myöskään ole IP-osoitetta. Tällöin voidaan konfigurointi tehdä konsoliportin kautta.

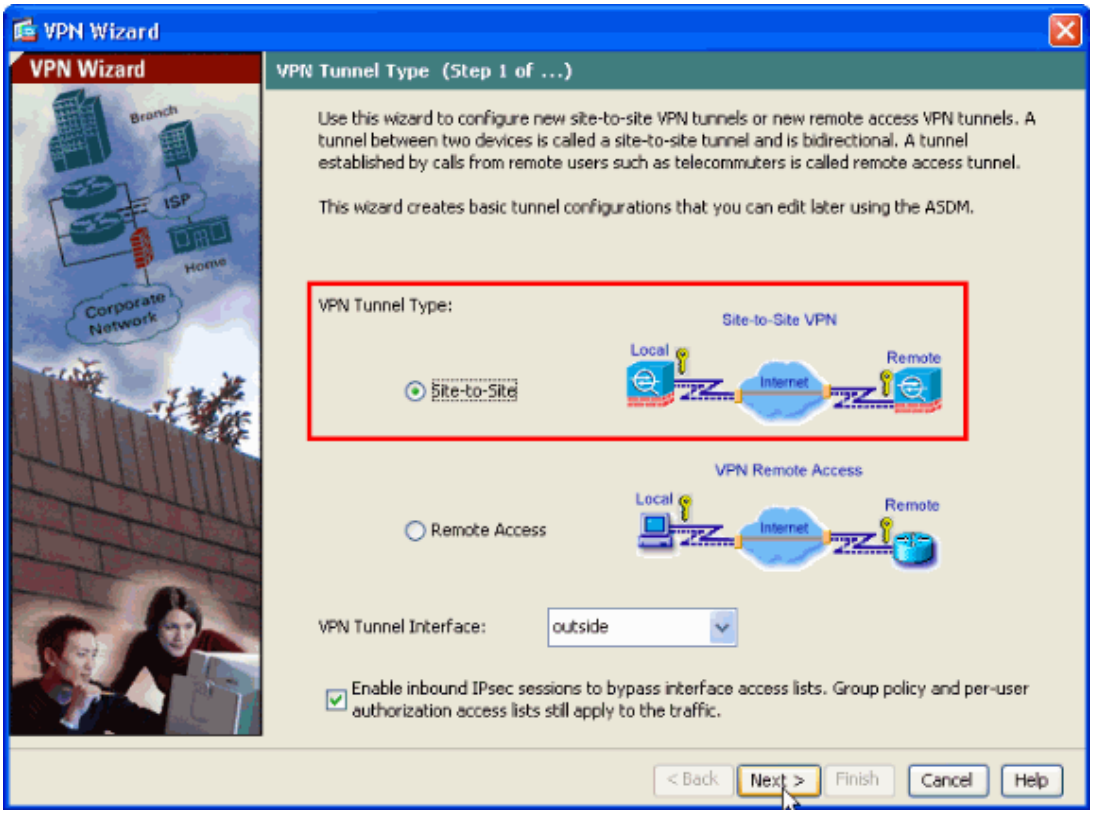
Cisco ASDM Launcher-ohjelmaan syötetään laitteen IP-osoite sekä käyttäjätunnus ja salasana, joilla saadaan yhteys laitteeseen. Tämän jälkeen ollaan laitteen hallintakonsolissa ja voidaan aloittaa määrittämään VPN-tunnelia. Myöhemmin tässä luvussa esitetyt konfiguraatiot tehdään tunnelin molempien päiden palomuureihin siten, että ne vastaavat toisiaan. Ainoat muutettavat asiat ovat IP-osoitteet mitkä muutetaan kohteen mukaiseksi, eli määritellään molempien laitteiden ulkoverkon osoite ja sisäverkon osoitealueet kohteen mukaisiksi.

Aloitetaan valitsemalla ”wizards” valikosta ”IPsec VPN Wizard”, kuva 11. IPsec-tunneli voidaan luoda myös niin sanottuun etäkäyttö (Remote Access) VPN-tunnelin suojaksi. Tässä työssä käytetään Site-To-Site VPN-tunnelia.



KUVA 11. IPsec VPN-tunnelin luonti (Cisco Systems b.)

Kun IPsec Wizard on valittu, aukeaa kuvan 12 mukainen valikko, jossa valitaan Site-To-Site VPN-tunneli tyyppi.

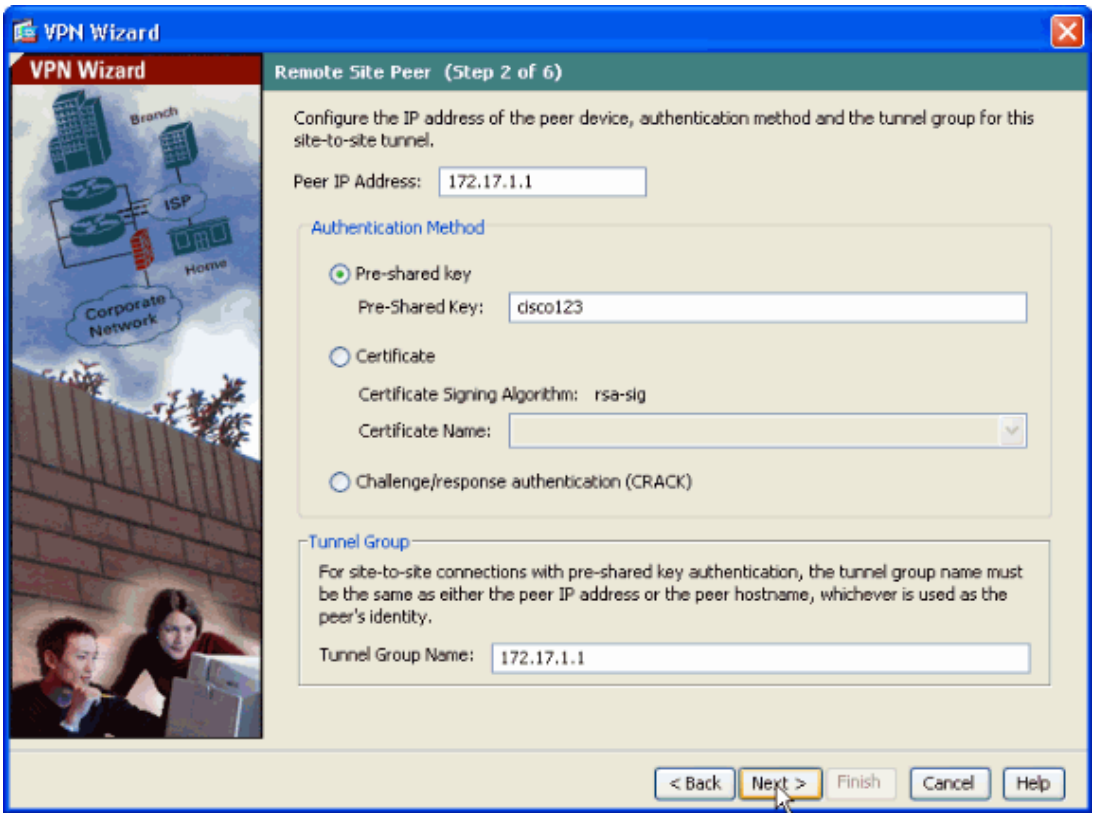


KUVA 12. Yhteystyypin valinta (Cisco Systems b.)

Kuvassa 13 määritellään laitteen IP-osoitealue, autentikointimenetelmä sekä tunnelin nimi. Tässä työssä käytetään esijaettua avain (Pre-Shared Key) -menetelmää. Voitaisiin käyttää myös sertifikaat-

tia, mutta se vaatisi sertifikaatin tekemisen ja luomisen, joten valitaan käytettäväksi esijaettua avainta.

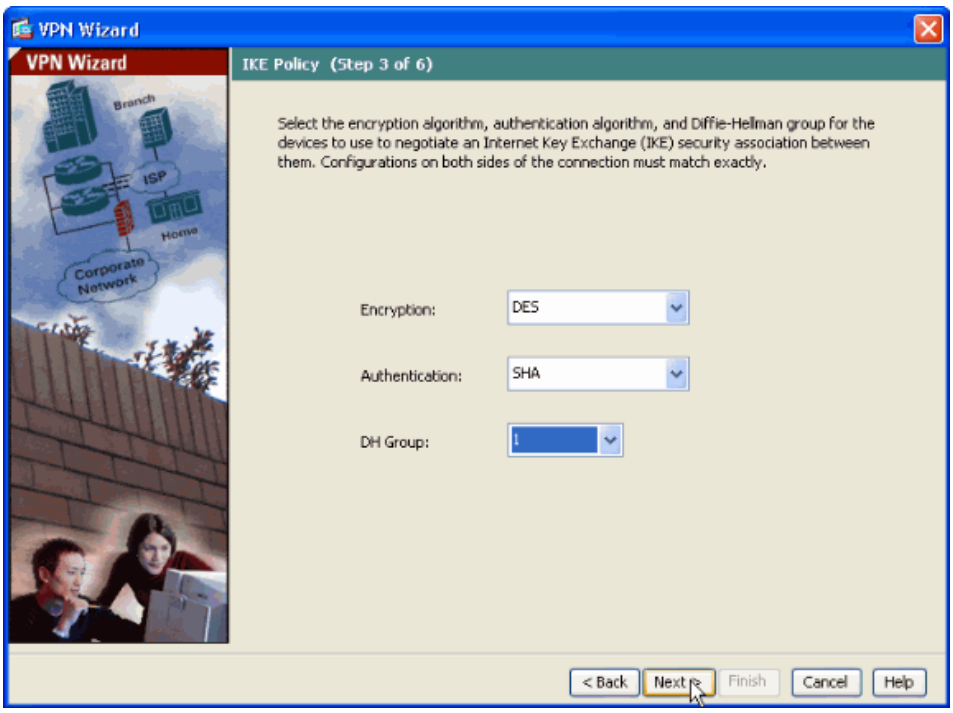
Esijaettu avain voi olla mikä tahansa, mutta ei kuitenkaan liian yksinkertainen, jotta se ei olisi niin helppo murtaa. Avain tulee märittää tunnelin molempiin päihin ja sen on oltava sama tunnelin kummassakin päässä. Tämä sen takia, että laitteet todentavat toisensa nimenomaan tämän esijaetun avain avulla.



KUVA 13. IP-osoitteen ja autentikoinnin määrittely (Cisco Systems b.)

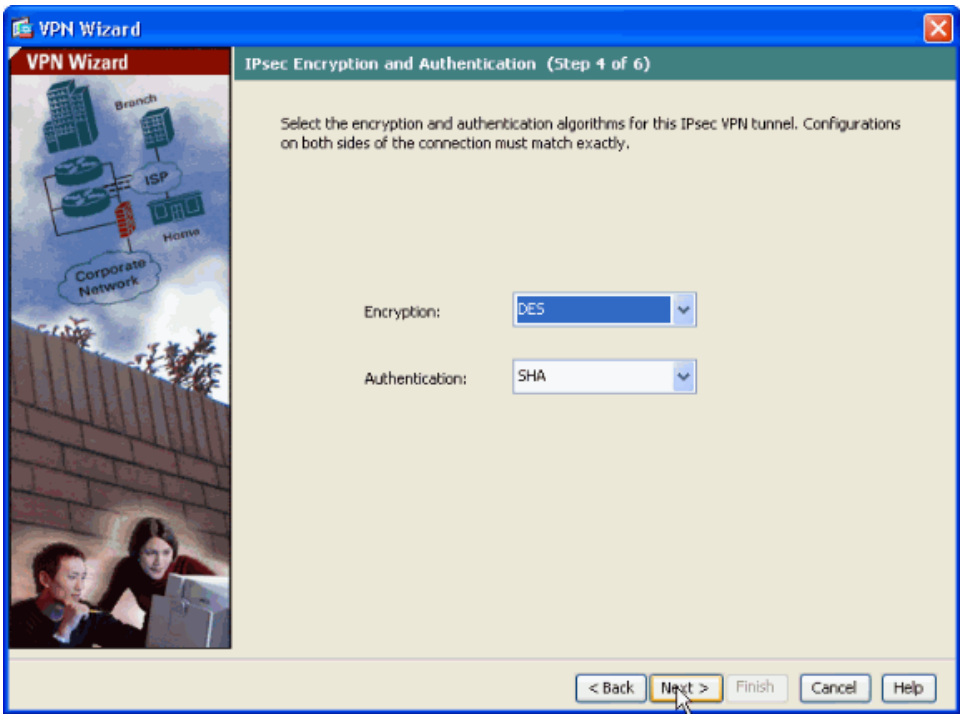
Kun laitteelle on annettu IP-osoite ja määritelty autentikointi tavaksi esijaetun avain käyttö, määritellään seuraavaksi IKE-protokolla eli millä tavalla esijaettu avain suojataan. Kuvasta 14 poiketen tässä työssä käytetään suojaukseen AES-menetelmää ja autentikointiin SHA-menetelmää sekä DH-ryhmää 5. Mitä suurempi kyseinen DH-ryhmä on, sitä enemmän se vaatii aikaa prosessointiin. Toisin sanoen suurempi on aina turvallisempi, mutta raskaampi ja hitaampi. DH-ryhmä 2 on 1024-bittinen kun taas 5-ryhmä on jo 1536-bittinen.

DH-2:en 1024 bittinen salaus on vielä murrettavissa, mutta vaati paljon prosessointi aikaa. DH-5:en 1536 bittistä salausta ei vielä ole onnistuttu murtamaan ja siitä johtuen tässä työssä käytämme DH-ryhmää 5. DH-2:en turvallisuutta voidaan tosin parantaa määrittelemällä avainten vaihtoväliksi lyhyempi aika, jolloin sen murtaminen hankaloituu johtuen avaimen tiheämmästä vaihtuvuus välistä (Cisco Systems d.)



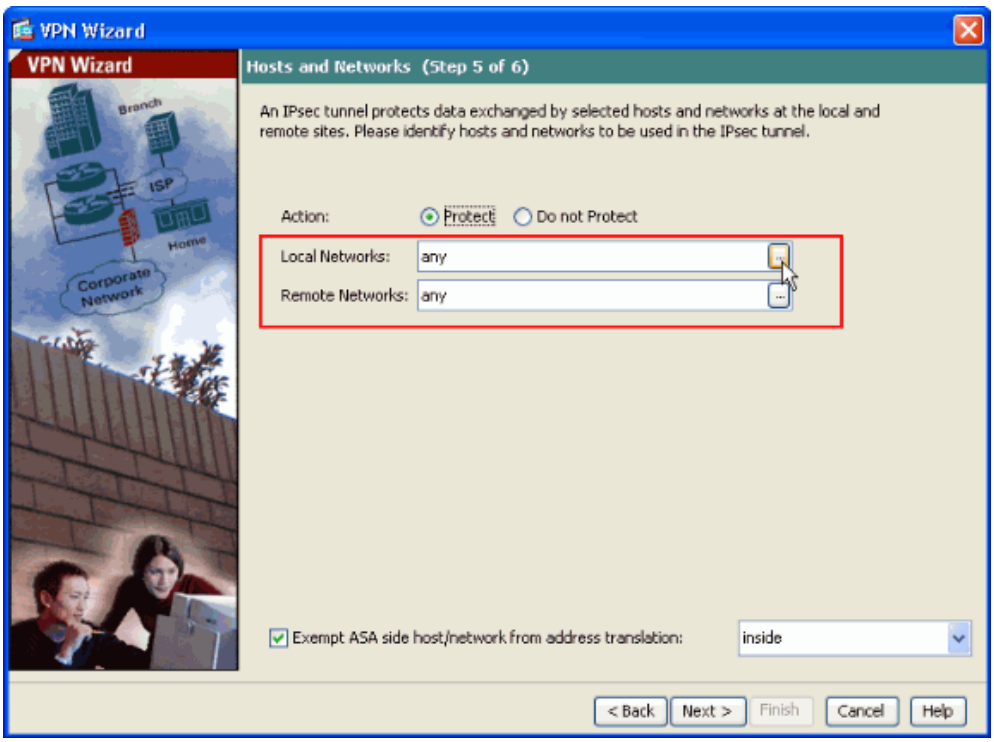
KUVA 14. Internet Key Exchange käytännön määrittely (Cisco Systems b.)

Kuvassa 15 määritellään millä tavalla IPsec-tunnelin suojaus ja autentikointi tapahtuu. Valitaan jälleen suojaustavaksi AES ja autentikointitavaksi SHA.



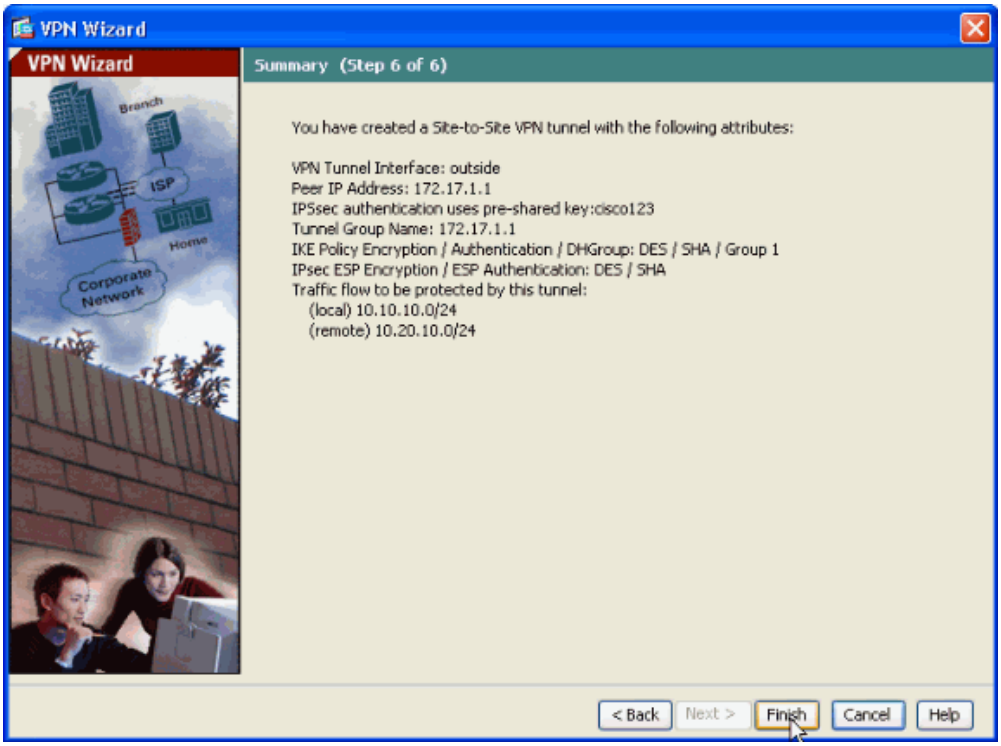
KUVA 15. IPsec-tunnelin suojaus ja todennus (Cisco Systems b.)

Kuvassa 16 määritellään laitteet ja verkot, eli paikallisen verkon ja etäverkon päät suojataan IPsec-tunnelilla, jolloin tunnelin sisällä liikkuva data on suojattu. Local Networks -kohdassa valitaan laitteen takana oleva sisäverkko ja Remote Networks valitaan nimensä mukaan etäpään verkkoalue.



KUVA 16. Verkkojen suojaaminen IPsec:llä (Cisco Systems b.)

Yhteenvetosivulla nähdään Site-To-Site tunnelin määrittelyt, kuva 17.



KUVA 17. Site-To-Site VPN-tunnelin määrittelyjen yhteenveto (Cisco Systems b.)

9 YHTEENVETO

Opinnäytetyössä saavutettiin sille asetetut tavoitteet eli tuotiin esille eri toteutustapoja sekä valittiin toteutustavoista yksi, joka sopisi parhaiten Pieksämäen kaupungin toteutettavaksi. Vaikka VPN-tunnelia ei vielä tässä vaiheessa toteuteta, on tämä työ Pieksämäen kaupungille hyvä pohja, jonka perusteella VPN-yhteys voidaan toteuttaa, kun se on ajankohtaista.

VPN-yhteyden toteutustapojen vertailu toi esille sen, kuinka monta erilaista tapaa VPN-yhteyden rakentamiselle oikeasti on. Käytettäviä protokollia toteutukseen on monia ja jokaisessa on omat hyvät ja huonot puolensa.

Opinnäytetyö oli mielenkiintoinen ja samalla haastava sen vuoksi että, koska työ oli pelkästään teoriapohjainen vertailutyö. Työstä jäi siis puuttumaan itse VPN-tunnelin toteutus käytännössä. Tunnelin käytännön toteutus olisi ainakin itseäni helpottanut opinnäytetyön teossa, koska silloin olisi saanut todeta, miten VPN-tunneli todella toteutetaan ja olisi todennäköisesti myös törmännyt ongelmatilanteisiin. Käytännön toteutuksen ja mahdollisten ongelmatilanteiden selvityksen myötä olisi tullut myös lisätietoa itse työhön ja olisin itse päässyt vielä paremmin perille VPN-yhteyden toteutuksesta. Työn haastavuutta lisäsi myös se, että VPN-tunnelin rakentaminen vaatii paljon tietoa tietoliikenteestä tietoverkossa sekä tietoturvallisuudesta.

LÄHTEET JA TUOTETUT AINEISTOT

CISCO SYSTEMS 2015 a. Configuring Failover. [Viitattu 2015-5-22.] Saatavissa: http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/failover.html#wp1041883

CISCO SYSTEMS 2015 b. Configuring Professional: Site-To-Site IPsec VPN. [Viitattu 2015-4-16.] Saatavissa: http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/112153-ccp-vpn-asa-router-config-00.html

CISCO SYSTEMS 2015 c. Configuring IPSec and ISAKMP. [Viitattu 2015-4-8.] Saatavissa: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/vpn_ike.html#wp1042167

CISCO SYSTEMS 2015 d. Configuring Internet Key Exchange Security Protocol. [Viitattu 2015-5-27.] Saatavissa: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfike.html

CISCO YSTEMS e. Configuring AnyConnect VPN Client Connections. [Viitattu 2015-4-23.] Saatavissa: http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/svc.html

CRAWFORD, Douglas. 2014 PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2. [Viitattu 2015-2-19.] Saatavissa: https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

HAKALA, Mika, VAINIO, Mika, 2005. Tietoverkon rakentaminen. 1. painos. Porvoo: WS Bookwell

HAKALA, Mika, VAINIO, Mika, & VUORIO, Olli. 2006. Tietoturvallisuuden käsikirja. 1. painos. Porvoo: WS Bookwell

HELPPARI Oy 2014. Verkon ja palveluiden etäkäyttö. [Viitattu 2015-3-16.] Saatavissa: http://www.helppari.fi/fi/tuotteet/etakaytto.html

HUSSAIN, Arshad 2006. Introduction to IPsec Virtual Private Networks. [Viitattu 2015-3-20.] Saatavissa: http://www.apca-att.org/4a/National/doc/IPSec_Presentation_Part_01.pdf

KAARIO, Kimmo 2002. TCP/IP -verkot. Porvoo: WS Bookwell.

TEARE, D. 2013. Implementing Cisco IP Routing (ROUTE). 5. painos. United State of America.

PITKÄNEN, Veijo 2015-1-26. Lehtori. [Palaveri.] Kuopio: Savonia-ammattikorkeakoulu.

Secure Sockets Layer Virtual Private Network. Wikipedia 2013. [viitattu 2015-2-25.] Saatavissa: http://fi.wikipedia.org/wiki/SSL_VPN

Secure Shell. Wikipedia 2015. [Viitattu 2015-3-15.] Saatavissa: http://fi.wikipedia.org/wiki/SSH

SSL-suojaus. If vakuutusyhtiö 2015. [Viitattu 2015-5-22] Saatavissa:
http://www.if.fi/web/fi/henkiloasiakkaat/ifkansio/pages/ssl-suojaus.aspx

VPN tunneling protocols. Microsoft Corporation 2014. [viitattu 2015-1-15.] Saatavissa:
http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx

2kmediat 2015. VPN-verkot. [Viitattu 2014-11-11.] Saatavissa:

http://www.2kmediat.com/vpn/yhteystyypit.asp