TURVALLINEN ETÄKÄYTTÖYHTEYS

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2008
Johannes Nurminen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

NURMINEN, JOHANNES: Turvallinen etäkäyttöyhteys

Tietoliikennetekniikan opinnäytetyö, 54 sivua, 9 liitesivua

Kevät 2008

TIIVISTELMÄ

Tämän opinnäytetyön tarkoitus on toteuttaa Päijät-Hämeen koulutuskonsernille tietoturvallinen, helppokäyttöinen ja kustannustehokas etäkäyttöyhteys ensisijaisesti opetushallinnollisiin tarpeisiin. Tähän asti mahdollisuus etätyöskentelyyn on ollut vain harvojen saatavilla, sillä yhteydet on toteutettu kiinteillä ADSL -yhteyksillä suoraan koulutus konsernin sisäverkkoon.

Mahdollisuuksia toteuttaa etätäityöskentely on muutamia: kiinteät yhteydet, kuten ADSL, tai jo valmista infrastruktuuria esim. internetiä, hyödyntävät ratkaisut, kuten IPsec tai SSL VPN. Kiinteät yhteydet tarjoavat aina samanlaatuisen yhteyden, mutta eivät ole kustannustehokkaita, koska yhteys on aina vuokrattava palvelun tarjoajalta. Tällöin ainoat mahdollisimman monen käyttäjän saavutettavissa oleva kustannustehokas ratkaisu on, joko IPsec- tai SSL VPN -tekniikalla toteutettu etäkäyttöratkaisu.

Koska, etäkäyttöjärjestelmältä haluttiin korkeaa tietoturvaa, otettiin asiakaskoneissa käyttöön tietokoneen tunnistavat sertifikaatit. Vain sellaiset tietokoneet, joilla on sertifikaatti voivat kirjautua järjestelmään. Lisäksi otettiin käyttöön vahva käyttäjän tunnistus kertakäyttöisillä salasanoilla. Järjestelmissä luotaviin yhteyksiin käytettiin vahvoja salausalgoritmeja.

Valinta SSL VPN- ja IPsec -ratkaisun välillä kääntyi Juniper Secure Access SSL VPN -järjestelmän hyväksi. IPsec ratkaisu ei ole optimaalinen laajassa mittakaavassa, koska yhteys vaatii asiakaskoneisiin asiakasohjelmien asennuksen ja konfiguroinin. SSL VPN toimii yleensä WWW-selaimella, mutta tarvitsee lisäksi asiakaskoneisiin asennettavia alijärjestelmiä, liikenteen tunneloimista varten yrityksen sisäverkkoon. Asennuksen jälkeen alijärjestelmät eivät kuitenkaan vaadi konfigurointia, vaan asetustiedot tulevat SSL VPN -palvelimelta. Lisäksi toteutettiin IP -sec-järjestelmän kaltainen OpenVPN SSL VPN -järjestelmä, joka toimii asiakkaalla lähes ilman konfigurointia, joka tekee siitä helposti ylläpidettävän.

Kahden SSL VPN -ratkaisun välillä päätettiin kohdentaa Juniper Secure Access opetushallinnollisiin tarpeisiin järjestelmän tarjoamien helppojen roolijakojen takia. Roolijaolla saadaan helposti kohdennettua oikeat palvelut, oikeille asiakkaille. OpenVPN kohdennettiin ylläpidollisiin tarpeisiin, koska järjestelmä mahdollistaa laajat oikeudet Päijät-Hämeen koulutuskonsernin sisäverkkoon.

Avainsanat: SSL VPN, OpenVPN, Juniper Secure Access

Lahti University Of Applied Sciences
Faculty of Technology

NURMINEN, JOHANNES: Safe remote working

Bachelor's Thesis in Telecommunications, 54 pages, 9 appendices

Spring 2008

ABSTRACT

The goal of this thesis was to create a safe, easy-to-use and cost-efficient system for remote working for the educational purposes of the Lahti Region Educational Consortium. Until now only a few people have had the possibility for remote working because connections have been made possible by dedicated ADLS lines directly to the internal network of the Lahti Region Educational Consortium.

Nowadays there are a few ways to create remote working systems: fixed lines, like ADSL, or technologies that use internet, like IPsec or SSL VPN. Fixed lines always offer connections of uniform quality but are not so cost-efficient and mobile. Instead, IPsec and SSL VPN systems are cost-efficient because they do not need any dedicated infrastructure and are not fixed to any physical location. Therefore these techniques were chosen for this thesis.

The system that was set to be built also had to have high security. Therefore certificates for computers and one-time passwords for system users were adopted. Only systems with the right certificate can connect to the remote work system. Data which is to be sent between the user and the remote end was encrypted with strong ciphers.

The Juniper Secure Access SSL VPN system was chosen instead of the IPsec system because it provides much better administrative control for a large-scale VPN infrastructure. The IPsec system requires manual client software installation and configuration to customer computers, which requires administration. SSL VPN is used by a WWW browser but it also requires some client software for tunnelling data between the client and the remote system. Software in SSL VPN does not require any configurations. An IPsec-like OpenVPN SSL VPN system was also established. OpenVPN differs from IPsec in some ways. OpenVPN requires almost no configurations and it operates in user space instead of kernel space.

Both SSL VPN systems remain in use after the establishment. Juniper offers easy casting for different roles. When using roles, it is easy to provide right services to the right users. Therefore Juniper Secure Access was reserved for educational purposes. OpenVPN was reserved for administrative purposes because it can provide much wider access to the internal network.

Keywords: SSL VPN, OpenVPN, Juniper Secure Access

SISÄLLYS

LYHENNELUETTELO

ADSL	Asymmetric Digital Subscriber Line, puhelinkaapelointia käyttävä laajakaistainen yhteys
AES	Advanced Encryption Standard, eräs symmetrinen lohkosalausmenetelmä
AH	Authentication Header, IPsec-protokollan tunnisteotsikko
CA	Certificate Authority, luotettu taho, joka myöntää sertifikaatteja
CBC	Chipher Block Chaining, symmetrisen salausalgoritmin moodi, jossa käytettävä kiinteäavain on vaikeasti ulkopuolisen havaittavissa
CPE	Customer Premises Equipment, verkon käyttäjän laitteisto jolla otetaan yhteys tietoverkkoon esim. ADSL-modeemi
CRL	Certificate Revocation List, lista sertifikaateista, jotka on poistettu käytöstä
CSU/DSU	Channel Service Unit/Data Service Unit, laite jolla yhdistetään reititin E1- tai T1 -liityntään
DCE	Data Communications Equipment, verkkopääte esim. ADSL-modeemi
DES	Data Encryption Standard, eräs symmetrinen lohkosalausmenetelmä
DHCP	Dynamic Host Configuration Protocol, verkkoprotokolla, joka jakaa IP -osoitteita

DMZ	Demilitarized zone, tietoverkon alue, johon voi ottaa internetistä loogisia yhteyksiä
DoS	Denial of Service, verkkopalvelun lamauttaminen niin, ettei se ole käytettävissä
DSL	Digital Subscriber Line, digitaalinen tilaajayhteys
DTE	Date Terminal Equipment , päätelaite, joka yrittää liikennöidä verkkoon
DUN	Dial-Up Networking, sovellus, jolla voidaan ottaa puhelinverkon välityksellä yhteys yrityksen verkkoon
ESP	Encapsulating Security Payload, käytetään IPsec-protokollan tiedon suojaamiseen
GPL	General Public License, GNU-projektin avoimen ohjelmiston lisenssi
HMAC	Hashed Message Authentication Code, eräs avaimellinen tiivistefunktio
HTTP	Hypertext Transfer Protocol, mm. WWW-selaimien käyttämä tiedonsiirto protokolla
IETF	Internet Engineering Task Force, taho, joka ylläpitää internetissä käytettävien tekniikoiden standardointiprosessia
IKE	Internet Key Exchange, salausavainten vaihtoprotokolla IPsec-protokollapinossa
IP	Internet Protocol, TCP/IP verkoissa käytettävä tietoliikenneprotokolla

IPsec	Internet Protocol Security, Internetissä yleisesti käytettävä tunnelointiprotokolla
ISAKMP	Internet Key Exchange and Key Management Protocol avainten hallintaprotokolla
ISDN	Integrated Services Digital Network, digitaalinen piirikytkentäinen puhelinverkkojärjestelmä
IVE	Instant Virtual Enviroment, Secure Access tuotteen käyttämä käyttöjärjestelmä
LDAP	Lightweight Directory Access Protocol, hakemistopalveluihin tarkoitettu verkkoprotokolla
MAC	Message Authentication Code, tiiviste, joka on riippuvainen symmetrisestä avaimesta
MD5	Message-Digest algorithm 5, eräs tiivistefunktio
MPLS	Multiprotocol Label Switching, kuituyhteyksiä käyttävä tiedonsiirtotekniikka
NAT	Network Address Translation, osoitteenmuuntotekniikka
OSI	Open Systems Interconnection Reference Model, kuvaa tiedonsiirtoprotokollia kerrosrakenteessa
PAM	Pluggable Authentication Modules, mm. Linux-järjestelmissä käytettävä ohjelmiston ulkoisen tunnistuksen mahdollistava järjestelmä
PHKK	Päijät-Hämeen koulutuskonserni, maakunnallinen koulutuksen järjestäjä, kehittäjä ja ylläpitäjä

PIN	Personal identification number, käyttäjän tiedossa oleva henkilökohtainen numerosarja
PKI	Public Key Infrastructure, tekniikka, jolla suojataan tietoa tietoverkoissa
PPP	Point-to-Point Protocol, tietoliikenneprotokolla
PSTN	Public Switched Telephone Network, valtakunnalinnen analoginen puhelinverkko
PVC	Permanent Virtual Circuit, pysyvä reitti X.25 verkossa
RADIUS	Remote Authentication Dial In User Service, protokolla, käyttäjien tunnistukseen
RC4	Ron's Code 4, Rivest Cipher 4, eräs symmetrinen jonosalausmenetelmä
RDP	Remote Desktop Protocol, mahdollistaa terminaalipalvelut Windows-ympäristössä
RFC	Request For Comments, Internetin standardit julkaistaan RFC-dokumentteina
SA	Security Associaton, määrittää IPsec-protokollan suojausparametreja
SMS	Systems Management Server, järjestelmä, jolla on mahdollista hallita keskitetysti suuria Windows-verkkoja
SMTP	Simple Mail Transfer Protocol, TCP-protokollaa käyttävä sähköpostin välitysprotokolla

SPI	Security Parameter Index, suojausparamentrin indeksi
SSL	Secure Socet Layer, tiedon salausprotokolla
SVC	Switched Virtual Circuit, väliaikainen reitti X.25 verkossa
TCP	Transmission Control Protocol, yhteydellinen tiedonsiirtoprtokolla
TLS	Transport Layer Security, tiedon salausprotokolla
VC	Virtual Circuit, virtuaalinen piiri
VPN	Virtual Private Network, näennäisesti yksityinen verkko
WINS	Windows Internet Naming Service, palvelu, jota käytetään Windows-verkoissa NetBIOS ja DNS-nimien selvitykseen
WWW	World Wide Web, Internetissä toimiva hyperteksti järjestelmä

1 JOHDANTO

Etätyöskentely on laajakaistaisten internet -yhteyksien yleistymisen myötä noussut suosituksi työskentelytavaksi. Osa työvaiheista ja viimehetken tilannetietojen päivityksistä on helppoa hoitaa kotona tai tien päältä.

Päijät-Hämeen koulutuskonsernissa etätyöskentely on ollut tähän asti mahdollista vain muutamilla henkilöillä, koska yhteydet on toteutettu kiinteillä ADSL -yhteyksillä (Asymmetric Digital Subscriber Line) työntekijän kodista suoraan koulutuskonsernin sisäverkkoon. Nykyään kiinteät linjat eivät kuitenkaan ole pakollisia, sillä internetin ylitse on mahdollista toteuttaa salattuja loogisia yhteyksiä luotettavasti ja kustannustehokkaasti.

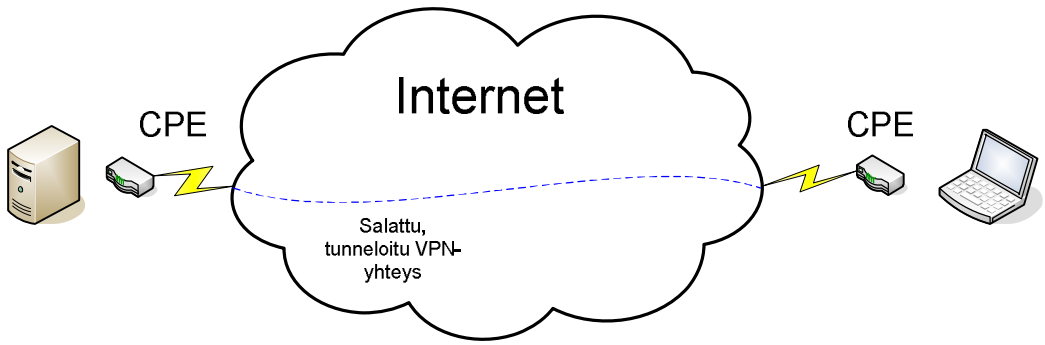
Tämän opinnäytetyön tarkoitus on luoda Päijät-Hämeen koulutuskonserniin toimiva etätyön mahdollistava järjestelmä opetushallinnollisiin tarpeisiin sekä mahdollisesti ylläpidon tarpeisiin. Toissijaisena tavoitteena on korvata tulevaisuudessa kiinteät ADSL -yhteydet ja luoda tilalle ympäristö, joka hyödyntää valmista tietoverkkoa, internetiä. Tällöin mahdollisuus etätyöskentelyyn on useamman henkilön saavutettavissa sekä myös Päijät-Hämeen koulutuskonsernille edullisempaa.

Tieto, joka tulee liikkumaan käyttäjän, käyttäjän tietokoneen ja Päijät-Hämeen koulutuskonsernin sisäverkon välillä, sisältää paljon salalaista tietoa, kuten henkilötunnuksia. Tämän vuoksi asetetaan tässä opinnäytetyössä erityishuomio sekä käyttäjän vahvaan tunnistukseen että käytettävän tietokoneen oikeellisuuteen ja turvallisuuteen. Lisäksi tulee ottaa huomioon etäkäyttöjärjestelmän helppokäyttöisyys ja selkeys etäkäyttäjälle sekä ylläpidolle.

2 VIRTUAALISET YKSITYISVERKOT

2.1 Yleistä VPN -verkoista

Kuviosta 1. nähdään, että VPN (Virtual Private Network) on tietoliikenneverkko, joka on rakennettu yleensä yrityksen yksityiseen käyttöön, jaetun julkisen infrastruktuurin välityksellä. Tämä määrittää kaksi ensisijaista topologiaa: etäyhteydet ja toimipisteiden väliset yhteydet. (Perlmutter & Zarkower 2001, 10.)



KUVIO 1. VPN -yhteys kahden laitteen välillä.

Yleensä käytössä oleva julkinen infrastruktuuri on internet, tämä ei kuitenkaan ole pakollista. Infrastruktuuri voi olla myös kiinteä puhelinlinja tai virtuaalipiirejä käyttävät verkko, kuten X.25. Toisin kuin internetiä käyttävät VPN -verkot, virtuaalipiirejä käyttävät tekniikat erottelevat datan jo siirtoyhteys- tai verkkokerroksella, jolloin palomuuria välttämättä tarvita. (Perlmutter & Zarkower 2001, 10.)

Nykyään kuitenkin internetin yleistettyä, tarkoitetaan VPN -verkoilla internetiä hyväksikäyttäviä verkkoja, koska internetin käyttämä IP (Internet Protocol) mahdollistaa tehokkaan ja kustannuksiltaan edullisen reitityksen eri CPE (Customer Premises Equipment) -laitteiden välillä. (Perlmutter ym. 2001, 11.)

Yleisesti eri VPN -ratkaisut toimivat OSI -mallin (Open Systems Interconnection Reference Model) eri kerroksilla. Kiinteät linjat toimivat ensimmäisellä tasolla. Pakettikytkentäiset yhteydet, kuten X.25 toimivat verkkokerroksella, kuten nykyaikainen IPsec -protokolla. Uusimmat tulokkaat, SSL VPN -yhteydet toimivat kerroksilla 4 – 7. (SSL VPN 2008.)

VPN -liikenne kahden eri CPE -laitteen välillä tunneloidaan. Tunnelointi tarkoittaa yksinkertaisemmillaan datapaketin kapselointia toisen datapaketin sisälle. Sama asia tapahtuu, kun kirje laitetaan kirjekuoreen, jonka posti vie oikeaan osoitteeseen, jossa kirje avataan. VPN -yhteyksissä kuori voi sisältää osoitteenmuunnoksen, salauksen, eheystarkistuksen, lähettäjän todennuksen ja pakkauksen. (Perlmutter ym. 2001, 12.)

2.2 Tiedon salaaminen ja toimijoiden todennus

Käyttäjien ja käytettävien laitteiden todennus sekä liikenteen salaus ovat tärkeässä osassa VPN -tekniikoissa. Todennuksen avulla pyritään selvittämään VPN -yhteyteen osallistuvien CPE -laitteiden ja käyttäjien oikeellisuus. Tällöin tiedon joutumista vääriin käsiin voidaan ehkäistä. (Perlmutter ym. 2001, 12.)

Hyvällä salauksella voidaan minimoida tiedon salakuuntelusta syntyvää haittaa. Yleisesti tiedon salaamisen käytetään kahta tekniikkaa: symmetristä salausta ja epäsymmetristä salausta. (Perlmutter ym. 2001, 106.)

Symmetrisessä salauksessa viestin lähettäjällä ja vastaanottajalla on käytössään sama salausavain. Avain on ennen VPN -yhteyden avaamista siirrettävä turvallisesti lähettäjältä vastaanottajalle. Symmetriset salausmenetelmät jaetaan kahteen osaan, jono- ja lohkosalausmenetelmiin. (Symmetric-key algorithm 2008.)

Lohkosalausmenetelmät salaavat aina määrämittaisen palan tietoa esim. 128 bittiä, jotka sitten salataan yksitellen ja lähetetään vastaanottajalle. Yleisiä symmetrisiä

lohkosalausmenetelmiä ovat DES (Data Encryption Standard), AES (Advanced Encryption Standard) ja Blowfish. (Symmetric-key algorithm 2008.)

Symmetriset jonosalausmenetelmät salaavat tietoa lähes lineaarisesti, jopa tavu kerrallaan. Salaus toteutetaan käyttämällä XOR -operaatiota, jossa sotketaan käytetty avain ja selkokielinen tieto. Yleisiä jonosalausmenetelmiä ovat RC4 (Ron's Code 4, Rivest Cipher 4) ja Salsa20. (Symmetric-key algorithm 2008.)

Epäsymmetrisessä salauksessa käytetään kahta avainta, yksityistä (private key) ja julkista (public key). Yksityisellä avaimella tieto salataan ja julkisella avaimella tieto puretaan tai toisinpäin. Julkisella avaimella ei kuitenkaan pysty purkamaan julkisella avaimella salattua tietoa, jolloin kolmannet osapuolet eivät voi purkaa tietoa vaikka tietäisivät julkisen avaimen. Yleinen epäsymmetrinen salausmenetelmä on RSA. (Public-key cryptography 2008.)

2.3 Tiedon eheys

Tiivistefunktioita käytetään yleisesti tietoliikenteessä varmistamaan tiedon eheys. Tiivistefunktio on yksisuuntainen operaatio, jossa saadaan aina määrämittainen tiiviste. Laskettu tiiviste liitetään mukaan lähetettävään tietoon, vastaavasti vastaanottopäässä lasketaan tiiviste uudelleen ja verrataan alkuperäiseen. Jos tiivisteet ovat samat, tieto on säilynyt muuttumattomana, muuten tieto hylätään. (Cyptographick hash funcktion 2008.)

Tiivistefunktion määrämittaisesta luonteesta johtuen voi tapahtua törmäyksiä. Törmäys tapahtuu, kun sama tiiviste lasketaan kahdesta eri tiedosta. Eri tiivistysfunktioiden paremmuutta mitataan mahdollisten törmäysten määrällä. Mitä pienempi on törmäyksen todennäköisyys, sitä parempi tiivistefunktio on. Tiivistefunktiot eivät ole yksikäsitteisiä, eli ne eivät sovellu tiedon salaamiseen tai pakkaamiseen. Yleisimpiä tiivistefunktioita ovat MD5 (Message-Digest algorithm 5) ja SHA-1. (Cyptographick hash funcktion 2008.)

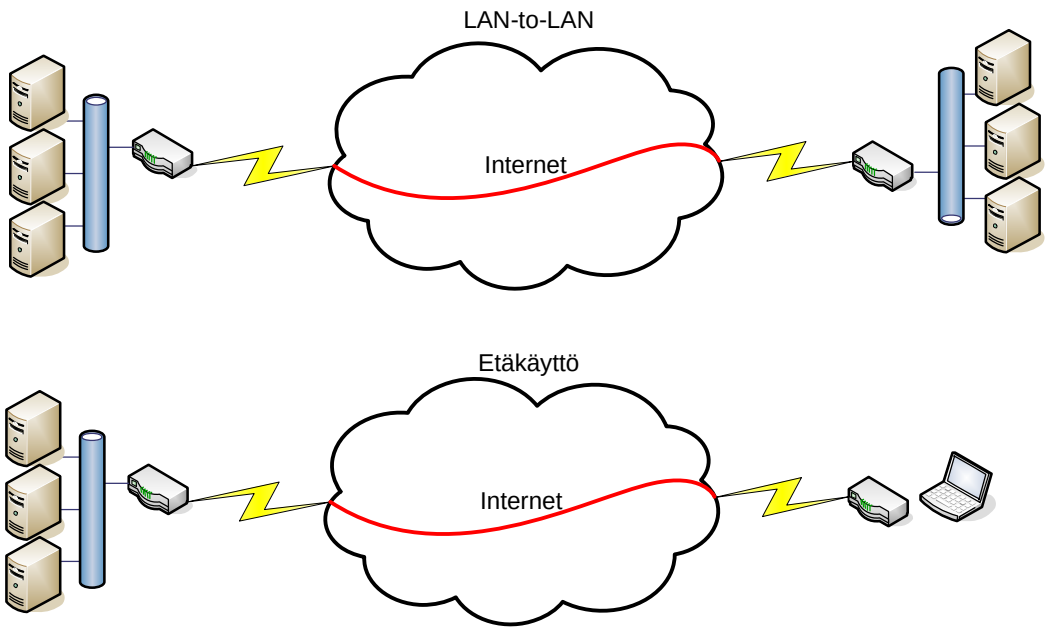
Lisäksi on mahdollista käyttää avaimellisia tiivistefunktioita. Avaimellinen tiivistefunktio tuottaa tiedosta ja symmetrisestä avaimesta tiivisteen, jolloin ainoastaan salausavaimen tunteva voi laskea oikean tiivisteen. Yleisesti käytössä olevia avaimellisia tiivistefunktioita ovat HMAC (Hash Message Authentication Code) ja MAC (Message Authentication Code). Molemmat tuottavat eheystarkistuksen, mutta HMAC on vaikeampi murtaa. (Cyptographick hash funcktion 2008.)

2.4 VPN -topologiat

Yleisesti on käytössä kaksi eri VPN -topologiaa, kuten kuviossa 2 on esitetty. Topologia, jolla yhdistetään yritysten eri toimipisteet toisiinsa (LAN-to-LAN) ja topologia, jolla yhdistetään yksittäinen työntekijä yrityksen verkkoon. (Perlmutter ym. 2001, 12, 48.)

Päästä päähän yhteydet tarjoavat yleensä OSI -mallin verkkokerroksella toimivan yhteyden eri toimipisteiden välille. Pääsääntöisesti yhteys toteutetaan reitittimien tai palomuurien välille. Yhteyden salauksessa käytetään yleensä ennalta sovittua symmetristä avainta tai sertifikaattia. Käytettäessä sertifikaatteja ei jokaiseen laitteeseen tarvitse asettaa samaa avainta, vaan yksilöllinen sertifikaatti. Yhteyttä varten VPN-yhteyden tekevässä laitteessa täytyy määrittää, mitkä aliverkot ovat käytössä VPN -yhteyksille. (Perlmutter ym. 2001, 12.)

Remote access VPN -yhteydessä yhdistetään yksittäinen työntekijä yrityksen verkkoon. Yleensä etäkäyttäjällä on jokin sovellus tai fyysinen laite, jolla yhteys luodaan yrityksen verkossa sijaitsevaan VPN -palvelimeen. VPN -palvelin voi olla esimerkiksi palomuuri. Etäkäyttäjä ottaa yhteyden palvelimeen käyttäen julkista IP -osoitetta. Jos yrityksessä on käytössä privaatti osoiteavaruus, saa käyttäjä yleensä siihen kuuluvan IP -osoitteen tiedon tunnelointia varten. (Perlmutter ym. 2001, 12.)

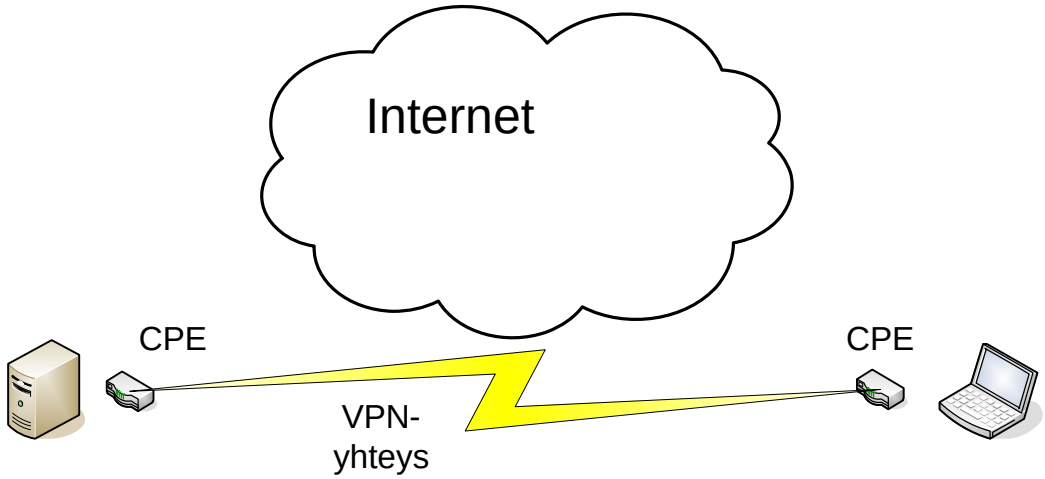


KUVIO 2. VPN -topologiat

Sekä käyttäjä että käytettävä kone on mahdollista tunnistaa. Käytettävän koneen tunnistukseen käytetään yleensä symmetristä avainta tai sertifikaattia. Käyttäjän tunnistus järjestetään yleensä käyttäjätietokannalla, johon otetaan yhteys käyttäen esimerkiksi RADIUS -protokollaa. Tarvittaessa suurempaa varmuutta käyttäjästä voidaan käyttää mm. kertakäyttöisiä salasanoja. (Authentication 2008.)

3 ERILAISET VPN -RATKAISUT

3.1 Kiinteät linjat



KUVIO 3. Kiinteälinjainen VPN -yhteys

Ennen internetin yleistymistä, yritykset vuokrasivat yleensä paikalliselta puhelinyhtiöltä puhelinkaapelipareja käyttöönsä, kahden toimipisteen tai toimipisteen ja etäkäyttäjän välille. Tähän oli yleensä kaksi mahdollisuutta, kiinteäkanavainen tai kanavoitu T1/E1 (nopeudet 1,544 Mbit/s ja 2,048 Mbit/s), jotka molemmat muodostavat omia fyysisiä verkkoja. Tällöin fyysiset verkot eivät ole osoitettavissa mistään julkisesta verkosta esimerkiksi internetistä kuvion 3 osoittamalla tavalla. Tällöin kyseessä on oikeasti yksityinen verkko. Kyseessä on nk. kultainen standardi, johon muita VPN -yhteyksiä pitäisi verrata. (Perlmutter ym. 2001, 35.)

Lisäksi T1/E1 -yhteys tarjoaa jatkuvatasoisen yhteyden eli käytettävissä oleva kaistanleveys ja viive ovat aina vakioita. Tämä on toinen kultainen standardi, johon muita VPN -palveluita tulisi verrata. (Perlmutter ym. 2001, 35.)

Käytettäessä kiinteäkanavaista yhteyttä tarvitaan kaksi fyysistä yhteyttä, kaksi CSU/DSU -yksikköä (Channel Service Unit/Data Service Unit) ja kaksi porttia verkkoreitittimessä. CSU/DSU -yksikön tehtävä on T1/E1 linjalle ajoitus synkronointi ja kehystäminen sekä signaalien muunto dataksi. Kanavoitua yhteyttä käy-

tettäessä riittää yksi fyysinen yhteys, yksi CSU/DSU ja yksi portti verkkoreitittimessä. Se, käytetäänkö kiinteäkanavaista vai kanavoitua yhtyettä riippuu, operaattorin tavasta tarjota yhteys. (Perlmutter ym. 2001, 38.)

Suuressa mittakaavassa käytettynä T1/E1 -linjat tulevat kalliiksi. Siksi nykyään kiinteitä linjoja toimitetaan eritasoisina DSL -linjoina, koska ne ovat operaattoreille ja yrityksille kustannustehokkaampia sekä helpompia toteuttaa. Suurempaa kaistanleveyttä tarvitseville tarjotaan mm. MPLS -yhteyksiä (Multiprotocol Label Switching). (Perlmutter ym. 2001, 40.)

3.2 Pakettikytkentäiset verkot

Vuonna 1976 määritettiin ensimmäinen pakettikytkentäinen yhteys X.25. X.25 on protokolla, joka määrittelee yhteyden DCE- (Data Terminal Equipment) ja DTE -laitteiden (Data Communications Equipment) välille. X.25 -verkoissa DCE -laite sijaitsee reitittimessä ja DTE -laite palveluntarjoajalla X.25 -yhdysvaihteessa. Yhteyksiä reitittää pilven sisällä DSE (Data Switching Equipment). (Perlmutter ym. 2001, 41.)

X.25 -verkon fyysiset kaapeloinnit ovat kaikille verkon käyttäjille (yrityksille) samat. Fyysisen yhteyden sisällä voidaan kuitenkin luoda virtuaalisia piirejä eri toimipisteiden välille. Virtuaaliset piirit näyttävät käyttäjälle samalta, kuin galvaanisesti erotettu yhteys. VC:t (Virtual Circuit) eli virtuaaliset piirit voivat olla väliaikaisia SVC (Switched Virtual Circuit) tai pysyviä PVC (Permanent Virtual Circuit). Yleensä yrityksellä on keskeisellä paikalla suurella nopeudella varustettu päätepiste, johon kaikki X.25 virtuaaliset piirit päättyvät. (Perlmutter ym. 2001, 42.)

X.25 verkoissa, ja muissa virtuaalipiirejä luovissa verkoissa, kuten Frame Relay:ssä, operaattori on vastuussa siirrettävän tiedon reitittämisessä pakettitasolla pilven läpi. Siirtyminen virtuaalisiin piireihin oli askel kustannustehokkaampaan liikennöintiin, koska operaattori kykeni nyt vuokraamaan samaa fyysistä kaapelointia useammalle yritykselle. (Perlmutter ym. 2001, 43.)

3.3 Puhelinverkko

PSTN (Public Switched Telephone Network) on laajasti käytetty tapa toteuttaa yksittäisen etäkäyttäjän yhteys yrityksen sisäverkkoon. Yhteys luodaan käyttäjän oman modeemin ja yrityksen modeemin välille, käyttämällä DUN -sovellusta (Dial-Up Networking) ja PPP -protokollaa (Point-to-Point Protocol). Kun PPP-yhteys saadaan muodostettua, voidaan PPP -yhteyden yli käyttää haluttua tiedonsiirtoprotokollaa liikennöimiseen (esimerkiksi IP). (Perlmutter ym. 2001, 41, 71.)

Modeemin tehtävä PSTN -verkossa on muuntaa digitaalinen datasignaali analogiseksi signaaliksi puhelinkaapelissa tapahtuvaa siirtoa varten. Analogisen modeemin tilalla voidaan käyttää myös ISDN, DSL tai kaapelimodeemia. (Perlmutter ym. 2001, 41, 71.)

3.4 IPsec

IPsec (Internet Protocol Security) on nykyaikainen tapa suojata liikennettä käytettäessä julkista verkkoa, esimerkiksi internetiä. IPsec ei ole itsessään protokolla vaan protokollakokoelma. Protokollien tehtävänä on tunneloida liikennettä tietoverkossa. IPsec on käyttäjälle toiminnoiltaan läpinäkyvä, ja sen tehtävä on suojata kaikki IPsec -protokollaa käyttävät yhteydet. (Perlmutter ym. 2001, 106.)

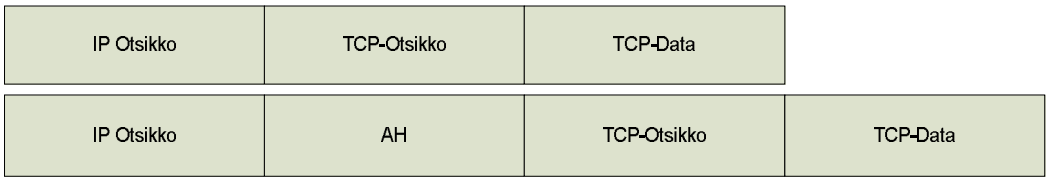
IPsec:n määritti ensimmäisen kerran IETF (Internet Engineering Task Force) vuonna 1995 RFC dokumentissa 1925. IPsec oli ensimmäinen määrittely, jonka avulla laitevalmistajat kykenivät tekemään laitteistoriippumattoman toteutuksen salatusta yhteydestä. IPsec koostuu kolmesta perustekijästä: todennus, salaus ja avaimenhallinta. Avaintenhallinta on toimenpide, jossa käytettävät salausavaimet neuvotellaan tai sovitaan yhteysosapuolten välillä. IPsec todentaa vain koneen, ei käyttäjää. (Perlmutter ym. 2001, 106.)

IPsec ei pakota käyttäjää tiettyyn toimintatapaan, vaan tarjoaa ainoastaan toiminnalle kehykset. Kehyksien sisällä on vaihtoehtoja käytettävien algoritmien ja para-

metrien osalta. Parametrien ja algoritmien on kuitenkin kohdattava yhteyden molemmissa päissä, jotta yhteys toimisi. (Perlmutter ym. 2001, 106.)

IPsec:llä on kaksi vaihtoehtoista toimintatapaa: tunnelointi (tunnel mode) ja kuljetus (transport mode). Tunnelointitilassa alkuperäinen IP -paketti paketoidaan uuden IP -paketin sisään, jossa on käytössä IPsec. Kuljetustilassa IP -pakettiin lisätään ainoastaan salausotsikko. Tunnelointitilaa voi käyttää esimerkiksi privaattiverkkojen osoitteilla, kun taas kuljetustilassa voi ainoastaan liikennöidä lopullisten pakettien vastaanottajien välillä. Toimintatavasta riippumatta IPsec luo aina verkkokerroksella toimivan yhteyden. (Perlmutter ym. 2001, 107.)

3.4.1 IPsec -tunnistusotsikko



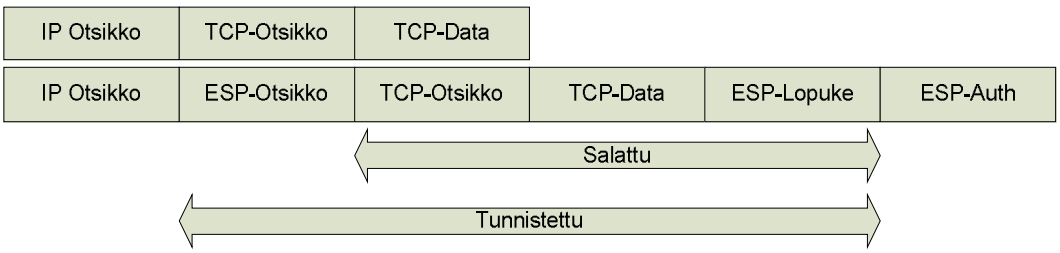
KUVIO 4. IP -viesti ennen ja jälkeen AH-otsikon lisäämistä

IPsec lisää normaaliin IP -kehykseen kentän AH (Authentication header), kuvion 4 mukaisesti. Tämän lisäksi IP -otsikon protokolla kentän arvoksi tulee 51, joka ilmaisee käytössä olevan IPsec tunnistusotsikon. Tunnistusotsikon tehtävä on tarkistaa paketin eheys ja estää paketin uudelleen lähetys tilanteessa, jossa paketti on kaapattu. AH ei salaa liikennettä. (Comer 2000, 584, 585.)

0-7 bit	8-15 bit	16-23 bit	24-31 bit
Seuraava otsikko	Hyötytiedon pituus	Varattu	
SPI			
Järjestysnumero			
Tunnistautumistieto (Vaihteleva)			

KUVIO 5. AH -tunnisteotsikko

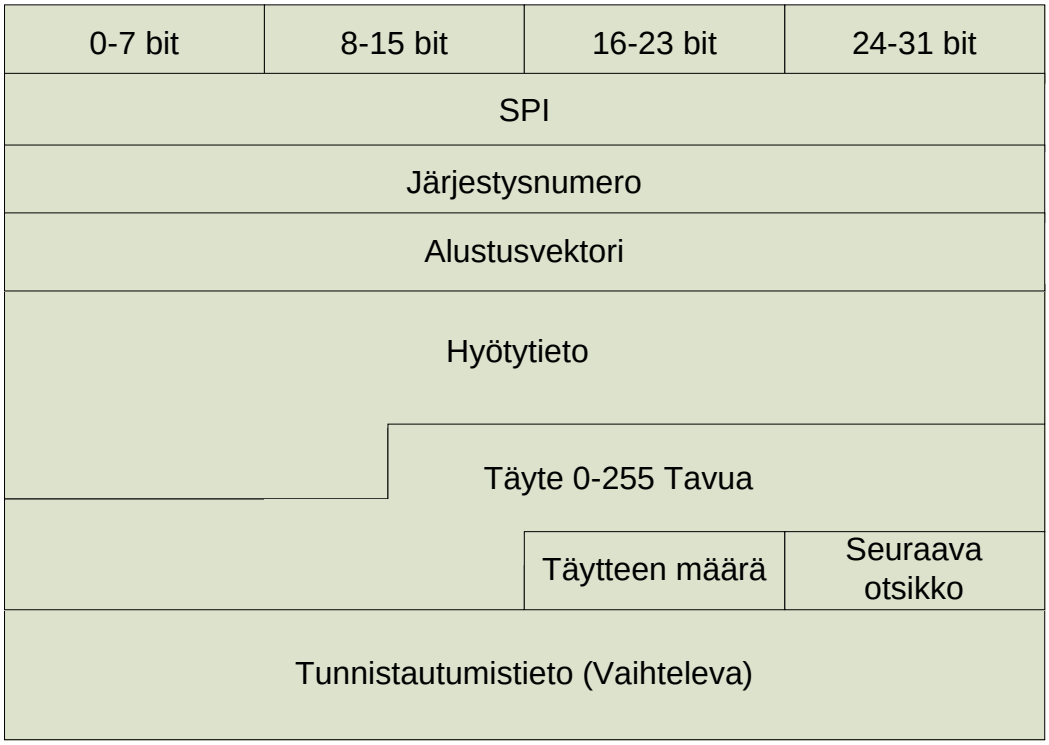
3.4.2 IPsec -salausotsikko



KUVIO 6. IP -viesti ennen ja jälkeen ESP -otsikon lisäämistä

Koska AH tarjoaa vain laillisuustarkistuksen, tarvitaan tiedon muuhun suojaamiseen toimivaa menettelyä. IPsec käyttää tähän tarkoitukseen ESP -protokollaa, (Encapsulating Security Payload) kuvion 6 osoittamalla tavalla. Käytettäessä ESP:tä IP -otsikon protokollakentän arvoksi tulee 50. ESP -protokolla salaa tiedon ESP -otsikon ja ESP -lopukkeen välillä. Lisäksi ESP suorittaa tiedon eheystarkistuksen. (Comer 2000, 586.)

Käytettävä salaus riippuu asetetusta suojaussidoksesta, valittavana voi olla mm. DES, 3-DES ja AES. Lisäksi ESP toteuttaa vähintään seuraavat eheystarkistusalgoritmit: HMAC MD5 ja HMAC SHA-1. (Comer 2000, 588.)



KUVIO 7. ESP -salausotsikko

3.4.3. IPsec suojaussidos ja suojausparametrien indeksi

Suojaussidos on IPsec -yhteyden sydän. Suojausparametrien indeksi eli SPI (Security Parameter Index), määrittää eheystarkistusalgoritmin, salausalgoritmin, algoritmin avaimen tai avaimet, avaimien voimassaoloajat, sen kuinka kauan valittu algoritmi on validi ja luettelon IP -osoitteista, joilla on järjestelmään käyttöoikeus. Nämä tiedot eivät mahdu otsikkotietoihin, vaan ne kerätään suojaussidokseen eli SA:han (Security Association). Jokaiselle SA:lle annetaan oma järjestysnumero, jota kutsutaan suojausparametrien indeksiksi. (Comer 2000, 585.)

IPsec -yhteyden toimintakuntoon saattaminen vaatii molemmilta osapuolilta tiedon käytettävästä suojausparametrin indeksistä. Liikenteen ollessa kaksisuuntaista, tarvitaan suojausparametrien indeksejä kaksi kappaletta, yksi molempiin suuntiin. Lisäksi jos käytössä on sekä AH että ESP, tarvitaan molemmille protokollille omat indeksinsä, jolloin niiden määrä nousee neljään. Suojausparametrin indeksin arvoja ei ole yleisesti määrätty vaan suojausparametrinindeksi yksilöidään kohteen mu-

kaan. Viestin lähettäjä tallentaa käytettävän suojausparametrin indeksin kehyksen SPI -kenttään, kuvion 7 mukaisesti. (Comer 2000, 586.)

3.4.4 IPsec -avaintenvaihto

IPsec -protokollan avaimenvaihtoprotokollana toimii yleensä IKE (Internet key exchange). IKE:n tehtävä on neuvotella käytettävät suojaussidokset. IKE ei kuitenkaan välitä liikennöintiin osallistuvien laitteiden luottosuhteista vaan olettaa, että luottosuhteet ovat jo olemassa. (Harkinsen, D & Carrel, D. 2008, 1.)

IKE on toiminnaltaan hybridi protokolla, sillä IKE toteuttaa aikaisemmin avaintenvaihtoon käytetyt ISAKMP (Internet Key Exchange and Key Management Protocol), Oakley ja SKME protokollat. Koska media, jolle IPsec yhteyttä ollaan useimmiten luomassa, on yleensä luonteeltaan turvaton esimerkiksi internet, täytyy avainten turvalliseen vaihtoon kiinnittää erityishuomiota. Tähän tarkoitukseen IKE käyttää epäsymmetristä Diffie-Hellman protokollaa. Protokollan avulla yhteyden osapuolet neuvottelevat yhteisen symmetrisen salausavaimen. IKE:n käyttö mahdollistaa myös sertifikaattipohjaisen tunnistuksen käytettäville laitteille. (Harkinsen, D & Carrel, D. 2008, 1.)

3.4.5 IPsec VPN

IPsec -yhteys sisältää aina kaksi osapuolta: lähettäjän ja vastaanottajan. Lähettäjän ja vastaanottajan suhdetta kutsutaan turvallisuusliitoksi. Turvallisuusliitto luodaan osoittamalla lähettäjälle ja vastaanottajalle yhteyttä suojaavat avaimet. Ne voidaan luoda, joko staattisesti tai dynaamisesti, käyttäen jotakin IPsec:n tuntemaa avaintenvaihtoprotokollaa. Heti avaintenvaihdon jälkeen turvallisuusliitto on luotu. IPsec turvallisuusliitto tarjoaa aina yhteyden OSI -mallin verkkokerroksella. (Perlmutter ym. 2001, 109.)

Käytettäessä AH -tunnisteotsikkoa tiedon lähettämisessä lähettäjä allekirjoittaa sovitulla avaimella jokaisen paketin. Allekirjoitettu paketti voidaan tulkita oikeaksi vain vastaanottajan avaimella. Jos käytössä on ESP, viesti lisäksi salataan jollakin sovitulla algoritmilla. Vastaanottaja ajaa algoritmit käänteisessä järjestyksessä, jolloin tuloksena on selväkielinen paketti. Tunnisteotsikkoa käytettäessä ei IPsec VPN pääse NAT:n läpi, koska AH suorittaa eheystarkistuksen myös IP osoitteille. (Perlmutter ym. 2001, 109, 110.)

IPsec voidaan toteuttaa ohjelmallisesti tai rautapohjaisesti. Yleensä ohjelmistopohjainen sovellus on käytössä etäkäyttäjän tietokoneessa, jolla otetaan yhteys yrityksen rautapohjaiseen IPsec -palvelimeen. Yritysten välisissä yhteyksissä IPsec muodostetaan yleensä rautapohjaisella toteutuksella. Jos vastaanottajalla on useita yhtäaikaisia IPsec -liittoja, joutuu vastaanottaja huolehtimaan yhteyskohtaisesti avaimista ja algoritmeista. Useiden yhtäaikaisten istuntojen ylläpito voi käydä laitteistolle raskaaksi. (Perlmutter ym. 2001, 111, 112.)

IPsec on erittäin joustava protokolla. Siinä on sisäänrakennettu salaus, mutta on hyvin joustava toteutuksen suhteen. IPsec ei määrää tiettyä salausalgoritmia vaan ainoastaan formaatin, mitä salausotsikko käyttää. Tämän ansiosta on helppo tehdä sovelluksia, sekä rautapohjaisia toteutuksia, jotka toimivat laitteistoriippumattomasti yhteen. Tämän lisäksi IPsec on integroitu syvälle yleisesti käytössä olevaan IP -protokollaan, joka lisää IPsec -protokollan käyttöönoton helppoutta. (Perlmutter ym. 2001, 113.)

Syvästä IP -protokollan integraatiosta johtuen IPsec:n käyttö muiden verkkoprotokollien käyttö ei ole optimaalista. Tällöin suojattava liikenne on ensin tunneloitava IP -pakettiin ennen turvallista siirtoa. Lisäksi standardoinnista huolimatta yhteensopivuusongelmia esiintyy eri laitevalmistajien IPsec -toteutusten välillä. IPsec ei myöskään todenna muuta kuin käytettävän laitteiston. Käyttäjän tunnistukseen on käytettävä jotakin muuta menetelmää. (Perlmutter ym. 2001, 113.)

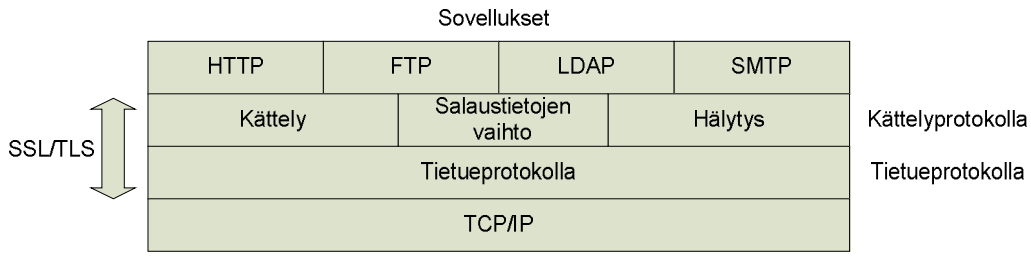
Ylläpidolle IPsec:n käyttö vaatii useita asiakasohjelmistojen asentamista ja ylläpitoa. Lisäksi ongelmia tuottavat IPsec:n yhteensopivuusongelmat NAT:n (network

address translation) kanssa. Lisäksi luotu yhteys on aina verkkokerroksella, joka on otollinen reitti madoille ja viruksille yrityksen sisäverkkoon. (Perlmutter ym. 2001, 115.)

3.5 SSL/TLS

SSL (Secure Socet Layer) protokollan kehitti Netscape Communications Corporation vuonna 1994, SSL kehitettiin alkujaan suojaamaan HTTP -protokollan (Hypertext Transfer Protocol) yhteyksiä HTTP -palvelimien ja WWW-selainten (World Wide Web) välillä. SSL -protokolla toimii OSI -mallin neljännellä kerroksella. Tästä johtuen sitä voidaan käyttää minkä tahansa TCP -protokollaa (Transmission Control Protocol) käyttävän liikenteen suojaamiseen, kuten SMTP (Simple Mail Transfer Protocol) tai LDAP (Lightweight Directory Access Protocol). (MicrosoftTechnet 2008.)

Myöhemmin IETF aloitti samantapaisen protokollan kehittämisen, jonka pohjana käytettiin SSL versiota 3.0. Tästä syntyi TLS -protokolla (Transport Layer Security). Erot SSL 3.0 ja TLS 1.0 välillä ovat pienet. SSL käyttää tiedon eheyden tarkistamiseen MAC -algoritmia ja TLS HMAC -algoritmia. Vaikka erot ovat pieniä, protokollat eivät toimi yhteen. (MicrosoftTechnet 2008.)



KUVIO 8. SSL/TLS -protokollan sijainti

TLS -protokolla koostuu kahdesta osasta, kättelyprotokollasta (Handshake Protocol) ja tietueprotokollasta (Record Protocol), kuvion 8 mukaan. Alemman tason protokollana käytetään jotakin yhteydellistä protokollaa. Tietueprotokollan tehtä-

vänä on tarjota yhteyden salaaminen ja fragmentointi. Kättelyprotokollan tehtävä on yhteyden muodostaminen sekä ylläpito. (Dierks, T. & Allen, C. 2007, 2.)

3.5.1 SSL/TLS -tietueprotokolla

Tietueprotokollalla on kaksi päätehtävää, tiedon eheyden tarkistaminen ja suojaaminen jollakin salausalgoritmilla. Molemmat tehtävät ovat valinnaisia. Käytettävät salausalgoritmit voivat olla joko symmetrisiä tai epäsymmetrisiä. Algoritmien avaimet luodaan aina yhteyskohtaisesti, ne ovat aina ainutlaatuisia. Avaimien neuvotteluun ei kuitenkaan käytetä tietueprotokollaa vaan yleensä TLS -tietueprotokollan kättelyprotokollaa. (Dierks, T. ym. 2007, 13.)

Eheyden tarkistamiseen käytetään HMAC- tai MAC -avaimellista tiivistefunktiota, joissa on mahdollista käyttää tiivisteen tekoon MD5- tai SHA -algoritmeja. Tämän lisäksi tietueprotokollaa käytetään ylemmiltä kerroksilta tulevan tiedon fragmentoimiseen. (Dierks, T. ym. 2007, 13.)

3.5.2 SSL/TLS -kättelyprotokolla

Kättelyprotokolla mahdollistaa yhteyden osapuolten välisen tunnistuksen, käytettävän salausalgoritmin ja symmetristen avainten neuvottelun. Lisäksi TLS kättelyprotokollalla ilmoitetaan tapahtuneista virheistä. TLS kättelyprotokolla on jaettu kolmeen pienempään protokollaan: salaustietojen vaihto (Change cipher spec), hälytys (Alert) ja kättely (Handshake). (Dierks, T. ym. 2007, 23.)

Kättelystä syntyvä istunto koostuu seuraavista osista. Nämä tiedot annetaan tietueprotokollalle, jonka tehtävänä on toteuttaa liikennöinti laitteiden välillä.

- istunnon tunnus
- osapuolten sertifikaatit (eivät ole pakollisia)

- tiedon pakkaustapa
- käytettävä salausalgoritmi
- salausalgoritmin avain
- tieto siitä, saako avatulla yhteydellä luoda uusia yhteyksiä

Kättelyprotokollaa käytetään vaihtamaan istuntokohtaista tietoa palvelimen ja asiakkaan välillä. Kättelyprotokollan käyttö on ensimmäinen vaihe muodostettaessa SSL/TLS -yhteyttä. Yhteyden avauksessa sovitaan käytettävän protokollan versio, salausalgoritmit, vaihtoehtoinen tunnistus ja salausavaimet. (Dierks, T. ym. 2007, 29.)

Tiedon salaamiseen SSL/TLS käyttää sekä symmetrisiä, että epäsymmetrisiä avaimia. Tiedonsiirtoon käytetään symmetrisiä avaimia, koska ne vaativat vähemmän laskentatehoa. Epäsymmetrisiä avaimia käytetään yhteyden osapuolten tunnistamiseen. Tiedon eheyden tarkistamiseen käytetään, joko HMAC- tai MAC -algoritmia. (Dierks, T. ym. 2007, 30.)

SSL/TLS -protokolla käyttää salausavaimien vaihtoon salausavaimien vaihtoprotokollaa. Protokolla koostuu ainoastaan yhdestä viestistä, jonka sisältönä on tieto siitä, kumpi osapuoli haluaa avainta vaihtaa. Uudet avaimet lasketaan informaatiosta, joka vaihdetaan kättelyprotokollalla. (Dierks, T. ym. 2007, 30.)

Virheiden ilmoitukseen SSL/TLS käyttää erillistä hälytysprotokollaa. Protokollan tehtävänä on lisäksi ilmoittaa yhteyden tilassa tapahtuvista muutoksista. Hälytysprotokollan toiminta on yksinkertainen. Virheen tapahtuessa virheen havainnut osapuoli lähettää viestin toiselle osapuolelle. Jos tapahtunut virhe on laadultaan vakava, yhteys katkaistaan välittömästi. Vakavan virheen sattuessa yhteyden osapuolet unohtavat välittömästi yhteyden parametrit. Mahdollisia virheitä ovat virheelliset sertifikaatit ja virheelliset eheystarkistukset. (Dierks, T. ym. 2007, 32.)

3.5.3 SSL/TLS yhteyden muodostus

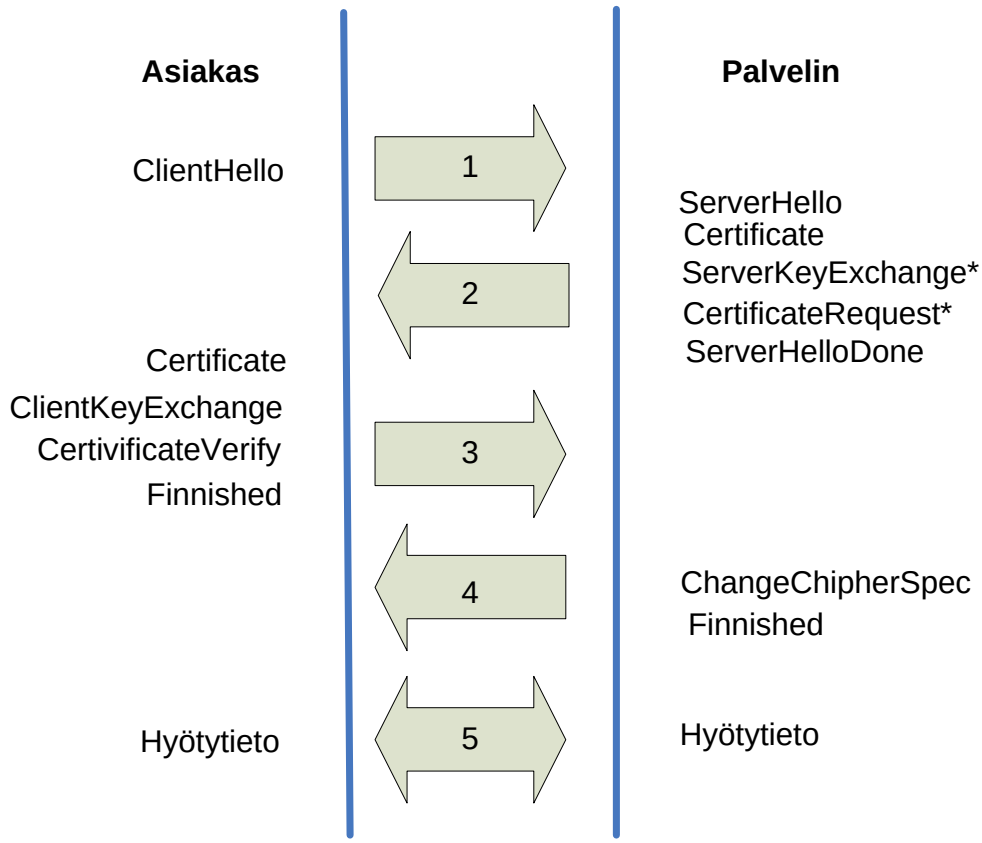
SSL/TLS -yhteyden alussa suoritetaan kättely, jossa vaihdetaan luotavan yhteyden kannalta kriittistä tietoa. Kättelyn suorittaa kättelyprotokolla kuvion 9 mukaisesti. Yhteyden avaaminen on jaettu erilaisiin vaiheisiin: jokaisessa vaiheessa siirretään viestejä asiakkaan ja palvelimen välillä. Kättelyn päätyttyä voidaan tietoa lähettää osapuolten välillä. (Wyler, Fausett, Fletcher, Foxhoven, Lucas, Miller, Peterson & Woodberg B. 2007 17.)

Yhteyden neuvottelu alkaa, kun asiakas lähettää Client Hello -viestin. Tähän palvelimen on vastattava Server Hello -viestillä tai yhteys katkaistaan. Asiakkaan Client Hello -viesti sisältää seuraavat asiat, tuetut protokollat ja versiot (SSL/TLS), tuetut salausalgoritmit, tuetut tiivistysalgoritmit, istunnon tunnuksen, ja satunnaista tietoa salausavainten luontia varten. Uuden istunnon tunnus on 0. Palvelin vastaa tähän viestiin määräämällä käytettävän protokollan, salausalgoritmin, istunnon tunnuksen, tiivistysalgoritmin ja satunnaista tietoa salausavainten luontia varten. (Wyler, ym. 2007 17.)

Seuraavassa vaiheessa palvelin lähettää oman sertifikaattinsa, johon asiakas vastaa lähettämällä omansa sitä vaadittaessa. Molempien osapuolten sertifikaatit ovat kuitenkin valinnaisia. Server Key Exchange -viestiä käytetään vain, jos palvelimella ei ole käytössä sertifikaattia. Viestin sisältönä on palvelimen julkinen avain, jota voidaan käyttää salausavaimena. Vaihe on valmis, kun molempien osapuolten sertifikaatit on lähetetty. Vaihtoehtoinen asiakkaan sertifikaatti tarkistetaan käyttämällä Certificate Verify -viestiä. Tämä tapahtuu salaamalla sertifikaatti asiakkaan salaisella avaimella, jonka palvelin avaa asiakkaan julkisella avaimella. (Wyler, ym. 2007, 17.)

Client Key Exchange-viesti lähetetään aina. Viestin avulla siirretään yhteyttä salaava symmetrinen avain osapuolten välillä käyttäen joko Diffie-Hellman tai RSA menettelyä. (Wyler, ym. 2007, 17.)

Lopuksi asiakas lähettää Change Chipher Spec -viestin, jonka jälkeen seuraa Finnished -viesti, joka kertoo kättelyn päättymisestä. Palvelin vastaa lähettämällä oman Change Chipher Spec -viestinsä ja tämän jälkeen välittömästi oman Finnished -viestinsä. Lähetettyään Change Chipher Spec -viestin, lähettäjä aloitta sovittujen suojaus parametrien käyttämisen. Finnishe -viestit ovat siis ensimmäiset salatut viestit, alussa neuvotelluilla parametreilla. Kättelyprosessi on valmis ja liikennöinti voi alkaa. (Wyler, ym. 2007, 17.)



Kuvio 9. SSL/TLS yhteyden muodostaminen

3.5.4 SSL VPN

SSL VPN on aina valmistajakohtainen toteutus, joka käyttää hyväkseen SSL/TLS -protokollan toimintaa. SSL VPN ei välttämättä tarvitse toimiakseen erillistä ohjelmistoa asiakkaalla vaan sitä voidaan käyttää usein WWW-selaimella. Tästä johtuen SSL VPN -yhteys voidaan luoda yrityksen sisäverkonpalveluihin mistä tahansa,

ainoa vaatimus on internet yhteys. SSL VPN -tekniikalla ei yleensä luoda toimipisteiden välisiä yhteyksiä. (Steinberg & Speed, 2005, 33.)

VPN -yhteydessä käytettään SSL/TLS -tekniikan osittaisesta riittämättömyydestä johtuen alijärjestelmiä. Alijärjestelmillä tarjotaan sovelluskohtaisia yhteyksiä ja asiakaskoneen tietoturvan tarkistamiseen liittyviä palveluita. Tietoturvan tarkistaminen on tarpeellista, koska SSL VPN -yhteys mahdollistaa laitteiden välisten luottamussuhteiden luomisen lennosta. Alijärjestelmällä voidaan mm. tarkistaa onko asiakaskoneessa vaadittavat virustorjuntasovellukset, tämän lisäksi voidaan poistaa istunnon aikana syntyneet, välimuistiin päätyneet tiedot. Jos asiakkaan tietokone ei saavuta vaadittua tietoturvatasoa, voidaan joko evätä yhteys tai sallia vain osa VPN -yhteyden takaa tarjottavista palveluista. Tällä voidaan ehkäistä asiakaskoneessa olevin mahdollisten matojen tai viruksien pääsyä sisäverkkoon. Käyttäjän tunnistukseen valmistajat tarjoavat valmiita rajapintoja esim. sertifikaatteja ja kertakäyttöisiä salasanoja. (Steinberg ym. 2005, 70, 74.)

Yhteyden muodostamiseksi yrityksen verkon palveluihin käytetään kahta tekniikkaa, sovelluskohtaisia yhteyksiä tai suoraan verkkokerroksella tapahtuvaa yhteyttä yrityksen aliverkkoon. Yhteyksien muodostaminen vaatii yleensä ohjelman asennuksen asiakkaan koneeseen. Ohjelmistot asentavat itsensä yleensä automaattisesti, mutta vaativat usein käyttäjältä järjestelmänvalvojaoikeudet. Tilanne voidaan kuitenkin kiertää asentamalla vaadittavat ohjelmat etukäteen. Asennuksen jälkeen ohjelmat heräävät automaattisesti, kun SSL VPN -palvelut niitä tarvitsevat. Palveluihin pääsyä voidaan rajata usein SSL VPN -palvelinpään ohjelmistossa erilaisilla rooleilla, jolloin erillistä palomuuria ei välttämättä tarvita yhteyksiä rajoittamaan. (Steinberg ym. 2005, 41.)

Sisäverkossa sijaitseviin HTTP -palveluihin yhteydet tarjotaan käyttämällä reverse proxy-tekniikkaa. Reverse proxy on palvelin, joka asennetaan SSL VPN -palvelinpäähän. Palvelimen tehtävänä on kuunnella HTTP ja HTTPS -protokollaa, sekä poimia siitä yrityksen sisäverkkoon menevät paketit, jotka palvelin reitittää edelleen oikeisiin osoitteisiin. Reverse proxy ei kuitenkaan toimi kuin HTTP- ja HTTPS -protokollien kanssa. (Steinberg ym. 2005, 45.)

Sovelluskohtaisia yhteyksiä varten tarjotaan yleensä porttien uudelleenohjausta (port forwarding). Tämä vaatii pääsääntöisesti asiakaskoneeseen asennettavan ohjelman, joka on yleensä toteutettu, joko ActiveX- tai Java -tekniikalla. Asennettavan ohjelman tehtävän on kuunnella asiakaskoneella tiettyä kohdeosoitetta ja porttia. Kun liikennettä havaitaan, lähetetään tieto SSL/TLS -tunnelin lävitse oikeaan osoitteeseen yrityksen sisäverkossa. Ongelmia voivat tuottaa sovellukset, jotka käyttävät dynaamisia portteja. (Steinberg ym. 2005, 47.)

Yhteyksien tuottamiseksi verkkokerroksella suoraan yrityksen sisäverkkoon käytetään kahta tekniikkaa: full tunneling ja split tunneling. Kuten edellä, palvelut tarjotaan erillisellä asennettavalla ohjelmistolla. Full tunneling -tilassa kaikki liikenne asiakkaan koneesta reititetään SSL VPN -palvelimen kautta. Split tunneling tilassa vain ennalta määrätyt verkot reititetään SSL VPN -palvelimelle. (Steinberg ym. 2005, 48.)

Verkkokerroksella yhteyden luova ohjelmisto voi asentaa virtuaalisen verkkokortin ja muokata reititystauluja, jolloin oikeat verkot reititetään virtuaalisen verkkosoittimen kautta yrityksen sisäverkkoon. Koska tarjottava palvelu toteutetaan verkkokerroksella, tällöin koko TCP/IP -protokolla on käytössä. Tämä vaatii asiakaskoneelle oikeanlaisen IP -osoitteen, joka yleensä saadaan sisäverkon DHCP -palvelimelta (Dynamic Host Configuration Protocol) tai erikseen SSL VPN -palvelimeen määritellystä osoitealueesta. (Steinberg ym. 2005, 48.)

SSL VPN -palvelun suurin etu on järjestelmän saavutettavuus mistä tahansa. Suurin murhe ovat mahdolliset tietoturvariskit käytettäessä etukäteen varmentamattomia tietokoneita. Lisäksi DoS (Denial of Service) -hyökkäykset saattavat aiheuttaa riskin, sillä SSL/TLS -protokolla sijaitsee korkealla OSI -mallissa, jolloin pakettia ei voida tiputtaa jo alemmilla kerroksilla. (Steinberg ym. 2005, 74.)

Ylläpidon kannalta SSL VPN on helppo ratkaisu, koska järjestelmä ei välttämättä vaadi asiakasohjelmistojen ennakkoon asentamista. Tietokoneen turvatason tarkistavien ohjelmien avulla on mahdollista estää turvattomien koneiden pääsy sisäverkon palveluihin. Lisäksi käyttämällä sertifikaatteja voidaan luoda ennakkoon luot-

tosuhteita tietokoneisiin, tällöin on mahdollista sallia vain sertifikaatillisten tietokoneiden yhteydet sisäverkkoon. Lisäksi käyttäjän tunnistukseen on usein mahdollista käyttää kertakäyttöisiä salasanoja.

4 TUNNISTAUTUMINEN

4.1 Sertifikaatit

PKI (Public-Key Infrastructure) eli julkisen avaimen infrastruktuuri on järjestelmä, jolla tietoverkoissa suojataan tietoa kryptograafisin menetelmin. PKI:n avulla voidaan varmistua viestin lähettäjän oikeellisuudesta, tiedon eheydestä ja lisäksi tieto voidaan tarvittaessa salata. PKI -järjestelmässä käyttäjien ja koneiden oikeellisuus todistetaan kolmannen osapuolen kautta, johon molemmat osapuolet luottavat. (PKI 2008.)

Yleisesti käytetty PKI -toteutus on ITU-T:n X.509, joka käyttää toimintaansa digitaalisia sertifikaatteja. X.509 on muodoltaan puumainen. Siinä luottamus luodaan puun juuressa ja jaetaan verkon käyttäjille. Järjestelmässä on sekä yksityisiä, että julkisia avaimia, jokaisella sertifikaatin omaavalla käyttäjällä on yksi kappale molempia. Yksityisellä avaimella suojatun tiedon voi avata julkisella avaimella ja julkisella avaimella suojatun viestin voi avata ainoastaan yksityisellä avaimella. Varmentaakseen viestin lähettäjän, osapuolten tulee käyttää toistensa julkisia avaimia. (X.509 2008.)

4.1.1 Certificate Authority

CA eli Certificate Authority on luotettu taho, joka varmistaa digitaalisella allekirjoituksella myöntämiensä sertifikaattien oikeellisuuden. CA allekirjoittaa sertifikaatteja juurisertifikaatin yksityisellä avaimella. Juurisertifikaatti voi olla CA:n itsensä allekirjoittama. CA:n julkisella juurisertifikaatilla voidaan todentaa kaikkien CA:n allekirjoittamien sertifikaattien oikeellisuus. (Certificate Authority 2008.)

CA:n myöntämät sertifikaatit sisältävät yksityisen ja julkisen avaimen, tiedot sertifikaatin omistajasta sekä sertifikaatin myöntäjästä. Tiedoista käy myös ilmi, minkä ajan sertifikaatti on validi. CA voi kirjoittaa sertifikaatteja monessa eri muodoissa, joista jokaiselle on omat käyttö kohteensa. (Certificate Authority 2008.)

4.1.2 Sertifikaatin kumoaminen

Yleisin syy sertifikaatin kumoamiseen on yksityisen avaimen paljastuminen. CRL (Certificate revocation list) on lista niistä sertifikaateista, jotka on kumottu. Listalla olevia sertifikaatteja ei tulisi hyväksyä. Jos CA:n käyttämän juurisertifikaatin yksityinen avain paljastuu, joudutaan uusimaan kaikki CA:n myöntämät sertifikaatit. (Certificate revocation list 2008.)

CRL -listalla oleva sertifikaatti voi olla kahdessa tilassa, kumottu tai odotustilassa. Kumotuista sertifikaateista ei voi tehdä uudestaan valideja. Sen sijaan odotustilasta on mahdollista tulla taas validi. Odotustilaan voi joutua, jos käyttäjä ei ole esimerkiksi varma yksityisen avaimen paljastumisesta. Listan kumotuista sertifikaateista tai oikeastaan niiden sarjanumeroista tuottaa CA. CA myös yleensä allekirjoittaa listan. (Certificate revocation list 2008.)

4.2 Kertakäyttöiset salasanat

Nykyään monet järjestelmät ovat luonteeltaan turvattomia. Pienellä vaivalla liikennettä pystyy salakuuntelemaan tai vaihtoehtoisesti asentamaan tietokoneeseen keylogger -ohjelman, joka lukee näppäimistöllä painettavat näppäimet. Käyttäjätunnusten ja salasanojen riski joutua vääriin käsiin on suuri, etenkin käytettäessä yrityksen verkkopalveluita internetistä käsin ja vieraalta tietokoneelta. Näitä uhkia vastaan on kehitetty käyttäjäntunnistusmenetelmiä, joissa käytettävät salasanat ovat kertakäyttöisiä. Tällöin verkon yli lähetettävä käyttäjänimi – salasana -pari ovat tiedon kaappaajille hyödyttömiä. (One-time Password 2008.)

Kertakäyttöinen salasana koostuu kahdesta osasta, käyttäjän tuntemasta salasanasta ja palvelimelta verkon yli saatavasta siemenestä. Käyttäjä laskee siemenestä ja salasanasta tiivisteen ja lähettää tiedon tunnistuspalvelimelle. Palvelin tuntee käyttäjän salasanan ja siemenen ja laskee niistä oman tiivisteen. Jos tiivisteet vastaavat, tunnistus on onnistunut. (Haller, N. Metz, C. Nesser, P. & Straw M. 2007, 13.)

Toinen tapa tuottaa kertakäyttöisiä salasanoja on käyttää ohjelmallisia tai rautatasolla toimivaa salasanageneraattoria. Salasanageneraattori on synkronoitu tunnistuspalvelimen kanssa, joten niissä on jatkuvasti sama salasananarvo. Salasanageneraattorista saamansa salasanan käyttäjä yhdistää henkilökohtaiseen salasanaansa. Tämän jälkeen käyttäjä laskee niistä tiivisteen ja lähettää saadun tuloksen tunnistuspalvelimelle. Palvelimella on tiedot, sekä käyttäjän salasanasta, että salasanageneraattorin tilasta, joista palvelin laskee vastaavan tiivisteen. Jos tiivisteet täsmäävät, tunnistus on onnistunut. (One-time Password 2008.)

Myös edellisten tekniikoiden yhdistelmä on mahdollinen. Siinä käyttäjällä on salasanageneraattori, johon on integroitu kiinteä siemen. Siemen on tiedossa palvelimella ja sitä ei lähetetä verkon ylitse. Kun käyttäjä lähettää oman henkilökohtaisen salasanansa ja generaattorin antaman salasanan palvelimelle, laskee palvelin omasta kellostaan ja käyttäjän siemenestä, mitä pitäisi salasanageneraattorissa olla. Tässä työssä käytettävät SecurID -varmistusavaimet, toimivat edellä kuvatulla tavalla. (SecurID 2008.)

5 PÄIJÄT-HÄMEEN KOULUTUSKONSERNIN ETÄKÄYTTÖRATKAISU

5.1 Yleistä Päijät-Hämeen koulutuskonsernista

Päijät-Hämeen koulutuskonserni on maakunnallinen koulutuksen järjestäjä, kehittäjä ja ylläpitäjä, johon kuuluvat Koulutuskeskus Salpaus, Lahden Ammattikorkeakoulu ja Tuoterengas. Laitokset tarjoavat toisen asteen ja ammattikorkeakoulutasoista koulutusta, kuntoutusta sekä työhön valmennusta.

Konsernin sisäisiä palveluyksiköitä ovat Yhteiset palvelut: Hallintopalvelut, Kirjasto- ja tietopalvelut, Kiinteistöpalvelut, Ravintolapalvelut ja Tietohallintopalvelut. Tämä lopputyö on toteutettu Päijät-Hämeen koulutuskonsernin Tietohallintopalveluille, joka on jakaantunut viiteen osaan: Tietojärjestelmäpalvelut, Verkkopalvelut, Infrapalvelut, Mikrotukipalvelut, sekä Puhelin- ja toimistopalvelut.

Tietohallinnon vastuualueeseen sisältyvät työasemat (n. 5 200 kpl), palvelimet (n. 100 kpl), verkon aktiivilaitteet (n. 400 kpl), käyttäjät (n. 20 000 kpl, joista opiskelijoita 18 000), lankapuhelinliittymät (n. 1 600 kpl), matkapuhelinliittymät (n. 850 kpl). ja verkkotulostimet (n. 600 kpl).

5.1.1 Etäkäyttöratkaisun tavoitteet

Tämän työn ensisijaisena tarkoituksena on toteuttaa opetushallinnollisiin tarpeisiin sopiva etätyöympäristö. Koska järjestelmän käyttäjillä on käytössään paljon luottamuksellista materiaalia, täytyy ratkaisun tekniseen turvallisuuteen kiinnittää erityistä huomiota. Koska käyttäjät ovat taidoiltaan eritasoisia, tulee järjestelmän olla helppokäyttöinen ja mielellään nojata aikaisempaan osaamiseen. Järjestelmän olisi hyvä omata myös hyvä liikkuvuus, jolloin käyttäjä ei ole sidoksissa vain yhteen fyysiseen paikkaan.

Päijät-Hämeen koulutuskonsernissa on useita kannettavia tietokoneita varustettuna eri käyttöjärjestelmillä, joilla järjestelmää tullaan käyttämään. Tämän vuoksi täytyy järjestelmän olla helposti ylläpidettävissä, seurattavissa ja tarvittaessa päivitettävissä. Lisäksi mahdollisista vikatilanteista järjestelmän pitäisi toipua nopeasti. Tavoitteena on myös erilaisten roolien luominen, joihin käyttäjiä voisi asettaa. Tällöin jokaiselle käyttäjälle ei tarjota kaikkia palveluja, vaan ainoastaan tarvittavat palvelut oikeille käyttäjille.

Toissijaisena tavoitteena on tulevaisuudessa korvata kiinteät ADSL -yhteydet koulutuskonsernin sisäverkkoon. Järjestelmän olisi myös hyvä soveltua mahdollisiin ylläpidollisiin tarpeisiin.

Usealla opetushallinnollisia järjestelmiä tarvitsevalla on kotona ADSL-yhteys. Siksi Internetin yli toimiva VPN -yhteys tarjoaa näihin tilanteisiin Päijät-Hämeen koulutuskonsernin kannalta kustannustehokkaan ratkaisun, koska tällöin ei tarvitse toteuttaa asiakkaan kotiin kiinteitä yhteyksiä. Vaihtoehdot työssä rajataan siis IPsec:llä toteutettavaan VPN -yhteyteen tai SSL/TLS -tekniikalla toteutettavaan VPN -yhteyteen.

5.1.2 IPsec VPN

IPsec -yhteyden etuna ovat valmiit luottosuhteet, koska protokolla tarvitsee käsin asennettavan ohjelman ja jolloin luottosuhteiden luominen tuntemattomiin koneisiin on lähes mahdotonta. Myös tekniikka on hyvin standardoitu, joka mahdollistaa periaatteessa eri laitevalmistajien VPN -toteutuksien yhteensopivuuden. Lisäksi Päijät-Hämeen koulutuskonsernilla on käytettävissään riittävä määrä VPN -lisenssejä, joten IPsec -toteutus on mahdollinen.

Huonona puolena IPsec -toteutuksessa on sen hallittavuus Päijät-Hämeen koulutuskonsernissa olemassa olevalla ohjelmistolla. Asiakaskoneen ohjelmistojen asentaminen staattisella konfiguraatiolla, etäyhteydellä on mahdollista. Staattisten asetusten muuttaminen tai mahdollisten vikatilanteiden selvittäminen vie kuitenkin

ylläpidolta paljon aikaa. Lisäksi yleisesti käytössä olevat NAT:n tekevät ADSL -modeemit haittaavat IPsec -liikennettä ja tuottavat lisätöitä ylläpidolle. Lisäksi asennettavat IPsec -ohjelmistot muokkaavat käyttöjärjestelmän TCP/IP pinoa.

5.1.3 SSL VPN

SSL/TLS -tekniikalla toteutetun VPN -ympäristön hyviä ominaisuuksia ovat keskitetty hallinta ja yleinen käytön helppous. Yhteys voidaan luoda mistä tahansa. Ainoa vaatimus on WWW-selain.

Päijät-Hämeen koulutuskonsernissa ei käyttäjillä pääsääntöisesti ole järjestelmävalvojatasoisia oikeuksia tietokoneisiin. Tarvittavat ohjelmat yhteyksien avaamiseen yrityksen sisäverkkoon on kuitenkin mahdollista asentaa etukäteen, jolloin niiden käyttäminen on mahdollista. Lisäksi sovellusten liikennettä tunneloivien ohjelmien liikennettä ei hallinnoida käyttäjän tietokoneelta käsin, vaan tarvittavat määritykset tulevat SSL VPN -palvelimelta.

Myös käyttäjien jako erilaisiin rooleihin on helposti toteutettavissa käytettäessä sertifikaatteja ja alijärjestelmiä. Tietoturvaa lisäävät kertakäyttöiset salasanat ovat yleensä helposti integroitavissa järjestelmään.

Suurimman ongelman aiheuttaa palvelun helppo saatavuus. Yhteys on mahdollista avata turvattomasta ympäristöstä, jolloin sisäverkon saastuminen on mahdollista. Tätä voidaan kuitenkin ehkäistä asentamalla sertifikaatit niihin koneisiin, joilta yhteydet sisäverkkoon sallitaan ja suorittamalla käytettävälle tietokoneelle ennakko tarkistuksia alijärjestelmillä. Turvallisuutta voidaan lisätä ottamalla käyttöön kertakäyttöiset salasanat. Tällöin voidaan ehkäistä käyttäjänimi – salasana -parien joutumista vääriin käsiin, käytettäessä esimerkiksi kioski-konetta.

5.1.4 IPsec vs. SSL VPN

TAULUKKO 1. SSL VPN ja IPsec vertailu

Ominaisuus	SSL VPN	IPsec
Yhteyksien hallinta	Ohjelmiston puitteet	Palomuurin puitteet
Sertifikaatti tunnistus	Kyllä	Kyllä
Hinta	n€	Jo olemassa oleva järjestelmä
Kertakäyttöiset salasanat	Kyllä	Kyllä
Käyttö	Käynnistyksen jälkeen selain-ikkunan oltava auki	Käynnistyksen jälkeen näkymätön
Käyttöympäristön tarkistus	Käyttäjän tietokoneen tarkistus ja sertifikaatit	Asennettava ohjelmisto, koneissa lisäksi sertifikaatit
Ongelmien ratkaisut	Useita työkaluja	lokit
Järjestelmän konfigurointi	WWW-selaimella	Komentoriviltä tai WWW-selaimella
Client/server sovellukset	Määritetään ohjelmakohtaisesti tai suora yhteys aliverkkoon	Suora yhteys aliverkkoihin
Salausalgoritmi	Riippuu WWW-selaimesta	Riippuvainen konfiguraatiosta
Käyttäjäryhmät	Sertifikaattien atribuutit	Eri konfiguraatiot eri asiakkaille

SSL VPN tarjoaa yhteyksien hallinnan WWW-selaimella käytettävään käyttöliittymän, kun taas Päijät-Hämeen koulutuskonsernissa tällä hetkellä käyttämätön IPsec -järjestelmää konfiguroidaan aina IPsec -yhteyksiä hallinnoivan palomuurin konsolista. Hallintanäkymällä ei kuitenkaan ole suurta merkitystä ylläpidon kannalta, koska pääpaino on hallintajärjestelmän toimivuudella, joka on molemmissa järjestelmissä hyvä.

Toinen tärkeä ominaisuus on mahdollisten vikatilanteiden selvittäminen ja vian korjaamisen helppous. SSL VPN -järjestelmät tarjoavat näihin valmiita työkaluja, kuten roolien jaon simuloimisen. Simuloimalla roolien jaon etukäteen, on mahdollista ennalta nähdä tulevat ongelmat, jolloin niihin voidaan varautua. Lisäksi tarjolla voi olla käyttäjän kirjautuminen ja roolijaon tallentaminen selkokielellä, jolloin mahdolliset virhetilanteet ovat helposti havaittavissa. Olemassa oleva IPsec -järjestelmä

osaa ainoastaan tuottaa palomuurin lokiin tietoa yhtyeksistä, josta on osattava tehdä päätökset virheen sijainnista.

Molemmissa järjestelmissä on tuki sekä sertifikaateille että kertakäyttöisille salasanoille. Ongelman aiheuttaa, kuitenkin IPsec -järjestelmän manuaalinen konfiguroinnin tarve liitettäessä sertifikaatti asiakasjärjestelmään, sillä IPsec -järjestelmä ei osaa lukea Windowsin sertifikaattitietokantaa, johon tarvittavat sertifikaatit on mahdollista asentaa keskitetysti. SSL VPN käyttää yleensä yhteyksien luomiseen WWW-selainta, eikä kärsi samasta ongelmasta, sillä sertifikaatit on mahdollista tallentaa keskitetysti Windowsin sertifikaattitietokantaan. IPsec -järjestelmän suurin etu on kuitenkin järjestelmän tarjoamat valmiit luottosuhteet, koska kyseessä on aina asennettava ohjelma. SSL VPN -järjestelmää voi sen sijaan käyttää lähes jokaisella WWW-selaimella.

Asiakkaan käytön kannalta IPsec -järjestelmä on helpompi, sillä IPsec -järjestelmä ei vaadi WWW-selaimen jättämistä taustalle. IPsec -järjestelmässä yhteyden luonnin jälkeen asiakasohjelmisto pienentyy Windows-käyttöjärjestelmän ilmaisualueelle. Seikka on kuitenkin vain esteettinen, sillä molemmat järjestelmät tarjoavat yhtä hyvät käyttömahdollisuudet Päijät-Hämeen koulutuskonsernin verkon resursseihin. Lisäksi SSL VPN -järjestelmällä voidaan sallia vain tietyt sovellukset tietyille henkilöille, IPsec -järjestelmässä tämä vaatisi suuria sääntölistoja, joiden hallittavuus on vaikeaa. IPsec -palvelu ei myöskään ole kaikkialta yhtä helposti saavutettavissa kuin SSL VPN, sillä asiakaspään palomuurisäännöt saattavat estää IPsec -liikenteen. SSL VPN -palvelu toimii porteissa, jotka ovat yleensä auki jokaisessa palomuurissa.

Koska Päijät-Hämeen koulutuskonsernilla on satoja potentiaalisia järjestelmän käyttäjiä, tulevat keskitetty hallinta ja helpot käyttäjien roolijaot tärkeään osaan valittaessa etäkäyttöjärjestelmää. IPsec -järjestelmä ei tarjoa tähän yhtä hyviä työkaluja, kuin SSL VPN -järjestelmä. IPsec -yhteys vaatii aina asiakaskoneeseen asennettavan ohjelmiston ja sen konfiguroinin. Lisäksi tulee huolehtia IPsec -ohjelmiston elinkaaresta. Koska kaikille käyttäjille ei haluta tarjota samoja verkon

palveluita, tulee käyttäjät jakaa käyttäjäryhmiin. Tämä on IPsec -järjestelmällä hankalaa.

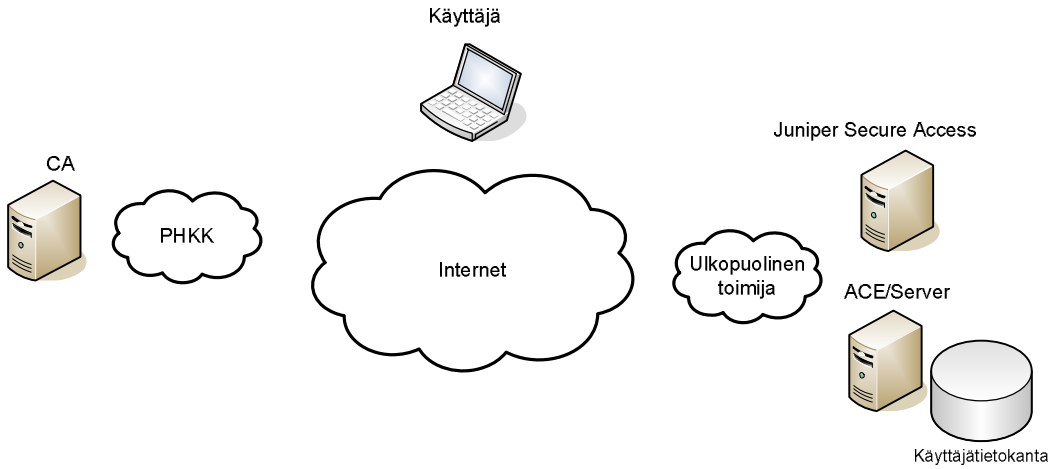
Vaikka SSL VPN -yhteys tarvitsee toimiakseen alijärjestelmiä. Niiden asentaminen tapahtuu yleensä joko automaattisesti tai sitten alijärjestelmät on mahdollista etäasentaa. Asennuksen jälkeen alijärjestelmät saavat konfiguraatiot aina SSL VPN -palvelimelta. Lisäksi käyttäjien jako erilaisiin rooleihin on helppoa sertifikaatin eri parametreilla sekä alijärjestelmien suorittamilla järjestelmäskannauksilla.

5.1.5 Toteutusympäristö

Toteutettavaksi alustaksi oli jo ennen tämän opinnäytetyön aloittamista valittu testattavaksi SSL VPN -ratkaisu, koska SSL VPN kykenee toteuttamaan halutut tavoitteet IPsec VPN ratkaisua tehokkaammin. Koska valmista infrastruktuuria ei ollut, päätettiin palvelu vuokrata ulkopuoliselta toimijalta kuvion 10 mukainen järjestelmä.

Lisäksi otettiin käyttöön käyttäjän tunnistukseen valmistettuja RSA Security:n valmistamia SecurID -varmistusavaimia. SecurID on fyysiseltä kooltaan pieni salasanageneraattori, joka luo kerran minuutissa uuden kuusinumeroisen salasanan. Luodun salasanan eteen lisätään käyttäjän tiedossa oleva PIN -koodi (Personal identification number), jonka jälkeen avaimesta laskettu tiiviste lähetetään niitä hallinnoivalle palvelimelle.

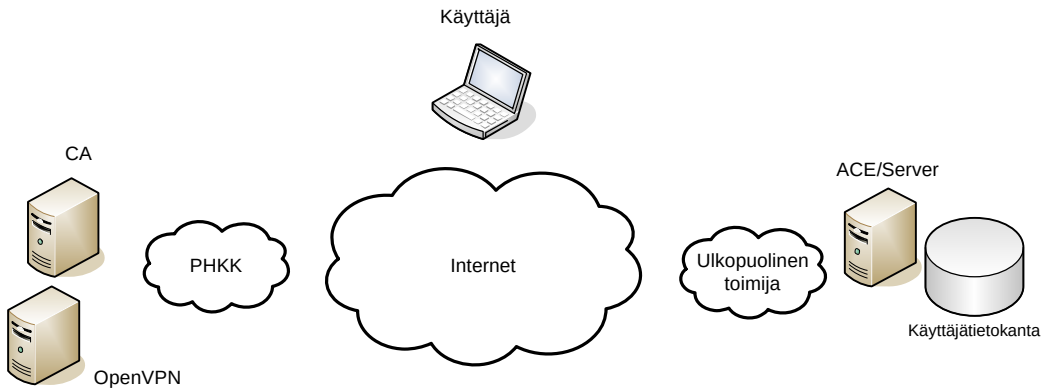
Varmistusavaimia hallinnoiva ACE/Server -palvelin ohjelmisto sijaitsee niin ikään palvelun SSL VPN -toimittajalla. Palvelun toimittajalla on galvaanisesti erotettu yhteys Päijät-Hämeen koulutuskonsernin sisäverkkoon, jolloin mitään tietoja ei lähetetä internetiä käyttäen.



KUVIO 10. Juniper Secure Access, fyysinen toteutus

CA:na toimii jo valmiiksi asennettu Päijät-Hämeen koulutuskonsernin oma sertifikaattipalvelin. Sertifikaattipalvelimen tehtävänä tässä työssä on tuottaa tietokoneen tunnistukseen sopivia sertifikaatteja. Sertifikaattipalvelimesta kuitenkin puuttuu automaattinen julkaisujärjestelmä tämän työn vaatimille sertifikaateille. Julkaisujärjestelmää ei ole kuitenkaan tämän työn puitteessa tehty, vaan tarvittavat sertifikaatit on luotu käsin.

Lisäksi toteutettiin vertaileva SSL VPN -toteutus, jossa käytettävä palvelin sijaitsee Päijät-Hämeen koulutuskonsernin tiloissa kuvion 11 mukaisesti, mutta käyttäjätunnistus tehdään SecurID -varmistusavaimilla. OpenVPN on asiakaskoneeseen asennettava ohjelmisto, joka tarjoaa ainoastaan OSI -mallin tason 2 ja tason 3 yhteyksiä



KUVIO 11. OpenVPN, fyysinen toteutus

5.2 Juniper Networks SSL VPN - Secure Access

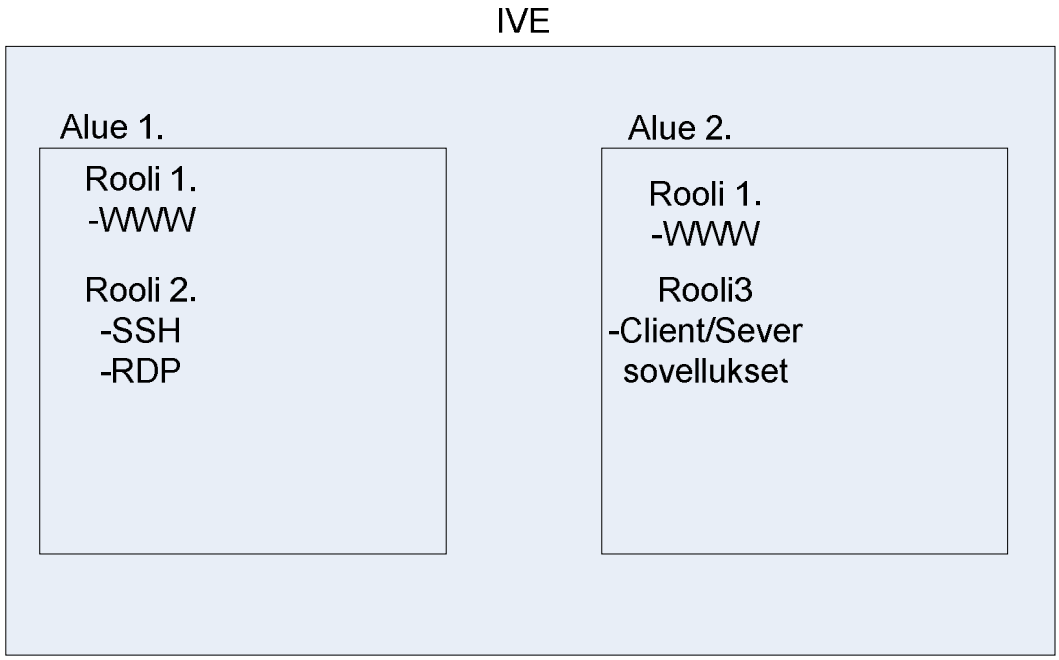
5.2.1 Toimintaperjaate

Juniper Networks:n valmistama Secure Access on tuoteperhe, joka käsittää ominaisuuksiltaan ja maksimi kaistanleveydeltään erikokoisia SSL VPN -ratkaisuja. Kaikki Secure Access -tuotteet ovat fyysisiä laitteita, joilla luodaan yrityksen käyttäjille mahdollisuus hyödyntää yrityksen sisäverkon palveluihin. Yhteys SSL VPN -palvelimeen otetaan käyttämällä WWW-selainta, joten sillä on korkea saatavuus.

Kaikki Secure Access laitteet käyttävät IVE -käyttöjärjestelmää (Instant Virtual Extranet), joka käyttää hyväkseen SSL/TLS -protokollaa. Vasta käyttäjän tunnistauduttua on käyttäjän mahdollista lähettää pyyntöjä IVE -järjestelmään, jonka tehtävänä on lähettää pyynnöt edelleen yrityksen sisäverkkoon. Toisin sanoen, IVE toimii välittäjänä käyttäjän ja yrityksen sisäverkon palveluiden välillä, joten käyttäjä ei voi koskaan lähettää suoraan tietoa palvelimille.

Secure Access tarjoaa erilaisia toiminnallisuuksia käyttäjilleen. Toiminnallisuuksia tarjotaan erilaisiin rooleihin (Role), jotka sijaitsevat eri alueilla (Realm), kuvion 12 mukaisesti. Eri alueille voi olla erilaiset tunnistautumistavat, kuten sertifikaatit ja niiden eri attribuutit. Käyttäjä voi olla yhdellä alueella kerrallaan.

Käyttäjien jako rooleihin alueiden sisällä tapahtuu erilaisten sääntöjen avulla. Sääntöinä voivat olla esim. sertifikaatit ja niiden eri attribuutit. IVE:n mahdollisia ominaisuuksia ovat mm. levyjaot, client/server -sovellukset, sekä suorat yhteydet TCP/IP -protokollalla sisäverkkoon. Suurinta osaa palveluista voidaan käyttää suoraan selaimella, mutta osa vaatii ylimääräisten komponenttien asennusta asiakaskoneisiin. Käyttäjän on mahdollista saada itsellensä monen eri roolin toiminnot; tämä mahdollistaa erittäin yksityiskohtaisen toimintojen jakamisen.



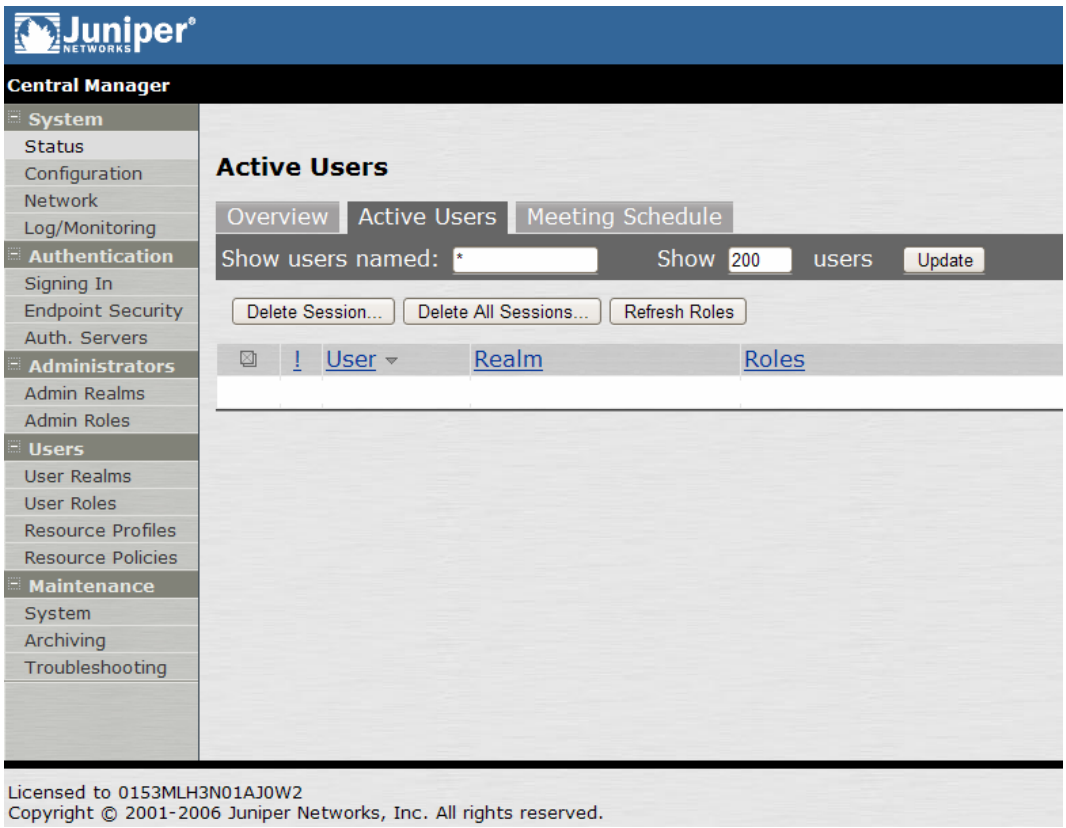
KUVIO 12. IVE: Roolit, alueet ja resurssit

Koska IVE:een saa yhteyden ainoastaan WWW-selaimella, on asiakaskoneen turvallisuus syytä varmistaa ennen yhteyden avaamista. Tähän ympäristö tarjoaa erilaisia alijärjestelmiä. Alijärjestelmillä on mahdollista tutkia asiakaskoneen tietoturva-asetuksia ja tarvittaessa siirtää käyttäjä roolin, josta ei ole mahdollista tunkeutua yrityksen resursseihin. Myös istunnosta syntyvien välimuistiin tallentuneiden tietojen poisto on mahdollista.

5.2.2 Ylläpito ja konfigurointi

Secure Access järjestelmän hallinta tapahtuu kuvion 13 mukaisesti käyttämällä WWW-selainta. Johtuen valmistajan SSL VPN -toteutuksesta jossa asiakas ottaa aina yhteyden laitteen WWW -sivuun, on keskitetty hallinta helppoa.

Ainoatakaan ohjelman asennusta ei oletusarvoisesti tarvitse tehdä asiakkaiden tietokoneisiin, koska suurimmassa osassa koneita on jo valmiina SSL/TLS -protokollaa tukeva WWW-selain. Tämä mahdollistaa sen, ettei asiakaskoneiden ohjelmien elinkaaresta tarvitse huolehtia Secure Access -laitteen kannalta.



KUVIO 13. Hallintanäkymä

Pääkäyttäjän tehtävänä on määrittää roolijaot alueisiin siten, että oikeat käyttäjät saavat oikeat palvelut. Lisäksi on hyvä varmistaa asiakaskoneiden turvallisuus. Tässä työssä asiakaskoneiden turvallisuus varmistettiin asentamalla luotettuihin tietokoneisiin etukäteen Päijät-Hämeen Koulutuskonsernin hyväksymät sertifikaatit. Vain oikean sertifikaatin omaavat tietokoneet voivat käyttää sisäverkon kriittisiä palveluita, muille laitteille tarjotaan vain vähemmän kriittisiä palveluita. Tietokoneen joutuessa vääriin käsiin on konekohtainen sertifikaatti helppo kumota CRL -listalla, jolloin kyseisellä koneella ei pääse kirjautumaan. Tämä vaatii kuitenkin asiasta välitöntä ilmoitusta ylläpidolle.

Koska järjestelmän pääsääntöinen käyttö tapahtuu WWW-selaimella, on siihen mahdollista ottaa yhteys lähes joka paikasta. Tästä saattaa aiheutua salasanojen ja käyttäjänimien joutuminen vääriin käsiin, käytettäessä ei luotettuja tietokoneita. Tämä haluttiin ehkäistä, ottamalla käyttöön henkilönkohtaiset SecurID -varmistusavaimet. SecurID -varmistusavaimet tuottavat muuttuvia salasanoja. Täl-

löin kaapatulla käyttäjänimi – salasana -parilla ei voi kirjautua myöhemmin uudelleen esim. Koulutuskonsernin sisäverkossa.

Kaikki tarjottavat palvelut eivät kuitenkaan toimi ainoastaan WWW-selaimessa, jolloin niiden käyttäminen tarvitsee erillisiä ohjelmia. Päijät-Hämeen Koulutuskonsernissa ei käyttäjillä pääsääntöisesti ole IVE -järjestelmän ohjelmien asentamiseen vaadittuja pääkäyttäjän oikeuksia luotettuihin tietokoneisiin. Tämä johtaa siihen, ettei kaikkia tarjottavia palveluita voi käyttää ennakkoasematta lisäohjelmia tietokoneisiin. Näitä palveluita ovat mm. client/server sovellukset ja TCP/IP -tunnelointi SSL VPN -yhteyden yli.

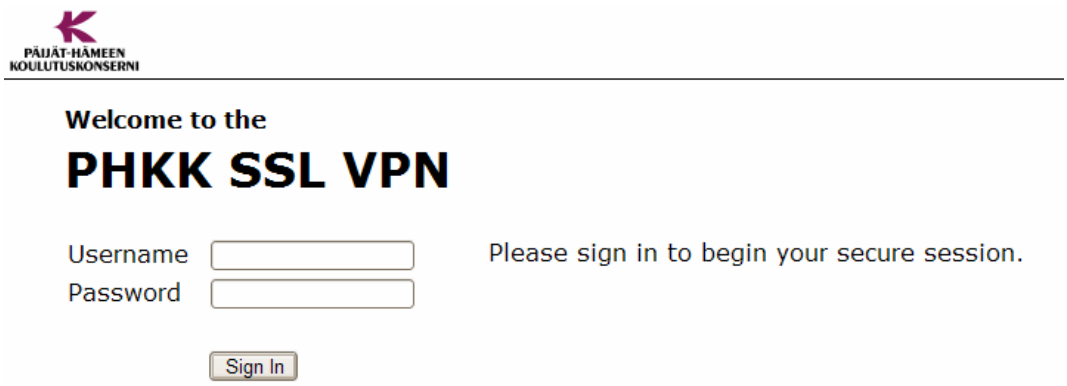
Esiasennetun ohjelman voi käynnistää ilman pääkäyttäjänoikeuksia, jolloin IVE:ssä tarjotut palvelut ovat käytettävissä. Jos käyttäjällä on sertifikaatilla varmistettuun tietokoneeseen pääkäyttäjän oikeudet, asentaa WWW-selain automaattisesti tarvittavat ohjelmat.

Ohjelmien asentamiseen tässä työssä käytettiin SMS -järjestelmää (Systems Management Server). SMS on Microsoftin tuote suurten Windows-verkkojen hallintaa. SMS mahdollistaa mm. sovellusten elinkaaren hallitsemisen tietoverkon lävitse tietokoneisiin, joihin tietokoneen pääasiallisella käyttäjällä ei ole tarvittavia oikeuksia.

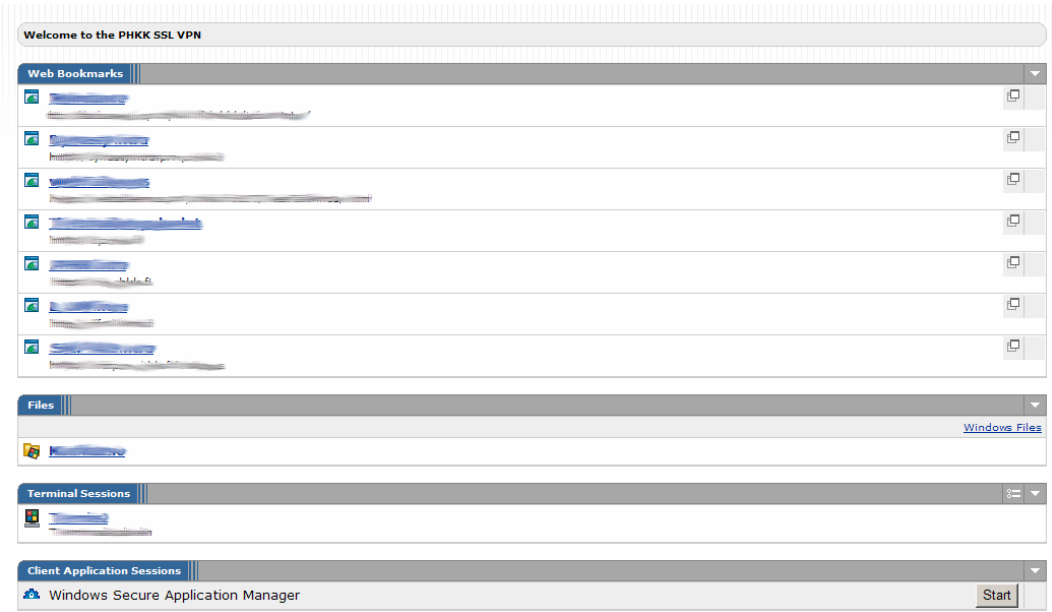
5.2.3 Käyttö

IVE:n käyttö tapahtuu SSL/TLS -protokollaa tukevalla WWW-selaimella, kuvion 15 mukaisesti. Yhteyden avauduttua tulee selaimeen järjestelmän kirjautumisnäkymä, kuvion 14 mukaisesti. Näkyviin kenttiin syötetään sekä käyttäjänimi, että SecurID -varmistusavaimessa näkyvä luku ja siihen lisätty henkilökohtainen PIN -koodi. Tunnistuksen onnistuttua ja alijärjestelmien latauduttua pääsee käyttäjä lopulliseen toimintaympäristöön. Käyttäjän näkymästä käyttäjä voi hiirtä käyttämällä valita halutun toiminnon.

IVE:n palvelut ovat käytössä siihen asti, kunnes istunnonaika päättyy. Istuntoajan päättymisestä tulee varoitus ennen sulkemista, joten käyttäjälle jää aikaa tallentaa työnsä. Istunto voidaan myös lopettaa kirjautumalla kesken ulos. Jotta SSL VPN -yhteys toimisi, täytyy WWW-selaimessa olla IVE:n ikkuna auki koko istunnon ajan. Lisäksi järjestelmä kirjaa käyttäjän ulos tietyn käyttämättä olon jälkeen, jolla estetään istunnon auki unohtaminen.



KUVIO 14. Kirjautumisnäkymä



KUVIO 15. Käyttäjän näkymä

5.3 OpenVPN

5.3.1 Toimintaperiaate

OpenVPN on GNU GPL version 2 (General Public License) lisenssin alainen SSL VPN -tuote. Lisensointi mahdollistaa käytettävän ohjelmistokoodin vapaan levittämisen ja käyttämisen.

OpenVPN on luonteeltaan SSL VPN ratkaisu, joka toiminnaltaan muistuttaa IPsec VPN ratkaisua. OpenVPN osaa luoda ainoastaan OSI -mallin toisen ja kolmannen kerroksen yhteyksiä, joita suojataan käyttämällä ESP -protokollan kaltaista protokollaa. Avainten vaihtoon OpenVPN käyttää SSL/TLS -protokollaa. Toisin kuin IPsec VPN, joka toimii OSI -mallin kolmannella kerroksella, toimii OpenVPN kerroksilla 4-7. Tämä mahdollistaa OpenVPN:n käyttämisen käyttäjän ympäristössä (user space), eikä käyttöjärjestelmän ytimessä (kernel space). Tämä mahdollistaa seuraavia asioita:

- Ohjelman asennuksessa ei tarvitse muuttaa käyttöjärjestelmän ydintä. Jos ohjelmassa havaitaan fataali virhe, ei virhe vaikuta muun järjestelmän toimintaan.

- Ohjelma on mahdollista suorittamisen alennetuilla käyttöoikeuksilla ja erillisessä ”hiekkalaatikossa”, jolloin järjestelmään tunkeutuminen ei anna järjestelmä tasoisia oikeuksia kaappaajalle.

- Ohjelma on helposti muunnettavissa toimimaan toisessa käyttöjärjestelmässä, koska usein monimutkaista käyttöjärjestelmän ydintä ei tarvitse muokata.

Vaikka OpenVPN on luonteeltaan SSL VPN, ei järjestelmään oteta yhteyttä WWW-selaimella. OpenVPN vaatii toimiakseen yhden palvelinkoneen, joihin järjestelmänkäyttäjät ottavat yhteyden OpenVPN -ohjelmistolla. OpenVPN -palvelimet ovat myös mahdollista ryvästää, joka mahdollistaa kuormantasauksen. Ryvästyksestä puuttuu kuitenkin ominaisuus, joka mahdollistaisi palvelimen kaatuessa katkenneiden yhteyksien automaattisen siirtämisen toiselle palvelimelle.

OpenVPN -asiakkaan liikenteen tunnelointi tapahtuu virtuaalisella verkkosovittimella, johon lähetetään sopiva reititystaulu OpenVPN -palvelimelta. Lisäksi virtuaalinen verkkosovitin saa tunnelointiin sopivan IP -osoitteen. Reititystaulu pitää sisällään ne verkot, joita käyttäjille halutaan tarjota yrityksen sisäverkossa. Halluttaessa voidaan käyttäjän kaikki liikenne tunneloida OpenVPN -palvelimelle, jolloin on mahdollista käyttää yrityksen sisäisiä palomuurisääntöjä liikenteen suodatukseen. Haittapuolena voi olla mm. käyttäjän internetoperaattorin DHCP -viestien reitittyminen väärään paikkaan.

Virtuaalisen verkkokortin IP -osoitteet jaetaan oletuksena 10.9.0.0/24 aliverkosta. Aliverkosta lohkaistaan 64 kpl 30-bitin aliverkkomaskilla varustettuja osoitteita. Yhdessä 30-bitin aliverkossa on ainoastaan kaksi käytettävää osoitetta, joista toinen annetaan OpenVPN -palvelimelle ja toinen asiakaskoneelle. Muodostettavat yhteydet ovat oletuksena luonteeltaan point-to-point -yhteyksiä, jolloin muiden saman palvelimen OpenVPN -käyttäjien välille ei luoda yhteyksiä. Varsinainen tiedon siirto koneiden välillä tapahtuu fyysisillä verkkosovittimilla, joilla on oltava reititettävät IP -osoitteet.

5.3.2 Yhteyden luonti

Ensimmäinen vaihe yhteyden luonnissa on vaihtoehtoinen HMAC -tunnistus. Tämä tapahtuu asentamalla etukäteen sekä palvelimeen että asiakaskoneisiin staattinen avain. Vain oikean staattisen avaimen omaavat koneet voivat yrittää aloittaa SSL/TLS -kättelyn. HMAC -tunnistuksessa allekirjoitetaan kaikki SSL/TLS -kättelyssä käytettävät paketit, ilman oikeaa staattista avainta on allekirjoitus väärä, tällöin OpenVPN -palvelin hylkää paketit ilman käsittelyä.

Seuraavassa vaiheessa tapahtuu avainten vaihto. OpenVPN:llä on avainten vaihtoon kaksi erilaista toimintatapaa, sertifikaatit ja etukäteen jaetut avaimet. Käytettäessä staattisesti etukäteen luotuja avaimia, täytyy käytettävien avainten olla molempien osapuolten tiedossa, jotta yhteys toimisi. Tällöin OpenVPN tarvitsee toi-

miakseen vain kaksi avainta, HMAC -avaimet ja tiedon salaamiseen ja purkamiseen käytettävät avaimet, jotka ovat samat yhteyden molemmilla osapuolilla.

Käytettäessä sertifikaatteja OpenVPN käyttää SSL/TLS -protokollaa avainten vaihtoon osapuolten kesken. SSL/TLS -protokollalla järjestelmä luo neljä avainta yhteyden osapuolten kesken; HMAC lähetys- ja vastaanottoavaimet ja tiedon salaamiseen ja purkamiseen tarkoitetut avaimet. Koska käytössä ovat sertifikaatit, eivät tiedon salaukseen ja purkuun käytetyt avaimet ole samat. OpenVPN osaa hakea käyttäjän sertifikaatit Windows-järjestelmän sertifikaattikannasta, tällöin ne on mahdollista luoda keskitetysti kaikille käyttäjille esimerkiksi käyttämällä AD-hakemistopalvelua.

Kolmas vaihe yhteyden luomisessa on vapaaehtoinen käyttäjän tunnistus. OpenVPN tarjoaa käyttäjän tunnistukseen mm. Linux -järjestelmissä toimivia PAM -moduuleita (Pluggable Authentication Modules). PAM -modulit mahdollistavat ohjelmiston ulkopuolisen tunnistusjärjestelmän tuomisen ohjelmistoon. Ulkopuoleinen järjestelmä voi olla esim. RADIUS ja LDAP. Yhteyden alustusta ei aloiteta ennen käyttäjän onnistunutta tunnistusta.

Käyttäjätunnistuksen jälkeen OpenVPN -palvelin voi työntää joitakin yhteysparametreja asiakaskoneeseen. Tämä tuo konfiguraatioihin joustavuutta, koska konfiguraatiota ei tarvitse kirjoittaa asiakaskoneelle uudestaan. Mahdollisia työnnettäviä parametreja ovat asiakkaan IP -osoite, DNS -palvelimet, WINS -palvelimet (Windows Internet Naming Service) ja asiakkaan käyttämä reititystaulu.

Työnnettyjen parametrien jälkeen voi tiedon siirtäminen alkaa. Siirrettävän tiedon salaamiseen OpenVPN käyttää ESP -protokollan kaltaista protokollaa. Käytettävä symmetrinen salausalgoritmi on erikseen määritettävissä, jolloin käytössä ovat kaikki OpenSSL -ohjelmiston tukemat protokollat. Oletuksena OpenVPN käyttää tiedon salaamiseen Blowfish algoritmia CBC -moodissa (Chipher Block Chaining) ja tiedon eheyden tarkistukseen SHA-1-algoritmia, vaikka SSL/TLS -kättelyssä neuvotellaan myös HMAC -avaimet. CBC vaikeuttaa kolmannen osapuolen työtä purkaa käytetty staattinen avain, vaikka hallussa olisi tarvittava määrä tietoa avai-

men purkamiseen. Tämän lisäksi OpenVPN oletuksena neuvottelee käytettävistä avaimista uudestaan kerran tunnissa SSL/TLS -neuvottelulla.

Yhteys uudistetaan aloittamalla koko kättelyprosessi alusta, alkaen HMAC -tunnistuksesta. OpenVPN, kuitenkin muistaa edellisen hyväksytyn käyttäjän tunnistustiedon, jolloin yhteyden uudistus tapahtuu ongelmitta. Jos käytössä ovat muuttuvat salasanat, on tunnistustieto kuitenkin joka kerralla eri. Tällöin automaattinen yhteyden uudistus epäonnistuu ja käyttäjälle näytetään järjestelmän kirjautumisikkunaa. Kättelyprosessin aikana ei hyötytieto liiku käyttäjän ja palvelimen välillä. OpenVPN ei myöskään varoita yhteyden uudistamisesta etukäteen.

Yhteyksistä OpenVPN tuottaa logia Linux järjestelmän Syslog -palveluun. Logista näkyvät oletuksena yhteyden yhteydenmuodostus ja sulkeminen. Logia voi tarvittaessa lisätä tuottamalla yhteyksistä tietoa esimerkiksi Iptables -palomuurilla.

TAULUKKO 2. OpenSSL ohjelmiston eri algoritmien nopeus tuhansissa tavuissa prosessoidun lohkon koko

Algoritmi	16 tavua	64 tavua	256 tavua
hmac(md5)	11960.38k	36744.88k	91270.26k
sha1	5647.15k	18607.15k	48782.01k
des cbc	29867.24k	32441.72k	33174.51k
des ede3	12051.44k	12724.94k	12980.20k
blowfish cbc	46316.69k	49618.23k	52365.69k
aes-128 cbc	32919.99k	34192.96k	34995.20k
aes-192 cbc	27920.95k	28766.68k	29602.25k
aes-256 cbc	25375.18k	25995.40k	26543.10k

Kuten taulukko 2 osoittaa, on Blowfish erittäin nopea symmetrinen salausalgoritmi. Käytettäessä 64 tavun lohkoa kykenee se käsittelemään lähes 50Mbit/s nopeudella tietoa, joka on neljä kertaa enemmän, kuin 3DES tai 1.5 kertaa nopeammin, kuin AES. Testissä käytetty prosessori oli UltraSPARC 1,5 Ghz.

OpenVPN osaa käyttää tiedonsiirtoon sekä TCP-, että UDP -protokollaa siirrettävän tiedon tunnelointiin. Oletuksena käytössä on UDP -protokolla, koska se soveltuu tunnelointiin TCP:tä paremmin. Esimerkiksi TCP pitää kirjaa pakettien järjestyksestä ja pakettien häviämisestä. Lisäksi TCP:ssä on laskuri, jonka kuluttua nol-

laan, laskuri olettaa paketin kadonneen ja pyytää uudelleen lähetystä. Jos paketteja katoaa matkalla, odotuslaskurin lähtöarvo nousee eksponentiaalisesti. Tunneloitaessa TCP -protokollaa TCP:n sisällä tulee uudelleen lähetyksiä hoitavia laskureita kaksi kappaletta. Jos alemman kerroksen TCP:n laskuri on nopeampi kuin ylemmän kerroksen laskuri, aiheuttaa se paljon uudelleen lähetyksiä. UDP -protokolla sopii yhteydettömän luonteensa takia paremmin emuloimaan kiinteätä yhteyttä osapuolten välille.

Työssä käytetty OpenVPN -versio 2.1RC4 ei mahdollista suurten käyttäjäryhmien tekoa esim. sertifikaattien attribuuttien perusteella, käyttämällä yksittäistä OpenVPN -prosessia. Tämä on kuitenkin mahdollista tehdä käynnistämällä useita eri OpenVPN -prosesseja samaan palvelimeen, jolloin niiden on kuitenkin kuunneltava eri portteja. Lisäksi järjestelmästä ei löydy tukea keskitettyyn hallintaan asiakkaalle asennettavaan ohjelmistoon. Ryhmäjäsenen tulee osata ottaa yhteys oikeaan porttiin, saadakseen oikeanlaiset oikeudet, tämä voidaan kuitenkin määrittää asiakkaan konfigurointitiedostossa.

5.3.3 Ylläpito ja konfigurointi

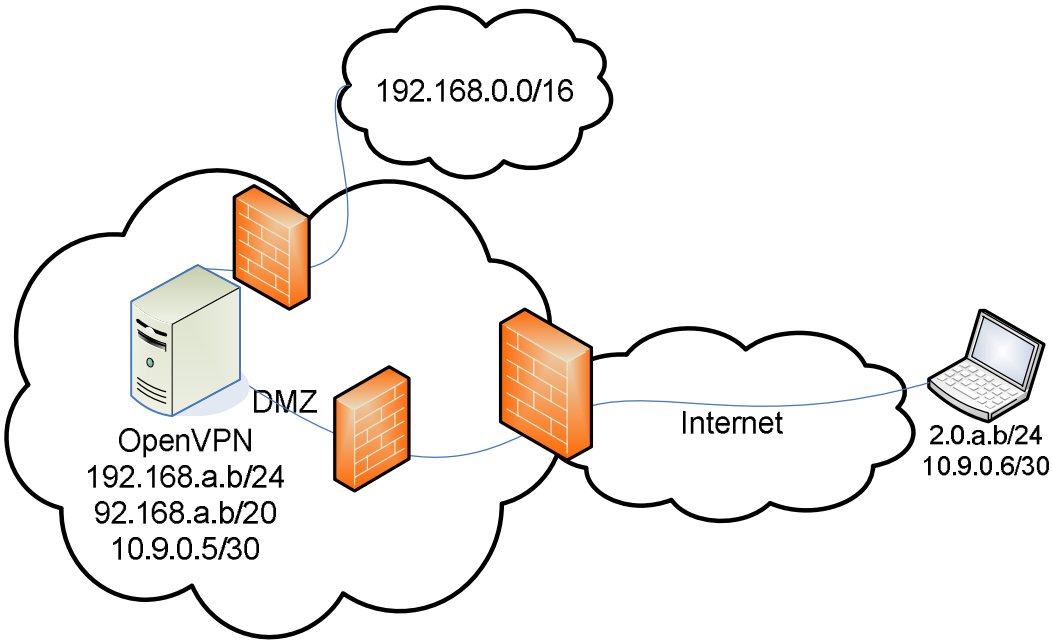
Johtuen kokeilujärjestelmän heikosta prosessorin suorituskyvystä, luotiin OpenVPN -palvelimia kaksi kappaletta, joiden välille tehtiin OpenVPN:n tarjoama kuormantasaus. Kuormantasaus toteutetaan lisäämällä asiakaskoneen konfigurointitiedostoon kaikkien OpenVPN -palvelinten IP -osoitteet, joista asiakaskone valitsee satunnaisen OpenVPN -palvelimen, jokaisella yhteydenluonti kerralla.

OpenVPN:n tekemä kuormantasaus valitsee satunnaisesti asiakkaan koneelle käytettävän palvelimen. Pahimmassa tapauksessa kaikki yhteydet otetaan vain toiselle palvelimelle, jolloin palvelin voi ruuhkaantua pahasti. Todellisuudessa ei tietovirta ole jatkuvaa, joten palvelimien ruuhkaantuminen ei ole todennäköistä.

Kummankin palvelimen Blowfish käsittely nopeus on 17Mbit/s, joka riittää teoriassa noin kymmenen tavallisen keskimäärin 2Mbit/s ADSL -yhteyden käsittelyyn

käytettäessä yhteyttä jatkuvasti. Tämä ei kuitenkaan ole käytännössä mahdollista, koska palvelimen prosessorin kuormitus nousee korkeaksi jo muutamalla yhteydellä.

Molemmat palvelimet ovat yhteydessä 100Mbit/s yhteydellä internetiin ja 100Mbit/s yhteydellä Päijät-Hämeen koulutuskonsernin sisäverkkoon. OpenVPN järjestelmän palvelimissa on käytössä Fedora Core käyttöjärjestelmät, jonka ytimenä on Linux. Palvelimen OpenVPN prosessia ajetaan ”hiekkalaatikossa” sekä alennetuilla järjestelmän käyttöoikeuksilla, mahdollisesta palvelinkaappauksesta johtuvien haittojen minimoimiseksi. Sekä OpenVPN palvelimen, että OpenVPN -asiakaskoneen konfigurointi tapahtuu muokkaamalla tekstitiedostoa.



KUVIO 16. OpenVPN palvelimen fyysiset ja loogiset yhteydet sekä palomuurit

Tässä työssä toteutetussa OpenVPN -palvelimessa on kaksi fyysistä verkkokorttia. Toinen verkkokortti on loogisessa yhteydessä Päijät-Hämeen koulutuskonsernin DMZ -alueeseen (Demilitarized zone) ja toinen koulutuskonsernin sisäverkkoon. Järjestelmä on mahdollista toteuttaa myös yhdellä verkkokortilla, mutta konfiguraation ja loogisen ymmärrettävyyden helpottamiseksi se toteutettiin kahdella.

Yhteydet sisäverkkoon päätettiin tehdä OSI -mallin kolmannella kerroksella siten, että käyttäjän kaikki verkkoliikenne ohjataan luotuun tunneliin. Toisen kerroksen toteutetut yhteydet olisivat vaatineet oman DHCP -palvelun asentamista VPN asiakkaille. Lisäksi Päijät-Hämeen koulutuskonsernissa ei ole käytössä kolmannen kerroksen protokollia, joita OpenVPN ei osaa käsitellä. Kaikki tietoliikenne OpenVPN -palvelimesta kulkee palvelimen ohjelmallisen palomuurin läpi.

Palomuurina työssä käytettiin Linux -ytimeen integroitua Iptables -ohjelmaa. Palomuuri sääntöihin kirjattiin Päijät-Hämeen koulutuskonsernin sisäverkkoon sallittavat yhteydet, lisäksi DMZ -alueelta OpenVPN -palvelimeen sallittiin ainoastaan OpenVPN:n käyttämä portti. Käyttäjän tunnelista internettiin DMZ:n läpi ottamat yhteydet kuitenkin sallittiin. Sisäverkkoon ja ulkoverkkoon menevissä yhteyksissä käytettiin palomuurisääntöjen lähdeosoitteena tunnelin IP -osoitealuetta (10.9.0.0/24).

Koska tunnelien käyttämä IP -osoiteavaruus ei sovellu reitittämiseen Päijät-Hämeen koulutuskonsernin sisäverkossa eikä julkisessa internetissä, täytyy sille tehdä NAT. NAT toteutettiin aina sen fyysisen verkkokortin loogisella osoitteella, johon käyttäjä halusi pakettiensa reitittyvän.

Palvelimissa valittiin TCP -tunnelointi tekniikaksi UDP:n sijaan, koska järjestelmän käyttäjien kotipalomuurit saattavat katkaista UDP -yhteydet. OpenVPN -palvelimissa käytettäväksi TCP -portiksi valittiin 80, koska se on useimmissa asiakkaiden palomuurijärjestelmissä oletuksena auki.

Käyttäjien tunnistukseen työssä käytettiin SecurID:n varmistusavaimia ja käyttäjien tietokoneiden tunnistukseen Päijät-Hämeen koulutuskonsernin CA:n kirjoittamia sertifikaatteja, sekä OpenVPN CA -palvelimella luotuja sertifikaatteja. Päijät-Hämeen koulutuskonsernin julkinen avain asennettiin OpenVPN -palvelimeen ja OpenVPN -palvelimien julkinen avain käyttäjien tietokoneisiin. Tällöin käyttäjien sertifikaatit voitiin luoda käyttämällä Päijät-Hämeen koulutuskonsernin juurisertifikaattia. OpenVPN -asiakassertifikaatit asennettiin Windows-käyttöjärjestelmän

sertifikaattikantaan, jolloin niitä on mahdollista hallita esimerkiksi AD-hakemistopalvelulla.

SecurID tietoja on mahdollista kysyä ACE/Server -palvelimelta käyttäen RADIUS -kyselyä. OpenVPN ei kuitenkaan tue natiivisti RADIUS:ta, mutta kyselyiden teko on mahdollista lataamalla OpenVPN käynnistyksessä siihen PAM -moduuli. PAM -moduulin tehtävän on hoitaa RADIUS -liikenne RADIUS -palvelimen ja OpenVPN:n välillä. Johtuen OpenVPN:n puutteellisesta SecurID -tuesta, eivät kaikki ACE/Serverin lähettämät virheviestit saavu oikeassa muodossa käyttäjälle. Näitä ovat mm. NextToken -viesti, joka näytetään, kun käyttäjä kirjoittaa kolme kertaa salasanan väärin. NextToken -viestiin tulisi vastata antamalla varmistusavaimessa oleva sen hetkinen numerosarja. Sen sijaan OpenVPN näyttää normaalin kirjautumisikkunan, jossa kysytän käyttäjänimi ja salasana.

Lisäksi OpenVPN -palvelimeen ja OpenVPN -asiakaskoneisiin välille määritettiin staattisella avaimella varustettu HMAC allekirjoituksen käyttöönotto SSL/TLS -kättelypaketeissa. Tällöin ainoastaan oikean avaimen omaavat laitteet voivat yrittää SSL/TLS -avaintenvaihtoa.

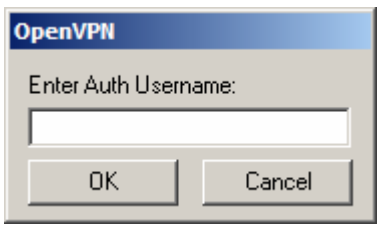
Vaikka OpenVPN -ohjelmisto toimii käyttäjän ympäristössä eikä järjestelmän ytimessä, vaatii OpenVPN kuitenkin oletusasetuksilla järjestelmävalvojan oikeudet käynnistyäkseen Windows-ympäristössä. Tämä johtuu OpenVPN:n tarpeesta muokata asiakaskoneen reititystauluja sekä aktivoida tarvittaessa virtuaalinen verkkosovitin. Ongelma on kuitenkin kierrettävissä käynnistämällä OpenVPN Windows koneessa järjestelmän palveluna, käyttämällä OpenVPN GUI -ohjelmaa. Tämän jälkeen käyttäjälle annetaan omaan tietokoneeseensa oikeudet käynnistää OpenVPN -palvelu. Palvelun käynnistämisen helpottamiseen luotiin käyttäjän työpöydälle batch-tiedosto, joka hoitaa yhteyden avaamisen ja purkamisen.

OpenVPN -ohjelmisto ja sen konfiguraatiotiedostot on mahdollista asentaa SMS -ohjelmistolla käyttäjien tietokoneisiin, mutta tässä työssä tehtävät asennukset tehtiin käsin.

5.3.4 Käyttö

Asiakas aloittaa OpenVPN -ohjelman käytön valitsemalla työpöydältä OpenVPN -kuvakkeen Käynnistämisen jälkeen ohjelma kysyy ensin käyttäjänimen, jonka jälkeen salasanan, kuvion 17 mukaisesti. Salasana koostuu PIN -koodista ja SecurID -varmistusavaimen tuottamasta lukusarjasta.

Ohjelman käynnistyttyä kaikki normaalit Päijät-Hämeen koulutuskonsernin tietoverkkoa vaativat palvelut ovat heti käytettävissä. Yhteys uudistuu automaattisesti kerran neljässä tunnissa, jolloin käyttäjän on oltava paikalla ja annettava tunnistustiedot. Tunnistustietojen syöttämisen jälkeen liikenne palvelimen ja käyttäjän koneen välillä jatkuu normaalisti. Yhteys lopetetaan valitsemalla OpenVPN -kuvake uudestaan työpöydältä.



KUVIO 17. OpenVPN -käyttäjäntunnistuskysely.

6 PÄÄTELMÄT

6.1 Palaute ja ongelmat

Jokaisessa projektissa on tärkeää kerätä palautetta ja tehdä jatkokehityssuunnitelmia, joiden perusteella on mahdollista määrittää projektin tulevaisuus. Tämän työn asiakaspalaute kerättiin lähettämällä sähköpostitiedustelu yleisistä käyttökokemuksista. Ylläpidon palautteesta vastasi järjestelmän sen hetkinen ylläpitäjä.

Kaikkia syntyneitä ongelmia ei ole mahdollista ratkaista. Syynä on yleensä kohdejärjestelmän kankeus asiaa kohtaan. Joitakin ongelmia on kuitenkin mahdollista kiertää tai toteuttaa haluttu toiminnallisuus tuomalla järjestelmään ulkopuolisia lisäkomponentteja. Lisäkomponentit vaativat kuitenkin aina ylimääräistä ylläpitoa ja niiden toiminnan pitäisi olla näkymätöntä käyttäjälle.

6.1.1 Juniper Networks SSL VPN - Secure Access

Järjestelmä ei ole ylläpidollisesti vaikea. Kaikki toiminta on keskitetty yhdelle WWW-sivustolle, jonka avulla on mahdollista tehdä kaikki ylläpidolliset toimenpiteet. Järjestelmä on lisäksi hyvin dokumentoitu ja erittäin helppokäyttöinen. Seuraavia ongelmia ja niiden ratkaisuja kuitenkin esiintyi palveluiden tuottamisessa asiakas näkymään.

- Päijät-Hämeen koulutuskonsernin sisäiset WWW-sivut eivät näkyneet aina oikein. Ongelmaan ei ole ratkaisua.

- Client/Server sovelluksia tunneloiva ohjelmisto rikkoi muutaman asiakaskoneen TCP/IP -pinon. Ongelma kuitenkin korjattiin vaihtamalla ohjelman asennusparametreja.

- 47 % asiakkaiden kirjautumisista epäonnistui. Syynä tähän on palveluntarjoajan käyttäjätietokanta, jonka tarjoamat käyttäjänimet ovat järjestelmän asiakkaille hankalat muistaa.

- Kaikkia levyjakoja ei saatu näkyviin. Ongelma korjattiin päivittämällä Secure Accesin käyttöjärjestelmä. Lisäksi kirjautuminen levyjakoihin on hidasta. Tarjottava levyjako ei myöskään sovellu nopeaan tiedostojen käsittelyyn johtuen selaimella toteutetusta ympäristössä.

- Alijärjestelmien suorittamat asiakaskoneen järjestelmäskannaukset ovat helposti kierrettävissä. Esimerkiksi, jos asiakasjärjestelmästä pitää löytyä hyväksyttävä palomuuri, voidaan palomuuri onnistuneen tarkistuksen jälkeen poistaa ja yhteys toimii edelleen, vaikka parempi toiminto olisi yhteyden katkaisu.

- Alijärjestelmä, joka on vastuussa väliaikaisten tiedostojen poistamisesta, toimii oikein vain, jos SSL VPN -istunto lopetetaan oikealla tavalla.

Järjestelmän käyttäjiltä saatu palaute oli positiivista. Järjestelmässä tarjottavat palvelut olivat juuri niitä, joita käyttäjäkunta halusi. Palvelut olivat helppokäyttöisiä ja helposti saatavilla. Muutamia ongelmia kuitenkin havaittiin.

- Suurta kaistanleveyttä vaativat sovellukset toimivat hitaasti. Korjattavissa käyttämällä järjestelmässä tarjottavaa RDP -yhteyttä (Remote Desktop Protocol), jolloin asiakas ottaa yhteyden Päijät-Hämeen koulutuskonsernin sisäverkossa sijaitsevaan etäyhteyspalvelimeen.

- Levyjaosta selaimella ladattu tiedosto ei aina aukea suoraan selaimesta. Ongelma on korjattavissa käyttämällä RDP -yhteyttä. Vaihtoehtoisesti ongelma on korjattavissa tallentamalla tiedosto ensin omalle kovalevylle ja avaamalla se tallennuksen jälkeen.

- Henkilökohtaisen levyjaon puute. Ongelma on korjattavissa käyttämällä RDP -yhteyttä.

- Istunnon aikakatkaisu koettiin liian nopeaksi. Ongelma korjattiin sallimalla istunnolle lisäaikaa ja kasvattamalla aikakatkaisua.

6.1.2 OpenVPN

OpenVPN -hallinta tapahtuu tekstimuokkaimella, Linux käyttöjärjestelmän konsolissa. Hallinta ei kuitenkaan ole vaikeaa, jos ylläpitäjä omaa aikaisempaa Linux -järjestelmän käyttökokemusta. OpenVPN -ohjelmisto on hyvin dokumentoitu ja sen käyttöön löytyy apua internetin keskustelufoorumeilta. Lisäksi ylläpitäjän tulee hallita Linux -koneella tapahtuvaa liikenteen reititystä ja palomuurin käyttöä.

Suurin ongelma on kuitenkin keskitetyn hallinnan puute. Asiakaskoneita ei pysty hallitsemaan kuin asiakaskoneella olevasta konfiguraatiotiedostosta, vaikka joitakin yhteysparametreja on mahdollista työntää asiakaskoneeseen. Lisäksi OpenVPN asiakaskoneen ohjelmiston elinkaaresta tulee pitää huolta kolmannen osapuolen ohjelmistolla. Seuraavia ongelmia ja niiden ratkaisuja esiintyi palveluiden tuottamisessa OpenVPN -asiakkaille.

- Asiakasohjelmiston elinkaaren hallinta, mahdollista esimerkiksi SMS palvelulla. Sama koskee myös asiakaskoneen järjestelmän konfiguraatiotiedostoa.

- Puutteellinen tuki SecurID protokollalle, joka näkyy väärinä viesteinä asiakkaalle. Näitä ovat mm. NextToken -viesti, joka näytetään, kun käyttäjä kirjoittaa kolme kertaa salasanan väärin. NextToken viestiin tulisi vastata antamalla varmistusavaimessa oleva sen hetkinen numerosarja. Sen sijaan OpenVPN näyttää normaalin kirjautumisikkunan, jossa kysytän käyttäjänimi.

  Tämä on kuitenkin mahdollista kiertää esim. hoitamalla käyttäjäntunnistus WWW-sivustolla ja tietokoneen tunnistus OpenVPN:n sertifikaatilla. Tällöin yhteys luotaisiin OpenVPN palvelimeen ilman käyttäjän tunnistusta. Yhteyden luonnin jälkeen käyttäjälle tulisi WWW-sivu johon tulee syöttää käyttäjän tunnistustiedot. Jos tunnistus menee väärin, osaa WWW-sivu antaa toimintaohjeet. Vasta onnistuneen tunnistuksen jälkeen sallittaisiin muu liikennöinti OpenVPN -palvelimen läpi.

- Käyttäjäryhmien luonti on hankalaa, ellei haluta tarjota kaikille käyttäjille kaikkia palveluita. Ratkaisuna toimii jokaiselle ryhmälle oman OpenVPN -palvelun perustaminen ryhmälle sopivilla palomuurisäännöillä.

- OpenVPN vaatii toimiakseen järjestelmävalvojan oikeudet asiakkaan järjestelmään. Palvelun asiakkailla ei kuitenkaan ole järjestelmävalvojan tunnuksia koneisiinsa. Tämä voidaan kiertää ajamalla järjestelmää Windowsin palveluna, jonka hallintaan annetaan käyttäjälle oikeudet. OpenVPN ei kuitenkaan osaa tällöin lukea sertifikaattitietoja käyttäjän sertifikaattikannasta, jolloin sertifikaatit pitää asentaa järjestelmän käyttäjätilille.

- Yhteyden kerran neljässä tunnissa tapahtuva uudelleenluonti, vaatii käyttäjänimen ja salasanan syöttämisen uudestaan, jolloin asiakkaan on oltava tietokoneen ääressä. Tämä on mahdollista kiertää hoitamalla käyttäjäntunnistus esim. WWW-sivustolla ja tietokoneen tunnistus OpenVPN:n sertifikaatilla. Tällöin yhteyden uudistus toimii OpenVPN asiakastietokoneen muistamilla tunnistusattribuuteilla automaattisesti.

- Järjestelmässä käytettävien palvelimien prosessorikuorma nousee helposti korkeaksi siirrettäessä paljon dataa asiakaan ja palvelimen välillä. Tämä on kuitenkin korjattavissa asentamalla OpenVPN -palvelu tehokkaampaan palvelimeen tai ryvästämällä pienempitehoisia palvelimia.

Järjestelmän käyttäjiltä saatu palaute oli positiivista. OpenVPN käyttö koettiin helpoksi ja tarjottavat palvelut toimivat. Suurimmaksi ongelmaksi muodostui yhteyden uudelleen luonti ilman erillistä ilmoitusta. Lisäksi alkuvaiheessa TCP -tunnelointi aiheutti pientä viivettä, tämä kuitenkin korjattiin konfiguroimalla OpenVPN -palvelimeen asetus, joka mahdollistaa pienemmän viiveen TCP -tunnelointiin.

6.2 Juniper Secure Access vs. OpenVPN

Juniper Secure Access ja OpenVPN edustavat molemmat erilaisia SSL VPN -ratkaisuja. Secure Access hyödyntää WWW-selainta sekä järjestelmän konfigurointiin, että yhteyksien luomiseen käyttäjän ja yrityksen verkonvälille. OpenVPN sen sijaan toimii, kuten IPsec -ratkaisu. Erona IPsec -järjestelmän ja OpenVPN -ohjelmiston välillä on se, että OpenVPN ei toimi käyttöjärjestelmän ytimessä (kernel space) vaan käyttäjän ympäristössä (user space). Lisäksi OpenVPN mahdollistaa erilaisten yhteysparametrien työntämisen asikaskoneeseen ja sertfifikaattien käytön Windowsin sertifikaattikannasta. Molemmissa SSL VPN -ratkaisuissa on hyvät ja huonot puolensa.

Juniper Secure Access -järjestelmällä saadaan helposti kohdennettua oikeat palvelut oikeille käyttäjille, kun taas OpenVPN tarjoaa ainoastaan verkkokerroksen yhteyksiä. OpenVPN -palvelimella voidaan suorittaa roolijakoja ainoastaan luomalla useita OpenVPN -prosesseja OpenVPN -palvelimeen. Molemmat järjestelmät osaavat käyttää sertifikaatteja, sekä kertakäyttöisiä salasanoja. Kuitenkin OpenVPN natiivin tuen puuttuminen SecurID-varmistusavaimille saattaa aiheuttaa vääriä virheilmoituksia, jotka pahimmillaan estävät järjestelmään kirjautumisen. Vääristä virheilmoituksista syntyneiden kirjautumisongelmien korjaaminen aiheuttaa ylläpidolle lisätöitä.

Ylläpidollisesti molemmat järjestelmät ovat lähes yhtä helppoja. Juniper Secure Access vaatii joidenkin alijärjestelmien ylläpidon kolmannen osapuolen järjestelmällä nykyisellä konfiguraatiolla, kuten myös OpenVPN. Erottava tekijä on OpenVPN -ohjelmiston tarve konfiguraatiotiedostolle asiakaskoneessa. Konfiguraatiotiedostoon ei kuitenkaan tarvitse tehdä juuri koskaan muutoksia, sillä suurin osa tärkeistä parametreistä voidaan työntää OpenVPN -asiakkaalle OpenVPN -palvelimelta. Muutoksia konfiguraatiotiedostoon aiheuttaa lähinnä OpenVPN -palvelimen IP -osoite muutokset.

Ongelman ratkaisuun molemmat tarjoavat hyvät työkalut. Secure Access tarjoaa valmiita työkaluja istuntojen nauhoittamiseen ja roolijakojen simuloinnin, tämän lisäksi Secure Access kirjoittaa helppolukuista lokitiedostoa. OpenVPN kykenee ainoastaan kirjoittamaan syslog -palveluun, mutta ohjelman kirjoittama loki on hyvin yksiselitteistä.

Suurin ongelma OpenVPN -ohjelmistossa on istuntoajan päättymisestä puuttuva ilmoitus. Kun taas Juniper Secure Access kärsii mm. väärin koodatuista WWW-sivuista ja kankeasta tiedostojenjaosta asiakkaan ja levyjakojen välillä. OpenVPN –palvelun ongelma on vaikeasti korjattavissa, mutta Secure Access-järjestelmän ongelmat voidaan kiertää käyttämällä RDP -yhteyttä.

6.3 Saavutetut tavoitteet

Projektille asetettuja tavoitteita olivat: helppokäyttöisyys, liikkuvuus, tietoturvallisuus ja ylläpidettävyys. Nämä asetetut tavoitteet saavutettiin toteutetuilla etäkäyttöjärjestelmillä lähes kokonaan.

Molemmat järjestelmät koettiin helppokäyttöisiksi ja työskentelyä helpottaviksi. Ainoastaan kirjautumisessa käytetty muista Päijät-Hämeen koulutuskonsernissa käytössä olevista kirjautumistavoista poikkeava tekniikka tuotti lieviä hankaluuksia. Kirjautumistekniikkaan ei ole kuitenkaan tulossa heti muutoksia, joten järjestelmienkäyttäjien täytyy omaksua uusi tekniikka.

Toteutetut etäkäyttöjärjestelmät tarjoavat myös hyvän liikkuvuuden. Järjestelmien käyttäjiä ei ole sidottu mihinkään yksittäiseen fyysiseen paikkaan, vaan järjestelmän käyttöön riittää ainoastaan internet -yhteys. Lisäksi opinnäytetyössä luodut etäkäyttöjärjestelmät käyttävät yleisesti asiakkaidenpalomuureissa auki olevia portteja, jolloin järjestelmien saavutettavuus on mahdollisimman hyvä. Asiakaskoneiden järjestelmät eivät myöskään esty yleisesti asiakapalomuureissa käytössä olevasta NAT:sta. Rajoittava tekijä luoduissa etäkäyttöyhteyksissä on henkilökohtaisen Päijät-Hämeen koulutuskonsernin myöntämän kannettavan tietokoneen tarve, mutta tietoturvasyistä etäkäyttöyhteyksiä ei tulla sallimaan muilta koneilta.

Tietoturvamielessä molemmat etäkäyttöjärjestelmät ovat turvallisia. Molemmat etäkäyttöjärjestelmät käyttävät vahvaa käyttäjän todennusta sekä sertifikaatteja käytettävän tietokoneen tunnistukseen. Järjestelmissä hyödynnetään lisäksi vahvoja salausmenetelmiä, jolloin salatun liikenteen purkaminen kolmannelta osapuolelta ei onnistu järkevässä ajassa. Jos asiakas hävittää, sekä kannettavatietokoneensa ja SecurID -varmistusavaimen, voidaan ne evätä etäkäyttöjärjestelmistä nopeasti, tämä kuitenkin vaatii asiakkaan välitöntä ilmoitusta asiasta.

Ylläpidettävyydeltään molemmat etäkäyttöjärjestelmät ovat helppoja. Vaikka luotuja järjestelmiä hallitaan eritavoilla, ovat ne kuitenkin loogisesti helppotajuisia. Asioita, joihin ylläpidon tulee kiinnittää huomioita, ovat sertifikaattien ja asiakas-

koneiden ohjelmistojen elinkaari, näihin eivät luodut järjestelmät kykene täysin itsenäisesti käytössä olevilla konfiguraatioilla.

6.4 Projektin tulevaisuus

Tässä työssä toteutetut SSL VPN -järjestelmät jäävät molemmat käyttöön. OpenVPN -ohjelmistoa tulee käyttämään ylläpito, koska ylläpidollisiin toimenpiteisiin voidaan toisinaan tarvita laajoja oikeuksia tietoverkkoon. Juniper Secure Access-järjestelmää tulevat käyttämään mm. opettajat, koska sillä saadaan helposti kohdennettua oikeat palvelut oikeille asiakkaille.

Molempia järjestelmiä tullaan laajentamaan hankkimalla lisää SecurID -varmistusavaimia, mikä aiheuttaa lisäkustannuksia. Syntyviä kustannuksia pyritään tulevaisuudessa pienentämään hankkimalla käyttöön Päijät-Hämeen koulutuskonsernille oma SecurID -varmistusavaimia hallinnoita ACE/Server. Toinen vaihtoehto on hankkia ainoastaan SecurID -varmistusavaimia, jotka liitetään ulkopuoliselta vuokrattuun ACE/Server -palvelimeen. Ennen hankintaratkaisua tulee kuitenkin suorittaa kustannustehokkuuslaskelma.

SecurID -varmistusavaimien lisäksi sertifikaattien hallintaa tullaan tulevaisuudessa kehittämään. Tässä työssä luodut sertifikaatit tehtiin kaikki käsin. Tulevaisuudessa järjestelmiin liitettävien koneiden määrän kasvaessa tulee käsinhallittavuudesta kuitenkin monimutkaista. Siksi Päijät-Hämeen koulutuskonsernin sertifikaattipalvelimeen tullaan luomaan automaattinen sertifikaattien hallintajärjestelmä. Hallintajärjestelmän tehtäväksi tulee asiakaskoneiden sertifikaattien koko elinkaaresta huolehtiminen.

Juniper Secure Access-järjestelmä tulee myös kokemaan muutoksia. Tulevaisuudessa järjestelmässä tullaan etätyöskentelyyn käyttämään pääsääntöisesti sen tarjoamaan RDP -yhteyttä. RDP -yhteys mahdollistaa paljon kaistanleveyttä tarvitsevien ohjelmien nopeamman käyttämisen sekä henkilökohtaisen levyjaon tuomisen käyttäjille.

Käytettäessä RDP -yhteyttä, ei asiakaskoneiden client/server -ohjelmistot tarvitse jatkuvaa päivitystä uuden ohjelmistoversion saavuttua. Tällöin etäkäyttöön riittää, että RDP -palvelimen client/server -ohjelmistot ovat ajan tasalla. Tämä skenaario tulee kysymykseen silloin, kun asiakkaan tietokone ei ole ollut Päijät-Hämeen koulutuskonsernin sisäverkossa hakemassa uusia ohjelmistopäivityksiä.

RDP -yhteydestä huolimatta client/server -sovelluksia tarjoavasta asiakaskoneisiin asennettavasta ohjelmasta ei tulla kuitenkaan luopumaan. Sen tehtävänä on palvella varajärjestelmänä, jos RDP -palvelin on saavuttamattomissa.

OpenVPN -palvelu tullaan säilyttämän projektin jälkeisessä tilassaan. Asiakaskoneen asennusohjelmasta tehdään kuitenkin SMS -palvelimella hallittava paketti. Tällöin ohjelmiston voi automaattisesti asentaa sitä tarvitseville koneille.

Tämän työn tuottamat etäkäyttöjärjestelmät ovat tietoturvallisia oikein käytettynä. Käytettäessä vahvoja salausalgoritmeja sekä käyttäjän että käytettävän tietokoneen tunnistusta, on järjestelmään murtautuminen tai tiedon salakuuntelu vaikeaa. Mahdolliset ohjelmistovirheet vaikuttavat kielteisesti toteutettujen järjestelmien tietoturvaan. Näitä on kuitenkin mahdollista ehkäistä päivittämällä ohjelmistot aina kun uudet tietoturvapäivitykset on julkaistu. Lisäksi tulee huolehtia asiakaskoneiden virustorjunnan ajantasaisuudesta ja palomuureista.

Tietoturvauhan aiheuttavat myös etäkäyttöjärjestelmien käyttäjät. Väärinkäytettynä ja saastuneelta tietokoneelta otettavat yhteydet Päijät-Hämeen koulutuskonsernin sisäverkkoon voivat olla tuhoisia. Lisäksi kadonneilta tietokoneilta on mahdollista yrittää ottaa yhteyksiä sisäverkkoon. Siksi on ensiarvoisen tärkeää, että käyttäjät ilmoittavat heti kadonneista tietokoneista ylläpitoon. Ilmoittamisen jälkeen kadonneilta tietokoneilta voidaan evätä kirjautumisoikeus CRL -listoilla. Ilmoitusvelvollisuus koskee myös SecurID -varmistusavaimia ja niiden henkilökohtaisia salasanoja.

Yleisesti etätyöskentely on nyky-yhteiskunnassa lisääntymässä. Enää ei haluta olla sidoksissa yhteen fyysiseen paikkaan työtavoitteiden saavuttamiseksi, vaan töitä halutaan tehdä siellä, missä parhaiten työnteko sillä hetkellä onnistuu. Molemmat

SSL VPN -toteutukset suoriutuivat erinomaisesti tämän ja muut niille asetetut tavoitteet. Luodut järjestelmät mahdollistavat tietoturvallisen ja helpon etätyöskentelyn lähes mistä tahansa. Tulevaisuudessa niiden levittyä laajempaan käyttöön tulevat ne helpottamaan käyttäjien etätyöskentelyä merkittävästi. Tämä tulee näkymään myös työnteossa parantuneena tuottavuutena.

LÄHTEET

Authentication 2008. [online]. Wikipedia [viitattu 12.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/Authentication

Certificate Authority 2008. [online]. Wikipedia [viitattu 7.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/Certificate_authority

Certificate revocation list 2008 [online]. Wikipedia [viitattu 8.2.2008]. Saatavissa: http://en.wikipedia.org/wiki/Certificate_revocation_list

Comer, D. 2000. TCP/IP. Jyväskylä: Gummerus Kirjapaino Oy

Cyptographick hash funcktion 2008. [online]. Wikipedia [viitattu 13.1.2008]. Saatavis-sa: http://en.wikipedia.org/wiki/Cryptographic_hash_function

Dierks, T. & Allen, C. The TLS Protocol 1999.[online]. IETF [viitattu 6.1.2008]. Saa-tavissa: http://www.ietf.org/rfc/rfc2246.txt

Encryption 2008. [online]. Wikipedia [viitattu 12.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/Encrypt

Haller, N. Metz, C. Nesser, P. & Straw, M. OTP 1998. [online]. IETF [viitattu 28.2.2008b]. Saatavissa: http://www.faqs.org/rfcs/rfc2289.html

Hosner, C. OpenVPN and the SSL VPN Revolution [verkkojulkaisu]. Sans Insti-tute [viitattu 5.1.2008]. Saatavissa: http://www.sans.org/reading_room/whitepapers/vpns/1459.php

Housley, R. Polk, W. Ford, W. & Solo, D. Internet X.509 Public Key Infrastructu-re Certificate and Certificate Revocation List (CRL) Profile 2002. [online]. IETF

[viitattu 7.1.2008]. Saatavissa: http://tools.ietf.org/html/rfc3280

Introduction (SSL/TLS in Windows Server 2003) 2003. [online]. Microsoft TechNet [viitattu 17.1.2008]. Saatavissa: http://technet2.microsoft.com/windowsserver/en/library/9d47b6a2-3216-45fc-9bb8-41a7d89e42d11033.mspx?mfr=true

One-time Password 2008. [online]. Wikipedia [viitattu 10.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/One-time_password

Perlmutter, B. & Zarkower, J. 2001. Virtuaaliset Yksityisverkot. Helsinki: Edita.

PKI 2008. [online]. Wikipedia [viitattu 8.1.2008f]. Saatavissa: http://en.wikipedia.org/wiki/Public_key_infrastructure

Public-key cryptography 2008. [online]. Wikipedia [viitattu 14.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/Asymmetric_key_algorithm

SecurID 2008.[online]. Wikipedia [viitattu 9.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/Securid

SSL VPN 2008. [online]. Wikipedia [viitattu 10.3.2008] Saatavissa: http://fi.wikipedia.org/wiki/SSL_VPN

Steinberg, J. & Speed, T. 2005. SSL VPN. Birmingham: Packt Publishing Ltd.

Symmetric-key algorithm 2008. [online]. Wikipedia [viitattu 14.1.2008], Saatavissa: http://en.wikipedia.org/wiki/Symmetric-key_algorithm

The Internet Key Exchange (IKE) 2008. [online]. IETF [Viitattu 16.1.2008]. Saatavissa: http://www.ietf.org/rfc/rfc2409.txt

Wyler, N. Fausett, T. Fletcher, K. Foxhoven, P. Lucas, M. Miller, K. Peterson K.

& Woodberg B. 2007. Juniper Networks Secure Access SSL VPN Configuration Guide. Burlington: Syngress Publishing Inc.

X.509 2008. [online]. Wikipedia [viitattu 8.1.2008]. Saatavissa: http://en.wikipedia.org/wiki/X.509

LIITTEET

Liite 1.

OpenVPN palvelin konfiguraatio

```
local a.b.c.d
port 80
proto tcp
dev tun
ca /kansio/certnew.cer
cert /kansio/server.crt
key /kansio/server.key  # This file should be kept secret
crl-verify poistot.pem
dh /kansio/dh1024.pem
server 10.9.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1"
push "dhcp-option DNS a.b.c.d"
keepalive 10 120
tls-auth ta.key 0 # This file is secret
comp-lzo
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
verb 3
plugin /kansio/openvpn-auth-pam.so /kansio/openvpn
chroot /kansio
reneg-sec 0
socket-flags TCP_NODELAY
push "socket-flags TCP_NODELAY"
```

Liite 2.

OpenVPN asiakaspään konfiguraatio

```
client
win32-gui
dev tun
proto tcp
remote a.b.c.d 80
remote a.b.c.d 80
remote-random
resolv-retry infinite
nobind
persist-key
persist-tun
ca cacert.crt
cryptoapicert "SUBJ:PHKK"
tls-auth ta.key 1
comp-lzo
verb 3
auth-user-pass
reneg-sec 14400
auth-retry interact
auth-nocache
```

Liite 3.

OpenVPN palomuuri säännöt

```
*filter
:INPUT ACCEPT [291:20553]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [364:35430]
:RH-Firewall-1-INPUT - [0:0]
:OPENVPN - [0:0]
#estetaan tunnelista ssh yhteys openvpn palvelimeen
-A INPUT -i tun+ -p tcp -s 10.0.0.0/8 -d 10.0.0.0/8 --dport 22 -j DROP
-A INPUT -i tun+ -p tcp -s 10.0.0.0/8 -d a.b.c.d/32 --dport 22 -j DROP
-A INPUT -i tun+ -p tcp -s 10.0.0.0/8 -d a.b.c.d/32 --dport 22 -j DROP
#sallitaan muut yhteydet tunnelista
-A INPUT -i tun+ -j ACCEPT
-A FORWARD -i tun+ -s 10.8.0.0/24 -j OPENVPN
#verkon 10.9.0.0/24 nat rajoitukset
#sallittuja palvelimia
-A OPENVPN -d a.b.c.d/24 -j ACCEPT
-A OPENVPN -d a.b.c.d/32 -j ACCEPT
#sallittu LAMK DMZ
-A OPENVPN -d a.b.c.d/24 -j ACCEPT
#dropataan loput
-A OPENVPN -d a.b.c.d/20 -j LOG --log-level 1 --log-prefix "DROP "
-A OPENVPN -d a.b.c.d/20 -j DROP
-A OPENVPN -d a.b.c.d/22 -j LOG --log-level 1 --log-prefix "DROP "
-A OPENVPN -d a.b.c.d/22 -j DROP
-A OPENVPN -d a.b.c.d/16 -j LOG --log-level 1 --log-prefix "DROP "
-A OPENVPN -d a.b.c.d/16 -j DROP
#sallitaan paasy internettiin
-A OPENVPN -d 0.0.0.0/0 -j ACCEPT
#kielletaan kaikki muut tunnelit
-A FORWARD -i tun+ -j DROP
#sisäänpäin sallitut yhteydet
-A INPUT -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -i eth1 --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
*nat
:PREROUTING ACCEPT [43:2096]
:POSTROUTING ACCEPT [1:67]
:OUTPUT ACCEPT [1:67]
-A POSTROUTING -s 10.0.0.0/8 -d a.b.c.d/22 -o eth0 -j SNAT --to-source a.b.c.d
-A POSTROUTING -s 10.0.0.0/8 -d a.b.c.d/24 -o eth0 -j SNAT --to-source a.b.c.d
-A POSTROUTING -s 10.0.0.0/8 -d a.b.c.d/25 -o eth0 -j SNAT --to-source a.b.c.d
-A POSTROUTING -s 10.0.0.0/8 -d 0.0.0.0/0 -o eth1 -j SNAT --to-source a.b.c.d
COMMIT
*mangle
:PREROUTING ACCEPT [43:2096]
:POSTROUTING ACCEPT [1:67]
:OUTPUT ACCEPT [1:67]
:INPUT ACCEPT
-A PREROUTING -s a.b.c.d/16 -p tcp --dport 80 -j MARK --set-mark 1
-A OUTPUT -d a.b.c.d/16 -p tcp --sport 80 -m tcp -j MARK --set-mark 1
COMMIT
```

Liite 4.

OpenVPN asiakaspään käynnistystiedosto

```
@echo off

net start | find "OpenVPN Service" /c > %temp%\TEMPIP.txt
FOR /F "tokens=1 delims=:" %%a in (%temp%\TEMPIP.txt) do set IP=%%a
del %temp%\TEMPIP.txt


if "%IP%" == "1" GOTO kala
if "%IP%" == "0" GOTO kissa

set valinta=

:kissa
echo VPN ei ole p„„ll„
set /p valinta=avataanko VPN yhteys [k/e]
if "%valinta%"=="k" goto avaa
if "%valinta%"=="e" goto loppu
echo "%valinta%" ei ole kelvollinen
echo.
set valinta=
goto kissa


:kala
echo VPN on p„„ll„
set /p valinta=suljetaanko VPN yhteys [k/e]
if "%valinta%"=="k" goto sulje
if "%valinta%"=="e" goto loppu
echo "%valinta%" ei ole kelvollinen
echo.
set valinta=
goto kala


:avaa
net start "OpenVPN Service"
echo VPN yhteys on p„„ll„
goto loppu

:sulje
net stop "OpenVPN Service"
echo VPN yhteys on pois p„„lt„
goto loppu

:loppu
pause
```

Liite 5.

Juniper Secure Access käyttäjän ohje kirjautumiseen

Kirjautuminen:

Tämän dokumentin tarkoitus on opastaa kirjautuminen Juniper VPN-SSL www liittymään.

Huom.

Järjestelmä sulkee istunnon automaattisesti 10min käyttämättömyyden jälkeen. Käyttöliittymä näyttää oikeassa ylänurkassa kellon, joka kertoo istunnon jäljellä olevan ajan (60min), jonka jälkeen järjestelmä sulkee istunnon automaattisesti.

Järjestelmässä on kaksi eri käyttöliittymää, käyttöliittymä valitaan sen mukaan, onko kone tunnistettu sertifikaatilla vai ei. Konsernin koneissa on vaadittava sertifikaatti, mutta esim. kioski koneissa ei ole. Koneissa, joissa on sertifikaatti, on myös enemmän palveluita saatavilla.

1 Avaa Internet Explorerilla osoite https://vpnintra.phkk.fi/

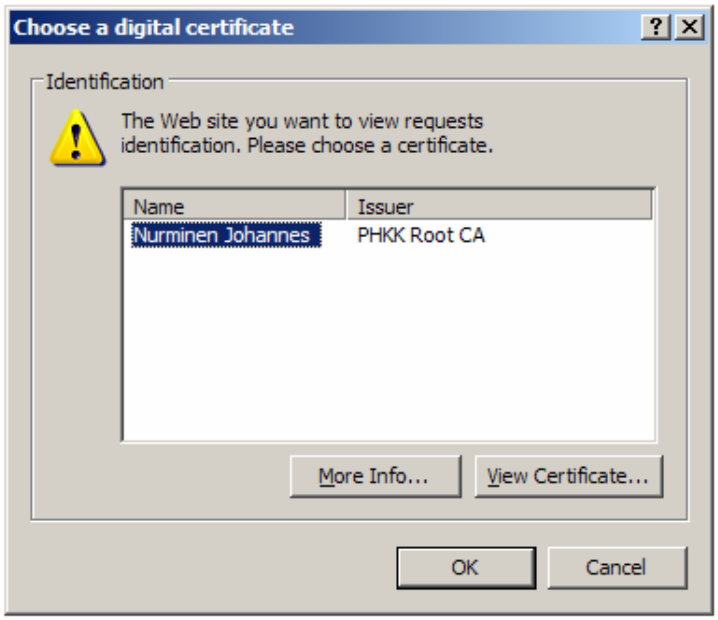
2. Selain antaa sertifikaatti varoituksen, paina "yes"

3. Syötä kohtaan ”Username” AD käyttäjänimi ja ”Password” kohtaa pinkoodi, jonka jälkeen tokenissa oleva luku. Esim. jos Pinkoodi on 1111 ja tokenissa oleva luku on 727548 niin ”Password” kenttään tulee 1111727548.

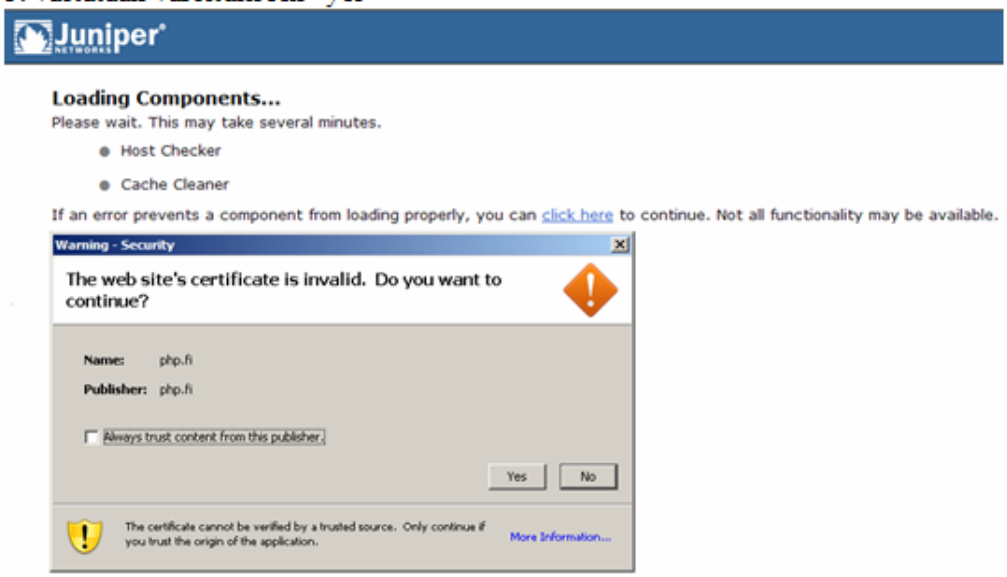
RSA SecurID Token

Tokenissa oleva luku vaihtuu aina 60s välein. Jäljellä oleva aika ilmaistaan vasemmassa nurkassa näkyvillä pylväillä. Yksi pylväs tarkoittaa 10s, eli kuvan tokenilla kestää noin 20s ennen, kuin luku vaihtuu. Jos luku vaihtuu juuri kirjautumisen aikana, on suuri todennäköisyys, että pääsy järjestelmään evätään. Sama luku ei myöskään käy kahta kertaa peräkkäin järjestelmään. Eli, jos pylväät ovat vähissä, niin kannattaa odottaa hetki uutta lukua.

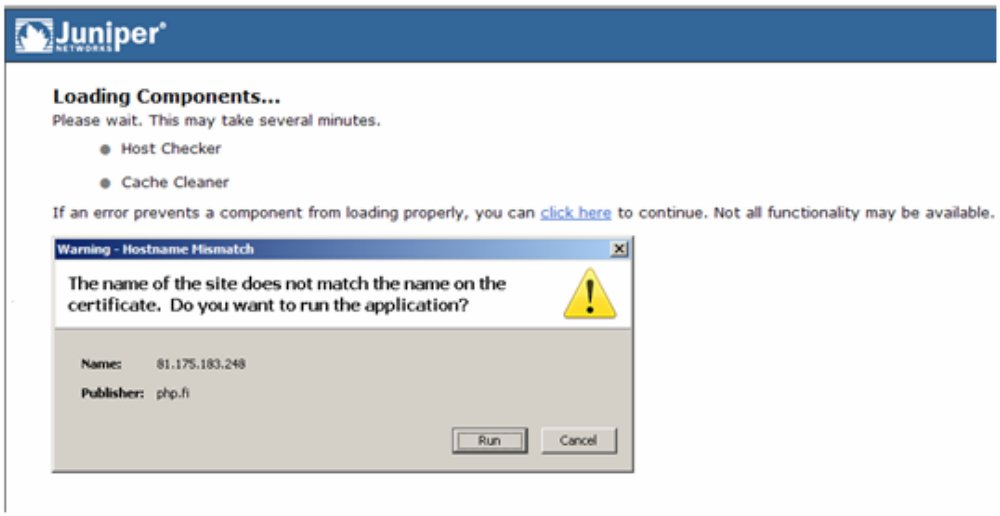
4. Järjestelmä kysyy sertifikaattia. Jos koneesta löytyy PHKK:n sertifikaatti valitaan se.



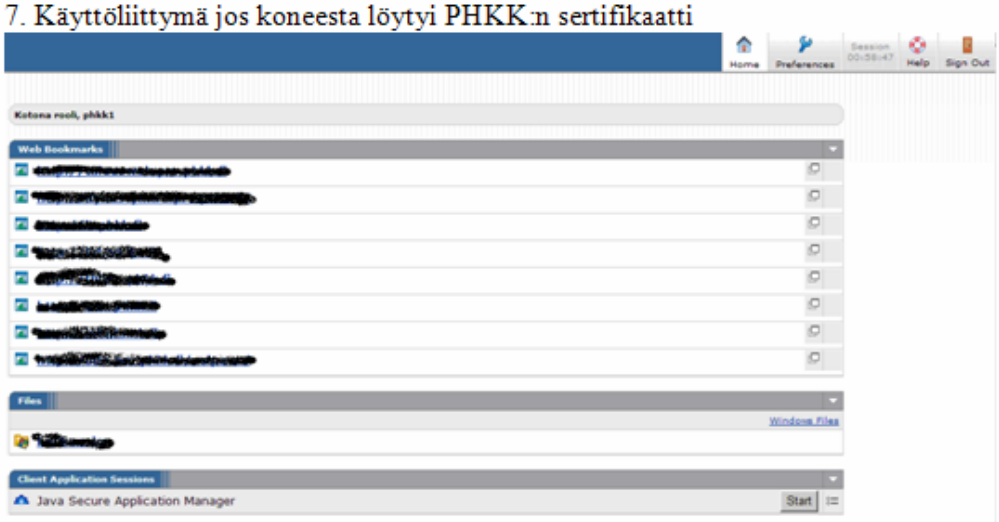
5. vastataan varoitukseen "yes"



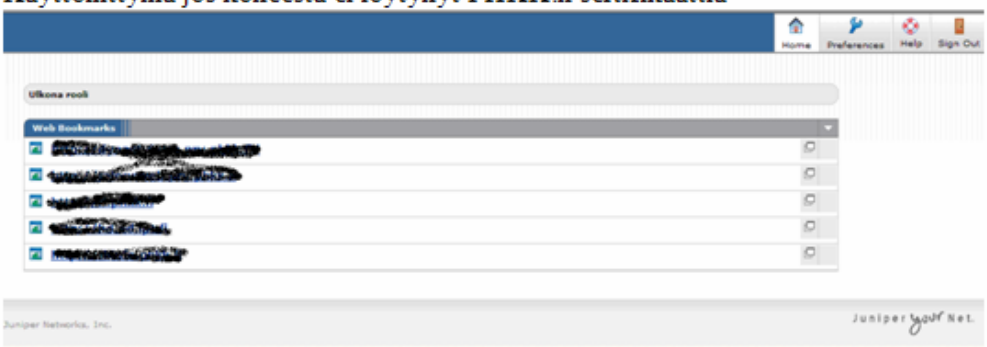
6. vastataan varoitukseen ”Run”



7. Käyttöliittymä jos koneesta löytyi PHKK:n sertifikaatti



Käyttöliittymä jos koneesta ei löytynyt PHKK:n sertifikaattia



8. Uloskirjautuminen tapahtuu painamalla oikeasta ylänurkasta löytyvää ”Sign out” nappulaa

9. sulje selain, kun tämä ilmoitus tulee ruutuun