KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Mika Koskinen

OHJELMAN ETÄKÄYTTÖ SSL VPN-YHTEYDELLÄ

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

KOSKINEN, MIKA	Ohjelman etäkäyttö SSL VPN-yhteydellä
Opinnäytetyö	32 sivua + 9 liitesivua
Työn ohjaaja	Yliopettaja Martti Kettunen
Toimeksiantaja	Cursor Oy
Huhtikuu 2011	
Avainsanat	clientless, SSL, VPN, palomuuri, etäkäyttö

Tässä opinnäytetyössä oli tarkoituksena testata Cisco ASA-palomuurin tarjoama SSL VPN-yhteys ja määrittää sen soveltuvuus Profimill Oy:n Mill-Planner-ohjelman ja SQL-palvelimen etäyhteyksiin.

Opinnäytetyön ensimmäisessä vaiheessa piti rakentaa toimiva testiympäristö, josta pääsi myös tuotantoverkkoon. Yhteyden muodostamisen jälkeen ohjelmalla tehtiin hakuja SQL-palvelimen tietokantaan ja mitattiin tiedonsiirron määrä. Tuloksia tutkittiin ja pääteltiin, kuinka suuri ohjelman kaistan käyttö on ja minkälaisen yhteyden ohjelman etäkäyttö vaatii asiakkaan ja palveluntarjoajan kannalta.

Toisessa vaiheessa rakennettiin samalla tekniikalla toteutettu etäyhteys Kymenlaakson ammattikorkeakoulun Simunet-laboratorion aktiivilaitteiden hallintaan. Hallintapalvelinta oli ohjattu web-sivujen kautta laboratoriosta käsin ja yhteys tuotantoverkosta oli estetty, joten SSL VPN-yhteyden avulla palvelinta pystyttiin hallitsemaan etänä ASA-palomurin toimiessa SSL VPN-yhdyskäytävänä.

Tulosten perusteella Mill-Planner-ohjelman testialusta ei vienyt kaistaa huomattavia määriä ja yhden yhteensopimattomuusongelman lisäksi yhteys toimi. Myös Simunet-laboratorion hallintapalvelimen web-sivujen etäkäyttö ja uudelleenohjaus toimi hyvin. Testituloksia ei kuitenkaan voinut soveltaa suoraan kaikkiin tilanteisiin, sillä SQL-palvelimen tietokanta oli näyteversio, joka ei vastannut oikeaa tuotantoversiota.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

KOSKINEN, MIKA	Application Running Over Clientless SSL VPN
Bachelor's Thesis	32 pages + 9 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Cursor Oy
April 2011	
Keywords	clientless, SSL, VPN, firewall, remote access

The purpose of this thesis was to study the Cisco ASA firewall's Clientless SSL VPN access and implement a test configuration for multiple SSL VPN connections from client to SQL server and analyze the bandwidth. The goal was to determine a minimum bandwidth customer and provider wise and provide an acceptable user experience.

In the second phase remote access was built using same methods and settings to control Simunet laboratory's management server.

Based on the results, the Mill-Planner test bench did not use the network resources significantly and despite one incompatibility, the setup worked. Because the SQL server database was a demo, not a production version, the results may not reflect real world scenarios. The Simunet management server worked flawlessly with Clientless SSL VPN.

SISÄLLYS

Liitteet

LYHENTEITÄ JA KÄSITTEITÄ

Varmentaja, CA, *certificate authority*: Varmenteita myöntävä osapuoli. Varmentajan tehtävänä on selvittää, onko varmenteen hakija oikeasti se, joka väittää olevansa.

Digitaalinen varmenne, *digital certificate*: Sähköinen asiakirja, joka käyttää digitaalista allekirjoitusta yhdistääkseen julkisen avaimen identiteettiin. Sisältää esim. henkilön tai yrityksen nimen, osoitteen jne.

Eheys, *integrity*: Varmistetaan tietosisällön muuttumattomuus tai ainakin havaitaan sen muuttuminen.

IETF, *The Internet Engineering Task Force*: Internet-yhteyskäytäntöjen standardoinnista vastaava organisaatio.

Tunkeutumisenestojärjestelmä, IPS, *intrusion prevention system*: Järjestelmä seuraa verkkoliikennettä ja yrittää etsiä liikenteestä tietynlaisia merkkejä, jotka viittaisivat siihen, että murtautuminen on käynnissä. IPS estää oletetun hyökkääjän yhteydet.

IPSec, *IP security architecture*: Joukko TCP/IP tietoliikenneyhteyskäytäntöjä Internet-yhteyksien suojaamiseen.

Kansainvälinen televiestintäliitto, ITU-T, *International Telecommunication Union*: YK:n alainen televiestintäverkkoja ja televiestintäpalveluja kansainvälisesti koordinoiva järjestö. Tehtävinä mm. standardisointi, radiotaajuuksien jakaminen jne.

Kumottujen varmenteiden lista, CRL, *certificate revocation list*: Lista kumotuista varmenteista, joihin ei pidä luottaa.

Luottamuksellisuus, *confidentiality*: Tietosisältö salataan yksityisyyden vuoksi.

OSI-malli, *Open Systems Interconnection Reference Model*: Kuvaa tiedonsiirtoyhteyskäytäntöjen yhdistelmän seitsemässä kerroksessa. Kukin kerros käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs.

Overhead-kuormitus: Kaikki ylimääräinen tieto, mitä tarvitaan lähettämään itse tietosisältö. Esimerkiksi otsakkeet, tarkistussummat sekä paketin uudelleenlähetys ovat overhead-kuormitusta.

Paketointi, *encapsulation*: Ylempien tasojen yhteyskäytännöt sulautetaan alempiin, joka onnistuu viestintäyhteyskäytäntöjen modulaarisuudesta johtuen. Tietosisältö (data) paketoidaan otsakkeeseen (header).

SSL, *secure sockets layer*: Kryptografinen yhteyskäytäntö, joka tarjoaa yhteyksien suojaamisen Internetissä. Toimii kuljetuskerrokselta ylöspäin.

TCP, *transmission control protocol*: Yksi Internet-yhteyskäytäntöperheen pääkomponenteista. Tarjoaa luotettavan, järjestyksellisen tiedonsiirron tietokoneen sovellukselta toisen tietokoneen sovellukselle.

TLS, *transport layer security*: IETF:n versio SSL-yhteyskäytännöstä. TLS 1.0 on SSL 3.0:n seuraaja.

Todennus, *authentication*: Käyttäjän identiteetti varmennetaan identiteettivarkauden varalta.

UDP, *user datagram protocol*: Yksi Internet-yhteyskäytäntöperheen pääkomponenteista. Tarjoaa luottamattoman, järjestyksettömän tiedonsiirron, jossa ei ole minkäänlaisia kättelyitä ja virheentarkistuksia. Tarkoituksena on pitää ylimääräinen viive ja ”overhead” kurissa.

Virtuaalinen yksityisverkko, VPN, *virtual private network*: Tapa, jolla kaksi tai useampia verkkoja yhdistetään julkisen verkon kautta muodostaen näennäisesti yksityisen verkon.

Älykäs tunneli, *smart tunnel*: Älykäs tunneli on yhteys TCP-pohjaisen sovelluksen ja yksityisen verkon välillä, käyttäen Clientless SSL VPN-istuntoa.

1 JOHDANTO

Virtuaaliset lähiverkot ovat Internetin aikakaudella merkittävä tapa toimia yritysmaailmassa. 1980-luvulla ja vielä 90-luvulla verkkoja yhdistettiin kalliilla suljetuilla verkoilla. Tässä opinnäytetyössä VPN-yhteyksillä tarkoitetaan salattuja yhteyksiä julkisen verkon yli, mikä on paljon suljettuja verkkoja halvempaa. Fyysiset liittymät voivat tulla miltä tahansa operaattorilta, ainoa vaatimus on pääsy julkiseen verkkoon, Internetiin.

Internetin alkuajoista asti verkon ylläpitäjät ovat etsineet tapoja hyödyntää tätä halpaa ja alati yleistyvää yhteyskanavaa siirtää tietoa samalla suojaten tiedon eheyttä ja luottamuksellisuutta. Tästä lähti konseptiajatus virtuaalisesta yksityisverkosta. Internet Engineering Task Force (IETF) kehitti standardikäytäntöjä ja -menetelmiä toimimaan julkisen Internet-verkon läpi jokaisen VPN-laitetoimittajan käytettäväksi. IETF määritteli useita VPN-yhteyskäytäntöjä, kuten Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F) Protocol, Layer 2 Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE) Protocol, Internet Protocol Security (IPsec) ja Secure Socket Layer VPN (SSL VPN). (1, 3.)

1.1 Tavoite

Tässä opinnäytetyössä oli tavoitteena toteuttaa Profimill Oy:n Mill-Planner-ohjelman ja SQL-palvelimen etäyhteys käyttäen SSL VPN-yhteyttä ja tarkastella, miten paljon resursseja etäyhteys vie. Tämän avulla pystyttäisiin hahmottelemaan, kuinka nopean Internet-yhteyden etäyhteys vaatisi.

Työn toinen tavoite oli tehdä samankaltainen ratkaisu tietotekniikan laboratorion Simunet-laboratorion Remote-palvelimen etähallintaan. Hallintaohjelmaa piti pystyä käyttämään etänä turvallisesti ja vain oikeilla tunnuksilla, muut yhteydenotot estäen.

1.2 Opinnäytetyön rakenne

Tässä opinnäytetyössä esitellään ensin käytettävät teknologiat ja kerrotaan niiden teoriasta, sen jälkeen käsitellään käytännön työ ja tulokset. Toisessa luvussa keskitytään VPN-yhteyksiin liittyvään teoriaan yleisesti. Kolmannessa luvussa keskitytään SSL

VPN-teknologiaan liittyvään teoriaan. Neljännessä luvussa kerrotaan testiympäristöstä ja käytetyistä laitteista, sekä käydään läpi Cisco ASA-palomuurin konfigurointi. Viidennessä luvussa esitellään tulokset ja niistä tehdyt päätelmät.

2 VPN-YHTEYDET

VPN-yhteyskäytännöt jaetaan kahteen luokkaan:

- Site-to-site
- Remote access

Ensimmäisen luokan VPN-yhteyskäytännöillä voidaan yhdistää kaksi tai useampi yrityksen verkkoa julkisen Internet-verkon läpi. Näitä yhteyksiä voidaan myös käyttää yksityisten tai osittain yksityisten verkkojen yhdistämiseen eri organisaatioiden välillä. Tämä poistaa tarpeen käyttää dedikoituja vuokrattuja linjoja (dedicated leased line) yrityksen eri toimipisteiden välillä. IPsec ja GRE ovat yleisemmin käytettyjä site-to-site VPN-yhteyskäytäntöjä. (1, 3)

Tämän lisäksi voidaan muodostaa yksittäinen etäyhteys julkisen verkon yli yrityksen verkkoon. Näistä yhteyskäytännöistä on hyötyä silloin, kun yrityksen työntekijän pitää työskennellä ja päästä yrityksen resursseihin käsiksi etäältä, kuten kotoa, hotellista, lentokentältä, Internet-kahvilasta aivan kuin he olisivat suoraan yhdistetty yrityksensä verkkoon. Yleisemmin käytetyt remote access VPN-yhteyskäytännöt ovat SSL VPN, IPsec, L2TP, L2TP over IPsec ja PPTP. Useat yritykset suosivat IPseciä, koska sitä voi käyttää sekä verkkojen välisenä että etäyhteys yhteyskäytäntönä. Tämän lisäksi se on ilmiselvä valinta laitevalmistajille sen laajan ominaisuusjoukon ja suojausmenetelmien takia. Muitakin VPN-menetelmiä on yleisesti käytössä riippuen tarpeista ja organisaation infrastruktuurista. SSL VPN on yleistymässä suositelluksi valinnaksi monissa organisaatioissa sen hyötyjen vuoksi. Monissa tapauksissa se tarjoaa etäyhteyden, jossa käyttäjät pääsevät käsiksi yrityksen resursseihin ilman lisäohjelmien asennuksia yhteisissä työasemissa. (1, 4-5.)

Salatut VPN-yhteydet paketoivat tiedon käyttäen kryptografisia menetelmiä kahden tai useamman verkkolaitteen välillä, jotka eivät ole samassa yksityisessä lähiverkossa. Tämä on tärkeää, sillä tiedon pitää olla suojattu ulkopuolisilta laitteilta, jotka sijaitsevat välissä olevissa yksityisissä tai julkisissa verkoissa.

2.1 Suojausmenetelmät

Salatut VPN-yhteydet käyttävät kryptografisia tunnelointiyhteyskäytäntöjä tarjotakseen tietosisällölle luottamuksellisuuden, jossa tietosisältö salataan yksityisyyden vuoksi. Todennuksen, jossa tietosisällön lähettäjän identiteetti varmennetaan identiteettiväärennöksen varata sekä eheyden, jolla varmistetaan tietosisällön muuttumattomuus tahattomasti tai tahallisesti tai ainakin havaitaan muuttuminen.

2.2 Suojausyhteyskäytännöt

Cisco ASAn käyttämiä suojattuja VPN-yhteyskäytäntöjä on IPsec ja SSL VPN. IPsec on yleisimmin käytetty yhteyskäytäntökokonaisuus, joka on tarkoitettu IP yhteyksien suojaamiseen. IPsec-yhteyskäytännöt toimivat OSI-mallin verkkokerroksen tasolla, joten se toimii kaikilla ylemmän kuljetuskerroksen yhteyskäytännöillä, kuten TCP, UDP, ICMP jne. Koska IPsec toimii verkkokerroksella, se tarjoaa suojatun yhteyden kahden yhdyskäytävän, kahden isäntäkoneen tai vaikka yhdyskäytävän ja isäntäkoneen välillä. IPsec-yhteyskäytäntöjen suojauskäytännöt sopivat yritysten ja palvelun-tarjoajien infrastruktuuriin. SSL VPN on teknologia, joka tarjoaa suojatun yhteyden yrityksen sisäisiin resursseihin web-selaimen avulla tai käyttäen dedikoitua asiakasohjelmaa. SSL VPN toimii kuljetuskerroksen ja sovelluskerroksien välillä.

3 SSL VPN-TEKNOLOGIA

SSL ja sen seuraaja TLS ovat kryptografisia yhteyskäytäntöjä yhteyksien suojaamiseksi Internetissä. SSL-yhteyskäytännön kehitti Netscape verkkokaupankäyntisivuille, jotka tarvitsivat tiedon salaamista ja käyttäjän varmentamista. Esimerkiksi verkkopankeissa käyttäjien istunnot ovat suojatusti luotu käyttäen tätä yhteyskäytäntöä. Vaikka teknologia kehitettiin suojattujen web istuntojen käyttöön, yritykset käyttävät yhteyskäytäntöä hyödyksi myös tavallisempien ohjelmien suojaamiseen, kuten Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3) ja Internet Message Access Protocol (IMAP).

SSL VPN-yhteyskäytännön tehokkuus johtuu sen kypsyydestä ja siitä, että se sisältyy käytännössä jokaiseen web-selaimeen. Käyttäjä voi turvallisesti selata hänen sisäistä web-palvelintaan tai katsoa sähköpostit julkiselta koneelta ilman VPN-asiakasohjelmaa. Cisco tarjoaa eri menetelmiä käyttää SSL VPN-yhteyksiä joihin sisältyy:

- Clientless mode: Turvallinen pääsy yrityksen resursseihin, lähinnä web- ja e-mail palvelimiin ilman erillistä ohjelmaa.
- Thin Client Mode: Pääsy useimpiin TCP-pohjaisiin yhteyskäytäntöihin, kuten SMTP, POP, Secure Shell (SSH), Terminal ja Telnet lataamalla Java-sovelman asiakaskoneella.
- Full tunnel mode: Tarjoaa täydellisen pääsyn yrityksen resursseihin aivan kuten käyttäjä olisi suoraan kiinni verkossa. Tila vaatii ladattavaksi SSL VPN-asiakasohjelman ennen kuin yhteyden voi aloittaa. (1, 7-8.)

3.1 Kryptografiset rakennuslohkot

Kuten kohdassa 2.1 kerrottiin, SSL VPN-yhteyden suojaus rakentuu kolmesta kohdasta; luottamuksellisuudesta, todennuksesta ja eheydestä. Seuraavissa kappaleissa kerrotaan, miten nämä kolme toteutetaan.

3.1.1 Hajautus ja viestin eheyden todennus

Hajautus (hashing) on tärkeä osa turvallisuutta takaamalla lähetetyn tiedon eheyden. Hajautusalgoritmissa vaihtelevan suuruinen tekstikenttä muunnetaan tietyn pituiseksi merkkijonoksi. Tietoturvalaitteiden hajautusalgoritmeihin kuuluu seuraavat ominaisuudet:

- One-way hashing mechanism: Tarkoittaa, että oli hajautuksen lopputuloste mitä tahansa, sitä on vaikea kääntää takaisin alkuperäiseen viestiin.
- Collision-free output: Hajautusalgoritmin tuotoksien pitää toimia niin, että on laskennallisesti liian vaativaa löytää kahta eri viestiä, jolla on sama hajautustuloste.

Näiden ominaisuuksien ansiosta hajautus on tunnettu myös viestin tiivisteenä (message digest) ja digitaalisen sormenjälkenä. Ihmiset voivat generoida pienen hajautustulosteen isosta dokumentista ja käyttää sitä dokumentin digitaalisena sormenjälkenä. Tätä sormenjälkeä voidaan käyttää varmentamaan, että viestiä ei ole kajottu kesken turvattoman lähetyksen. Tästä sormenjäljestä ei voi myöskään päätellä alkuperäisen viestin sisältöä.

Tällä hetkellä suosituimmat kryptografiset hajautusalgoritmit ovat message digest algorithm 5 (MD5) ja Secure Hash Algorithm 1 (SHA-1). MD5 tarjoaa 128-bittisen tulosteen ja SHA-1 tarjoaa 160-bittisen. Suuremman kokonsa vuoksi SHA-1-algoritmi on pidetty turvallisempana, mutta laskennallisesti kalliimpana kuin MD5-algoritmia. Tämän päivän laitteilla ja ohjelmistoilla laskentavaatimusten ero ei yleensä ole huolenaihe, joten SHA-1 on suositeltu hajautusalgoritmi käytettäväksi VPN-yhteyksiin.

Viestin suojakoodi (message authentication code) on kryptografinen tarkistussumma, jota käytetään varmistamaan viestin eheys lähetyksessä. MAC-tarkistussumman generoimiseksi voidaan käyttää joko salausalgoritmia, kuten Data Encryption Standard (DES) tai hajautusalgoritmia. Hajautus on yleisesti paljon nopeampi kuin salaus, joten hajautuspohjainen MAC (HMAC) on suosituin tapa. HMAC on avaimellinen hajautus funktio. Jotta voidaan generoida HMAC-hajautusalgoritmi viestistä M, tarvitaan kaksi systeemiparametria, hajautusfunktio H ja avain K. Viestin HMAC lasketaan seuraavasti:

$$HMAC(K,M) = H(K \text{ XOR } opad, H(K \text{ XOR } ipad, M))$$

jossa opad on merkkijono 0X5c ja ipad on merkkijono 0x36.

Kryptausmenetelmässä avain K on normaalisti generoitu avainneuvottelussa ja perustamisprosessissa kahden vertaisen (peer) välillä. Huomaa, että kaksitasoinen hajautus tekee HMAC-funktiosta paljon yksinkertaista avaimellista hajautusfunktiota turvallisemman. (2, 2.)

3.1.2 Salaus

Salausalgoritmit muuntavat selväkielisen tekstin salatuksi. Toisin kuin hajautus, salausalgoritmit tarvitsevat avaimet sekä salaukseen, että purkamiseen. Salausalgoritmit jakaantuvat kahteen luokkaan:

- Symmetrinen salaus: Käyttää samaa avainta sekä salaukseen, että purkamiseen. Tunnetaan myös nimellä salainen avain kryptografia (secret-key cryptography). Symmetrisiä algoritmeja käytetään yleensä viestin sisällön suojaamiseen. Symmetrisessä salauksessa on kaksi pää algoritmityyppiä:
    - bittivirtasalaus (stream cipher), kuten RC4
    - lohkosalaus (block cipher), kuten DES, 3DES, AES
- Epäsymmetrinen salaus: Käyttää eri avaimia salaukseen ja purkamiseen. Tunnetaan myös nimellä julkinen avain kryptografia (public key cryptography).

> Epäsymmetrinen salausmenetelmä perustuu kahteen laskennallisesti yhdistävään avaimeen. Yksi avain, jonka julkinen Internet-toimialue tietää, on nimeltään julkinen avain; toisen avaimen tietää vain avainten omistaja. Riippuen julkisen ja yksityisen avaimen käytöstä, epäsymmetristä algoritmia voi käyttää sekä salaukseen, että todentamiseen. RSA ja DSA ovat tunnetuimmat julkisen avaimen algoritmit. (1, 20.)

3.2. Digitaaliset allekirjoitukset ja digitaalinen varmenne

Todennus ja eheys ovat tärkeitä ominaisuuksia suojatuissa VPN-yhteyksistä. Näitä ovat kokonaisuuden todennus, tiedon alkuperän todennus, eheys ja kiistämättömyys, eli viestin lähettäjä ei pysty kiistämään lähettäneensä viestiä. Digitaaliset allekirjoitukset ja varmenteet tarjoavat skaalautuvan luottamusjärjestelmän. (1, 24.)

3.2.1 Digitaalinen allekirjoitus

Suojatussa kommunikoinnissa pitää yleensä pystyä todentamaan, että viesti tuli oikealta lähettäjältä, eikä vihamieliseltä osapuolelta joka väärentää ja uskottelee olevansa oikea lähettäjä. Vastaanottaja saattaa myös haluta, että lähettäjä ei pysty myöhemmin kiistää lähettäneensä viestiä, tästä termi kiistämättömyys.

Digitaalisessa allekirjoittamisessa viestin hajautus salakirjoitetaan käyttäen lähettäjän omaa yksityistä avainta. Tuloste on digitaalinen allekirjoitus. Allekirjoittaminen käyttäen omaa yksityistä avainta takaa alkuperän oikeellisuuden, sillä vain yksi henkilö, joka allekirjoittaa viestin, tietää yksityisen avaimen. Allekirjoituksen voi helposti vahvistaa käyttäen vastaavaa julkista avainta joka on listattuna julkisessa domainissa. (Jazib Frahim, Qiang Huang, 24-25.)

3.2.2 Julkisen avaimen infrastruktuuri, digitaaliset varmenteet ja varmennus

Digitaalisen varmenteen todentamiseksi vastaanottajan pitää saada käyttöönsä lähettäjän julkinen avain. Avainta ei pidä luovuttaa vain skaalautuvalla tavalla, vaan myös luotettavasti, jotta avainta voidaan pitää oikeana. Tämän tähden on perustettu luottamusjärjestelmä joka takaa kolmansille osapuolille käyttäjien identiteettien tarkastamisen ja vahvistamisen. Julkisen avaimen infrastruktuuri (PKI) koostuu yhteyskäytännöistä, standardeista ja palveluista jotka mahdollistavat ja tukevat luottamusjärjestelmän sovelluksia. PKI mahdollistaa käyttäjien todentaa toisensa käyttämällä digitaalisia varmenteita, jotka varmentajat (CA) ovat myöntäneet.

- X5.09: ITU-T:n standardi PKI:lle joka määrittelee standardiformaatit julkisen avaimen varmenteille.
- Julkisen avaimen infrastruktuuri X5.09 (PKIX): IETF työryhmä, joka määrittelee digitaalisten varmenteiden käyttötavan.
- Julkisen avaimen kryptografia-yhteyskäytännöt (PKCS): RSA-laboratorioiden suunnittelema ja julkaisema joukko julkisen avaimen kryptografia standardeja. PCKS on PKI:n kryptografinen perusta.
    - PKCS 1 määrittelee RSA-kryptografian standardin.
    - PKCS 7 määrittelee kryptografisen viestin syntaksi standardin, joka määrittää PKI:n alaisen viestin allekirjoittamisen ja salauksen.
    - PKCS 10 määrittelee varmennuspyynnön standardin, joka määrittää formaatin, jossa viestit lähetetään varmentajalle pyytääkseen avainparille varmennetta.

Digitaalinen varmenne sitoo käyttäjän identiteetin ja julkisen avaimen. Digitaalisen varmenteen myöntää kolmannen osapuolen kokonaisuus varmentajat, joilla varmistetaan varmenteen luotettavuus.

Versio	
Sarjanumero	
Allekirjoitusalgoritmi ID	
Myöntäjä (CA) X.500 Nimi	
Voimassaoloaika	
Kohde X.500 Nimi	
Kohteen julkisen avaimen tieto	Algoritmi ID
	Julkisen avaimen arvo
Myöntäjän uniikki ID	
Kohteen uniikki ID	
Laajennus	

CA Digitaalinen allekirjoitus

Taulukon kohdat:

- Allekirjoitusalgoritmi ID: Määrittää allekirjoitusalgoritmin esim. RSA käyttäen SHA1 tai DSS käyttäen SHA-1.
- Myöntäjä (CA) X.500 Nimi
- Voimassaoloaika
- Kohde X.500 Nimi
- Kohteen julkinen avain
- Laajennus
- CA Digitaalinen allekirjoitus

Varmennus on prosessi, jossa CA myöntää digitaalisia varmenteita. CA on luottamuksen perusta koko PKI-systeemille ja on vastuussa käyttäjien identiteettien varmenta-

misesta, digitaalisten varmenteiden myöntämisestä, kumoamisesta ja kumottujen varmenteiden listan (CRL) julkaisemisesta.

Esimerkki varmennuksesta: Henkilö X haluaa osoittaa olevansa luotettava henkilölle Y käyttämällä digitaalista varmennetta. Ensin hänen täytyy rekisteröityä CA-palvelimelle saadakseen identiteettinsä varmenteen.

1. Henkilö X pyytää juurivarmennetta, joka on CA-palvelimen varmenne.
2. CA-palvelin lähettää juurivarmenteensa X:lle.
3. X luo varmennepyynnön, jossa on X:n identiteettitiedot ja hänen julkinen avaimensa. X allekirjoittaa varmennepyynnön käyttäen CA:n julkista avainta, joka on CA:n juurivarmenteessa.
4. CA-palvelin saa varmennepyynnön, varmentaa X:n identiteetin ja luo digitaalisen varmenteen X:lle, sitoen hänen identiteettinsä ja julkisen avaimen. Digitaalinen varmenne on CA:n allekirjoittama ja tuo toisen sidoksen X:n ja CA:n identiteeteille.
5. CA-palvelin myöntää varmenteen X:lle.
6. Saadessaan identiteettinsä varmenteen, X esittää sen Y:lle osoittaakseen olevansa luotettava.
7. Y seuraa digitaalisen varmenteen todentamisprosessia tarkistaakseen X:n varmenteen oikeellisuuden ja sitten osoittaa luottamusta X:n julkiseen avaimeen. (1, 25-30.)

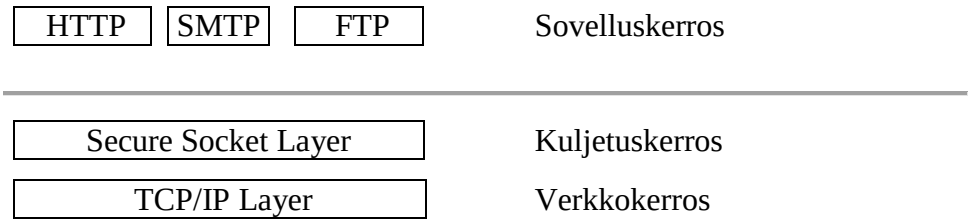
3.3 SSL/TLS-yhteyskäytäntö

SSL-yhteyskäytäntö on kehittänyt Netscape omaan Netscape-selaimeensa. Se kehitettiin vastaamaan kasvavaan huoleen Internetin turvallisuudesta. SSL oli alun perin kehitetty selaimen ja palvelimen väliseen kommunikointiin. SSL-yhteyden kautta oli tarkoitus ajaa muita sovelluksia, kuten TELNET ja FTP. (3.)

Netscapen luovutettua kehityksen IETF-standardointiorganisaatiolle, IETF kehitti yhteyskäytännöstä oman versionsa ja antoi sille nimeksi TLS. TLS 1.0 pohjautui SSL 3.0 versioon.

3.3.1 OSI-mallissa sijaitseminen ja TCP/IP-yhteyskäytäntötuki.

SSL on järjestelmäriippumaton ja sovellusriippumaton yhteyskäytäntö jota käytetään TCP-pohjaisissa sovelluksissa. Se sijaitsee TCP-kerroksen huipulla, sovelluskerroksen alapuolella ja toimii kuin pistokkeina (socket) TCP-yhteyksissä.



SSL olettaa luotettavaa paketin kuljetusta, joten se toimii aina TCP-yhteyskäytännön päällä, ei UDP-yhteyskäytännön tai suoraan IP-yhteyskäytännön päällä. Käytetyimpien sovellusten, jotka on määritelty TCP/IP-perheessä, kuten HTTP ja SMTP, standardit on kehitetty kaikkine teknisine yksityiskohtineen, jotta SSL-yhteyttä voidaan käyttää näiden yhteyksien suojaamiseen. Näistä kerrotaan kaksi yleisesti tunnettua esimerkkiä. HTTP over SSL: web-selainten suojaus oli SSL-yhteyskäytännön kehittämisen eteenpäin vievä voima ja HTTP on ensimmäinen sovelluskerroksen yhteyskäytäntö joka on suojattu SSL-yhteydellä.

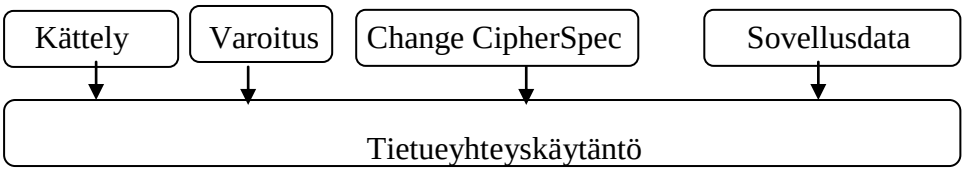
Netscapen toteutettua HTTP over SSL-yhteyden Navigatorissaan, se käytti https://-skeemaa sivuissa, jotka haettiin käyttäen HTTP over SSL-yhteyttä. Näin ne eroteltiin tavallisista sivuista, jotka haettiin käyttäen http://-skeemaa. HTTP over SSL tulikin tunnetuksi nimellä HTTPS. HTTPS standardisoitiin myöhemmin RFC 2818-standardissa. HTTPS operoi portissa 443, kun http operoi normaalisti TCP-portissa 80. Käyttäjät kokevat HTTPS-yhteyden ja http-yhteyden samanlaisesti. Kun käyttäjä on yhdistänyt selaimellaan käyttäen HTTPS-yhteyttä, asiakkaana hän muodostaa yhteyden palvelimeen ja neuvottelee SSL-yhteyden. Kun SSL-yhteys on muodostettu, HTTP-data kulkee SSL-tunnelin läpi.

Email over SSL: Samankaltaisesti kuin http over SSL, sähköpostiyhteyskäytännöt kuten SMTP, POP3 ja IMAP voivat tukea SSL-yhteyttä. (4.)

3.3.2 SSL-tietueyhteyskäytäntö (record protocol) ja kättely-yhteyskäytännöt

SSL-yhteys muodostuu kahdesta vaiheesta. Ensimmäinen vaihe on kättelyvaihe, jolloin neuvotellaan kryptografisista algoritmeista, todennetaan palvelin ja perustetaan avaimet datan suojaamiseksi ja MAC. Toinen vaihe on suojattu datansiirtovaihe, jolloin SSL suojaa yhteyttä.

SSL on kerroksinen yhteyskäytäntö. Alimmalla kerroksella on SSL-tietueyhteyskäytäntö. Tietueyhteyskäytäntö rakentuu muutamista viestityypeistä tai yhteyskäytännöistä, jotka hoitavat erilaisia tehtäviä.



Tietueyhteyskäytäntö on suurimmaksi osaksi paketointiyhteyskäytäntö. Se siirtää erilaisia suurempien kerrosten yhteyskäytäntöjä ja sovellusten dataa. Tietueyhteyskäytäntö ottaa viestit siirrettäväksi; tekee tarvittavat toimenpiteet, kuten sirpaloinnin, pakkaamisen, MACin asetuksen ja suojauksen; ja sitten lähettää datan. Se tekee myös päinvastaiset toimenpiteet - suojauksen purun, todennuksen, paketoidun tiedon purkamisen ja uudelleenasettelun – vastaanotettavalle datalle. Tietueyhteyskäytäntö koostuu neljästä ylemmän kerroksen asiakasyhteyskäytännöstä: Kättely-yhteyskäytäntö, hälytysyhteyskäytännöstä Change CipherSpec yhteyskäytäntö ja sovellusdatayhteyskäytäntö.

Kättely-yhteyskäytännöt ovat vastuussa SSL-istuntojen perustamisesta ja jatkamisesta. On kolme aliyhteyskäytäntöä:

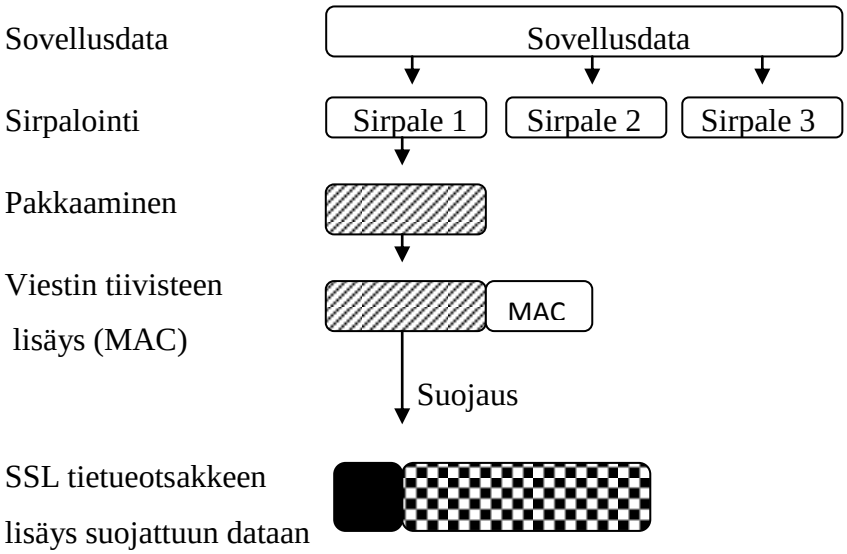
- Kättely-yhteyskäytäntö neuvottelee SSL-istunnon suojausominaisuuksista.
- Hälytysyhteyskäytäntö on yhteyskäytäntö, jota käytetään välittämään hälytysviestejä SSL-vertaisten välillä. Hälytysviestit sisältävät virheitä, poikkevia tiloja kuten virheellisen MACin tai suojauksen purkamisen epäonnistumisen tai ilmoituksen, kuten istunnon päättämisen.
- Change CipherSpec-yhteyskäytäntöä käytetään avainmateriaalin vaihtoon.

Sovellusdatayhteyskäytäntö huolehtii ylemmän kerroksen sovellusdatan siirrosta.

Asiakas ja palvelin neuvottelevat tilallisen yhteyden käyttäen kättely-yhteyskäytäntöä. Kättelyn aikana asiakas ja palvelin sopivat tietyt parametrit, joita käytetään yhteyden suojauksen toteuttamiseen.

- Kättely alkaa, kun asiakas yhdistää TLS-yhteensopivaan palvelimeen pyytäen suojattuan yhteyttä ja esittää listan sopivista salakirjoituskokoelmista.
- Tästä listasta palvelin valitsee tehokkaimman salakirjoituksen ja tiivisteen (*cipher and hash functions*) ja ilmoittaa asiakkaalle valinnasta.
- Palvelin lähettää asiakkaalle identiteettinsä tiedot digitaalisessa varmenteessa. Varmenne sisältää useimmiten palvelimen nimen, luotetun varmentajan ja palvelimen julkisen salausavaimen.
- Asiakas saattaa ottaa yhteyttä palvelimeen, joka myönsi varmenteen ja varmistaa, että varmenne on pätevä ennen eteenpäin jatkamista.
- Luodakseen istunnon avaimet suojattua yhteyttä varten asiakas kryptaa satunnaisen numeron yhdessä palvelimen julkisen avaimen kanssa ja lähettää lopputuloksen palvelimelle. Vain palvelimen pitäisi osata purkaa salaus yksityisellä avaimellaan.
- Satunnaisen numeron avulla kummatkin osapuolet luovat avainmateriaalin jolla he salaavat ja purkavat tiedon.

Kättely päättyy ja salattu yhteys alkaa käyttäen aiemmin muodostettua avainmateriaalia, kunnes yhteys suljetaan. Mikäli yksikin ylemmistä kohdista epäonnistuu, kättelykin epäonnistuu ja yhteyttä ei muodosteta. Kättelyn jälkeen sovellus voi aloittaa yhteydenpidon turvattuna SSL-yhteydellä tietueyhteyskäytännön hoitaessa tarvittavista toimenpiteistä. (5.)



4 TESTIYMPÄRISTÖ JA LAITTEISTO

Testiympäristönä käytettiin Kymenlaakson ammattikorkeakoulun tietotekniikan laboratorion tiloja ja Cisco ASA-palomuurilaite kytkettiin tuotantoverkkoon Lohi-nimiselle kytkimelle, jolloin ASA-palomuuriin saatiin yhteys julkisesta Internetistä. SQL- ja Remote-palvelimet perustettiin tietotekniikan laboratorion Vsphere-palvelimelle virtuaalisena. Etätietokone otti SQL-palvelimen tietokantaan yhteyden Mill-Planner-ohjelmalla ja Remote-palvelimen kautta Simunet-laboratorion verkkolaitteiden etäkäyttö-palvelimiin yhteyden Teraterm Pro-ohjelmalla.

4.1 Laitteisto

Testiympäristön laitteet olivat tietotekniikan laboratorion tilojen laitteita, jotka varattiin tai joista varattiin osia testiä varten. Lohi-kytkimeen (VLAN 40, 123, 125, 131, 201) kytketyn Cisco ASA-palomuurilaitteen julkinen IP-osoite oli 193.167.58.126 (VLAN 123) ja sisäinen IP-osoite oli 192.168.201.1 (VLAN 201). SQL-palvelin oli laboratorion Vsphere-palvelimelle asennettu virtuaalinen Windows Server 2003 ja sen IP-osoite oli 192.168.201.2 (VLAN 201). Remote-palvelin oli myös Vsphere-palvelimelle asennettu, käyttöjärjestelmänä CentOS ja IP-osoite oli 192.168.201.3 (VLAN 201). Reititin- ja kytkinryhmän, johon Remote-palvelin otti yhteyttä, IP-osoitteet olivat 192.168.58.161-165 (VLAN 131).

4.2 Cisco ASA

Cisco ASA on tietoturvalaite, joka sisältää mm. palomuurin, IPS- ja VPN-toiminnot. Cisco ASA-palomuurista on monia erilaisia malleja, jotka sopivat eri tarkoituksiin, kuten 5505, joka sopii kotiin tai pieneen toimistoon, sekä 5580-40, joka on sopiva suuren yrityksen pääkonttoriin. Opinnäytetyössä käytetty malli oli 5510, joka on taloudellinen vaihtoehto, johon saa lisämoduuleilla erilaisia toimintoja, kuten IPS-toiminnon AIM-SSM moduulilla tai antivirustoiminnon CSC SSM-moduulilla. Laitteita voi tarvittaessa klusteroida, jolloin yhtäaikaisten VPN-käyttäjien määrä kasvaa. Alla on lyhyt listaus ominaisuuksista.

Kuva 1: Cisco ASA 5510

Ominaisuus	**Kuvaus**
Palomuurin nopeus	Jopa 300 Mb/s
Maks. palomuurin ja IPS:n nopeus	• Jopa 150 Mb/s AIP SSM-10:n kanssa • Jopa 300 Mb/s AIP SSM-20:n kanssa
VPN nopeus	Jopa 170 Mb/s
Yhtäaikaiset istunnot	50,000; 130,000*
IPsec VPN yhtäaikaiset käyttäjät	250
AnyConnect VPN yhtäaikaisten käyttäjien lisenssi-tasot**	2,10, 25, 50, 100, tai 250
Turva konteksti (virtuaalinen palomuuri)	Jopa 5***
Liityntäportit*	5 100Mb/s porttia; 2 1Gb/s porttia + 3 100Mb/s*
Virtuaaliset liityntäportit (VLANit)	50; 100*
Skaalautuvuus*	VPN-klusterointi ja kuorman jakaminen
Korkea saatavuus	Ei tuettu; Aktiivi/Aktiivi****, Aktii-vi/Valmiustila*

* Päivitys mahdollinen Cisco ASA 5510 Security Plus lisenssillä

** Erikseen ostettava lisensoitu toiminto; kaksi sisältyy peruslaitteeseen

*** Erikseen ostettava lisensoitu toiminto; kaksi sisältyy Cisco ASA 5510 Security Plus lisenssiin

**** Saatavana palomuuritoimintoversioon

ASA-palomuurin pystyy konfiguroimaan sekä IOS–ohjelmistolla CLI komentoriviltä, että graafisella ASDM-ohjelmistolla, jolla pystyy helposti konfiguroimaan ASA-palomuurin sekä seuraamaan lokeja ja prosessorin käyttöastetta jne. (6.)

4.3. Asiakasyhteydetön SSL VPN

Cisco ASA-palomuurin tarjoama Clientless SSL VPN toimii selaimen päällä, eikä vaadi minkäänlaista asiakasohjelmaa. Clientless SSL VPN sopii tilanteisiin, joissa käyttäjän pitää päästä käsiksi yrityksen resursseihin, mutta päätteellä ei voi ajaa SSL VPN-asiakasohjelmaa. Nämä käyttäjät saattavat ottaa yhteyden jaetulta työasemalta tai jopa hotellin tai muun julkisen laitoksen päätteeltä. (Jazib Frahim, Qiang Huang, 114)

Portaalin voi räätälöidä tarpeen mukaisesti ja sivuille voi luoda kirjainmerkkejä. Clientless SSL VPN-yhteyksien tietoturvaa voi parantaa web-pääsylistoilla, joilla hallitaan verkon eri liikennettä, kuten web, telnet, ssh, citrix, ftp, tiedosto- ja sähköpostipalvelimet tai muun tyyppistä liikennettä. Nämä pääsylistat vaikuttavat vain Clientless SSL VPN-yhteyksiin. (1, 152-153.)

4.4 Älykäs tunneli

Älykäs tunneli on yhteys sovelluksen ja etäverkon välillä käyttäen web-selainpohjaista SSL VPN-istuntoa, jossa Cisco ASA-palomuuri toimii yhdyskäytävänä ja välityspalvelimena. Älykkään tunnelin pystyy konfiguroida päästämään tiettyjä sovelluksia ja tietyllä tiedostopolulla sekä tarkistamaan SHA-1-tiivisteen ennen yhteyden avaamista. Älykkäälle tunnelille voi konfiguroida politiikat ja rajoitukset ja se tukee myös tunnelin jakamista, jolloin tietyn IP-osoitteen omaavat paketit lähetetään tunnelissa palomuurilaitteelle ja edelleen kohdekoneelle ja loput paketit lähetetään tunnelin ulkopuolelta normaaleja reittejä pitkin maailmalle. Älykkäällä tunnelilla on omat rajoituksensa. Se toimii kaikkien x86 ja x64 - Windows-käyttöjärjestelmien sekä Mac OS X 10.6-käyttöjärjestelmän päällä. Älykäs tunneli tarvitsee toimiakseen myös ActiveX-komponentin tai Javan. (7.)

4.5 Cisco ASA -konfiguraatio

Tietotekniikan laboratorion kytkinlaitekaapin Lohi-kytkimessä oli vain yksi liityntäportti vapaana, joten ASA-palomuurissa käytettiin vain yhtä liityntäporttia, jossa oli sekä julkisen verkon (lohi VLAN 123) aliliityntäportti että sisäverkon (VLAN 201) aliliityntäportti. Cisco ASA-palomuuri konfiguroitiin Clientless SSL VPN-yhteyttä varten konsolin kautta komentoriviltä ja kirjainmerkkilista lisättiin Cisco Adaptive Security Device Manager (ADSM)-ohjelman avulla.

4.5.1 CLI komennot

ASDM-valmius täytyi laittaa päälle, sillä kirjanmerkit pystyi konfiguroimaan vain sen avulla. ASDM-yhteys sallittiin SQL-palvelimen IP-osoitteelle.

```
ciscoasa(config)#http server enable
ciscoasa(config)#http 192.168.201.2 255.255.255.255 VPN-inside
```

Varmenne täytyi tehdä itse, sillä opinnäytetyötä varten ei hankittu virallista varmennetta. Itsekirjoitettu varmenne ei haitannut laboratorio-olosuhteissa.

```
ciscoasa(config)#crypto key generate rsa label "kirjoita tähän jokin uniikki"
ciscoasa(config)#crypto ca trustpoint ASDM_TrustPoint0
ciscoasa(config-ca-trustpoint)#enrollment self
ciscoasa(config-ca-trustpoint)#subject-name CN=sslvpn.ciscoasa.com
ciscoasa(config-ca-trustpoint)#keypair sslvpnkeypair
ciscoasa(config-ca-trustpoint)#crypto ca enroll ASDM_TrustPoint0 noconfirm
ssl encryption aes128-sha1 aes256-sha1 3des-sha1
ciscoasa(config)# ssl trust-point ASDM_TrustPoint0 lohi
```

Asiakasyhteydetön SSL VPN-yhteyskäytäntö sallittiin julkiselle liityntäportille.

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable lohi
ciscoasa(config-webvpn)#exit
```

Remote-palvelimen täytyi päästä toiseen verkkoon, joten sille luotiin PAT-käännös, jolla sen yksityinen IP-osoite käännettiin ASA-palomuurin julkiseksi osoitteeksi. Tämän lisäksi lisättiin neljän nollan reitti tietotekniikan laboratorion yhdyskäytävän IP-osoitteeseen.

```
ciscoasa(config)#nat-control
ciscoasa(config)#global (lohi) 1 interface
ciscoasa(config)#nat (VPN-inside) 1 192.168.201.3 255.255.255.255
ciscoasa(config)#route lohi 0.0.0.0 0.0.0.0 193.167.58.1 1
```

WebVPN-tunneliryhmä määritti politiikan SSL VPN-yhteyskäytännön käyttöön.

```
ciscoasa(config)#tunnel-group TestiVPN type remote-access
ciscoasa(config-tunnel-webvpn)#group-alias mill-Planner enable
ciscoasa(config-tunnel-webvpn)#exit

ciscoasa(config)#tunnel-group Remote type remote-access
ciscoasa(config-tunnel-webvpn)#group-alias remote enable
ciscoasa(config-tunnel-webvpn)#exit

ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
```

Luotiin ryhmäpolitiikka SSL VPN-yhteyskäytännön käyttäjille ja sidottiin se tunneli-ryhmään.

```
ciscoasa(config)#group-policy mill-planner internal
ciscoasa(config)#group-policy mill-planner attributes
iscoasa(config-group-policy)#vpn-tunnel-protocol  svc webvpn
ciscoasa(config-group-policy)#group-lock value TestiVPN
ciscoasa(config-group-policy)#exit

ciscoasa(config)#group-policy remote internal
ciscoasa(config)#group-policy remote attributes
iscoasa(config-group-policy)#vpn-tunnel-protocol svc webvpn
ciscoasa(config-group-policy)#group-lock value Remote
ciscoasa(config-group-policy)#exit
```

Luotiin Mill-Planner-ohjelman käyttäjät, jotka sidottiin oikeaan ryhmäpolitiikkaan sekä tunneliryhmään. Alla olevan lisäksi vielä tarpeeksi monta mill-käyttäjää, tyyliin mill2, mill3 jne.

```
ciscoasa(config)#username mill1 password "salasana" privilege 0
ciscoasa(config)#username mill1 attributes
ciscoasa(config-username)#vpn-group-policy mill-planner
ciscoasa(config-username)#group-lock value TestiVPN
ciscoasa(config-username)#service-type remote-access
ciscoasa(config-username)#exit
```

Luotiin myös kaksi Remote-palvelimen käyttäjää, jotka sidottiin omaan ryhmäpolitiikkaansa.

```
ciscoasa(config)#username remote1 password "salasana" privilege 2
ciscoasa(config)#username remote1 attributes
ciscoasa(config-username)#vpn-group-policy remote
ciscoasa(config-username)#group-lock value Remote
ciscoasa(config-username)#exit

ciscoasa(config)#username remote2 password "salaista" privilege 2
ciscoasa(config)#username remote2 attributes
ciscoasa(config-username)#vpn-group-policy remote
ciscoasa(config-username)#group-lock value Remote
ciscoasa(config-username)#exit
```

Konfiguroitiin älykäs tunneli sekä Mill-Planner-ohjelmalle, että teratermpro ohjelmalle.

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#smart-tunnel list mill-Planner mill-Planner mill-planner.exe platform windows
ciscoasa(config-webvpn)# smart-tunnel list teratermpro teraterm ttermpro.exe platform windows
ciscoasa(config-webvpn)#exit
ciscoasa(config)#group-policy mill-planner attributes
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)#smart-tunnel auto-start mill-Planner
ciscoasa(config-group-webvpn)#exit
ciscoasa(config-group-policy)#exit

ciscoasa(config)#group-policy remote attributes
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)#smart-tunnel auto-start teratermpro
ciscoasa(config-group-webvpn)#exit
```

Myös tunneliryhmät täytyi yhdistää ryhmäpolitiikkaan , jotta ne eivät käyttäisi oletusryhmäpolitiikkaa.

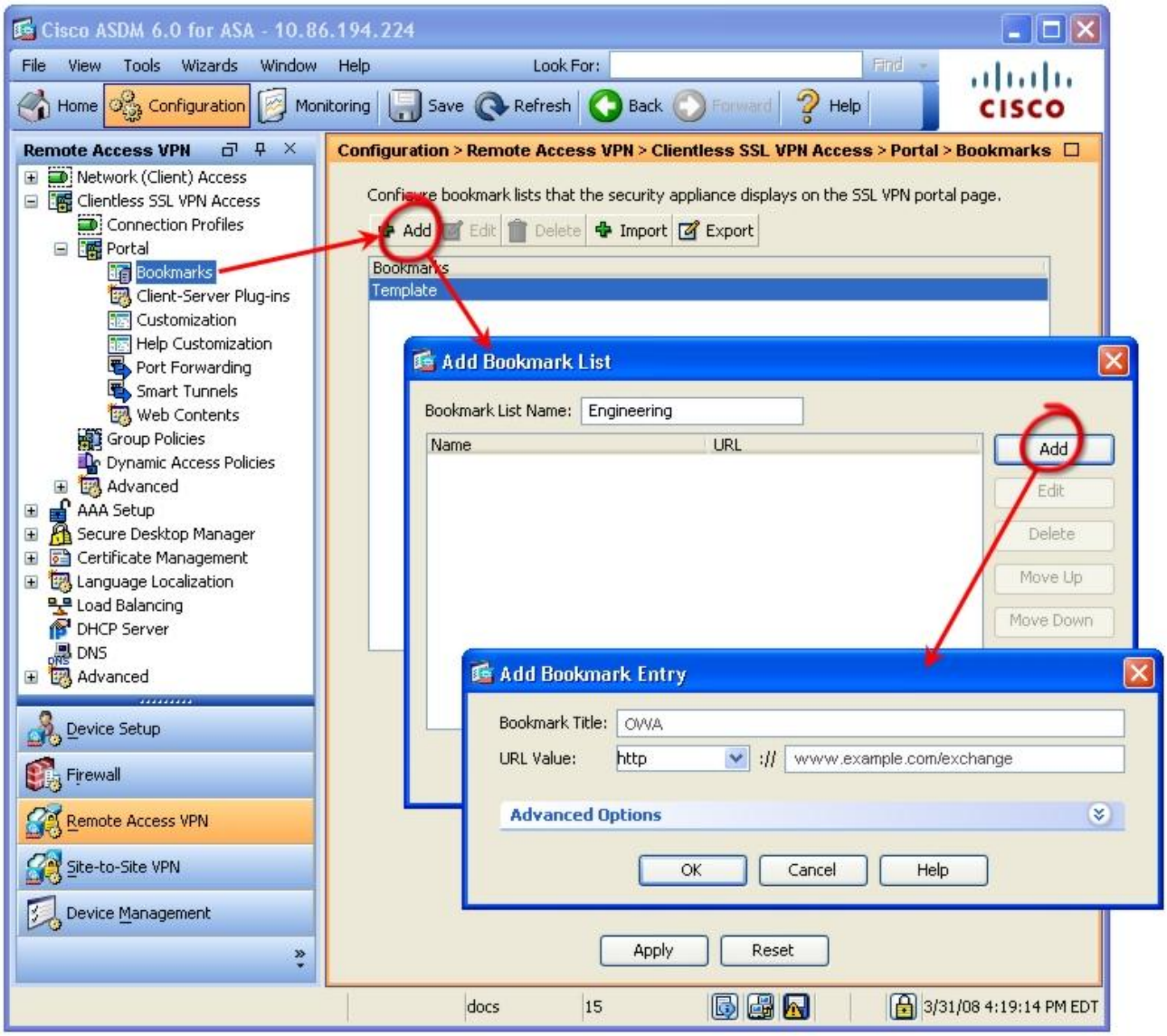
```
ciscoasa(config)#tunnel-group TestiVPN general-attributes
ciscoasa(config-tunnel-general)#default-group-policy mill-planner
ciscoasa(config-tunnel-general)#exit

ciscoasa(config)#tunnel-group Remote general-attributes
ciscoasa(config-tunnel-general)#default-group-policy remote
ciscoasa(config-tunnel-general)#exit
```

Näiden komentojen lisäksi tehtiin objektiryhmä etäkäyttö-palvelimille ja nimipalvelimelle. Pääsylistat luotiin, jotta palomuuri päästi laitteet keskustelemaan keskenään. Sallittiin myös objektiryhmän NAT-muunnos ja kulku sekä tehtiin WebACL Mill-Planner –ryhmälle. (8.)

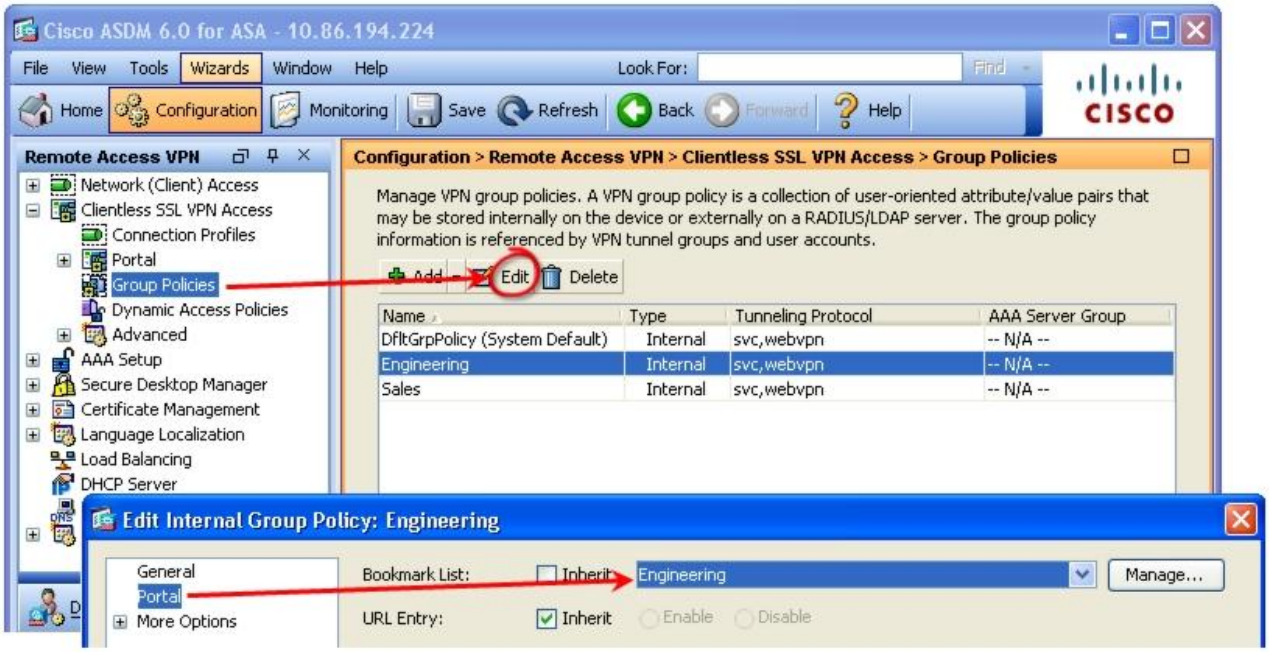
4.5.2 Kirjanmerkin lisääminen ASDM-ohjelmalla

SQL-palvelimelta otettiin selaimella yhteys ASA-palomuuriin ja asennettiin ASDM-ohjelma. Tämän jälkeen mention Configuration-lehdelle. Valittiin Remote Access VPN -> Clientless SSL VPN -> Portal -> Bookmarks. Klikattiin Add, nimeksi remote ja klikattiin Add ja kirjoitettiin remote_simunet ja osoitteeksi 192.168.201.3.



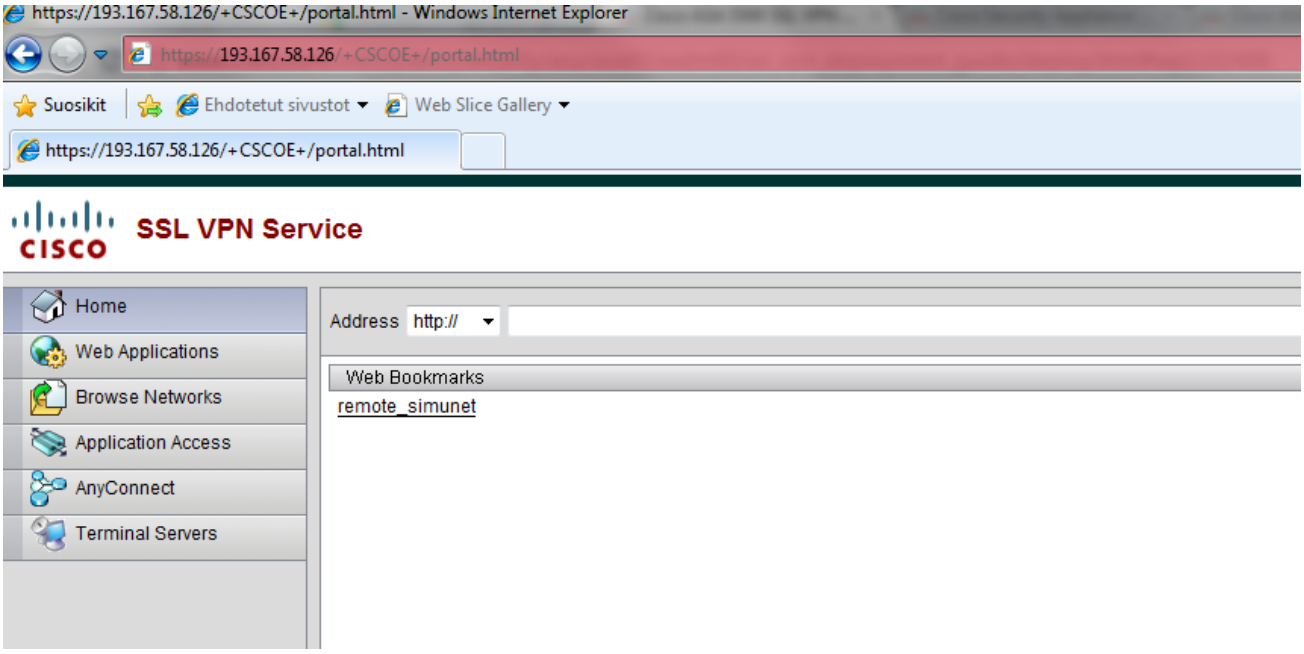
Kuva 2:Esimerkkikuva kirjainmerkistä

Seuraavaksi siirryttiin Clientless SSL VPN Access -> Group Policies -välilehdelle ja klikattiin remote-ryhmää ja edit. Portal-lehdellä valittiin kirjainmerkiksi aiempi remote ja klikattiin ok. (9.)



Kuva 3: Esimerkkikuva kirjainmerkin yhdistämisestä

Alla kuva kirjainmerkistä, joka vei remote-käyttäjät hallintaohjelman sivuille.

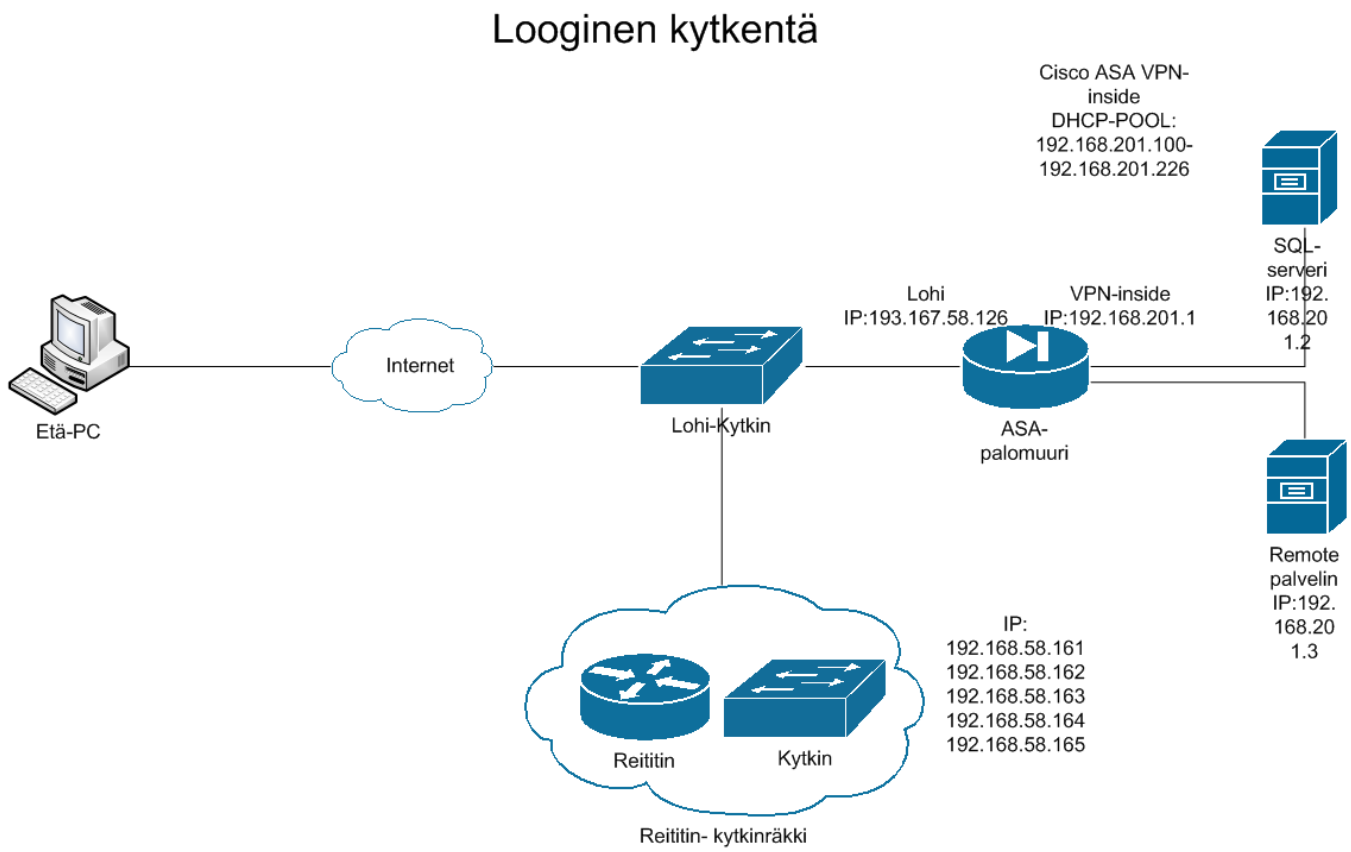


Kuva 4: Esimerkki kirjainmerkistä ASAn osoitteessa

Tässä vaiheessa Cisco ASA-palomuurin konfigurointi oli valmis ja ohjelmat valmiita käyttöön.

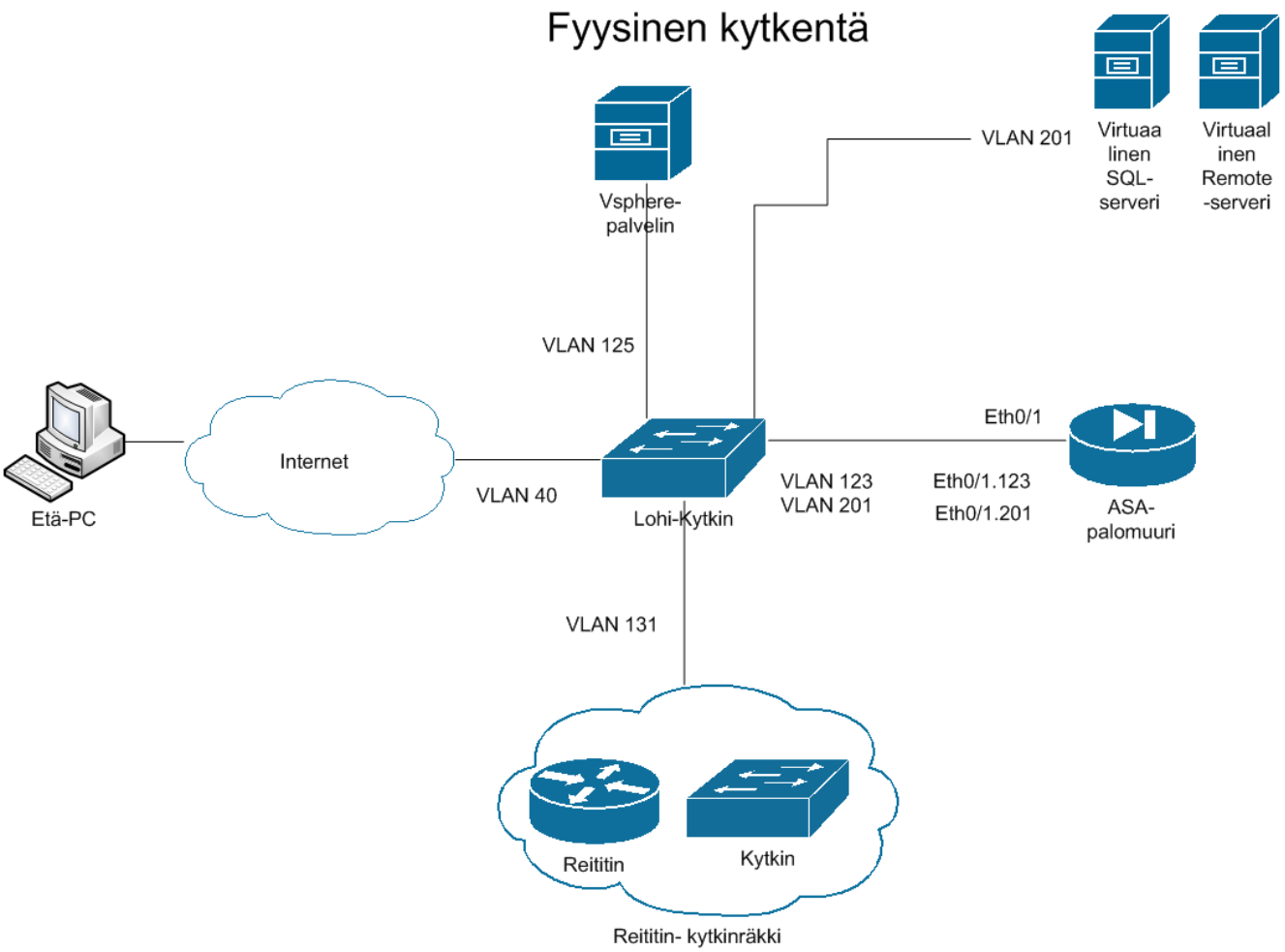
4.6 Looginen ja fyysinen kytkentä

Cisco Asa-palomuurilaite oli sijoitettu laboratorion verkkolaitetilaan, jossa se toimi palomuurina ja VPN-yhdyskäytävänä palvelimille. Kuvasta 5 näkyy testiympäristön looginen kytkentä. Etätietokone otti yhteyden ASA-palomuurilaitteeseen, joka ohjasi etätietokoneen sallituille kohteille.



Kuva 5: Looginen kytkentä

Kuvasta 6 näkyy testiympäristön fyysinen kytkentä. Fyysisesti ASA-palomuuri oli yhdistetty Lohi-kytkimeen yhdellä verkkokaapelilla ja liityntäporttiin oli konfiguroitu kaksi aliliityntäporttia, julkinen ja sisäinen. Kun käyttäjä oli onnistuneesti avannut Clientless SSL VPN-yhteyden ASA-palomuuriin, ohjasi se käyttäjän verkon muihin sallittuihin osiin.



Kuva 6: Fyysinen kytkentä

Sekä SQL- että Remote-palvelin toimivat sisäverkon VLANissa 201, johon pääsi käsiksi vain ASA-palomuurin kautta. Clientless SSL VPN-yhteys muodostettiin avaamalla web-selain etätietokoneella ja yhdistämällä ASA-palomuurin julkiseen IP-osoitteeseen porttiin 443 (https://193.167.58.126). Kirjautumissivulla valittiin ryhmä, jonka jälkeen kirjoitettiin käyttäjänimi ja salasana. Aloitussivu käyttäytyi sen mukaan, millä ryhmällä oli sisään kirjauduttu.

4.7 Etäyhteys Mill-Planner-ohjelmalla

Kun käyttäjä kirjautui ASA-palomuurin kirjautumissivulle sisään Mill-Planner-ryhmään oikeilla tunnuksilla, aloitussivulla käynnistyi automaattisesti älykäs tunneli joko ActiveX kontrollin tai Javan päälle, jonka läpi Mill-Planner-ohjelma ottaisi yhteyden SQL-palvelimeen. Käyttäjä käynnisti Mill-Planner-ohjelman ja antoi Efficiency tietokanta-asetuksiin SQL-palvelimen osoitteen 192.168.201.2, tietokannan nimeksi mill-planner, käyttäjätunnus: sa ja salasana: srv. Käyttäjän hyväksyessä muutokset, tuli

vastaan yhteensopimattomuusongelma. Mill-Planner-ohjelma ei mennyt älykkääseen tunneliin, joten ASA-palomuuri esti ohjelman yhteydenoton. Ongelman sai kierrettyä käynnistämällä Mill-Planner-ohjelman ensin, minkä jälkeen kirjauduttiin ASA-palomuuriin, aloitettiin SSL VPN-yhteys ja älykäs tunneli käynnistyi automaattisesti. Tällöin myös Mill-Planner-ohjelma kulki älykkäässä tunnelissa. Mill-Planner-ohjelma otti yhteyden palvelimeen älykkään tunnelin avulla ja kysyi tietokannan käyttäjätunnusta ja salasanaa. Oikeiden tunnusten antamisen jälkeen Mill-Planner-ohjlema käynnistyi ja tiedonsiirto ja hakujen tekeminen SQL-tietokannasta onnistui aivan kuin paikallisella yhteydellä. Kunhan käyttäjä ei sulkenut web-selainta, suojattu yhteys oli auki.

4.8 Etäyhteys Remote-hallintaohjelmaan

Kun käyttäjä kirjautui kirjautumissivulle sisään Remote-ryhmään oikeilla tunnuksilla, aloitussivulla oli kirjainmerkki remote_simunet, jolla käyttäjä ohjattiin Remote-palvelimen osoitteeseen 192.168.201.3 porttiin 80. Remote-palvelimen hallintaohjelmalla käyttäjä pystyi ohjaamaan Simunet-laboratorion etäkäyttö-palvelimia ja antamaan niille tiettyjä käskyjä. Hallintaohjelmassa oli myös linkit suoraan etäkäyttö-palvelimien osoitteisiin ja oikeisiin portteihin, joiden avulla käyttäjä pystyi käynnistämään Teraterm Pro-ohjelmalla telnet-yhteyden tiettyyn verkkolaitteeseen ja konfiguroimaan sitä suoraan.

Remote-palvelimelle oli annettu pääsylista, jotta se pystyi antamaan käskyjä Simunet-laboratorion etäkäyttö-palvelimille. Kun käyttäjä käytti Remote-palvelimen hallintaohjelmaa ja Remote-palvelin antoi käskyjä etäkäyttö-palvelimille, ne keskustelivat selkokielisenä pääsylistojen avulla keskenään, eikä käyttäjän etäyhteys häirinnyt niiden toimenpiteitä. Kun käyttäjä valitsi Remote-palvelimen hallintaohjelmassa linkin etäkäyttö-palvelimen tiettyyn porttiin avaten telnet-yhteyden tietyn verkkolaitteen kanssa, tieto kulki selkokielisenä ASA-palomuurilta etäkäyttö-palvelimelle ja takaisin. Käyttäjän SSL VPN-yhteys oli salattua ASA-palomuuriin saakka, jolloin telnet-yhteys oli pakattu salatun putken sisään, mutta ASA-palomuurilta eteenpäin sisäverkkoon putki päättyi, joten sisäverkon laitteet tukivat yhteyksiä suoraan.

5 KAISTANKÄYTTÖ JA TULOKSET MILL-PLANNER-OHJELMALLA

Tärkeä osa opinnäytetyötä oli tutkia, paljonko Mill-Planner-ohjelma vei kaistaa SSL VPN-yhteydellä. Tulokset otettiin ylös Cisco ASA-palomuurin omalla monitorointityökalulla. Sekä sisäisen, että ulkoisen verkon liityntäportteja seurattiin ja kummastakin otettiin ylös tavujen määrä, pakettien määrä, paketteja/sekunti ja bittejä/sekunti.

Testihenkilö otti yhteyden ASA-palomuuriin ja aloitti SSL VPN-yhteyden. Tämän jälkeen tiedonsiirron taltioiminen aloitettiin ja Mill-Planner-ohjelmalla haettiin tietokannasta tietoja. Tietoliikenteen määrä tallennettiin lokeihin (kts. liite 8.2).

Kaistankäyttötestin alussa julkisen liityntäportin kilotavujen määrä oli 353 Kt sisään ja 595 Kt ulos. Testin lopussa luvut olivat 467 Kt ja 1452 Kt. Yksityisen liityntäportin kilotavujen määrä oli alussa 772 Kt sisään ja 16947 Kt ulos sekä lopussa 1344 Kt ja 17057 Kt. Näitä tuloksia tarkastelemalla pääteltiin, että kaistankäyttö on vähäistä testin aikana. SSL VPN-tunnelin läpi kulki käyttäjältä palvelimelle 114 Kt liikennettä ja palvelimelta käyttäjälle 857 Kt. Yksityisen liityntäportin läpi kulki käyttäjältä palvelimelle 110 Kt liikennettä ja palvelimelta käyttäjälle 572 Kt. SSL VPN-yhteys selvästi lisää tiedonsiirron määrää overhead-kuormituksen muodossa n. 50% palvelimelta käyttäjälle, mutta absoluuttinen tiedonsiirron määrän lisäys siitä huolimatta pieni, 4 Kt käyttäjältä palvelimelle ja 285 Kt palvelimelta käyttäjälle.

Toinen hyödyllinen kuvaaja oli bittien määrä sekunneissa. Testin aikana suurimmat piikit tulivat ajassa 0:8:18:23, jolloin SSL VPN-tunnelin läpi kulki käyttäjältä palvelimelle 27 Kb/s ja palvelimelta käyttäjälle 219 Kb, sekä ajassa 0:8:18:43, jolloin SSL VPN-tunnelin läpi kulki käyttäjältä palvelimelle 9 Kb ja palvelimelta käyttäjälle 231 Kb/s. Näistä tuloksista pääteltiin, että tiedonsiirto on vähäistä myös testin tiedonsiirtojen piikkien aikana. Käyttäjältä palvelimelle siirrettävän tiedon suurin piikki 27 Kb/s on kilotavuiksi käännettynä 3.375 Kt tai n. 0.0033Mt/s. Palvelimelta käyttäjälle siirrettävän tiedon suurin piikki 231 Kb/s on kilotavuiksi käännettynä 28.875 Kt/s tai n.0.028 Mt/s.

Näiden tulosten perusteella todettiin, että kaistankäyttö on todella pientä ja useampikin käyttäjä olisi voinut työskennellä yhtäaikaisesti SSL VPN-tunnelin läpi etänä. Tiedonsiirron määrä oli niin vähäistä, että mikä tahansa nykyaikainen laajakaista riittää. Esi-

merkiksi hidaskin 1 Mb/s-laajakaista riittää ainakin neljän yhtäaikaisen käyttäjän etäkäyttöön.

Testituloksia ei kuitenkaan voinut soveltaa suoraan kaikkiin tilanteisiin, sillä SQL-palvelimen tietokanta oli näyteversio, joka ei välttämättä vastannut oikeaa tuotantoversiota, jolloin tiedonsiirron määrä olisi voinut olla suurempaa.

6 YHTEENVETO

SSL VPN-yhteyskäytäntö toimi odotusten mukaisesti ja on erittäin kypsä ja helppo käyttää. Cisco ASA-palomuurin konfigurointi SSL VPN-yhteyskäytäntöä varten onnistui helposti CLI-komentoriviltä ja tarvittaessa olisi onnistunut myös täysin ASDM-ohjelmistolla, joka oli käyttäjäystävällisempi kuin komentorivi.

Opinnäytetyön tärkein tavoite, Mill-Planner-ohjelman kaistankäytön tarkastelu SSL VPN-tunnelissa, saavutettiin. Absoluuttinen kaistankäyttö oli vähäistä, mutta SSL VPN-yhteyskäytäntö vei lisää kaistaa testin aikana suurimmillaan n.50 % salaamattomaan liikenteeseen verrattuna.

Opinnäytetyön toinen tavoite, Remote-palvelimen etähallinta samoilla tekniikoilla ja menetelmillä, saavutettiin myös. Laitteet saatiin keskustelemaan keskenään ja Simunet-laboratorion laitteita voitiin hallita etänä ASA-palomuurin avulla turvallisesti.

Ongelmitta opinnäytetyön tekemisessä ei päästy. Ratkaisemattomaksi jäi ongelma, jossa Mill-Planner-ohjelma ei toiminut älykkäässä tunnelissa, mikäli SSL VPN-istunnon käynnisti ennen Mill-Planner-ohjelmaa. Ongelma jouduttiin kiertämään käynnistämällä Mill-Planner-ohjelma ennen SSL VPN-istuntoa. Toinen ongelma oli tarvittavan testiryhmän saaminen. Alun perin oli suunniteltu, että kaistankäyttötestiä varten kokonainen testiryhmä käyttää Mill-Planner-ohjelmaa etänä ja tulokset otetaan tarkasteluun. Käytännön järjestelyt kuitenkin estivät tämän, joten kaistankäyttötesti suoritettiin yhden testihenkilön voimin tietotekniikan laboratoriotiloissa.

Opinnäytetyön aihe oli melko suppea ja helppo toteuttaa konfiguroimisen ja käyttöönoton kannalta, mutta jo esitetyt ongelmat veivät paljon aikaa. Ohjeita ja oppaita löytyi tarvittaessa kiitettävästi. Koko prosessi antoi minulle hyvin kokemusta etäyhteyksien suunnittelusta ja toteuttamisesta.

LÄHTEET

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

2. Krawczyk, H, Bellare, M & Canetti, R . 1997. HMAC: Keyed-Hashing for Message Authentication. Saatavissa: http://tools.ietf.org/html/rfc2104 [viitattu 15.2.2011]

3. History of SSL. saatavissa: http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzain/rzainhistory.htm [viitattu 19.2.2011]

4. SSL/TLS Scenarios. Saatavissa: http://technet.microsoft.com/en-us/library/cc779109(WS.10).aspx [viitattu 19.2.2011]

5. Overview of SSL/TLS Encryption. Saatavissa: http://technet.microsoft.com/en-us/library/cc781476(WS.10).aspx [viitattu 19.2.2011]

6. Cisco ASA 5500 Series Adaptive Security Appliances. Saatavissa: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html [viitattu 20.2.2011]

7. ASA: Smart Tunnel using ASDM Configuration Example. Saatavissa: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080affd2d.shtml [viitattu 20.2.2011]

8. Cisco ASA 5500 Series Configuration Guide using the CLI 8.2; Configuring Clientless SSL VPN. saatavissa: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/webvpn.html [viitattu 22.2.2011]

9. Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x. Saatavissa: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html [viitattu 22.2.2011]

Liite 1

Cisco ASA -konfiguraatio

```
ASA Version 8.2(2)

hostname ciscoasa
domain-name ciscoasa.com
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet0/1
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1.123
 vlan 123
 nameif lohi
 security-level 0
 ip address 193.167.58.126 255.255.255.128
!
interface Ethernet0/1.201
 vlan 201
 nameif VPN-inside
 security-level 100
 ip address 192.168.201.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
```

```
 ip address 192.168.1.1 255.255.255.0
 management-only
!
ftp mode passive
clock timezone GMT 0
dns domain-lookup management
dns server-group DefaultDNS
 domain-name ciscoasa.com
object-group network comserver
 network-object host 193.167.58.161
 network-object host 193.167.58.162
 network-object host 193.167.58.163
 network-object host 193.167.58.164
 network-object host 193.167.58.165
object-group network DM_INLINE_NETWORK_1
 network-object host 193.167.58.2
 group-object comserver
access-list no_nat extended permit ip host 192.168.201.2 192.168.10.0 255.255.255.0
access-list no_nat extended permit ip 192.168.10.0 255.255.255.0 host 192.168.201.2
access-list split-tunnel standard permit host 192.168.201.2
access-list split-tunnel_remote standard permit host 192.168.201.3
access-list VPN-inside_access_in extended permit ip host 192.168.201.3 object-group
DM_INLINE_NETWORK_1
access-list mill-planner webtype permit url smart-tunnel://192.168.201.2 log default
access-list mill-planner webtype deny url any log default
pager lines 24
logging enable
logging asdm informational
mtu lohi 1500
mtu management 1500
mtu VPN-inside 1500
ip local pool vpnpool 192.168.10.2-192.168.10.254 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat-control
global (lohi) 1 interface
nat (VPN-inside) 1 192.168.201.3 255.255.255.255
access-group VPN-inside_access_in in interface VPN-inside
route lohi 0.0.0.0 0.0.0.0 193.167.58.1 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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 management
```

```
http 192.168.201.2 255.255.255.255 VPN-inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=sslvpn.ciscoasa.com
 keypair asa_ictlabra
 crl configure
crypto ca certificate chain ASDM_TrustPoint0
 certificate 435fe64c
    308201ff 30820168 a0030201 02020443 5fe64c30 0d06092a 864886f7 0d010105
    05003044 311c301a 06035504 03131373 736c7670 6e2e6369 73636f61 73612e63
    6f6d3124 30220609 2a864886 f70d0109 02161563 6973636f 6173612e 63697363
    6f617361 2e636f6d 301e170d 31303131 31393131 32383033 5a170d32 30313131
    36313132 3830335a 3044311c 301a0603 55040313 1373736c 76706e2e 63697363
    6f617361 2e636f6d 31243022 06092a86 4886f70d 01090216 15636973 636f6173
    612e6369 73636f61 73612e63 6f6d3081 9f300d06 092a8648 86f70d01 01010500
    03818d00 30818902 818100be 07b17fd3 3e0c8794 e568242b 61c786c1 f46c7b0f
    1fa3173a 43e677b6 cb9af5cb a7366046 956aa2a3 07d9e130 614d4731 ff31bf53
    c5a7ea1e b01f7120 45ad0e48 3d9e34eb 21775373 fdaccdb7 5df40770 fcfe45cb
    e4b72b9e 5bca9ceb 2c1d5b67 351b883a dae1a75e 1d70c05e 3ef70498 67dc1040
    8dba881b 4db8f327 8e120302 03010001 300d0609 2a864886 f70d0101 05050003
    81810049 48a9c588 02f1df8a 07dee983 a246d724 4163c861 9a51df32 9c6397a8
    8da135ec 6d72f3af 39d1b66b c210a3d4 d0451bc3 26e596f7 7c90e55e 09495993
    f4154c42 04c60982 9424f565 0a3c2b12 6a764320 0be84922 6e917ff8 664bc68b
    539a84e0 f39f03a4 e6ca7612 ab1d6044 b9b9b7c4 43d0f2b2 2fd2feb8 873a3bdc
aa6073
  quit
telnet 192.168.1.0 255.255.255.0 management
telnet 192.168.201.2 255.255.255.255 VPN-inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl encryption aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 lohi
webvpn
 enable lohi
 svc image disk0:/anyconnect-dart-win-2.5.0217-k9.pkg 1
 svc enable
 tunnel-group-list enable
 smart-tunnel list mill-planner mill-planner Mill-Planner.exe platform windows
```

```
 smart-tunnel list teratermpro teraterm ttermpro.exe platform windows
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec
group-policy mill-planner internal
group-policy mill-planner attributes
 vpn-tunnel-protocol webvpn
 group-lock value TestiVPN
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-tunnel
 address-pools value vpnpool
 webvpn
  url-list none
  filter value mill-planner
  smart-tunnel auto-start mill-planner
group-policy remote internal
group-policy remote attributes
 vpn-tunnel-protocol svc webvpn
 group-lock value Remote
 address-pools value vpnpool
 webvpn
  url-list value remote
  svc keep-installer installed
  svc ask none default webvpn
  smart-tunnel auto-start teratermpro
username mill8 password aNejcJ1yokEi56aa encrypted
username mill8 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill9 password aNejcJ1yokEi56aa encrypted
username mill9 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill4 password aNejcJ1yokEi56aa encrypted
username mill4 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill5 password aNejcJ1yokEi56aa encrypted
username mill5 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill6 password aNejcJ1yokEi56aa encrypted
username mill6 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill7 password aNejcJ1yokEi56aa encrypted
```

```
username mill7 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill10 password aNejcJ1yokEi56aa encrypted
username mill10 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill1 password aNejcJ1yokEi56aa encrypted
username mill1 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill2 password aNejcJ1yokEi56aa encrypted
username mill2 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username mill3 password aNejcJ1yokEi56aa encrypted
username mill3 attributes
 vpn-group-policy mill-planner
 group-lock value TestiVPN
 service-type remote-access
username remote1 password vDhvl/bydnvugSDx encrypted
username remote1 attributes
 vpn-group-policy remote
 group-lock value Remote
username remote2 password Zwxhy9a1NElv/3j. encrypted
username remote2 attributes
 vpn-group-policy remote
 group-lock value Remote
tunnel-group TestiVPN type remote-access
tunnel-group TestiVPN general-attributes
 address-pool vpnpool
 default-group-policy mill-planner
tunnel-group TestiVPN webvpn-attributes
 group-alias mill-planner enable
tunnel-group Remote type remote-access
tunnel-group Remote general-attributes default-group-policy remote
tunnel-group Remote webvpn-attributes
 group-alias remote enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
```

```
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:aa935c017c7d31c0f118630441160c93
: end
no asdm history enable
```

Liite 2

Cisco ASA -monitorointi

Cisco ASDM 6.4 for ASA - 192.168.201.1 - Graph (1)

Interface VPN-inside, Byte Counts

"ASA Time (GMT)","Input Byte Count (KB)","Output Byte Count (KB)"

6.4 08:17:33,772,16947
6.4 08:17:43,772,16950
6.4 08:17:53,773,16957
6.4 08:18:03,773,16967
6.4 08:18:13,777,16974
6.4 08:18:23,1038,17013
6.4 08:18:33,1048,17019
6.4 08:18:43,1325,17036
6.4 08:18:53,1344,17051
6.4 08:19:03,1344,17057

Interface VPN-inside, Packet Counts

"ASA Time (GMT)","Input Packet Count (Kpackets)","Output Packet Count (Kpackets)"

6.4 08:17:33,13,23
6.4 08:17:43,13,23
6.4 08:17:53,13,23
6.4 08:18:03,13,23

Interface VPN-inside, Packet Rates

"ASA Time (GMT)","Input Packet Rate (pps)","Output Packet Rate (pps)"

6.4 08:17:33,0,0
6.4 08:17:43,0,0
6.4 08:17:53,1,2
6.4 08:18:03,1,3
6.4 08:18:13,1,3
6.4 08:18:23,21,24
6.4 08:18:33,1,3
6.4 08:18:43,21,22
6.4 08:18:53,3,4
6.4 08:19:03,0,1

Interface VPN-inside, Bit Rates

"ASA Time (GMT)","Input Bit Rate (Kbps)","Output Bit Rate (Kbps)"

6.4 08:17:43,0,2
6.4 08:17:53,0,6
6.4 08:18:03,0,7
6.4 08:18:13,2,5
6.4 08:18:23,209,31
6.4 08:18:33,8,5
6.4 08:18:43,221,13
6.4 08:18:53,15,12
6.4 08:19:03,0,4

Cisco ASDM 6.4 for ASA - 192.168.201.1 - Graph (2)

Interface lohi, Byte Counts

"ASA Time (GMT)","Input Byte Count (KB)","Output Byte Count (KB)"

6.4 08:17:33,353,595
6.4 08:17:43,354,595
6.4 08:17:53,362,615
6.4 08:18:03,397,834
6.4 08:18:13,401,840
6.4 08:18:23,435,1115
6.4 08:18:33,439,1127
6.4 08:18:43,451,1416
6.4 08:18:53,461,1436
6.4 08:19:03,467,1452

Interface lohi, Packet Counts

"ASA Time (GMT)","Input Packet Count (Kpackets)","Output Packet Count (Kpackets)"

6.4 08:17:33,2,2
6.4 08:17:43,2,2
6.4 08:17:53,2,2
6.4 08:18:03,3,3
6.4 08:18:13,3,3
6.4 08:18:23,3,3
6.4 08:18:33,3,3
6.4 08:18:43,3,4
6.4 08:18:53,3,4
6.4 08:19:03,3,4

Interface lohi, Packet Rates

"ASA Time (GMT)","Input Packet Rate (pps)","Output Packet Rate (pps)"

6.4 08:17:33,1,0
6.4 08:17:43,0,0
6.4 08:17:53,5,7

6.4 08:18:03,22,40
6.4 08:18:13,3,3
6.4 08:18:23,22,42
6.4 08:18:33,2,4
6.4 08:18:43,21,36
6.4 08:18:53,3,4
6.4 08:19:03,4,4

Interface lohi, Bit Rates

"ASA Time (GMT)","Input Bit Rate (Kbps)","Output Bit Rate (Kbps)"

6.4 08:17:33,0,0
6.4 08:17:43,0,0
6.4 08:17:53,6,15
6.4 08:18:03,26,175
6.4 08:18:13,3,5
6.4 08:18:23,27,219
6.4 08:18:33,2,10
6.4 08:18:43,9,231
6.4 08:18:53,8,16
6.4 08:19:03,4,12