VPN-YHDYSKÄYTÄVÄ

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2011
Lauri Syrjä

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

SYRJÄ, LAURI: VPN-yhdyskäytävä

Tietoliikennetekniikan opinnäytetyö, 55 sivua

Kevät 2011

TIIVISTELMÄ

Lahden ammattikorkeakoulun tekniikan alan tietoverkkolaboratorion käyttämän VPN-yhdyskäytäväohjelmiston kehittänyt yritys siirtyi toisen yrityksen omistukseen loppuvuodesta 2008. Ohjelmiston tuki lopetettiin ja sen avoin kehitys jatkui toisella tuotenimellä ja siirtyi lopulta OpenVPN:n vastuulle. Tästä syystä käytössä olevalle VPN-yhdyskäytävälle tarvittiin korvaava ratkaisu.

Tavoitteena oli tutustua erilaisiin VPN-yhdyskäytäväratkaisuihin ja valita ympäristöön parhaiten soveltuva tuote sekä asentaa ja konfiguroida tuote käyttövalmiiksi. Vertailtaviksi ratkaisuiksi valittiin OpenVPN Access Server -ohjelmisto sekä Cisco ASA 5505 Adaptive Security Appliance -palomuurilaite.

Työn teoriaosuudessa käydään läpi VPN-tekniikoita ja -protokollia. Aluksi tarkastellaan lyhyesti vanhempia PPTP- ja L2TP-protokollia. Seuraavaksi tutustutaan tarkemmin IPSec- ja Secure Socket Layer -tekniikoiden toimintaan sekä VPN-verkon kryptografisiin tekniikoihin. Lisäksi tutkitaan etätyöpöytäprotokollista RDP:aa, X Window Systemiä, NoMachine NX:ää sekä RFB:a.

OpenVPN Access Serverin ja Cisco ASA 5505:n vertailussa keskityttiin ratkaisujen VPN-ominaisuuksiin. Myös järjestelmien käyttöä testattiin. Molemmat ratkaisut todettiin toimiviksi ja helppokäyttöisiksi sekä helposti asennettaviksi ja ylläpidettäviksi.

Toteutettavaksi järjestelmäksi valittiin OpenVPN Access Server -ohjelmisto. OpenVPN:n hinnoittelu todettiin edullisemmaksi kuin ASA 5505:n. Ciscon palomuurilaite voitaisiin käytön lisääntyessä joutua päivittämään astetta suurempaan ja kalliimpaan malliin. Access Server tarjoaa kaikki tarvittavat ominaisuudet ja soveltuu myös käyttäjäystävällisyytensä puolesta nykyisen SSL-Explorerin korvaajaksi.

Tulevaisuuden kannalta OpenVPN Access Server on helppo ylläpidettävä. Ratkaisu ei vaadi esimerkiksi opiskelijoiden vaihtuessa toimenpiteitä ulkoisen LDAP-käyttäjäautentikoinnin ansiosta.

Avainsanat: VPN, SSL VPN, OpenVPN, IPSec

Lahti University of Applied Sciences
Degree Programme in Information Technology

SYRJÄ, LAURI: VPN gateway

Bachelor's Thesis in Telecommunications Technology, 55 pages

Spring 2011

ABSTRACT

The developer of the VPN gateway software used by the telecommunications laboratory of the Faculty of Technology in Lahti University of Applied Sciences was acquired by another company near the end of 2008. Support for the software ended and open development of the software continued under a different name and was eventually taken over by OpenVPN. A replacement for the VPN gateway was required.

The goal of this thesis was to explore different VPN gateway solutions, to select the most suitable product, and to install and configure it for use. Solutions selected for the comparison were the OpenVPN Access Server software suite and the Cisco ASA 5505 Adaptive Security Appliance firewall device.

The theory section of the thesis covers VPN techniques and protocols. In the beginning older PPTP and L2TP protocols are covered in general. Next, IPSec and Secure Socket Layer techniques as well as the cryptographic technologies used in VPN networks are examined. Remote access protocols RDP, X Window System, NoMachine NX and RFB are also studied.

The focus in the comparison between OpenVPN Access Server and Cisco ASA 5505 were the VPN features of the solutions. The systems were also tested in practical use. Both solutions were found viable and easy to use, and also easy to install and maintain.

The OpenVPN Access Server software suite was selected as the system to be implemented. The price of OpenVPN was found less expensive than that of ASA 5505. With increased use, the Cisco firewall device would require to be upgraded to a bigger and more expensive product. Access Server provides all the required features and suits as a replacement for the current SSL-Explorer due to its user-friendliness.

OpenVPN Access Server will be easy to maintain. The solution does not require action for example when students change over time, thanks to its external LDAP user authentication system.

Key words: VPN, SSL VPN, OpenVPN, IPSec

SISÄLLYS

LYHENNELUETTELO

3DES	Triple Data Encryption Algorithm. Symmetrinen lohkosalausalgoritmi, joka perustuu DES-algoritmiin. Käyttää kolmea avainta datan salaamiseen.
AD	Active Directory. Microsoft Windows Server -käyttöjärjestelmien käyttäjätietokanta ja hakemistopalvelu.
AES	Advanced Encryption Standard. Lohkosalausalgoritmi, joka on laskennallisesti kevyempi ja kryptografisesti vahvempi kuin 3DES. Kehitettiin korvaamaan DES-salausalgoritmi.
AH	Authentication Header. IPSecin toinen suojausprotokolla, jonka palveluihin kuuluvat datan eheyden, datan autentikoinnin ja toiston suojan toteuttaminen.
ASA	Adaptive Security Appliance. Ciscon verkon suojalaitteiden tuotesarja.
ATM	Asynchronous Transfer Mode. Pakettikytkentäinen tietoliikenneprotokolla.
AS	OpenVPN Access Server. OpenVPN:n SSL VPN -ohjelmisto.
BGP	Border Gateway Protocol. Internetin runkoreititysprotokolla.
CA	Certificate Authority. Digitaalisia sertifikaatteja myöntävä luotettu taho.
DES	Data Encryption Standard. Vuonna 1976 kehitetty lohkosalausalgoritmi. Korvattu AES-protokollalla.

DH	Diffie-Hellman. Ensimmäinen julkistettu julkiseen avaimeen perustuva algoritmi. Avainten vaihtoon ja VPN-tunnelin luontivaiheessa käytetty algoritmi.
DSA	Digital Signature Algorithm. Digitaalisissa allekirjoituksissa käytetty julkisen avaimen algoritmi.
DSS	Digital Signature Standard. Yhdysvaltojen hallituksen standardi DSA:lle.
DXPC	Differential X Protocol Compression. Sovellus, jota NX:n X-ikkunoinnin pakkauksessa käytetään perustana.
ESP	Encapsulating Security Payload. IPSecin toinen suojausprotokolla, jonka palveluihin kuuluvat datan salauksen, yhteydettömän datan eheyden, datan autentikoinnin ja toiston suojan toteuttaminen.
FTP	File Transport Protocol. Asiakas-palvelin-arkkitehtuuria toteuttava TCP-perustainen tiedonsiirtoprotokolla.
GRE	Generic Routing Encapsulation. Ciscon kehittämä tunnelointiprotokolla, joka voi kapsuloida monia OSI-mallin verkkotason protokollia virtuaalisen point-to-point-linkin sisään.
HMAC	Hash-based Message Authentication Code. Salaisen avaimen ja tiivistefunktion avulla laskettu MAC, jota käytetään sekä datan eheyden tarkistukseen että datan autentikointiin.
HTTP	Hypertext Transfer Protocol. World Wide Webin tiedonsiirron perusta. Selainten ja web-palvelinten käyttämä tiedonsiirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure. SSL- tai TLS-salattu HTTP. Käyttää TCP-porttia 443.

IETF	Internet Engineering Task Force. Organisaatio, joka vastaa Internet-protokollien standardoinnista.
IIS	Internet Information Services. Apachen jälkeen käytetyin, Microsoftin kehittämä HTTP-palvelinohjelmisto.
IKE	Internet Key Exchange. IPSecin käyttämä protokolla, jolla määritellään salausasetukset.
IPSec	Internet Protocol Security. Protokollajoukko IP:n suojaamiseen. Suojaa autentikoimalla ja salaamalla IP-paketin.
ISAKMP	Internet Security Association and Key Management Protocol. Internet-ympäristöön määritelty protokolla salausasetusten ja kryptografisten avainten luontiin.
IV	Initialization Vector. Määrämittainen syöte kryptografiselle algoritmille.
L2F	Layer 2 Forwarding Protocol. Ciscon kehittämä tunnelointiprotokolla VPN-yhteyden luontiin Internetin yli.
L2TP	Layer 2 Tunneling Protocol. VPN-tunnelointiprotokolla, joka ei itsessään salaa liikennettä, vaan luottaa tunnelissa kulkevaan salausprotokollaan.
LDAP	Lightweight Directory Access Protocol. Sovellusprotokolla hakemistojen lukemiseen ja muokkaamiseen IP-verkon yli.
LSP	Layered Service Provider. DLL, joka voi TCP/IP-pinossa siepata ja muokata internetliikennettä.

MAC	Message Authentication Code. Viestin autentikointikoodi, joka lasketaan MAC-algoritmilla salaisesta avaimesta ja mielivaltaisen pituisesta viestistä.
MD5	Message-Digest algorithm 5. Vuonna 1991 kehitetty tarkistussummafunktio, joka tuottaa 128-bittisen tarkistussumman.
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol. Microsoftin versio CHAP:sta. Käyttäjän tai verkon laitteen autentikointiprotokolla.
NAT	Network Address Translation. Osoitteenmuunnos.
NIST	National Institute of Standards and Technology. Yhdysvaltalainen mittaus-standardilaitos.
PKCS	Public-key cryptography standards. RSA Securityn kehittämä ja julkaisema joukko julkisen avaimen standardeja.
PKI	Public Key Infrastructure. Digitaalisten sertifikaattien hallinnointijärjestelmä.
POP3	Post Office Protocol version 3. Sähköpostin hakuprotokolla, joka toimii TCP/IP-yhteyden päällä.
PPP	Point-to-Point Protocol. Datalinkkiprotokolla, jota yleensä käytetään tuottamaan datalinkkikerroksen palveluja yhteyksiin, joihin niitä ei ole sisäänrakennettu.
PPTP	Point-to-Point Tunneling Protocol. VPN-protokolla, joka käyttää TCP:tä komentokanavana ja GRE-tunnelointia PPP-pakettien kapsulointia varten.

QoS	Quality of Service. Mekanismi resurssienvarauksen hallintaan tietoliikenneverkoissa.
RC4	Rivest Cipher 4. Yleisin jonosalausmenetelmä, jota käytetään mm. SSL:ssä.
RDP	Remote Desktop Protocol. Microsoftin etätyöpöytäprotokolla.
RFB	Remote Framebuffer. VNC:ssa käytetty etätyöpöytäprotokolla.
RFC	Request for Comments. IETF:n kokoelma internetstandardeja.
RSA	Rivest, Shamir & Adleman. Yleensä digitaalisissa allekirjoituksissa ja salaisten avainten salauksessa käytetty algoritmi.
SHA-1	Secure Hash Algorithm 1. Törmäyksettömänä ja yksisuuntaisena pidetty tiivistefunktio, jonka tiiviste on suurempi kuin MD5:n ja siksi SHA-1:tä pidetään turvallisempana.
SMTP	Simple Mail Transfer Protocol. Sähköpostin lähetysprotokolla.
SPI	Security Parameter Index. Otsikkoon lisätty tunnistetieto IPSec-tunnelointia käytettäessä.
SSH	Secure Shell. Unix-järjestelmien suojattu etähallintaprotokolla.
SSL	Secure Sockets Layer. TLS:n edeltäjä. Netscapen alunperin kehittämä kryptografinen protokolla, joka suojaa tietoliikenteen internetin yli.
TLS	Transport Layer Security. SSL:n pohjalta kehitetty IETF:n standardoima protokolla, joka suojaa tietoliikenteen internetin yli.

URL	Uniform Resource Locator. Määritelmä, mistä resurssi löytyy ja mekanismi resurssin hakemiseen. Parhaiten tunnettu esimerkki URL:n käytöstä on web-sivujen osoitteet.
VNC	Virtual Network Computing. Graafinen työpöydän jakamisjärjestelmä, joka käyttää RFB-protokollaa etäyhteyden luontiin.
VPN	Virtual Private Network. Julkista tietoliikenneverkkoa käyttävä verkko, joka mahdollistaa etäkäyttäjien ja -toimipisteiden yhdistämisen yksityiseen verkkoon.
WAN	Wide Area Network. Laajan alueen kattava verkko, joka on yhdistää LAN:t ja muut verkot toisiinsa. Tarkoittaa yleensä kaupungin, maantieteellisen alueen tai maan rajat ylittävää verkkoa.

1 JOHDANTO

1.1 Työn tausta

Työn tavoitteena oli tutkia ja toteuttaa Lahden ammattikorkeakoulun tekniikan alan tietoverkkolaboratoriolle VPN-yhdyskäytäväratkaisu nykyisen tilalle. Käytössä oleva järjestelmä on täysversio avoimen lähdekoodin SSL-Explorerista, jota kehittänyt 3SP Ltd vuoden 2008 lopussa siirtyi Barracuda Networksin omistukseen. Barracuda Networksin ostettua 3SP Ltd loppui myös SSL-Explorerin tukipalvelut ja avoin kehitys. SSL-Explorerin kehitys haarautui ensin Adito-nimiseen ohjelmistoon, joka toimi myöhemmin pohjana OpenVPN ALS:lle (OpenVPN ALS 2011).

Nykyinen järjestelmä palvelee lähinnä kolmannen ja neljännen vuoden opiskelijoita ja henkilökuntaa, joiden yhteismäärä on arviolta hieman alta 80 henkilöä. Tavoitteena oli alustavasti pystyttää järjestelmä palvelemaan samaa käyttöä kuin nykyinen järjestelmä, eli toimimaan VPN-yhdyskäytävänä laboratorioiden etäkäyttöä varten.

Potentiaaliksi ehdokkaiksi SSL-Explorerin korvaajaksi valittiin OpenVPN Access Server -palvelinohjelmisto sekä Cisco ASA 5505 -palomuurilaite. Tutkimusongelmana oli selvittää, kumpi järjestelmistä soveltuu paremmin SSL-Explorerin korvaavaksi tuotteeksi. Lisäksi selvitettiin tuotteiden ominaisuudet, hintaluokka, ylläpitoon liittyvät tehtävät, asennus sekä käyttöön ja käyttäjäkokemukseen liittyvät tekijät.

Korvaavalla järjestelmällä ei ollut kiire, koska nykyinen järjestelmä on edelleen toiminnassa. Parhaaksi nähtiin, että ratkaisut testataan ensin monipuolisesti asennuksesta loppukäyttöön ja korvataan myöhemmin nykyinen järjestelmä paremmaksi todetulla ratkaisulla.

Työssä keskitytään VPN-yhteystekniikoihin ja ominaisuuksiin sekä OpenVPN Access Serverin ja Cisco ASA 5505:n yleisten ominaisuuksien vertailuun. Jonkin verran tutkitaan myös etätyöpöytäprotokollia, vaikka niiden osalta ei nykyiseen järjestelmään tarvitse tehdä muutoksia.

1.2 Työn tavoitteet

Tavoitteena oli hyödyntää ulkoista Active Directory (AD) -käyttäjätietokantaa VPN-käyttäjien tunnistukseen. Haluttiin myös selvittää, voidaanko tunnistukseen käytetty yhteys salata. Lisäksi haluttiin selvittää Access Serverin reititystilan verkolle asettamat vaatimukset, mikä mahdollistaisi etäkäyttäjien väliset suorat yhteydet. Työn tavoitteisiin kuului myös tutkia, onnistuuko Access Serverin palomuurin konfigurointi manuaalisesti.

Tavoitteena oli verrata valittujen VPN-tuotteiden asiakasohjelmia ja testata niiden käyttöä. Asiakasohjelmista tahdottiin mielipiteitä ja käyttökokemuksia. Ratkaisuille päätettiin tehdä myös suuntaa antava hintavertailu. Molempien tuotteiden asennuksen kulku dokumentoidaan, jotta järjestelmien käyttöönotto tapahtuisi sujuvasti. VPN-ratkaisujen ylläpidolliset tehtävät haluttiin selvittää, jotta voitaisiin verrata tuotteiden mahdollisesti vaatimia ylläpitotoimenpiteitä tulevaisuudessa. Lisäksi tavoitteena oli testata nykyisten etäyhteyksien yhteensopivuus ja toiminta uuden VPN-tuotteen kanssa.

2 VPN-TEKNIIKAT

2.1 VPN-yhteydet

Virtual Private Network (VPN) on yksityinen dataverkko, joka toimii julkisen tietoliikenneinfrastruktuurin päällä säilyttäen yksityisyytensä käyttämällä tunnelointiprotokollia ja erilaisia tietoturvamenetelmiä (Scott, Wolfe & Erwin 1999, 6). VPN-verkko voidaan rinnastaa järjestelmään, jossa yksi yritys omistaa tai vuokraa linjan, jota ainoastaan kyseessä oleva yritys voi käyttää. Päätarkoituksena VPN-verkkoille on tuottaa samat edut kuin yksityisellä linjalla hyödyntäen julkista, jaettua infrastruktuuria pienentäen näin kuluja. (VPN Consortium 2008.)

VPN-verkkoteknologiat voidaan jakaa kolmeen kategoriaan: luotetut, suojatut ja hybridi-VPN:t. On huomioitava, että luotetut ja suojatut VPN:t eivät liity toisiinsa teknisesti ja voivat toimia samanaikaisesti yhdessä järjestelmässä. (VPN Consortium 2008.)

2.1.1 Luotetut VPN-verkot

Luotettujen VPN:ien nimi juontaa juurensa ajalta ennen internetin yleistymistä, jolloin VPN-verkko muodostui yhdestä tai useammasta piiristä, joka vuokrattiin yhteyden tarjoajalta. Perusajatuksena oli asiakkaan mahdollisuus käyttää vuokrapiirejä kuin fyysisiä kaapeleita omassa lähiverkossaan. Asiakkaan oli mahdollista käyttää omia IP-osoitteitaan ja toteuttaa tietoturvapolitiikkaansa. Vuokrapiiri kulki useamman kytkimen läpi ja liikennettä oli mahdollista kuunnella. Yhteyden tarjoaja oli vastuussa piirin yksityisyydestä, ja asiakkaan oli luotettava palveluntarjoajan sanaan, että piirillä ei ollut muita käyttäjiä. (VPN Consortium 2008.)

Nykyään palveluntarjoajat ovat alkaneet käyttää internetiä luotetun VPN-verkon välittäjänä. Tietoturvaa ei voida vieläkään taata, mutta uusi tapa mahdollistaa verkkosegmenttien helpon luonnin WAN-ympäristöissä. Lisäksi luotettujen VPN-

verkkojen osien hallinnointi on mahdollista tehdä keskitetysti ja yleensä palveluntarjoaja takaa palvelun laadun (Quality of Service, QoS). (VPN Consortium 2008.)

Luotettua VPN:ä käytetään yleensä, koska halutaan käyttää tiettyä reittiä, jolla on määrätyt ominaisuudet ja joka on yhden palveluntarjoajan tai luotetun palveluntarjoajaliiton hallinnassa. Asiakas voi käyttää omaa yksityistä IP-osoiteavaruuttaan ja mahdollisesti myös hoitaa liikenteen reitityksen. Asiakkaan on yleensä mahdotonta tietää VPN:n reitit, tai edes olla varma koko VPN:n olevan olemassa. Palveluntarjoajaan on vain luotettava. (Lewis 2006.)

Luotetun VPN:n vaatimuksiin kuuluu, että ainoastaan palveluntarjoaja voi vaikuttaa VPN-yhteyden reitin luontiin ja muutoksiin. Kukaan muu paitsi palveluntarjoaja ei myöskään saa päästä muuttamaan, lisäämään tai poistamaan dataa VPN-yhteyden reitillä. Lisäksi verkon ylläpidon suunnittelua varten on reititys ja osoitteistus tehtävä ennen VPN:n luontia. (VPN Consortium 2008.)

Nykyään tarjolla on erilaisia tekniikoita luotettujen VPN-yhteyksien luontiin. Eri tekniikat voidaan jakaa OSI-mallin tasoilla kaksi ja kolme toimiviin luokkiin. L2-tekniikoihin kuuluvat Frame Relay, ATM sekä L2-kehysten kuljettaminen MPLS-verkon yli. L3-tekniikkana toimii MPLS käyttäen BGP-protokollaa VPN-reititykseen. (Lewis 2006.)

2.1.2 Suojatut VPN-verkot

Internetin yleistyessä käytettynä datasiirtotienä kasvoi myös datan tietoturvan tarve sekä asiakkaille että palveluntarjoajille. Laitevalmistajat alkoivat kehittää protokollia, jotka mahdollistivat liikenteen kryptaamisen verkon reunalla tai lähtöpisteenä toimivalla tietokoneella ja dekryptaamisen liikenteen saapuessa yrityksen verkkoon tai vastaanottavalle tietokoneelle. Kryptattu liikenne toimii kuin se kulkisi tunnelissa reitin päästä päähän. Vaikka hyökkääjä saisi kaapattua liikennettä, ei siihen voi tehdä muutoksia ilman, että muunnetut paketit huomattaisiin ja hylättäisiin vastaanottopäässä, eikä liikenteestä saa luettua mitään selväkielistä infor-

maatiota. Kryptausta hyödyntäviä verkkoja sanotaan suojatuiksi VPN:ksi. (VPN Consortium 2008.)

Suurin syy käyttää suojattua VPN:a on mahdollisuus lähettää arkaluontoista informaatiota julkisen verkon yli tarvitsematta huolehtia siitä, kuka datan saattaa matkalla nähdä. Suojatut VPN-yhteydet ovat erityisen arvokkaita etäkäyttöön, kun käyttäjä on yhteydessä internetiin oman verkonvalvojansa toimiympäristön ulkopuolella, kuten kotona, hotellihuoneessa tai lentokentällä. (VPN Consortium 2008.)

Suojatun VPN:n vaatimuksiin kuuluu kaiken liikenteen kryptaaminen ja autentikointi. Monet protokollat mahdollistavat kryptaamattomien VPN:ien luonnin. Ilman liikenteen salausta on verkko toki turvallisempi kuin ilman sekä salausta että autentikointia, mutta koska verkolta puuttuu salaus ja sitä kautta myös yksityisyys ei kyseessä ole vielä VPN. Muita vaatimuksia suojatulle VPN:lle on tunnelin molempien päiden ylläpitäjien yhteinen päätös yhteyden tietoturvaominaisuuksista. VPN-yhteyden tietoturvaominaisuuksiin ei myöskään saa olla pääsyä kenelläkään ulkopuolisella, muutoin mahdollinen hyökkääjä voi esimerkiksi heikentää salausta tai vaikuttaa käytössä oleviin salausavaimiin. (VPN Consortium 2008.)

Vaatimukset täyttäviä tekniikoita suojatuille VPN:ille ovat IPsec käyttäen salausta joko tunnelointi- tai kuljetustilassa tai IPsec L2TP:n sisällä. Jälkimmäinen on merkittävässä client-server-etäkäytössä suojatuissa VPN-verkoissa. Tekniikoihin lukeutuu myös joko SSL 3.0:n tai TLS:n käyttäminen salattuna. Kaikki edellä mainitut tekniikat poislukien SSL 3.0 ovat IETF:n standardoimia, ja kaikilla tekniikoilla on monia laitevalmistajia, joiden tuotteet ovat osoittautuneet hyvin yhteensopiviksi käytännössä. (Lewis 2006.)

2.1.3 Hybridi-VPN

Suojattu VPN voidaan toteuttaa osana luotettua VPN:a luoden markkinoille paljon uudemman hybridi-VPN:n. Yhteyden suojattu osa voi olla joko asiakkaan hallin-

nassa tai saman palveluntarjoajan ylläpidossa, kuin joka toteuttaa VPN:n luotetun osan. Joskus koko hybridiverkko on salattu suojatun VPN:n tekniikalla, mutta yleensä yhteydestä on suojattu vain osa. (VPN Consortium 2008.)

Hybridi-VPN:n yleisin käyttöönottokohde on jo ennalta käytössä oleva luotettu VPN-yhteys, ja osa yritystä tarvitsee osan yhteydestä myös suojattuna. Mikään nykyisistä luotetuista VPN-tekniikoista ei estä ottamasta hybridiverkkoa käyttöön. Osa valmistajista tekee jo järjestelmiä, jotka tukevat nimenomaan hybridi-VPN:ien luontia. (VPN Consortium 2008.)

Suojatun VPN:n osoiterajojen on oltava erittäin tarkat toimiessaan luotetun VPN:n sisällä. Verkon ylläpitäjän on oltava varma kulkeeko liikenne suojatun VPN:n sisällä hybridiverkon minkä tahansa osoiteparin välillä. Suojatun VPN:n käyttöönotto luotetussa VPN-verkossa ei lisää koko luotetun verkon turvaa, vaan ainoastaan suojatun osan turvaa. Hybridiverkossa suojattu VPN hyötyy luotetun VPN:n ominaisuuksista, kuten QoS:stä. (VPN Consortium 2008.)

2.2 VPN-verkon kryptografiset tekniikat

Turvallinen VPN-yhteys muodostuu kolmen perusedellytyksen täyttyessä. VPN-yhteydeltä vaaditaan ensinnä autentikointia, eli VPN:n käyttäjä voi olla varma, että yhteys on tiettyyn laitteeseen, esimerkiksi palvelimeen. Tunnistus pätee niin ikään käyttäjiin, eli palvelin voi tunnistaa käyttäjän tai tämän päätelaitteen. (Frahim & Huang, 2008, 17.)

Toisena vaatimuksena on VPN-verkon luotettavuus, joka takaa datan tietosuojan salaamalla datan sisällön. Viimeisenä vaatimuksena on datan sisällön koskemattomuus tiedonsiirron aikana. Vaatimusten täyttymiseksi VPN-verkoissa käytetään erilaisia kryptografisia menetelmiä. (Frahim & Huang 2008, 17.)

2.2.1 Tiiviste ja tiivistefunktiot

Tiiviste eli hajautusarvo varmistaa siirretyn viestin eheyden. Tiivistealgoritmin ominaisuuksiin kuuluvat yksisuuntaisuus ja törmäyksettömyys. Yksisuuntaisuus tarkoittaa, ettei tiivisteestä saa laskettua alkuperäistä dataa mitenkään. Törmäyksettömyys taas tarkoittaa, että samaa tiivistettä ei synny kahdelle eri viestille. Määrämittaisia tiivisteitä voidaan käyttää eräänlaisina digitaalisina sormenjälkinä, koska isommastakin tiedostosta voidaan laskea tiiviste. Kun tämä tiedosto lähetetään turvattoman kanavan yli ja lasketaan uusi tiiviste, voidaan vertaamalla tiivisteitä keskenään todeta, onko tiedosto muuttunut siirron aikana. (Network Associates, Inc. 1998, 19 - 20.)

Yleisimmät tiivistefunktiot ovat Message Digest Algorithm 5 (MD5) ja Secure Hash Algorithm 1 (SHA-1). Molempia pidetään yksisuuntaisina ja erittäin törmäyksettöminä algoritmeina. MD5 tuottaa 128-bittisen tiivisteen ja SHA-1 160-bittisen. SHA-1 on pidetty turvallisempana suuremman kokonsa puolesta. Nykypäivänä ei yleensä ole suorituskyvyn kannalta enää merkitystä, kumpaa algoritmia käytetään, niinpä SHA-1 on suositeltava hajautusarvoalgoritmi VPN-käyttöön. (Frahim & Huang 2008, 18.)

Message Authentication Code (MAC) eli viestin autentikointikoodi on kryptografinen tarkistussumma, jota käytetään todentamaan viestin eheys siirron aikana. MAC:n luontiin voidaan käyttää joko salausalgoritmia, kuten Data Encryption Standard (DES), tai hajautusarvoalgoritmia. Hajautusarvon laskenta on yleisesti paljon nopeampi kuin salausalgoritmit, minkä takia tiivisteperustainen MAC, tai HMAC, hash-based MAC, on yleisin tapa eheyden tarkistukseen. HMAC on avaimellinen tiivistefunktio. HMAC-tarkistussumman laskemiseksi on valittava kaksi parametria: tiivistefunktio ja avain. Avain luodaan yleensä avaimen neuvottelu- ja vahvistusvaiheessa kahden laitteen välillä. HMAC on kaksitasoinen tiiviste, eli haluttu viesti lasketaan kaavasta, jossa tiivistefunktio laskee viestistä ja merkkijonosta avaimen avulla tiivisteen, joka vielä uudelleen lasketaan toisen merkkijonon ja avaimen avulla uudeksi tiivisteeksi. Kaksitasoisuus tekee

HMAC:sta paljon turvallisemman kuin yksinkertaisemmat avaimelliset tiiviste-funktiot. (Frahim & Huang 2008, 18 - 19.)

MAC voidaan muodostaa myös salausalgoritmin avulla. Salausalgoritmi voi olla joko jonosalaus- tai lohkosalausmenetelmä. Jonosalauksen avulla muodostettavassa MAC:ssa voidaan käyttää Lain, Rueppelin ja Woolvenin algoritmia, joka toimii käyttämällä todistetusti vahvaa jonosalainta. Salain pilkkoo alkuperäisen viestin kahdeksi bittivirraksi, jotka syötetään LFSR:ihin (linear feedback shift registry). Tarkistussummaksi muodostuu LFSR:jen lopullinen tila. (EMC Corporation 2010.)

Lohkosalausmenetelmän avulla muodostetun MAC:n perusajatus on salata viesti-lohkot ja tulostaa viimeinen lohko salattuna tarkistussummaksi. Yleinen kansainvälinen standardi lohkosalausmenetelmän käyttöön MAC:n muodostukseen on DES-CBC MAC. (EMC Corporation 2010.)

2.2.2 Salaus

Salausalgoritmit muuttavat selkokielisen tekstin salakieleksi. Erona hajautusarvo-algoritmeihin on salausalgoritmien tarve avaimelle sekä salaukseen että purkuun. Salausalgoritmeja on symmetrisiä ja asymmetrisiä. Symmetrinen salausalgoritmi käyttää samaa avainta sekä kryptaukseen että dekryptaukseen ja on yleensä paljon nopeampi kuin asymmetrinen salausalgoritmi (EMC Corporation 2011). Symmetrisiä algoritmeja käytetään yleensä salamaan viestin sisältö. Symmetriset algoritmit voidaan jakaa vielä vuosalaaviin, esim. RC4, ja lohkosalaaviin, esim., DES, 3DES, AES. (Russell, Kaminsky, Puppy, Grand, K2, Ahmad, Flynn, Dubrawsky, Manzuik & Permeh 2002, 167 - 168.)

Asymmetrisessä salauksessa käytetään eri avainta salaukseen ja purkuun. Toinen avaimista on julkinen ja toinen on ainoastaan omistajansa tiedossa. Riippuen avainparien käyttötavasta voidaan asymmetristä algoritmia käyttää salaukseen tai tunnistukseen. Yleisimmät asymmetriset algoritmit ovat Diffie-Hellman (DH)

-algoritmi sekä Rivest, Shamir and Adelman (RSA) -algoritmi. (Frahim & Huang 2008, 20.)

Vuonna 1987 kehitetty Rivest Cipher 4 (RC4) on käytetyin jonosalausmenetelmä. Nopeutensa ja yksinkertaisuutensa ansiosta RC4 on käytössä monessa sovelluksessa, esimerkiksi SSL ja Wired Equivalent Privacy (WEP) -protokollissa. SSL-käytössä useimmat webselaimet tukevat kahta eri avainkokoa RC4:lle: 40- ja 128-bittistä avainta. Internet Explorer 7.0 ja Firefox-selaimista lähtien on alettu tukea vahvempia salausalgoritmeja, kuten AES:ia. (Frahim & Huang 2008, 21.)

Data Encryption Standard (DES) on IBM:n 1970-luvulla suunnittelema, käytetyin symmetrinen salausalgoritmi. DES on 64-bittinen lohkosalausmenetelmä, joka työstää kahdeksan tavun datalohkoja. Salattu data on myös kahdeksan tavun kokoinen. Purkuvaiheessa samaa algoritmia käytetään takaperin saman salausavaimen kanssa kuin salausvaiheessa. DES:n salausavaimen koko on 56 bittiä tarvittavien pariteettibittien takia. Nykyisin 56-bittinen salausavain on liian lyhyt, mikä tekee DES:stä heikon salausalgoritmin. 3DES vastaa DES:n salausavaimen pituusongelmaan. 3DES suorittaa DES-algoritmin kolme kertaa kolmella eri avaimella, mikä johtaa yhteensä 168-bittiseen salausavaimeen. (Russell ym. 2002, 170 - 172.)

Vuonna 1997 National Institute of Standards and Technology (NIST) etsi DES:n korvaavaa algoritmia, Advanced Encryption Standardia (AES). Monista ehdokkaista standardiksi valittiin Rijndael. AES on lohkosalausmenetelmä, joka työstää 128-bittisiä datalohkoja ja käyttää 128-, 192- tai 256-bittistä salausavainta. AES on laitteistoille laskennallisesti kevyempi ja kryptografisesti vahvempi kuin 3DES. AES on yksi salausvaihtoehdoista SSL v3:lle ja TLS:lle. (Russell ym. 2002, 172 - 173.)

Vuonna 1976 julkistettu Diffie-Hellman (DH) oli ensimmäinen julkistettu julkiseen avaimeen perustuva algoritmi. DH on yleensä avainten vaihtoon ja VPN-tunnelin luontivaiheessa käytetty algoritmi. Diffie-Hellman toimii seuraavasti: liikennöivät osapuolet valitsevat kaksi parametria, joista toinen on suuri alkuluku

ja toinen on luku, jonka avulla voidaan muodostaa kaikki luvut yhdestä yhtä vaille valittuun alkulukuun matemaattisen kaavan kautta. Molemmat osapuolet luovat yksityiset avaimet, jotka ovat valittua alkulukua pienemmät, sekä yksityisiä avaimia vastaavat julkiset avaimet. Julkiset avaimet vaihdetaan suojaamattoman yhteyden yli. Saatuaan vastapuolen julkisen avaimen laskevat molemmat osapuolet yhteisen salaisuuden ja päätyvät samaan lukuun, jota voidaan käyttää yhteyden salaamiseen, ja joka ei ole muiden tiedossa. (Frahim & Huang 2008, 23.)

DH:n julkisen avaimen vaihdon aikana ei ole määritetty autentikointiprosessia. Ilman osapuolten tunnistusta on algoritmi haavoittuvainen man-in-the-middle-hyökkäyksille. Autentikoitu DH-vaihto poistaa haavoittuvuuden. DH-algoritmi on käytössä muun muassa IPSec VPN:n avaimenvaihto- eli Internet Key Exchange (IKE) -protokollassa sekä TLS-protokollan avaimenvaihdossa. (Frahim & Huang 2008, 23.)

Vuonna 1977 suunniteltu RSA saa nimensä kehittäjiensä Rivestin, Shamirin ja Adlemanin mukaan. RSA:n perustana toimii fakta, että hyvin suuria numeroita ei ole mahdollista käsitellä tehokkaasti. Yleisimmät avainkoot RSA:lle ovat 512, 1024 ja 2048 bittiä. Toimintanopeudeltaan RSA on paljon hitaampi kuin salaiseen avaimeen perustuvat algoritmit, kuten DES. Hitautensa takia RSA:ta ei yleensä käytetäkään salaamaan suurta määrää dataa. RSA:n pääasialliset käyttökohteet ovat digitaaliset allekirjoitukset tai salaisten avainten salaus. (Frahim & Huang 2008, 24.)

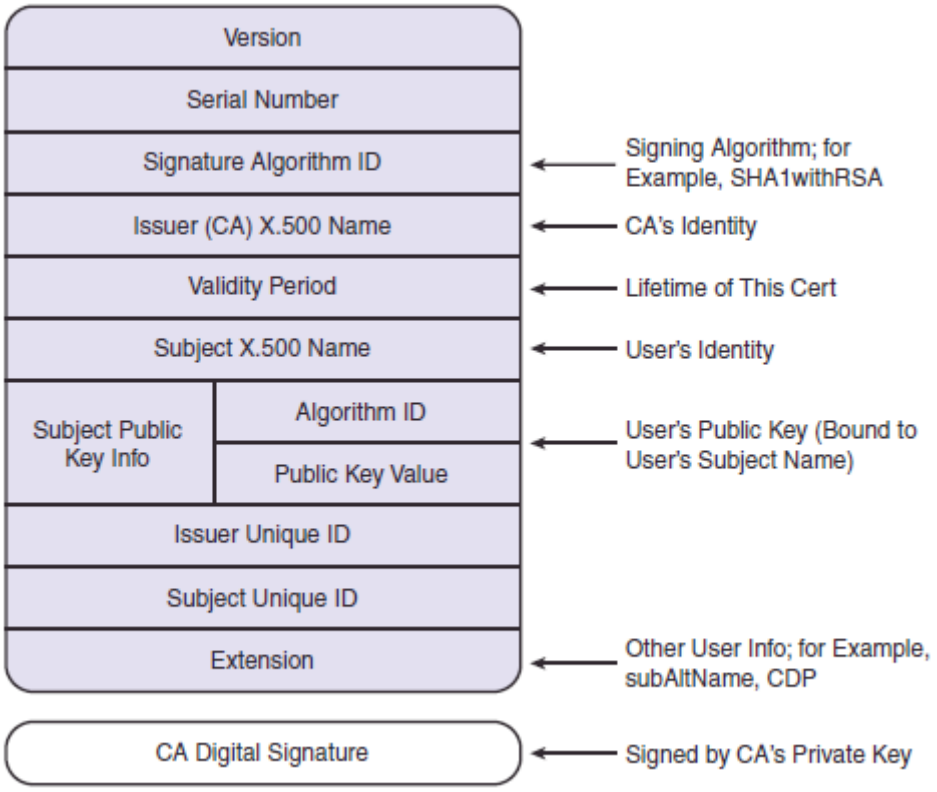
Rivest, Shamir ja Adleman, sekä Digital Signature Algorithm (DSA) ovat yleisimmät digitaalisissa allekirjoituksissa käytetyt julkisen avaimen algoritmit. Vuonna 1991 NIST ehdotti, että DSA:ta käytettäisiin sovellutuksissa, joissa tarvitaan digitaalisia allekirjoituksia. Yhdysvaltain hallitus standardoi DSA:n Digital Signature Standardina (DSS). (Frahim & Huang 2008, 24.)

2.2.3 Digitaaliset allekirjoitukset ja PKI

Digitaalinen allekirjoittaminen tarkoittaa viestin tiivisteen salausta käyttäen lähettäjän salaista avainta. Viestin tiiviste luo laskennallisesti helpon, yksisuuntaisen digitaalisen sormenjäljen viestistä. Allekirjoittaminen yksityisellä avaimella varmistaa viestin lähettäjän oikeellisuuden, koska ainoastaan allekirjoittajalla on kyseinen yksityinen avain. Allekirjoitus on helppo todentaa käyttäen vastaavaa julkista avainta. Digitaalisesti allekirjoitetun asiakirjan vastaanottaja suorittaa kaksi laskua. Vastaanottaja purkaa vastaanotetun allekirjoituksen käyttäen lähettäjän julkista avainta saaden hajautusarvon. Lisäksi vastaanotetusta viestistä lasketaan hajautusarvo ja mikäli tiivisteet täsmäävät on allekirjoitus aito. Yleisimmät digitaalisissa allekirjoituksissa käytetyt algoritmit ovat RSA MD5:n tai SHA-1:n kanssa sekä DSS SHA-1:n kanssa. (Frahim & Huang 2008, 24 - 25.)

Julkisten avainten hallintajärjestelmä (public-key infrastructure, PKI) muodostuu protokollista, standardeista ja palveluista ja tukee vastaavien järjestelmien sovelluksia. PKI mahdollistaa käyttäjien toistensa tunnistuksen käyttämällä varmentajien myöntämiä digitaalisia varmenteita. PKI-järjestelmän tärkeimmät osat ovat X.509, Public-Key Infrastructure X.509 (PKIX) sekä Public key cryptography standards (PKCS). X.509 on ITU-T:n PKI-standardi, joka määrittelee julkisten avainten varmenteiden rakenteet. PKIX on IETF:n työryhmä, jonka tehtävänä on X.509-varmenteiden pohjalta PKI:een liittyvä dokumentointi ja standardien kirjoitus. PKCS on joukko RSA-laboratorioiden suunnittelemia ja julkaisemia kryptografisia standardeja. PKCS on PKI-järjestelmän kryptografinen perusta. (Frahim & Huang 2008, 25 - 26.)

Digitaalinen varmenne eli sertifikaatti on pohjimmiltaan sidos käyttäjän henkilöllisyyden ja julkisen avaimen välillä. Varmenteet myöntää varmentajaksi (certificate authority, CA) kutsuttu kolmas osapuoli, joka vakuuttaa varmenteen aitouden. Kuviossa 1 on esitetty X.509-varmenteen rakenne. (PGP Corporation 2004.)



KUVIO 1. X.509-varmenteen rakenne (Frahim & Huang 2008)

VPN:n kannalta kiinnostavat kentät ovat allekirjoituksen algoritmi, CA:n X.500-nimi, voimassaoloaika, kohteen nimi, kohteen julkinen avain, lisäkentät sekä CA:n digitaalinen allekirjoitus. CA:n X.500-nimi kertoo käytännössä, kuka varmenteen on myöntänyt. Voimassaoloaika tarkistetaan VPN-yhdyskäytävän toimesta yhteyttä muodostaessa. Kohde tarkoittaa kenelle varmenne on myönnetty. (Frahim & Huang 2008, 27 - 28.)

Certificate Authority, CA, on luotettava taho, joka allekirjoittaa sertifikaatteja. CA:yyn luottava luottaa myös kaikkiin CA:n myöntämiin sertifikaatteihin. Yritys tai henkilö, joka haluaa allekirjoitetun sertifikaatin, lähettää hakemuksen CA:lle. CA kerää tietoja hakijasta ja sertifikaatin käyttötarkoituksen mukaan tarkistaa hakijan tietojen todenpitävyyden ennen varmenteen myöntämistä. Julkista avainta käyttävät sovellukset, kuten web-selain, tarkistavat, että varmenteen myöntäjä on luotettu CA. (EMC Corporation 2011.)

2.3 PPTP ja L2TP

2.3.1 Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) kehitettiin Point to Point Protocolin (PPP) pohjalta VPN-tunnelointia varten. PPTP:ia ei ole standardoitu, mutta sen määritykset löytyvät dokumentista RFC 2637. (Hamzeh, Pall, Verthein, Taarud, Little & Zorn 1999.)

PPTP-tunnelin hallintaa varten muodostetaan TCP-yhteys, joka käyttää porttia 1723. TCP-yhteyttä käyttäen muodostetaan toinen tunnelointiyhteys käyttäen Generic Routing Encapsulation (GRE) -protokollaa. GRE-tunnelia käytetään siirtämään kapseloituja PPP-paketteja, mikä mahdollistaa minkä tahansa PPP:n tukeman protokollan siirtämisen, tärkeimpänä IP. (Hamzeh ym. 1999.)

PPTP:n ongelmana on sen käyttämä autentikointiprotokolla Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), joka periytyy PPP:sta. MS-CHAP on heikko protokolla, koska se perustuu vahvoihin salasanoihin, jotka puolestaan ovat vaikeita muistettavia. Vuonna 2004 Joshua Wright julkaisi päivityksen kirjoittamaansa ohjelmaan ASLEAP, joka lisäsi tuen PPTP-salasanojen murtamiseen. PPTP-protokollan käyttöä ei nykyään suositella juuri sen heikkoutensa takia. (Ou 2004.)

Windows-käyttöjärjestelmissä on ollut tuki PPTP-asiakasohjelmille Windows 98:sta lähtien. Asiakasohjelma on ollut käyttöjärjestelmässä sisäänrakennettuna Windows XP:stä lähtien. PPTP-palvelintuki tuli Windows-palvelimiin Windows NT 4.0 Remote Access Servicen myötä. (Microsoft 2005.)

2.3.2 Layer Two Tunneling Protocol

Layer Two Tunneling Protocol (L2TP) on määritelty RFC-dokumentissa 2661. Protokolla pohjautuu PPTP- ja Cisco Layer Two Forwarding (L2F) -protokolliin, joista L2TP on perinyt toimintamallinsa. L2TP on VPN-tunnelointiprotokolla, jonka avulla PPP-istuntoja tunneloidaan. (Townsley, Valencia, Rubens, Pall, Zorn & Palter 1999.)

L2TP:n uusin versio, L2TPv3 on määritelty RFC-dokumentista 3931. L2TPv3 mahdollistaa muidenkin OSI-mallin toisella kerroksella toimivien protokollien, kuten Ethernet ja Frame Relay, tunneloinnin. (Lau, Townsley & Goyret 2005.)

L2TP:n datakanava ei tarjoa minkäänlaista kryptografista suojaa. Mikäli L2TP-tunneli kulkee julkisen tai turvattoman verkon yli, jossa hyökkäykset protokollaa vastaan ovat odotettavissa tai protokollan datasisällön turva on huolenaihe, voidaan ottaa käyttöön IPsec tuomaan L2TP-tunnelille turvallinen kanava. (Lau, Townsley & Goyret 2005.)

IPSec:iä käyttämällä yhdessä L2TP:n kanssa saavutetaan IPSec:n tarjoama tietoturva, johon kuuluvat pakettikohtainen datan alkuperän todennus, tiedon eheys, toistohyökkäykseltä suojaus sekä tietosuoja. L2TP/IPSec-asiakasohjelmatuki löytyy kaikista nykyisistä 32- ja 64-bittisistä Windows-käyttöjärjestelmistä viimeisimpien päivitysten myötä. (Microsoft 2002.)

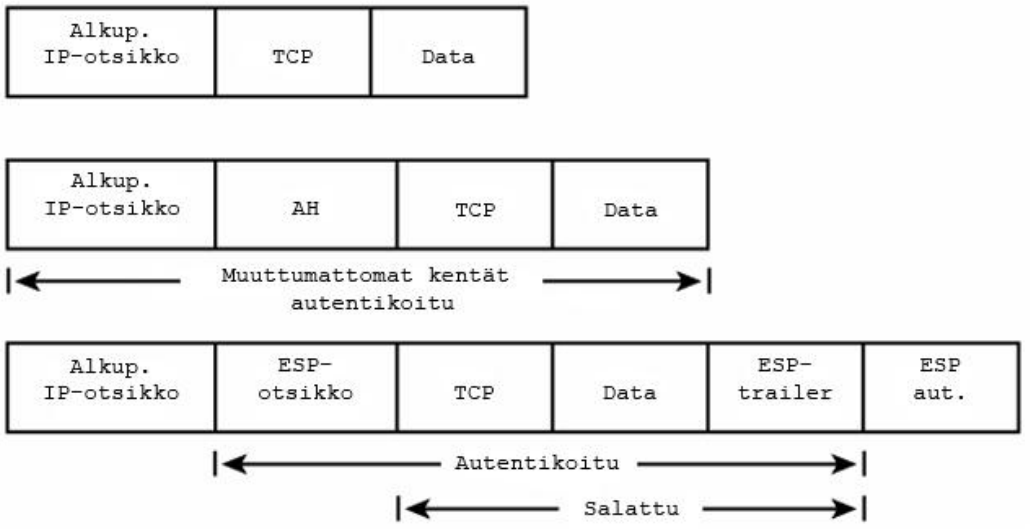
2.4 IPSec VPN

IPSec ei ole yksittäinen protokolla, vaan joukko IETF:n IPSec-työryhmän määrittelemiä protokollia. Encapsulation security payload (ESP) ja authentication header (AH) ovat IPSecin kaksi suojausprotokollaa. Avaintenhallintaan IPSec käyttää ISAKMP:ia, IKE:iä ja SKEME:ä. Lisäksi IPSeciin kuuluu algoritmeja salausta ja todentamista varten. (Bollapragada, Khalid & Wainner 2005.)

IPSec:n tehtävä on IP-paketin suojaus OSI-mallin verkkokerroksella. Suojauksella tarkoitetaan tässä tapauksessa pääsynhallintaa, tiedon eheyttä, todennusta, turvaa toistohyökkäystä vastaan sekä tietosuojaa. Toimintatiloja IPSec:lla on kaksi, kuljetus- ja tunnelointitila. (Scott, Wolfe & Erwin 1999, 32.)

2.4.1 IPSec-kuljetustila

Kuljetustilassa IP-pakettiin tehdään seuraava muutos: IP-otsikkotiedon ja ylemmän kerroksen protokollan otsikkotiedon väliin tulee IPSec-otsikko. IP-otsikkoon ei tehdä muita muutoksia, kuin IP-protokollakentän arvon muuttaminen vastaamaan käytettyä suojausprotokollaa, sekä IP-otsikon tarkistussumman uusiksi laskenta. Kuviossa 2 esitetään IP-pakettiin tehtävät muutokset IPSec kuljetustilassa. (Bollapragada, Khalid & Wainner 2005.)



KUVIO 2. IP-kehys IPSec-kuljetustilassa

IPSec olettaa IP-päätepisteiden olevan saavutettavissa. Kuljetustilassa IPSec-päätepiste ei muuta vastaanottajan IP-osoitetta IP-otsikossa. Kuljetustilaa voidaankin käyttää pakettien suojaamiseen vain, kun IP- ja IPSec-päätepisteet ovat samat. Pakettien osoitteenmuunnosta ei voida käyttää kuljetustilassa. Useimmille salauslaitteistoille tunnelointitila on tehokkaampi kuin kuljetustila, koska kuljetus-

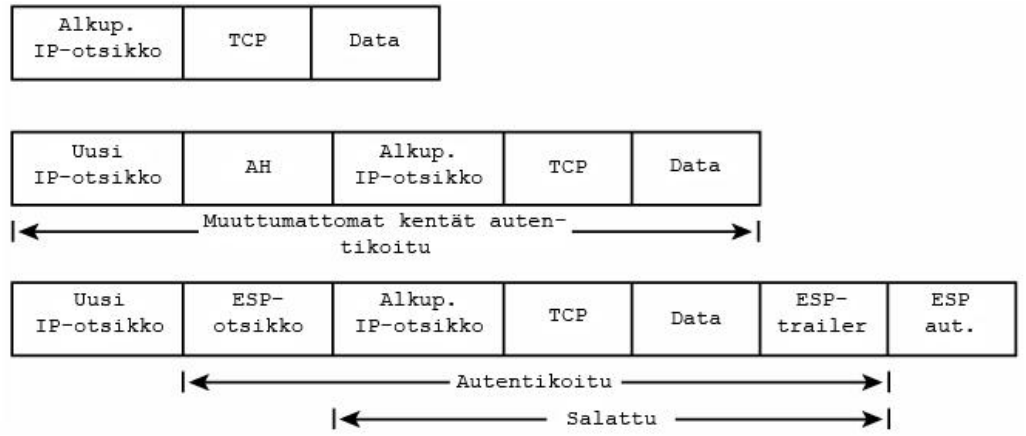
tilassa IP-otsikkoa täytyy siirtää tehden tilaa ESP- tai AH-otsikolle. (Bollapragada, Khalid & Wainner 2005.)

VPN:n kannalta kuljetustila on hyödyllisin, kun kahden päätelaitteen välinen liikenne täytyy suojata. Site-to-site-mallin suurin haaste kuljetustilan kannalta on IPsec:n suojauksen hallinnan vaikeus, kun kaikkien mahdollisten vertaispäätelaitteiden pitää pystyä avaamaan suojattu yhteys kaikkiin mahdollisiin päätelaitteisiin. Lisäksi molempien päätelaitteiden IP-osoitteiden täytyy olla reititettävissä koko IP-reitityspolulla. Vaikeuksien takia tyypillisessä VPN-ratkaisussa käytetään VPN-yhdyskäytäviä kahden sijainnin välillä. IPSec-tunnelin päätepisteet toimivat VPN-yhdyskäytävinä, joiden takana on useampia laitteita. IPSec:n kuljetustilan hyöty on rajattu, koska VPN-yhdyskäytävä suojaa joukkoa päätelaitteiden IP-osoitteita. IPSec:n kuljetustilaa voidaan silti hyödyntää VPN-yhteyden luomiseen käyttämällä Generic Route Encapsulation (GRE) -IP-tunnelia VPN-yhdyskäytävien välillä. IPSec suojaa GRE-tunnelin liikenteen kuljetustilassa. (Bollapragada, Khalid & Wainner 2005.)

2.4.2 IPSec-tunnelointitila

Kahden sijainnin välisen VPN-yhteyden luonti käyttäen IPSecin kuljetustilaa ja GRE-paketointia VPN-yhdyskäytävien välillä on hyvin suosittua. Joskus IP-solmulla, esim. etätyöntekijällä, ei ole GRE-tukea mutta IPSec VPN-yhteys olisi saatava. Tunnelointitila mahdollistaa IPSec VPN-yhteyden luomisen päätelaitteiden välille ilman GRE:n käyttöä. Myös kahden lähiverkon eli LAN:ien yhdistäminen toisiinsa on mahdollista. (Bollapragada, Khalid & Wainner 2005.)

Tunnelointitilassa alkuperäinen IP-kehys paketoidaan toiseen IP-kehykseen ja kehysten väliin lisätään kuvion 3 mukaisesti IPSecin otsikko, joko AH tai ESP tai molemmat. Paketoinnin ansiosta tunnelointitilaa voidaan käyttää kahden sijainnin välisen yhteyden turvaamiseen yhdyskäytävien takana olevien IP-solmujen kustannuksella. Tunnelointitilaa voidaan käyttää myös päätelaitteen ja IPSec-yhdyskäytävän yhdistämiseen. (Bollapragada, Khalid & Wainner 2005.)



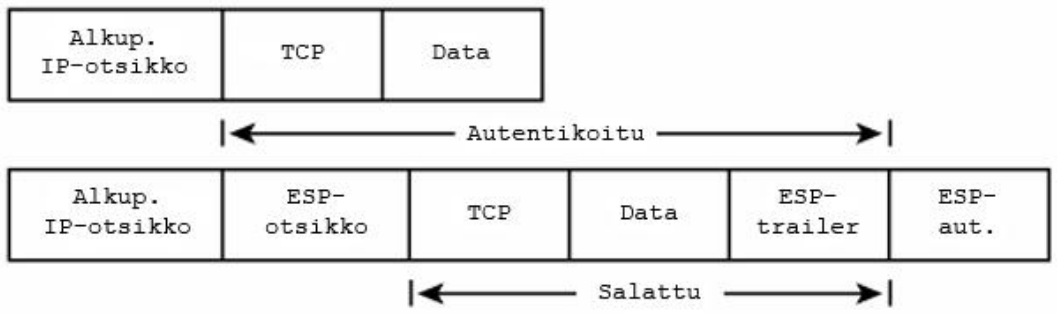
KUVIO 3. IP-kehys IPSec-tunnelointitilassa

2.4.3 Encapsulating Security Payload (ESP)

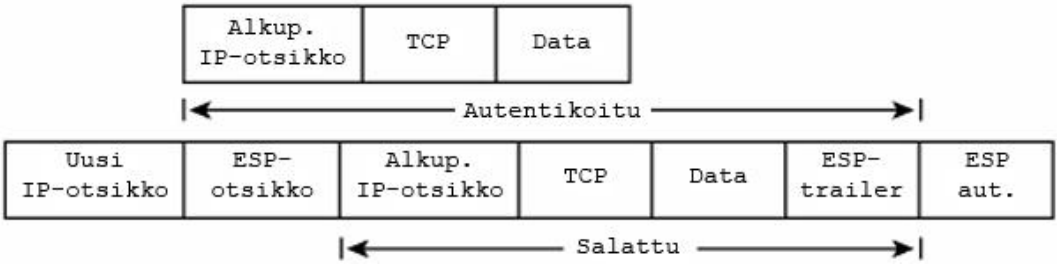
Encapsulating Security Payload salaa alkuperäisen IP-paketin hyötykuorman ja lisää alkuperäisen hyötykuorman ESP-otsikon ja -trailerin väliin kuvion 4 mukaisesti. Datan salaus, tiedon eheys, lähtöpisteen autentikointi sekä toistohyökkäyksen vastainen palvelu ovat kaikki ESP:n tuottamia palveluja. (Scott, Wolfe & Erwin 1999, 34.)

KUVIO 4. ESP:n suojaama IP-paketti

ESP saa arvon 50 IP-paketin otsikkotiedossa. ESP-otsikon paikka on IP-paketin ja ylemmän kerroksen protokollan otsikon välissä. IP-otsikko voi olla joko alkuperäinen otsikko IPSec:n kuljetustilassa tai uusi otsikko tunnelointitilassa. Kuvioissa 5 ja 6 on esitetty ESP:n suojaamat IP-paketit kuljetus- ja tunnelointitiloissa. (Bollapragada, Khalid & Wainner 2005.)

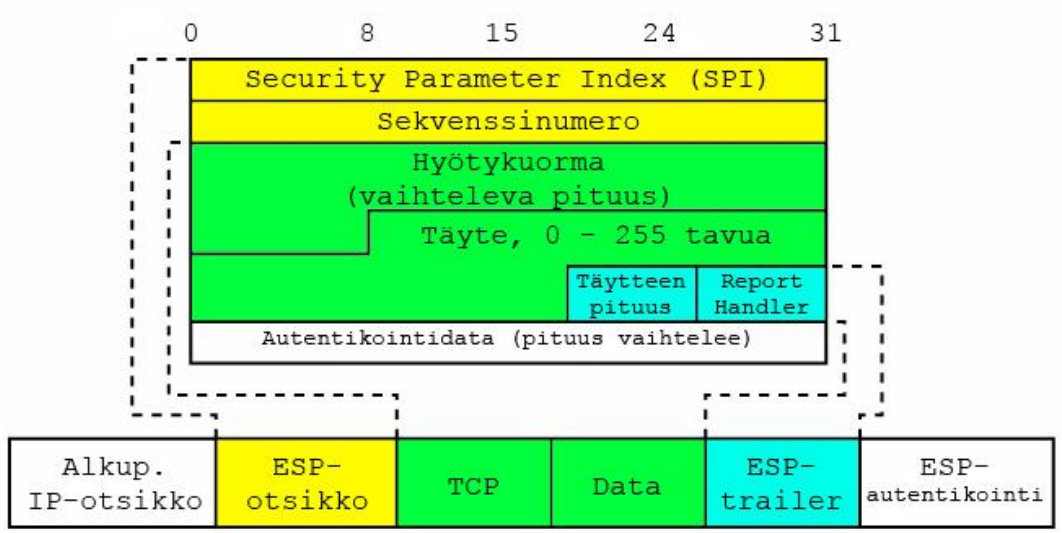


KUVIO 5. ESP:n suojaama IP-paketti IPSec:n kuljetustilassa



KUVIO 6. ESP:n suojaama IP-paketti IPSec:n tunnelointitilassa

ESP:n rakenne on avattu kuviossa 7. Security Parameter Index (SPI) aloittaa ESP-otsikon. SPI saa 32-bittisen arvon, joka yhdistettynä kohdeosoitteen ja edeltävän IP-otsikon protokollan kanssa tunnistaa paketin prosessointiin käytetyn security associationin (SA). SPI on kohdelaitteen valitsema satunnaisluku. Vastaanottaja valitsee SPI:n Internet Key Exchange -neuvottelun (IKE) aikana IPSec-tunnelia muodostaessa. SPI toimii indeksinä, jonka avulla SA eli salausasetukset voidaan etsiä SA-tietokannasta. (Bollapragada, Khalid & Wainner 2005.)



KUVIO 7. ESP:n rakenne IP-paketin ympärillä

Sekvenssinumero on yksilöllinen monotonisesti kasvava numero, jonka lähettäjä lisää otsikkotietoon. Yhdessä liukuvan vastaanottoajan (sliding receive window) kanssa sekvenssinumerot toteuttavat ESP:n toistohyökkäyksiltä suojaavan palvelun. ESP:n ja AH:n toimintatapa toistolta suojautumiseen on samanlainen. (Bollapragada, Khalid & Wainner 2005.)

ESP:n salaama data on hyötykuormakentässä. Käytetty salausalgoritmi voi vaatia aloitusvektorin eli IV:n (initialization vector) käytön, jolloin myös IV kulkee hyötykuormana datan alussa. IV:tä ei salata, vaan ainoastaan autentikoidaan. (Bollapragada, Khalid & Wainner 2005.)

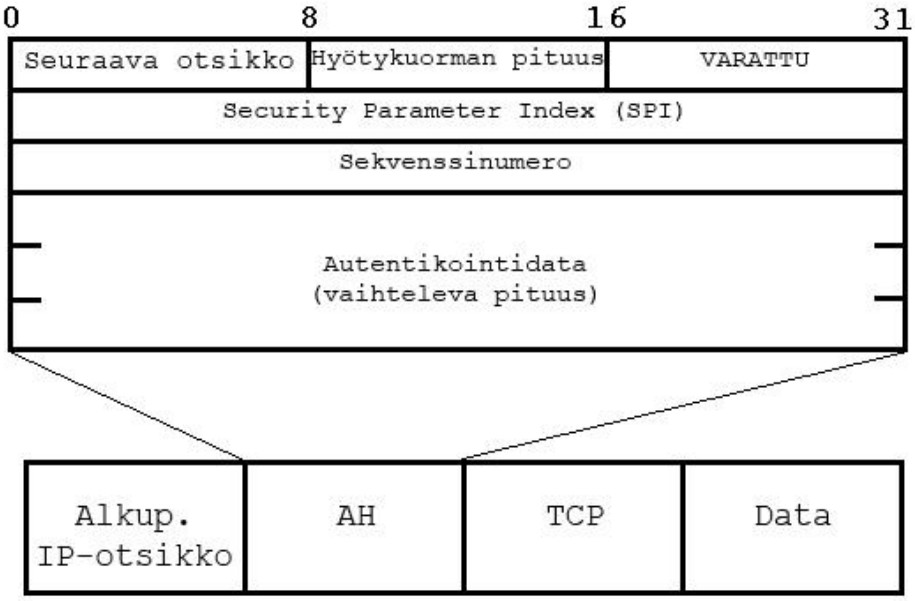
Täytekenttä sisältää ESP-otsikkoon lisättyjä bittejä, joita on eri määrä riippuen käytetystä salausalgoritmista. Täytekentän pituus kertoo kuinka monta bittiä täytekenttä sisältää ja mahdollistaa näin alkuperäisen datan palautuksen dekryptausvaiheessa. (Bollapragada, Khalid & Wainner 2005.)

Trailer-kenttä määrittelee minkä tyyppistä dataa kehyksellä on kuormana. Autentikointitiivistettä käytetään todentamaan datan eheys. Eheys tarkistetaan aina pake-

tin saapuessa vastaanottajalle ja ennen dekryptausta, koska autentikointi lisätään kehykseen aina salauksen jälkeen. (Bollapragada, Khalid & Wainner 2005.)

2.4.4 Authentication Header (AH)

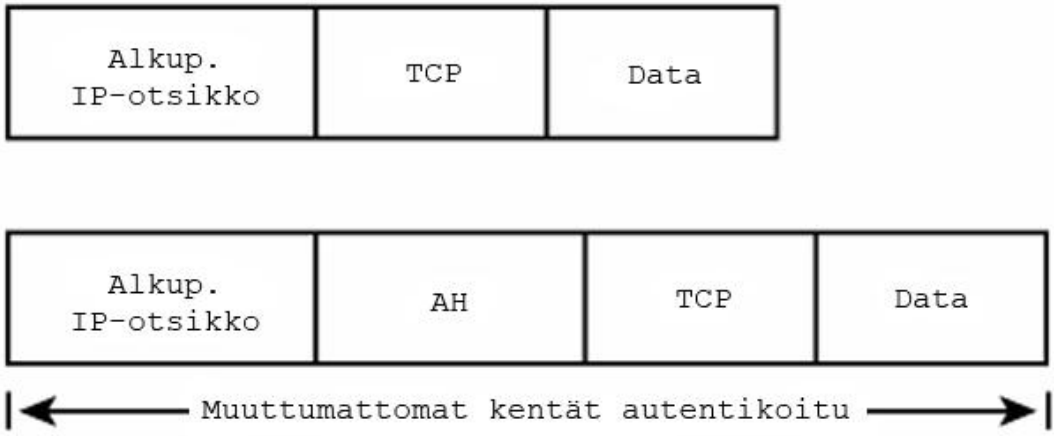
AH:n tehtäviin kuuluvat yhteydettömän datan eheyden, datan autentikoinnin ja vaihtoehtoinen toiston suojan toteuttaminen. Toisin kuin ESP, AH ei tarjoa datan salausta. Salauksen puutteen vuoksi AH:n otsikon rakenne on paljon yksinkertaisempi kuin ESP:n, kuten kuviosta 8 käy ilmi. (Scott, Wolfe & Erwin 1999, 34 - 35.)



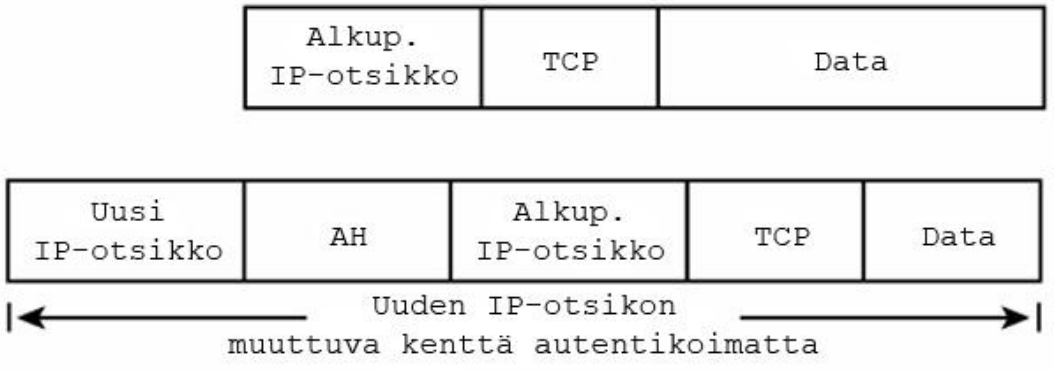
KUVIO 8. Authentication Headerin rakenne.

AH saa IP-paketin otsikossa arvon 51. Next Header -kenttä eli seuraava otsikko kertoo, mitä AH-otsikon jälkeen on kehyksessä. Kuljetustilassa Next Header saa suojattavan ylemmän tason protokollan arvon, esimerkiksi TCP tai UDP. Tunnelointitilassa Next Headerin arvo on 4. Muut kentät toimivat kuten edellä ESP:n yhteydessä. Kuvioissa 9 ja 10 on esitetty AH:n sijoittuminen kehyksessä IPSec:n kuljetus- ja tunnelointitiloissa. (Bollapragada, Khalid & Wainner 2005.)

AH:n rakenteessa (kuvio 8) Payload Lenght -kenttä kertoo otsikon pituuden. Reserved-kenttä ei nykyisellään ole käytössä, joten se asetetaan nolliksi. SPI:llä ja sekvenssinumerolla on sama merkitys kuin ESP:ssa. Autentikointitiivisteellä on ESP:aan verrattuna yksi huomattava ero. AH todentaa hyötykuorman lisäksi myös IP-otsikon. Koska AH luo todennustiedon koko paketista osa IP-kentistä muuttuu siirrettäessä. Kaikki mahdollisesti muuttuvat kentät nollataan, koska niiden muuttuessa myös todennustiiviste muuttuu ja vastaanottaja hylkää paketin. Muuttuviin kenttiin kuuluvat type of service (ToS), liput (flags), fragment offset, time-to-live (TTL) and otsikon tarkistussumma. (Bollapragada, Khalid & Wainner 2005.)



KUVIO 9. AH:n sijoittuminen kuljetustilassa



KUVIO 10. AH:n sijoittuminen tunnelointitilassa

Kuljetustilassa AH:n käyttö on hyödyllistä, mikäli liikennöivät laitteet ovat myös IPSec-yhteyden päätepisteet. Kuljetustila ei toimi NAT:n kanssa, joten site-to-site-malliin kuljetustilaa ei suositella. Kuljetustilan liikenteen salaus on myös tehotto-

mampaa kuin tunnelointitilan, koska kuljetustila vaatii IP-otsikon siirron (kuvio 10). Tunnelointitilassa AH kapsuloi IP-paketin ja ylimääräinen IP-otsikko lisätään ennen AH-otsikkoa. Tunnelointitilassa AH:n käyttämistä IPSec VPN-yhteyden päästä päähän suojaamiseen ei ole mielekästä, koska dataa ei salata. (Bollapragada, Khalid & Wainner 2005.)

2.5 Secure Socket Layer (SSL)

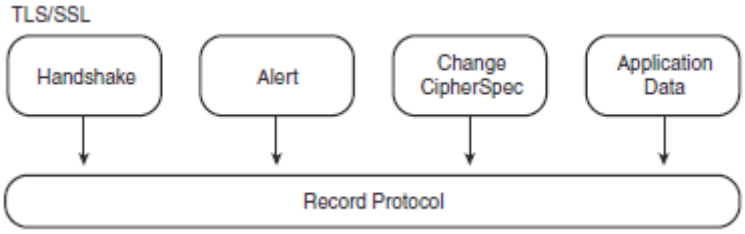
Secure Socket Layer (SSL) on Netscape Communicationsin kehittämä protokolla, joka sijoittuu OSI-mallin kuljetus- ja sovelluskerrosten väliin. Vaikka protokolla luotiin alkujaan suojaamaan web-yhteyksiä, on SSL:n käyttö VPN-tarkoituksiin yleistynyt viime vuosina. SSL-yhteys luodaan joko suoraan selaimesta tai SSL-ohjelmiston avulla. Vuonna 1996 Internet Engineering Task Force (IETF) perusti Transport Layer Security (TLS) -työryhmän, jonka tarkoitus oli standardoida eri valmistajien, pääasiassa Netscapen ja Microsoftin, SSL-protokollat. Työryhmän tuloksena syntyi TLS-protokolla, joka muistuttaa paljon SSL:n kolmatta versiota (SSL v3) muutamin poikkeuksin ja lisäyksin. (Frahim & Huang 2008, 30.)

SSL:n vahvuuksiin kuuluu tekniikan valmius. Protokollaa voidaan käyttää lähes missä tahansa web-selaimessa, eikä esimerkiksi käyttöjärjestelmällä ole merkitystä. Yhteyden mahdollisissa ongelmatilanteissa ei myöskään tarvitse etsiä vikaa kolmannen osapuolen VPN-asiakasohjelmistosta. (Lewis 2006.)

SSL vaatii luotettavan datan toimituksen ja toimii siksi vain TCP:n päällä. Vaikka ideaalitilanteessa SSL:n pitäisi toimia minkä tahansa staattisen asiakas-palvelin-mallin TCP-ohjelman kanssa, niin todellisuudessa ei pelkkä TCP-socket-pyyntöjen vaihto SSL-pyynnöiksi riitä. Yleisimmille TCP/IP-sovellutuksille, kuten Hypertext Transfer Protocol (HTTP) ja Simple Mail Transport Protocol (SMTP), on määritelty protokollat SSL:n käyttöön. (Frahim & Huang 2008, 31.)

2.5.1 SSL:n rakenne

SSL on kerroksista muodostuva protokolla, jonka rakenne on esitetty kuviossa 11. Alimmalla kerroksella on record-protokolla, joka on pääasiassa kapsulointia varten. Record kuljettaa useita ylemmän kerroksen protokollia sekä sovellusdataa ja ottaa vastaan ylemmän kerroksen protokollien viestejä. Record hoitaa muun muassa datan pilkkomisen ja kasaamisen, pakkauksen ja purkamisen, tiivisteen lisäyksen ja tarkistuksen sekä salauksen ja salauksen purun. (Frahim & Huang 2008, 33.)



KUVIO 11. SSL/TLS-protokollan rakenne (Frahim & Huang 2008)

SSL:n Record muodostuu neljästä ylemmän tason asiakasprotokollasta. Handshake eli kättely neuvottelee SSL-istunnon suojausmääritteet. Alerts välittää huomautusviestejä SSL-yhteyden päiden välillä, esimerkiksi ilmoitus dekryptauksen epäonnistumisesta tai istunnon päättymisestä. Change Cipher Spec -protokollaa käytetään ilmoittamaan salakoodausmuutoksista. Application Data -protokolla hoitaa ohjelman datan välittämisen. Huomioimisen arvoista on, että TLS:n record-protokolla suunniteltiin frameworkina ja uusia ylemmän tason asiakasprotokollia voidaan lisätä tulevaisuudessa. (Frahim & Huang 2008, 33 - 34.)

SSL-yhteyden muodostus alkaa kättelyprotokollilla, joiden tehtävinä on määrittää käytettävän SSL-protokollan versio ja salausominaisuudet, tunnistautuminen, avainten vaihto sekä yhteisen salaisuuden laskenta. Yhteyden muodostuksen aloittaa asiakas lähettämällä ClientHello-viestin palvelimelle. ClientHello sisältää asiakkaan tukeman suurimman protokollaversion, esimerkiksi SSL v3:n versio on 3.0 ja TLS on 3.1. Lisäksi viestiin kuuluu Client random -tietue, joka sisältää päivämäärän ja kellonajan sekä 28-tavuisen pseudosatunnaisen luvun. Client random

-tietuetta käytetään yhteisen salaisuuden laskuun ja estämään uudelleenlähetys-hyökkäyksiä. ClientHello-viestissä istuntokentän arvoa käytetään, mikäli asiakas ei halua luoda uutta SSL-yhteyttä, vaan jatkaa vanhaa istuntoa. Asiakas kertoo ClientHello-viestillä myös kaikki tukemansa SSL-yhteyden aikana tarvittavat kryptografiset algoritmit sekä tuetut pakkaustavat. (Lewis 2006.)

Palvelin vastaa ClientHello-viestiin ServerHello-viestillä, jonka rakenne on samanlainen kuin ClientHellolla. Vastausviestissä on korkein molempien tuettu protokollaversio, jota käytetään koko yhteyden ajan. Palvelin myös luo oman satunnaisluvun, josta myöhemmin luodaan salaisuus. Kättelyvaiheen jälkeen palvelin ja asiakas ovat muodostaneet loogisen yhteyden ja neuvotelleet yhteyden suojausominaisuudet. (Lewis 2006.)

Hello-viestien vaihdon jälkeen palvelin ja asiakas käyttävät sovittuja suojausominaisuuksia siirtyen tunnistukseen ja avainten vaihtoon. SSL v3 ja TLS tukevat useita autentikointi- ja avaimenvaihtomenetelmiä. Yleisin menetelmä on RSA:n käyttö. Myös Diffie-Hellmanin käyttö on mahdollista. Tunnistuksen ja avainten vaihdon aikana palvelin ja asiakas laskevat jaetun salaisuuden, jota käytetään seuraavaksi pääsalaisuuden luontiin. (Lewis 2006.)

Asiakas ja palvelin luovat pääsalaisuuden suojatusti vaihdettujen tietojen perusteella. Pääsalaisuutta ei ikinä lähetetä, vaan molemmat osapuolet luovat pääsalaisuuden itsenäisesti. Pääsalaisuudesta johdetaan useita avaimia viestien salausta ja eheyden todentamista varten. Avainten johtamisten jälkeen palvelin ja asiakas ovat valmiit päättämään kättelyn ja lähettämään ohjelmadataa käyttäen muodostettua turvallista yhteyttä. (Frahim & Huang 2008, 36 - 37.)

2.5.2 SSL VPN

SSL toteuttaa turvallisia yhteyksiä sovelluksille ja on näkymätön ylemmän tason sovelluksille. Onnistunein SSL-sovellus on HTTPS internetin valtavan suosion takia. Kaikki kaupalliset web-selaimet, jotka ovat oletuksena saatavilla kaikille

käyttöjärjestelmille, tukevat HTTPS:a. VPN-käytössä mahdollisuus muodostaa yhteys periaatteessa mistä tahansa suo huomattavia etuja. Ensinnäkin yhteys on suojattu ja yhteyden muodostus onnistuu mistä tahansa miltä tahansa PC:ltä asentamatta VPN-ohjelmistoa. Ohjelmiston asennuksen tarpeettomuus taas pienentää esimerkiksi yrityksen IT-osaston asiakaspään ylläpitokulut lähes nollaan. Lisäksi SSL VPN käyttää samaa TCP-porttia 443 kuin HTTPS. Palomuurit, välityspalvelimet ja NAT-laitteet päästävät pääasiallisesti liikenteen TCP/443-portista läpi. Käytetyn portin ansiosta SSL VPN -liikenne ei vaadi mitään erityisiä konfiguraatioita verkon ja verkkolaitteiden osalta. (Frahim & Huang 2008, 49 - 50.)

SSL VPN mahdollistaa VPN-käyttäjien pääsyn esimerkiksi yrityksen sisäisiin web-sovelluksiin ja muihin palvelimiin, jotka eivät välttämättä edes tue HTTP:aa. Pääsy on mahdollista käyttämällä useampaa tekniikkaa, joita kutsutaan yhteisesti reverse proxy -teknologiaksi eli käänteiseksi välityspalvelimeksi. Reverse proxy -palvelin on välityspalvelin, joka sijaitsee sovelluspalvelinten edessä. Reverse proxy -palvelin näyttää VPN-asiakkaille aidolta web-palvelimelta. Pyynnön saatuaan reverse proxy -palvelin välittää pyynnön sisäiselle web-palvelimelle käyttäjän puolesta ja välittää pyydetyn sisällön käyttäjälle. (Frahim & Huang 2008, 50.)

SSL VPN:n reverse proxy -tekniikka ei vaadi erillisten VPN-sovellusten asentamista. Monet web-palvelimet tukevat reverse proxy -tekniikkaa, mutta SSL VPN tarjoaa paljon enemmän toiminnallisuutta kuin tavalliset reverse proxy -teknologiat. SSL VPN:n tuki monimutkaisille web-sovelluksille ja muille sovelluksille on parempi kuin yksinkertaisilla reverse proxy -palvelimilla. SSL VPN tukee suurta määrää sovelluksia, ja mikäli sovelluksen sisältöä ei voida muuntaa web-muotoon, saa SSL VPN jollain muulla tapaa sovelluksen sisällöstä kiinni. SSL VPN:lla saadaan myös verkkotason yhteys etäjärjestelmän liittämiseksi verkkoon. Tavalliseen reverse proxy -tekniikkaan verrattuna SSL VPN toteuttaa myös suojatun VPN-yhteyden kaikkine etuineen. (Frahim & Huang 2008, 50 - 51.)

SSL VPN -yhdyskäytävä tekee käyttäjän URL-pyynnöille URL-muunnoksen. URL:n muunnokselle ei ole olemassa standardia ja muunnetut osoitteet voivat olla

hyvinkin erinäköisiä laitevalmistajasta tai ohjelmistokehittäjästä riippuen. Käyttäjän syöttämä URL-pyyntö muuntuu JavaScriptillä, joka on ladattu SSL VPN -yhdyskäytävältä sisäänkirjautuessa. Yhdyskäytävä jäsentelee muunnetusta URL:sta todellisen osoitteen ja välittää käyttäjän pyynnön eteenpäin. Esimerkiksi käyttäjän SSL VPN -yhdyskäytävälle lähettämä pyyntö http://mail.esimerkki.fi voisi muuntua muotoon https://10.0.0.1/http/0/mail.esimerkki.fi. Mikäli sisäverkon web-infrastruktuuria ei haluta paljastaa edellisen esimerkin tavalla vaikkapa tietoturvasyistä, voidaan käyttää URL:n salausta, jolle ei vielä ole omaa standardia. (Frahim & Huang 2008, 52 - 53.)

URL-muunnosten lisäksi sisällön uudelleenkirjoitus on tärkeä osa asiakasohjelmattoman SSL VPN:n tekniikka. Päätarkoitus uudelleenkirjoitukselle on ohjata käyttäjän pyynnöt osoittamaan SSL VPN -yhdyskäytävään muuttamalla URL-viittaukset ja Java socket -kutsut. Haasteelliseksi muunnokset tekee HTML-standardin löyhyys ja web-sovellukset. Muunnettavia URL-viittauksia löytyy mm. HTML-, JavaScript-, Java Applet-, ActiveX-, Flash- ja XML-sisällöstä. (Frahim & Huang 2008, 53.)

Sisällön uudelleenkirjoituksen voi tehdä joko SSL VPN -yhdyskäytävä tai asiakaspään selain. Asiakaspään muunnoksessa on etuina dynaamisen web-sisällön luomisen helpottuminen sekä palvelimen laskentatehon säästäminen. Yhdyskäytävä voi merkitä osan web-sisällöstä ja lähettää merkityn sisällön muuntamattomana käyttäjälle JavaScript-tiedoston kera. Käyttäjän selain ajaa tiedoston tehden loput muutokset ennen sisällön esittämistä käyttäjälle. (Frahim & Huang 2008, 53.)

Koska sisällön uudelleenkirjoitus on ajoittain hyvin monimutkaista ja lähes mahdotonta toteuttaa tukien kaikkia web-sovelluksia, ovat jotkut SSL VPN -toimittajat sisällyttäneet välityspalvelimen ohitusominaisuuden vikaturvallisena ominaisuutena laitteistoonsa tai ohjelmistoonsa. Välipalvelimen ohitus sivuuttaa tavallisen sisällön uudelleenkirjoituksen ja muuttaa vain yksinkertaisen web-sisällön. Monissa tapauksissa ratkaisu toimii paremmin kuin monimutkainen uudelleenkirjoituslogiikka tuntemattoman sovelluksen kanssa. (Frahim & Huang 2008, 54.)

Tavallisen uudelleenkirjoitettavan liikenteen ja välityspalvelimen ohittavan liikenteen erottamiseen on kaksi tapaa. Ensimmäinen tapa on käyttää epästandardia isoa porttinumeroa ohitettavalle liikenteelle. SSL VPN -yhdyskäytävän saadessa pyynnön määriteltyyn porttiin välittää yhdyskäytävä pyynnön sisäverkon palvelimelle ja ohittaa uudelleenkirjoituksen palvelimen sisällölle. Portin käyttö voi vaatia portin avaamisen palomuuriin eikä tue asiakaspään JavaScript-muunnosta. Toinen tapa ohitettavan liikenteen erottamiseen on käyttää yhdyskäytävälle vaihtoehtoista isäntänimeä. Vaihtoehtoinen isäntänimi ei tarvitse ylimääräisiä portteja mutta DNS-palvelimen asetuksiin pitää tehdä tarvittavat muutokset ja isäntänimiin viittaavat varmenteet on lisättävä. (Frahim & Huang 2008, 54.)

Odottamattomien tilanteiden varalta on hyvä olla mahdollisuus räätälöidä uudelleenkirjoitusta. Nykyään SSL VPN -toimittajilla on eri tekniikoita uudelleenkirjoituksen räätälöintiin. Käyttäjän rajapinnan esi- ja jälkikäsittely lisäävät mukautettuja sisällönmuokkaustoimintoja uudelleenkirjoitusta ennen ja uudelleenkirjoituksen jälkeen. Esikäsittelyllä voidaan esimerkiksi siistiä HTML-sisältöä uudelleenkirjoituksen helpottamiseksi etsimällä ja korvaamalla tiettyjä malleja. Esi- ja jälkikäsittely helpottavat myös ongelmatilanteiden ratkontaa. Yleisimmille web-sovelluksille, kuten Citrix, Outlook Web Access ja iNotes, voidaan myös hienosäätää uudelleenkirjoitusasetuksia varmistaen, että sovellukset käsitellään sulavasti. (Frahim & Huang 2008, 54 - 55.)

Oletuksena SSL VPN -yhdyskäytävä yleensä kirjoittaa uudelleen kaiken palvelimen sisällön. Osa SSL VPN -toimittajista tarjoavat mahdollisuuden valikoida uudelleenkirjoitettavan sisällön, puhutaan ”split tunneling”:sta eli jaetusta tunneloinnista. Ylläpitäjät voivat käyttää toimintoa määrittämällä listan domain-nimistä, jotka eivät tarvitse uudelleenkirjoitusta. Käyttäjän selain ottaa yhteyden suoraan palvelimeen lähettämättä pyyntöä ensin SSL VPN -yhdyskäytävälle. Esimerkiksi kaikki muu internetliikenne, paitsi sisäverkkoon kohdistuva, voidaan ohjata suoraan sivustoille, jolloin reverse proxylla ei ole täyttä hallintaa asiakkaan liikenteestä. (Frahim & Huang 2008, 55.)

Ohjelmistoton SSL VPN -etäyhteys tukee vain osaa yritysten käyttämistä ohjelmistoista. Käytetyissä ohjelmissa on yleensä valmiiksi web-käyttöliittymä, tai niiden sisältö on helposti esitettävissä web-sisältönä. Portin edelleenvälitys eli port forwarding lisää SSL VPN -ratkaisun tukemaan muitakin ohjelmia kuin valmiin web-käyttöliittymän omaavia. Portin edelleenvälityksestä vastaa asiakaspään ohjelma, joka sieppaa tiettyjen ohjelmien liikenteen ja lähettää liikenteen SSL VPN -yhdyskäytävälle muodostetun SSL-yhteyden yli. (Frahim & Huang 2008, 55.)

Portin edelleenvälitysohjelma on ns. thin client, eli hyvin pieni ohjelma tai sovelma. Eri kehittäjät käyttävät edelleenvälitykseen tekniikoina mm. Java Appletteja, ActiveX:ää, Windows Layered Service Provideria (LSP) tai Windows Transport Data Interfacea (TDI). Yleisin tekniikka on Java Applet, koska se on riippumaton käyttäjän käyttöjärjestelmästä ja toimiakseen vaatii vain Java-tuen. (Frahim & Huang 2008, 55.)

Java Applet -pohjaiset portin edelleenvälitysohjelmat tukevat yleensä vain yksinkertaisia client-server-pohjaisia, yksikanavaisia TCP-sovelluksia, kuten Telnetiä, SMTP:a, POP3:a ja Windows Remote Desktop-palvelua. Useampaa TCP-porttia tai dynaamisia TCP-portteja käyttäviä sovelluksia, esim. aktiivista FTP:a tai Microsoft Exchange Protocolia varten Java-sovelma ei ole hyvä ratkaisu. Jotkin Windows-pohjaiset port forwarding -ohjelmat tukevat myös dynaamisia TCP-portteja tai useampaa TCP-porttia käyttäviä sovelluksia mutta vaativat käyttäjältä Windows-käyttöjärjestelmän ja mahdollisesti ylläpitäjän käyttöoikeudet. (Frahim & Huang 2008, 55.)

Portin edelleenvälitystekniikoiden käyttöä varten on käyttäjällä oltava ohjelma asennettuna ja konfiguroituna osoittamaan paikalliseen loopback-osoitteeseen tai sisäisen palvelimen osoitteeseen. Ei voida olettaa, että käyttäjältä aina löytyy vastaava ohjelma. Joillekin yleisimmille, yksinkertaisille etähallintasovelluksille, kuten Windows terminal servicelle, Citrix terminal servicelle, VNC:lle, Telnetille ja SSH:lle on osalla valmistajista helpotettu ratkaisu, joka lataa etähallintasovelluksen käyttäjän koneelle. Asennus tapahtuu yhdyskäytävälle sisäänkirjautumisen

jälkeen yleensä ActiveX:n tai Java-sovelman kautta ja sisältää valmiiksi konfiguroidun ohjelman. (Frahim & Huang 2008, 56.)

Ohjelmistoton tai portin edelleenvälittävä yhteys ei riitä tehokäyttäjille tai etätyöntekijöille, jotka käyttävät VPN-yhteyksiä yritysten työasemilla ja tarvitsevat täyden pääsyn yrityksen sisäverkon resursseihin. IPSec VPN soveltuu paremmin täyden verkkotason yhteydeksi VPN-käyttöön. Mikäli IPSec VPN -ratkaisu on jo käytössä, voidaan sitä laajentaa ohjelmatason yhteyksiin asiakasohjelmattomalla SSL VPN -ratkaisulla. Nykyään useimmat SSL VPN -ratkaisut sisältävät myös tunneliohjelman. (Frahim & Huang 2008, 58.)

SSL VPN tunneliohjelmat eivät ole standardoitu kuten IPSec VPN:ssa. Eri valmistajat käyttävät eri tekniikoita tunnelia varten. Yhteistä tekniikoille on kuitenkin yleensä lennosta asentaminen, työaseman ylläpito-oikeuksien vaatiminen käyttäjältä, virtuaalisen verkkosovittimen asentaminen sekä toiminta käyttäjän eikä kernelin tilassa. Lennosta jakelu ja asentaminen säästävät ylläpitokuluissa sekä työtunneissa verrattuna IPSec VPN-ratkaisuun. (Frahim & Huang 2008, 58 - 59.)

2.6 Yhteenveto VPN:sta

VPN on yksityinen dataverkko, joka hyödyntää julkista tietoliikenneinfrastruktuuria. VPN:n avulla voidaan yhdistää kahden toimipisteen lähiverkot toisiinsa tai mahdollistaa yksittäisten työasemien pääsy yrityksen verkkoon etänä. Luotettavaa yhteyttä varten käytetään kryptografisia menetelmiä, joilla salataan VPN-päätelaitteiden välinen liikenne.

IPSec on OSI-mallin verkkokerroksella toimiva protokollajoukko, jota voidaan käyttää VPN-yhteyden luomiseen. IPSecillä on kaksi toimintatilaa, kuljetus- ja tunnelointitila, joista tunnelointi sopii paremmin yksittäisten käyttäjien VPN-yhteyden luontiin. ESP-protokolla hoitaa IPSecin tiedon salauksen. ESP ja AH -protokollat takaavat datan eheyden, autentikoinnin sekä suojan toistohyökkäyksiltä.

VPN-käyttöön soveltuu myös SSL, joka toimii osoitteenmuunnosten ja palomuurien kanssa. SSL VPN ei yleensä vaadi asiakaspäässä erillisten ohjelmistojen asentamista, mikä vähentää IT-osaston työmäärää sekä kuluja. SSL VPN mahdollistaa etäpääsyn web-sovelluksiin ja eri tekniikoidensa ansiosta myös muihin sovelluksiin, joten se soveltuu hyvin tilanteisiin, joissa ei tarvita täyttä verkkoyhteyttä etäympäristöön.

3 VPN-JÄRJESTELMÄT

3.1 OpenVPN Access Server

OpenVPN Access Server (AS) on avoimeen lähdekoodiin perustuvan OpenVPN:n päälle rakennettu SSL VPN -ohjelmisto. AS muodostuu asennus- ja konfigurointityökaluista, jotka mahdollistavat yksinkertaisen ja nopean VPN-ratkaisun käyttöönoton. Asennuksen helppous juontuu asetusten valintojen vähäisestä määrästä. AS:n konfigurointia helpottaa web-käyttöliittymä, joka tekee Access Serverin asetusten määrittämisestä ja ylläpidosta yksinkertaista. (OpenVPN Technologies 2010c.)

AS:n nopeaa käyttöönottoa edesauttaa myös mahdollisuus autentikoida käyttäjät monella eri tapaa. Jokaista käyttäjätunnusta ei tarvitse luoda ja hallinnoida erikseen, vaan tunnistukseen voidaan käyttää Pluggable Authentications Modulea (PAM) eli yleistä Unixin käyttäjäntunnistusjärjestelmää, ulkoista Lightweight Directory Access Protocol (LDAP) tai Active Directory -palvelinta, tai yhtä tai useampaa ulkoista Remote Authentication Dial In User Service (RADIUS) -palvelinta. (OpenVPN Technologies 2010c.)

Käyttäjä liittyy VPN-palvelimeen web-selaimen kautta tunnistautumalla. Tunnistautumisen jälkeen Windows-käyttäjä voi ladata dynaamisesti luodun, esikonfiguroidun asiakasohjelman. Ohjelma sisältää käyttäjäkohtaiset asetukset eikä vaadi käyttäjältä ohjelman konfigurointia. Muita käyttöjärjestelmiä varten AS luo asetustiedoston, jota voidaan käyttää OpenVPN:n muiden käyttöjärjestelmien asiakasohjelmissa. (OpenVPN Technologies 2010c.)

Access Server asentuu toistaiseksi vain Linux-käyttöjärjestelmän päälle. Asennusta varten löytyy sekä 32- että 64-bittisille käyttöjärjestelmille RPM- ja Deb-paketit. Testattuihin käyttöjärjestelmiin kuuluvat CentOS 4 ja 5, Fedora 9 ja 10, Red Hat Enterprise Linux 4 ja 5, Ubuntu 8, 9 ja 10 sekä Debian 4 ja 5. (OpenVPN Technologies 2010a.)

AS käyttää asiakasohjelmana OpenVPN Connect Client -ohjelmaa, joka on samalla myös Access Serverin tunnistuspalvelu. Connect Client on ainoa tapa, jolla OpenVPN asiakasasennukset levitetään käyttäjille. Connect Client luo ja jakelee käyttäjien asetustiedostot sekä asiakasohjelman asennustiedostot tunnistautuneille käyttäjille. Asetus- ja asennustiedostot ovat käyttäjäkohtaisia. Käyttäjät eivät voi käyttää toistensa asetustiedostoja VPN-yhteyden luomiseen. Yhdellä työasemalla voi olla useampi yhteysprofiili, mikäli useampi käyttäjä jakaa saman työaseman. Vaihtoehtoisesti voidaan myös käyttää palvelimelle lukittua profiilia, joka on kaikille käyttäjille yhteinen. (OpenVPN Technologies 2010c.)

Asiakasohjelma Connect Client on selaimeen integroitu, pienikokoinen sovellus. Vaihtoehtoisena asiakasohjelmana voidaan käyttää Desktop Client -ohjelmaa, joka on itsenäinen, selaimeen integroimaton ohjelma. (OpenVPN Technologies 2010c.)

Access Serveriin on sisäänrakennettu UCARP:ia käyttävä vikasietojärjestelmä. UCARP on Common Address Redundancy Protocol:n (CARP) siirrettävä, kernelin ulkopuolella ajettava versio (Denis, UCARP). Järjestelmää käyttämällä voidaan ajaa primäärisolmua ja sekundäärisolmua, jotka jakavat saman virtuaalisen IP-osoitteen. Mikäli primäärisolmu kaatuu, jatkaa sekundäärisolmu palvelimen toimintaa. Vikasietojärjestelmää varten tarvitaan kaksi ylimääräistä vapaata IP-osoitetta: yksi molemmille palvelimille ja virtuaalinen osoite järjestelmälle. (OpenVPN Technologies 2010c.)

OpenVPN Access Server toimii kahdessa eri VPN-tilassa. VPN-tunnelointitopologia voidaan valita OSI-mallin kerroksen mukaan. L2-tason tilassa AS siltaa Ethernet-liikennettä. L3-tilassa AS reitittää ja tekee IP-paketeille osoitteenmuunnoksen. L3-tila vaatii vähemmän toimenpiteitä toimiakseen mutta NAT voi haitata joidenkin ohjelmien toimintaa (OpenVPN Technologies 2011). Access Server voidaan konfiguroida myös toimimaan L3-tilassa ilman NAT:ia. (OpenVPN Technologies 2010c.)

Access Server tukee samanaikaisia käyttäjiä kymmenestä sataantuhanteen asti (OpenVPN Technologies 2010b). Yhtäaikaisia käyttäjälisenssejä voi ostaa vähimmillään kymmenen kerrallaan ja aktivoitujen lisenssien käyttäjämäärä summautuu, joten lisenssejä voi helposti ostaa tarpeen mukaan lisää. AS on erittäin hyvin skaalautuva erikokoisten yritysten käyttöön. (OpenVPN Technologies 2010c.)

3.2 Cisco ASA 5505 Adaptive Security Appliance

Cisco ASA 5505 Adaptive Security Appliance on verkkolaite, joka tuottaa IPSec ja SSL VPN -palvelujen lisäksi palomuuri- ja verkkopalveluja. Oletuksena ASA 5505 tukee kymmentä samanaikaista IPSec VPN-käyttäjää. Erikseen ostettavalla Security Plus -lisenssillä voidaan samanaikaisten IPSec VPN -käyttäjien määrä nostaa 25:een. (Cisco Systems 2010a.)

VPN-yhteyden muodostukseen ASA 5505 tarjoaa kaksi eri tapaa, ohjelmaton SSL-yhteys sekä IPSec tai SSL-yhteyttä käyttävä AnyConnect-niminen ohjelma. AnyConnectin jakelu voidaan toteuttaa ASA:n kautta kirjautumalla VPN-yhdyskäytävään ja lataamalla ohjelma tai käyttämällä yrityksen ohjelmien levitysjärjestelmää. Mikäli jakelu tapahtuu ASA:n kautta, on helppo pakottaa käytettävä ohjelmaversio. AnyConnectia on mahdollista muokata ulkoasun ja kielen osalta. (Cisco Systems 2011.)

AnyConnect on mahdollista ajaa kahdessa eri tilassa. Standalone-tilassa AnyConnectia voidaan ajaa tavallisen ohjelman tavoin ja yhteyden muodostuksen jälkeen ASA tarkistaa ohjelman version. Mikäli versio on vanhentunut, tarjoaa ASA uutta versiota käyttäjälle. WebLaunch-tilassa ohjelma voidaan käynnistää selaimesta kirjautumalla ASA:een. (Cisco Systems 2011.)

ASA 5505 on laajennettavissa lisämoduuleilla, jotka lisäävät laitteen ominaisuuksia. Erilaisilla erikseen ostettavilla lisensseillä voidaan esimerkiksi käyttää ohjelmatonta SSL-yhteyttä VPN:iin tai lisätä tietoturvaa, mikäli järjestelmä kytketään

toimimaan Cisco IronPort Web Security Appliancen (WSA) kanssa. On myös mahdollista pakottaa käyttöön käyttäjän virusturva- ja palomuuriohjelmistot ja niiden päivitykset. ASA voi olla yhdistämättä käyttäjää, mikäli tämän käyttämät tietoturvaohjelmistot eivät ole ajan tasalla. (Cisco Systems 2011.)

Cisco 5500 Adaptive Security Appliance -sarjan laitteiden ominaisuuksiin kuuluvat VPN-toiminnallisuuden lisäksi palomuuri ja tunkeutumisen estojärjestelmä (IPS, intrusion prevention system). IPS-järjestelmä suojaa mm. sovellus- ja käyttöjärjestelmätason hyökkäyksiä, rootkittejä, spywarea ja muita haittaohjelmia vastaan ja suojaa peer-to-peer-tiedostonjako- sekä pikaviestintäliikenteen. Laite toimii sekä IPv6- että IPv4-verkoissa. (Cisco Systems 2010b.)

Taulukossa 1 on vertailtu ASA 5500 -sarjan laitteiden suorituskykyjä sekä VNP-istuntojen maksimimääriä. 5505 on sarjan pienimpiin kohteisiin tarkoitettu palomuurilaite. 5505:n Security Plus -lisenssin hankkimalla voidaan IPSec VPN -istuntojen maksimimäärä nostaa 25:een. Taulukosta 1 käy hyvin ilmi VPN-puolen valtava harppaus kymmenkertaisiin istuntomääriin vaihtamalla ASA 5505 sarjan toiseksi pienimpään ASA 5510:een. Vaikka työn kannalta yksityisen ostajan hinnalla ei ole merkitystä oppilaitosalennuksien vuoksi, saadaan silti hintasuhde selville. ASA 5505 kymmenen käyttäjän lisenssillä maksaa hintaluokkaa $300 (PriceGrabber.com 2011c). ASA 5510 on halvimmillaan noin $1700 (PriceGrabber.com 2011e). ASA 5520 hinta on alimmillaan luokkaa $3000 (PriceGrabber.com 2011f).

TAULUKKO 1. Cisco ASA 5500 -sarjan laitteiden vertailu

Malli	ASA 5505	ASA 5510	ASA 5520
Palomuurin suorituskyky (Mbps)	150	300	450
3DES/AES VPN-suorituskyky (Mbps)	100	170	225
IPSec VPN-istuntoja, max.	10/25	250	750
SSL VPN-istuntoja, max.	25	250	750

Laitteiden lisäksi voidaan hankkia vielä Ciscon SSL VPN -lisenssi, joka nostaa ohjelmattomien ja AnyConnect-käyttäjien maksimimäärän joko 10:een tai 25:een.

Kymmenen käyttäjän SSL VPN -lisenssillä on hintaa alimmillaan $750 (PriceGrabber.com 2011a) ja vastaavasti 25 käyttäjän lisenssi maksaa halvimmillaan $1800 (PriceGrabber.com 2011b). SSL VPN -lisenssien hinnat ovat riippumattomia käytettävästä laitteesta.

4 ETÄYHTEYSPROTOKOLLAT

4.1 Remote Desktop Protocol (RDP)

Microsoftin Remote Desktop Protocol (RDP) on suunniteltu tukemaan erilaisia verkkotopologioita ja useita LAN-protokollia. RDP mahdollistaa etänäyttö- ja etäsyöttötoiminnot palvelimella ajettaville Windows-pohjaisille ohjelmille verkkoyhteyden yli. (Microsoft 2011.)

RDP on ITU T.120-protokollaperheeseen pohjautuva protokolla. RDP käyttää useaa, erillistä virtuaalista kanavaa datan kuljettamiseen. Yhteensä 64 000 kanavaa voidaan käyttää samanaikaisesti tiedonsiirtoon. Salaukseen RDP käyttää RSA Securityn RC4-salainta. (Microsoft 2011.)

RDP hyödyntää välimuistia ja pakkausta verkon yli lähetettävän datan määrän pienentämiseksi. Bittikarttavälimuistin käyttö voi nopeuttaa suorituskykyä huomattavasti hitailla yhteyksillä käytettäessä, etenkin, jos ajettavat ohjelmat hyödyntävät suuria bittikarttoja. (Microsoft 2011.)

Käyttäjä voi katkaista yhteyden etätyöpöytäistuntoon kirjautumatta ulos. Yhteyden katketessa verkon taikka asiakkaan takia käyttäjää ei kirjata ulos. Kirjautuessaan takaisin järjestelmään samalta tai toiselta työasemalta yhdistyy käyttäjä takaisin katkaistuun istuntoon. (Microsoft 2011.)

Käyttäjä voi kopioida, poistaa ja liittää tekstiä ja kuvia paikallisen ja etäohjelman välillä sekä etäistuntojen välillä. Etätyöpöytäistunnossa ajettavat ohjelmat voivat myös tulostaa käyttäjän työasemaan liitettyyn tulostimeen. (Microsoft 2011.)

Etätyöpöytäistuntoja voidaan seurata ja ohjata. Syötteiden ja näyttöjen jakaminen useamman istunnon välillä helpottaa ylläpidon ongelmanratkaisua ja diagnosointia. (Microsoft 2011.)

4.2 X Window System

X Window System, yleisesti tunnettu X:nä, on erittäin muunneltava, järjestelmäriippumaton ja ilmainen asiakas-palvelin-järjestelmä graafisten käyttöliittymien hallintaan yksittäisillä tietokoneilla ja tietokoneverkostolla. X on laaja ja monimutkainen järjestelmä, jonka monimutkaisuutta voidaan verrata käyttöjärjestelmään. X on de facto grafiikkamoottori Linux-käyttöjärjestelmille ja muille Unixin kaltaisille käyttöjärjestelmille. X on yksi menestyksekkäimmistä ilmaisista ohjelmistoista. (The Linux Information Project 2006a.)

Yksi X:n suurimmista ominaisuuksista on sen irrallisuus käyttöjärjestelmästä. Jos palvelimeen ei tarvita graafista käyttöliittymää, voidaan X helposti jättää asentamatta ja näin säästetään prosessorikuormassa ja muistin käytössä. X ei itsessään määrittele tai tarjoa käyttöliittymää tai määrittele käyttöliittymän ulkonäköä millään tavalla eikä sovellusten käyttäytymistä tai ikkunanhallintaohjelman toimintoja. Käyttöliittymä toteutetaan toisella ohjelmalla, minkä takia X-pohjaiset ympäristöt ovat erittäin joustavia ja monia käyttöliittymätyylejä voi olla yhdellä tietokoneella useita. Käyttäjä ei ole suoraan vuorovaikutuksessa X:ään. (The Linux Information Project 2006a.)

X on enemmänkin standardi kuin yksittäinen ohjelmisto, ja mitä tahansa standardia toteuttavaa ohjelmaa kutsutaan X Window Systemiksi. X piirtää suorakulmion muotoisia ikkunoita. Ikkunoihin voidaan piirtää tekstiä ja grafiikkaa. X tukee myös syöttölaitteita, kuten näppäimistöjä ja hiiriä. Kaikkien graafisten toimintojen on noudatettava X-standardia, mikäli halutaan taata sujuva toimivuus Unix-pohjaisten käyttöjärjestelmien kanssa. (The Linux Information Project 2006a.)

X:n monimuotoisuus johtuu X:n käyttöjärjestelmäriippumattomuudesta ja asiakas-palvelin-rakenteesta. X:n asiakas-palvelin-malli toimii poiketen yleisesti totutusta mallista. Jokaisella paikallisella laitteella on X server-ohjelma ja paikalliselta laitteelta voidaan ottaa yhteys etälaitteisiin, joilla ajetaan X client-ohjelmaa. X server on ohjelma, jota ajetaan paikallisella laitteella, ja joka hoitaa yhteyden näytönohjaimiin, näyttöihin ja syötelaitteisiin. (The Linux Information Project 2006a.)

X client voi olla mikä tahansa sovellus. X client esiintyy X serverillä mutta on muuten erillään serveristä. X client pääsee ikkunointipalveluihin kiinni Xlib-kirjaston kautta. Xlib-kirjasto on kokoelma yleisiä X:n tehtäviä. Järjestelmä kääntää käskyt X-protokollaviesteiksi X serverille. Työpöytäympäristö tai ikkunanhallintaohjelma toimii myös clientina. (The Linux Information Project 2006a.)

Asiakas-palvelin-arkkitehtuuri mahdollistaa X:n toiminnan irrallaan sekä sovelluksesta että käyttöjärjestelmästä, mikä on luotettavin ja turvallisin ratkaisu. Etuna ratkaisussa on X serverin vuorovaikutus käyttöjärjestelmään ja laitteistoon. X clientin ei tarvitse ottaa kantaa alla piilevään käyttöjärjestelmään ja laitteistoon, mikä yksinkertaistaan X clientin suunnittelua. Ohjelma, joka toimii X clientina voi esiintyä missä tahansa järjestelmässä, joka käyttää X serveriä. (The Linux Information Project 2006a.)

Asiakas-palvelin-arkkitehtuuria ei käytetä pelkästään laitteiden välillä verkon yli vaan myös yksittäisellä työasemalla. Etuna arkkitehtuurin käytössä yksittäisellä asemalla on johdonmukaisuus paikallisten ja verkkotoimintojen välillä. Toinen etu on järjestelmän vakauden lisääminen. X serverin kaatuessa voidaan tilanne yleensä korjata vielä komentoriviltä käynnistämättä koko työasemaa uudestaan. (The Linux Information Project 2006a.)

X clientin ja X serverin irrallisuus vaatii enemmän resursseja laitteistolta kuin integroidut ratkaisut. Muistin, prosessointitehon ja kovalevytilan suhteellisten hintojen laskun ansiosta X:n raskaus korvautuu helposti monimuotoisuudellaan ja muilla eduilla. (The Linux Information Project 2006a.)

X protokolla on pakettipohjainen protokolla. Kun X clientia ajetaan X serverin kanssa eri laitteilla, reititetään X protokolla lähiverkon, internetin tai muun verkon yli käyttäen TCP/IP-siirtopalvelua. Samalla laitteella ajaessa nopein tiedonsiirtokanava on Unix domain sockets (UDS), joka on prosessien välinen kommunikointimekanismi. (The Linux Information Project 2006b.)

4.3 NoMachine NX

NX Distributed Computing Architecture on kokoelma tekniikoita ja kaupallisia työkaluja, jotka on suunniteltu tekemään verkon yli työskentelystä yhtä helppoa ja laajalle levinnyttä kuin web-selailu. NX Distributed Computing Architecturen palvelinohjelmisto mahdollistaa minkä tahansa Unix-laitteen toimimisen terminaalipalvelimena. Valmistaja NoMachine on valinnut ohjelmiston pohjaksi X Window Systemin, joka toimii Unix-järjestelmien graafisen käyttöliittymän takana. (Regis 2009.)

NX-projektin päämäärä alusta pitäen on ollut kehittää X:n pakkausteknologiaa. Kehityksen tavoitteena on mahdollistaa kenen tahansa käyttäjän ajaa muokkaamatonta versiota X työpöytäympäristöstä tavallisella X serverillä minkälaisen verkkoyhteyden tahansa yli. Tavoitteen täyttyminen on NoMachinen mukaan vaatimus, jotta X Window System saisi takaisin verkkotyöskentelyprotokollan asemansa. (Regis 2009.)

NoMachine on kehittänyt X protokollan pakkaustekniikoita sekä integroidun kokoelman proxy agentteja. Kehitystyön ansiosta on mahdollista ajaa kokonaista etätyöpöytäistuntoa täydessä ruudussa käyttäen kapeakaistaista internetyhteyttä. Parhaimmillaan voidaan onnistua jopa 9600 modeemin nopeuksilla, eli 9,6 kilobitin sekuntinopeuksilla. (Regis 2009.)

NX:n pakkaus toimii X protokollan kolmella eri tasolla. Verkkoliikenteen pakkaus tapahtuu monella eri tavalla, mm. viestikohtaisilla algoritmeilla, kehittyneillä välimuistitekniikoilla sekä häviöttömillä ja häviöllisillä kuvan pakkaustekniikoilla. NX:n tekniikka myös vähentää verkon edestakaista liikennettä maksimoiden suoritustehon. Kolmanneksi, mukautuminen siirtonopeuteen tapahtuu reaaliajassa verkon olosuhteiden mukaan. (Regis 2009.)

NX:n X protokollan pakkaus on johdettu Differential X Protocol Compression (DXPC) -hankkeesta. DXPC tarjoaa monille X protokollaytimen lähes 160 pyyn-

nöstä, vastauksesta ja tapahtumasta tarkan differentiaalisen koodauksen. (Pinzari 2003.)

NX pitää päämuistissaan yllä MessageStore-nimistä välimuistia viimeisistä X:n viesteistä. Nopean haun takaamiseksi NX laskee MD5-tarkistussumman kaikista uusista pyynnöistä tai vastauksista, jotka pitää koodata. Tarkistussummaa varten pitää olla huomioimatta saman X:n pyynnön eri instanssien välillä todennäköisesti muuttuvat kentät. (Pinzari 2003.)

MessageStore-välimuistin tila- ja sijaintitietojen koodaukset vaativat tilaa kahden ja kuuden bitin väliltä riippuen protokollaviestistä. 64-bittiset Drawable ja Gcontext saadaan koodattua kahdesta kahdeksaan bittiin, mikä mahdollistaa 176-bittisen eli 22-tavuisen PolySegment-pyynnön koodauksen neljästä 14 bittiin. Pakkaussuhde saadaan siis nostettua yli 10:1:een. (Pinzari 2003.)

Mikäli viestiä ei löydy välimuistista, koodaa proxy viestin kenttä kentältä. Proxy myös merkitsee sijainnin, mihin dekoodaava osapuoli tallettaa viestin välimuistiinsa. Koska koodaava puoli määrää viestin paikan välimuistissa, voidaan sanoa, että jokainen proxy hallitsee vastapuolensa välimuistin. Proxy tietää tarkalleen millä tahansa ajan hetkellä, mikäli viesti voidaan hakea välimuistista ilman, että verkkoon aiheutetaan edestakaista liikennettä. Koodaavan osapuolen tarvitsee laskea vain viestien tarkistussummat, koska dekoodaavan osapuolen tarvitsee tallentaa vain hyötykuorma. Muistin tarve molemmille pienenee huomattavasti. (Pinzari 2003.)

NX:n palvelintuotteet toimivat Linux-käyttöjärjestelmän päällä. NX:n käyttömahdollisuudet ja etätyöskentelytoiminnallisuudet eivät kuitenkaan rajoitu pelkästään Linux-työasemiin ja palvelimiin. NX osaa kapsuloida X protokollan sisään sekä Microsoft Windows Terminal Serverin ja Citrix Metaframen käyttämän Remote Desktop Protocol:n sekä Virtual Network Computingin käyttämän Remote Frame Buffer-protokollan. (Regis 2009.)

NX Distributed Computing Architecture on suunniteltu alusta pitäen kuorman jakoon solmujen välillä WAN-verkossa. NX Serverit hoitavat esimerkiksi autentikoinnin ja käyttäjäistuntojen aktivoinnin. NX Node -tietokoneilla ajetaan istunnot virtuaaliklusterissa. Sadat NX-solmut voivat liittyä yhteen tai useampaan palvelimeen tukien tuhansia samanaikaisia istuntoja. NX-verkko on hyvin samankaltainen peer-to-peer-verkon kanssa, mutta käyttäjä etsiikin sovellusta tai työpöytäympäristöä ja hakukone ohjaa käyttäjän tarkoituksenmukaiselle palvelimelle, mikäli käyttäjän tunnistus onnistuu. (Regis 2009.)

Monimutkaisuudestaan huolimatta Unixiin sisäänrakennetut verkkotyöskentelyominaisuudet ja X Window Systemin skaalautuvuus tekevät NX:stä suoraviivaisen. Kaikki dataliikenne kulkee salattuna SSH-kanavassa, joten etätyöpöytäyhteys voidaan toteuttaa SSH-protokollan avulla. (Regis 2009.)

4.4 Remote Framebuffer (RFB)

Remote Framebuffer (RFB) on yksinkertainen protokolla, joka mahdollistaa etäyhteyden graafiseen käyttöliittymään. Framebuffer-tason toimintansa ansiosta RFB soveltuu kaikkiin ikkunointijärjestelmiin, mukaan lukien X11, Windows ja Macintosh. RFB on Virtual Network Computingissa (VNC) käytetty protokolla. (Richardson 2010.)

Käyttäjä on RFB-asiakaspäässä yhteyttä. RFB-palvelin on yhteyden toisessa päässä, missä muutokset framebufferiin tapahtuu. RFB on ”thin client”-protokolla. Suunnittelun pääpaino on asettaa asiakasohjelmalle mahdollisimman vähän vaatimuksia. Suunnittelun ansiosta asiakasohjelma voidaan ajaa suurella määrällä eri laitteistoja. Asiakasohjelman toteutus on myös tehty mahdollisimman yksinkertaiseksi. (Richardson 2010.)

Protokolla tekee asiakasohjelmasta tilattoman. Mikäli asiakasohjelman yhteys palvelimeen katkeaa, käyttöliittymän tila säilyy uudelleen yhdistäessä palvelimeen. Samaan RFB-palvelimeen voi yhdistää myös toisesta asiakaspäästä. Uusi

asiakas näkee täysin saman näkymän kuin ensimmäinenkin. Käytännössä käyttäjän ohjelman käyttöliittymä on täysin mobiili. (Richardson 2010.)

Protokollan esityspuoli perustuu yksinkertaiseen graafiseen käskyyn: ”aseta pikselidataa ruutu annettuun x,y-sijaintiin”. Tehottoman oloisella piirtotavalla on myös puolensa. Erilaiset koodaukset pikselidatalle mahdollistavat monipuolisen, eri parametrien huomioon ottamisen, mukaan lukien verkon kaistanleveyden, asiakkaan piirtonopeuden ja palvelimen prosessointinopeuden. Ruudunpäivityspyynnöt ovat asiakaslähtöisiä. (Richardson 2010.)

Syöttöpuoli protokollasta perustuu tavallisen työaseman malliin näppäimistöstä ja moninäppäimisestä osoitinlaitteesta, yleensä hiirestä. Syötetapahtumat lähetetään palvelimelle asiakkaan painaessa näppäimistön tai hiiren nappia tai hiirtä liikuttaessa. Syötetapahtumia kuten näppäinpainalluksia voidaan luoda myös muilla epästandardeilla laitteilla, kuten kynäpohjaisella käsialatunnistuksella. (Richardson 2010.)

4.5 Etähallintaprotokollat ja VPN

Etähallintaprotokollat liittyvät työhön olennaisesti, koska pelkästä VPN-yhteydestä tietoverkkolaboratorioon on rajallinen hyöty. Etähallinnan ansiosta VPN-yhteyden yli voidaan tehdä erilaisia laboratorioharjoituksia esimerkiksi kotoa käsin.

Etähallinta tarjoaa mahdollisuuden käyttää hallittavaa työasemaa toiselta työasemalta näppäin- ja hiirisyötteillä. Etähallintaprotokollat tarvitsevat yleensä reilusti kaistaa, koska kuvan siirto tapahtuu bittikarttoihin perustuen. NoMachinen NX on käsitellyistä protokollista ainoa, joka voi toimia reilusti hitaammilla yhteyksillä pakkauksensa ansiosta. Lisäksi NoMachine-yhteys voidaan luoda SSH:n yli, minkä ansiosta tarvitaan vähemmän portteja käyttöön kuin VNC- tai X-ikkunoinnilla. NX-ikkunointi onkin valittu laboratorion Linux-palvelimien etäyhteysprotokollak-

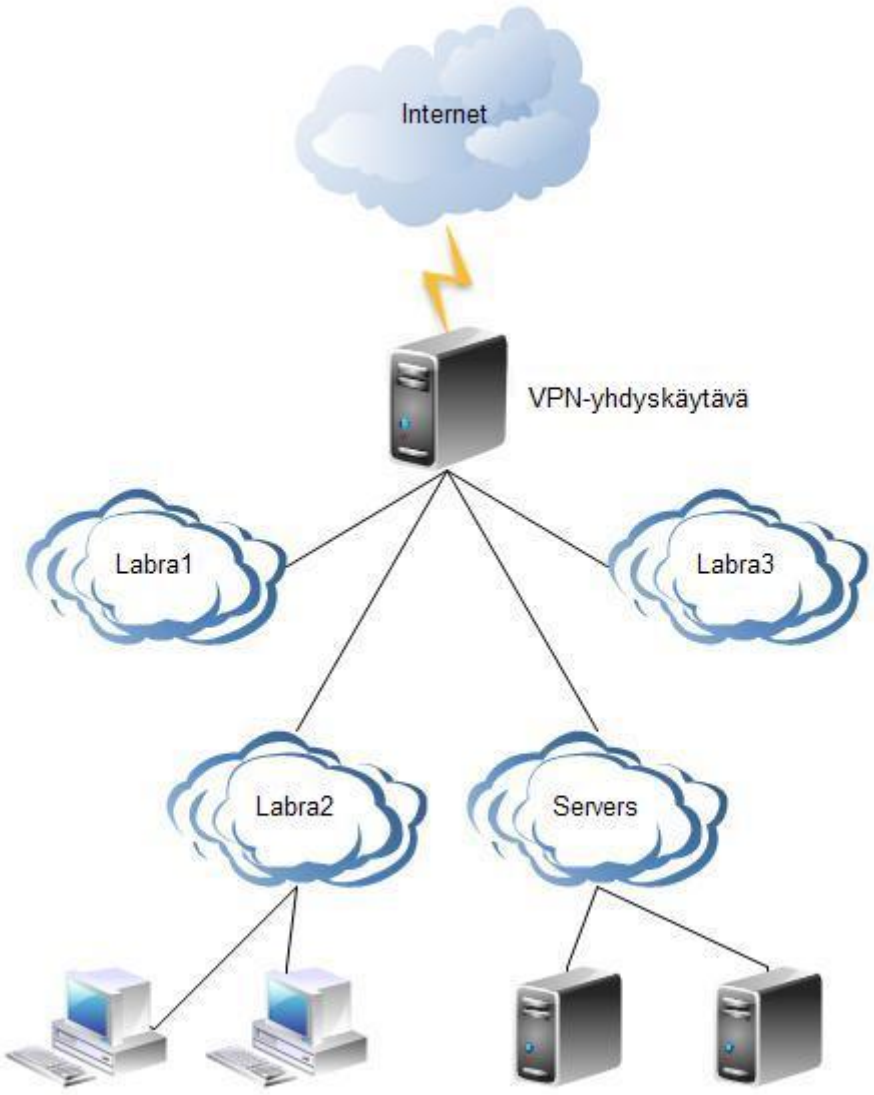
si ja RDP puolestaan Windows-työasemien ja -palvelimien etäyhteysprotokollaksi. Lisäksi hyödynnetään SSH-protokollaa tekstipohjaisiin etäyhteyksiin.

Työssä ei tarvinnut toteuttaa etäyhteyksiä, koska nykyistä ympäristöä varten toteutettuja yhteyksiä voitiin hyödyntää. Nykyisiä etäyhteyksiä piti kuitenkin testata uusilla VPN-yhteyksillä yhteensopivuuden varmistamiseksi.

5 TOTEUTETTU YMPÄRISTÖ

5.1 Testiympäristön kuvaus

Testattaviksi VPN-yhdyskäytäviksi valittiin OpenVPN Access Server -ohjelmisto ja Cisco ASA 5505 -palomuurilaite. Molempiin tutustuttiin ja ratkaisujen tarjoamia ominaisuuksia testattiin monipuolisesti.



KUVIO 12. Laboratorioverkon malli

Kuviossa 12 on esitetty malli laboratorioverkosta, johon etäyhteys haluttiin toteuttaa VPN:n avulla. Yhdyskäytävän takana on useita aliverkkoja, joissa on esimerkiksi palvelimia tai etähallittavia Linux- ja Windows-työasemia laboratorioharjoituksia varten.

OpenVPN:n eri ominaisuuksia ja niiden toimivuutta kokeiltiin asentamalla OpenVPN virtuaalikoneelle. Käyttäjien autentikointia LDAP:lla AD-käyttäjätietokantaa vasten testattiin ajamalla OpenVPN-palvelimen rinnalla Windows Server 2008 R2 -palvelinta. Server 2008 -palvelimelle otettiin käyttöön Active Directory -rooli ja luotiin muutama käyttäjä. Tavoitteena oli testata tuotteita ensin testiympäristössä ja toteuttaa lopuksi valittu ratkaisu testatuilla asetuksilla myös tuotantoympäristöön.

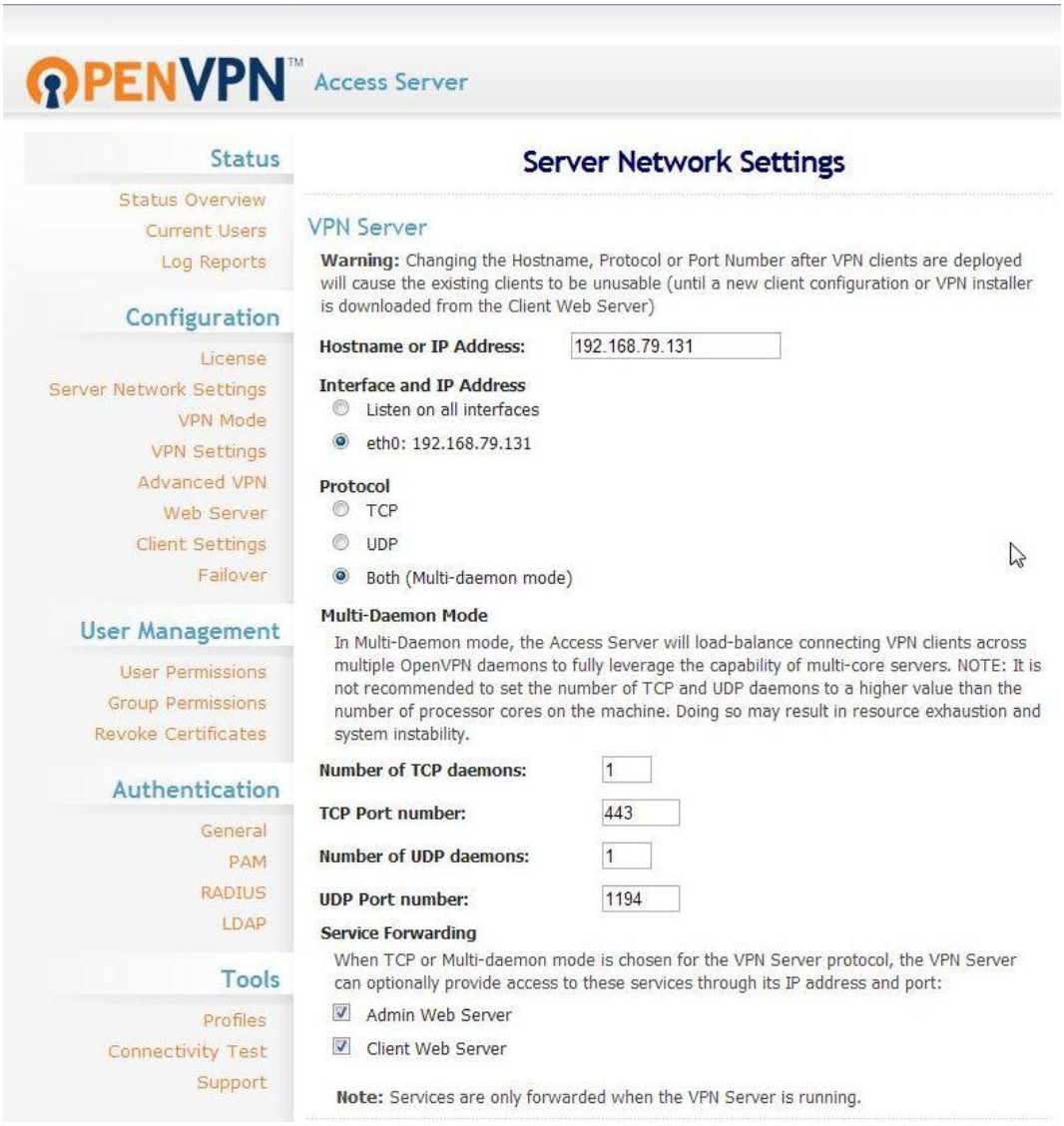
5.2 Asennus ja konfigurointi

OpenVPN:n asennus käy melko vaivattomasti, kun palvelimelle on ensin suunniteltu IP-osoitteistus ja lisenssiavain on hankittu. Asennus alkaa lataamalla käyttöjärjestelmälle tarkoitettu paketti OpenVPN:n web-sivustolta osoitteesta www.openvpn.net. Tämä onnistuu esimerkiksi komentoriviltä wget-ohjelmalla komennolla wget http://swupdate.openvpn.net/as/openvpn-as-1.6.1-CentOS5.x86_64.rpm. Paketin latauksen jälkeen asennetaan ohjelmisto. Käsky riippuu käyttöjärjestelmästä. Esimerkiksi CentOS:ssa paketin asennus tapahtuu käskyllä rpm -i openvpn-as-1.6.1-CentOS5.x86_64.rpm. Asennuksen yhteydessä ohjelma kysyy ulkoisen sekä sisäisen IP-osoitteen, käytettävät portit, lisensointiin liittyviä seikkoja ja sen, onko palvelin varmistusjärjestelmän toinen solmu.

Access Serverin konfigurointi voidaan aloittaa, kun asennus on valmis. Konfigurointi käy helpoiten web-käyttöliittymän kautta HTTPS-yhteyden yli. Selaimeen annetaan osoitteeksi palvelimen IP-osoite ja hallintaportti sekä alikansioksi admin, esimerkiksi https://192.168.79.131:943/admin. Sisäänkirjautumisen jälkeen AS:n konfigurointi tapahtuu valitsemalla valikosta kategoria ja syöttämällä halutut asetukset. Asetuksista voidaan lisätä hankitut lisenssit, muuttaa palvelimen verkko-

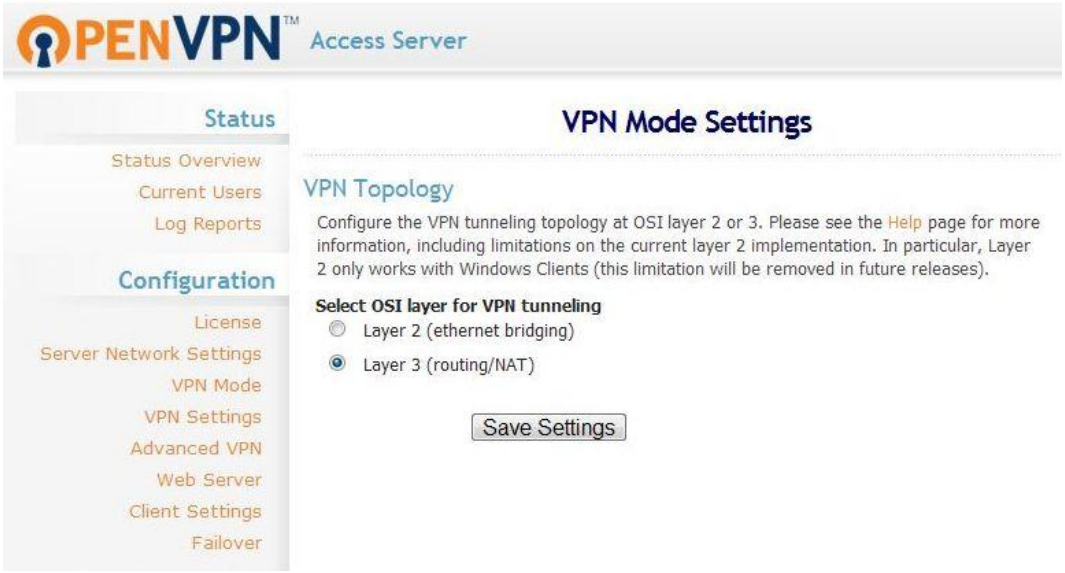
asetuksia, vaihtaa AS:n VPN-tila, määrittää VPN-asetukset, hallita käyttäjiä ja käyttäjäryhmiä sekä valita autentikointitapa.

Palvelimen verkkoasetuksista (kuvio 13) voidaan vaihtaa AS:n ulkoinen IP-osoite tai isäntänimi ja käytetty verkkoliitäntä. Lisäksi VPN Server -palvelun käyttämä portti sekä protokolla voidaan määrittää ja sallia tai estää Web Server -palvelujen uudelleenohjaus VPN Server -palvelun osoitteesta. Käytännössä uudelleenohjaus tarkoittaa, että käyttäjät voivat kirjautua samasta osoitteesta, kuin mihin he ottavat yhteyden VPN-yhteyden muodostusta varten.



KUVIO 13. OpenVPN verkkoasetukset

VPN-tila -asetuksista (kuvio 14) voidaan VPN-tilaksi määrittää joko L2 tai L3 eli ethernet-siltaus tai reititys/NAT. L3-tila NAT:n kanssa ei vaadi verkon muiden laitteiden asetusten muuttamista. L3-tila ilman NAT:ia vaatii palvelimen ulkopuolista konfigurointia. Käytännössä reitittimelle tarvitaan reitti, joka ohjaa VPN-käyttäjän IP-osoitteeseen tarkoitetut vastauspaketit OpenVPN-palvelimelle. VPN-asetuksista voidaan määrittää käyttäjille IP-osoiteavaruus sekä erilaisia reititys-sääntöjä. Säännöt määräävät, pääsevätkö VPN-käyttäjät AS:n takana oleviin yksityisiin aliverkkoihin.



KUVIO 14. OpenVPN:n VPN-tila-asetukset

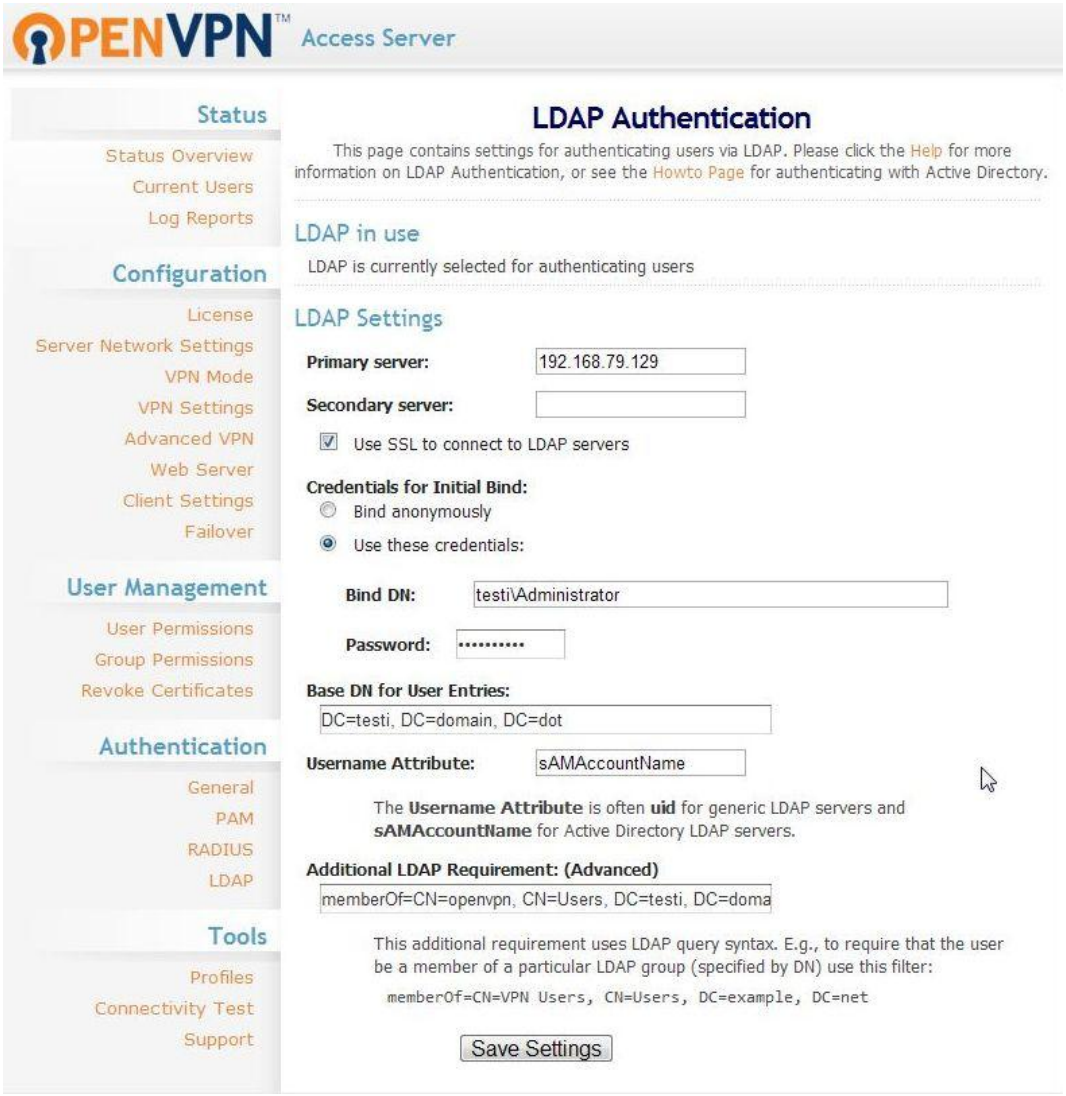
Autentikointiasetuksista voidaan määrittää käyttäjien tunnistukseen käytettävä tietokanta. Vaihtoehtoina ovat paikallinen käyttäjäkanta, jota hallitaan web-käyttöliittymästä, PAM eli Pluggable Authentication Modules, joka autentikoi käyttäjät Access Serveriä ajavan Unix-järjestelmän käyttäjäkantaan, yhdestä viiteen RADIUS-palvelinta tai LDAP-palvelin, joka voi olla esimerkiksi Active Directory -palvelin. Useampaa tapaa ei voida käyttää samanaikaisesti. Työssä käytettiin LDAP-käyttäjätunnistusta, jonka konfigurointia varten tarvitaan AD-palvelimen isäntänimi tai IP-osoite sekä käyttäjätunnus ja salasana käyttäjätiliin, jolla on ylläpito-oikeudet AD:yyn. Lisäksi tarvitaan tietää polku, mistä käyttäjät löytyvät AD-palvelimelta. LDAP-asetuksista voidaan myös vaatia, että käyttäjä kuuluu johonkin tiettyyn ryhmään, jotta kirjautuminen VPN:iin onnistuu.

Cisco ASA 5505 oli helppo konfiguroida selaimen kautta ajettavan Java-sovelluksen avulla ja asennus-wizardin kautta. Laitteen ominaisuudet ovat monipuoliset, tosin palomuuriominaisuuksista ei tarkoitetussa käytössä ole hyötyä. ASA 5505 voidaan myös konfiguroida käyttämään LDAP-autentikointia. Muutenkin Ciscon laitteeseen voidaan ottaa käyttöön samat asetukset kuin OpenVPN:iin. Ciscon palomuurilla onnistuu myös site-to-site-IPSec-yhteys.

5.3 Testatut ominaisuudet ja hinnoittelu

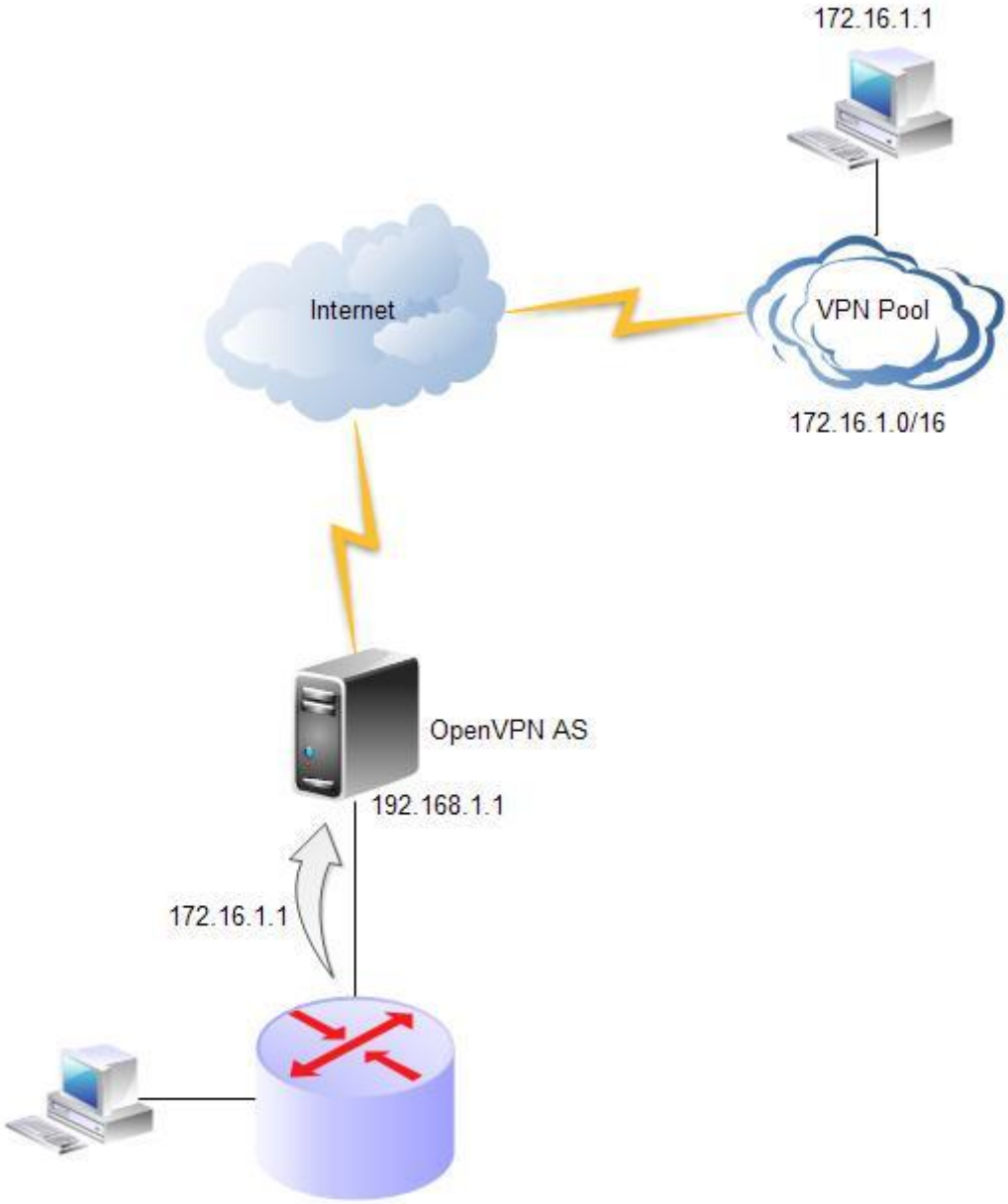
OpenVPN:ään konfiguroitiin LDAP-autentikointi web-käyttöliittymän kautta. OpenVPN tarvitsi autentikointiin käytettävän tunnuksen AD-palvelimeen, sekä AD-palvelimen IP-osoitteen ja oikean polun käyttäjäkantaan. Kirjautuminen luodulla käyttäjätunnuksella onnistui välittömästi asetusten muutosten tekemisen jälkeen. Kokeiltiin vielä tunnuksen kytkemistä pois käytöstä, minkä jälkeen kirjautuminen luonnollisesti epäonnistui.

LDAP-autentikoinnin yhteys on mahdollista salata SSL-tekniikalla. SSL-salaus vaatii Windows Serveriltä IIS ja Certificate Services -roolien käyttöönottoa. Mikäli SSL-salaus oli käytössä, mutta Server 2008:n roolit ja asetukset eivät olleet kunnossa, ei kirjautuminen onnistunut. Kuviossa 15 on esitetty OpenVPN:n asetukset LDAP-autentikointia varten. Asetuksissa on määritetty LDAP-palvelimen ip-osoite tai isäntänimi sekä autentikointiin tarkoitettu käyttäjätunnus ja salasana. Testitoimialueena oli testi.domain.dot. AD-palvelimella oli käyttäjäryhmä ”openvpn”, joka OpenVPN-palvelimelle konfiguroitiin käyttäjän vaadituksi ryhmäksi. Muiden ryhmien käyttäjien ei onnistunut liittyä VPN:iin.



KUVIO 15. OpenVPN LDAP-autentikointiasetukset

Työssä testattiin myös OpenVPN:n L2- ja L3 VPN-tiloja. L3-tila NAT-toiminnon kanssa ei vaatinut minkäänlaisia toimenpiteitä ja on vakiona OpenVPN:ssä päällä. L3-tila ilman NAT:ia vaatii sisäverkon reitittimen reititystauluun muutoksen, joka ohjaa vastauspaketit VPN-käyttäjille OpenVPN-palvelimen sisäverkon IP-osoitteeseen. Ilman reititystaulun päivitystä jäävät paketit matkalle, koska sisäverkon reititin ei tunne reittiä VPN-käyttäjien aliverkkoon. Kuviossa 16 on esimerkki OpenVPN:n L3-tilasta ilman NAT:ia. VPN-käyttäjä saa osoitteen VPN-yhteyksille annetusta osoiteavaruudesta, esim. 172.16.1.0/16. Mikäli sisäverkon reititin ei tunne reittiä lähdeosoitteelle, eli ei osaa lähettää pakettia OpenVPN-palvelimelle, ei käyttäjä saa vastausta. L2-tilassa VPN-käyttäjä saa IP-osoitteen suoraan sisäverkon IP-avaruudesta.



KUVIO 16. Esimerkki OpenVPN:n L3 VPN-tilasta ilman NAT:ia

OpenVPN tekee palvelimen palomuuriasetukset automaattisesti, tosin sääntölista on sekava ja pitkä. Toiminnallisuuden saa myös pois päältä. Työn aikana kokeiltiin ottaa iptables-sääntöjen automaattinen luonti pois ja tietoturvan lisäämiseksi säätää avoimet portit käsin. Portteja avattiin ja verrattiin palomuurisääntöjä automaattisesti luotuihin, mutta jostain syystä kirjautuminen ei onnistunut VPN:ään. Todettiin palomuurisääntöjen hallinnoinnin olevan käsin liian työlästä.

Ciscon web-selainpohjaista asiakasohjelmaa ei päästy kokeilemaan käytössä olevan Essentials-lisenssin takia. Mallikappaleeseen oli mahdollista ottaa VPN-yhteys esiasennettavalla AnyConnect-ohjelmalla. Sekä OpenVPN:n että Ciscon asiakasohjelmat olivat käyttäjän kannalta yksinkertaiset ja helppokäyttöiset.

ASA 5505:n heikkoutena oli hinnoittelu. Laitteeseen on saatavilla kolme eri lisenssiä, jotka määräävät samanaikaisten VPN-käyttäjien maksimimäärän. Valittavana on kaksi, kymmenen tai 25 samanaikaista VPN-käyttäjää. 10 samanaikaisen IPSec VPN-käyttäjän Security Plus-lisenssin hinta on halvimmillaan lähes 500 dollaria (PriceGrabber.com 2011d). ASA 5505-palomuuriin ei myöskään ole saatavilla enempää samanaikaisia VPN-yhteyksiä mahdollistavaa lisenssiä, vaan laite olisi tarpeen vaatiessa vaihdettava ASA 5510-malliin.

OpenVPN:n samanaikaisten VPN-käyttäjien määrä riippuu myös lisenssistä, mutta OpenVPN:ään on mahdollista ostaa haluamansa kokoinen lisenssi. Minimiostos on kymmenen yhtäaikaisen käyttäjän lisenssi. Jokainen ostettu käyttäjälisenssi maksaa viisi dollaria käyttäjältä. OpenVPN:n hinnoittelu on hyvin skaalautuva ja soveltuu erikokoisten yritysten tarpeisiin. Hinnoittelunsa ansiosta OpenVPN:ää varten voidaan ostaa juuri sopiva määrä käyttäjälisenssejä tarpeisiin nähden. Lisenssi hankittiin lopulta sadalle samanaikaiselle käyttäjälle ja hintaa ostokselle tuli noin 360 euroa.

Lopulta toteutus päädyttiin tekemään OpenVPN AS:llä, jonka hinnoittelulogiikka sopi tarkoitukseen paremmin kuin Ciscon vastaava. Lisäksi voitiin käyttää hyväksi käytössä olevan SSL-Explorer-palvelimen laitteisto.

Lopulta OpenVPN AS asennettiin tuotantoympäristöön CentOS-palvelimelle ja annettiin testattavaksi muutamalle käyttäjälle samalla, kun AS:n ominaisuuksiin ja asetuksiin tutustuttiin tarkemmin. AS:n versio päivittyi työn aikana, mikä nähtiin positiivisena seikkana. Päivityksen myötä OpenVPN sai tuen asiakasohjelmattomalle VPN-yhteydelle.

6 YHTEENVETO

Työn tavoitteena oli korvata nykyinen, käytössä ollut SSL-Exploreria käyttävä VPN-ratkaisu toisella järjestelmällä. OpenVPN Access Server paljastui helposti ylläpidettäväksi, käyttäjän kannalta helppokäyttöiseksi ja lisenssipolitiikkansa puolesta sopivaksi ratkaisuksi. Myös Cisco ASA 5505 olisi soveltunut kaikin puolin korvaamaan nykyisen järjestelmän, mutta laitetta ja Ciscon lisensointia pidettiin kalliina. OpenVPN:n edullisuutta lisäsi vielä mahdollisuus käyttää hyväksi käytössä olevaa palvelinta, eli laitteistosta ei kertynyt lisäkuluja.

OpenVPN Access Serverin ja Ciscon ASA 5505:n välillä ei SSL VPN:n kannalta ole juuri eroa. Molempien konfigurointi käy helposti. Testatun ASA-mallin heikkoudeksi jäi SSL VPN -käyttäjien maksimimäärän pienuus. Molempien asiakasohjelma on hyvin helppokäyttöinen ja yksinkertainen.

Tulevaisuudessa OpenVPN AS:ä voidaan joutua päivittämään tai siirtämään toiseen palvelimeen. Käyttäjien vaihtuminen ei aiheuta toimenpiteitä, koska autentikointi tapahtuu AD-palvelimen kautta. Käyttäjämäärän lisääntyminen voi johtaa lisälisenssien hankintaan. OpenVPN:n käyttöönoton jälkeen on huolehdittava myös varmuuskopioinnista ja mahdollisesti varajärjestelmän pystyttämisestä.

SSL VPN yleistynee helppoutensa ja toimintansa ansiosta. SSL-protokolla on standardoitu ja käytetty TCP/443-portti on lähes aina palomuureissa sallittu. Asiakasohjelman tarpeettomuus helpottaa käyttäjän toimintaa entisestään. IPSec tuskin häviää VPN-rintamalta, koska tekniikka soveltuu hyvin verkkojen yhdistämiseen, esimerkiksi eri paikoissa sijaitsevien toimistojen yhteen liittämiseen.

LÄHTEET

Bollapragada, V., Khalid, M. & Wainner, S. 2005. IPSec VPN Design. Cisco Press.

Cisco Systems. 2010a. Cisco ASA 5500 Series Adaptive Security Appliances [viitattu 22.2.2011]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.pdf

Cisco Systems. 2010b. Cisco ASA 5500 Series Adaptive Security Appliances [viitattu 18.3.2011]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd80285492.pdf

Cisco Systems. 2011. Cisco AnyConnect Secure Mobility Client Administrator Guide [viitattu: 22.2.2011]. Saatavissa: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/acadmin30.pdf

Denis, F. UCARP [viitattu 17.2.2011]. Saatavissa: http://www.ucarp.org

EMC Corporation. 2010. RSA Laboratories - 2.1.7 What are Message Authentication Codes? [viitattu: 31.3.2011]. Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2177

EMC Corporation. 2011a. Certificate authority, certification authority (CA) [viitattu: 31.3.2011]. Saatavissa: http://www.rsa.com/glossary/default.asp?id=1010

EMC Corporation. 2011b. Symmetric key cryptography. [viitattu: 31.3.2011]. Saatavissa: http://www.rsa.com/glossary/default.asp?id=1053

Frahim, J. & Huang, Q. 2008. SSL Remote Access VPNs. Cisco Press. Indianapolis, USA.

Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. & Zorn, G. 1999. Point-to-Point Tunneling Protocol (PPTP). RFC 2637 [viitattu 14.12.2010]. Saatavissa: http://tools.ietf.org/html/rfc2637

Lau, J., Townsley, M. & Goyret, I. 2005. Layer Two Tunneling Protocol – Version 3 (L2TPv3). RFC 3931 [viitattu 11.1.2011]. Saatavissa: http://tools.ietf.org/html/rfc3931

Lewis, M. 2006. Comparing, Designing, and Deploying VPNs. Cisco Press. Indianapolis, USA.

Microsoft. 2002. Administrator's Guide to Microsoft L2TP/IPSec VPN Client [viitattu 18.3.2011]. Saatavissa: http://technet.microsoft.com/en-

gb/library/bb742553.aspx

Microsoft. 2005. Point-to-Point Tunneling Protocol [viitattu 18.3.2011]. Saatavissa: http://technet.microsoft.com/en-us/library/cc738852(WS.10).aspx

Microsoft. 2011. Remote Desktop Protocol [viitattu: 23.2.2011]. Saatavissa: http://msdn.microsoft.com/en-us/library/aa383015.aspx

OpenVPN ALS. 2011. [Viitattu 17.3.2011]. Saatavissa: http://sourceforge.net/projects/openvpn-als/

OpenVPN Technologies. 2010a. Access Server FAQ [viitattu 16.2.2011]. Saatavissa: http://openvpn.net/index.php/access-server/section-faq-openvpn-as

OpenVPN Technologies. 2010b. OpenVPN Access Server [viitattu 17.2.2011]. Saatavissa: http://www.openvpn.net/images/OpenVPNAccessServerDataSheet.pdf

OpenVPN Technologies. 2010c. OpenVPN Access Server v1.6 System Administration Guide [viitattu 16.2.2011]. Saatavissa: http://openvpn.net/images/pdf/OpenVPN_Access_Server_v1_6_Sysadmin_Guide_Rev_1.pdf

OpenVPN Technologies. 2011. How to setup Global Routing in OpenVPN Access Server [viitattu: 17.2.2011]. Saatavissa: http://www.openvpn.net/index.php/access-server/docs/admin-guides/215-how-to-setup-routing-in-openvpn-access-server.html

Ou, G. 2004. PPTP VPN authentication protocol proven very susceptible to attack [viitattu 14.12.2010]. Saatavissa: http://www.zdnet.com/blog/ou/pptp-vpn-authentication-protocol-proven-very-susceptible-to-attack/21

PGP Corporation. 2004. An Introduction to Cryptography [viitattu: 31.3.2011]. Saatavissa: http://download.pgp.com/pdfs/Intro_to_Crypto_040600_F.pdf

Pinzari, G. 2003. NX X Protocol Compression [viitattu: 25.2.2011]. Saatavissa: http://www.nomachine.com/documents/pdf/NX-XProtocolCompression.pdf

PriceGrabber.com. 2011a. Cisco ASA 5500 Series SSL VPN - License - 10 User. [viitattu: 31.3.2011]. Saatavissa: http://software.pricegrabber.com/networking-connectivity/Cisco-ASA-5500-SSL-VPN-10-User-Lic/m19875428.html

PriceGrabber.com. 2011b. Cisco ASA 5500 Series SSL VPN - License - 25 User [viitattu: 31.3.2011]. Saatavissa: http://software.pricegrabber.com/networking-connectivity/Cisco-ASA-5500-SSL-VPN-25-User-license/m17744253.html

PriceGrabber.com. 2011c. Cisco ASA 5505 10-User Bundle Specs and Deals [viitattu: 18.3.2011]. Saatavissa: http://computers.pricegrabber.com/firewall-security-devices/Cisco-Asa-5505-Appliance-10-User-K9/m34879390.html

PriceGrabber.com. 2011d. Cisco ASA 5505 Security Plus – ASA550ECPL [viitattu 28.2.2011]. Saatavissa: http://software.pricegrabber.com/security/Cisco-ASA-5505-Plus-license/m29564034.html

PriceGrabber.com. 2011e. Cisco 5510 Adaptive Security Appliance Specs and Deals [viitattu: 18.3.2011]. Saatavissa: http://computers.pricegrabber.com/firewall-security-devices/Cisco-ASA-5510-Appliance-3DES-AES/m9023031.html

PriceGrabber.com. 2011f. Cisco ASA 5520 VPN/Firewall Specs and Deals [viitattu: 18.3.2011]. Saatavissa: http://computers.pricegrabber.com/firewall-security-devices/ASA-5520-Appliance3DES-AES/m9023035.html

Regis, S. 2009. Introduction to NX Technology [viitattu: 25.2.2011]. Saatavissa: http://www.nomachine.com/documents/pdf/intr-technology.pdf

Richardson, T. 2010. The RFB Protocol [viitattu: 26.2.2011]. Saatavissa: http://www.realvnc.com/docs/rfbproto.pdf

Russell, R., Kaminsky, D., Puppy, R., Grand, J., K2, Ahmad, D., Flynn, H., Dubrawsky, I., Manzuik, S. & Permeh, R. 2002. Hack Proofing Your Network, Second Edition. Syngress Publishing, Inc. Rockland, USA.

Scott, C., Wolfe, P. & Erwin, M. 1999. Virtual Private Networks, Second Edition. O'Reilly Media.

The Linux Information Project. 2006a. An Introduction to X by Linux Information Project (LINFO) [viitattu: 23.2.2011]. Saatavissa: http://www.linfo.org/x.html

The Linux Information Project. 2006b. X Protocol Definition by The Linux Information Project (LINFO) [viitattu: 24.2.2011]. Saatavissa: http://www.linfo.org/x_protocol.html

Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. & Palter, B. 1999. Layer Two Tunneling Protocol "L2TP". RFC 2661 [viitattu 11.1.2011]. Saatavissa: http://tools.ietf.org/html/rfc2661

VPN Consortium. 2008. VPN Technologies: Definitions and Requirements [viitattu 11.1.2011]. Saatavissa: http://www.vpnc.org/vpn-technologies.html