LAUREA AMMATTIKORKEAKOULU Uuden edellä

SSL VPN –harjoitus tietoverkko-opintoihin

Sederholm, Thomas

2011 Leppävaara

LAUREA AMMATTIKORKEAKOULU Uuden edellä

SSL VPN –harjoitus tietoverkko-opintoihin

Sederholm, Thomas

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

SSL VPN -harjoitus tietoverkko-opintoihin

Thomas Sederholm
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
5, 2011

Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Yritysten tietoverkot

Thomas Sederholm

SSL VPN -harjoitus tietoverkko-opintoihin

Vuosi 2011 Sivumäärä 41

SSL VPN on uudehko tekniikka joka on kovalla vauhdilla korvaamassa aikaisempia VPN -tekniikoita. SSL VPN -yhteyden muodostamista varten ei tarvitse asentaa mitään asiakasohjelmaa vaan se toimii Internet-selaimen kautta. Tämän ansiosta melkein kaikilla tietokoneilla sekä mobiililaitteilla voi muodostaa SSL VPN -yhteyden.

Osana opinnäytetyötä tein SSL VPN -harjoituksen, joka on tarkoitettu käytettäväksi Laurean opiskelijoille. Harjoitus on samankaltainen kuin aiemmin jo käytössä olevat verkkoharjoitukset, kuten reititin-, kytkin- ja WLAN -tukiasemaharjoitukset. Vanhat kytkin- ja reititinharjoitukset toimivat hyvänä oppimispohjana uutta harjoitusta varten. Harjoitusta tullaan käyttämään Laurean tietoliikennelaboratoriossa, jossa opiskelijat saavat suorittaa harjoituksen johonkin opintojaksoon liittyen. Uuden harjoituksen tarkoituksena on laajentaa oppimista kytkimen ja reitittimien peruskonfiguroinnista. Harjoituksen avulla opiskelijat oppivat ymmärtämään SSL VPN -tekniikkaa sekä konfiguroimaan SSL VPN -palvelun Ciscon IOS -käyttöjärjestelmää käyttäen. Harjoituksessa tullaan myös konfiguroimaan ACS -palvelinta Radius protokollaa käyttäen. Laitteistona käytetään Laurean tietoliikennelaboratoriossa olevia Ciscon 2811:n modulaarisia reitittimiä sekä Windows 2000 Server -käyttöjärjestelmän päällä pyörivää Cisco ACS -palvelinta. Työn suorittamiseen menee 30–45 minuuttia ja 12 opiskelijaa voi samanaikaisesti tehdä harjoitusta. Kun yksi ryhmä on saanut harjoituksen tehdyksi, voidaan reitittimet nopeasti nollata alkutilaan, minkä jälkeen toinen ryhmä voi aloittaa harjoituksen tekemisen.

Harjoituksen tarkoituksena on konfiguroida SSL VPN -yhdyskäytävä oman ryhmän reitittimeen. Harjoituksessa käytetään 10.8.4.0 sekä 172.16.0.0 -aliverkkoa. Aliverkoista 10.8.4.0 on laboratoriossa käytössä oleva verkko. Siihen on kytketty kaikki laboratoriossa olevat laitteet. Harjoituksessa 172.16.0.0-aliverkko simuloi Internetiä ja se on konfiguroitu valmiiksi ennen harjoituksen aloittamista. Ryhmät aloittavat reitittimien konfiguroinnin laboratorioverkossa 10.8.4.0 ottamalla yhteyden oman ryhmänsä reitittimeen. Kun laite on saatu valmiiksi konfiguroitua, siirretään oman ryhmän tietokone 172.16.0.0 -aliverkkoon. Tämän jälkeen muodostetaan SSL VPN -yhteys selaimen kautta. Harjoituksen viimeinen vaihe on siirtää tiedosto ryhmän tietokoneelta verkossa olevalle verkkolevylle. Tämä osoittaa, että SSL VPN -yhteys on onnistuneesti muodostettu.

Asiasanat ssl, vpn, harjoitus, cisco

Laurea Leppävaara
Business information technology
Business networks

Thomas Sederholm

SSL VPN exercise for data network studies

Year 2011 Pages 41

SSL VPN is a relatively new technology that is growing in popularity. The SSL VPN technology differs from other VPN technologies in a few ways. The biggest difference is that there's no need to install any software on the client machine. All that is needed to establish a SSL VPN connection is to have web browser that supports SSL cryptography. Most of today's computers and mobile devices are compatible with SSL VPN. This makes SSL VPN accessibility very good. You can connect to your SSL VPN almost from anywhere. The flexibility and amount of devices that can be used with SSL VPN is much larger than with the older VPN technologies like IPSEC.

Part of this thesis is a SSL VPN exercise that was made for student use. It was meant to be used on network courses like the previously created switch and router courses. The exercise has been done in a similar manner as the already existing courses. There's a handout that contains the exercise and it also has all the router commands that are needed to complete the exercise. It might sound too easy to complete with all the commands printed out but it still takes quite a bit of knowledge to complete the exercise without assistance. It takes about 30-45 minutes to complete the exercise. It is meant to be done in pairs so as there are 6 routers there can be 12 students simultaneously working on the exercise. It doesn't take more than 5 minutes to reset the hardware back to its original state after a group of students have completed the exercise. This enables a lot of students to complete exercise even if the schedule between groups is tight.

The main idea of the exercise is that all the groups try to setup a SSL VPN gateway on their router. When this is done they can connect to VPN gateway and access a network drive that is not in their subnet. To notify that they have completed the exercise the students need to copy a file to the network drive. There are two subnets 10.8.4.0 and 172.16.0.0 that are used. The 172.16.0.0 subnet simulates the Internet. In the beginning of the exercise the students are connected to the laboratory network (10.8.4.0) and they connect to the router that they need to configure. Once this is done they switch their computer to 172.16.0.0 subnet and try to establish the SSL VPN connection. During the exercise there's also a step in configuring accounts to the Cisco IOS server. This is done on a separate computer that is the server.

Key Words ssl, vpn, exercise, cisco

Sisällys

1 TAUSTA, TARKOITUS JA LÄHTÖKOHDAT

Opinnäytetyöni aiheena on SSL VPN -etäyhteys tekniikka. SSL VPN on uudenlainen VPN-tekniikka, joka poikkeaa muista tällä hetkellä olemassa olevista VPN -teknikoista. SSL VPN -tekniikka mahdollistaa yhteyden muodostamisen ilman erillistä asiakas-sovellusta. Yhteyden muodostamiseen käytetään SSL -salausta tukevaa internet-selainta. Kaikki nykypäivänä käytettävät selaimet (Internet Explorer, Mozilla, Firefox, Opera) tukevat SSL -salausta.

Työn tarkoituksena on käydä läpi SSL VPN -tekniikkaan liittyvät käsitteet ja se miten tekniikka käytännössä toimii. Aikomuksena on myös tutkia, miten SSL VPN – tekniikka eroaa muista VPN -tekniikoista. SSL VPN -harjoituksen teko ja suunnittelu on myös osa työtä. Työssä perehdytään myös Cisco ACS -järjestelmään ja sen toimintaan.

Opinnäytetyöhön on liitetty SSL VPN -harjoitus joka on tarkoitettu käytettäväksi Laurean opiskelijoille. Harjoitus on samankaltainen kuin aiemmin jo käytössä olevat verkkoharjoitukset, kuten reititin-, kytkin- ja WLAN -tukiasema–harjoitukset. Vanhat kytkin- ja reititinharjoitukset toimivat hyvänä oppimispohjana uutta harjoitusta varten. Harjoitusta tullaan käyttämään Laurean tietoliikennelaboratoriossa, jossa opiskelijat saavat suorittaa harjoituksen johonkin opintojaksoon liittyen. Uuden harjoituksen tarkoituksena on laajentaa oppimista kytkimen & reitittimien peruskonfiguroinnista. Harjoituksen avulla opiskelijat oppivat ymmärtämään SSL VPN – tekniikkaan sekä konfiguroimaan SSL VPN -palvelun Ciscon IOS – käyttöjärjestelmää käyttäen. Harjoituksessa tullaan myös konfiguroimaan ACS – palvelinta Radius -protokollaa käyttäen. Laitteistona käytetään Laurean tietoliikennelaboratoriossa olevia Ciscon 2811 modulaarisia reitittimiä sekä Windows 2000 Server-käyttöjärjestelmän päällä pyörivää Cisco ACS -palvelinta.

2 TIETOPERUSTA JA TEOREETTINEN TAUSTA

2.1 Keskeiset käsitteet

2.1.1 VPN (Virtual Private Network)

VPN -yhteydellä tarkoitetaan salattua etäyhteyttä julkisen verkon yli (internet) esimerkiksi yrityksen verkkoon. VPN -yhteys tarjoaa turvatun pääsyn yrityksen lähiverkon resursseihin (mm. verkkolevyllä olevat tiedostot, sähköposti, tietokannat ja intranet – sivuille). VPN-järjestelmän avulla työnteko helpottuu niin matkoilla kuin kotona ollessa (Steinberg, Speed 2005, 11).

2.1.2 SSL (Secure Sockets Layer)

SSL on salausprotokolla, jonka avulla voidaan suojata Internet-sovellusten yhteydet IP -verkkoissa. SSL -protokolla on yksi yleisimmin käytetyistä salausprotokollista, esimerkiksi verkkopankit käyttävät SSL -salausta. Käytettäessä SSL – salattua sivustoa on osoite https:// -alkuinen. SSL -protokolla käyttää TCP – porttia 443 (Huang Q., Frahim J., Waheed W. 2008, 19).

2.1.3 SSL VPN (Secure Socekts Layer Virtual Private Network)

SSL VPN eroaa perinteisestä VPN -yhteydestä siinä, että se on toteutettu ylemmillä OSI -mallin kerroksilla 4-7 kuin esim. suosittu IPSec, joka toimii verkkokerroksella 3. IPSec joutuu kantamaan itse huolta tiedonsiirron luotettavuudesta siinä missä SSL VPN -yhteydessä OSI -mallin kuljetuskerros 4 hoitaa sen. Järjestelmä tarjoaa erilaisia autentikointimenetelmiä kuten käyttäjätunnus & salasana, älykortti tai biometrinen tunnistus (Steinberg, Speed 2005, 16).

2.1.4 Autentikointipalvelin - AAA

Autentikointi palvelimen avulla voidaan keskitetysti hallita VPN -järjestelmän käyttäjiä. Kun käyttäjä muodostaa VPN -yhteyttä tarkistetaan hänen käyttäjätunnus & salasana autentikointi palvelimelta. Tunnukset todennetaan ja jos ne läpäisevät todennuksen jatkuu yhteyden muodostaminen, muussa tapauksessa yhteyden muodostaminen epäonnistuu. Cisco ACS on yksi esimerkki AAA –järjestelmästä (Cisco. 2008).

2.1.5 Cisco IOS (Internetwork Operating System)

Cisco IOS on Ciscon kehittämä käyttöjärjestelmä. IOS – käyttöjärjestelmää käytetään kaikissa Ciscon kytkimissä sekä suurimassa osassa Ciscon valmistamista reitittimistä. Kyseinen käyttöjärjestelmä on komentokehotepohjainen jota ohjataan tietyillä komennoilla. Ensimmäisen Cisco IOS – käyttöjärjestelmän ohjelmoi William Yeager (Cisco. 2009).

2.1.6 OSI – malli (Open Systems Interconnection Refernce Model)

OSI -malli kuvaa tiedostonsiirtoprotokollia ja niiden yhdistelmiä seitsemässä kerroksessa. 1980-luvun alussa kehitetty OSI -malli on ISO:n kansainvälinen standardi. OSI -mallin kerrokset ovat (Steinberg, Speed 2005, 8):

1) Fyysinen kerros (*Physical layer*)
2) Siirtoyhteyskerros (*Data Link layer*)
3) Verkkokerros (*Network layer*)
4) Kuljetuskerros (*Transport layer*)
5) Istuntokerros *(Session layer)*
6) Esitystapakerros (*Presentation layer*)
7) Sovelluskerros (*Application layer*)

2.1.7 Symmetrinen salausmenetelmä

Käyttää yhtä avainta (symmetrinen algoritmi) salaamiseen ja salauksen purkamiseen. Merkittävin etu symmetrisessä salausjärjestelmässä on nopeus. Ongelmana on avainten hallinta, sillä sekä viestin lähettäjällä että vastaanottajalla tulee olla tiedossaan sama salausavain. Salausavaimien välittämiseen osapuolien välillä tarvitaan jokin turvallinen menetelmä (Steinberg, Speed 2005, 38).

2.1.8 Epäsymmetrinen salausmenetelmä

Menetelmässä käytetään avainparia, joista toinen avain on julkinen (public key) ja toinen vastaavasti yksityinen (private key). Julkisella avaimella salattu viesti voidaan avata kyseessä olevan avainparin yksityisellä avaimella ja päinvastoin. Merkittävin etu symmetrisiin salausalgoritmeihin verrattuna on avaintenhallinnan yksinkertaisuus. Menetelmän heikkoutena on hitaus (Steinberg, Speed 2005, 39).

2.1.9 Kämmentietokone eli PDA (Personal Digital Assistant)

Kämmentietokone on pieni kämmenellä pidettävä tietokone. Kämmentietokonetta ohjataan yleensä kosketusnäytön avulla eikä siinä ole fyysistä näppäimistöä. Suorituskyvyn osalta kämmentietokoneet jäävät jälkeen isommista kannettavista tietokoneista. Kämmentietokonetta käytetään sähköisenä kalenterina, sähköpostin lukemiseen, muistikirjana tai internetsivujen selaamiseen.

2.2 Tutkimusmenetelmä

Tutkimukseni on suunnittelutieteellinen, konstruktiivinen tutkimus sillä tutkimuksen tarkoitus on tutkia SSL VPN -tekniikkaa sekä luoda uusi harjoitus kyseisen tiedon perusteella. Suunnittelutieteellisessä tutkimuksessa on kaksi lähestymistapaa, jotka ovat rakentaminen ja arviointi. Nämä kaksi näkemystä yhdistyvät toimintatutkimuksessa ja työssäni, joten tarkemmin sanottuna tutkimukseni on toimintatutkimus. Toimintatutkimuksessa on viisi vaihetta, jotka ovat diagnosointi, suunnittelu, toteutus, arviointi ja oppiminen. Vaiheet käydään tarvittaessa läpi useita kertoja. Käytännössä toimintatutkimuksessa suoritetaan yhden tai useamman kerran ensin tarvittavan muutoksen toteuttamista ja sitten saavutetun muutoksen arviointia. (Järvinen & Järvinen 2004, 103, 128–129).

3 VPN

VPN (Virtual Private Networking) – tekniikalla tarkoitetaan etäyhteyttä lähiverkkoon internetin yli. VPN -yhteyden avulla voidaan myös liittää yrityksen kaksi tai useampaa verkkoa toisiinsa julkisen verkon (Internetin) yli. Salattuja VPN -protokollia on useita:

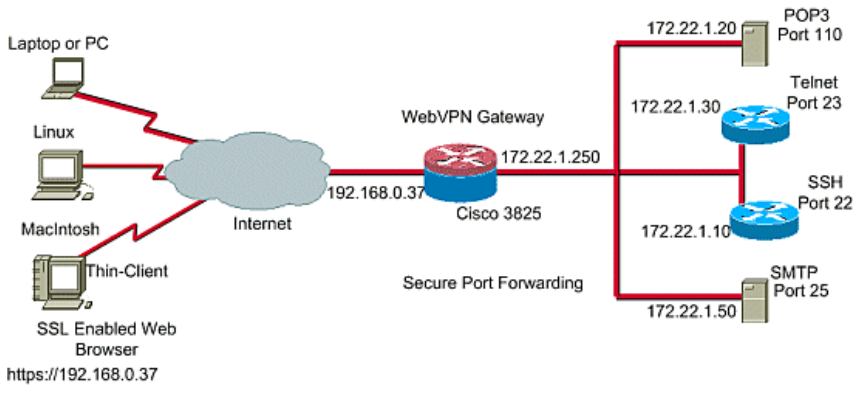
- *Ipsec* -protokolla. Voidaan käyttää niin lähiverkkojen yhdistämiseen kuin etäkäyttöönkin.
- *L2TP* -tunnelointiprotokolla, Voidaan käyttää ainoastaan etäkäyttöön. Protokollassa ei ole omaa salausta, vaan sen kanssa käytetään Ipsec -protokollaa datan salaukseen.
- *L2F* -tunnelointiprotokollaa käytetään vain lähiverkkojen yhdistämiseen. Se on Ciscon protokolla, jonka päälle L2TP-protokolla paljolti perustuu. Se käyttää Point to point (ECP) -protokollaa salaukseen.

- *PPTP* on Microsoftin oma etäkäyttöprotokolla, joka käyttää Microsoft Point-to-Point Encryption (MPPE) -protokollaa salaukseen.
- *SSL* -protokolla Voidaan käyttää niin lähiverkkojen yhdistämiseen kuin etäkäyttöönkin.

IPsec -protokolla on eniten käytetty VPN -markkinoilla mutta jo nyt SSL VPN on ottanut oman osansa markkinoista. Tulevaisuudessa SSL VPN -tekniikan markkinaosuus tulee vielä nousemaan (Steinberg, Speed 2005, 11-17).

3.1 SSL VPN

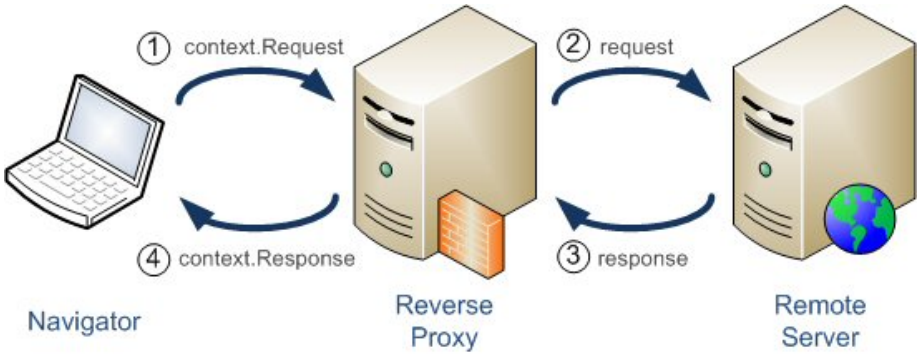
Muista VPN -tekniikoista hieman poikkeava ratkaisu on SSL VPN -tekniikka, missä tarjotaan pääsy yrityksen tietojärjestelmiin salatun liikenteen kautta, mutta varsinaista pakettiliikennettä ei päästetä yrityksen verkkoihin. SSL VPN – tekniikka toimii OSI -kerroksen tasoilla 4-5 kun muut perinteiset VPN -tekniikat toimivat alemmilla kerroksilla kun IPSec kerroksella 3. SSL VPN – tekniikka ei tarvitse erikseen asennettavaa asiakasohjelmaa laitteelle jolla yhteys muodostetaan. SSL VPN -yhteyden muodostamiseen riittää Internet selain kuten Internet Explorer, Mozilla Firefox tai Opera. Ainoa vaatimus selain ohjelmalta on että se tukee SSL- protokollaa. Tämä mahdollistaa yhteyden muodostamisen useilla eri laiteilla kuten Windows, Linux & Mac OS – tietokoneilla. Yhteyden muodostaminen onnistuu myös PDA - laitteilla & matkapuhelimilla joista löytyy internet selain. Kaikkien ohjelmistojen käyttäminen ei välttämättä onnistu suoraan selaimen avulla. Näissä tapauksissa tarvitsee selaimeen asentaa Active X -komponentti tai Java -appletti joka mahdollistaa ohjelmiston käyttämisen. Nämä komponentit asentuvat yleensä käyttäjän laitteeseen taustalla joten käyttäjän ei tarvitse osallistua asennukseen. SSL VPN -tekniikka käyttää kahta asiaa muodostaessa salattua ”tunnelia” käyttäjän koneelta kohdeverkkoon. Käyttäjiä vaaditaan todentautumaan ennen kuin päästään muodostamaan salattu ”tunneli”. Kaikki salatun ”tunnelin” sisäinen liikenne salataan SSL – protokollaa käyttäen (Huang Q., Frahim J., Waheed W. 2008, 35-40).



Kuva 1: Esimerkki SSL VPN -verkon topologiasta

3.2 Käänteinen -proxy (reverse proxy)

SSL VPN -tekniikan perus toimintoihin kuuluu toimia kuten käänteinen -proxy (reverse proxy). Tämä perustuu käyttäjän pyyntöjen vastaanottamiseen sekä niiden välittämiseen sisäiseen verkkoon. Verkon ulkopuolelta käänteinen -proxy palvelin näyttää koneelta joka sisältää kaikki palvelut vaikka se itse asiassa vain välittää tietoa sisäverkossa sijaitseville palvelimille. Yleisin käyttötarkoitus käänteiselle -proxylle on kuormantasaus tai tietoturva syyt. Etäyhteys käyttöä varten käänteiset -proxyt ovat heikkoja koska niistä puuttuu olennaisia ominaisuuksia kuten: palvelin/asiakaskoneen välisen verkkoliikenteen salaaminen tai etäyhteys käyttöön suunniteltu käyttöliittymä (Steinberg, Speed 2005, 45 -46). SSL VPN – tekniikka korjaa nämä puutteet.



Kuva 2: Käänteisen proxyn toiminta

Yllä oleva kuva kuvaa miten käänteinen -proxy käytännössä toimii. Käyttäjän kone on yhteydessä käänteiseen -proxyn joka välittää tiedon sisäverkossa olevalle palvelin koneelle. Palvelin lähettää halutut tiedot käänteiselle -proxylle joka välittää tiedot eteenpäin käyttäjän koneelle. Käyttäjän kone luulee että tiedot tulevat käänteiseltä -proxylta eikä se tiedä sisäverkossa olevasta palvelimesta mitään. Tämä lisää tietoturvaa verkon ulkopuolelta tuleviin hyökkäyksiin ja murtautumisyrityksiin. Tekniikan ansiosta palvelimella oleva data on täysin näkymätön käyttäjälle joten palvelimella oleviin tiedostoihin on vaikea, ellei mahdoton päästä käsiksi.

3.3 SSL VPN – tekniikan tarjoamat edut

3.3.1 Käänteiseen proxyn verrattuna

SSL VPN -tekniikka tarjoaa useita etuja käänteiseen proxyn verrattuna:

- SSL VPN – tekniikka mahdollista SSL tunnelin käyttämisen niin web-pohjaisten ohjelmien kuin ei web-pohjaisia ohjelmien liikennöintiä varten.
- Mahdollistaa pääsyn tiedosto-, printteri- sekä muihin palvelimiin.
- Mahdollisuus käyttää intranetistä löytyviä ohjelmia Internetin yli.
- Sisältää etäyhteyskäyttöön suunnitellun käyttöliittymän

3.3.2 Muihin VPN -tekniikoihin verrattuna

SSL VPN – tekniikka eroaa muista VPN tekniikoista huomattavasti. Suurimpia etuja SSL VPN tekniikan hyväksi ovat:

- Helppokäyttöisempi
- Helpompi implementoida ja ylläpitää
- Mahdollistaa yhteyden muodostamisen useammasta paikasta ja laitteesta
- Halvempi ylläpitää

3.4 SSL (Secure Sockets Layer)

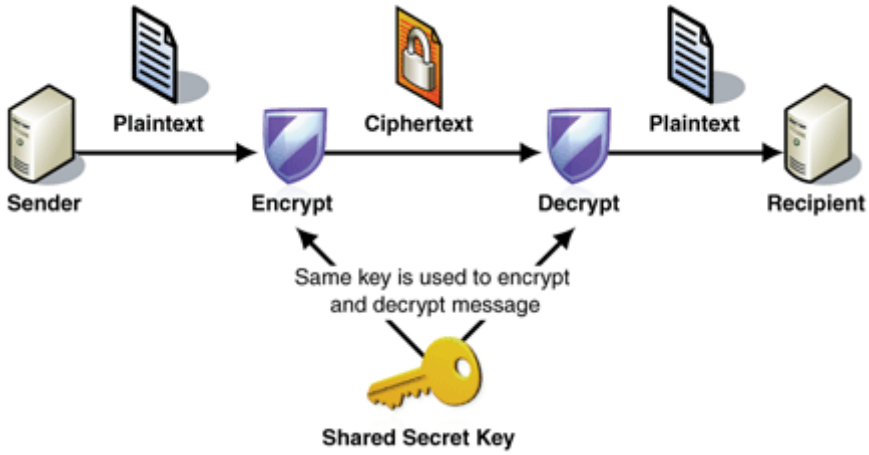
SSL on protokolla jonka avulla verkkoliikenne voidaan salata. Kaikissa nykyaikaisissa Internet-selaimissa kuten Internet Explorer, Mozilla Firefox sekä Opera on SSL tuki. SSL – protokollan avulla voidaan palvelimen ja asiakaskoneen välillä lähettää salasanoja sekä muita ”arkoja” tietoja salattuina. Kaikki SSL -salattu verkkoliikenne on palvelimen ja asiakaskoneen välillä salattu käyttäen julkista salausavainta sekä sovittua salausalgoritmia.

Ensimmäinen versio SSL -protokollasta julkaistiin vuonna 1984 Mosaic selaimen kanssa. Myöhemmin samana vuonna julkaistiin SSL versio 2.0 kun Mosaic – selaimen keksijät muodostivat Netscape Communications -yhtiön joka julkaisi Navigator nimisen Internet-selaimen. Salatut Internetsivut käyttivät https -alkuista osoitetta kun taas normaalit sivut alkoivat http etuliitteellä. Oletusportti http -liikenteelle on TCP 80 ja https -liikenteelle TCP 443. Vuonna 1999 SSL -protokollan kehitys luovutettiin IETF -standardointiorganisaatiolle joka kehitti siitä oman

version nimellä TLS (Transport Layer Security). TLS 1.0 on SSL 3.0:n (julkaistu 1996) seuraaja (Huang Q., Frahim J., Waheed W. 2008, 22-25).

3.4.1 Symmetrinen salausmenetelmä

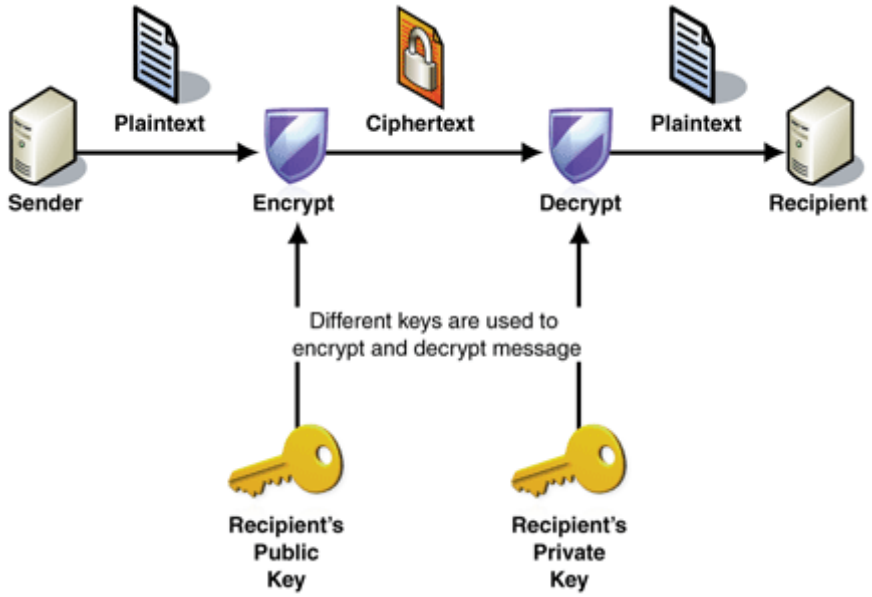
Käyttää yhtä avainta (symmetrinen algoritmi) salaamiseen ja salauksen purkamiseen. Merkittävin etu symmetrisessä salausjärjestelmässä on nopeus jonka ansiosta se soveltuu hyvin verkkoliikenteen salaamiseen. Ongelmana on avainten hallinta, sillä sekä viestin lähettäjällä että vastaanottajalla tulee olla tiedossaan sama salausavain. SSL VPN -tekniikassa tämä on ratkaistu käyttämällä epäsymmetristä salausmenetelmää symmetrisen avaimen välittämiseen käyttäjien välillä (Steinberg, Speed 2005, 38).



Kuva 3: Symmetrinen salausmenetelmä

3.4.2 Epäsymmetrinen salausmenetelmä

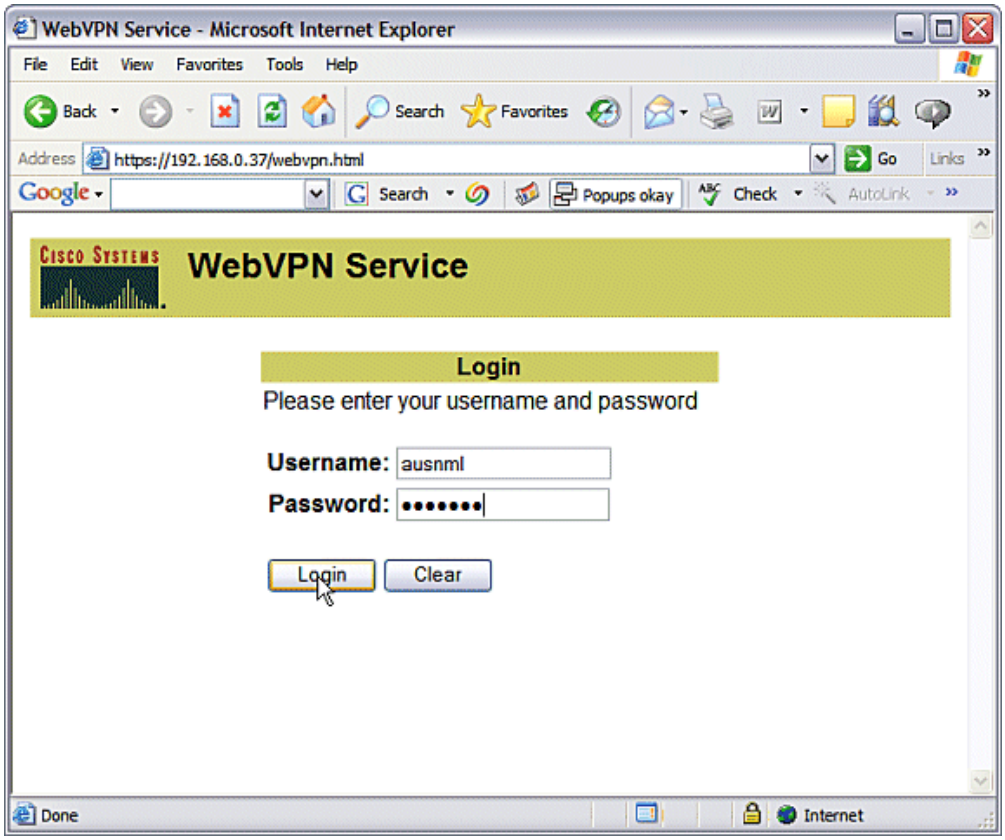
Menetelmässä käytetään avainparia, joista toinen avain on julkinen (public key) ja toinen vastaavasti yksityinen (private key). Julkisella avaimella salattu viesti voidaan avata kyseessä olevan avainparin yksityisellä avaimella ja päinvastoin. Merkittävin etu symmetrisiin salausalgoritmeihin verrattuna on avaintenhallinnan yksinkertaisuus.. Menetelmän heikkoutena on sen hitaus jonka takia sitä ei voida käyttää VPN – yhteyden salaamiseen (Steinberg, Speed 2005, 39–41).



Kuva 4: Epäsymmetrinen salaus

3.5 SSL VPN -yhteyden muodostus

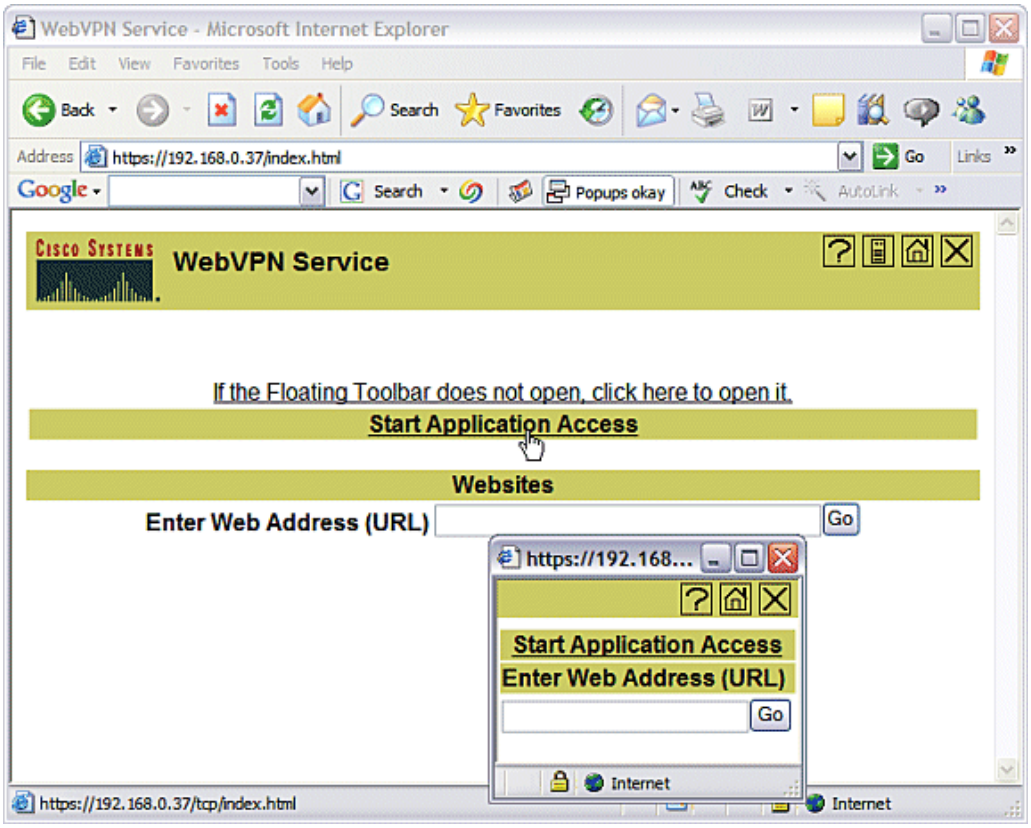
Alla esimerkki siitä miten yhteydenmuodostus käyttäjän ja SSL päätelaitteen välillä tapahtuu ja mitä se tyypillisesti vaatii.



Kuva 5: SSL VPN -kirjautumis-sivu

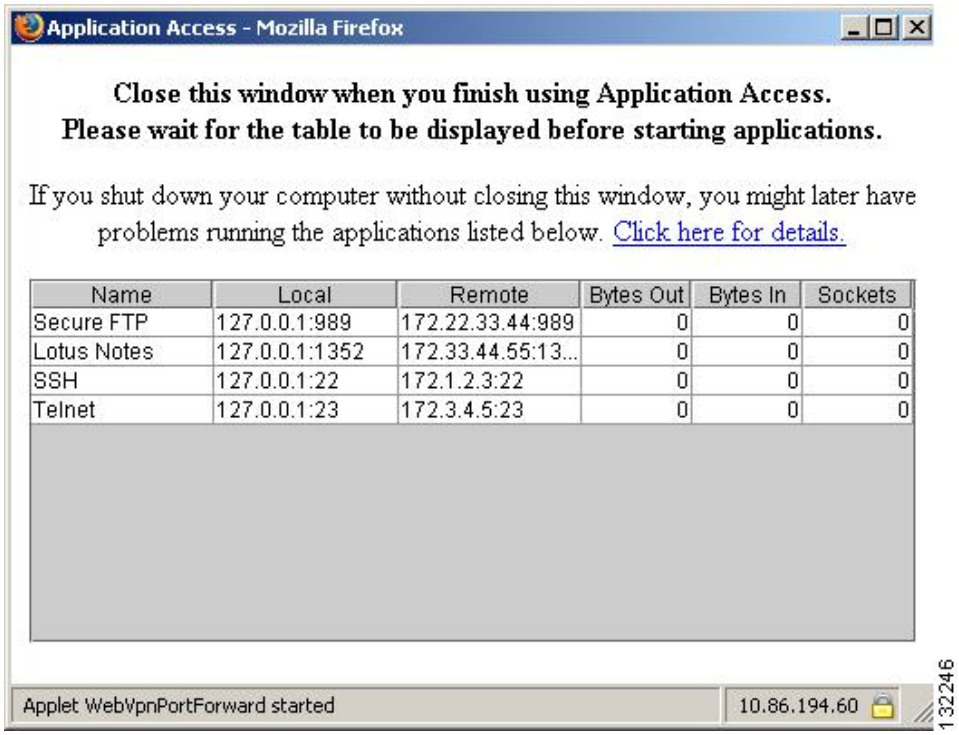
1. Käyttäjä yrittää ottaa yhteyttä SSL VPN -päätelaitteeseen lähettää käyttäjän internet selain tiedot tuetuista salaus menetelmistä päätelaitteelle.
2. VPN -päätelaite lähettää myös tiedot tukemistaan salaus menetelmistä mukaan lukien SSL -sertifikaatin joka sisältää julkisen salausavaimen.
3. Käyttäjän Internet selain varmentaa SSL -sertifikaatin
4. Internet selain luo tämän jälkeen ”pre-master” salausavaimen jonka se salaa VPN -päätelaitteelta saamallaan julkisella salausavaimella. Selain lähettää luomansa ”pre-master” salausavaimen VPN -päätelaitteelle

5. SSL VPN -päätelaite luo saamansa ”pre-master” salausavaimen avulla ”master” salausavaimen jonka se lähettää käyttäjän Internet selaimelle.
6. Internet selain sekä VPN -päätelaite käyttävät nyt ”master” salausavainta sekä sovittua salaus algoritmia. Tästä eteenpäin dataliikenne salataan molemmissa päissä samalla salausavaimella. Tätä kutsutaan symmetriseksi salaukseksi.
7. SSL VPN -yhteys on nyt muodostettu, lähetetään käyttäjän Internet selaimelle SSL VPN -kirjautumissivu
8. Käyttäjä syöttää käyttäjätunnuksen & salasanan kirjautumissivulle sekä mahdollisesti toimialueen
9. Jos käyttäjän syöttämä toimialue todentaa käyttäjätunnuksen & salasanan Radiuksen, LDAP:n tai Active Directory:n kautta lähetetään tiedot kyseiselle palvelimelle joka todentaa käyttäjän



Kuva 6: Cisco Web VPN -portaalisivu

10. Todennus on tapahtunut, nyt avautuu SSL VPN -portaali käyttäjälle. Käyttäjällä on pääsy sisäverkosta löytyviin palveluihin. Yleisimmät palvelut mitä sisäverkossa halutaan käyttää, ovat Intranet - sivut, tiedostopalvelimet sekä sähköposti.



Kuva 7: Cisco Web VPN Application access -ikkuna

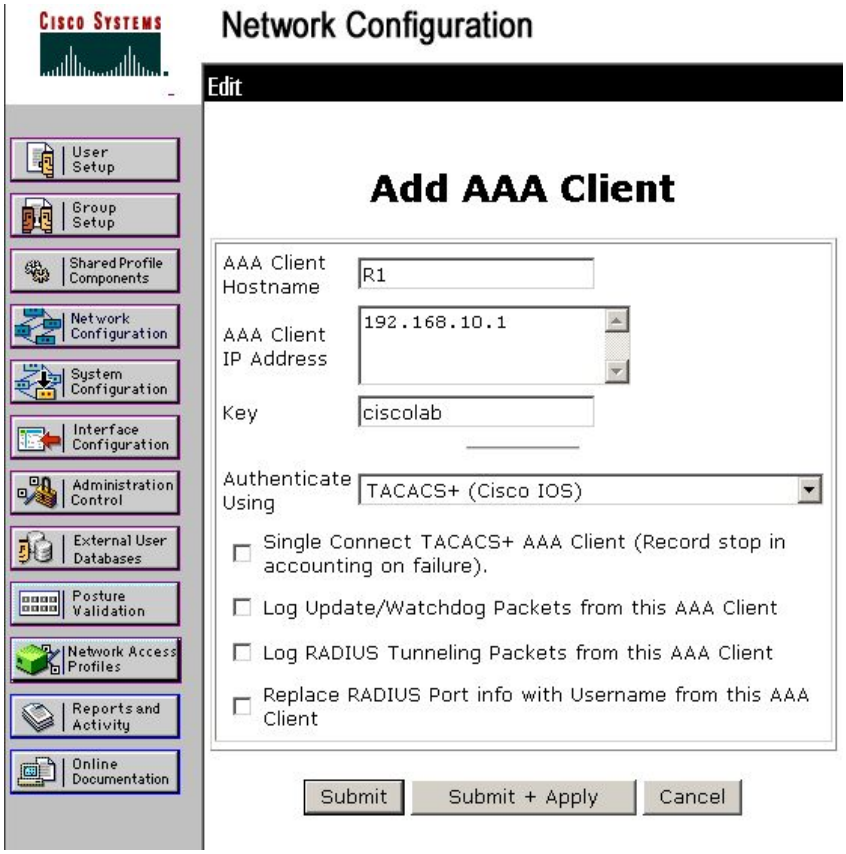
Käyttäjät voivat portaali -sivulta avata ”Application access” – ikkunan. Tämä ikkuna näyttää ohjelmat jotka käyttäjä on käynnistänyt omalla koneellaan ja niiden muodostamat yhteydet yrityksen sisäverkossa oleville palvelimille. Nämä ohjelmat tulevat olla määritelty SSL VPN – järjestelmään jotta niitä voi käyttää Application Access -ikkunan avulla joten kaikkien lokaalisti asennettujen ohjelmien käyttäminen ei onnistu. Yleisimmät toimistosovellukset kuten Microsoft Outlook sekä Lotus Notes ovat esimerkiksi käytettävissä SSL VPN -yhteyden kautta.

4 CISCO ACS PALVELIN (ACCESS CONTROL SERVER)

Ciscon ACS -palvelin on yks tapa hallita VPN -järjestelmän käyttäjiä keskitetysti yhdestä paikasta. ACS -palvelin käyttää AAA -protokollaa (**A**uthentication (todentaminen tai autentikointi, **A**uthorization (valtuutus) ja **A**ccounting (tilastointi) tunnistamaan toisen osapuolen tietoverkossa. Yleisimmät käytössä olevat AAA -protokollat ovat RADIUS ja TACACS. SSL VPN -harjoituksessa sekä reitittimille että ACS -palvelimelle luodaan identtiset tunnukset jotta laitteet voivat kommunikoida keskenään.

4.1 Verkkolaitteiden määrittäminen ACS -palvelimelle

ACS -palvelimelle tulee yksitellen määritellä kaikki verkossa olevat laitteet jotka käyttävät ACS -palvelinta käyttäjän todentamiseen. Tämä tapahtuu ACS -palvelimella ”Add AAA Client” kohdassa. Syötetään laitteen verkkonimi, IP -osoite sekä salasana. Sama salasana mikä on määritelty ACS -palvelimelle, tulee määrittää kaikkiin verkkolaitteisiin jotta ne voivat keskustella ACS -palvelimen kanssa. Salasanan (key) määrittäminen tapahtuu reitittimen tai kytkimen muokkaus tilassa komennolla: *radius-server key ciscolab.* Näin sekä ACS -palvelimella että verkkolaitteessa on määritelty salasana (key) *ciscolab* jota laitteet käyttävät toistensa todentamiseen kun ne keskustelevat keskenään. Tämän lisäksi tulee määrittää mitä todentamisprotokollaa palvelin sekä verkkolaite käyttävät toistensa todentamiseen. Tämä tapahtuu valitsemalla *Authenticate using* pudotusvalikosta TACACS+ tai RADIUS. Sama määritys tehdään verkkolaitteen määrityksiin komennolla *aaa authentication login default group tacacs+* tai *aaa authentication login default group radius.*

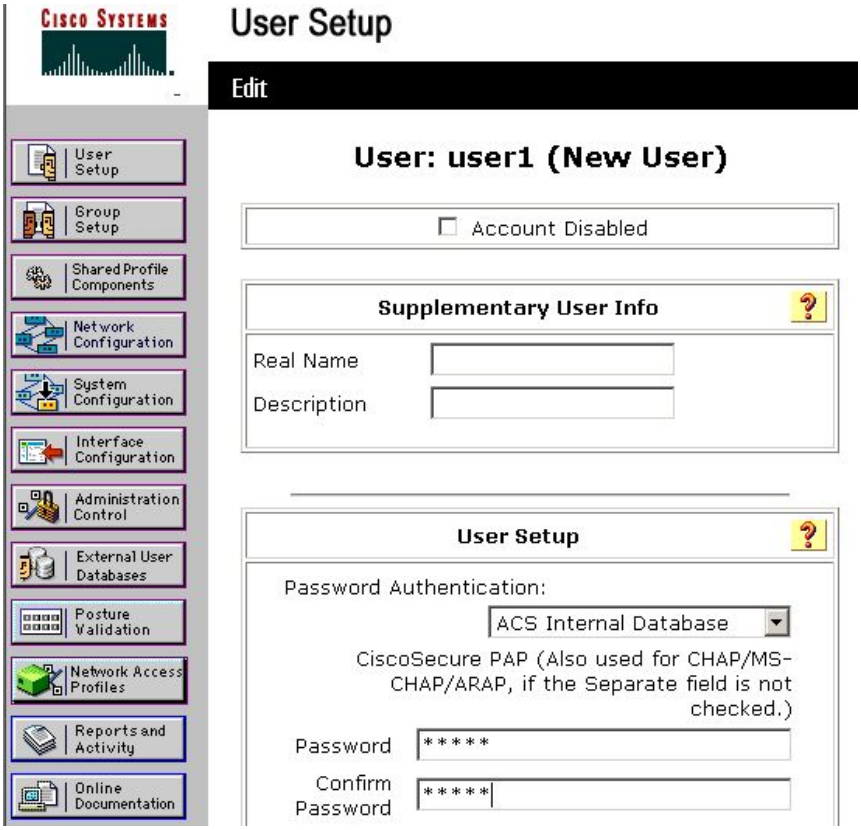


Kuva 8: Laitteiden lisääminen Cisco AAA -palvelimelle

Verkkolaitteille tulee myös määrittää mistä IP -osoitteesta ACS -palvelin löytyy komennolla *radius-server host 10.8.4.251.* Eli tässä tapauksessa palvelimen IP -osoite on 10.8.4.251.

4.2 Käyttäjän luominen ACS -palvelimelle

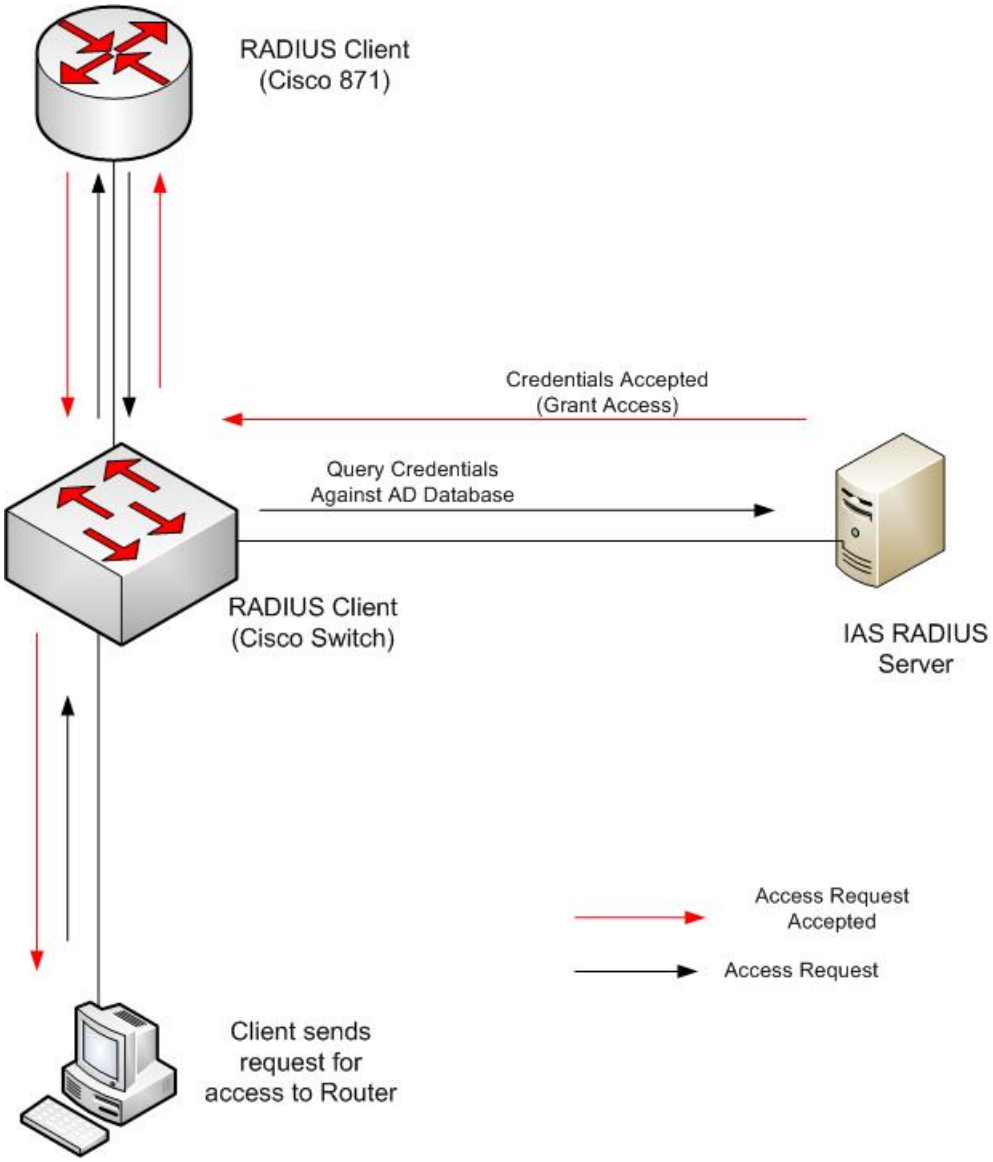
ACS -palvelimelle voidaan tämän jälkeen luoda haluttu määrä käyttäjiä joilla on oikeudet kirjautua SSL VPN -järjestelmään. Käyttäjien lisääminen tapahtuu *User setup* kohdasta. Alla olevassa kuvassa luodaan uusi käyttäjä *user1.*



Kuva 9: Käyttäjän luominen Cisco AAA -palvelimelle

Käyttäjä voi kirjautua SSL VPN -järjestelmään, minkä tahansa reitittimen kautta kunhan tunnus jolla käyttäjä kirjautuu on määritelty ACS -palvelimelle. Tämä helpottaa käyttäjien tunnusten ja salasanojen hallintaa kun kaiken voi tehdä ACS -palvelimen kautta, riippumatta siitä montako SSL VPN -reititintä on käytössä. Jos käytössä ei ole ACS -palvelinta joutuu tunnukset ja salasanat määrittämään kaikkiin käytössä oleviin laitteisiin joka vaikeuttaa tunnusten ylläpitoa. ACS -palvelimeen voidaan käyttää esimerkiksi kytkinten, reitittimien ja langattomien tukiasemien kanssa. Cisco ACS -palvelinta hallitaan web-selaimen toimivan graafisen käyttöliittymän kautta.

4.3 AAA -todennuksen vaiheet



Kuva 10: AAA -todennuksen vaiheet

1. Käyttäjän kone lähettää pyynnön ottaa yhteyttä reitittimeen.
2. Reititin lähettää pyynnön RADIUS -palvelimelle jossa käyttäjän tunnuksia verrataan palvelimelta löytyviin tunnuksiin. Tässä tapauksessa tunnukset löytyvät palvelimelta joten kirjautuminen on hyväksytty.
3. Tieto lähetetään takaisin käyttäjän koneelle jonka jälkeen käyttäjän tietokone saa muodostettua yhteyden reitittimeen.

5 SSL VPN HARJOITUS

5.1 Harjoituksen suunnittelu

SSL VPN -harjoituksen suunnittelun pohjana käytettiin aiempia opiskelijoiden tekemiä verkkoharjoituksia kuten reititin ja kytkinharjoituksia. Harjoitukset oli toteutettu siten että oli tehtävämoniste sekä komentolistaus erikseen. Harjoituksessa oli kohta kohdalta kerrottu mitä tulee tehdä siihen malliin että opiskelijat kuitenkin joutuvat itse vähän miettimään ratkaisua. Harjoitusten mukaan on lisätty komentolistaus josta löytyi kaikki tarvittavat komennot reitittimen ja/tai kytkimen konfigurointia varten. Muuten harjoitukset saattaisivat olla liian vaikeita ja niiden tekeminen kestäisi liian kauan. SSL VPN -harjoitus toteutettiin siis samaa kaavaa käyttäen kuin aiemmat verkkoharjoitukset.

Harjoituksen olennaisena osana olivat uudet Ciscon 2811 modulaariset reitittimet joiden IOS käyttöjärjestelmä sisälsi WebVPN (Verkkojätti Ciscon nimitys SSL VPN:lle) -ominaisuuden. Harjoitusta siis sisältäisi Cisco 2811 reitittimen perus konfiguroinnin sekä WebVPN -ominaisuuden konfiguroimisen. Vaihtoehtona olisi ollut käyttää reitittimistä löytyvää web-selaimella toimivaa konfigurointi mahdollisuutta mutta se jätettiin käyttämättä koska sen katsottiin olevan liian ”helppo”.

Harjoitus rakennettiin kasaan käyttämällä Ciscon Internetsivuilta löytyviä ohjekirjoja PDF -muodossa sekä komentolistauksia. Näitä käyttämällä saatiin toteutettua harjoitus jonka pystyi tekemään tietoliikennelaboratoriossa olemassa olevalla laitteistolla ilman suurempia muutoksia verkon topologiaan.

Harjoituksen voi tehdä kuudella koneella samaan aikaan esimerkiksi pari työnä joten 12 henkilöä voi olla samaan aikaan sitä tekemässä. Harjoituksen suorittamiseen menee noin 30-45 minuuttia. Sen jälkeen kun harjoitus on tehty, voidaan reitittimet palauttaa helposti takaisin aloitustilaan käyttämällä tekstilistausta Cisco IOS -komennoista jotka kumoavat harjoituksessa tehdyt määritykset.

5.2 Laitteisto

Laurean -tietoliikennelaboratoriosta löytyy suuri osa verkkolaitteita joita hyödynnettiin harjoitusta tehdessä. Alla listaus käytetyistä laitteista sekä kuva lopullisesta verkkotopologiasta.

6 kpl Cisco 2811 modulaarista reititintä

Cisco 2811 tekniset tiedot:

Laitteen tyyppi: Reititin
Koko tai muoto: Ulkoinen - modulaarinen - 1U
Ulkomitat: (PxSxK) 43.8 cm x 41.7 cm x 4.5 cm
Paino: 6.4 kg
Käyttömuisti: (RAM) 256 Mt (asennettu) / 768 Mt (enintään) - DDR SDRAM
Flash-muisti: 64 Mt (asennettu) / 256 Mt (enintään)
Tiedonsiirtoprotokolla: Ethernet, Fast Ethernet
Verkko / Siirtoprotokolla: IPSec
Kaukohallintaprotokolla: SNMP 3
Ominaisuudet: Modulaarinen rakenne, palomuurisuojaus, laitteistosalaus, VPN-tuki, MPLS tuki, Quality of Service (QoS)
Yhteensopivuusstandardit: IEEE 802.3af
Virransyöttö: AC 120/230 V (50/60 Hz)

Kuva 11: Cisco 2811 reititin

6 kpl Cisco 2950 kytkintä

Cisco 2950 tekniset tiedot:

Laitteen tyyppi: Kytkin
Kotelon tyyppi: Telineasennettava - ulkoinen - 1U Leveys44.5 cm Syvyys24.2 cm Korkeus4.4 cm Paino3 kg
Flash -muisti: 8 Mt Flash
Porttien lukumäärä: 24 x Ethernet 10Base-T, Ethernet 100Base-TX
Tiedonsiirtonopeus:100 Mbit/s
Tiedonsiirtoprotokolla: Ethernet, Fast Ethernet
Kaukohallintaprotokolla: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, HTTP
Kommunikointimuoto: Half-duplex, full-duplex
MAC osoitetaulukon koko (Address Table Size) 8000 osoitetta
Tilan ilmaisimet: Linkkiaktiviteetti, portin lähetysnopeus, portin kaksisuuntaisuustoiminto, kaistanleveyden käyttöprosentti, teho, linkki OK, tila
Ominaisuudet: Vuonhallinta, täysi kaksisuuntaisuuden tuki, väylöitys, VLAN-tuki, IGMP snooping, Syslog tuki, Weighted Round Robin (WRR) queuing, päivitettävä valmisohjelmisto
Yhteensopivuusstandardit: IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Liitännät:1 x hallinta - konsoli - RJ-45 - 24
24 x verkko - Ethernet 10Base-T/100Base-TX - RJ-45 - 1
Tunnistusmenetelmä: RADIUS, TACACS+, Secure Shell v.2 (SSH2)
Yhteensopivuusstandardit: CE, FCC Luokka A sertifioitu, CISPR 22 Class A, BSMI CNS 13438 Class A, EN 60950, VCCI Class A ITE, IEC 60950, CSA 22.2 No. 950, EN55022 Class A, UL 60950, ACA TS001, AS/NZS 3260, FCC Part 15, MIC
Virtalähde: - Sisäinen
Vaadittava jännite: AC 120/230 V Vaihtovirta 110/220 V ± 10% (50/60 Hz)
Virran kulutus: 30 wattia (toiminnassa)

Kuva 12: Cisco 2950 kytkin

1 x Cisco 3500XL kytkin

Cisco 3500XL tekniset tiedot:

Laitteen tyyppi: Kytkin
Kotelon tyyppi: Telineasennettava - ulkoinen - 1U Leveys 40.46 cm Syvyys 44.45 cm Korkeus 4.45 cm Paino 5.45 kg
Flash -muisti: 8 Mt Flash
Porttien lukumäärä: 24 x Ethernet 10Base-T, Ethernet 100Base-TX
Tiedonsiirtonopeus:100 Mbit/s
Tiedonsiirtoprotokolla: Ethernet, Fast Ethernet
Kaukohallintaprotokolla: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, HTTP
Kommunikointimuoto: Half-duplex, full-duplex
MAC osoitetaulukon koko (Address Table Size) 8000 osoitetta
Tilan ilmaisimet: Linkkiaktiviteetti, portin lähetysnopeus, portin kaksisuuntaisuustoiminto, kaistanleveyden käyttöprosentti, teho, linkki OK, tila
Ominaisuudet: Vuonhallinta, täysi kaksisuuntaisuuden tuki, väylöitys, VLAN-tuki, IGMP snooping, Syslog tuki, Weighted Round Robin (WRR) queuing, päivitettävä valmisohjelmisto
Yhteensopivuusstandardit: IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Liitännät:1 x hallinta - konsoli - RJ-45 - 24
24 x verkko - Ethernet 10Base-T/100Base-TX - RJ-45 - 1
Tunnistusmenetelmä: RADIUS, TACACS+, Secure Shell v.2 (SSH2)

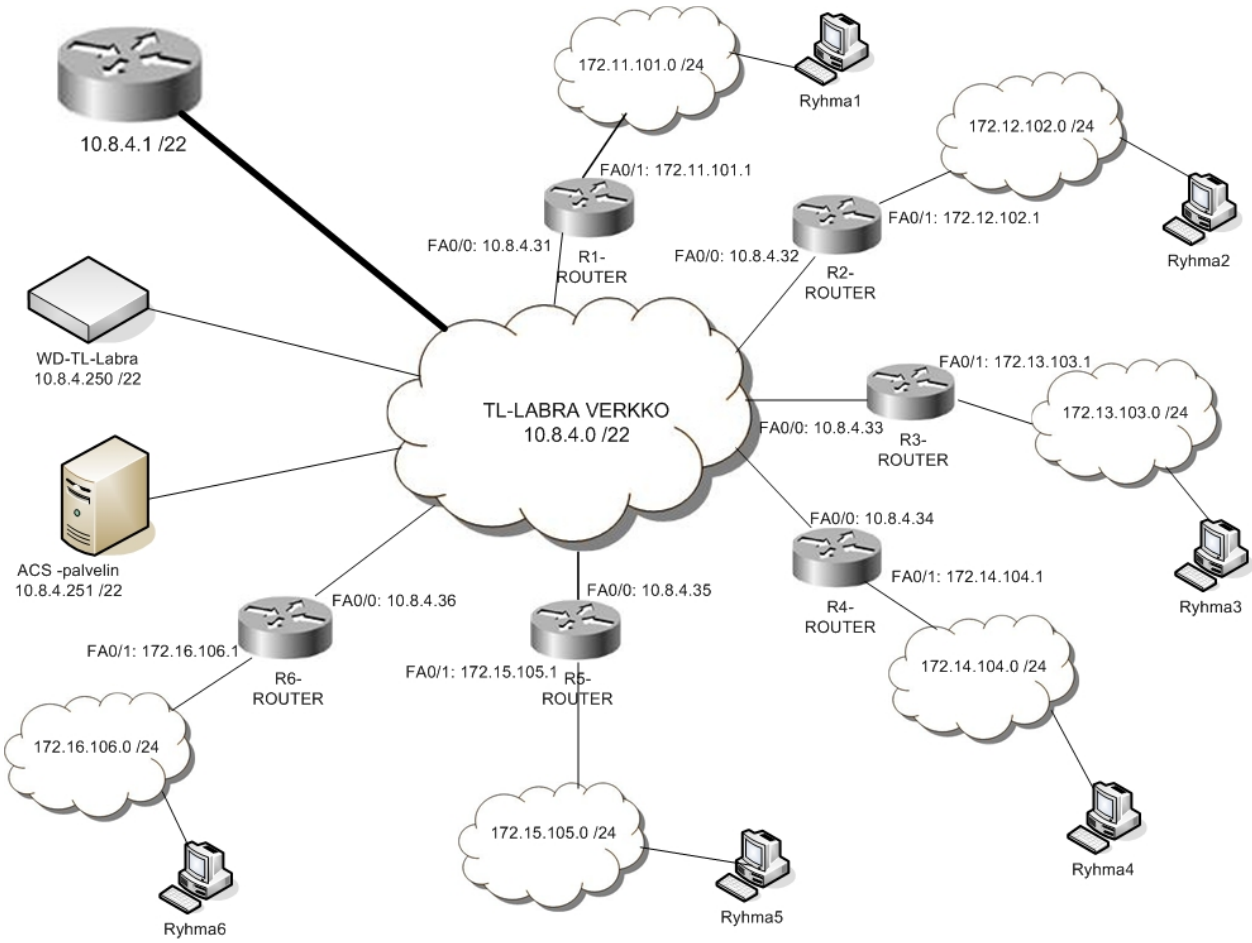
Virtalähde: - Sisäinen

Vaadittava jännite: AC 120/230 V Vaihtovirta 110/220 V ± 10% (50/60 Hz)

Virran kulutus: 50 wattia (toiminnassa

Kuva 13: Cisco 3500 XL kytkin

Verkon topologia



Kuva 14: SSL VPN -harjoituksen verkon topologia

Verkon topologia muodostui yllä olevan kuvan mukaiseksi. Jokaisen ryhmän (1-6) koneen vieressä oli 2 verkkopaikkaa. Vasemmanpuoleinen verkkopistoke kytkettiin jakorasian kautta Cisco 2950 kytkimen porttiin joka oli TL -laboratorion verkossa 10.8.4.0 /22 (vlan 8). Kaikki 6 reititintä oli myös laboratorio verkossa toisen porttinsa kautta. Harjoituksen aikana reitittimien toiseen verkkoporttiin määritellään 172.*.*.* verkossa oleva verkko. Tällä simuloidaan laboratorion ulkopuolista verkkoa kuten esimerkiksi Internetiä. Kun ryhmät ovat harjoituksen loppu puolella, kytketään tietokoneet oikeanpuoleiseen verkkopistokkeeseen joka on 172 – alkuisessa verkossa. Tästä verkosta ryhmät voivat muodostaa VPN yhteyden laboratorioverkkoon 10.8.4.0/ 22 jos reititin on konfiguroitu oikein. Tarkoituksena on päästä 172-alkuisesta verkosta laboratorioverkon verkkokiintolevylle ”WD-TL-Labra” (10.8.4.250) jonne ryhmät tallentavat tiedoston harjoituksen läpäisemisen merkiksi.

Verkossa (vlan8) on myös Ciscon ACS -palvelin jolla hallitaan keskitetysti VPN -yhteydessä käytettyjä käyttäjätunnuksia sekä salasanoja. ACS -palvelinta käytetään erilliseltä koneelta tietoliikennelaboratoriossa. ACS -palvelin pyörii Windows 2000 palvelimessa. Kun harjoituksessa

tullaan ACS -palvelimen konfigurointi kohtaan siirrytään oman ryhmän koneelta ACS -palvelin koneelle. Kun oman ryhmän reititin on konfiguroitu ACS –palvelimelle, siirrytään takaisin oman ryhmän koneelle jossa harjoitus suoritetaan loppuun.

6 YHTEENVETO

Kuten on jo aikaisemmin todettu, on SSL VPN -tekniikka uudenlainen tapa toteuttaa etäyhteyksiä. Se poikkeaa vanhemmista VPN -tekniikoista merkittävästi. Suurin ero on että SSL VPN -yhteyden muodostamiseen riittää laite jossa on Internet selain joka tukee SSL/TLS -salausta. Tämä löytyy käytännössä kaikista tämän päivän tietokoneista sekä mobiililaitteista. Mitään VPN -asiakas-sovellusta ei tarvitse asentaa kuten muissa VPN tekniikoissa. Tämän ansiosta VPN -yhteyden voi muodosta melkein mistä vaan ja melkein millä laitteella tahansa, esim. kirjaston yhteiskäyttötietokoneelta. SSL VPN –tekniikka on myös helppokäyttöinen, sillä mitään asetuksia ei tarvitse määritellä käyttäjän tietokoneelle. Yhteyden saa muodostettua menemällä tietylle Internet sivulla kuten https://vpn.yrityksendomain.com ja kirjautumalla sinne. Käyttäjän kirjautuminen järjestelmään voidaan todentaa monella eri tavalla kuten: salasanalla, biometrinen tunnistus tai vaihtuva numerosarja (token).

Harjoituksen suunnittelu ja toteuttaminen oli haastavaa sekä palkitsevaa. Harjoitusta suunniteltaessa ei tarvinnut aivan tyhjältä pöydältä lähteä. Laboratoriossa jo käytössä olevat verkkolaiteharjoitukset toimivat oivana pohjana oman harjoituksen suunnittelulle. Nämä jo käytössä olevat harjoitukset oli todettu toimiviksi joten oli turha lähetä muuttamaan toimivaa konseptia. Näinpä myös SSL VPN -harjoitus toteutettiin samaa kaavaa käyttäen. Seuraava vaihe oli suunnitella sopivan pituinen (30 - 45 min) kestävä harjoitus joka opettaisi SSL VPN -tekniikan ja sen konfiguroimisen laboratoriossa oleviin reitittimiin. Lähtökohtana käytettiin Ciscon websivuilta löytyviä harjoituskonfiguraatioita. Näitä soveltamalla saatiin sopiva harjoitus toteutettua. Toteuttamisessa meni oma aikansa koska SSL VPN -tekniikka oli itselleni aika tuntematon projektin alussa. Ajan myötä ja testejä tehtyä sai kuitenkin hyvän käsityksen siitä miten SSL VPN -tekniikka toimii sekä miten sitä hallinnoidaan Cisco IOS -käyttöjärjestelmää käyttäen. Harjoitus tultaisiin siis tekemään reitittimistä löytyvää Ciscon IOS -käyttöjärjestelmää käyttäen. Harjoitus koostui tehtävä monisteesta sekä erillisestä komentomonisteesta. Tarkoituksena on suorittaa harjoitus käyttäen apuna komentomonistetta. Komentomoniste sisältää kaikki tehtävässä käytettävät komennot. Alussa tuntui että harjoitus olisi liian helppo kun kaikki komennot on valmiina käytössä mutta näin ei kuitenkaan ollut. Tehtävän tekeminen olisi ollut huomattavasti helpompi jos se olisi toteutettu Internet selaimessa konfiguroitavaksi. Selaimen kautta tapahtunut konfigurointi päätettiin kuitenkin unohtaa ja näin harjoitus toteutettiin Cisco IOS -käyttöjärjestelmää käyttäen. Samalla tavalla kuin aikaisemmat kytkin sekä reititinharjoitukset.

Lähteet

Cisco. 2003. Catalyst 3500 XL Switch Hardware Installation Guide, August 2003. Viitattu 14.8.2009
http://www.cisco.com/en/US/docs/switches/lan/catalyst2900xl_3500xl/3500switches/3500hig/35spec.html

Cisco. 2008. Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide, Version 8.1. Viitattu 3.12.2009.
http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/webvpn.html

Cisco. 2008. Cisco IOS Security Cofinguration Guide, Release 12.2 - AAA Overview Cisco Systems. Viitattu 13.12.2009.
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfaaa.html

Cisco. 2009. Cisco IOS Technologies. Viitattu 4.8.2009.
http://www.cisco.com/en/US/products/ps6537/products_ios_sub_category_home.html

Cisco. 2009. EAP Authentication with RADIUS Server. Viitattu 13.3.2010
http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801bd035.shtml

Deny IP. 2008. Simple AAA lab. Viitattu 6.6.2010
http://denyip.wordpress.com/2008/07/30/simple-aaa-lab/

Huang Q., Frahim J., Waheed W. 2008. SSL and Remote Access VPNs (Networking Technology) (Paperback): Cisco Press

Järvinen, A., & Järvinen, P. 2004. Tutkimustyön metodeista. Tampere: Opinpajan kirja

Microsoft. 2005. Data Confidentiality. Viitattu 10.9.2009
http://msdn.microsoft.com/en-us/library/aa480570.aspx

Steinberg J., Speed T. 2005. SSL VPN Understanding, evaluating, and planning secure, web-based remote access. Birmingham: Packt Publishing

The Code Porject. 2004. Simple HTTP Reverse Proxy with ASP.NET and IIS. Viitattu 13.10.2009
http://www.codeproject.com/KB/web-security/HTTPReverseProxy.aspx?display=Print

The Code Project. 2008. Simple Reverse Proxy in C# 2.0 (description and deployment). Viitattu 16.5.2010
http://www.codeproject.com/KB/IP/SimpleReverseProxy.aspx?msg=2909393

Trainsingnaltraining. 2009. Configure a Cisco Router to use RADIUS for Authentication. Viitattu 14.2.2010
http://www.trainsignaltraining.com/using-radius-for-authentication/2009-08-20/

Kuvat

Liitteet

SSL VPN –harjoitus

Tietoliikennelaboratorion SSL VPN-harjoitus
OPETTAJA

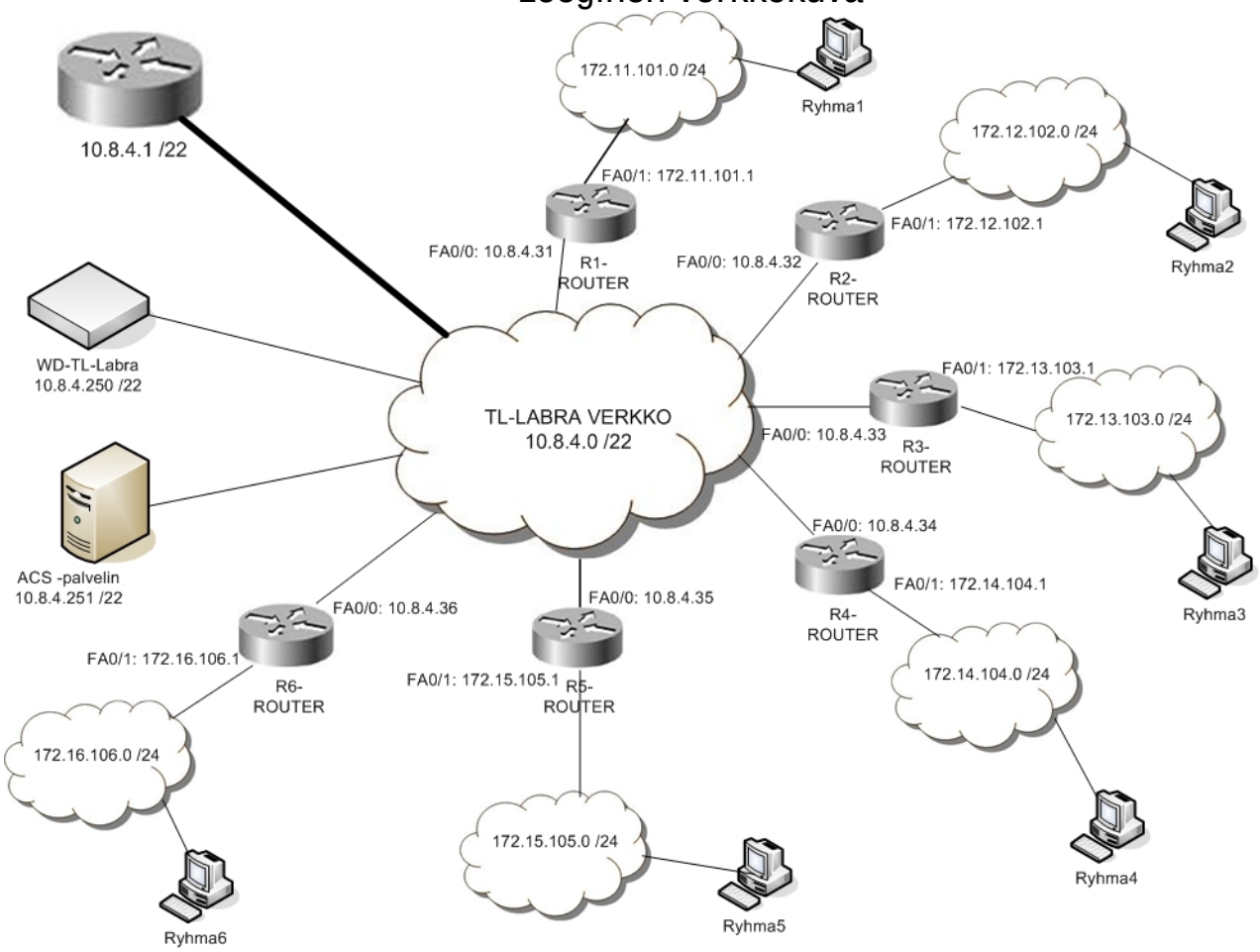
Pvm

Nimi Opiskelijanumero

Nimi Opiskelijanumero

SSL VPN -harjoitus

Looginen verkkokuva



Käynnistä koneen komentokehoite eli CMD:

Tarkista koneen IP-osoite ja muut verkkoasetukset komennolla:

ipconfig /all

Täytä seuraavat tiedot, jotka sait ylläolevalla komennolla.

IP Address:

Subnet Mask:

Default Gateway:

DHCP Server:

DNS Server:

Muodosta telnet-yhteys ryhmän 1 reitittimeen komennolla telnet 10.8.4.31.

Kirjaudu sisään käyttäjätunnuksella *cisco.* Salasana on *cisco*.

Tarkista reitittimen ajonaikainen konfiguraatio RAM-muistista:

show run

Tarkista reitittimen ohjelmistoversio sekä RAM, FLASH, ja NVRAM muistien määrät:

show version

VERSION:

RAM:

NVRAM:

FLASH:

Määritä interface FastEthernet 0/1:lle ip-osoite 172.11.101.1 /24 ja käynnistä se:

interface fa 0/1
ip address 172.11.101.1 255.255.255.0
no shutdown

Käynnistä DHCP-palvelu nimellä ”R1_dhcp” (katso verkkokuvasta tarvittavat tiedot):

router(config)#ip dhcp pool R1_dhcp

router(dhcp-config)#network 172.11.101.0 255.255.255.0
router(dhcp-config)#default-router 172.11.101.1
router(dhcp-config)#dns-server 10.2.8.20

Määritä etäkäyttäjille ip-osoiteavaruus (172.10.110.10 -172.10.110.20) jota asiakasohjelmat käyttävät:

router(config)# **ip local pool 172.10.110.10 172.10.110.20**

Tarkista muutokset ajonaikaisesta konfiguraatiosta:

show run

AAA-protokolla

Käynnistä AAA-protokolla (Authentication, Authorization & Accounting). Autentikointiin käytetään ACS –palvelinta (RADIUS) Salasana (key) on cisco123. *AAA-protokolla on menetelmä, jolla voidaan identifioida toinen osapuoli tietoverkossa*:

router(config)# **aaa new model**
router(config)# **aaa authentication login default group radius**
router(config)# **radius-server host 10.8.4.251 key cisco123**

SSL VPN

Luo uusi SSL VPN-yhdyskäytävä FastEthernet 0/1 –porttiin nimellä ”R1_gateway” HTTP –liikenne ohjataan portista 80 porttiin 443. Käynnistä yhdyskäytävä:

router(config)# **webvpn gateway R1_gateway**
router(config-webvpn-gateway)# **ip address 172.11.101.1**
router(config-webvpn-gateway)# **http-redirect port 80**
router(config-webvpn-gateway)# **inservice**
SSL VPN –palvelun sisällön asetukset (context)

Luo uusi asetusmalli SSL VPN kontekstille nimellä ”vpn”:

router(config)# **webvpn context vpn**

Lisää NetBIOS nimipalvelu nimellä ”verkkolevy”:

router(config-webvpn-context)# **nbns-list verkkolevy**
router(config-webvpn-nbnslist)# **nbns-server 10.8.4.250**

Luo uusi policy group nimellä “R1_policy”. Policy groupin tulee sisältää viittaus luotuun NetBIOS palveluun sekä pääsy lukemaan ja muokkaamaan jaettuja verkkolevyjä (access, browse & entry –toiminnot). Myös osoiterivi tulee piilottaa:

router(config-webvpn-context)# **policy group R1_policy**

router(config-webvpn-group)# **functions file-access**
router(config-webvpn-group)# **functions file-browse**
router(config-webvpn-group)# **functions file-entry**
router(config-webvpn-group)# **hide-url-bar**
router(config-webvpn-group)# **nbs-list verkkolevy**

Määritetään oletus policy groupiksi “R1_policy”:

router(config-webvpn-context)# **default-group-policy R1_policy**

Yhdyskäytäväksi asetetaan aiemmin luotu ”R1_gateway”:

router(config-webvpn-context)# **gateway R1_gateway**

Ota asetukset käyttöön:

router(config-webvpn-context)# inservice

ACS –palvelimen (Access Control Server) konfigurointi

Siirry ACS –palvelin koneen ääreen.

Lisää ryhmän reititin AAA –asiakaslistaan käyttäen RADIUS –protokollaa salasana on *cisco123*:

Lisää uusi käyttäjätunnus (”ryhma1”) ja salasana (”ryhma1”) jolla voidaan kirjautua SSL VPN -palveluun:

SSL VPN –yhteyden testaaminen

Kirjaudu ulos reitittimeltä. Siirrä kone uuteen verkkoon (oikean puoleinen liitin pöytärasiassa) ja tarkista seuraavat tiedot:

IP Address:

Subnet Mask:

Default Gateway:

DHCP Server:

DNS Server:

Avaa Internet Explorer –selain ja suuntaa osoitteeseen http://172.11.101.1/vpn

Kirjaudu sisään aiemmin luoduilla käyttäjätunnuksilla

ryhma1 , ryhma1

Siirry verkkolevyn ”WD-TL-Labra” *vpn* kansioon, käyttäjätunnus on *guest* ja salasana *cisco*:

\\WD-TL_Labra\vpn tai \\10.8.4.250\vpn

Luo uusi kansio ”Ryhma1” verkkolevylle

SSL VPN Cisco IOS komennot

Komento	Tila	Toiminto
Configure Terminal	Router#	Siirtyminen yleiseen konfiguraatiotilaan.
Exit	Router(config)#	Siirtyminen yleisestä konfiguraatiotilasta pääkäyttäjätilaan tai yhden askelen verran taaksepäin alitilasta.
End	Router(config)#	Siirtyminen mistä tahansa pääkäyttäjätilaan.
Show version	Router#	Näyttää IOS-käyttöjärjestelmän tiedot.
Show running-config	Router#	Näyttää ajoaikaisen konfiguraation RAM-muistista.
Show ip route	Router#	Näyttää reititystaulun sisällön.
Copy running-config startup-config	Router#	Kopioi ajonaikaisen konfiguraation RAM-muistista NVRAM-muistiin.
Interface	Router(config)#	Konfiguraatiotila jonkun tietyn portin konfiguroimiseen (esim. Interface FastEthernet 0/1).
Shutdown	Router(config-if)#	Portin sammuttaminen.
No shutdown	Router(config-if)#	Portin käynnistäminen.
Router rip	Router(config)#	Käynnistää (dynaamisen) RIP-reititysprotokollan.
Network	Router(config-router)#	Määrittää reititysprotokollan ”mainostamat” verkot.
Ip dhcp pool	Router(config)#	Luo uuden DHCP-palvelun
Network	Router(dhcp-config)#	
Default-router	Router(dhcp-config)#	Määrittää DHCP-palvelun käyttämän oletusreitittimen.
Dns-server	Router(dhcp-config)#	Määrittää DHCP-palvelun käyttämät nimipalvelimet.
Ip local pool	Router(config)#	Määrittää asiakasohjelmien käyttämät ip-osoitteet.
Aaa new-model	Router(config)#	Luo uuden autentikointimallin.

Aaa authentication login	Router(config)#	Määrittää miten SSL VPN -käyttäjät autentikoidaan.
Radius-server	Router(config)#	Määrittää RADIUS -palvelimen ip-osoitteen ja salasanan.
Webvpn gateway	Router(config)#	Luo uuden SSL VPN-yhdyskäytävän ja / tai siirtyy sen määrittämiseen tarkoitettuun alitilaan.
Webvpn context	Router(config)#	Luo uuden asetusmallin SSL VPN -palvelun kontekstille.
Ip address	Router(config-webvpn-gateway)#	Määrittää SSL VPN-yhdyskäytävän ip-osoitteen.
Http-redirect	Router(config-webvpn-gateway)#	Ohjaa liikenteen portista 80 porttiin 443.
Inservice	Router(config-webvpn-gateway)#	Käynnistää palvelun.
Default-group-policy	Router(config-webvpn-context)#	Määrittelee oletus group policyn.
Gateway	Router(config-webvpn-context)#	Määrittelee käytettävän SSL VPN–yhdyskäytävän.
Inservice	Router(config-webvpn-context)#	Ottaa asetukset käyttöön.
Policy group	Router(config-webvpn-context)#	Luo uuden policy groupin ja / tai siirtyy sen määrittämiseen tarkoitettuun alitilaan.
Nbns-list	Router(config-webvpn-context)#	Luo uuden NetBios –palvelin listan ja / tai siirtyy sen määrittämiseen tarkoitettuun alitilaan.
Nbns-server	Router(config-webvpn-nbnslist)#	Määrittää nbns-palvelimen tiedot.
Functions file-access	Router(config-webvpn-group)#	Sallii pääsyn verkossa jaettuihin tiedostoihin.
Functions file-browse	Router(config-webvpn-group)#	Sallii jaettujen tiedostojen selaamisen.
Functions file-entry	Router(config-webvpn-group)#	Sallii jaettujen tiedostojen muokkaamisen.
Hide-url-bar	Router(config-webvpn-group)#	Piilottaa http-osoiterivin pois VPN –sivulta.
Nbns-list	Router(config-webvpn-group)#	Määrittää käytettävän nbns-listan policy groupiin.

Reitittimen valmis Cisco IOS –konfiguraatio

```
Building configuration...

Current configuration : 6218 bytes
!
! Last configuration change at 10:16:16 UTC Thu Mar 15 2007 by cisco
! NVRAM config last updated at 08:48:09 UTC Thu Mar 15 2007 by cisco
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1-RO2811
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
aaa new-model
!
!
aaa authentication login default group radius
!
aaa session-id common
!
resource policy
!
!
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool R1_dhcp
   network 172.11.101.0 255.255.255.0
   default-router 172.11.101.1
   dns-server 10.2.8.20
!
!
ip domain name yourdomain.com
!
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-1225457800
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1225457800
 revocation-check none
 rsakeypair TP-self-signed-1225457800
!
!
crypto pki certificate chain TP-self-signed-1225457800
 certificate self-signed 01
  30820250 308201B9 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31323235 34353738 3030301E 170D3036 31323238 31313031
  32345A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 32323534
  35373830 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100C613 927CD5D2 D13D4530 6B639517 3B2846BC DF22081E F09AA175 D3D16E77
  0D5D46DC 25043565 35CF94FF F60DE395 0466DCB6 AC794B52 E1641D16 44CA218D
  DA96032B 7FC33EE9 099D2B5F 283108A2 8F4784AA B8198F26 3AD633CC A624418F
  5340C32C BC2810E9 15F5B5E4 29D979D5 9C98B1F7 36C6C194 2422DEAC C51980CD
  69370203 010001A3 78307630 0F060355 1D130101 FF040530 030101FF 30230603
  551D1104 1C301A82 1852312D 524F3238 31312E79 6F757264 6F6D6169 6E2E636F
  6D301F06 03551D23 04183016 801497BD DAE2B1FE 1EBE7B62 B39D7A5A 5058DE08
  193B301D 0603551D 0E041604 1497BDDA E2B1FE1E BE7B62B3 9D7A5A50 58DE0819
  3B300D06 092A8648 86F70D01 01040500 03818100 B4473D16 A6DC453A F9186F0F
  29AD2F28 38A5A3BE 29586F9E 1B0A6655 136FFCE0 B2D2E771 2934F698 81787799
  C2B0AEFF 36FE6F36 BD8D6550 C7043738 69CC731A F652FD39 050072DB 2BDDD136
  FFD3C3E6 B8045C2C 4F3B496F 8E949867 30E5AF9F 1FC11472 89AD1EE1 ED5E200E
  54DD7DEF 3DF1F36E ECD9D3FE ECC32BA2 B643541D
  quit
!
!
username cisco privilege 15 secret 5 $1$nP7R$b/KfcXLy6Wv.xjAxYOsua.
!
!
!
!
!
!
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
 ip address 10.8.4.31 255.255.252.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.11.101.1 255.255.255.0
 duplex auto
 speed auto
!
ip local pool 172.10.110.10 172.10.110.20
```

```
!
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:
!
access-list 23 permit 10.8.4.0 0.0.0.255
!
!
!
!
!
radius-server host 10.8.4.251 auth-port 1645 acct-port 1646 key cisco123
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C .....IZNNNNN:.....:NNNNNNND$+.....
.....
.....,ZNNNNNNNNN$,.....ONNNNNNNNNNNN~,.....
.....,ONNNNNNNNNNNNNN8.....,ONNNNNNNNNNNNNNNNND:.....
.....,8NNNNNNNNNNNNNNNN.....$NNNNNNNNNNNNNNNNNNN$~.....
.....?DNNNNNNNNNNNNNNNNNNO,.....NNNNN:...=DNNNNNNNNNNNNN7.....
....+NNNNNNNNNNNNNNNNNNNNN7.....,NNNND.....INNNNNNNNNNNNNN7.....
..,NNNNNNNNNNNNNNNNNNNNNNNNN.....,NNNNN~...?DNNNNNNNNNNNNNNNN:.....
..ZNNNNNNNNNNNNNNNNNNNNNDZ.....,NNNNNNNDNNNNNNNNNNNNNNNNNN8.....
..
.ZNNNNNNNNNNNNNNNNNNI~::::::,.....,NNNNNNNNNNNNNNNNNNNNNNNNNN.....
.8NNNNNNNNNNNNNNNNNNNNNNNNNNNN.....NNNNNNNNNNNNNNNNNNNNNNNNNNN=
.....
.8NNNNNNNNNNNNNNNNNNNNNNNNNNN$.....DNNNNNNNNNNNNNNNNNNNNNNNNNN:
.....
.7NNNNNNNNNNNNNNNNNNNNNNNNNN$~.....8NNNNNNNNNNNNNNNNNNNNNNNNN..
.....
..+NNNNNNNNNNNNNNNNNNND=,.....$NNNNNNNNNNNNNNNNNNNNNNNN7.....
.
...DNNNNNNNNNNNNNNNNNNNNNNNNNNN+.....7NNNNNNNNNNNNNNNNNNNNNNNND...
.....
....:NNNNNNNNNNNNNNNNNNNNNNNNNN.....$NNNNNNNNNNNNNNNNNNNNNN~.....
....
.....:ZNNNNNNNNNNNNNNNNNNNNNNN=.....DNNNNNNNNNNNNNNNNNNNO~.....
...
.....ZNNNNNNNNNNNNNNNNNNNNNNNI.....+NNNNNNNNNNNNNNNNNNN=.....
.....7NNNNNNNNNNNNNNNNNNNND.....INNNNNNNNNNNNNNNNNN7.....
.....+ZNNNNNNNNNNNNNNNNN+....:ONNNNNNNNNNNNNNN$+.....
.....:I8DNNNNNNNNNNNNN~..~NNNNNNNNNNNND8I.....
.....,,=?Z8DDNNNND=8NNNDD87?,.....
.....
.....
```

```
.....
IIIIIIIIII:I+.............?7,............,?=....,7777777I,..=7777777?,....,I=....
NNNNNNNNNN+D$,....,,,,,,..8N:...........NNN8...:NNNNNNNNN7.$NNNNNNNNN...?NNN~...
....8D~...+D$,...ONNNNNN=.8N:..........DN?ON7..:NNNNNNNNN7.$NNNNNNNNN,.:NN~$NZ..
....8D~...+D$,.............8N:.........~NNNNNN$.:N$IIIII7ND.$NZ?????NN:.8NNNNNN,.
....8D~....?NNNNNNNNN.....:ZNNNNNNNNO$N7....8N=:NNNNNNNNO~.$N?.....DN:7N....,8N+
....,,.....,,,,,,,.....,,,,,,,,,,,,,.....,..,,,,,,,,,....,.....,,.,,.....,,
^C
!
line con 0
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
webvpn gateway R1_gateway
 ip address 172.11.101.1 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1225457800
 inservice
 !
webvpn context vpn
 ssl authenticate verify all
 !
 nbns-list verkkolevy
   nbns-server 10.8.4.250
 !
 policy group R1_policy
   nbns-list "verkkolevy"
   functions file-access
   functions file-browse
   functions file-entry
   hide-url-bar
 default-group-policy R1_policy
 gateway R1_gateway
 inservice
!
!
end
```