KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma / tietoliikennetekniikka

Kantola Markus
Voutilainen Tommi

ETÄTYÖPÖYTÄYHTEYS KÄYTTÄEN SSL VPN -TEKNIIKKAA

Opinnäytetyö 2010

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Elektroniikan koulutusohjelma

KANTOLA, MARKUS	Etätyöpöytäyhteys käyttäen SSL VPN -tekniikkaa
VOUTILAINEN, TOMMI	
Opinnäytetyö	39 sivua + 7 liitesivua
Työn ohjaaja	Yliopettaja Martti Kettunen
Toimeksiantaja	Optimiratkaisut Oy
Toukokuu 2010	
Avainsanat	etätyöpöytäyhteys, SSL VPN, RDP, VPN, etäkäyttö, etähallinta, palomuurit, tietoturva

Etätyöpöytäyhteys voi helpottaa yrityksen toimintaa. Jos etähallinta halutaan toteuttaa julkisen verkon kautta, siihen vaaditaan tietoturvallinen yhteys, joka voidaan toteuttaa jollakin VPN-tekniikalla (Virtual Private Network). SSL VPN tarjoaa turvallisen yhteyden, joka ei tarvitse työasemaan erillistä ohjelmaa, sillä yhteys muodostetaan tunneloimalla yhteys selainrajapinnassa. Optimiratkaisut Oy halusi saada opinnäytetyön avulla selvityksen SSL VPN:n eri toteutusmahdollisuuksista löytääkseen hyvän ratkaisun omaan etähallintatoteutukseensa.

Opinnäytetyön tavoitteena oli rakentaa etätyöpöytäyhteys käyttäen eri SSL VPN –tekniikoita ja tutkia niiden ominaisuuksia. Tavoitteeksi asetettiin kahden erilaisen VPN-tuella varustetun laitteen käyttöönotto, konfiguroiminen, testaaminen ja testi-tulosten analysointi. Ensimmäisessä toteutetussa ratkaisussa käytettiin Ciscon 2811-sarjan reititintä ja toisessa Ciscon ASA 5505 -palomuurilaitetta.

Rakennetut SSL VPN –yhteydet ovat perusrakenteiltaan samanlaiset, mutta ASA 5505 -palomuurin ja sen yhteyden monipuolisempi hallinta aikaansaivat sen, että laboratoriotestien jälkeen päädyttiin suosittamaan ASA 5505 -palomuurilla toteutettua vaihtoehtoa. Palomuurilla pystytään ratkaisemaan yksittäisen käyttäjän porttiohjauslista. Reititin tarjoaa mahdollisuuden yhteen listaan, jonka kaikki sisään kirjautuneet näkevät. Palomuuri tarjoaa käyttäjäkohtaisen palvelun, jossa porttiohjauslistassa näkyy vain käyttäjän omat palvelut ja laitteiden IP–osoitteet.

Opinnäytetyössä toteutetut kytkennät ja suoritetut testaukset osoittavat, että etätyöpöytäyhteys voidaan toteuttaa eri tavoilla ja verkon rakenteelliset ratkaisut voivat vaikuttaa valintaan, mutta monipuolisempien ominaisuuksien vuoksi palomuurilaitteen valinta on järkevämpi ratkaisu.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Electronics

KANTOLA, MARKUS

VOUTILAINEN, TOMMI

Remote desktop using SSL VPN Technology

Bachelor's Thesis

39 pages + 7 pages of appendices

Supervisor

Kettunen Martti, Principal Lecturer

Commissioned by

Optimiratkaisut Oy

May 2010

Keywords

remote desktop connection, SSL VPN, RDP, VPN, remote login, remote system management, information security

A Remote Desktop connection can make a company's activities easier. Implementing remote management via a public network requires a secure connection, which can be realized using the VPN (virtual private network) technology. SSL VPN offers a secure connection that does not require a workstation to have a dedicated program for the tunnel. The web browser establishes the tunneled connection. Optimiratkaisut Oy wanted to obtain a report on the possible settings for the Secure Sockets Layer (SSL) virtual private network (VPN) implementation to find a good solution for their own remote access solutions.

The main aim of this work was to build a remote desktop connection using different SSL VPN technologies and examine their properties. Two VPN- supported devices were implemented, configured and tested. The test results were analyzed. One completed solution used a Cisco 2811 series router and the other solution used the Cisco ASA 5505 firewall.

The SSL VPN connections built were similar but built the ASA 5505 firewall connection was a better solution. The study concluded that the firewall solution was a better choice due to its more versatile connection management. A firewall can be used to solve an individual user's port forwarding list problem. The router offers the possibility of a single port forwarding list, which that all logged in users will see. The firewall offers a user based service whose the port forwarding list only shows the user's is displayed and has user's own services and equipment and their IP addresses.

The connections used in this study and the results of those connections indicated that remote desktop connections can be made in different ways. We feel the firewall solution is the best choice due to its more versatile features .

SISÄLLYS

KÄSITELUETTELO 6

1 JOHDANTO 8

2 SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORK 9

3.1 Internet Protocol security 10

3.2 Virtual Private Network -yhteydenotto 11

3.3 Virtual Private Network -tunnelointiprotokollat 12

3.4 Internet Protocol security -yhteyden toimintatavat ja sen käyttämät protokollat 13

4 SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORKIN OMINAISUUKSIA 15

5 SECURE SOCKET LAYER JA HYPERTEXT TRANSFER PROTOCOL SECURE 16

6 SYMMETRINEN SALAUS 16

6.1 Hash-based Message Authentication Code ja Hashing 18

6.2 Message Digest 19

6.3 Asymmetrinen salaus 19

8 REITITIN VERKKOLAITTEENA 20

8 PALOMUURI VERKKOLAITTEENA 20

9 REITITINPOHJAINEN RATKAISU 21

9.1 Reitittimen konfigurointi 22

9.2 Reitittimen Secure Socket Layer Virtual Private Network -konfiguraatio 23

9.3 Yhteydenotto reitittimen Secure Socket Layer Virtual Private Network -palveluun 24
9.4 Etäyhteyden muodostus 25

10 PALOMUURIPOHJAINEN RATKAISU 28
10.1 Palomuuripohjainen Secure Socket Layer Virtual Private Network -konfiguraatio 29
10.2 Yhteydenotto Secure Socket Layer Virtual Private Networkiin 34

11 WINDOWS-ETÄKÄYTTÖKONE 35

12 YHTEYKSIEN EROAVAISUUDET 37

13 LOPPUPÄÄTELMÄT 38

LÄHTEET 39

LIITTEET
Liite 1. Cisco 2811 -sarjan reitittimen loppukonfiguraatio 40
Liite 2. Ciscon ASA 5505 palomuurin loppukonfiguraatio 44

KÄSITELUETTELO

AH	Authenticating Headers, todennusprotokolla
ASA	Adaptive Security Appliance, Cisco-palomuuri
ASDM	Adaptive Security Device Manager, graafinen käyttöliittymä
CA	Certificate Authority, sertifikaattien jakaja
CHAP	Challenge Handshake Authentication Protocol, todennusprotokolla
Clientless VPN	epävirallinen nimi SSL VPN -konfiguraatiolle, palomuuri käyttää Clientless VPN -nimeä SSL VPN -konfiguraatiosta. Graafisessa käyttöliittymässä.
DoS	Denial of Service, palvelunesto
ESP	Encapsulating Security Payload, salausprotokolla
HMAC	Hash-based Message Authentication Code, todennusalgoritmi
HTTP	Hypertext Transfer Protocol, tiedonsiirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure, salattu tiedonsiirto-protokolla
IDS	Intrusion Detection System, havainnointipalvelu
IETF	Internet Engineering Task Force, Internet-verkon vapaaehtoiseen kehittämistyöhön osallistuvista henkilöistä muodostuva ryhmä
IKE	Internet Key Exchange, avaintenvaihtoprotokolla
IOS	Internetwork Operating System, käyttöjärjestelmä
IP	Internet Protocol
IPS	Intrusion Prevention System, tunkeutumisenestopalvelu
IPsec	Internet Protocol Security, protokolla sisältää salauksen, todennuksen ja varmentaa tiedon eheyttä
L2F	Layer 2 Forwarding, Ciscon tunnelointiprotokolla
L2TP	Layer 2 Tunneling Protocol, tunnelointiprotokolla

OSI-malli	Open Systems Interconnection Reference model, kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PGP	Pretty Good Privacy, tiedonsalausjärjestelmä
PPTP	Point-to-Point Tunneling Protocol, tunnelointiprotokolla
POP	Post Office Protocol, postiprotokolla
pre-shared keys	Ennalta jaetut avaimet
RDP	Remote Desktop, etätyöpöytäyhteys
RFC	Request for Comments, IETF-organisaation internet-standardi
RSA	epäsymmetrinen julkisen avaimen salausalgoritmi, nimi tulee kolmen kehittäjän sukunimien alkukirjaimista (Ron Rivest, Adi Shamir ja Len Adleman)
selfsigned certificate	itse allekirjoitettu sertifikaatti
SMTP	Simple Mail Transport Protocol, sähköposti-protokolla
SSH	Secure Shell, salausprotokolla
SSL	Secure Socket Layer, salausprotokolla
SSL VPN	Secure Socket Layer Virtual Private Network, VPN-yhteys, jossa käytetään SSL-salausprotokollaa
TCP	Transmission Control Protocol, tietoliikenne-protokolla
Telnet	yhteysprotokolla
TLS	Transport Layer Security, salausprotokolla
VPN	Virtual Private Network, tunneloitu yhteys
WebVPN	epävirallinen nimi SSL VPN -konfiguraatiolle, reititin käyttää WebVPN-nimeä SSL VPN -konfiguraatiosta

1 JOHDANTO

Etätyöpöytäyhteyksiä käytetään yrityksissä yleensä etähallintaan, tiedostojensiirtoon ja verkkoresurssien hallintaan. Jos etähallinta halutaan toteuttaa julkisen verkon kautta, siihen vaaditaan tietoturvallinen yhteys, joka voidaan toteuttaa jollakin VPN-tekniikalla (Virtual Private Network).

Optimiratkaisut Oy halusi saada opinnäytetyön avulla selvityksen SSL VPN:n eri toteutusmahdollisuuksista löytääkseen hyvän ratkaisun omaan etähallinta-toteutukseensa, jolla pääsisi turvallisesti käsiksi yhtiön tiedostoihin ja verkkoresursseihin.

Tavoitteena työssä oli rakentaa kahdella eri verkkolaitteella SSL VPN -yhteys. SSL VPN tarjoaa turvallisen yhteyden, joka ei tarvitse erillistä tunnelointi ohjelmaa, sillä yhteys muodostetaan tunneloimalla yhteys selainrajapinnassa. Optimiratkaisut Oy antoi tehtäväksi rakentaa ja tutkia SSL VPN -yhteyttä. Rakennetut mallit tehtiin Kymenlaakson ammattikorkeakoulun tietoliikennelaboratoriossa.

Reititinpohjainen ratkaisumalli rakennettiin käyttämällä Cisco 2811 -sarjan reititintä ja siihen konfiguroitiin komentorivipohjaisesti SSL VPN -yhteys. Palomuuripohjainen ratkaisumalli rakennettiin käyttämällä Cisco ASA 5505 -palomuuria, johon SSL VPN -konfiguraatio rakennettiin käyttämällä graafista käyttöliittymää.

Tietoturvan tarve on kasvussa jatkuvasti. SSL VPN tarjoaa erittäin helpon ja kevyen tavan tunneloida yhteys. Yhteyden tunnelointi hankaloittaa muiden pääsyä käsiksi arkaluonteisiin dokumentteihin. SSL VPN ei tarvitse erillisiä ohjelmia muodostaakseen yhteyttä, vaan yhteys muodostetaan selainrajapinnassa.

Tämän opinnäytetyön käytännön osiossa on tarkoitus luoda kaksi toimivaa ratkaisumallia etätyöpöytäyhteydestä käyttäen SSL VPN -tekniikkaa.

2 SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORK

SSL VPN on etäkäyttöteknologia, jonka käyttömäärät kasvavat nopeasti. Se tarjoaa turvallisen yhteyden yrityksen sisäiseen käyttöön käyttäen selainta tai määritettyä VPN-client-ohjelmaa. SSL VPN sijoittuu OSI mallissa kuljetuskerroksen ja sovelluskerroksen väliin. SSL-salausprotokolla kehitettiin Netscape-selaimeen mahdollistamaan sen toiminta sivuilla, jotka vaativat datan salauksen ja käyttäjän todennuksen. (Frahim & Huang 2008, 7.)

SSL VPN -yhteyden suurin vahvuus on se, että kehittynyt protokolla on jo valmiiksi saatavilla lähes jokaisessa selaimessa. SSL VPN -yhteyden ulkonäön voi muokata yrityksen tarpeisiin sopivaksi. Yhteys sisältää pääsyn yrityksen resursseihin, ilman että tarvitsee ladata VPN-ohjelmia. Se tarjoaa myös vahvan datan salassapidon käyttäen vähäisiä resursseja mutta joustavan tavan siirtää tietoa. Cisco on kehittänyt eri tapoja parantaakseen VPN-yhteyden toimivuutta. (Frahim & Huang 2008, 7-8.)

Clientless mode tarjoaa turvallisen pääsyn yrityksen resursseihin, kuten sisäverkkoon ja sähköpostipalvelimille, ilman että yhteys ruuhkauttaa sovelluksia tai ohjelmia. Thin client mode tarjoaa pääsyn useimpiin TCP-pohjaisiin protokolliin, kuten SMTP, POP, SSH, terminal- ja telnet-yhteyteen lataamalla Java-sovelluksen tietokoneelle. Full tunnel mode tarjoaa täydellisen pääsyn yrityksen resursseihin, ikään kuin olisit suoraan yhteydessä yrityksen sisäverkkoon. Tämä tapa vaatii lataamaan SSL VPN -ohjelman ennen kuin pääsy on sallittu. (Frahim & Huang 2008, 8.)

SSL VPN –tekniikan etuja on myös käyttöjärjestelmäohjaukset. SSL VPN ei ole riippuvainen tietystä käyttöjärjestelmästä, vaan jokaiselle käyttöjärjestelmälle on omat sovellukset. Ladattavat sovellukset ohjataan käyttöjärjestelmien mukaan. (Frahim & Huang 2008, 8.)

3 VIRTUAL PRIVATE NETWORK

Virtual Private Network eli VPN tarkoittaa joko laitteisto- tai ohjelmistototeutuksena tehtävää ratkaisua, jolla organisaation sisäverkko voidaan ulottaa turvallisesti turvattoman julkisen verkon, kuten Internetin, yli. VPN-tekniikkaa käytetään yhdistämään sisäverkkoja keskenään tai yksittäinen tietoliikennelaite, esimerkiksi etätyöntekijän työasema, organisaation verkkoon. VPN:ssä siirrettävän tiedon suojaamiseen käytetään salausta, joka estää julkisessa verkossa välitettävän liikenteen sisällön paljastumisen kolmansille osapuolille. Liikennöivät osapuolet myös todennetaan vahvasti ennen yhteyden muodostusta. Käytännössä VPN-yhteys muodostetaan tunneloimalla kaikki liikenne jonkin liikenteen salaavan protokollan sisään. Yleisesti käytössä olevia VPN-protokollia ovat IPSec, L2TP ja PPTP. (Viestintävirasto - VPN 2007.)

3.1 Internet Protocol security

IPsec VPN –yhteyksiä muodostetaan tekniikalla, jossa etätyöasemaan tarvitaan erityinen client-ohjelma. Tällainen perinteinen VPN-yhteysmalli on yleisesti käytössä yritysverkoissa. VPN voi käyttää OSI-mallista kerroksia 2, 3 ja 4. VPN käyttää tunnelointiprotokollia tarjotakseen lähettäjälle todennuksen ja viestin varmuuden sekä luotettavaa suojaa pakettien nuuskijoita vastaan. Tärkein VPN-yhteyden merkitys on turvallisuus, joka toteutetaan joko kapseloimalla data tai käyttäen sekä datan kapselointia että salausta. VPN-yhteystyypit jaetaan kahteen eri ryhmään: Site-to-Site IPsec VPN ja Remote Access VPN. (OpenVPN and the SSL VPN Revolution 2004, 8.)

Vuonna 1998 ilmestynyt IETF (Internet Engineering Task Force) tarjosi sarjan RFC-määrityksiä, jotka määrittävät protokollia, joita tarvitaan luotaessa VPN-yhteyttä. RFC 2401-2412 -protokollat ovat muodostuneet pohjaksi teknologialle, joka tunnetaan paremmin nimellä IPsec. IPsec perustuu joukkoon standardoituja protokollia ja sääntöjä, joiden avulla muodostetaan VPN-yhteys. IPsec luo turvallisen tunnelin käyttäen alussa kättelyprotokollaa, joka tunnetaan IKE handshake -toimintona. IKE varmentaa tunnelien päätepisteet, minkä jälkeen muodostuu pysyvä tunneli. Tämä tunneli käyttää symmetristä

salausta, ja tunnelissa kulkeva tieto salataan. (OpenVPN and the SSL VPN Revolution 2004, 8-9.)

IPsec luotiin komiteassa, jonka uskotaan lisänneen tarpeellisia toimintoja VPN-yhteyteen. Komiteaa kuitenkin arvosteltiin heikosta turvallisuudesta, minkä takia kehitettiin uusia salaustapoja. AES salaus julkistettiin turvallisuusstandardiksi kritiikin jälkeen. (OpenVPN and the SSL VPN Revolution 2004, 10.)

3.2 Virtual Private Network -yhteydenotto

VPN-yhteys syntyy muodostamalla yhteys yli julkisen verkon. IPsec VPN -tunnelia luotaessa käytetään symmetrisiä avaimia. Tunnelin molemmat päätepisteet jakavat tunnetut salaus- ja salauksenpurkuavaimet, joita tunneli käyttää salatakseen liikennettä.

Symmetrinen salaus on erittäin nopea ja siinä on käytössä on monta algoritmia. AES- ja 3DES-algoritmit ovat tämän hetken yleisimmät johtuen paremmasta turvallisuudesta. Symmetrisessä salauksessa on kaksi ongelmaa. Nämä ongelmat ovat julkisten avainten jako sekä varmistus siitä, että vaihdetaan avaimia halutun päätelaitteen kanssa. (OpenVPN and the SSL VPN Revolution 2004, 10.)

On olemassa useampi vaihtoehto, miten avaimia voidaan vaihtaa. Yksi vaihtoehto avainten vaihtoon on soittaa järjestelmänvalvojalle ja kysyä avainta. Toinen vaihtoehto on lähettää avain esimerkiksi sähköpostissa käyttäen PGP-tiedonsalausjärjestelmää vaihdon salaukseen. Kumpikaan aiemmin mainituista tavoista ei ole kuitenkaan tehokas. Yleisimmin käytetty vaihtoehto on kuitenkin pre-shared secret. Pre-shared secret ei ole kuitenkaan kovin skaalautuva verkoissa. (OpenVPN and the SSL VPN Revolution 2004, 10.)

Pohja hyvälle salaustekniikalle saadaan vaihtamalla salausavaimet usein. Salausavaimille on laskettu teoreettisia arvoja, kuinka kauan kestää, että ne saadaan auki. Avaimet tulisikin uusia aina, ennen kuin niiden teoreettinen murtoaika täyttyy.

Päästäkseen eroon hankalasta avaintenvaihto-tekniikasta VPN käyttää sertifikaatteja. Sertifikaatit käyttävät Public Key Cryptography -salaustekniikkaa. Tämä tarkoittaa sitä, että käyttäjä muodostaa julkisen ja yksityisen avainparin, jotka ovat matemaattisesti sidoksissa toisiinsa. Mikä tahansa julkisella avaimella salattu materiaali voidaan avata vain käyttäen yksityistä avainta ja toisinpäin. (OpenVPN and the SSL VPN Revolution 2004, 11.)

Jokaisella päätelaitteella on sen omat julkiset sekä yksityiset avainparit. Julkinen avain annetaan laitteen käyttäjälle, jotta hän voi salata siihen laitteeseen lähetettävät tiedot. Yksityistä avainta pidetään salassa ja sitä käytetään saapuvan viestin salauksen purkamiseen. Ongelmana on kuitenkin useiden yhteyksien avaimien säilytys. Usean käyttäjän VPN-yhteys vaatii, että jokaisen käyttäjän julkinen avain kopioidaan ja se pitää säilyttää. (OpenVPN and the SSL VPN Revolution 2004, 11.)

3.3 Virtual Private Network -tunnelointiprotokollat

CHAP-protokolla perustuu PPP-todennusprotokollaan. CHAP edustaa vanhempaa avaimenvaihtotekniikkaa. L2F-tunnelointiprotokolla perustuu vanhaan tekniikkaan, joka hyödyntää dial-up-tekniikkaa.

PPTP-tunnelointiprotokolla on tapa implementoida virtuaalisia yksityisiä verkkoja. PPTP on vanhentunutta tekniikkaa johtuen L2TP- ja IPsec- tunnelointiprotokollista. PPTP on Windows-käyttöjärjestelmissä ollut suosittu aina Windows 95 -käyttöjärjestelmästä asti, mikä johtuu PPTP:n helppokäyttöisyydestä. PPTP:n heikkouksia ovat heikko salaus, todennus sekä omien avainten hallinta. Istuntojen skaalautuvuus aiheuttaa myös rajoituksia serverissä. Hyödyt ovat laaja tuki Windows-käyttöjärjestelmissä sekä usean protokollan tuki. Etuina pidetään myös MPPE-salausta ja MPPC-pakkausta. (Tietoliikenteen suojaaminen 2003, 26.)

L2TP-tunnelointiprotokolla koostuu L2F-protokollan sekä PPTP-protokollan ominaisuuksista. L2TP hyödyntää L2F- ja PPTP-protokollan parhaita ominaisuuksia, joista on muodostettu L2TP-tunnelointiprotokolla. L2TP:stä on julkaistu päivitettyjä

versioita, joissa on parannettu yhteyden turvallisuutta ja yhteystyyppien yhteensopivuutta. L2TP toimii täysin itsenäisesti OSI-kerroksella kaksi. L2TP-tunnelointiprotokolla ei itsessään sisällä datan minkäänlaista salausta, mutta sen paketteja voidaan suojata käyttämällä apuna IPSec:n kuljetustilaa ja salausta. (Tietoliikenteen suojaaminen 2003, 27.)

IPsec-tunnelointi on melkein ideaali VPN-ratkaisu. IPsec tukee vahvaa todennusta ja salausta sekä yhdistäviä turvallisuusstandardeja. IPsec käyttää ESP- ja AH-protokollia suorittaakseen erinäisiä toimintoja. IKE ja IKEv2 suorittavat protokollaneuvotteluja, algoritmeja ja muodostavat salaus- sekä todennusavaimia. (Tietoliikenteen suojaaminen 2003, 27.)

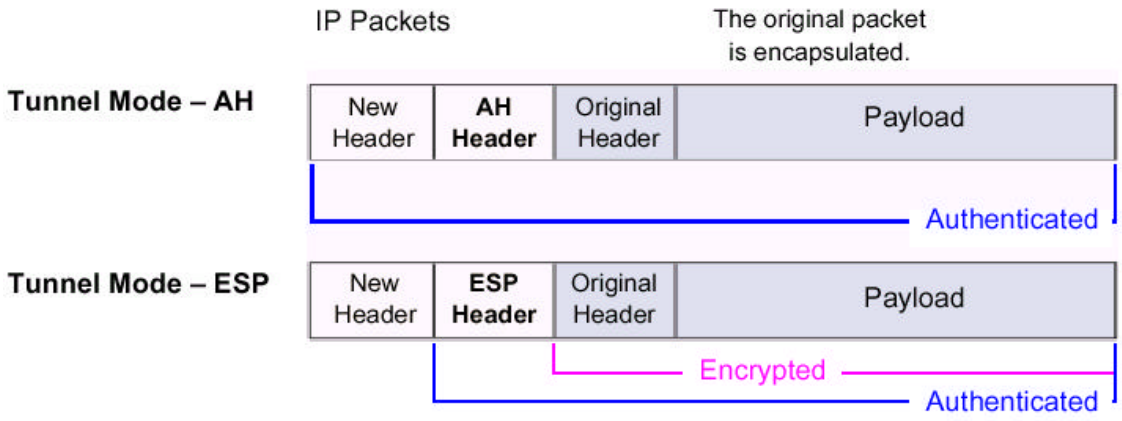
3.4 Internet Protocol security -yhteyden toimintatavat ja sen käyttämät protokollat

IPsec:llä on kaksi tapaa toimia, transport mode ja tunnel mode. Laite voidaan konfiguroida käyttämään joko transport- tai tunnel-siirtotapaa. Transport mode salaa tai todentaa IP-paketin datan. Tunnel mode salaa tai todentaa koko IP-paketin, sen datan sekä IP-otsikon. Paketti kapseloidaan uudeksi IP-paketiksi uudella IP-otsikolla. Ainoa etu Transport mode -tavan käytössä on se, että se kuluttaa hieman vähemmän prosessoritehoa. Suositeltavaa on ottaa aina Tunnel mode käyttöön. (A Cryptographic Evaluation of IPsec 1999, 6.)

IPsec käyttää tukenaan kahta protokollaa, AH ja ESP. AH tarjoaa todennuksen ja ESP tarjoaa todennuksen, salauksen tai molemmat. Protokollista AH todentaa datan ja paketin otsikon, kun taas ESP todentaa ja salaa datan. Käytettäessä transport mode -toimintoa AH tarjoaa vahvemman todennuksen kuin ESP. Tämä johtuu siitä, että AH todentaa myös IP-otsikon kentät. Käytettäessä Transport mode -toimintoa olisi järkevintä käyttää kumpaakin AH- ja ESP -protokollaa. Käytettäessä Tunnel mode -toimintoa ESP tarjoaa samantasoisen todennuksen kuin AH-protokolla. Alkuperäinen IP-osoite sisältyy hyötykuormaan tunnel mode -paketeissa. Koska ESP- ja AH-protokollissa ei ole suurta

eroa niiden toimiessa tunnel mode -siirtotapana, suositaan ESP-protokollan käyttöä. (A Cryptographic Evaluation of IPsec 1999, 6-9.)

ESP-protokolla sallii hyötykuorman salauksen ilman todennusta, mutta yleensä silloin on laitettu AH-protokolla todentamaan tiedon. ESP-protokollan tulisi aina hoitaa todennus, koska salauksen voi hoitaa vain ESP-protokolla. ESP-protokollan salaus on valittavissa, halutaanko salaus ottaa käyttöön vai ei. Yleisin virhe on konfiguroida ESP-protokolla vain salaamaan. ESP-protokollan tulisi aina todentaa sekä salata tieto. (A Cryptographic Evaluation of IPsec 1999, 8.)



Kuva 1. AH- ja ESP-protokollien erot (Tietoliikenteen suojaaminen 2003, 14)

4 SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORKIN OMINAISUUKSIA

SSL VPN eroaa normaalista VPN-tekniikasta usealla tavalla. SSL VPN käyttää hyödykseen SSL-protokollaa ja on yhdistettävissä selaimella kirjoittamalla *https* selaimen osoiterivin alkuun. Yhteys muodostetaan käyttämällä selainta, mikä tarjoaa turvallisen yhteyden eikä ole riippuvainen fyysisestä sijainnista. SSL VPN –yhteyden voi muodostaa joka puolelta maailmaa, mikäli pääsyä ei ole rajoitettu. SSL VPN tarjoaa etäkäyttömahdollisuuden ja pääsyn sisäisen verkon palveluihin. SSL VPN ei tarvitse erillisiä ohjelmia muodostaakseen VPN-yhteyttä. SSL VPN on tämän takia saanut lisänimikseen ”clientless VPN” ja ”WebVPN.”

SSL VPN tarjoaa pääsyn yrityksen käyttämiin ohjelmiin ja jaettuihin tiedostoihin vain käyttämällä tietokoneen selainta. SSL VPN tarjoaa myös monipuolisen, helppokäyttöisen ja turvallisen etäkäyttömahdollisuuden. SSL VPN käyttää porttia 443. Tämä portti on normaalisti auki jokaisessa yritysverkossa, joten kyseiselle palvelulle ei tarvitse avata uutta porttia liikenteeseen. SSL VPN -salaus perustuu joko SSL-protokollaan tai TLS-protokollaan. SSL- tai TLS-pohjainen VPN kykenee samanlaiseen yhteyteen kun IPsec VPN. RSA-kättely toimii samalla tavalla, kuin IPsec käyttää sen IKE-neuvotteluissa. SSL-salauskirjastoa käytetään tämän jälkeen symmetrisen tunnelin luomiseen. IPsec käyttää hyvin samankaltaista tekniikkaa suojellakseen tunnelia.

SSL VPN -yhteyksiä voidaan rakentaa kahdella tavalla. SSL VPN -portaalirakennelmassa otetaan yhteys yhteen sivuun, josta voi ottaa yhteyden moneen verkkoon. Tässä tapauksessa yhteys on kuin ovi: avaat oven, joka tarjoaa mahdollisuuden mennä moneen suuntaan. Tunnelointi vaatii kuitenkin selaimelta sen, että se kykenee käyttämään aktiivista sisältöä. Tämä sallii yhteyden tarjoamien toimintojen käytön. Esimerkkejä aktiivista sisältöä tarjoavista ohjelmista ovat Java, JavaScript, Active X ja Flash-sovellukset. Selain voi omistaa myös rakennetun lisäosan, joka tarjoaa tuen yhteydelle.

5 SECURE SOCKET LAYER JA HYPERTEXT TRANSFER PROTOCOL SECURE

SSL on salausprotokolla, joka on ilmestynyt jo 1990-luvun alussa. Se ei ole sidottu vain selaimeen, vaan se voi salata myös muita protokollia. HTTPS on HTTP -protokollan salaukseen kykenevä versio. HTTPS käyttää hyödykseen SSL-salausta. HTTPS-yhteyttä käytetään tiedon suojattuun siirtoon tietoliikenneverkossa. SSL-salausta käytettäessä yhteys kysyy varmenteen, joka tulee hyväksyä tai ladata. SSL-yhteys salaa tiedon ennen lähetystä. HTTP-protokolla käyttää porttia 80 ja HTTPS porttia 443. TLS on uudempi versio SSL-salauksesta. (OpenVPN and the SSL VPN Revolution 2004, 12)

TLS-protokollan ensisijainen tehtävä on tarjota salausta ja tiedon yhtenäisyyttä kahden osapuolen välillä. Symmetristä salausta käytetään yhteyden muodostuksessa. Symmetriset avaimet muodostetaan jokaiselle yhteydelle erikseen, joten yhteys on myös luotettava. TLS-yhteyttä käytetään ylempien kerrosten protokollien kapseloinnissa. SSL-versiota 3.0 käytettiin TLS-protokollan pohjana, kun protokollaa alettiin kehittää. Erot ovat todella pienet verrattessa kyseisiä protokollia. TLS ja SSL eivät ole kuitenkaan keskenään yhteensopivia, vaan yhteydenmuodostus vaatii joko TLS- tai SSL-salausprotokollan. (OpenVPN and the SSL VPN Revolution 2004, 12)

6 SYMMETRINEN SALAUS

Symmetrisissä salausalgoritmeissa viesti salataan ja salaus puretaan samalla avaimella. Symmetriset salausalgoritmit jaetaan jono- ja lohkosalausmenetelmiin. Symmetristen salausmenetelmien suurin etu on salausmenetelmän nopeus. Symmetristä salausta varten rakennetut laitetoteutukset pääsevät satojen megatavujen nopeuteen sekunnissa. (Viestintävirasto - Symmetrinen salaus 2007.)

Symmetrisen salauksen ongelma on avainten hallinta, sillä sekä viestin lähettäjällä että vastaanottajalla tulee olla tiedossaan sama salausavain. Yleisimmin tämä tunnetaan nimellä pre-shared keys. Avaimen välittämiseen osapuolten välillä tarvitaan aina jokin turvallinen lisämenetelmä. (Viestintävirasto - Symmetrinen salaus 2007.)

Symmetrisistä salausalgoritmeista tunnetuin on edelleen laajasti käytetty DES. DES-algoritmia ei pidetä enää riittävän turvallisena kaikkiin käyttötarkoituksiin, joten sen seuraajaksi onkin valittu AES. AES:n salausalgoritmina käytetään Rijndaelia, joka on lohkosalaukseen perustuva symmetrinen salausalgoritmi. AES:n avainpituudet ovat 128, 192 ja 256 bittiä. On myös muita käytössä olevia symmetrisiä algoritmeja, esimerkiksi 3DES,IDEA, RC4 ja CAST. Symmetrisistä salauksista kannattaa käyttää AES-algoritmia, sillä se on nopea ja turvallisin. (Viestintävirasto - Symmetrinen salaus 2007.)

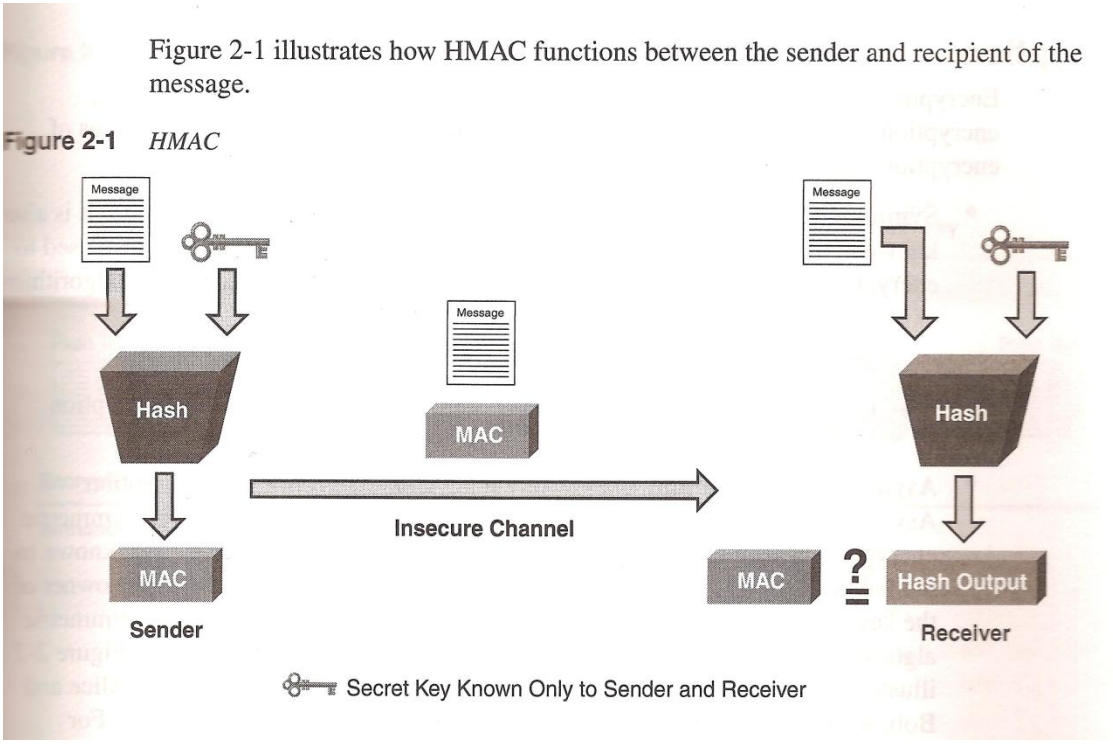
Algoritmi	Turvataso	Työtaso
DES, MD5	Todella heikko	2^{40}
RC4, SHA-1	Heikko	2^{64}
3DES	Heikohko	2^{80}
AES-128, SHA-256, Blowfish	Perusturva	2^{128}
AES-192, SHA-384	Korkea	2^{192}
AES-256, SHA-512	Erittäin korkea	2^{256}

Kuva 2. Avainten turvatasoesimerkkejä

6.1 Hash-based Message Authentication Code ja Hashing

Kun salausavaimet on vaihdettu ja käytetään symmetristä algoritmia tunnelin muodostamiseen, voidaan aloittaa datan lähetys. Tiedon oikeellisuuden varmistukseen käytetään hash-sekoitusta. Siinä viestin teksti ajetaan yhden suunnan funktion läpi, joka muodostaa määrätyn mittaisen jonon. 128-bittisen jonon tekee MD5 ja 160-bittisen SHA1. Tämän jälkeen data lähetetään salakirjoitetun tekstin ollessa liitettynä viestin perään. Kun viesti on vastaanotettu toisessa päässä, vastaanottaja ajaa viestin läpi käyttäen samaa funktiota ja vertaa tuloksia. Mikäli jono on samanlainen kuin lähtiessä, vastaanottaja varmistuu viestistä. (OpenVPN and the SSL VPN Revolution 2004, 25.) (Kuva 3.)

HMAC-avain liitetään datan eteen ennen sen ajamista funktion läpi. Tämän jälkeen avain menee sekaisin datan kanssa. Mikäli tämä avain on datan edessä sen tullessa vastaanottajalle, on data oikein. (OpenVPN and the SSL VPN Revolution 2004, 25.) (Kuva 3.)



Kuva 3. HMAC-toimintoja (Frahim & Huang 2008, 19.)

6.2 Message Digest

Message Digest on peruuttamaton matemaattinen funktio, joka ottaa viestin riippumatta sen koosta ja koodaa viestin uudelleen. Jokaisella viestillä on vain yksi avain, joten kahdelle viestille ei ikinä pitäisi luoda samaa avainta. Yhden kirjaimen muutos lähetettävässä viestissä tarkoittaa sitä, että koko viesti koodataan uudelleen ja sillä on eri avain. Ennen viestin lähetystä se käytetään Message Digest -funktion läpi. Vastaanottajalla tulee olla sama Message Digest -funktio. Vastaanottaja voi näin tarkastaa, onko viesti muuttunut lähetyksen jälkeen. Avaimen lisäys Message Digest -toimintoon on mahdollista, jotta saavutettaisiin parempi tietosuoja. (OpenVPN and the SSL VPN Revolution 2004, 6.)

6.3 Asymmetrinen salaus

Asymmetrisessä salauksessa käytetään avainparia, joista toinen avain on julkinen ja toinen yksityinen. Avaimet ovat vaihtokelpoisia siten, että julkisella avaimella salattu viesti voidaan avata kyseessä olevan avainparin yksityisellä avaimella ja päinvastoin. (Viestintävirasto - Epäsymmetrinen salaus 2007.)

Asymmetrisen salauksen suurin etu symmetriseen salausalgoritmiin verrattuna on avaintenhallinnan yksinkertaisuus. Julkisen avaimen algoritmien heikkoutena pidetään salauksen hitautta sekä avaimen pituutta verrattuna yksityisen avaimen algoritmiin. (Viestintävirasto - Epäsymmetrinen salaus 2007.)

Asymmetrisen salauksen kehittivät Whitfield Diffie ja Martin Hellman. Suosituin asymmetrinen salausalgoritmi on RSA. Sen vahvuus perustuu suurten lukujen tekijöiden jakamisen vaikeuteen. Muita asymmetrisia salausalgoritmeja ovat esimerkiksi DIffie-Hellman ja ElGamal. (Viestintävirasto - Epäsymmetrinen salaus 2007.)

8 REITITIN VERKKOLAITTEENA

Reitittimen pääasiallinen tehtävä tietoverkossa on hoitaa pakettien reititys. Reititin voidaan konfiguroida käyttämään staattista reititystä, jossa verkon ylläpitäjä itse määrittää reitittimeen reitit seuraaviin verkkolaitteisiin. Reititin voidaan määrätä käyttämään erilaisia reititysprotokollia, joilla saman organisaation reitittimet mainostavat toisilleen tuntemiaan reittejä eri osiin verkkoa.

Reititin ohjaa paketin sille reitille, jolla on paras metric-arvo yhteydelle. Reititin pitää yllä reititystaulua ja lisää siihen omissa liitäntäporteissaan olevat verkot. Reitittimellä voi olla useita reittejä yhteen reitittimeen ja niistä osa menee monen muun reitittimen kautta. Reititystaulu voi näyttää vain yhden eli parhaan reitin, ja sitä reititin käyttää, koska paketti menee perille nopeimmin sitä kautta. Staattinen reitti on aina ensisijainen reitti johtuen linkin cost-arvosta. Cost-arvo voidaan muuttaa, mutta staattisen reitin oletusarvo on niin pieni, että se tulee käyttöön.

Reitittimellä on muitakin ominaisuuksia, mutta pääasiassa reititintä käytetään vain reititykseen. Reititin toimii yleensä organisaation sisäverkon reunalla, jossa se ohjaa esimerkiksi IP VRF -toiminnoilla verkkoa tai hoitaa verkon VLAN-reititystä. Reititin hoitaa yleensä VLAN-reitityksen, ellei sisäverkosta löydy multilayer-kytkintä. Multilayer-kytkinten kallis hinta aiheuttaa vielä sen, että reititintä käytetään VLAN-reitityksessä.

8 PALOMUURI VERKKOLAITTEENA

Palomuurit ovat joko ohjelmistolla tai laitteistolla toteutettuja järjestelmiä, jotka valvovat tietoliikennettä verkkojen välillä. Palomuureja käytetään suojelemaan sisäverkkoa ulkoverkosta tulevilta hyökkäyksiltä sekä rajoittamaan liikennettä eri sisäverkkoavaruuksien välillä. Perusedellytykset toiminnalle ovat, että kaikki verkkoliikenne kulkee sen läpi ja että palomuuri päästää lävitseen vain halutunkaltaisen verkkoliikenteen. (Viestintävirasto - Palomuuri 2007.)

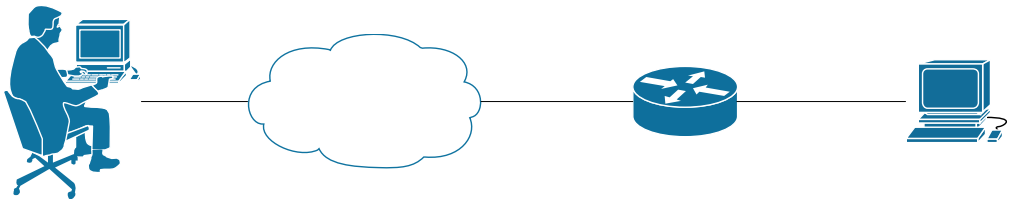
Palomuuri tarjoaa mahdollisuuden verkkoliikenteen seuraamiseen, koska kaikki verkkoliikenne kulkee palomuurin läpi. Esimerkiksi tapahtumalokeja ja hälytystoimintoja voidaan toteuttaa palomuurin yhteyteen. Palomuuri voi myös toimia verkkopalveluiden alustana. Näitä ovat esimerkiksi NAT, VPN ja IDS. (Viestintävirasto - Palomuuri 2007.)

Palomuurikin on haavoittuva, sillä hyökkääjä voi käyttää hyväkseen palomuurin sallimia palveluita, esimerkiksi www-palvelimien tietoturva-aukkoja. Palomuuri voidaan myös ohittaa tai kiertää. Palomuuri ei myöskään puutu liikenteen sisältöön eli se ei estä haittaohjelmien siirtymistä ulkoverkosta sisäverkkoon tai toisinpäin. (Viestintävirasto - Palomuuri 2007.)

9 REITITINPOHJAINEN RATKAISU

Saimme aiheen reititinpohjaisen SSL VPN:n suunnitteluun jo erikoistyökurssilla. Silloin teimme Kymenlaakson ammattikorkeakoulun tietoliikennelaboratoriossa yhden version SSL VPN -yhteydestä sekä sen etäkäytöstä.

Tämä reititinpohjainen työ tehtiin Ciscon 2811 -sarjan reitittimellä ja komentorivipohjaisella konfiguraatiolla. Tarkoituksena oli luoda turvallinen etätyöpöytäyhteys käyttäen SSL VPN -yhteyttä. (Kuva 4.)



Kuva 4. Kuvassa nähdään yksinkertaistettu malli siitä, miten rakennettiin SSL VPN -yhteys.

Tietokoneessa tarvitaan Internet-selain ja Java-sovellus. Yhteys perustuu etäkäyttäjän ottamaan yhteyteen, jossa otetaan selaimella yhteys reitittimen julkisen verkon porttiin. Yhteydenotto alkaa IKE-kättelyllä käyttäjän ja reitittimen välillä. Kättely tapahtuu vaihta-

malla sertifikaatteja, jolloin kerrotaan oma public key -avain. Vaihtamalla public key -avaimia ja varmentamalla oma private key -avain kättelyssä muodostuu varmennettu yhteys, minkä jälkeen voi kirjautua sisään palveluun. Kirjautumisen jälkeen on mahdollista avata porttiohjaukset ja niiden kautta etäkäyttöyhteys.

9.1 Reitittimen konfigurointi

Konfiguraatio aloitettiin IP-osoitteiden valinnalla. Reititin oli eri verkossa kuin testauksessa käytetyt etäkäyttökoneet. Jotta SSL VPN -ominaisuus saatiin toimimaan, reitittimeen oli asennettava uusi, testausvaiheessa oleva käyttöjärjestelmä eli IOS-image.

IOS-image käynnistettiin seuraavasti:

Router(config)#boot system flash flash:/imagen nimi.bin

Käsky oli tarpeellinen, koska mikään aiempi versio Cisco 2811 -reitittimistä ei tukenut SSL VPN -yhteyttä. Testiversio oli ensimmäinen versio kyseiselle reitittimelle, jossa oli SSL VPN -tuki.

Seuraavaksi määriteltiin liityntäporttien IP-osoitteet sekä luotiin oletusreitti, joka osoitti oman verkon gateway-osoitetta. Etäkäyttökoneisiin laitettiin staattiset osoitteet, minkä jälkeen testattiin, että yhteydellä pääsee julkiseen verkkoon. Yhteys tuli varmistaa, jotta saataisiin yhteys julkisesta verkosta varmasti myös etäkäyttökoneisiin. IP-osoitteiden määrittämisen jälkeen määritettiin käyttäjänimi ja salasana.

Seuraavassa vaiheessa siirryttiin luomaan http server -sääntöä, johon määritettiin käyttäjät ja se, että palvelu käyttää local aaa –listaa. Luotiin käyttäjätunnukset ja salasanat suoraan reitittimen käyttäjälistaan. Käskyt annettiin seuraavalla tavalla, jotta käyttäjälistat tulivat voimaan. (Liite 1.)

Router(config)#ip http server

Router(config)#ip http secure-server
Router(config)#ip http authentication local
Router(config)#aaa new-model
Router(config)#aaa authentication login listannimi local

9.2 Reitittimen Secure Socket Layer Virtual Private Network -konfiguraatio

Aloitettiin määrittämällä nimet ja osoitteet. Määritetty gateway on selaimella muodostettavan yhteyden IP-osoite. (Liite 1.)

Router(config)#webvpn gateway ”nimi"
Router(config-webvpn-gateway)#ip address 10.10.10.10
Router(Config)#webvpn context ”nimi2”

Router(config-webvpn-context)#port-forward "listan_nimi"
Router(config-webvpn-port-fwd)#local-port 10000 remote-server "etäkäyttökoneen IP -osoite" remote-port 3389 description "Esimerkki porttiohjaus"

Yllä on esimerkki porttiohjauksesta. Portti 3389 on Windowsin etätyöpöytäyhteyden portti, joka on oletusarvo. Local port kertoo ohjauksesta, mihin IP-osoitteeseen se ohjataan yhteyttä otettaessa. (Liite 1.)

Router(config-webvpn-context)#policy group “nimi3”
Router(config-webvpn-group)#port-forward "listan_nimi" auto-download

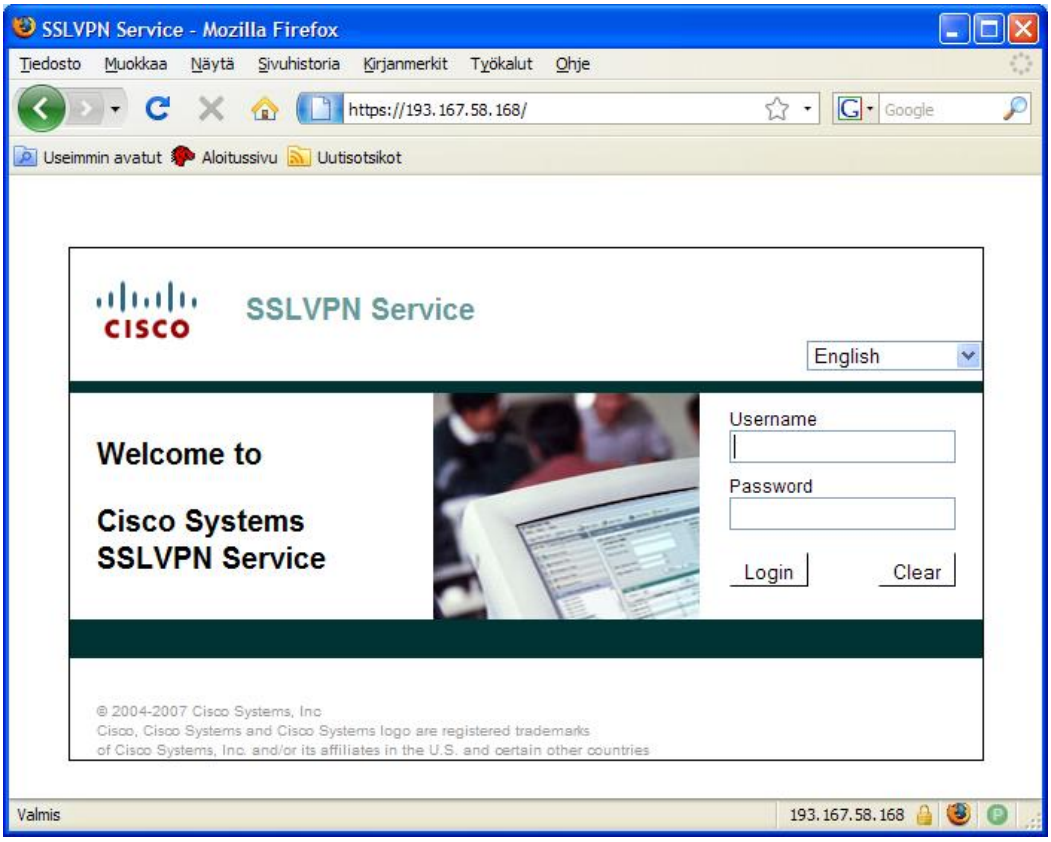
Käskyssä käytettiin aiemmin määritettyä port-forward listaa. Käsky annetaan group policy -säännön sisällä, jossa käskyllä määritettiin porttiohjauslista, jota yhteydessä käytettiin. Port-forwarding -listoja voi olla useita, mutta ainakaan käytetyssä testiversiossa ei ollut tukea useamman port-forwarding -listan käyttöön. Auto-download -lisämääre ei ole välttämätön, mutta käskyllä saatiin automaattisesti ladattua Java-sovellus, joka ohjasi porttiohjausta. (Liite 1.)

Router(Config)#webvpn context ”nimi2”
Router(config-webvpn-context)#default-group-policy nimi3
Router(config-webvpn-context)#aaa authentication list listannimi
Router(config-webvpn-context)# gateway “nimi” (webvpn gatewayn nimi, aiemmin määritelty)

Käskyt olivat säännöstö SSL VPN -yhteydelle, kokoelma aiemmin kasatuista säännöstöistä, jotka otettiin lopulta käyttöön. Kohdassa kasattiin aiemmat käskyt yhdeksi toimivaksi kokonaisuudeksi. Käskyillä määritettiin, mitä käytäntöä käytettiin. Käyttäjän todennus hoidettiin esimerkissä aaa local -todennuksen avulla, eli käyttäjät kirjautuivat itse määritettyjen käyttäjien pohjalta. Tartunta-IP-osoite oli määritetty aiemman gateway-säännön kautta; käskyllä otettiin tartuntapisteen määritykset voimaan. (Liite 1.)

9.3 Yhteydenotto reitittimen Secure Socket Layer Virtual Private Network -palveluun

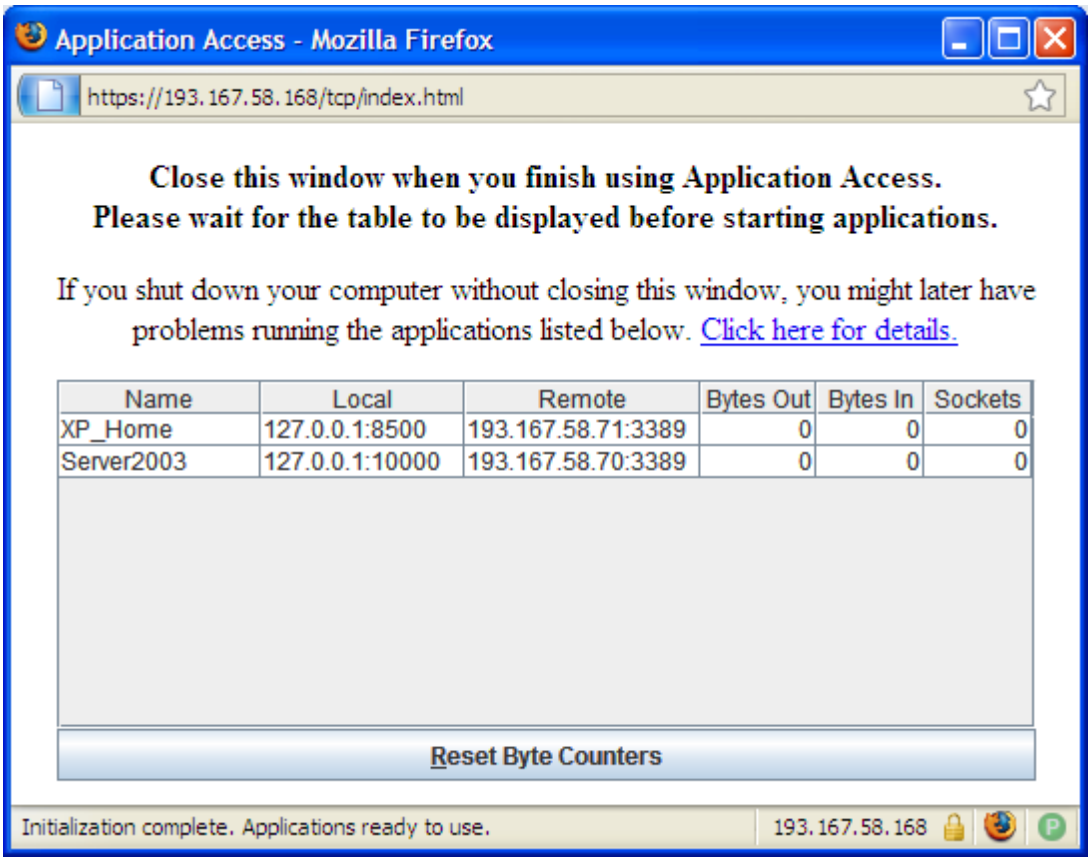
Yhteys aloitettiin ottamalla yhteyttä reitittimen IP-osoitteeseen, joka määritettiin konfiguraatiossa SSL VPN -yhteyden tartuntapisteeksi käyttämällä selaimen osoiteriviä. Selaimesta riippuen yhteys aloitettiin lataamalla varmenne. Kirjauduttaessa palveluun kysyttiin käyttäjätunnus ja salasana. Sertifikaattien hyväksynnän jälkeen aukesi selainpohjainen yhteys. Mikäli Java-sovellusikkuna ei auennut, täytyi painaa thin client -kohdan alla olevaa start-nappulaa, jotta porttien ohjaus alkoi toimia. Ilman Java-sovellusikkunaa ei voitu muodostaa RDP SSL VPN -yhteyttä. Yhteydenotto aloitettiin muodostamalla yhteys Internetin yli reitittimeen, johon SSL VPN -konfiguraatio on rakennettu. (Kuva 5.)



Kuva 5. Reitittimen oletuksena oleva kirjautumisikkuna. Kirjautumissivua voidaan muokata yrityksen tarpeiden mukaan.

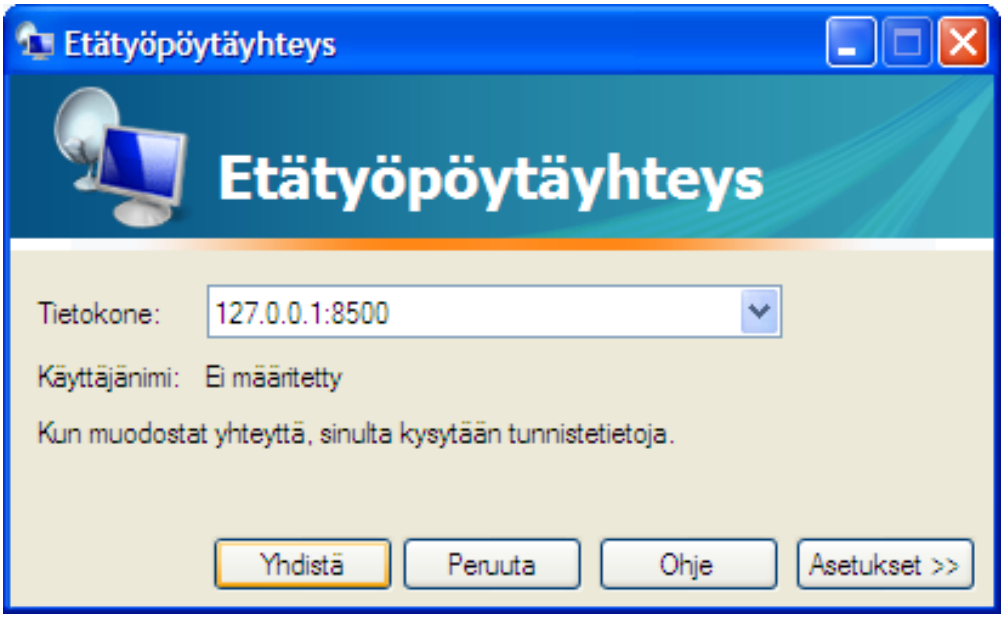
9.4 Etäyhteyden muodostus

Yhteys muodostetaan selaimella osoiterivin kautta, ja heti aluksi tuli hyväksyä sertifikaatti, joka oli luotu reitittimeen selfsigned-tyyppisenä sertifikaattina. Reitittimeen oli määritetty käyttäjätunnukset sekä salasanat, joita käytettiin kirjauduttaessa SSL VPN -palveluun. Kirjautumisen jälkeen Java-sovellusikkuna esitti port-forwarding -listan mahdollisuudet, joita muodostettu yhteys tarjosi. Port-forwarding -konfiguraatio määritti, mitä ohjelmia käytettiin ja millä porteilla ohjelmia voitiin avata.



Kuva 6. Porttiohjauslista, josta nähdään sidotut IP-osoiteparit. Ellei kuvassa oleva sovellus ole auki yhteyden aikana, eivät porttiohjaukset toimi.

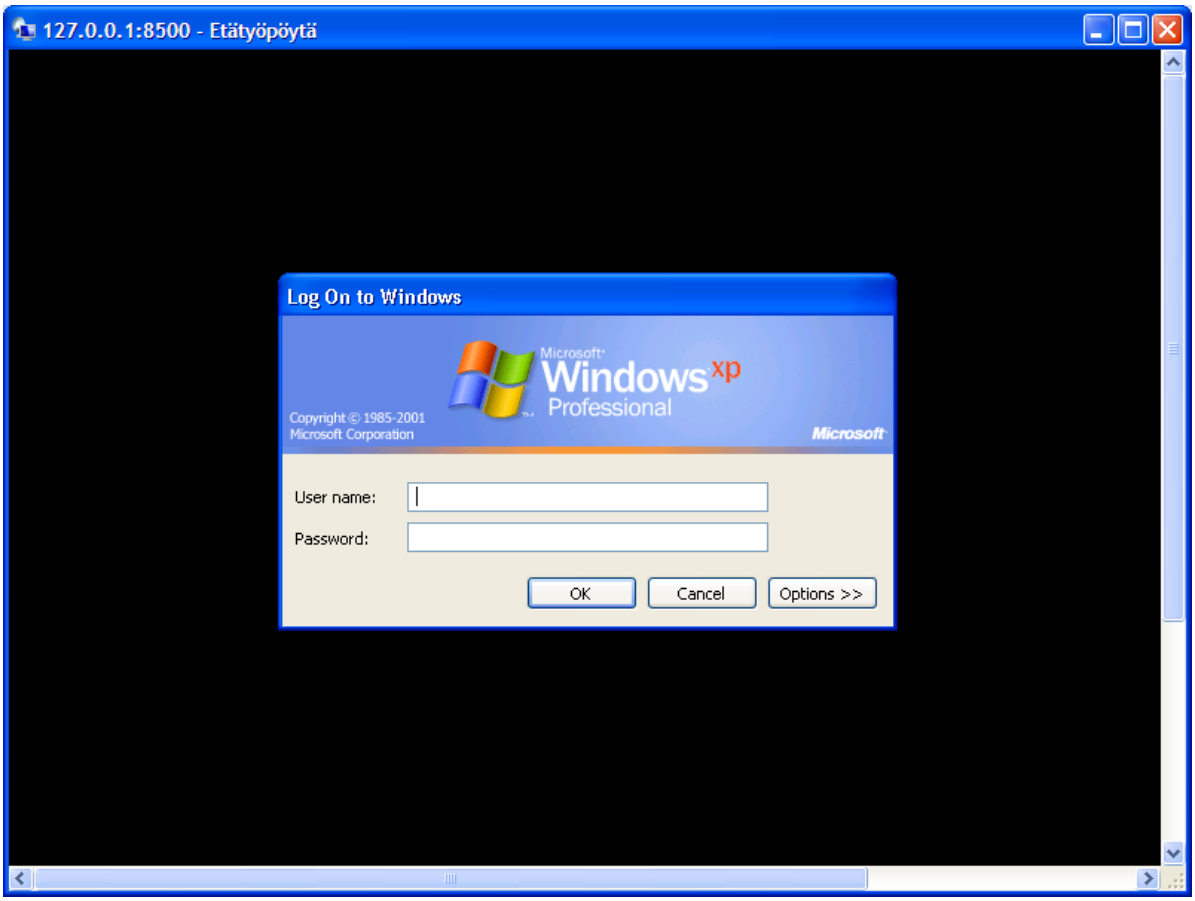
Java-sovellusikkunan tuli olla auki, mikäli haluttiin muodostaa RDP SSL VPN -yhteys. Kuvasta 6 nähdään käytetyt ohjaukset eli mitä porttia käytettiin, ja tässä tapauksessa se oli Windowsin etäkäyttöportti 3389. Sovelluksen auettua mentiin Windows-käyttöjärjestelmän Käynnistä-valikkoon. Valikosta valittiin ohjelmat, apuohjelmat, minkä jälkeen listassa näkyy etätyöpöytäyhteys. Kyseiseen ohjelmaan syötetään osoite ja portti, mihin halutaan ottaa yhteys.



Kuva 7. Yhteydenottoesimerkki, miten otetaan yhteyttä serveriin.

Yhteys otetaan aina osoitteella 127.0.0.1, porttinumero on ainoa, joka vaihtuu. Porttinumero määrää, mihin osoitteeseen otetaan yhteyttä. Kuvasta 7 näkyy esimerkki, miten portti sidottiin osoitteeseen, minkä jälkeen yhteys muodostui 193.167.58.71-osoitteeseen.

Käyttäjätunnus ja salasana kysyttiin, ennen kuin etätyöpöytäyhteys saatiin luotua. Kun yhteys oli muodostettu, tuli koko näytön kokoinen sovellus etäkoneen työpöydästä. Vasemmassa yläkulmasta nähtiin osoite, johon oli otettu yhteys, minkä jälkeen tuli sisään kirjautuminen. Sisään kirjauduttaessa tuli muistaa, että kirjauduttavaan koneeseen tuli laittaa käyttäjänimet ja salasanat, ketkä saivat kirjautua palveluun (Kuva 8).



Kuva 8. Kirjautuminen etätyöpöytäyhteyskoneelle.

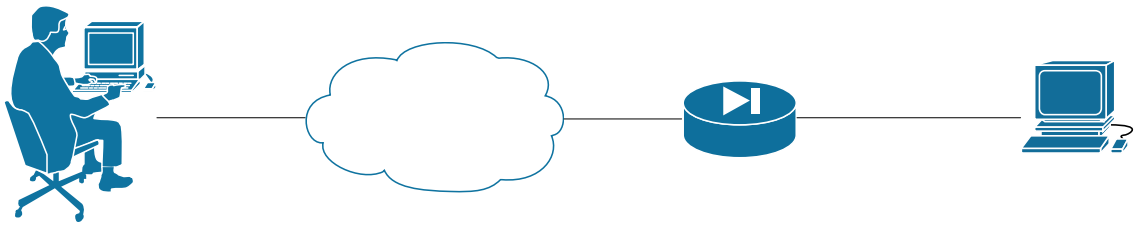
10 PALOMUURIPOHJAINEN RATKAISU

Opinnäytetyön tavoitteena oli testata myös palomuuriin perustuva ratkaisumalli turvallisesta etätyöpöytäyhteydestä.

Palomuuriin määritykset tehtiin graafisella käyttöliittymällä eli käyttämällä ASDM-yhteyttä. Yhteyden muodostaminen vaatii tietokoneelta selaimen ja Java-sovelluksen.

ASDM-yhteys on graafisen käyttöliittymän yhteys, joka on tarkoitettu palomuurin konfigurointiin. Graafinen käyttöliittymä on epävakaa tietyissä tapauksissa: koska yhteys käyttää porttia 443, muutokset kyseiseen porttiin katkaisevat ASDM-yhteyden. ASDM-yhteys on tarkka tehdystä konfiguraatiosta ja korruptoituu helposti. ASDM-yhteys rajaa muutok-

sien määrän. Komentorivillä voi tehdä tarkemman konfiguraation kuin ASDM-yhteydellä. ASDM-yhteys tarjoaa kuitenkin helpommin hallittavan kokonaisuuden kuin komentorivipohjainen yhteys.

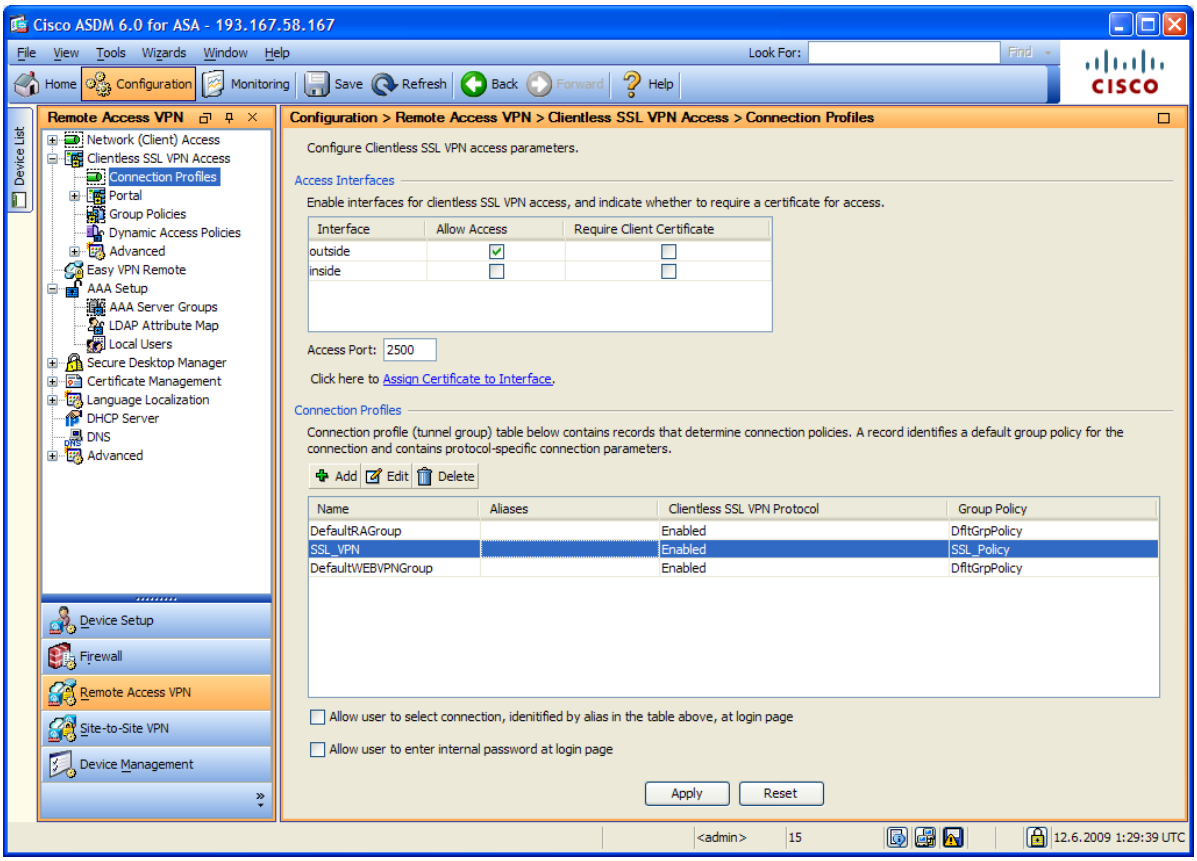


Kuva 9. Yksinkertaistettu malli palomuuripohjaisesta konfiguraatiosta

10.1 Palomuuripohjainen Secure Socket Layer Virtual Private Network -konfiguraatio

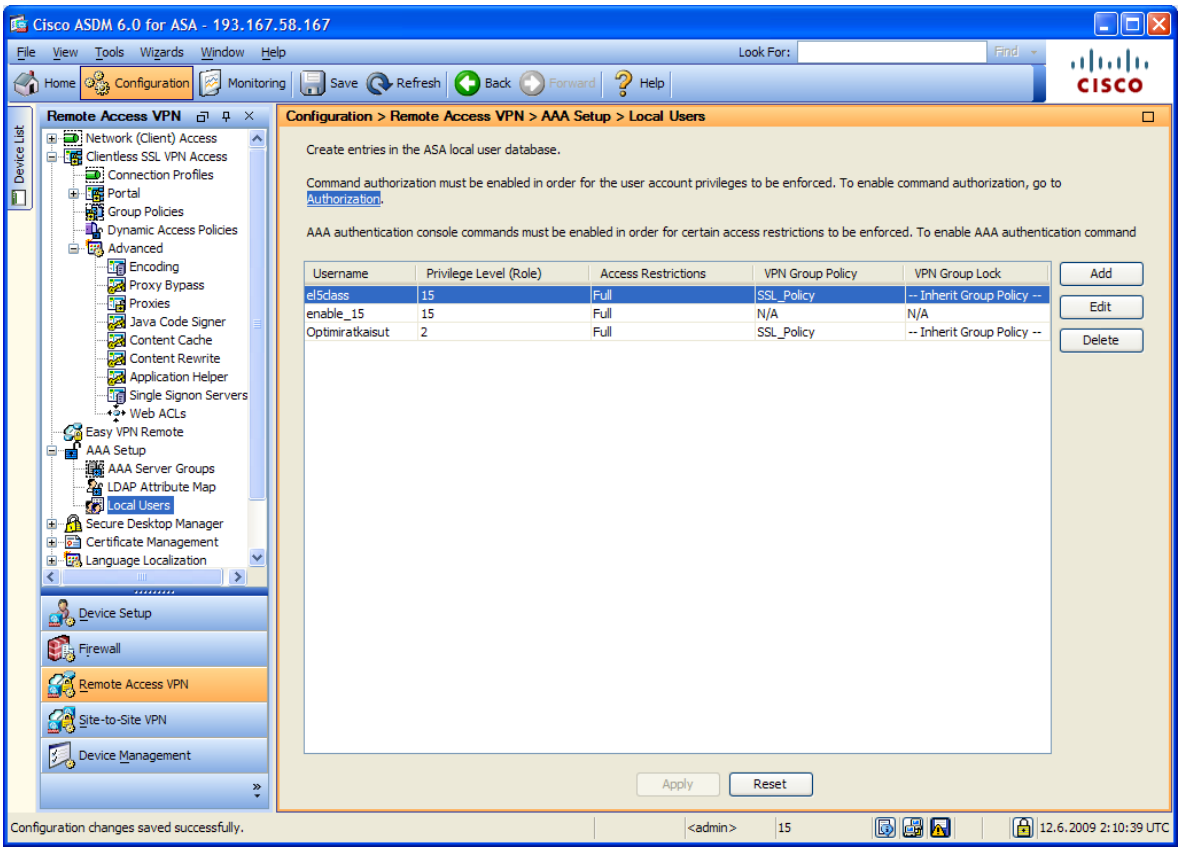
Yhteys muodostettiin julkisen verkon yli koulun laboratoriossa sijainneeseen ASA 5505 -palomuuriin. ASA-palomuurin konfiguraatio tehtiin ASDM-yhteydellä. SSL VPN käyttää porttia 443 oletusarvona, eli samaa porttia kuin ASDM-yhteys. Tämän takia SSL VPN -yhteyden portti määritettiin portiksi 2500. (Liite 2.)

Palomuurin konfiguraatio tehtiin julkisen verkon yli, joten alun konfiguraatio tehtiin komentorivillä. Konfiguraatio aloitettiin käyttämällä Putty-nimistä ohjelmaa, jolla otettiin yhteys koulun verkkoon, minkä jälkeen otettiin yhteys palomuuriin. Komentorivillä tehdyt muutokset liittyivät ainoastaan IP-osoitealueisiin, jotka saivat ottaa ASDM-yhteyden.



Kuva 10. Osa ASDM-konfiguraatiosta.

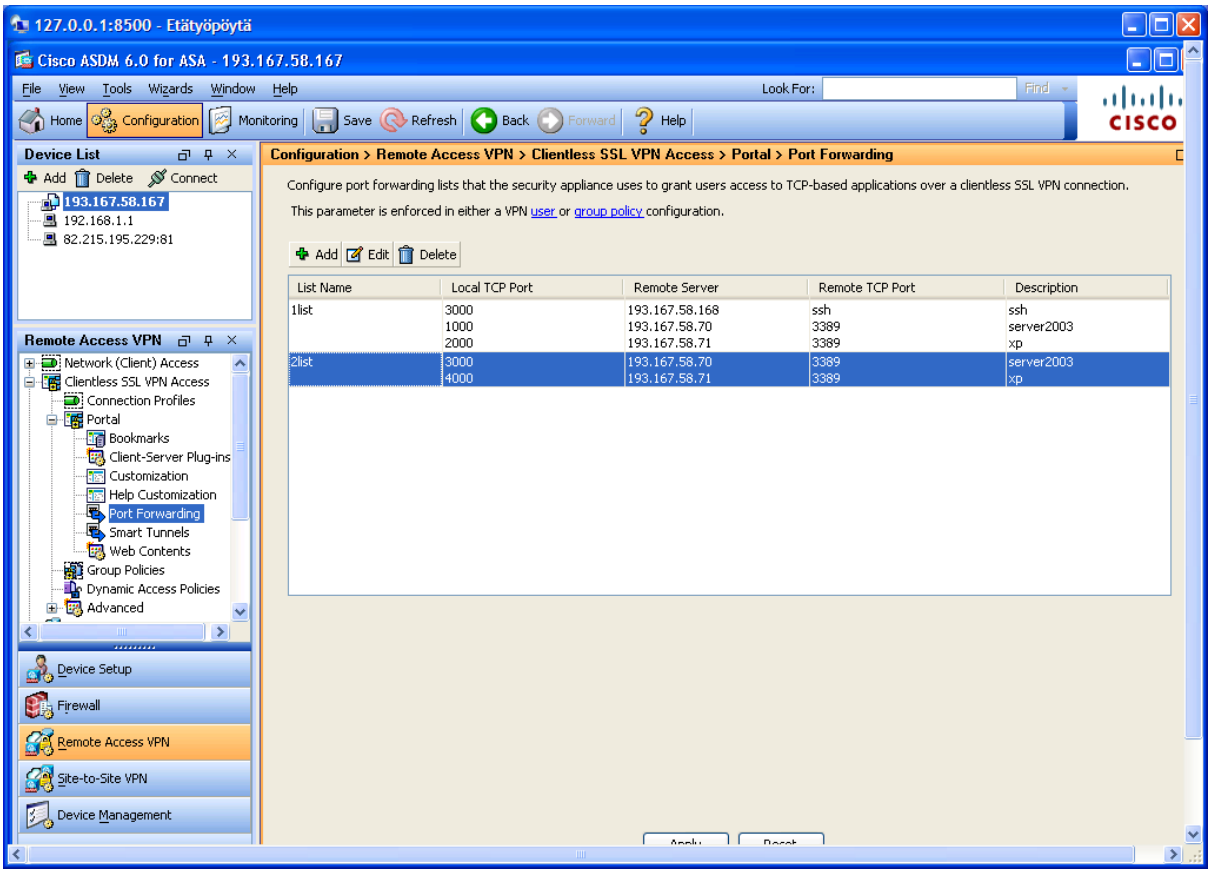
Kuvassa 10 on ASA-palomuurin konfiguraatio, jossa oli määritetty liityntäportti, johon SSL VPN on otettu käyttöön. SSL VPN -yhteydenottoportti on muutettu arvoon 2500. Yhteydelle määritettiin oma profiili ja käytetty group policy -sääntö. (Liite 2.)



Kuva 11. Käyttäjämääritykset

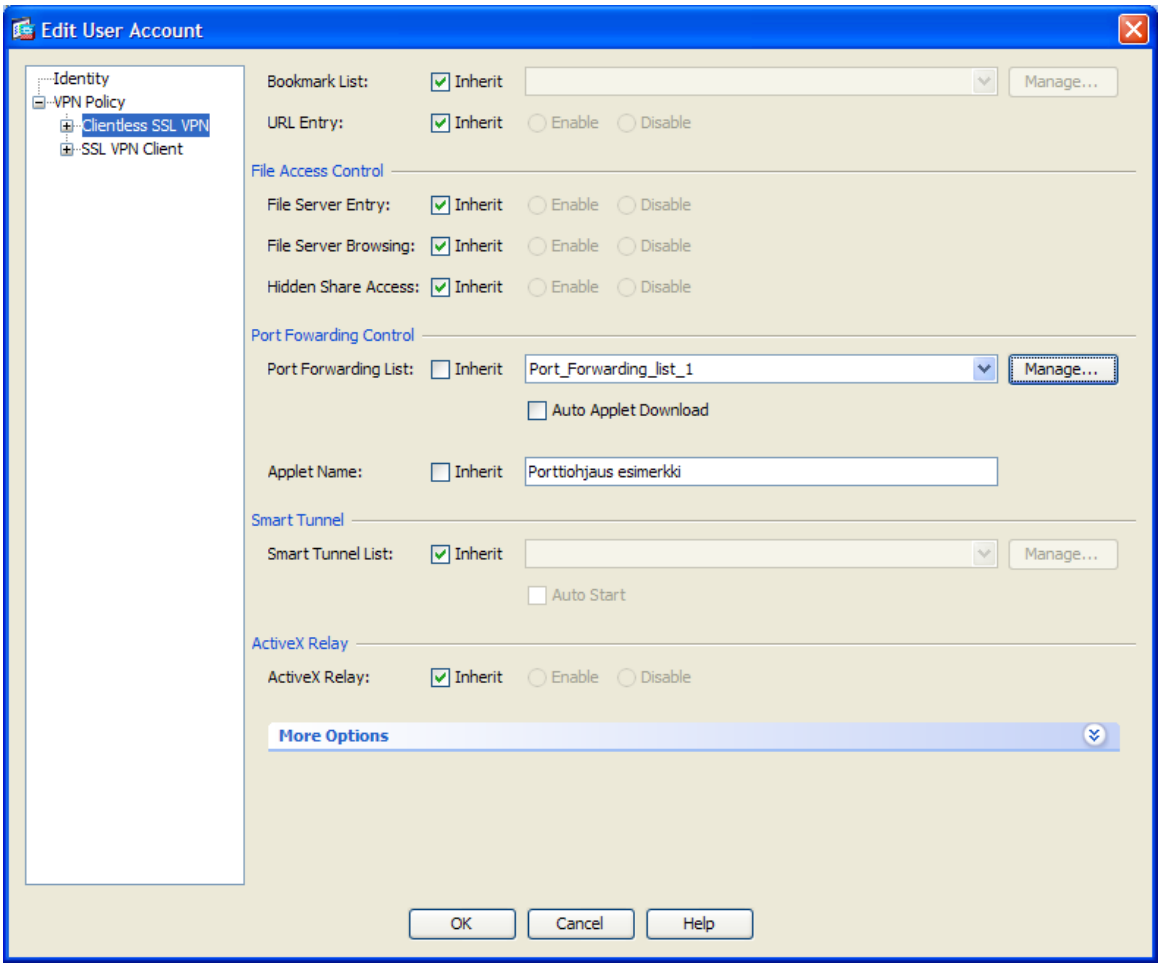
Kuvassa 11 on määritetty käyttäjät ja niille group policy –säännöt.

Käyttäjien määrityksissä sidottiin käyttäjä käyttämään yhtä porttiohjauslistaa. (Liite 2.)



Kuva 12. Porttiohjauslistaryhmät

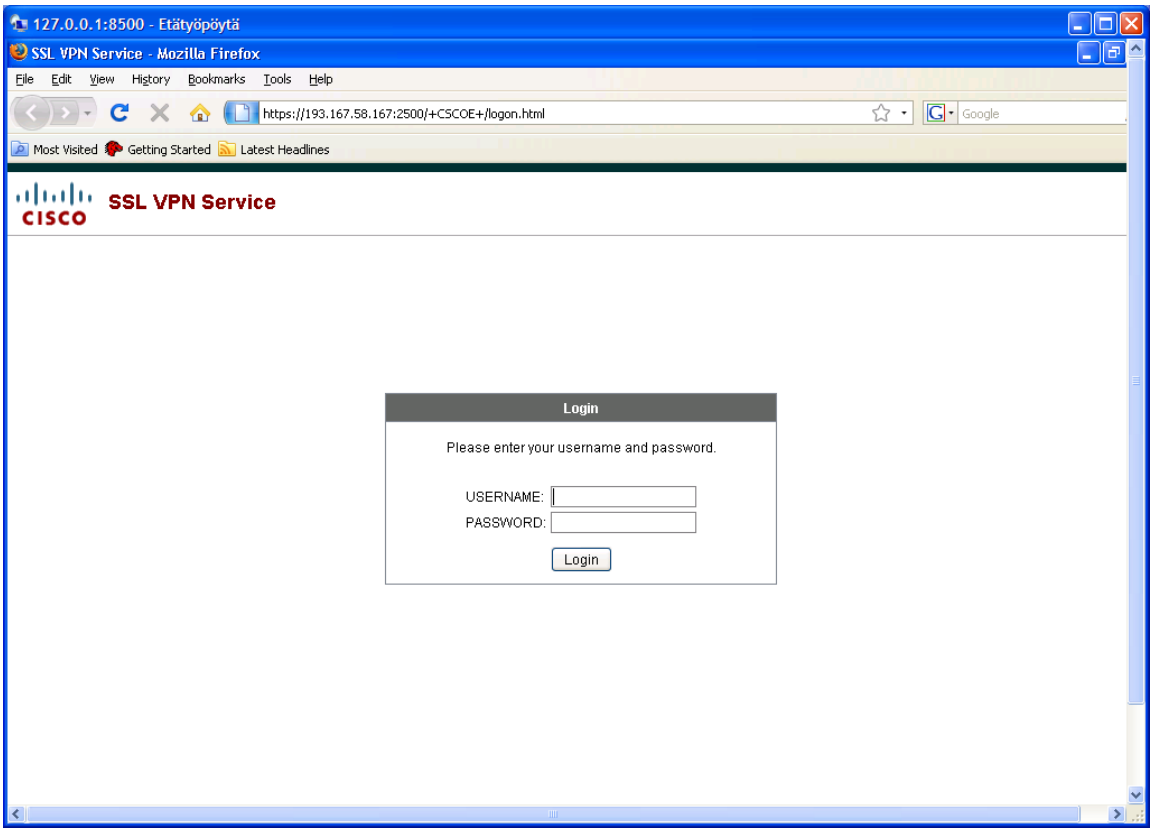
Kuvassa 12 määritettiin kaksi porttiohjauslistaa, joista toiselle sallittiin myös SSH-yhteys. Porttiohjauslistat sisältävät kaksi etäkäyttökoneen porttiohjausta. Porttiohjauksia muodostettaessa on huomioitava, että Windows-käyttöjärjestelmällä on etäkäyttöportti määritetty ja se portti on 3389. Tämä täytyy olla porttiohjauslistan remote TCP port -osiossa, jos halutaan muodostaa etäyhteys. (Liite 2.)



Kuva 13. Käyttäjätilin editointi

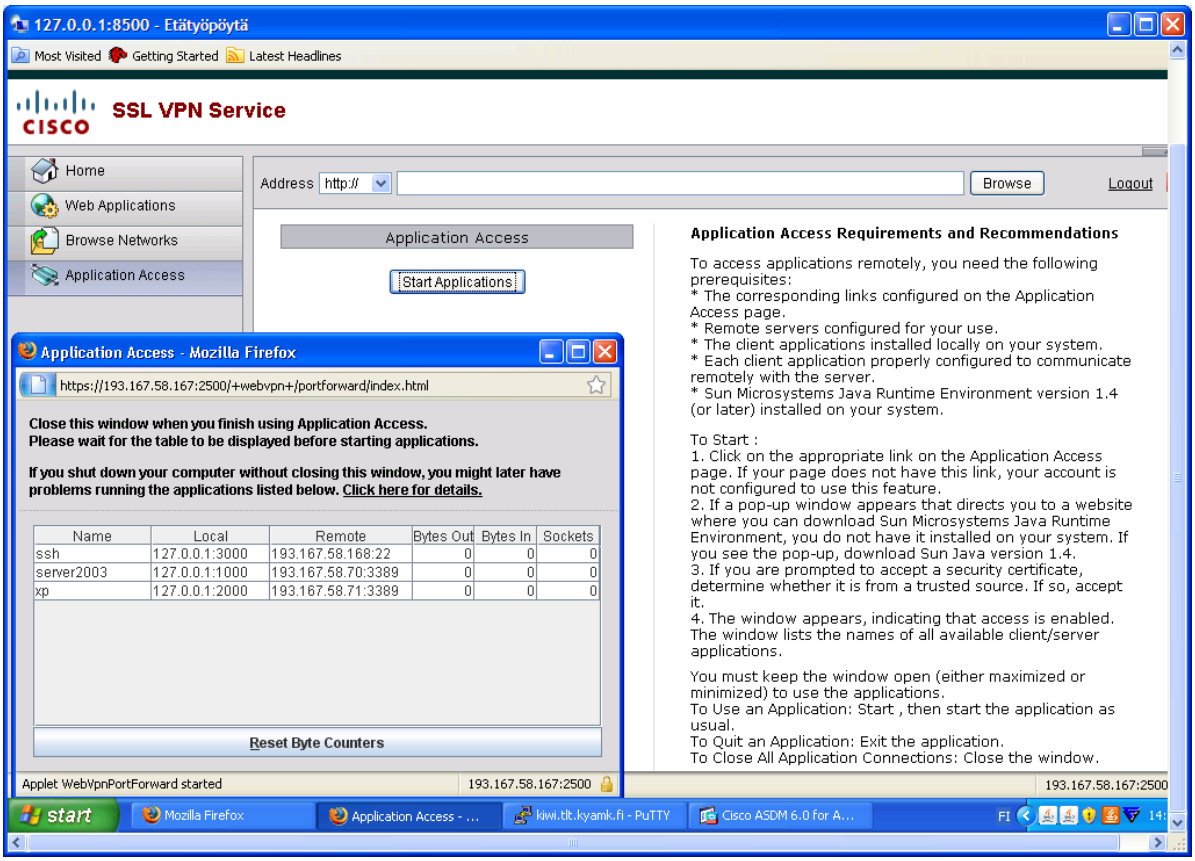
Käyttäjätiliä editoitaessa voi esimerkiksi sitoa tietyn porttiohjauksen käyttäjään. Sidonta yhteen käyttäjään parantaa tietoturvaa ja helpottaa myös kokemattoman käyttäjän toimintaa, koska käyttäjän listalle ilmestyy vain hänelle sallitut ohjaukset. (Liite 2.)

10.2 Yhteydenotto Secure Socket Layer Virtual Private Networkiin



Kuva 14. Yhteydenotto

Kuvan 14 osoiterivillä näkyy, miten SSL VPN -yhteys voidaan luoda. Aiemmin määritetyn käyttäjän tulee kirjautua palveluun sisälle. Sisään kirjautumisen jälkeen on muodostettu SSL VPN -yhteys, joka on salattu käytetyn laitteen ja sen laitteen, johon on otettu yhteyttä, välillä.



Kuva 15. Porttiohjauslistat SSL VPN -yhteydessä.

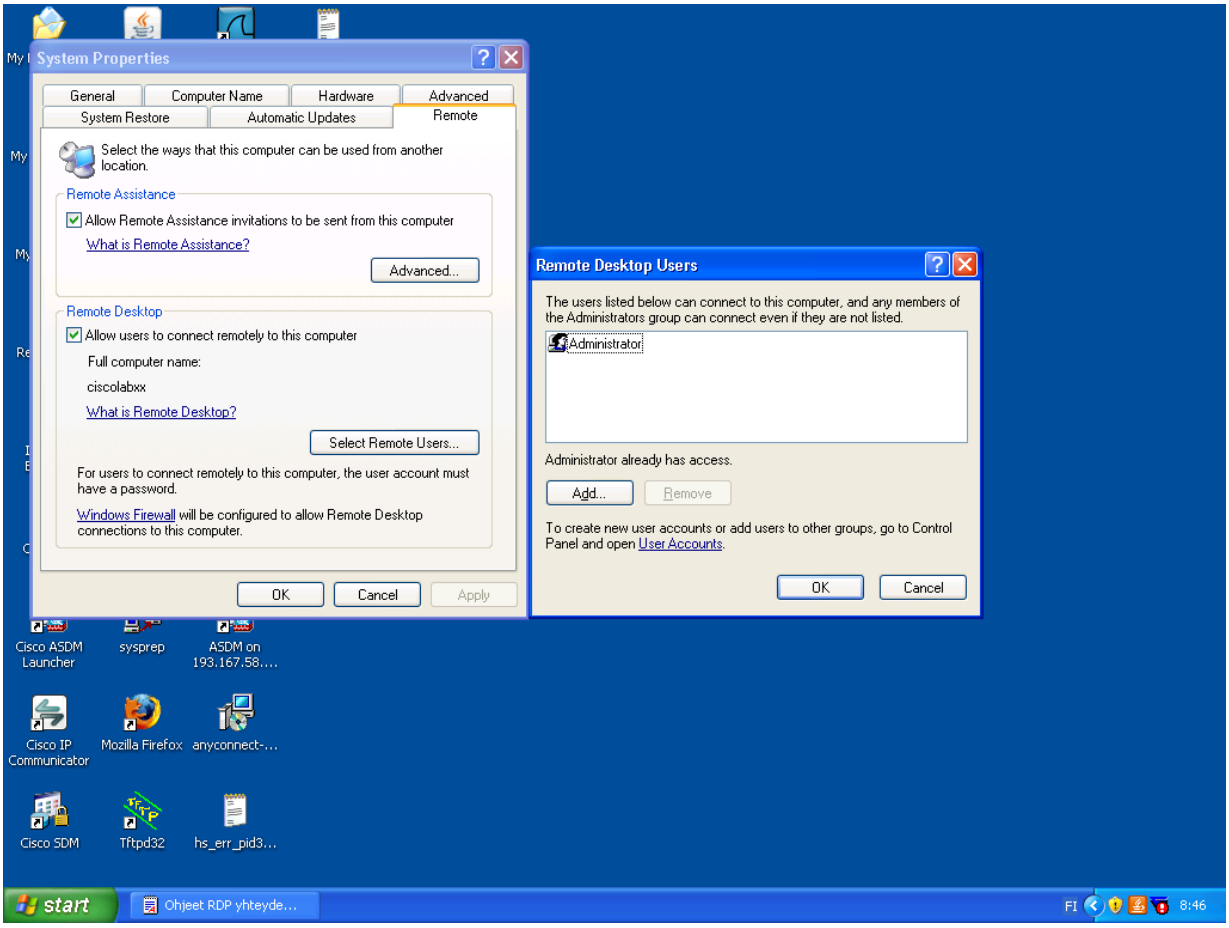
Kuvassa 15 on porttiohjauslista, jossa käyttäjälle on määritetty porttiohjaukset. Taustalla näkyy kirjautumisen jälkeen avautuva sivu, jossa on käynnistetty Java-sovellus painamalla Start Applications -nappulaa. Application Access -ikkunassa näkyy Java-sovelluksen porttiohjaukset. Kyseisellä käyttäjällä olisi siis mahdollista muodostaa SSH-yhteys sekä etäkäyttöyhteys kahteen koneeseen.

11 WINDOWS-ETÄKÄYTTÖKONE

Opinnäytetyön testausvaiheessa otettiin yhteys kahteen etäkäyttökoneeseen, joista toisessa oli käyttöjärjestelmänä Windows XP ja toisessa Windows Server2003. Windows XP -käyttöjärjestelmässä ja uudemmissa käyttöjärjestelmissä on valmiiksi asennettu etätyöpöytäyhteysmahdollisuus, mutta jos vanhempaan käyttöjärjestelmään haluttaisiin ottaa etätyöpöytäyhteys, tulisi järjestelmään asentaa etätyöpöytäyhteyttä tukeva ohjelma. Oletusarvot ovat Windows-käyttöjärjestelmissä siten, ettei järjestelmä hyväksy etäkäyttöä.

Oletus on muutettava, jotta voidaan ottaa etätyöpöytätuki käyttöön. Tukea käyttöön otettaessa on syytä määrittää käyttäjät, jotka voivat kirjautua sisään koneelle. Oletusarvona on Windows-käyttöjärjestelmissä etäkäyttöportti 3389. (Kuva 16.)

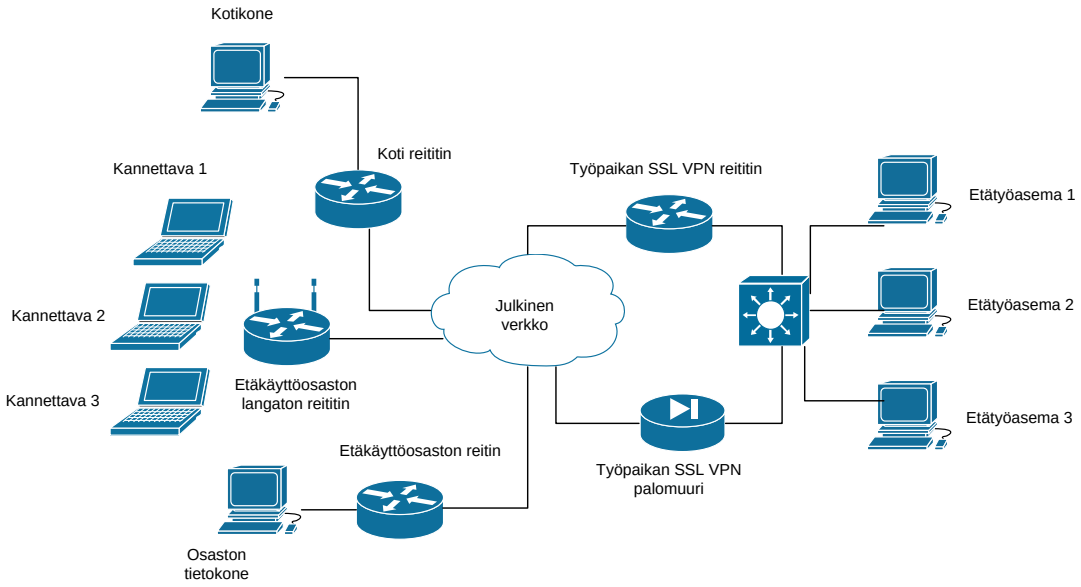
Etäyhteyden salliminen tapahtuu oman tietokoneen ominaisuuksista. Valitaan etäjärjestelmävälilehti, jossa hyväksytään etätyöpöytäyhteysmahdollisuus. Käyttöönottoa varten on syytä määritellä käyttäjät, jotka saavat ottaa yhteyden etätyöpöytään. Käyttäjien määritys tapahtuu etäkäyttäjien valinnoista. Valitaan joko valmis käyttäjä ja lisätään käyttäjälle etäkäyttömahdollisuus lisää-nappulasta. Mikäli käyttäjiä ei ole, käyttäjien luonti onnistuu käyttäjätileistä. Huomioitavaa XP-käyttöjärjestelmän kannalta on se, että käyttäjää luotaessa käyttäjä ei saa salasanaa. Salasana tulee määrittää itse. Käyttäjien luonnin jälkeen voit palata takaisin etäkäyttöyhteyden käyttäjälistaan ja lisätä tehdyn käyttäjän. (Kuva 16.)



Kuva 16. Etätyöpöytäyhteystietokoneeseen tehtäviä muutoksia.

12 YHTEYKSIEN EROAVAISUUDET

Työssä tehtiin kaksi erilaista ratkaisua, joita käytettiin koko työn aikana. Kytkentä muodostui erittäin monimutkaiseksi selittää, koska yhteyteen tarttuva tietokone voi sijaita missä vain.



Kuva 17. Esimerkkikuva, miten tartuttiin konfiguroituihin palveluihin.

Kuvasta 17 nähdään, että SSL VPN -palvelut voivat toimia myös rinnan eri alustoilla. Opinnäytetyö tehtiin hyvin samankaltaisella idealla julkisen verkon yli. Sisäverkossa oli kaksi laitetta, joihin voitiin ottaa SSL VPN -yhteys. Laitteet ohjasivat myös porttiohjauksensa samoihin etäkäyttökoneisiin. Yhteyksien vertailu onnistui reaaliaikaisesti, koska molemmat laitteet olivat yhtä aikaa toiminnassa.

Palveluiden vakaudessa oli eroja. Reitittimen kautta otettu SSL VPN -yhteys oli selkeästi epävakaampi kuin palomuurin kautta otettu yhteys. Reitittimelle ei ollut kuitenkaan tarjolla kuin testivaiheessa ollut IOS-image, joten päätelmä saattaa olla kuitenkin hieman keskeneräinen verrattaessa valmiiseen IOS-imageen. Reititin katkoi yhteyksiä melko yleisesti, mikä olisi huono asia etäkäyttäjän kannalta. Etäkäyttötietokone kuitenkin jää valmiustilaan, eli mitään ei hukata satunnaisessa yhteyden katkoksessa. On kirjauduttava uudel-

leen ja sen jälkeen jatkettava töitä. Tehokkuus kärsii, mikäli yhteys on katkonainen, ja samalla myös etätyöntekijä voi hermostua. Palomuurilla ei havaittu yhteydenkatkoksia. Palomuurilla yhteys vaikutti todella hyvältä ja vakaalta.

13 LOPPUPÄÄTELMÄT

SSL VPN on tärkeä osa nyt ja tulevaisuudessa tietoliikenneverkoissa. On syytä olettaa, että SSL VPN yleistyy jatkossakin. SSL VPN -etäyhteys tuo helpottavan vaihtoehdon, koska töitä voidaan silloin tehdä missä vain ja aina samat resurssit ovat käytössä. SSL VPN tuo yritykselle säästöä, kun sitä vertaa perinteiseen IPsec-tunnelointiin. IPsec-tunnelointi on huomattavasti kalliimpi tapa tehdä tunneli, koska se tarvitsee VPN-client-ohjelman, joka ei ole ilmainen. Yhteyden helppous on todella ratkaisevaa, koska SSL VPN -yhteys ei vaadi mitään erillisiä ohjelmia, joita pitäisi asentaa koneelle. SSL VPN -yhteyden monipuolinen käyttö, etenkin ASA-palomuureissa, on helppoa ja hyvin hallittavissa. Tulevaisuudessa jo pienetkin yritykset käyttävät SSL VPN -yhteyksiä, koska kyseinen etätyöpöytäyhteys helpottaa yrityksen verkkoresursseihin ja materiaaliin käsiksi pääsyä.

Reititin- tai palomuuripohjaisesta ratkaisusta palomuuripohjainen ratkaisu on järkevämpi. Palomuurilla oli vakaampi yhteys kuin reitittimellä. Käytännöllisyys ja hallittavuus ovat selvästi parempia palomuurissa kuin reitittimessä. Palomuurille liikenteen suodatus on ominaista, ja senkin takia valinta on parempi kohdistaa palomuuriin. Palomuurin suurin etu on SSL VPN -yhteyden monipuolisuus ja muokattavuus. Porttiohjauslistojen hallinta ja käyttäjäsidonnaisuus on todella suuri etu verrattuna reitittimen versioon, jossa kyettiin listaamaan vain yhteen listaan kaikki porttiohjaukset. Tartunta palomuuriin tapahtuu verkon reunalla, mistä yhteyttä ohjataan jatkossa SSL VPN -yhteyden avulla. Tietoturvan kannalta tämä on myös järkevämpi ratkaisu kahdesta ratkaisumallista.

LÄHTEET

A Cryptographic Evaluation of IPsec 1999. Saatavissa: http://www.schneier.com/paper-ipsec.pdf [viitattu 23.08.2009].

Frahim, J. & Huang, Q. 2008. SSL Remote Access VPNs. 1.painos. United States of America: Cisco Press.

OpenVPN and the SSL VPN Revolution 2004. Saatavissa: http://www.sans.org/reading_room/whitepapers/vpns/openvpn-ssl-vpn-revolution_1459 [viitattu 29.10.2009].

Tietoliikenteen suojaaminen 2003. Saatavissa: http://www.cs.uta.fi/titu/luennot/10_luento_turvaprotokollat.pdf [viitattu 24.09.2009].

Viestintävirasto - Epäsymmetrinen salaus 2007. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/epasymmetrinensalaus.html [viitattu 17.04.2010].

Viestintävirasto - Palomuuri 2007. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/palomuuri.html [viitattu 16.04.2010].

Viestintävirasto - Symmetrinen salaus 2007. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/symmetrinensalaus.html [viitattu 17.04.2010].

Viestintävirasto - VPN 2007. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html [viitattu 16.04.2010].

Liite 1/1

Cisco 2811 -sarjan reitittimen loppukonfiguraatio

```
hostname Router
boot-start-marker
boot system flash flash:/WebVPN/c2801-advipservicesk9-mz.124-22.T.bin
boot-end-marker
logging message-counter syslog
aaa new-model
aaa authentication login auth local
aaa session-id common
dot11 syslog
ip source-route
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
crypto pki trustpoint TP-self-signed-490156231
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-490156231
 revocation-check none
 rsakeypair TP-self-signed-490156231
crypto pki certificate chain TP-self-signed-490156231
 certificate self-signed 01
  3082023C 308201A5 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34393031 35363233 31301E17 0D303930 37313331 32303134
  355A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3439 30313536
  32333130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  974EE808 A6995721 7CB9F0B1 AC0B1F58 87072F38 6EA174CD F625CD13 0BD3CAFF
  F06E0690 BC0A2E32 6C7163C8 8AF589C7 C9A47F33 BE4B960F 194065BE D6A680FD
```

Liite 1/2

```
 06B6F745 34983153 4253592F 83D43BE6 855D6AFD D4313428 A7105476 4EF174DD
 8C77F91E 5855BF0F 08AB9CCF 2E52F80E B2387061 1878CC78 DE7D061C 4285670D
 02030100 01A36630 64300F06 03551D13 0101FF04 05300301 01FF3011 0603551D
 11040A30 08820657 65625650 4E301F06 03551D23 04183016 8014441B 82889CDE
 60649B39 8C8D8ECD 4C9C15DB 304A301D 0603551D 0E041604 14441B82 889CDE60
 649B398C 8D8ECD4C 9C15DB30 4A300D06 092A8648 86F70D01 01040500 03818100
 7658797A 6CE3D514 49FF6FD8 176D5593 12C42ABB 3CBFEF9D 3EAD4D65 75F34454
 C69F8947 09C0C41E F8F599C7 1BB8AFE1 1A81B8B7 34DFB21B F808B1AD 06DB03BF
 FD244D4E 6579BC44 23DF6A2C A5C2B2F4 A3F01082 FB4C7D22 5F1B38CB E3427ADE
 54FA82F7 6A5D42FB 29CF5C27 BB2B0ACE CF3BF42A 494A4521 19F0BB2D 281F061E
      quit
username ciscosdm privilege 15 password 0 cisco
username el5 password 0 el5class
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 193.167.58.168 255.255.255.192
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
interface Serial0/1/0
 no ip address
 shutdown
```

```
 no fair-queue
 clock rate 2000000
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
ip default-gateway 193.167.58.129
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 193.167.58.129
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 70 interface FastEthernet0/1 overload
access-list 70 permit 0.0.0.0 255.255.255.0
control-plane
ccm-manager fax protocol cisco
mgcp fax t38 ecm
line con 0
line aux 0
line vty 0 4
 transport input ssh
scheduler allocate 20000 1000
webvpn gateway alkupiste
 ip address 193.167.58.168 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-490156231
 inservice
webvpn context sisalto
 secondary-color white
 title-color #669999
```

```
 text-color black
 ssl authenticate verify all
 port-forward "portforward_list_1"
   local-port 8500 remote-server "193.167.58.71" remote-port 3389 description "X
P_Home"
   local-port 10000 remote-server "193.167.58.70" remote-port 3389 description "
Server2003"
 policy group kaytto
   port-forward "portforward_list_1" auto-download
   timeout idle 180
 default-group-policy kaytto
 aaa authentication list auth
 gateway alkupiste
 max-users 200
 inservice
end
```

Liite 2/1

Ciscon ASA 5505 palomuurin loppukonfiguraatio

```
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 193.167.58.167 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-603.bin
```

Liite 2/2

```
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 193.167.58.129 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 inside
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd enable inside
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
```

Liite 2/3

```
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
service-policy global_policy global
webvpn
 port 2500
 enable outside
 port-forward list 10000 193.167.58.70 3389 Server2003
 port-forward list 8500 193.167.58.71 33389 XP
group-policy WebVPN internal
username el5class password /r6f5BJVrlLzDdGa encrypted
prompt hostname context
Cryptochecksum:9b6043aff61a001c37ee1688068cd66b
end
```