Tuomo Valtari

Mobiilin työntekijän tietoturva

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan ko
Insinöörityö
3.6.2012

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Tuomo Valtari Mobiilin työntekijän tietoturva 51 sivua + 1 liite 3.6.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan ko
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Lehtori Marko Uusitalo

Mobiilin työntekijän mahdollisuus yritysverkon etäkäyttöön on usein yritysverkon ulkopuoliselta käytöltä eristämisen vuoksi varsin rajoittunut. Työn tarkoituksena on toteuttaa myös pienille yrityksille tietoturvallinen sekä topologialtaan mahdollisimman yksinkertainen ratkaisu, joka mukautuu kuitenkin moneen käyttötarkoitukseen, poistamaan yrityksen verkon etäkäytön rajoitteita. Verkon on tarkoitus tarjota samat palvelut etäkäyttäjälle, kuin sillä verkon sisältä käytettäessä on.

Työ jakautuu teoria- ja työosuuteen. Teoriaosuudessa käydään yleisiä etätyöntekijän tietoturvatekniikoita ja niiden käyttötarkoituksia läpi sekä mahdollisia etäkäytön turvauhkia työntekijän ja yrityksen kantilta. Työosuudessa käydään luonteeltaan opastyyppisesti läpi käytetyt tekniikat ja laitteet sekä tekninen toteutus ratkaisun jokaisen komponentin osalta.

Käytännön työosuudessa luodaan etätyöntekijälle soveltuva, tietoturvallinen ratkaisu turvattoman internetin yli. Virtuaalinen lähiverkko toteutetaan käyttäen Juniper-laitteen dynaamista Remote Access VPN -toteutusta, jolla luodaan IPSec VPN -tunneli. Käyttäjän autentikointiin käytetään IKE-avaimenvaihdon lisäksi erillistä Radius-autentikointia. Autentikointipalvelimelle määritetään LDAP-käyttäjäkantaan käyttäjä, jonka autentikointiin käytetään LDAP-käyttäjätunnusten lisäksi kertakäyttösalasanaa. Kertakäyttösalasana eli OTP generoidaan käyttäen Yubikeyn OTP-syötteitä.

Avainsanat	Etätyöntekijä, VPN, RADIUS, Juniper SRX, Yubikey, OTP, kahden tekijän autentikointi

Metropolia

Abstract

Author Title Number of Pages Date	Tuomo Valtari Mobile worker's security 51 pages + 1 appendice 3 June 2012
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data Networks
Instructor	Senior lecturer Marko Uusitalo

In most cases a company's network is firewall protected and the private network is completely inaccessible from the outside network. Meaning of this work is to create as simple topology as possible which can be easily adjusted to different environments. The aim is to provide the same functions for remote workers as the persons working from inside the company have.

This thesis is divided in two parts, i.e. theory and practical implementation. In the theoretical part, general security considerations for remote workers and the company are considered as well as common technologies for strengthening security and applications in which those technologies are used. The practical implementation is presented in a guide like format. The used technologies and machines are reviewed and each part of the design is closely described.

In this project a strong security solution suitable for remote workers is implemented over the unsecured Internet connection. This VPN solution is carried out by Dynamic VPN which is Juniper's implementation of Remote Access VPN. Remote Access VPN is secured in IPSec network tunnel mode. In IPSec tunnel, IKE key negotiation is used for phase one authentication and for phase two IPSec extended XAuth is used for RADIUS based authentication. On Radius server LDAP user is created with LDAP+OTP as authentication method, meaning a one-time password is added to the normal user password. OTPs are generated via Yubikey.

Keywords	Remote worker, VPN, Radius, Juniper SRX, Yubikey, OTP, 2-factor authentication

Sisällys

Lyhenteet

3G	Kolmannen sukupolven matkapuhelinteknologia, joka tukee suurempia bittinopeuksia.
802.1x	IEEE:n standardi porttikohtaiselle valtuutukselle. Estetään luvaton kommunikointi 802.1x-liityntäpisteen kautta.
cli	Komentorivipohjainen käyttöliittymä.
DHCP	Verkkoprotokolla, jonka pääasiallinen tehtävä on jakaa IP-osoitteita sille määritellylle asiakaskoneille.
DMZ	Demilitarisoitu alue, joka yhdistää yrityksen yksityisen verkon turvattomampaan liityntään kuten internetiin.
EAP	Tunnistusprotokolla, joka välittää viestejä käytännössä Radius-asiakkaan ja -palvelimen välillä.
http(s)	Protokolla, jota WWW-palvelimet ja selaimet käyttävät tiedonsiirtoon. https tarjoaa salauksen http:n ollessa salaamaton.
IKE	Sovellustason avaintenvaihtoprotokolla. IKE-osapuolet neuvottelevat yhteiset turvaparametrit.
IPSec	Joukko verkkoprotokollia suojaamaan yksityistä liikennettä verkon yli.
MAC-osoite	Verkkosovittimen 48-bittinen yksilöivä tunniste, joka on useimmiten fyysisesti kirjoitettuna kortille.
mbitps	Megabittiä per sekunti -tiedonsiirtoyksikkö.
NAT	Osoitteenmuunnos IP-osoitteille, jossa julkiset IP-osoitteet käännetään yksityisen verkon osoitteiksi.
OATH	Avoimiin standardeihin pohjautuva arkkitehtuuri autentikoinnille.

OTP	**O**ne **T**ime **P**assword eli kertakäyttösalasana, joka siis generoidaan kertaalleen autentikointia varten ja tämän jälkeen luodaan uusi syöte.
PoE	Virta ethernetin yli, eli tarjoaa tehonsyötön ethernet-liitäntään liitetylle laitteelle.
QoS	Liikenteen luokittelu ja priorisointi sovellusten, käyttäjien tai liitäntöjen perusteella reitittimissä.
RADIUS	IETF:n standardoima verkkoprotokolla, joka tarjoaa keskitetysti autentikoinnin, valtuutuksen sekä tilastoinnin.
SDK	Kokoelma ohjelmiston kehitystyökaluja, jolla voidaan muokata tai luoda sovelluksia.
SSH	Salattu tietoliikenneprotokolla, jota yleisemmin käytetään SSH-asiakassovelluksen ja SSH-palvelimen välisiin yhteyksiin.
SSL	Tietoverkkosalausprotokolla liikenteen salaukseen turvattoman verkon yli.
token	Kertakäyttösalasanoista puhuttaessa laite tai ohjelma, joka näyttää tai generoi kirjautumiseen käytettävän avaimen käyttäjälle.
UTM	**U**nified **T**hreat **M**anagement. Sisältää keskitetysti esimerkiksi palomuurin ja virustorjunnan.
Virtualisointi	Tekniikka, joka eriyttää raudan, käyttöjärjestelmät ja sovellukset omiin kerroksiinsa.
VPN	Virtuaalinen lähiverkko – näennäisesti muodostettu lähiverkko laajemman verkon yli.
WLAN	Langaton lähiverkko.
Yubikey	Yubico –yrityksen kehittämä laitteistopohjainen token-laite.

1 Johdanto

Työn tarkoituksena on toteuttaa hyödyntäen Metropolia Ammattikorkeakoulun laboratorion laitteita sekä avoimen lähdekoodin tekniikoita hyödyntäen pienelle tai keskisuurelle yritykselle hyvin soveltuva ja mukautuva etätyöntekijän tietoturvaratkaisu. Kyseisessä ratkaisussa julkisen verkon yli luodaan tietoturvallinen yhteys, jossa etätyöntekijän laitteiden aiheuttamat uhat ovat huomioituina sekä riski tietomurtoon on minimoitu sekä käyttäjän että yrityksen kantilta.

Aihe insinöörityöhön heräsi kiinnostuksesta yrityksissä jatkuvasti yleistyvän etätyön käytöstä yrityksissä sekä sen kasvavien tarpeiden täyttämisestä ja tästä suoranaisesti aiheutuvien turvallisuustekijöiden pohdinnasta. Työ on jaettu kahteen osaan: teoreettiseen pohdintaan ja käytännön toteutukseen.

Teoriaosuudessa pohditaan etätyöntekijän tietoturvaa sekä käyttäjän itsensä kannalta että sen luomista haasteista yrityksen tietoturvalle. Samalla käsitellään yleisesti toimintaperiaatteet seuraavista työssä käytössä olevista tekniikoista ja laitteista: VPN:ää, 802.1x:ää, Juniper-laitteita, kahden tekijän autentikointia. Tekniikat käydään läpi teoreettiselta toiminnaltaan ja samalla pohditaan mahdollisia käyttökohteita mobiilin työntekijän kannalta.

Käytännön työosuudessa toteutetaan suunnittelun pohjalta etäkäyttöratkaisu. Osuudessa lähdetään liikkeelle verkon rakenteesta, siirrytään käymään läpi ratkaisun laitteita ja tekniikoita, jonka jälkeen käydään opasluonteisesti toteutusvaihe, jossa käydään läpi Yubikeyn implementointi järjestelmään, Radius-autentikointipalvelimen määrittely sekä VPN-yhteyden luonti.

2 Etätyöntekijän tietoturva

2.1 Etätyöntekijän laitteet

Työntekijän työssä tarvitsemat laitteet eivät enää usein rajoitu pelkkään työasemaan sekä tämän sisältämään dataan, vaan yhä useammin yritykset tarjoavat työntekijöilleen henkilökohtaisen kannettavan tietokoneen, mobiililaitteita, USB-muisteja, optisia medioita ja niin edelleen. Mikäli näille välineille tallennetaan yrityksen tietoja ja niitä kanniskellaan jatkuvasti mukana, aiheutuu riski välineiden katoamisesta tai joutumisesta vääriin käsiin. Yrityksen tietojen katoamisen ohella eräs riski voi olla esimerkiksi matkapuhelimelle asetettu kertakäyttösalasanoihin perustuva kirjautuminen, jolloin vääriin käsiin joutuessaan hakkeri saattaa päästä käsiksi suoraan yrityksen tietoverkkoon.

Fyysiseen tietoturvaan perustuvat riskit usein sivuutetaan, vaikka ne ovat ratkaistavissa suhteellisen yksinkertaisin keinoin. Tietoja sisältävien laitteiden levyt voidaan esimerkiksi salata, jolloin tietoihin ei pääse käsiksi tietämättä salauksen purkavaa salasanaa. Muutenkin estämällä laitteisiin kirjautuminen riittävän vahvalla käyttäjätunnus - salasana – yhdistelmällä, voi estää pääsyn tietoihin. Viimeisenä keinona tietojen säilyttämisen strategiassa voisi toimia esimerkiksi niin kutsuttu ”myrkkypilleri”, jossa tietoväline pyyhkisi automaattisesti levynsä tiettyjen hallinnallisten attribuuttien toteutuessa.

Etätyöntekijän käyttämien laitteiden sisältämä tietoturva voi olla myös tietoturvariski itsessään. Esimerkiksi niinkin yksinkertainen asia kuin kirjautuminen avoimiin langattomiin verkkoihin paljastaa toisille verkkokäyttäjille avoimesti verkossa liikkuvan liikenteen ja jo yksinkertaisilla työkaluilla tästä liikenteestä voi kaapata esimerkiksi sivustoille syötetyt salasanat, mikäli kirjaudutaan tavalliselle http-sivulle. Muina uhkina tietoturvalle voivat toimia muun muassa käyttöjärjestelmän tietoturvaohjelmistot tai niiden puuttuvuus, ohjelmistoversiot sekä käyttäjän itsensä aiheuttamat. Yleisesti ottaen tämä tarkoittaa sitä, että laitteille tulisi olla asennettuna tietoturvaohjelmistoina vähintäänkin palomuuri- ja virustorjunta-yhdistelmä, asettaa ohjelmistot ja käyttöjärjestelmä päivittymään automaattisesti, mikäli vain mahdollista, sekä estää esimerkiksi langattoman verkkolaitteen asetuksista liittyminen avoimiin WLAN-verkkoihin. Kyseisillä tekijöillä saadaan myös käyttäjän itse aiheuttamia riskejä vähennettyä. (Hines: Mobile workers still struggling with security.)

2.2 Yrityksen näkökulma

Yrityksen kannalta etätyöntekijät aiheuttavat sekä riskin tietojen häviämiseen että hakkereille mahdollisen pääsyn järjestelmiin. Peruspilarina etätyöntekijän tietoturvalle voidaan pitää, että yhteys asiakaskoneeseen suoritetaan käyttäen vahvaa kaksisuuntaista tunnistautumista. Kriittisiin verkkopalveluihin olisi esimerkiksi hyvä lisätä token-pohjainen todennus turvan lisäämiseksi.

Laitteistovalinnat ja sovellustoteutukset toimivat fyysisenä pohjana yrityksen tietoturvalliselle ympäristölle. Tästä syystä yrityksen IT-henkilökunnan koulutuksen on tärkeä olla nykyajan tarpeita vastaavalla tasolla tai vaihtoehtoisesti voidaan hyödyntää ulkoisia asiantuntijapalveluita. Pienemmissä yrityksissä jo pienillä panostuksilla saadaan erittäin tietoturvallisia toteutuksia. Valitettavasti IT-kulut ovat varsin usein kohde, josta säästetään, vaikka panostukset voisivat helposti maksaa itsensä moninkertaisesti takaisin.

Kuitenkaan aina ei edes varautuminen riitä, vaan yrityksen on syytä kehittää strategia erilaisten kriisitilanteiden varalle, sillä yritys on aina vastuussa esimerkiksi asiakastietojensa häviämisestä. Yrityksen tietoturvan ei tule olla vain panostamista yrityksen tarpeisiin, vaan turvallisuutta tulee vaalia työntekijöiden jokapäiväisiin toimiin. Riittävällä ohjeistuksella sekä yhtenäistämällä turvallisuuskäytännöt etätyöntekijöille päästään jo hyvään alkuun. Tämä tarkoittaa nykyaikana esimerkiksi sitä, että etätyöntekijät eivät käytä sosiaalista mediaa työaikana paikkatietojensa osoittamiseksi pitkäkyntisille. Sosiaalinen media toimii myös samalla helppona keinona esimerkiksi perheenjäsenten nimien kalastamiseksi, jotka valitettavan usein ovat käytössä tärkeiden järjestelmien salasanoina.

Tärkeiden tietojen säilyvyys käyttäjällä on asia, johon tulee kiinnittää huomiota. Esimerkiksi suojakalvon asettaminen näytölle estää näkyvyyden sivullisille, kun liikutaan yleisillä paikoilla. Työntekijöitä on syytä myös opastaa lukitsemaan työasemansa aina sen läheisyydestä poistuessa. Tietojen säilyvyydellä voidaan tarkoittaa myös fyysisten tietojen säilyvyyttä. Tärkeiden tietojen etätyöpisteiltä varmistus yrityksen palvelimille tulisi olla käytössä vähentämään levyn hajoamistilanteiden vaikutuksia. (Dubrawsky: s. 86.)

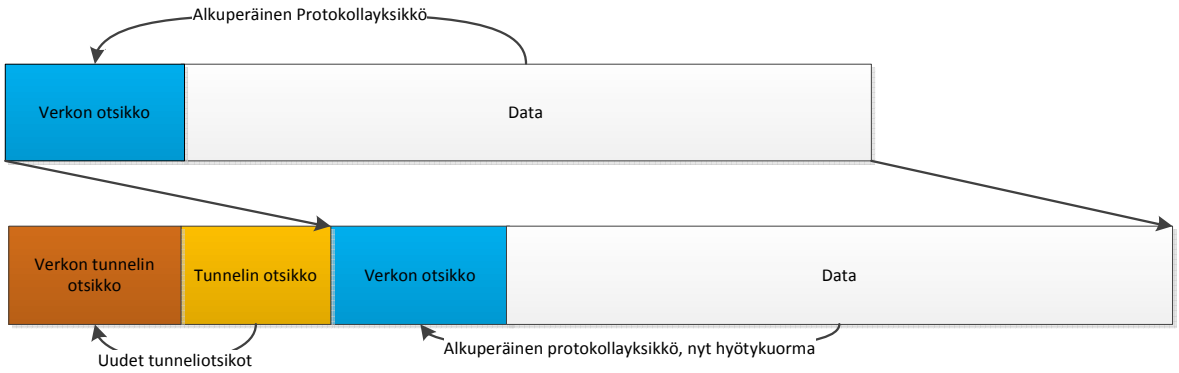
3 VPN

3.1 Taustaa

VPN tarkoittaa vapaasti suomennettuna virtuaalista yksityisverkkoa. Nimensä mukaisesti sillä muodostetaan näennäisiä yksityisiä verkkoja laajemman verkon avoimen verkon, kuten Internetin yli, joka Internetistä poiketen on suljettu, salattu, ja jaettu vain osapuolten kesken.

VPN:llä voidaan yhdistää useampi verkkoympäristö toisiinsa virtuaalisen yksityisverkon muodostamiseksi pisteiden välille. Tätä VPN-yhteystapaa kutsutaan Site-To-Site VPN:ksi ja sitä käytetään esimerkiksi yrityksen etätoimipisteiden liittämiseksi yhteiseen yksityisverkkoon. Etätyöntekijälle oleellisempi VPN-yhteystapa on Remote Access VPN, jossa yhdeltä työasemalta muodostetaan virtuaalinen yhteys haluttuun verkkoon tai laitteeseen. Site-To-Site VPN:ssä yhteys usein muodostetaan täysin laitteistopohjaisena, eli muun muassa kytkimillä, reitittimillä tai palomuureilla, jolloin molemmat osapuolet voivat jakaa yksityiset verkkonsa. Remote access VPN taas voidaan toteuttaa täysin ohjelmistopohjaisena, jolloin VPN-asiakaan puolelta riittää asiakasohjelmien käyttö yksisuuntaisen virtuaaliyhteyden luomiseksi työasemalta verkkoon tai laitteeseen.

Käytännössä VPN-yhteyspisteiden välille muodostetaan tunneli liikenteelle, jossa alkuperäinen paketti sisällytetään ulomman, salatun paketin sisään ennen kuin se lähetetään turvattoman julkisen verkon yli. Tällä ulommaisella paketilla varmistetaan, että tieto säilyy ulkopuolisten näkymättömissä ja vain kyseisen tunnelin sisällä. Yhteyspisteiden päissä sijaitsevat tunneliliitännät, jotka vastaavat sekä lähtevien pakettien kapsuloinnista että niihin saapuvien pakettien jälleen avaamisesta. Tunneliliitännät asetetaan käyttämään tiettyä tunnelointiprotokollaa, joiden tarkoituksena on lisätä turvallisuuskerros. Verkon yksityisyys ja turvallisuus voidaan kuitenkin hoitaa myös fyysisesti, josta esimerkkinä operaattoriverkot fyysisesti muusta verkosta eristettynä. Fyysisesti toteutetut VPN-ratkaisut ovat kuitenkin usein varsin kalliita toteuttaa perinteisiin ratkaisuihin verrattuna, eivätkä ne täten palvele etätyöntekijän tarpeita, sillä etätoimipiste harvoin sijaitsee tietyn yhteyden takana.



Kuva 1. Tunneloinnin kehysrakenne

Tietoturvallisen VPN-yhteyden perusta ovat autentikointi, kapselointi sekä salaus. Kun turvallisuustekijät huomioidaan oikein, saavutetaan toteutuksessa turvallinen taso autentikoinnin, tiedon luotettavuuden sekä tiedon eheyden osalta. Autentikoinnilla varmistetaan, että tieto tulee vain valtuutetulta taholta tai laitteelta. Autentikointi tunnelin muodostamiseksi voidaan hoitaa muun muassa seuraavilla tavoilla ja niiden kombinaatioilla:

- käyttäjänimi ja salasana
- kertakäyttösalasanat
- biometrinen tunnistautuminen
- etukäteen määritellyt avaimet
- digitaaliset sertifikaatit.

Tiedon luotettavuudella varmistetaan, ettei tiedon kulku keskeydy valtuuttamattomien tahojen toimesta. VPN:n tapauksessa luotettavuus varmistetaan kapseloimalla ja salaamalla liikenne. Tiedon eheydellä varmistetaan, että tieto säilyy muuttumattomana kulkiessaan verkossa. VPN käyttää muun muassa yksisuuntaisia tiivistysfunktioita sekä Mac-osoitteita tiedon eheyden varmistamiseksi. (Dubrawsky: s. 72-74.)

3.2 Tunnelointiprotokollat

Yleisesti käytössä olevat tunnelointiprotokollat ovat IPSec, SSL, GRE, L2TP ja PPTP. Protokollat tulee olla määriteltyinä molempiin tunnelin päihin. Seuraavassa luvussa käsitellään tarkemmin IPSec:iä, joka on myös käytännön osuudessa käytetty tunnelointiprotokolla.

3.2.1 IPSec

IPSec on joukko TCP/IP-perheeseen kuuluvia protokollia suojaamaan IP-liikennettä. Toisin kuin eräät salausprotokollat kuten SSL, TLS ja SSH, jotka toimivat korkeammilla sovelluskerroksilla, operoivat IPSec-verkkokerroksessa. IPSec onkin kyseisiä protokollia joustavampi toimiessaan alemmalla tasolla. Tämä siksi, että sitä voidaan käyttää suojaamaan sekä verkkokerroksen että viitemallissa sen yläpuolisia kerroksia. Kuitenkin IPSec:iä käyttävien VPN-asiakassovelluksien tulee olla varta vasten IPSec:lle suunniteltuja, toisin kuin esimerkiksi TLS:n tai SSL:n tapauksissa. Eräs ongelma verkkokerroksessa toimivassa IPSec:ssä verrattuna alemman tason protokolliin on, että IPSec:n tulisi pystyä hallitsemaan myös liikenteen vakaus- ja pirstoutumisongelmat, jotka yleisesti hoidetaan kuljetuskerroksessa.

IPSec:n käyttö ei ainoastaan rajoitu VPN-tunneleihin, vaan sillä voidaan suojata erinäisiä sovelluksia. Yksi käyttötarkoitus on suojata langattomia WLAN-lähiverkkoja joko laitteiden käyttämien suojauksien sijasta tai niiden lisänä. IPSec:ssä eräs puute on kuitenkin, että sen standardissa ei ole määritelty lainkaan IP-osoitteiden hallintaa. Valmistajakohtaiset ratkaisut tarjoavat erinäisiä tapoja, kuten DHCP:llä IP-osoitteen jakamista VPN-asiakkaalle, joka kuitenkin tarvitsee erillistä asiakasohjelmaa osoitteen saamiseksi.

IPSec:iä voidaan käyttää seuraavissa moodeissa:

- Kuljetusmoodi: käytetään isäntä-isäntä – liikenneyhteyksiin. IP-paketin hyötykuorma salataan ja/tai autentikoidaan. Koska IP-paketin otsikkotietoa ei muokata tai salata, säilyy paketti eheänä reitityksessä. Mikäli AH on käytössä, ei IP-osoitteille voi tehdä osoitteenkäännöstä, sillä tämä mitätöisi tiivistysfunktion. Kuljetus- ja sovelluskerros on suojattu aina tiivisteellä, joten niitä ei voi muokata mitenkään.

- Tunnelimoodi: koko IP-paketti on salattu ja/tai autentikoitu. Tällöin alkuperäinen paketti sisällytetään uuteen ja sille lisätään uusi otsikkotieto. Tätä moodia käytetään muun muassa yksityisverkkojen liikenteen yhdistämiseksi (Site-To-Site VPN) tai isäntä-verkko yhteyksissä (Remote Access VPN).

IPSec käyttää seuraavia protokollia moniin toiminteisiinsa, jotka voidaan jakaa luokittain:

- avaintenvaihtoprotokolliin
- protokollat pakettivirtojen suojaamiseksi.

Avaintenvaihtoprotokollaksi IPSec-toteutuksissa suositellaan IKE-protokollaa. IKE:n tarkoituksena on luoda turvallisuusassosiaatio käsittelemällä neuvotteluprotokollia ja -algoritmejä, joilla luodaan autentikointiavaimet IPSec:lle. IKE käyttää Diffie-Hellman-avaintenvaihtometodia luodakseen istunnon aikaisen salausavaimen salatakseen muun IKE-liikenteen.

IPSec tarjoaa kaksi pakettivirtojen turvaamiseen käytettävää protokollaa, joista harvemmin käytetty AH tarjoaa todennuksen sekä viestien eheyden, mutta ei sisällä luottamuksellisuutta. Useimmin käytetään ESP-protokollaa, jota käytetään pakettivirtojen luottamukselliseen salaamiseen, yhtenäisyyteen ja oikeellisuuteen. ESP tukee myös ”ainoastaan autentikointi” ja ”ainoastaan kryptaus” -tiloja, mutta näiden käyttö, varsinkaan ilman autentikointia, ei ole suositeltavaa. Toisin kuin AH, ESP ei suojele IP-paketin otsikkotietoa. Kuitenkin tunnelointitilassa alkuperäinen IP-paketti on salattuna lisätyllä pakettiotsikkotiedolla, jolloin ESP-suojaus on käytössä kokonaan kyseisessä paketissa salaten sisäisen otsikkotiedon ulkoisen otsikkotiedon jäädessä salaamattomaksi. (Wikipedia: IPSec-dokumentti.)

3.2.2 SSL VPN

SSL VPN käyttää SSL-protokollaa tietoturvallisen etäyhteyden muodostukseen. SSL VPN:llä voidaan tunneloida koko verkon liikennettä tai tiettyä sovellusta, joten se sopii sekä Site-To-Site VPN että Remote Access VPN -toteutuksiin. Tällöin perinteisellä SSL:ää tukevalla web-selaimella muodostetaan yhteys haluttuun yksityisverkkoon. Ylei-

nen käyttötarkoitus etäkäyttäjälle on pääsy esimerkiksi tiettyyn verkkosovellukseen, asiakas- tai serveriohjelmistoihin tai määriteltyyn sisäverkkoon. Yhteys ei ole rajattu vain tiettyyn paikkaan, sillä SSL VPN pohjautuu http- sekä https -protokollien käyttöön, jolloin verkkojen ulospäin menevän liikenteen estot eivät merkitse kuin vaikkapa IP-Sec:ssä. Etäkäytön kannalta SSL VPN ei myöskään IPSec:stä poiketen kohtaa ongelmia verkon mahdollisesta NAT:sta johtuen. Etäkäyttäjän kannalta SSL VPN -toteutukset voidaan jakaa seuraavasti:

- asiakasohjelmaton moodi
- ohut asiakasohjelma -moodi
- tunnelimoodi.

Asiakasohjelmaton moodi turvautuu täysin web-selaimen varaan toimien sovelluskerroksella. Tällöin tarvitaan pohjalle käyttöjärjestelmällä varustettu etätyöasema, mutta nykyään myös matkapuhelimet sisältävät riittävät edellytykset verkkoselainkäyttöön. Tällöin http:n tai https:n välityksellä päästään selaamaan hakemistosivua, jossa voi olla esimerkiksi linkkejä verkkopalvelimiin tai kirjautumissivu Outlook Web Accessiin. Tiedostojen jako onnistuu myös CIFS:n välityksellä, jolla palvelimilta voidaan esimerkiksi ladata tiedostoja. Tunnelin yhdyskäytävä hoitaa osoitteiden tai protokollien muunnon sekä sisällön uudelleen kirjoituksen.

Ohut asiakasohjelma -moodissa, jota kutsutaan myös TCP-porttien uudelleenohjaukseksi, oletetaan että asiakasohjelma käyttää TCP:tä yhdistymään esimerkiksi tunnettuun palvelimeen ja porttiin. Yhteyteen vaaditaan asiakasohjelma, joka usein on Java-pohjainen appletti. Ohjelma avaa portit, jotka ylläpitäjä on konfiguroinut sitä varten ja toimii näin TCP-välityspalvelimena asiakaskoneella palveluille, jotka yhdyskäytävään on määritelty. Käyttökohteena ohut asiakasohjelma -moodissa on yleensä sähköpostipalvelut, kuten SMTP-, POP3- tai IMAP-pohjaiset sovellukset.

Tunnelimoodissa siirretään tietoa verkkokerroksella, joten se tukee kaikkia IP-pohjaisia sovelluksia. Tunnelimoodi vaatii asiakasohjelman, jolla etäkone kirjautuu VPN-yhdyskäytävään, ja tämän jälkeen uudelleen luo kyseisen verkon asiakaskoneelle. Tä-

mä mahdollistaa, että kaikki verkon liikenne kulkee SSL-tunnelin läpi, jonka kautta työasema on suoraan yhteydessä määriteltyyn etäverkkoon tai palveluun.

SSL VPN on varsin tietoturvallinen ratkaisu etätyöntekijälle, eikä sen määrittäminen asiakaskoneisiin vaadi paljoakaan toimia. Ylläpidollisesti yritykselle ratkaisu on myös suhteellisen yksinkertainen, sillä se ei vaadi erityismäärittelyjä palomuureihin, eikä määrittelyjä esimerkiksi NAT:n ohittamiseksi. SSL VPN etäkäyttäjän näkökulmasta sisältää kuitenkin muutaman turvariskin. Koska se on avoin järjestelmä, ovat sovellukset avoinna myös kaikille muille laajemman verkon käyttäjille, mikäli erityismäärittelyjä autentikoinnin suhteen ei ole tehty. Etäkäyttäjät voivat myös siirtää yrityksen verkosta tietoa käyttäjien kotikoneille, jolloin yrityksen sisäinen tietoturva voi olla uhattuna. (NCP Network Communications Products engineering, Inc.: SSL VPN – alternative Remote Access technology.)

4 802.1x

4.1 Taustaa

802.1x on IEEE:n standardi porttikohtaiselle autentikoinnille ja valtuutukselle IEEE 802 -standardin määrittelemissä lähiverkoissa eli Ethernet- sekä WLAN-verkoissa. Se operoi OSI-mallin toisella kerroksella eli siirtokerroksella. Porttikohtaisella autentikoinnilla voidaan myös estää asiakaslaitteen pääsy esimerkiksi tiettyyn kytkimen porttiin tai muuhun fyysiseen tai loogiseen Ethernet-liittyntään.

Aikoinaan, kun ensimmäiset langattomat puhelimet ja analogiset matkapuhelimet tulivat markkinoille, kuka tahansa pystyi yksinkertaisesti oikealla taajuudella toimivalla skannerilla kuuntelemaan heille tarkoittamattomia puheluita. Sama kuitenkin päti myös ensimmäisiin 802.11-standardin laitteisiin. Nykyään etenkin paljolti yleistynyt siirtyminen langallisista siirtoteistä radiotaajuuksilla toimiviin langattomiin loi tarpeen 802.1x:n kehittämiselle, sillä esimerkiksi yritysverkoissa kantama saattoi helposti ulottua sen tilojen ulkopuolelle. Pian langattomien verkkolaitteiden markkinoille saapuessa kehitettiin laitteille yksinkertainen WEP-salaus, jossa salausavain on staattinen ja kaikille yhteinen, ja pian salaus todettiin kuitenkin helposti murrettavaksi. WEP:ssä ei myöskään ollut keinoja yksinkertaiseen salausavaimien jakeluun tai hallinnointiin ja tämän vuoksi

useat yritykset halusivat lisää turvallisuutta perinteisen käyttäjänimi – salasana -yhdistelmän lisäksi, jolloin kehitettiin 802.1x.

802.1x soveltuu erinomaisesti esimerkiksi yrityksen WLAN-vierasverkon autentikointiin sekä myös sisällytetyksi olemassaoleviin VPN-toteutuksiin, joissa voidaan kuvitella IP-Sec:iä verkon sisäänpääsyn väylänä 802.1x:n toimiessa sisäänkäyntinä. Eli esimerkiksi etäkäyttäjän kotiverkossa muut perheenjäsenet eivät pääse VPN:n ”sisään” vaan heiltä vaaditaan erillinen 802.1x-autentikointi. 802.1x-toteutukset vaativat kuitenkin aina erillistä autentikointipalvelinta kuten RADIUS:sta, jolle ehdoton vaatimus on tuki EAP-protokollalle. Jokaisella yhdistävällä koneella tulee myös olla 802.1x-yhteensopiva asiakasohjelmisto käytössä, jossa käyttäjä-salasana-yhdistelmää käytetään valtuutukseen. (Microsoft Corporation: IEEE 802.1X for Wired Networks and Internet Protocol Security with Microsoft Windows.)

4.2 Toiminta

802.1x avainprotokollana toimii EAP-lähiverkon yli eli EAPOL. 802.1x korvasi käytännössä piirikytkentäiset PPP-verkot, mutta tätä nykyäänkin EAP sijaitsee PPP-autentikointiprotokollan sisällä tarjoten näin pohjan useille eri autentikointitavoille. EAP:n avulla päästään eroon vain yhdentyyppisistä autentikoinneista ja sitä voidaan käyttää kaikkiin salasanoista sekä haaste-vastaus-tokeneista julkisen avaimen sertifikaatteihin perustuviin tapoihin. 802.1x sisältää kolme osapuolta, jotka ovat:

- Asiakas eli supplikantti on fyysiseen tai loogiseen porttiin kytkeytyvä asiakaslaite (esimerkiksi langaton verkkokortti), joka pyytää palveluun (porttiin) kytkeytymistä. Asiakkaan tehtävä on vastata autentikointitietoihin, joiden avulla asiakas hakee valtuutusta palveluun kytkeytymiselle.

- Autentikaattori on laite (esimerkiksi kytkin tai 802.11-standardin tukiasema), joka sisältää fyysisen/loogisen portin tai portteja. Toisaalta autentikaattori voidaan käsittää myös itsenäisenä komponenttina – tukiaseman sisältämänä palveluna, mutta autentikaattori voi myös sijaita kokonaan erillisessä laitteessa. Autentikaattori tarjoaa asiakkaalle valtuutuksen loppupään palveluihin, mikäli asiakas on oikeutettu tähän.

- Autentikointipalvelin on laite (esimerkiksi RADIUS-palvelin tukiaseman fyysisen liitynnän puolella), joka tutkii asiakkaan autentikaattorin kautta lähettämää valtuutusta. Autentikointipalvelimen tehtävä on välittää autentikaattorille tieto valtuutuksesta, mikäli tiedot vastaavat vaadittuja. Vaatimuksena on tuki EAP-protokollalle.

802.1x-autentikointi noudattaa pääpiirteittäin seuraavia vaiheita:

1. Aina uuden asiakkaan ilmentyessä autentikaattori asettaa kyseisen liityntäportin luvaton-tilaan. EAP:n käyttämät protokollat toimivat linkkitasolla, jolloin se toimii ilman korkeamman tason rajoitteita. Tällä tavoin se myös estää korkeammilla tasoilla tapahtuvan liikennöinnin, kuten DHCP:n ja HTTP:n. Autentikaattori lähettää asiakkaalle aluksi ”EAP-pyyntö/identiteetti”-paketin tunnistaakseen asiakkaan.

2. Asiakas vastaa autentikaattorille ”EAP-vastaus/identiteetti”-paketilla, jonka autentikaattori välittää suoraan autentikointipalvelimelle.

3. Autentikointipalvelin lähettää takaisin autentikaattorille haasteen (kuten salasanakyselyn). Autentikaattori riisuu saapuneen haasteen IP:stä sekä pakkaa paketin uudelleen EAPOL:ksi ja lähettää sen edelleen asiakkaalle. Riippuen autentikointitavasta viestin sisältö sekä viestien vaihdon määrä vaihtelee.

4. Asiakas vastaa autentikointipalvelimen haasteeseen lähettäen palvelimelle vastauksen autentikaattorin välityksellä.

5. Mikäli asiakkaan tiedot vastaavat palvelimeen määritettyihin, autentikointipalvelin vastaa hyväksymisviestillä, joka välitetään asiakkaalle. Tämän jälkeen asiakkaalla on pääsy esimerkiksi tiettyyn lähiverkkoon, johon voi olla asiakaskohtaisesti määritetty myös muita attribuutteja. Autentikaattori voi muun muassa liittää asiakkaan tiettyyn VLAN:iin tai asettaa sille listan palomuurisääntöjä.

Langattomissa verkoissa autenkointi noudattaa hieman eri proseduuria, sillä laitteet eivät ole fyysisesti yhteydessä verkkoon, vaan jakavat saman siirtokanavan. Langattomissa verkoissa asiakkaan ja liityntäpisteen välille täytyy ensin muodostaa assosiaatio.

Assosiointiprotokollan avulla kommunikoivat laitteet sallitaan oppimaan toistensa MAC-osoitteet. Näiden toimenteiden avulla muodostetaan liityntäpisteeseen virtuaalinen kanava, jonka jälkeen EAP-autentikointi voidaan toteuttaa.

802.1x:n oletuksena on fyysisissä toteutuksissa, että vain yksi laite yhdistetään kerrallaan 802.1x-liitännäiseen kytkinporttiin. Muussa tapauksessa laitteen ollessa autentikoitu ja tätä myötä myös liityntäportti autorisoitu-tilassa muut laitteet voisivat liittyä verkkoon autentikoimattomana. Kyseistä toiminnetta kutsutaan yhden asiakkaan operoinniksi. Jotkin kytkimet kuitenkin poikkeavat standardista sen verran, että pystyvät autentikoimaan useamman laitteen samaan porttiin, jota kutsutaan usean asiakkaan operoinniksi. Yrityksissä yleisesti kyseiset kytkimet ovat avoimesti esillä, joten useiden laitteiden yhtäaikainen pääsy on käytännössä mahdoton estää. Useimmat 802.1x:ään kykenevät kytkimet pystyvät kuitenkin estämään kaikki kehykset, joissa MAC-lähtöosoite ei ole yhtäläinen, tai vaihtoehtoisesti 802.1x-kehykset välitetään vain tiettyyn kytkimen VLAN:iin. ACL-listauksilla voidaan myös estää muiden laitteiden pääsyä verkkoon.

802.1x ei kuitenkaan ole täysin aukoton ratkaisu. Se on todettu alttiiksi mies-keskellä-tyyppiselle hyökkäykselle. Tällöin tunkeutuja liittää laitteensa fyysisesti jo autentikoidun laitteen porttiin asettaen esimerkiksi hubin kytkimen ja työaseman väliin, ja mikäli porttikohtainen port-security on käytössä, asettaa tunkeutuja jo käytössä olevan MAC-osoitteen. Mahdollisuus kyseisen tyyppisen hyökkäyksen estoon on käyttää 802.1AE-standardiin pohjautuvaa MACSec:iä, joka muodostaa turvallisuusassosiaation tietyn laitteen kanssa. Toinen suositumpi vaihtoehto langallisissa verkoissa on käyttää esimerkiksi IPSec:iä 802.1x:n ohella. Sekä langalliset että langattomat verkot ovat myös alttiita EAPOL-logoff-tyyppiselle DOS-hyökkäykselle. Siinä asiakkaan selväkielisiä EAPOL-logoff-kehyksiä lähetetään kyseisen asiakkaan MAC-osoitteesta, jolloin autentikaattori uskoo asiakkaan haluavan katkaista autentikointi-istunnon ja se katkaiseekin tämän todelliselta asiakkaalta estäen samalla koko verkkoyhteyden. MAC-osoite voidaan myös helposti väärentää, jolloin verkkoon on mahdollista päästä jo autentikoidun laitteen MAC-osoitteella. 802.1x-2010-standardi on kehitteillä, jonka tulisi estää edellisen tyyppiset hyökkäykset käyttämällä IEEE 802.1AE MACSec:iä sekä IEEE 802.1AR -autentikoituja laitteita.

Työntekijöiden hyväksyttyihin laitteisiin tulisi myös, joka kirjautumiskerralla pakottaa uudelleenautentikoinnin autentikaattorille. Tällöin estetään esimerkiksi työasemalle luodun lokaalin järjestelmänvalvojan suora kirjautuminen verkkoon. Esimerkiksi Windows XP:ssä käyttöjärjestelmän tulisi katkaista verkkoyhteys 2 minuuttia käyttäjän kirjautumisen jälkeen, mikäli käyttäjä ei onnistu tarjoamaan oikeita tietoja. Käyttötarkoitukseen sopivan autentikointimetodin valinta on myös erittäin oleellinen osa tietoturvaa 802.1x-pohjaisissa verkkototetuksissa, mistä lisää seuraavassa luvussa. (Snyder: What is 802.1X?)

4.3 RADIUS

RADIUS on IETF:n standardoima verkkoprotokolla, joka tarjoaa keskitetysti autentikoinnin, valtuutuksen sekä tilastoinnin eli AAA-palvelut kohdistetulle käyttöryhmälle tai verkon osalle. RADIUS-termin yhteydessä AAA-palvelut voidaan jakaa seuraaviin osiin:

- Autentikointi: Prosessi käyttäjän tunnistamiseksi, josta yleisin tapa on käyttäjätunnus/salasana-yhdistelmä.

- Valtuutus: Käyttäjäoikeuksien hallinta. Valtuuttaminen vaatii aina käyttäjäidentiteetin selvittämistä autentikointivaiheessa. Autentikoitu käyttäjä autorisoidaan esimerkiksi haulla tiedostosta, tietokannasta tai vaikkapa LDAP-kannasta.

- Tilastointi: Ylläpidetään tietoa verkon käytöstä. Talletetaan tieto jokaisesta käyttäjäsessioista, sen kestosta sekä tiedonsiirtomääristä.

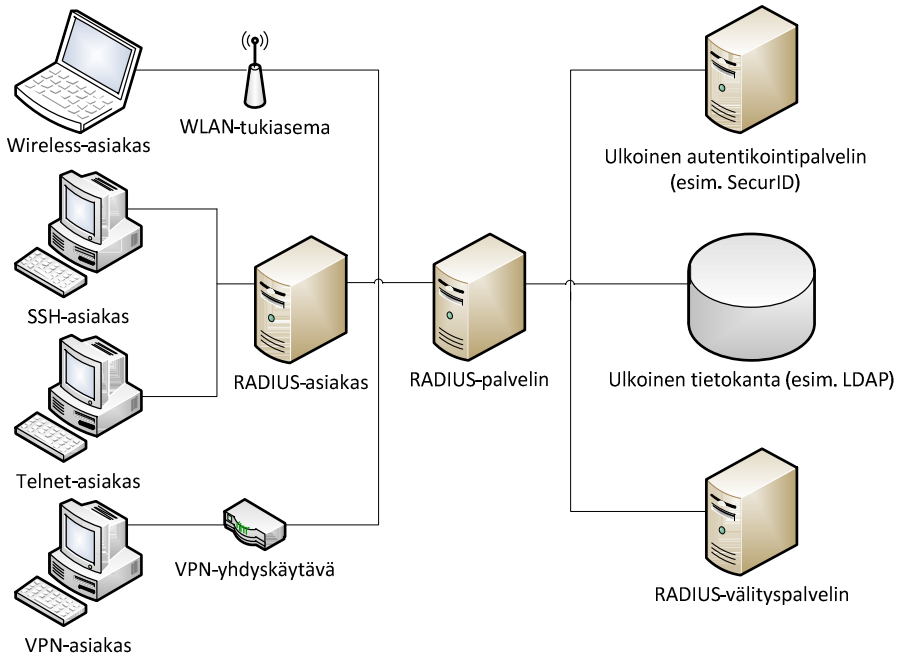
RADIUS-pohjaiseksi rakennettu etäkäyttäjän ympäristö koostuu pääosin neljästä osasta:

- Yhdistävä asiakas käynnistää verkkoyhteyden. Asiakas voi olla esimerkiksi langattomaan 802.1x-pohjaiseen tukiasemaan kytkeytyvä laite.

- RADIUS-asiakas tunnistaa ja välittää pyynnöt verkon reunan ulkopuolelta. Radius-asiakas voi olla esimerkiksi langaton tukiasema tai palomuuri, jonka tulee autentikoida käyttäjä. RADIUS-asiakas voi kysyä yhdistävältä asiakkaalta käyttäjätietoja, jotka se edelleen välittää RADIUS-palvelimelle.

- RADIUS-palvelin vertaa autentikointi- ja valtuutuspyyntöä palvelimen käyttäjätietokantaan. Mikäli lähetetyt tiedot täsmäävät tietokannan kanssa, RADIUS-palvelin hyväksyntä - hyväksyntä-viestin RADIUS-asiakkaalle. Jos taas tiedot eivät täsmää tai tiedoissa on jokin ongelma, lähettää palvelin hyväksyntä-hylkäys-viestin.

- Mahdollisesti ulkoisesta autentikointipalvelimesta, kuten Active Directory, ulkoisesta tietokannasta, kuten LDAP-tietokanta, tai mahdollinen toinen RADIUS-palvelin asetettuna välityspalvelimeksi, johon autentikointipyyntöä verrataan. Tämä ulkoinen palvelin vastaa RADIUS-palvelimelle edellisen kohdan mukaisilla viesteillä tietojen oikeellisuuden perusteella.



Kuva 2. Radiuksen toiminta

RADIUS-asiakas sekä RADIUS-palvelin kommunikoivat RADIUS-pakettien välityksellä, jotka sisältävät pyyntö-vastaus -viestejä – asiakas lähettää pyynnön ja odottaa vastausta palvelimelta. Mikäli viestiä ei vastaanoteta palvelimelta, voi asiakas uusia pyynnön aikajaksoittain. Jokainen paketti ajaa tiettyä tarkoitusta autentikointiin tai tilastointiin liittyen. Paketit voivat sisältää tiettyjä attribuutteja – esimerkiksi RADIUS-asiakkaan laitetiedot.

RADIUS-standardin mukaisesti autentikointi- ja tilastointi-paketit käyttävät UDP-portteja 1645 ja 1646. Standardia on kuitenkin hiottu sen verran, että porttimäärittelyt ovat vaihtuneet porteiksi 1812 ja 1813. Monet yritykset kuitenkin käyttävät vielä vanhan standardin portteja, joten on syytä tarkistaa sekä RADIUS-asiakkaan että RADIUS-palvelimen porttien yhtäläisyys. Molemmat laitteet tulee kuitenkin konfiguroida ennen kuin laitteet voivat kommunikoida RADIUS-pakettien välityksellä. (Juniper Networks: Radius Overview.)

5 Kahden tekijän autentikointi

5.1 Taustaa

Mobiilin työntekijän kannalta salasana on tärkein yksittäinen turvallisuuden tae. Liian yksinkertainen salasana altistaa tietomurrolle, kun taas erityisen monimutkainen on usein vaikeasti muistettavissa ja tästä syystä mahdollisesti jopa tallennettuna ulkoiselle tietovälineelle, mikä aiheuttaa tietoturvariskin etenkin paljon matkustavalle. Eräät palvelut myös tarjoavat salasanan nollausta, joka voi pahimmillaan toimia väylänä salasanamurtautumiselle.

Kahden tekijän autentikointi tai useamman tekijän autentikointi perustuu ajatukseen ”jotakin mitä omistat” tai ”jotakin mitä olet”. Ajatusta voi verrata johonkin, mitä kaikilla on – kotiavain lukkoon. Yksistään keino ei ole turvallinen, sillä kotiavaimen voi hukata. Tällöin keinona pääsyn estoon on vaihtaa asunnosta ovilukko. Kahden tekijän autentikoinnissa yhdistellään siis ainakin kaksi autentikointitapaa tuvallisuuden parantamiseksi, jotka voivat olla:

- käyttäjän tiedossa oleva osa (salasana tai tunnusluku)
- käyttäjän omistama osa (laitteistopohjainen token-avain, pankkikortti tai avain)
- käyttäjän ominaisuus (biometrinen tunniste, allekirjoitus tai ääni).

Eräs tapa välttää ainoastaan salasanaan pohjautuvat tietoturvariskit on sertifikaatteihin pohjautuva ratkaisu. Tällöin voidaan käyttää sertifikaattien valtuuttajia jakamaan erik-

seen käyttäjille sertifikaatit. Kyseinen tapa vaatii käyttämään kuitenkin PKI:tä (Public Key Infrastructure), joka on usein kallis toteuttaa sekä ylläpitää, eikä ole välttämättä kovin yksinkertainen toteuttaa etäkäyttäjille. Toinen hyvin yleinen tapa on käyttää RSA:n SecureID:tä, joka pohjautuu kertakäyttösalasanojen käyttöön. SecureID ei kuitenkaan pohjaudu standardiin, joten se voi aiheuttaa yhteensopivuusongelmia muiden järjestelmien kanssa. Lisensointikulujen johdosta se ei myöskään ole optimiratkaisu pienempien yritysten käyttöön. (Dubrawsky: s. 17.)

5.2 Kertakäyttösalasanat

Yleinen standardeihin pohjautuva kertakäyttösalasana on usein hyvin kustannustehokas ja melko yksinkertaisesti toteutettava ratkaisu. Kertakäyttösalasana on siis salasana, joka on voimassa vain yhden kirjautumissession ajan, jonka jälkeen se uusiutuu. Kertakäyttösalasana ei ole altis perinteisten salasanojen tyyppisille hyökkäyksille, jossa hyökkääjä salasanan haltuunsa saadessaan pääsee kirjautumaan järjestelmään, sillä useampaa yhtäläistä salasanaa ei voi olla. Kertakäyttösalasanat vaativat kuitenkin jonkin ulkoisen laitteen käyttöönsä, sillä ne on lähes mahdoton muistaa. Ulkoisina laitteina voivat toimia muun muassa laitteistopohjaiset token-avaimet, tekstiviestit ja matkapuhelimet.

Kertakäyttösalasanojen luomisalgoritmit pohjautuvat usein satunnaisuuteen, jolloin estetään seuraavien salasanojen ennustaminen. Kertakäyttösalasanat luodaan kahdella tapaa:

- Aikasynkronoidusti-ratkaisu synkronoi tokenit kellonajan perusteella autentikointipalvelimen ja asiakkaan välillä. Se on yleisesti käytössä, mutta voi aiheuttaa ongelmia, mikäli kellot eivät ole täysin samassa ajassa. Aikasynkronoidussa käyttäjän pitää yleensä antaa salasana tietyn aikamääreen puitteissa, jonka jälkeen salasana vaihtuu.

- Laskurisynkronoidusti-ratkaisu synkronoi laskurin autentikointipalvelimen ja asiakkaan välillä. Laskuria siirretään aina, kun laite pyytää kertakäyttösalasanan arvoa. Edellisen aikasynkronoidun tapaan kertakäyttösalasana saadaan laitteen sillä hetkellä näyttämästä arvosta.

Näissä algoritmeissa käyttäjän täytyy syöttää jokin tiedetty arvo, kuten PIN (personal identification number), jotta OTP voidaan luoda. Nykyaikaiset algoritmit käyttävät jotain kryptografista prosessointia luodakseen sen hetkisen salasanan synkronisointiparametrista, salaisesta avaimesta tai aiemmin mainitusta PIN:stä. Esimerkiksi tiivisteiisin pohjautuvat OTP:t käyttävät kryptografisia tiivistealgoritmeja laskeakseen salasanan. (Safer Authentication with a One-Time Password Solution.)

5.3 Yubikey

Yubikey on ruotsalaisen Yubicon kehittämä laitteistopohjainen token-laite, joka näyttää pieneltä USB-tikulta, mutta toimii USB-näppäimistönä. Se tarjoaa turvaa hakkereilta ja haittaohjelmilta lähes yhtäläisellä tasolla esimerkiksi huomattavasti kalliimpien älykorttien kanssa. Kuitenkin suhteessa moneen muuhun vastaavaan toteutuksen ratkaisuun se on erittäin kustannustehokas - hankinta vaatii vain kyseisen avaimen hankintaa, ja Yubico tarjoaa sille pysyvää tunnistautumispalvelua ja useita ilmaisia avoimen lähdekoodin sovelluksia kuten Radius-palvelimen. Yubikeyn hinta tällä hetkellä on 25 dollaria, johon lisätään viiden dollarin postikulut. Isompiin hankintaeriin saa alennusta.

Yubikey käyttää kahden tekijän autentikointia yhdistäen käyttäjän tunteman PIN:n tai salasanan ja laitteen luoman salatun kertakäyttösalasanan. Yubikey käyttää autentikointiin tapahtumapohjaista avointa OATH:iin pohjautuvaa OTP:tä, ja on salattu 128-bittisellä AES-salausavaimella. Aluksi Yubikey liitetään validointipalvelimeen (YubiCloud), jonka jälkeen validointipalvelin laskee seuraavan OTP:n tietyn kaavan mukaisesti. Mikäli tämä OTP on kelvollinen, synkronoituvat Yubikey ja validointipalvelin uudelleen.

Yubikeyn käyttämät todennusmetodit ovat: perinteinen Yubico 12-merkin julkinen ID + 32-merkin OTP, OATH 6- tai 8-numeron OTP, staattinen 1-64 merkin salasana kirjautumissovelluksiin ja haaste-vastaus-toiminnallisuus asiakasohjelmille. Yubikeyllä autentikointiin voidaan käyttää joko Yubicon tarjoama YubiCloud-validointipalvelinta tai uudelleenohjelmoimalla sitä voidaan paikallisesti käyttää eri järjestelmissä, jotka tätä toimintoa tukevat.

Yubikey on hiljattain tullut yhteensopivaksi useiden eri järjestelmien kanssa, kuten LastPass:n, joka salaa esimerkiksi verkkopalveluiden salasanoja. Myös Bitcoin-virtuaalivaluuttaa käyttäviä lompakko- sekä valuutanvaihtopalveluja on siirtynyt käyttämään Yubikey-autentikointia palveluissaan. Käyttökohteet pohjautuvat avoimiin tekniikoihin, ja niiden määrä on räjähdysmäisessä kasvussa, mutta myös muita etuja käytölle löytyy. Yubikey ei esimerkiksi tarvitse lainkaan asiakasohjelmaa ja toimii natiivisti useilla eri käyttöjärjestelmissä sekä ohjelmistoissa, joissa sitä koskettamalla Yubikey luo automaattisesti uuden kertakäyttösalasanan haluttuun kenttään. Yubikeyn rakenteellisiin etuihin voidaan laskea, että se on erittäin pienikokoinen, vedenpitävä, käytännössä tuhoutumaton, eikä se vaadi paristoja lainkaan.

Yubikey on Yubicon lippulaiva tuotteissa, mutta Yubico tarjoaa tämän ohella muita tuotteita muun muassa serverituotteiden salaukseen, NFC-pohjaisiin maksujärjestelmiin matkapuhelimissa ja RFID-lukijoihin. Myös yrityksille suunnattuja tukipalveluita on saatavilla, johon sisältyy teknistä tukea sekä tuotetukea kaikille heidän avoimen lähdekoodin sovelluksilleen. (Yubico: Yubikey-esittelysivu.)

6 Juniper Networks

6.1 Yritys ja tietoturvalaitteiden historia

Juniper Networks on yhdysvaltalainen verkkotuotteiden valmistaja, joista päämääräinen erityisesti reititin- ja palomuurilaitteet laajempiin verkkototeutuksiin. Juniper käyttää laitteissaan kehittämäänsä JunOS-käyttöjärjestelmää.

Palomuurilaitteistoissa Juniper aloitti vuonna 2003 NetScreen Technologiesin rahallisella avustuksella edullisemman luokan J-sarjan reitittimien kehityksen. Sarjan laitteet eivät kuitenkaan lyöneet läpi Juniperin kohdatessa ongelmia markkinoilla samaan aikaan yritystason reitittimissä. NetScreen valmisti myös omia laitteitaan, jotka olivat turvaominaisuuksiltaan mainioita, mutta eivät reitittimenä niinkään, kun taas Juniper oli reitittimenä edistyneempi kuin turvaominaisuuksiltaan. Ajan kuluessa J-sarja vaati muutoksia muun muassa nopeampien Ethernet-liitäntöjen ja virta-perustaisen turvallisuuskäsittelyn suuntaan, joita NetScreen valmistamat laitteet sisälsivät. Vuonna 2006 tuotiin toisen sukupolven laitteet markkinoille, jotka toivat nopeat PCI Express Ether-

net-liitännät sekä jaetun laitteistoalustan NetScreen SSG-laitteiden kanssa. Laitteistoyhtäläisyyksistä huolimatta molemmat laitteet käyttivät silti omia käyttöjärjestelmiään. Vuonna 2010 yhtiöiden tuotteet lopullisesti yhdistettiin kokonaisuudeksi Junos 10-käyttöjärjestelmäversion alle matalamman hintaluokan SRX-tuotesarjaksi. Sarjan laitteet sisältävät muun muassa useamman ytimen Octeon-suorittimia, jotka hallitsevat ja välittävät liikennettä ydinkohtaisesti. Myöhemmin valmistetut SRX-tuotteet lainasivat taas ominaisuuksia Juniper:n suositusta MX-sarjasta, kuten ulkokuoren, rakenteen sekä verkkoon päin olevat moduulit. (Wikipedia-artikkeli: Juniper Networks.)

6.2 Juniper SRX-sarja

SRX-sarjan yhdyskäytävälaitteet tarjoavat siis tietoturvaa ja hallintaa pienistä yrityksistä järeimpiin konesaleihin. Laitteet toimivat reitittiminä, kytkiminä sekä tietoturvalaitteina, joten alustana se tarjoaa kustannustehokkaan ja yksinkertaisen tavan yritysten verkkototeutuksille ja sovelluksille.

Laitteet SRX-sarjassa on jaettu käyttäjän tarpeiden mukaisesti muutaman käyttäjän tarpeista useamman tuhannen käyttäjän verkkoihin toiminnallisuuksien määrässä sekä laitteiden hinnoissa. Toimipisteiden käytössä laitteilla etuja ovat ainakin reitityksen keskittämisen mahdollisuus, ulkoverkkoon kytkettävyys, kytkintoiminteita ja Unified Threat Management -tietoturvaratkaisun, joka keskittää tietoturvapalveluiden hallinnointia ja sisältää muun muassa virustorjunnan, palomuurin, VPN-tekniikoita, App Secure-sovellustason protokollien valvonnan ja roskapostisuojan. Reitityspalveluista SRX-sarjan laitteet sisältävät muun muassa IPv4:n sekä IPv6:n multicast- ja unicast-osoitteilla, laajennetun NAT:n, QoS:n, suorituskyvyn- sekä käyttöasteen valvonnan ja tietovirran hallinnan.

Käytännön työosuudessa käytetty Juniper SRX 210 on fyysisesti toisiksi pienin SRX-sarjan laitteista SRX 100:n ollessa pienin, joten se soveltuu erityisesti kaiken kattavaksi yhdyskäytävä-laitteeksi pieniin ja keskisuuriin yrityksiin keskittämään tietoturvaa ja reititystä. Laitteen voi myös sijoittaa yrityksessä verkon reunalle, sillä se tukee muun muassa ADSL-moduuleja. SRX-sarjan laitteet on tuotu korvaamaan aiempaa Netscreen:n SSG-sarjan laitteistoa, ja kyseiset 100- sekä 200- sarjan laitteet ovat fyysisesti lähes identtiset SSG5 sekä SSG20-sarjan laitteiden kanssa käyttöjärjestelmän ollessa

kuitenkin eri. Verratessa SRX 210:llä SRX 100:aan eroja 210:n eduksi kuitenkin ovat muun muassa 100 Mbps suurempi reitityksen suorituskyky, kaksi gigabitin Ethernet-liitäntää, lisäkorttiliitäntä 3G-modeemeille, yksi mini-pim-paikka sekä useita sovellustason lisäyksiä, kuten maksimimäärä turvallisuusmäärittеissä ja yhtäaikaisten sessioiden määrässä. Sarjan pienimmät laitteet eivät kuitenkaan sisällä WLAN:ia, mutta SRX 210 sisältää sen sijaan esimerkiksi PoE- ja VoIP-toiminteita. (Juniper Networks: Juniper SRX-esittelysivu.)

6.3 Junos-käyttöjärjestelmä

Junos on Juniper Networksin laitteissaan käyttämä ohjelmistopohjainen- tai verkkokäyttöjärjestelmä. Juniper on kehittänyt asiakkailleen myös Junos SDK-työkalut, joilla käyttäjä voi itse muokata käyttöjärjestelmää haluamallaan tavalla. Junos on kehitetty vakaan ja toimivaksi todetun avoimen lähdekoodin FreeBSD-ytimen päälle. Unix-ytimen päällä toimivan käyttöjärjestelmän etuna on, että käyttäjät pääsevät käsiksi Unix-konsoliin, josta voidaan myös käyttää perinteisiä Unix-komentoja. Uudet versiopäivitykset ilmestyvät tasaisesti 90 päivän välein ja viimeisin versio käyttöjärjestelmästä on tällä hetkellä 12.1R1, joka julkaistiin maaliskuussa 2012. Päivityksillä on päästy eroon esimerkiksi 10-versiota alkuun vaivanneista lastentaudeista, kuten hitaudesta ja sessioiden satunnaisista katkeiluista. Juniper käyttää Junos:ää kaikissa verkkolaitteissaan, ja versiopäivitykset ovat käytettävissä myös yhtäläisesti kaikissa laitteissa.

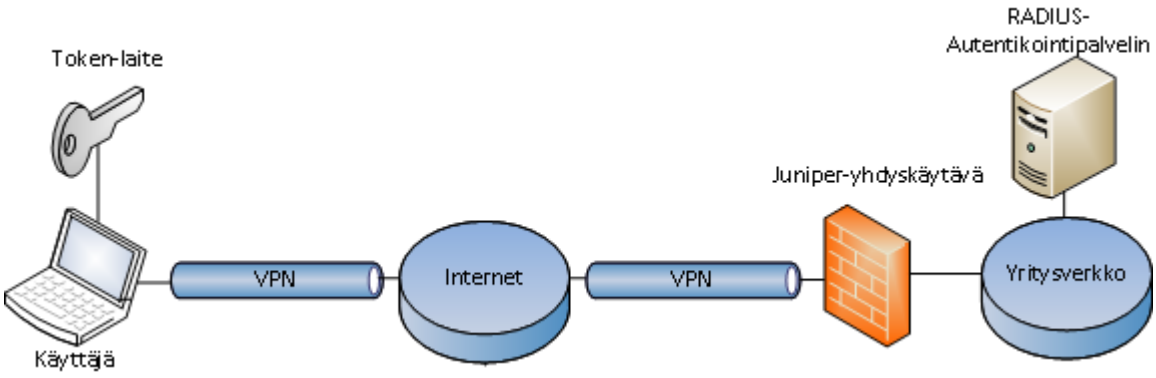
Käyttöjärjestelmä sisältää sekä graafisen että komentoriviltä käytettävän käyttöliittymän. Graafisessa käyttöliittymässä on karsittu osa komentorivin toiminteista, mutta useimmat yleisimmät määrittelyt onnistuvat graafisestikin. Graafista käyttöliittymää käytetään web-selaimen kautta ottamalla yhteys joko http:llä tai salatulla https:llä. Komentoriviltä käytettäessä se jakautuu kahteen erilliseen toimintatilaan: toiminnalliseentilaan ja määrittelytilaan. Toiminnallisessa tilassa voidaan hallita komentorivin ympäristöä, valvoa ja etsiä ongelmia verkon toiminnasta, siirtyä määrittelytilaan sekä käyttää muun muassa traceroute- ja ping-toimintoja verkon testaukseen. Konfigurointitiedot muokkautuvat XML-muotoon, jossa ne ovat hierarkkisessa järjestyksessä. Määrittelytilaan siirrytään toimintatilasta configure-komennolla, kun taas exit-komento palaa takaisin toimintatilaan Komennot voidaan laittaa manuaalisesti yksi kerrallaan tai vaihtoehtoisesti liittää ASCII-pohjaisen tekstitiedoston, joka sisältää listan komennoista.

Set-komennolla aloitetaan tietyn komennon syöttö, jossa määritetään mihin hierarkkiseen osioon komento kohdistetaan jonka jälkeen määritetään haluttu toiminne. Edit-komennolla voidaan siirtyä haluttuun osioon muokkaamaan sitä tai tulostamaan määrittelyt. Hierarkiassa korkeammalle liikutaan up-komennolla. Unix-käyttöjärjestelmien tapaan komentoa voidaan täydentää sarkain-näppäimellä, kun taas kysymysmerkki näyttää valittavissa olevat komennot ja selitteet. Määrittelytilassa tehdyt muutokset otetaan käyttöön commit-komennolla. (Juniper Networks: Junos-esittelysivu).

7 Ympäristö

7.1 Verkon rakenne ja suunnittelu

Mobiilin työntekijän tietoturvallisen etätyöskentelyratkaisun suunnittelussa ideana oli implementoida hyvin yleiseen yritysverkon topologiaan tietoturvallinen etäkäyttö vahvistetulla autentikoinnilla. Perinteisessä pienemmän yrityksen verkossa verkon reunalla, DMZ-vyöhykkeellä sijaitsee jokin palomuurilaite, joka toimii yhdyskäytävänä yrityksen sisäverkolle sekä sen laitteille. Kyseisellä vyöhykkeellä voivat myös sijaita yrityksen julkinen web-palvelin sekä lähtevän sähköpostin smtp-palvelin. Tällöin etätyöntekijän ja tietoturvallisen yritysverkon välille jää turvaton ja salaamaton internet. Etätyöntekijä haluaa kuitenkin päästä käsiksi yrityksensä verkkoon kuin toimiston työntekijä konsanaan ja siksi muodostetaan päätepisteiden välille dynaaminen Remote Access VPN-yhteys.



Kuva 3. Työssä käytetyn verkon topologia

VPN-yhteys ei kuitenkaan ainoastaan riittävä tietoturvalliseen yhteyteen, vaan käytetään sopiva tunnelointiprotokolla, tässä tapauksessa IPSec, sekä oleellisena osana avaintenvaihtoprotokollan ja pakettivirtojen salaustavan valinta. Suunnittelussa halutaan kuitenkin myös tavallista vahvempi autentikointi, joten tavallinen paikallisessa käyttäjäkannassa sijaitseva käyttäjätunnus – salasana -yhdistelmä ei ole riittävä tähän tarkoitukseen. Lisätään siis verkkoon RADIUS-autentikointipalvelin, jossa käytetään ulkoista LDAP-tietokantaa käyttäjille. LDAP-tietokannan lisäksi vaaditaan autentikointipalvelimelta tukea OTP:n käytölle, eli autentikointitavaksi valitaan LDAP+OTP, jossa OTP-autentikontiin käytetään Yubikeytä. Autentikointipalvelin käyttää sisäistä validointipalvelinta OTP-tokenien oikeellisuuden tarkistukseen.

Etätyöntekijän laitteen tietoturvan suunnittelussa vaaditaan perinteisten tietoturvan vahvistuskeinojen, kuten palomuurin ja virustorjunnan, lisäksi IPSec VPN -asiakasohjelman asennusta VPN-tunnelin käyttöönottamiseksi. Tämän lisäksi etätyöntekijä tarvitsee Yubikey:n, jota käytetään käyttäjätunnus - salasana-yhdistelmän lisänä VPN-tunnelin autentikointiin.

Näillä tekijöillä yhdessä pyritään luomaan tietoturvallinen ympäristö, jota voidaan aukottomasti käyttää etätyöntekijän sijainnista huolimatta. Kyseisillä tekijöillä myös varmistetaan, että mikäli etätyöntekijä hävittäisi jonkin käytetyistä laitteistaan tai tunnuksistaan, ei ulkopuolisella silti ole pääsyä yrityksen verkkoon. Tähän päämäärään ratkaisevana tekijänä on vahvan autentikointitavan valinnalla.

7.2 Käytössä olevat laitteistot ja tekniikat

Etäkäyttäjän laitteistona käytetään laboratorion tarjoamia pöytäkoneita. Käytännössä mikä tahansa USB-liitännät tarjoava laitteisto sopii yhteen Yubikeyn kanssa. OATH-pohjaiseen autentikointiin valittiin siis kyseinen Yubikey. Autentikointipalvelimeksi valittiin ilmainen ja Yubikey-yhteensopiva RCdevs OpenOtp -autentikointipalvelin sisäisellä LDAP-kannalla. VPN-tunnelin päätepisteeksi sekä yrityksen verkon yhdyskäytäväksi valitaan laboratoriosta löytyvä Juniper SRX 210 -palomuurilaite.

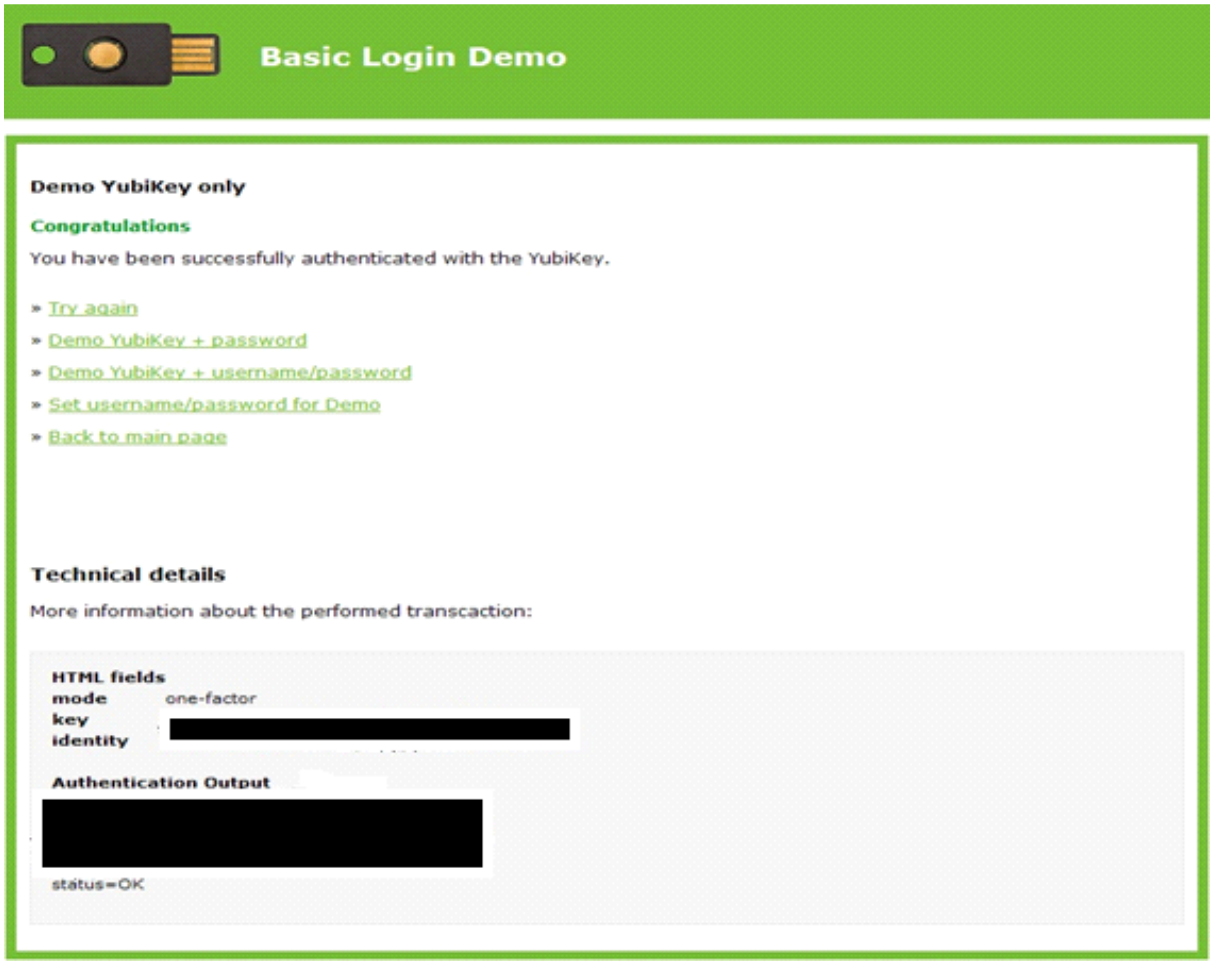
RCDevs-autentikointipalvelimesta on käytössä virtuaalikone suoraan virtuaalialustan päälle asennetavaksi, joka valitaan sen yksinkertaisuuden ja simulaatioluontoisuuden

vuoksi. Vituaalikonetta käytetään Oracle:n VirtualBox-virtualisointiohjelmiston päällä. VPN-asiakasohjelmistona käytetään Juniper SRX:stä verkon kautta ladattavan asiakasohjelman kokeiluversiota, josta ilmainen lisenssi kattaa kaksi asiakasyhteyttä, mutta lisensoimalla käyttäjiä voi tarpeen mukaan lisätä.

8 Toteutus

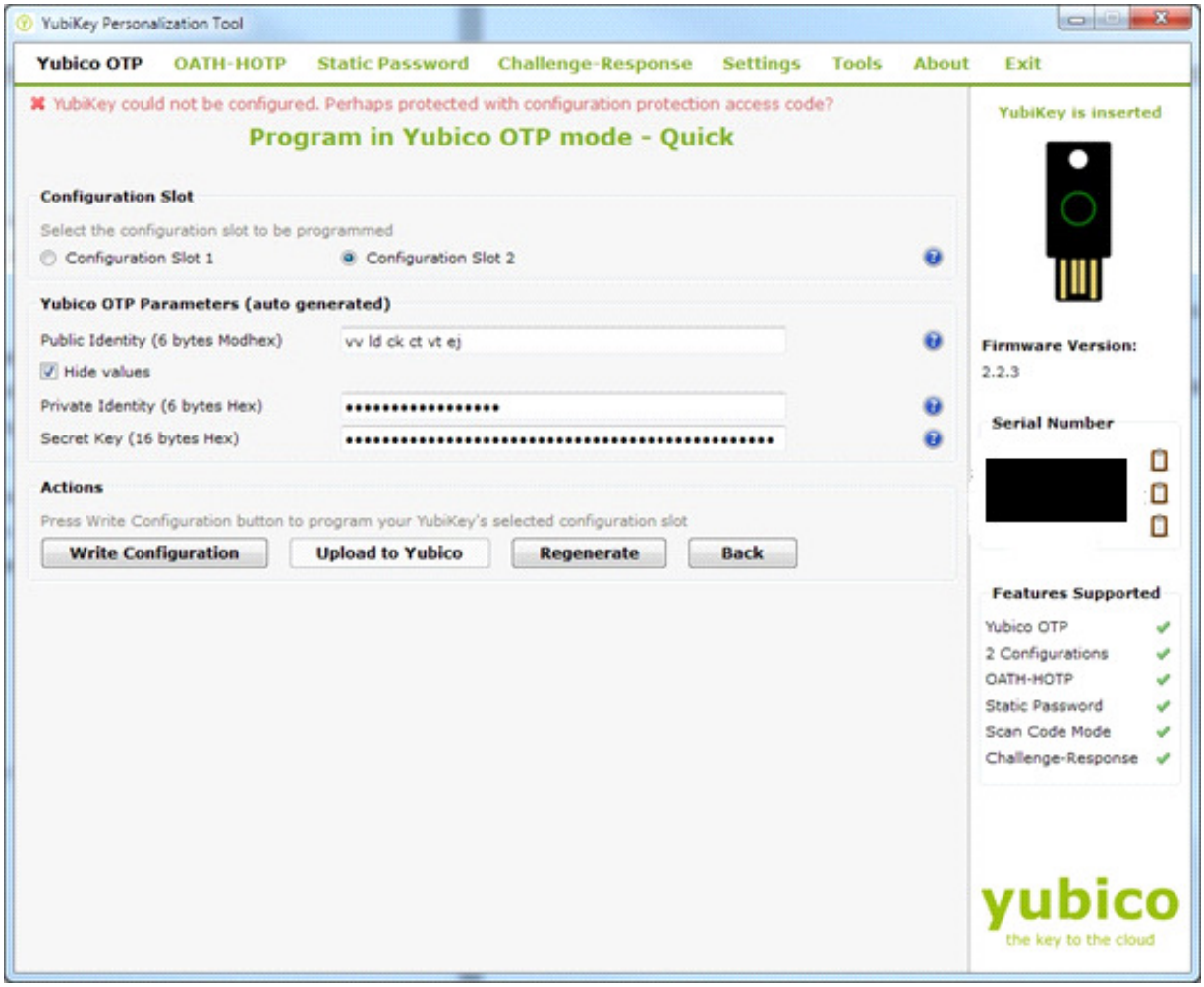
8.1 Yubikey-implementointi

Yubikeyssä on käytössä oletuksena kertakäyttösalasanojen validointi YubiCloudiin. Toteutuksessa käytetään kuitenkin autentikointipalvelinta, jossa OTP-validointi hoidetaan sisäisesti autentikointipalvelimella. Testataan kuitenkin aluksi OTP Yubikeyn toimivuutta YubiCloudin kanssa Yubicon internetsivustoilta löytyvän työkalun avulla.



Kuva 4. Onnistunut kirjautuminen Yubicon testaustyökalulla

Koska toteutuksessa käytetään sisäistä validointipalvelinta, tulee Yubikeystä selvittää sen yksityinen ID sekä käytetty AES-salaisuus. Näitä asioita ei voida selvittää jo ohjelmoidusta konfiguraatiosta, vaan laite tulee uudelleenohjelmoida kyseisillä tiedoilla. Yubikey, alkaen laitteen Firmware-versiosta 2.2, sisältää kaksi ohjelmoitavaa muistipaikkaa, jossa ensimmäisessä valmiiksi YubiCloudin kanssa synkronoitu OTP ja toinen tyhjäksi jätetty muistipaikka. Näitä muistipaikkoja on mahdollista ohjelmoida Yubicon tarjoamalla Yubikey Personalization Tool -työkalulla, jotta saadaan selville tarvittavat tiedot. Asennetaan työkalu ja valitaan metodiksi Yubico OTP -tila, jossa on optiona Yubikeyn uudelleenohjelmointi validoimaan YubiCloudin kautta. ”Quickly”-valinnalla uudelleenohjelmoimalla ohjelmisto tarjoaa automaattisesti generoidut parametrit, joten käytännössä riittää, että valitaan Write Configuration -toiminto, joka aloittaa Yubikeyn uudelleenohjelmoinnin. Valitaan kuitenkin ruksi pois kohdasta ”Hide values”, jolla saadaan näkyviin autentikointipalvelimelle vaadittavat parametrit.



Kuva 5. Yubikeyn uudelleenohjelmointi

8.2 Autentikointipalvelin

8.2.1 RCdevs OpenOTP

RADIUS-palvelimeksi työhön valittiin RCdevs:n OpenOTP, josta löytyy tuki Yubikey OATH:lle. Ohjelmisto sisältää kaksi versiota - suoraan raudan päälle asennettavan sekä virtuaalikoneen, joista työssä käytetään OVF-muotoista virtuaalikonetta. Virtuaalikoneesta löytyy eri käyttäjätietokannoille soveltuvia toteutuksia. Valitaan työosuuteen verkon topologian yksinkertaistamiseksi versio, joka sisältää sisäisen LDAP-käyttäjätietokannan.

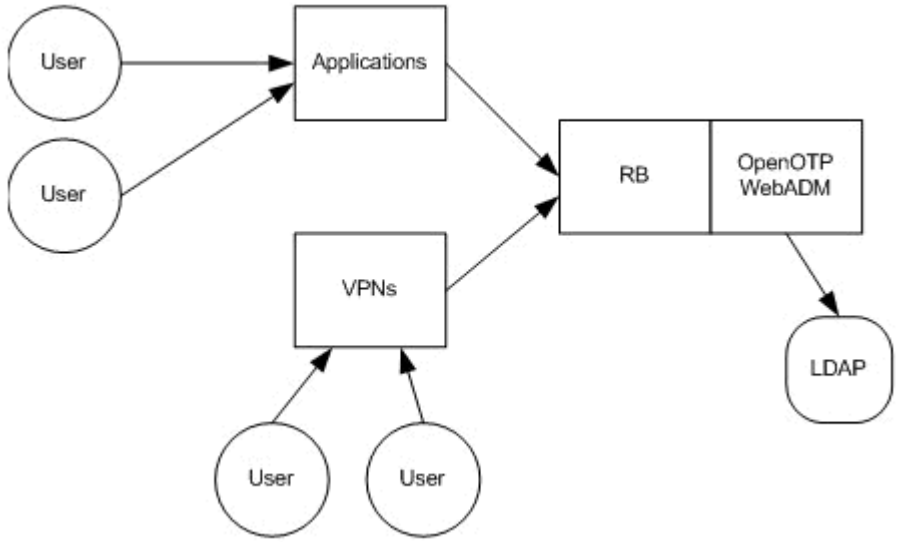
OpenOTP on yritystason autentikointipalvelin, jossa käytetään avoimia standardeja. Ilmainen lisenssi sisältää autentikointipalvelimelle 25 käyttäjän määritystä, mutta lisensoimalla käyttäjiä saa lisää. Laitteistopohjaisen Yubikey-autentikoinnin kaikkien autentikointitapojen lisäksi. Alusta tukee muun muassa seuraavia kertakäyttösalasanoja:

- OATH:iin pohjautuvat aika-, tapahtuma- sekä haaste –pohjaisiin ohjelmisto- ja laitetokenit
- Google Authenticator
- kertakäyttösalasanat matkapuhelimiin ohjelmistotokeneilla
- SMS-kertakäyttösalasanat
- sähköpostin ja salatun sähköpostin kertakäyttösalasanat.

Ohjelmaan voi määrittää lisäksi muun muassa graafisen WebAdmin-työkalun, josta voidaan hallita suurinta osaa autentikointipalvelimen toiminnoista sekä LDAP-käyttäjätietokantaa, RADIUS-sillan VPN-toteutuksiin asiakkaan ja jaetun salaisuuden määrittelyillä sekä Self-Service Desk -toiminnon käyttäjän tietojen hallintaan, tokenien synkronointiin ja niin edelleen. (RCdevs: OpenOTP-esittelysivu.)

8.2.2 Määrittely

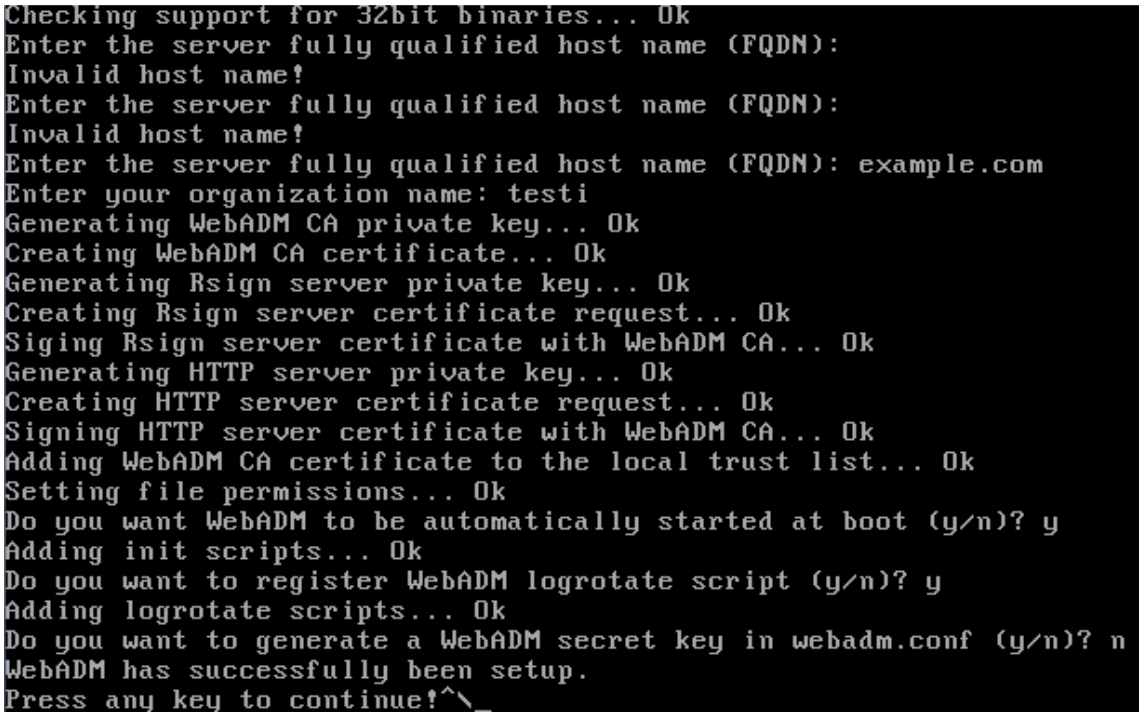
Tarkoitus RADIUS-autentikoinnin toteutuksessa on luoda autentikointipalvelimelle testikäyttäjä, jolle autentikointitavaksi valitaan LDAP+OTP. LDAP-käyttäjätunnusten salasanan jatkoksi lisätään siis Yubikeyn generoima kertakäyttösalasana. OpenOTP Radius-siltaan määritellään taas RADIUS-asiakkaan sekä jaettu salaisuus, jolla RADIUS-viestit saadaan kulkemaan Radius-palvelimen ja -asiakkaan välille. Palvelinta voidaan käyttää myös erinäisten sovellusten, kuten SSH:n, Apachen tai PHP-applettien autentikointiin.



Kuva 6. OpenOTP:n käyttötavat (Setup Two-Factor Authentication using OpenOTP.)

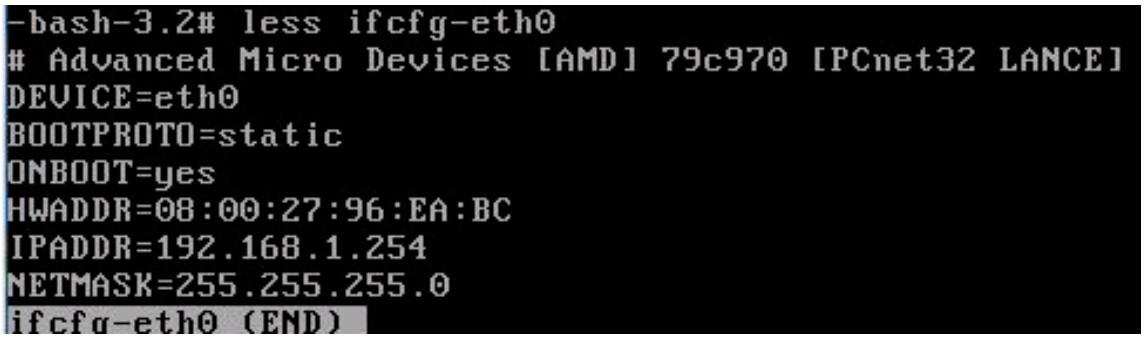
Lähdetään kuitenkin liikkeelle virtuaalikoneen asennuksesta. OVF-formaatissa oleva virtuaalikone tuodaan aluksi VirtualBox-virtualisointiohjelmistoon. Automaattisten määritysten jälkeen käynnistetään virtuaalikone, jolloin avautuvat linux-pohjaisen CentOS-käyttöjärjestelmän käynnistysvaihtoehdot. Ohitetaan tämä käynnistysvalikko oletusvalinnalla. Järjestelmäkomponenttien määrittelyiden jälkeen käynnistyy ensimmäisellä käynnistyskerralla velho muun muassa domain-nimeen sekä WebAdmin-hallintatyökaluun liittyen – työssä käytetään esimerkkinä example.com, mutta kenttään voidaan asettaa yrityksen sisäinen domain-nimi.

Laite pyrkii hakemaan osoitteen oletuksena DHCP-palvelimelta, ja mikäli osoitetta ei DHCP:n kautta tarjota, laitteen palveluita voida käyttää verkon yli. IP-määrityksiä tarvitaan myös Radius-sillan ja Radius-asiakkaan välille yhteyden toimintaan saattamiseksi.



Kuva 7. OpenOTP-alkumäärittelyt

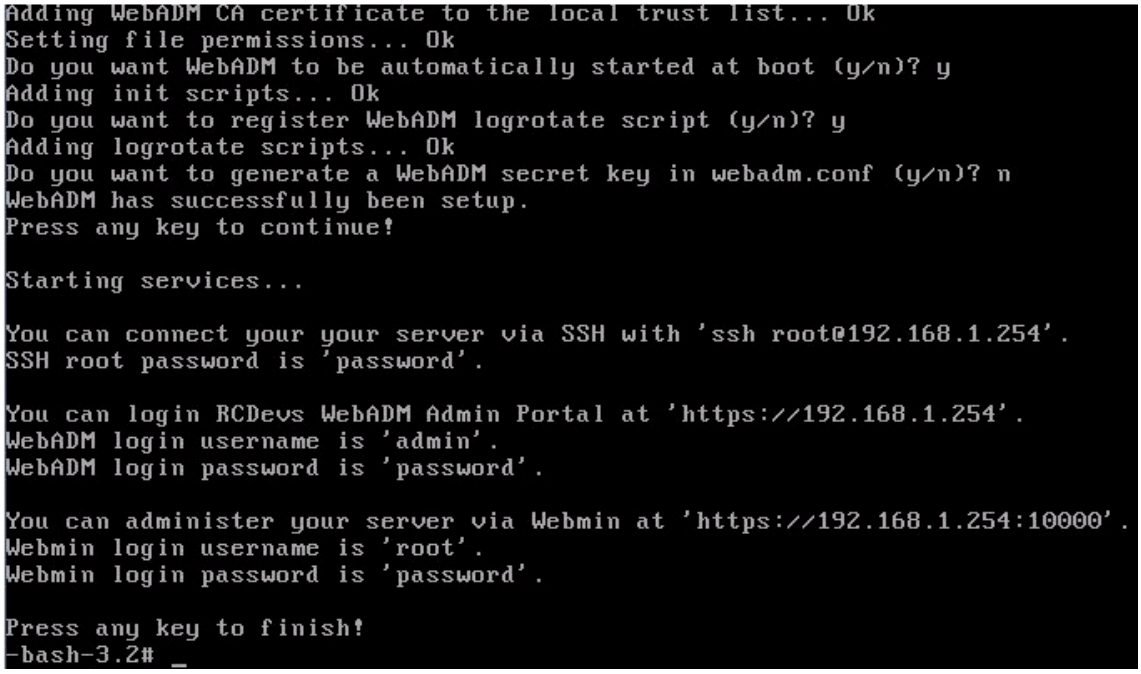
Käytössä ei ole erillistä DHCP-palvelinta, joten IP-asetukset määritetään staattisiksi käyttöjärjestelmän verkkoasetuksiin, jotta osoite voidaan määrittää Radius-asiakkaalle. Kirjaudutaan root-tunnuksilla järjestelmään (käyttäjätunnus root ja salasana password). Tehdään määritykset manuaalisesti muokkaamalla ethernet-liitäntää hakemistossa /etc/sysconfig/network-scripts/. Muokkauksen jälkeen käytetään liitäntä alhaalla ja nostetaan ylös ifcfg eth0 down ja -up komennoilla, jonka jälkeen tuloste näyttää



Kuva 8. Staattiset IP-määrittelyt

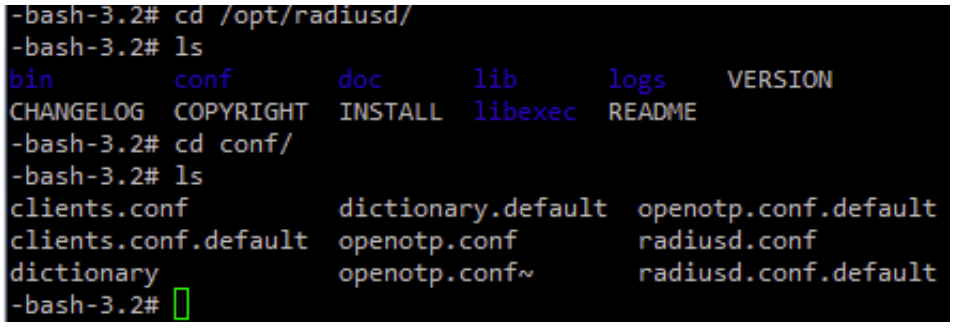
Halutaan ottaa muutokset käyttöön myös autentikointipalvelimelle, joten määritetään alkuasetukset uudelleen resetoimalla virtuaalikone vm_init –komennolla. Tulosteessa

näkyvät palvelut ja osoitteet, jonka kautta palveluita voidaan web-selaimella ja ssh-sovelluksella käyttää.



Kuva 9. OpenOTP:n uudelleenkäynnistys staattisilla määritteillä

Määritellään Radius-silta tämän jälkeen käyttöön. Radius-määrittelytiedostot löytyvät polusta /etc/, jossa oleelliset määrittelytiedostot ovat clients.conf ja radiusd.conf -tiedostot.



Kuva 10. RADIUS-sillan konfigurointitiedostot

Clients.conf -tiedostoon muutetaan Radius-asiakkaan tiedot, tässä tapauksessa hyväksytään kaikki asiakkaat, ja määritellään yhtäläinen jaettu salaisuus asiakkaan kanssa. Radiusd.conf-tiedostoon määritetään taas käytettäväksi autentikointitavaksi LDAP+OTP.

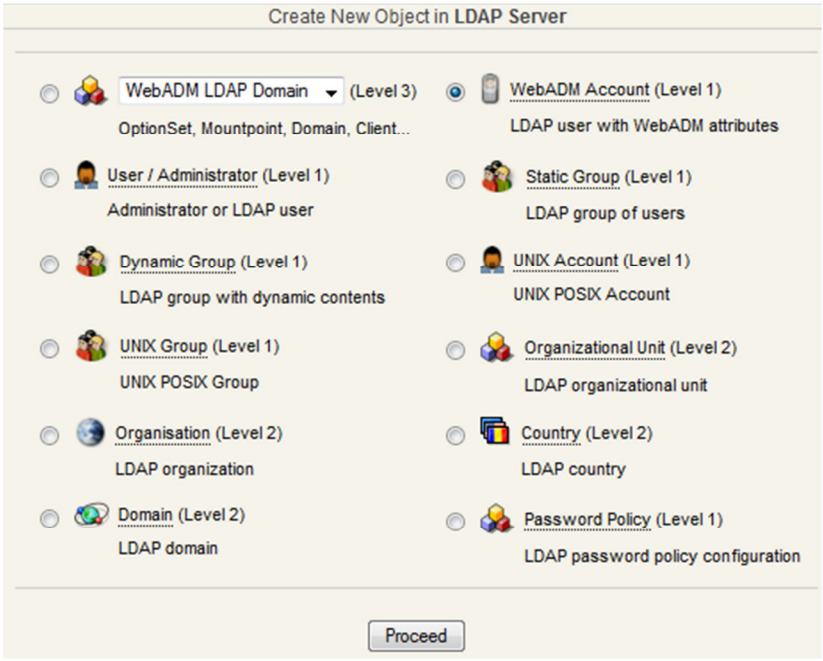
```
# By default, OpenUTP Radius Bridge allows any client to connect
#
client 0.0.0.0/0 {
        secret          = secret
        shortname       = Juniper-VPN
}
```

Kuva 11. Clients.conf -tiedostoon RADIUS-asiakkaan määrittely

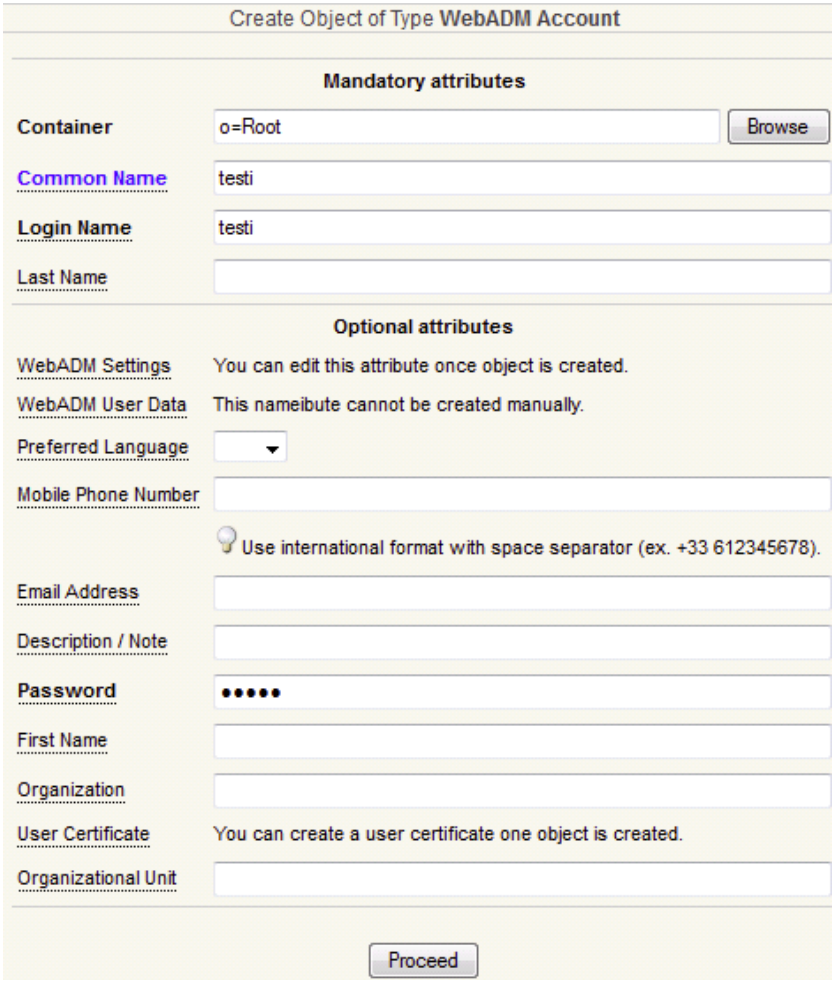
Tämän jälkeen kirjaudutaan web-selaimella WebAdmin-hallintaportaalin virtuaali-isäntäkoneelta LDAP:iin oletuksena luodulla admin-tunnuksilla (käyttäjätunnus admin, salasana password).

Kuva 12. WebAdmin-kirjautuminen

Aloitetaan LDAP-määrittely määrittelemällä testikäyttäjä palvelimelle. Luodaan vasemmalta root:n alle lapsiobjekti. Määrittelyksi valitaan LDAP-käyttäjätunnus WebAdm-määritteillä, jolla voidaan siis kirjautua WebAdm-portaaliin.

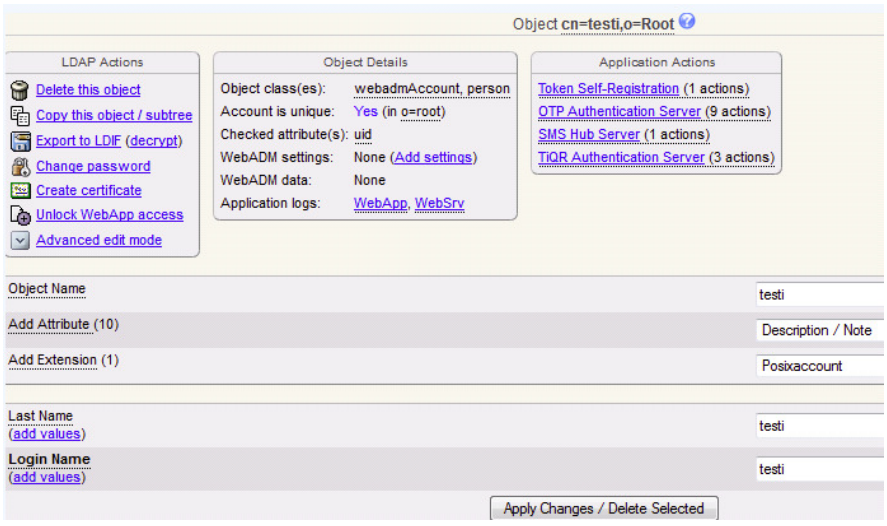


Kuva 13. WebAdm LDAP -käyttäjätunnuksen valinta

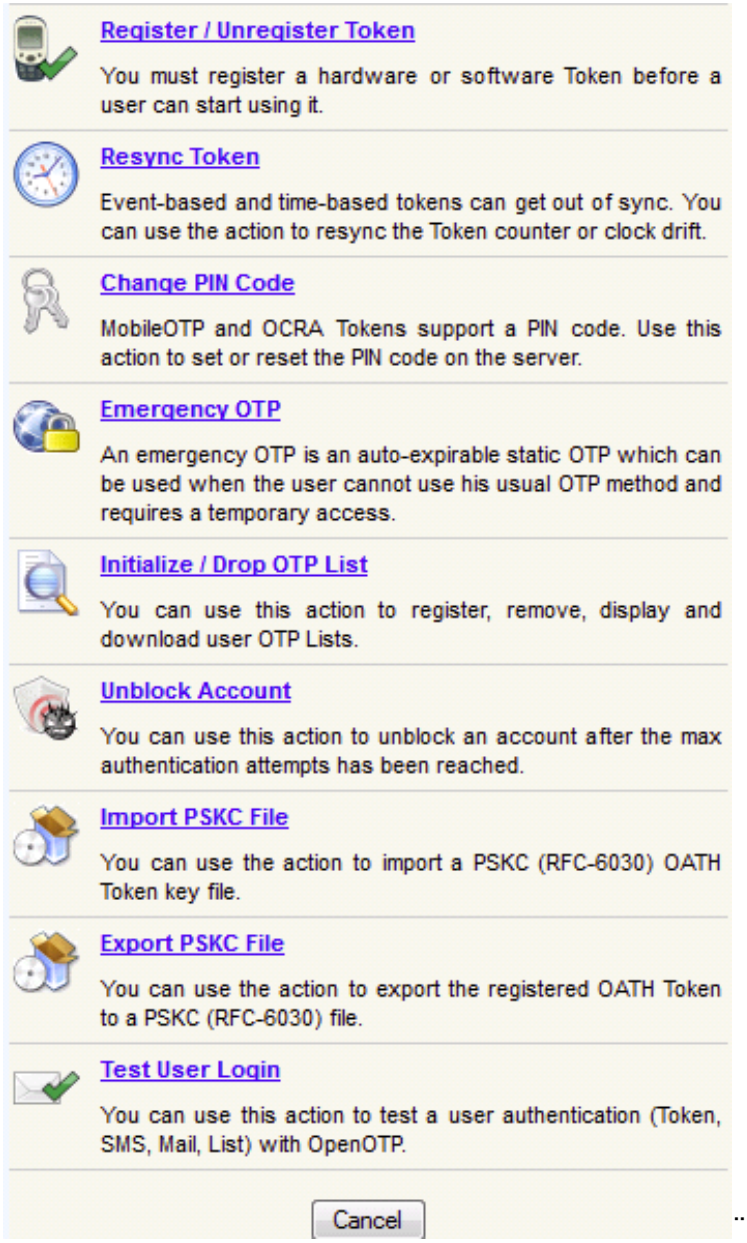


Kuva 14. Testikäyttäjän tunnusten luonti

LDAP:iin luodun testikäyttäjän jälkeen rekisteröidään OTP-autentikointipalvelimelle Yubikey käyttöön valitsemalla OTP Authentication Server ja Register Token.

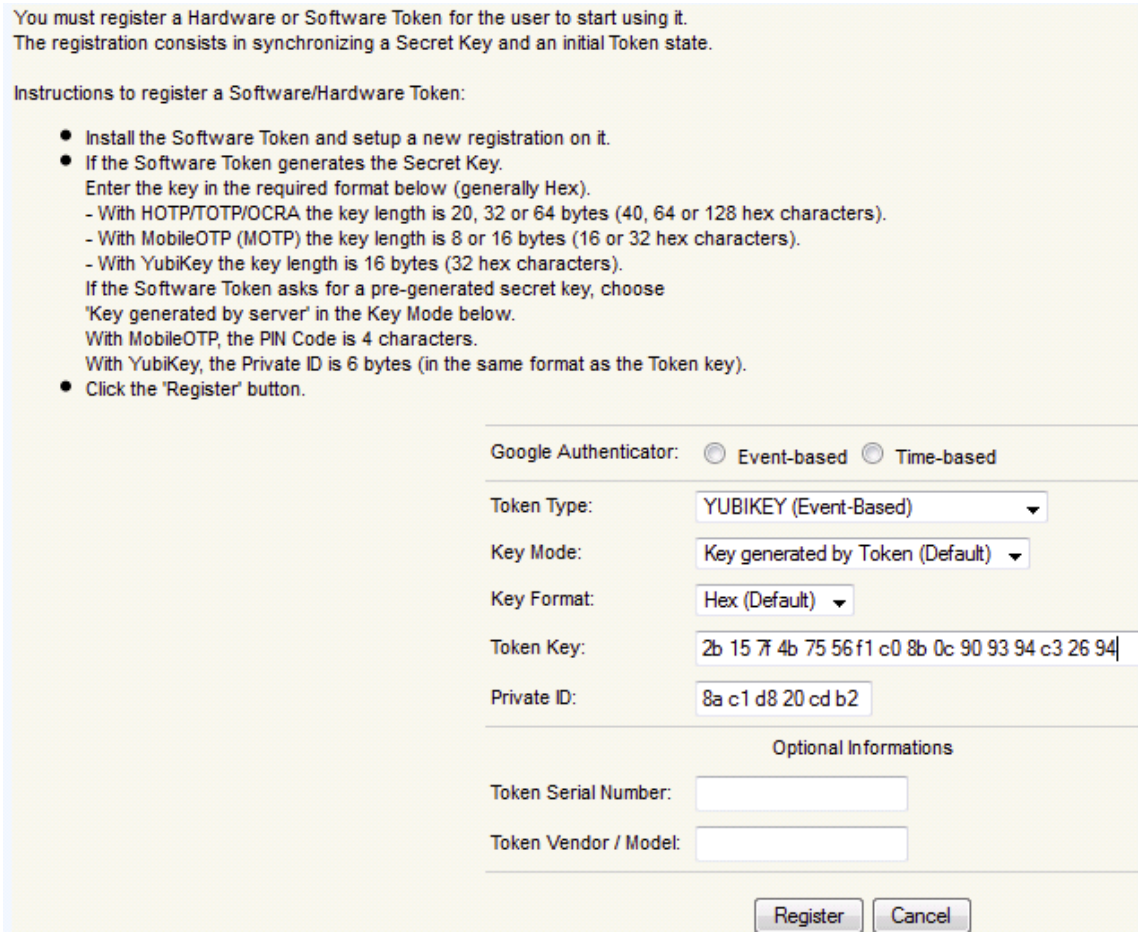


Kuva 15. Testikäyttäjä-objekti



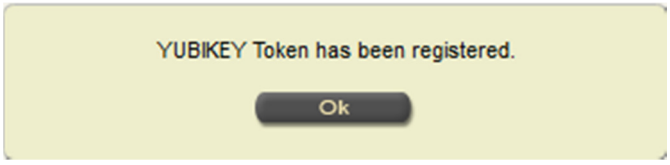
Kuva 16. Tokenien määritykset

Rekisteröidään Yubikey valitsemalla (Yubikey Event Based) se alasvetovalikosta ja aiemmin uudelleenohjelmoiduilla Yubikeyn parametreillä, jotka saadaan aiemmin mainitulla Personalization Toolilla. Vaihtoehtona on käyttää palvelimen luomia parametrejä ja ohjelmoida Yubikey kyseisellä autentikointitavalla ja käyttämällä sille palvelimeen määriteltyjä parametreja. Resync token -kohdasta saadaan aika- ja tapahtumapohjaiset tokenit synkronoitua uudelleen, mikäli tarvetta on token-laskurin nollaamiselle tai aikajakso muuttuu palvelimella. Test User Login -toiminteella voidaan taas kokeilla testaustarkoituksessa kirjautumista esimerkiksi OTP:n toiminnan kokeilemiseksi.



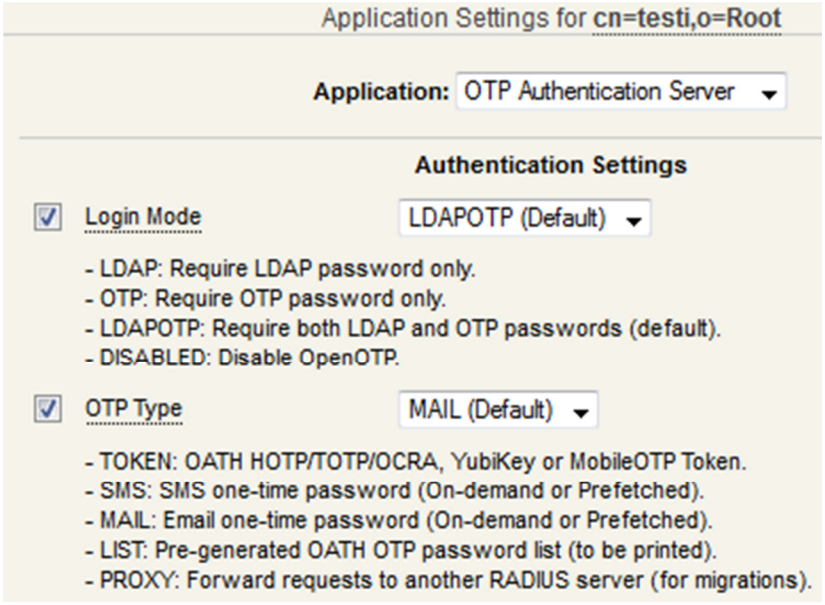
Kuva 17. Yubikey-tokenin rekisteröinti

Tokenin rekisteröinti ilmoittaa määrittelyn onnistuneisuudesta.



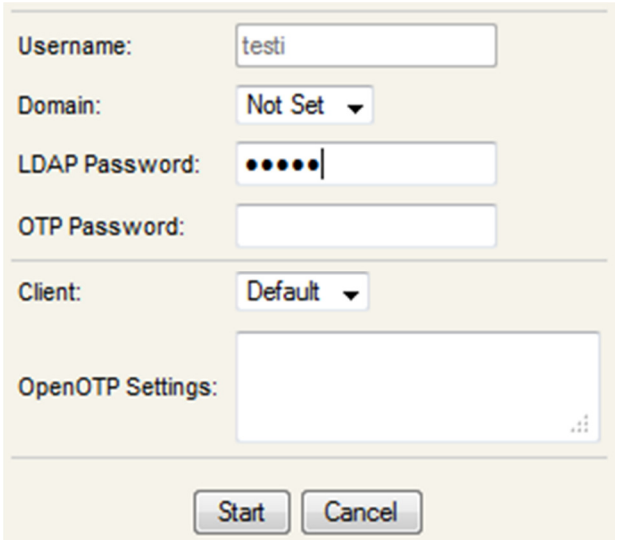
Kuva 18. Token-rekisteröinnin onnistumisilmoitus

Määritellään vielä testikäyttäjälle LDAP+OTP kirjautuminen käyttöön autentikointipalvelimelle eli ruksitetaan Login mode ja OTP mode käyttöön ja asetetaan vetovalikoihin LDAPOTP ja TOKEN.



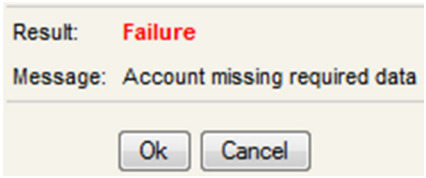
Kuva 19. Autentikointipalvelimen LDAP+OTP-määritykset testikäyttäjälle.

Tämän jälkeen kokeillaan Test-työkalulla kirjautumista ja syötetään luotuun LDAP-salasana -kenttään password, Yubikeyn generoima syöte kohtaan OTP ja muut jätetään oletukselle.



Kuva 20. Käyttäjän testaus

Kirjautuminen antaa herjan käyttäjätilin puuttuvista tiedoista, johon paneudutaan enemmän työn Toiminta ja ongelmatilanteet -osiossa.



Kuva 21. Tieto epäonnistuneesta kirjautumisesta

8.3 Juniperin määrittely

8.3.1 Komentorivi

Juniperissa määrittelyyn päästään käsiksi etupaneelista löytyvän Console-portin kautta. Etupaneelista voidaan myös palauttaa laite tehdasasetuksille pitämällä pohjassa Reset-painiketta. Konsoliporttiin paikallisesti yhdistämällä laite käynnistyy tilaan, jossa se kysyy käyttäjätietoja. Pääkäyttäjän tunnukset ovat oletuksena root ja salasana tyhjä. Yhdistäminen on myös mahdollista muun muassa SSH:lla samoin kuin salaamattomalla telnet:llä, jolloin tosin pääkäyttäjäksi kirjautuminen on estetty. Kirjautumisen jälkeen mennään unix-käyttöliittymään, jossa tarkasteltavissa muun muassa käyttäjän profiili- sekä lokitiedot. Tästä tilasta siirrytään käyttämään komentoriviä komennolla cli. Tällöin käynnistyy toimintatila, josta voidaan muun muassa tarkistaa sen hetkinen käytössä oleva konfiguraatio.

Aloitetaan konfiguroimalla SRX:ään perusasetukset, johon kuuluvat:

- salasana root-tunnukselle sekä erillinen superuser –käyttäjä tietoturvan parantamiseksi
- laitteen isäntänimen asetus
- IP-osoite ja prefiksi Ethernet-liitännöille
- default router –osoite oletusreititimeksi määrittelyyn.

Siirrytään siis aluksi komentoriviltä määrittelytilaan komennolla

configure

Asetetaan pääkäyttäjän salasana komennolla

Set system root-authentication plain-text-password

Komennolla commit check voidaan tarvittaessa jokaisen komennon jälkeen tarkastaa, että muutokset on mahdollista ottaa myöhemmin käyttöön.

Tietoturvan kannalta on myös hyvä luoda järjestelmään muita käyttäjiä rootin ohella, joten luodaan testi-käyttäjä superuser-oikeuksilla

edit system

set login user testi class super-user authentication plain-test-password

Laitteelle isäntänimi, jolloin nähdään komentoriviltä mitä laitetta konfiguroidaan

set host-name testilab-srx

Asetetaan reitittimen tunnistamiseksi -osoite

edit routing-options

set router-id 192.168.1.1

Fyysiset ethernet-liitännät SRX -laitteessa ovat välillä 0/0/0 – 0/0/7, joista kaksi ensimmäistä (ge-0/0/0 – 0/0/1) ovat gigabitin siirtonopeuteen kykeneviä, kun taas loput (fe-0/0/2-fe-0/0/7). Näistä ge-0/0/0 toimii oletuksena DHCP-asiakkaana, kun taas muut liitännät DHCP-palvelimena verkolle 192.168.1.0/24, jolloin liitäntöihin kytketty asiakaskone saa oletuksena tästä verkosta osoitteen. Työssä simuloidaan Internetin yli yhteyttä, joten asetetaan ulkoverkon liityntä gigabit-liitäntään 0/0/0, yrityksen simuloitu sisäverkko kytketään taas liitäntään ge-0/0/1, jossa ovat kiinni ulkoinen RADIUS- sekä varmistuspalvelin. Määritetään IP-osoitteet manuaalisesti molemmille liitännöille, sillä työssä ei ole erillistä DHCP-palvelinta.

Asetetaan Ethernet-liitännöille IPv4-osoitteet ilman erillisiä VLAN-määritteitä (unit 0)

edit interfaces

set ge-0/0/0 unit 0 family inet address 192.168.5.1/24 // simuloitu internet-liityntä eli VPN-asiakkaan puoli

set ge-0/0/1 unit 0 family inet address 192.168.1.1/24 // simuloitu yrityksen LAN-liityntä, jossa Radius-autentikointipalvelin sijaitsee

ge0/0/1 –liitäntä on oletuksena kytkinportti, joten vaihdetaan se reitittäväksi

delete ge-0/0/1 unit 0 family ethernet-switching

Lisätään vielä simulaatioluonteinen reititys kahden verkon välille, joka voidaan hoitaa esimerkiksi OSPF:llä, jossa area 0 –määrittely ja OSPF käyttöön untrust-vyöhykkeessä

set protocols ospf area 0.0.0.0 interface ge-0/0/0.0

set protocols ospf area 0.0.0.0 interface ge-0/0/1.0

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic protocols ospf

SRX:ään voidaan määritellä tiettyjä turvallisuusalueita, jotka on jaettu ei-luotettaviin sekä luotettaviin (untrust ja trust). Näihin alueisiin voi tehdä rajoittavia määrityksiä esimerkiksi tiettyjen palvelujen osalta. Liitäntä ge-0/0/0 on ulkoverkkoon päin suuntautuvana liitäntänä oletuksena untrust-vyöhykkeessä, joten suuri osa palveluista on käyttämättömissä, joka tietenkin on hyödyllistä tietoturvan kannalta liitännän ollessa internetiin päin suuntautuvana. Tehdään kuitenkin työn simulaatioluonteisuuden vuoksi määritys kaiken useimpien protokollien käytölle kyseiselle liitynnälle, eli voidaan esimerkiksi ottaa yhteyttä ping:llä testaustarkoituksessa.

edit zones

set security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services any-service

Lisätään ge-0/0/1.0 –liitäntä määritellään taas trust-alueelle.

set security-zone trust interfaces ge-0/0/1.0

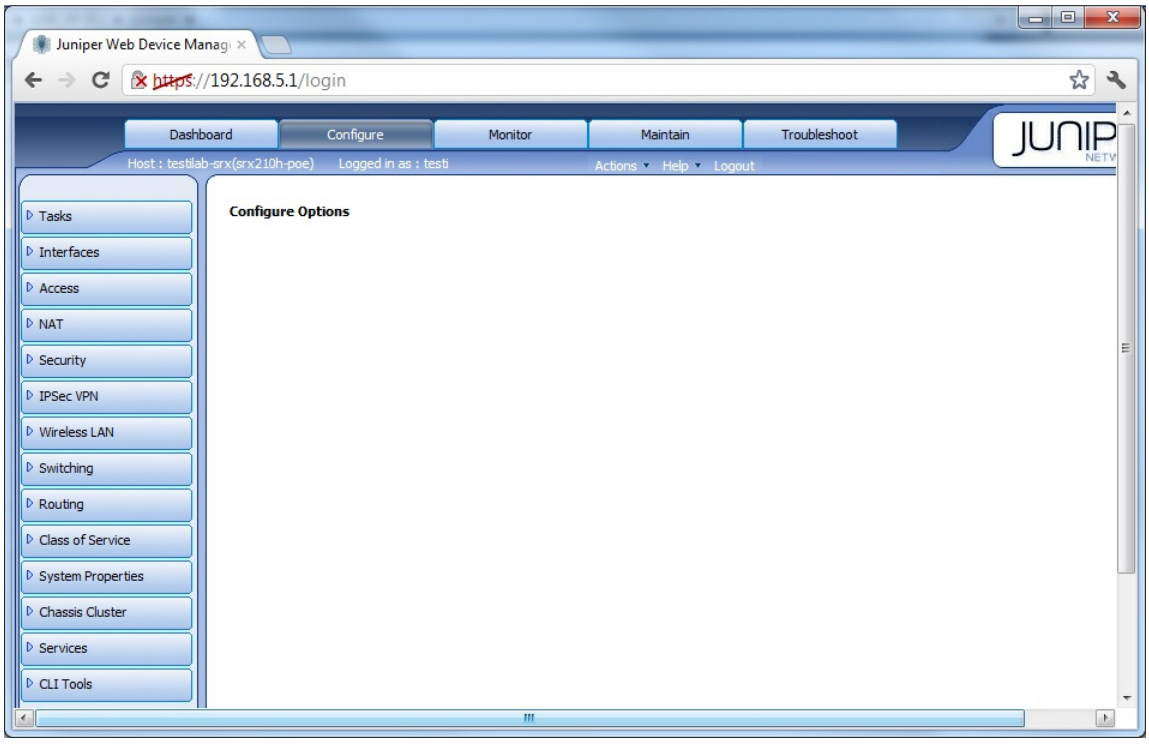
Komento commit ottaa lopulta määritellyt konfiguraatiot käyttöön. Vaihtoehtona on esimerkiksi commit and-quit, joka käyttöönoton jälkeen palaa takaisin toimintatilaan. Rollback-komennolla voidaan palata aiempiin commit-tilanteisiin.

8.3.2 Graafinen käyttöliittymä

Juniper tarjoaa graafista käyttöliittymää laitteissaan, jonka käyttö onnistuu selaimella yhdistämällä laitteen osoitteeseen http- tai https-protokollalla. Graafisesta liittymästä onnistuvat lähes samat toiminteet kuin komentoriviltä. Graafinen käyttöliittymä otetaan käyttöön halutulle liitännälle komennolla.

set system services web-management https interface ge-0/0/0.0

Kirjaudutaan web-liittymään esimerkiksi aiemmin luodulla testikäyttäjällä ottamalla yhteyttä johonkin reitittimen liitännän osoitteeseen, eli tässä tapauksessa käytössä 192.168.5.1. Kirjautumisen jälkeen Juniper avaa oletuksena konfigurointitilan, jossa erilliset valikot eri toiminteille.



Kuva 22. Graafisen käyttöliittymän etusivu

Graafinen liittymä toimii samalla perusperiaatteella kuin komentorivi, jossa tehtyjen määrittelyjen jälkeen commit-komento ottaa muutokset käyttöön. Määrittely onnistuu yksinkertaisesti vasemman palkin luokitelluista kohdista, joista avautuu jaetusti kyseisen kategorian toiminteita.

Graafinen käyttöliittymä sisältää konfigurointityökalujen ohella muitakin toiminteita monipuolisesti. Käyttöliittymän kautta voi muun muassa tutkia yleisesti laitetietoja, laitteen käytönvalvontaa, lisenssien ja tiedostojen hallintaa sekä vianselvitystyökaluja.

8.3.3 Remote Access VPN

Remote Access VPN yleisesti vaatii yleisesti erillistä asiakassovellusta muodostaakseen VPN-yhteyden, ja tämän tyyppisiä toteutuksia Juniper myös tukee. Juniper kuitenkin tarjoaa SRX-laitteensa mukana modifikaatiota tyypilliseen Remote Access -toteutukseen dynaamista VPN-toteutusta, jossa laite tarjoaa asiakassovelluksen valmiiksi määriteltynä yhteyttä varten. Asiakas hakee kyseisen asiakasohjelman ottamalla suoran yhteyden laitteen IP-osoitteeseen web-selaimella, jota käyttää autentikoitumiseen.

Dynaamisen VPN:n prosessi tunnelin muodostamiseksi menee seuraavasti:

- Asiakas yrittää avata VPN-yhteyden muodostaa https-yhteyden autentikointiportaaliin, joka on VPN-tunnelin päätepiste, eli tässä tapauksessa yrityksen reunalla oleva laite osoitteessa 192.168.5.1.

- Asiakas yhdistyy portaaliin, jossa kysytään asiakkaan käyttäjätietoja.

- Onnistuneen autentikoinnin jälkeen sovellus tutkii asiakkaan sovellusversiota ja päivittää sovelluksen tarpeen vaatiessa uusimmaksi mahdolliseksi. Mikäli sovellusta ei ole ollenkaan asennettuna tai versio on vanha, tarjoaa portaali uusinta versiota asennettavaksi.

- VPN-sovellus avautuu ja uutta autentikointia vaaditaan. Mikäli autentikointi jälleen onnistuu, asiakassovellus lataa viimeisimmät konfiguraatio-optiot palvelimelta, jolloin asiakkaalla on aina viimeisimmät konfiguraatiot tunnelia muodostaessa.

- Tunneli muodostetaan, jonka jälkeen autentikoidaan uudestaan. Tässä tapauksessa autentikointiin käytetään ulkoista RADIUS-autentikointipalvelinta, jonka LDAP-kannassa sijaitsevat käyttäjätiedot. Kyseinen toiseen vaiheen autentikointi on osa tunnelin asetusta, jossa käytetään IPSec:n laajennettua autentikointia: XAuth:ia

- Kun VPN-asiakasohjelma on asennettu, voidaan sovellus avata portaalista uudelleen tai käynnistämällä sovellus suoraan työpöydältä. Molemmilla tavoilla VPN-asiakassovellus autentikoi SRX:n kautta ja lataa aina uusimmat konfiguraatiot käyttäjälle.

Dynaamisen VPN:n määrittely SRX:llä pääperiaatteiltaan menee seuraavien kolmen vaiheen mukaisesti:

- Konfiguroidaan VPN-tunneli.

- Konfiguroidaaan autentikointi sekä IP-osoitteen jakamistapa.

- Assosioidaan VPN-käyttäjät dynaaminen VPN -konfiguraatioilla.

Dynaamisen VPN:n määrittelyssä voidaan käyttää useamman käyttäjän toteutuksissa tarpeiden mukaisesti joko ryhmä IKE ID tai jaettu IKE ID, joista ensimmäiseksi mainittu on suositellumpi sen tarjotessa jokaiselle käyttäjälle uniikin ID:n, eli esimerkiksi käyttäjän ollessa testi1 voi käyttäjän kokonainen IKE ID olla esimerkiksi ”testi.juniper.net”, missä ”juniper.net” on kaikille käyttäjille yhteinen ID. Kaikki käyttäjät jakavat kuitenkin molemmilla tavoilla laitteessa saman IKE-yhdyskäytävän, jolloin käyttäjille ei tarvitse jokaiselle määrittää erillistä VPN-konfiguraatiota. Jaetussa IKE ID:ssä kaikki käyttäjät jakavat yhden IKE ID:n sekä yhden ennalta jaetun IKE avaimen. Tällöin siis asiakkaan yhdistäessä jaetulla IKE ID:llä ja toisen yrittäessä samaan aikaan toisaalta katkeaa ensimmäinen yhteys jälkimmäisen päästessä läpi. Käyttäjän täytyy käyttää jaetussa IKE ID:ssä myös samoja tunnuksia niin WebAuth:iin kuin tunnelin muodostukseen.

Käytetään tässä toteutuksessa yksilöillistä IKE-avainta vähäisen käyttäjämäärän ja verkon topologian yksinkertaisuuden vuoksi, mutta yrityksen todellisessa käyttöympäristössä useilla VPN-asiakkailla ryhmä IKE ID:n käyttö on suositellumpi sekä turvallisuuden että käyttäjärajoitusten poissaolon vuoksi. Käytetään myös konfiguraation yksinkertaistamiseksi Juniperin tarjoamia valmiiksi määriteltyjä proposal-määritteitä dynaamisen VPN ensimmäiseen ja toiseen vaiheeseen.

Aloitetaan määrittelemällä dynaamisen VPN:N määrittely luomalla XAuth-profiili RADIUS-palvelimelle. Määrittelyssä käytetään autentikointipalvelimen IP-osoitetta sekä yhteistä jaettua salaisuutta. Määritellään myös oletukseksi radius-profiili autentikoimaan oletuksena web-portaaliin sekä autentikointipalvelimen käyttämä RADIUS-portti 1812.

edit access

set profile radius-profile authentication-order radius

set profile radius-profile radius-server 192.168.1.254 secret secret

set firewall-authentication web-authentication default-profile radius-profile

set access profile radius-profile radius-server 192.168.1.254 port 1812

Asetetaan SRX jakamaan osoitteet asiakkaalle lokaalista IP-poolista ja sijoitetaan pooli käyttämään XAuth:ia sillä ehdolla, että asiakkaalle jaetun poolin verkon tulee olla erillinen jo käytössä olevaan verkkoon nähden

set access profile radius-profile address-assignment pool dyn-vpn-pool

set access address-assignment pool dyn-vpn-pool family inet network 192.168.2.0/24 // verkko, josta IP jaetaan dynaamisen VPN:n käyttäjälle

set access address-assignment pool dyn-vpn-pool family inet range dyn-vpn-pool-range low 192.168.2.1 // poolista jaettava ensimmäinen IP-osoite

set access address-assignment pool dyn-vpn-pool family inet range dyn-vpn-pool-range high 192.168.2.254 // poolista jaettava viimeinen IP-osoite

Määritellään dynaaminen VPN yhdelle käyttäjälle seuraavasti:

- IKE-käytäntöjen määrittely ennalta jaetulla avaimella sekä käyttöön vaaditulla aggressive-tilalla
    - edit security ike policy
    - set client1pol mode aggressive
    - set client1pol proposal-set compatible
    - set client1pol pre-shared-key ascii-text client1avain
- Määritellään yhteinen IKE-yhdyskäytävä sekä otetaan RADIUS-profiili käyttöön ja asetetaan isäntä
    - edit security ike gateway
    - set client1gw ike-policy client1pol
    - set client1gw dynamic hostname example.com

    - set client1gw external-interface ge-0/0/0.0
    - set client1gw xauth access-profile radius-profile

- IPSec-käytäntöjen määrittely
    - edit security IPSec
    - set policy client1vpnpol proposal-set compatible
    - set policy client1vpn ike gateway client1gw
    - set vpn client1vpn ike IPSec-policy client1vpnpol

- Turvallisuuskäytäntöjen määritys epäluotetusta luotettuun vyöhykkeeseen
    - edit security policies from-zone untrust to-zone trust policy
    - set client1-sec-policy match source-address any
    - set client1-sec-policy match destination-address any
    - set client1-sec-policy match application any
    - set client1-sec-policy then permit tunnel IPSec-vpn client1vpn

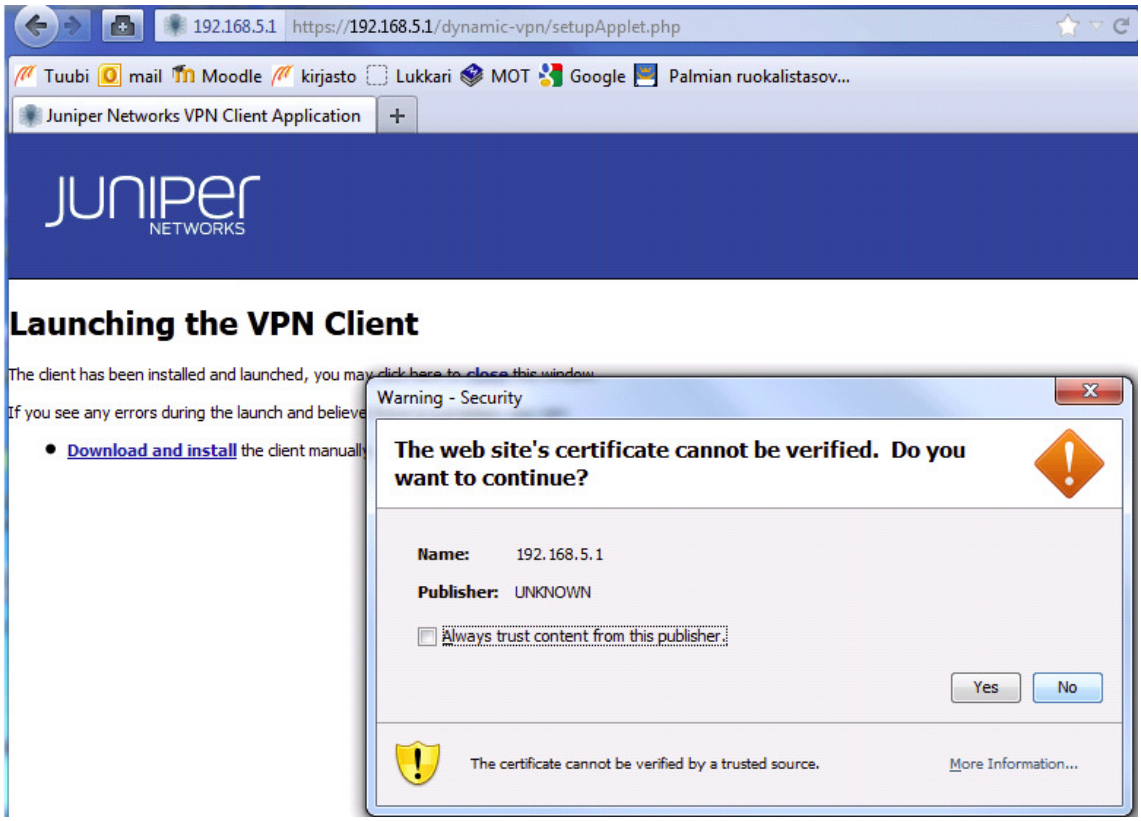
- Määritellään host:lle päin auki tarpeelliset protokollat muun muassa IKE:n sekä web-portaalin käyttöä varten
    - edit security zones security-zone untrust interfaces ge-0/0/0.0
    - set host-inbound-traffic system-services ike
    - set host-inbound-traffic system-services https
    - set host-inbound-traffic system-services http

- set host-inbound-traffic system-services ping
- set host-inbound-traffic system-services ssh

- Radius-profiilin määrittely käyttämään dynaamista VPN:ää
  - edit security dynamic-vpn
  - access-profile radius-profile

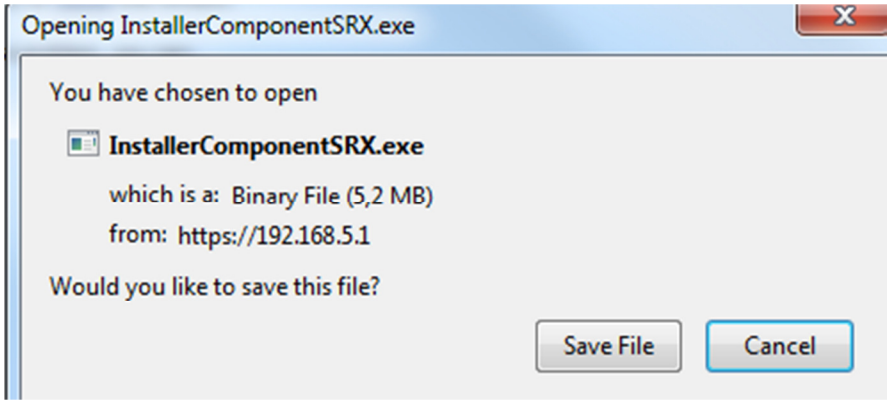
- Asiakkaan määrittely dynaamiselle VPN:lle. VPN on salattu yritysverkkoon 192.168.1.0/24 muun liikenteen kulkiessa salaamattomana
  - edit security dynamic-vpn clients
  - set cfg1 remote-protected-resources 192.168.1.0/24
  - set cfg1 user testi \\ Yhtäläinen autentikointipalvelimelle määritettyyn käyttäjään
  - set cfg1 remote-exceptions 0.0.0.0/0
  - set cfg1 IPSec-vpn client1vpn

Kun muut vaiheet on määritelty, voidaan siirtyä asiakasohjelman määrittelyyn VPN-asiakaskoneelle. Otetaan asiakaskoneella aluksi yhteyttä VPN-yhdyskäytävään, eli työssä käytettyyn osoitteeseen 192.168.5.1, kirjaudutaan testikäyttäjänä 1-vaiheen autentikoinnin ohi ja hyväksytään laitteen generoima sertifikaatti.



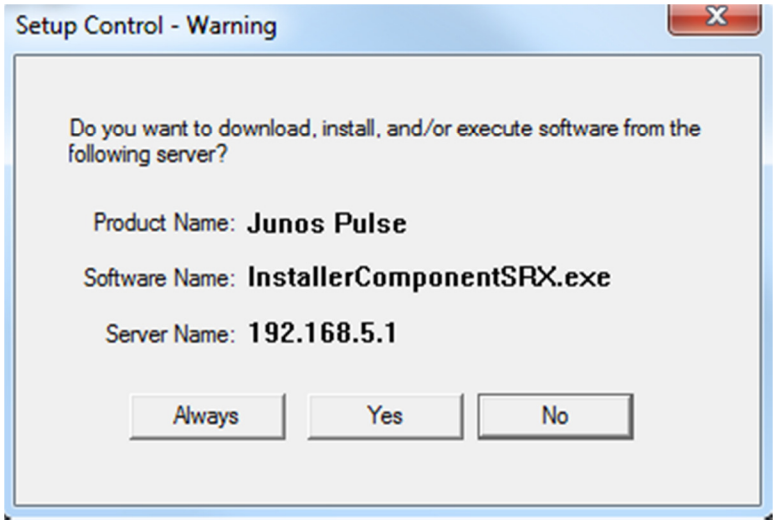
Kuva 23. VPN-asiakkaan yhteydenotto yhdyskäytävään ja sertifikaatin hyväksyminen

Koska asiakaslaitteelle ei ole asennettuna VPN-asiakasohjelmaa, ladataan se Juniper-laitteelta ja hyväksytään asennusohjelman suorittaminen.

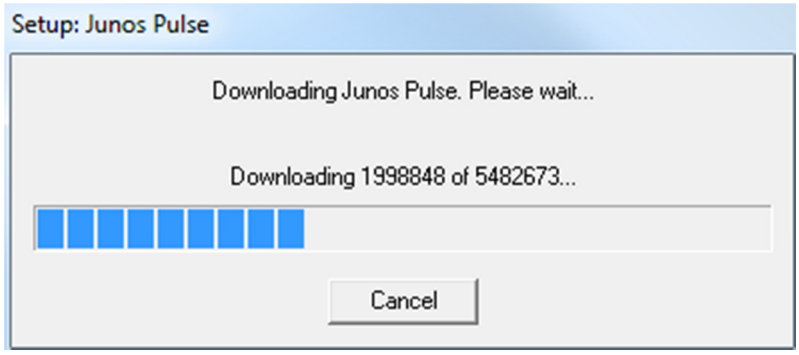


Kuva 24. Asennussovelluksen käynnistävä komponentti

Asennussovellus on tuettuna useimmilla Windows Client -käyttöjärjestelmillä. Tuetut selaimet käyttöön ovat Internet Explorer ja Mozilla Firefox, joissa tulee olla Java JRE -sovellus asennettuna.

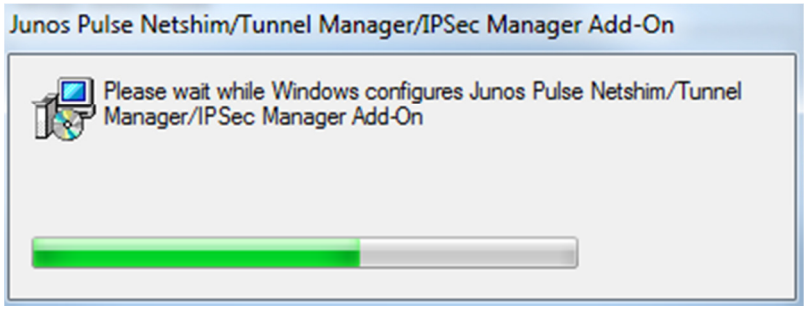


Kuva 25. Asennusohjelman suorituksen hyväksyminen



Kuva 26. Asennusohjelman lataus palvelimelta

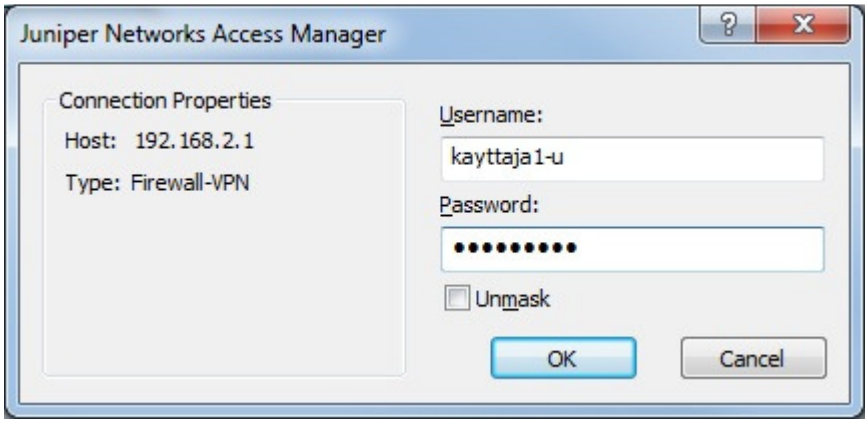
Asennusohjelman suoriuduttua, käynnistyy asiakasohjelma automaattisesti



Kuva 27. Tunneliasetusten automaattinen määritys

Tämän jälkeen siirrytään toisen vaiheen autentikointiin, jossa käytetään RADIUS-autentikointia. Radius-palvelimelle lisättyä testikäyttäjää ei voida tässä tapauksessa

kokeilla käyttäjän kaksisuuntaisen autentikoinnin määritysongelmien vuoksi, joten VPN-tunnelin luonti jää tähän vaiheeseen.



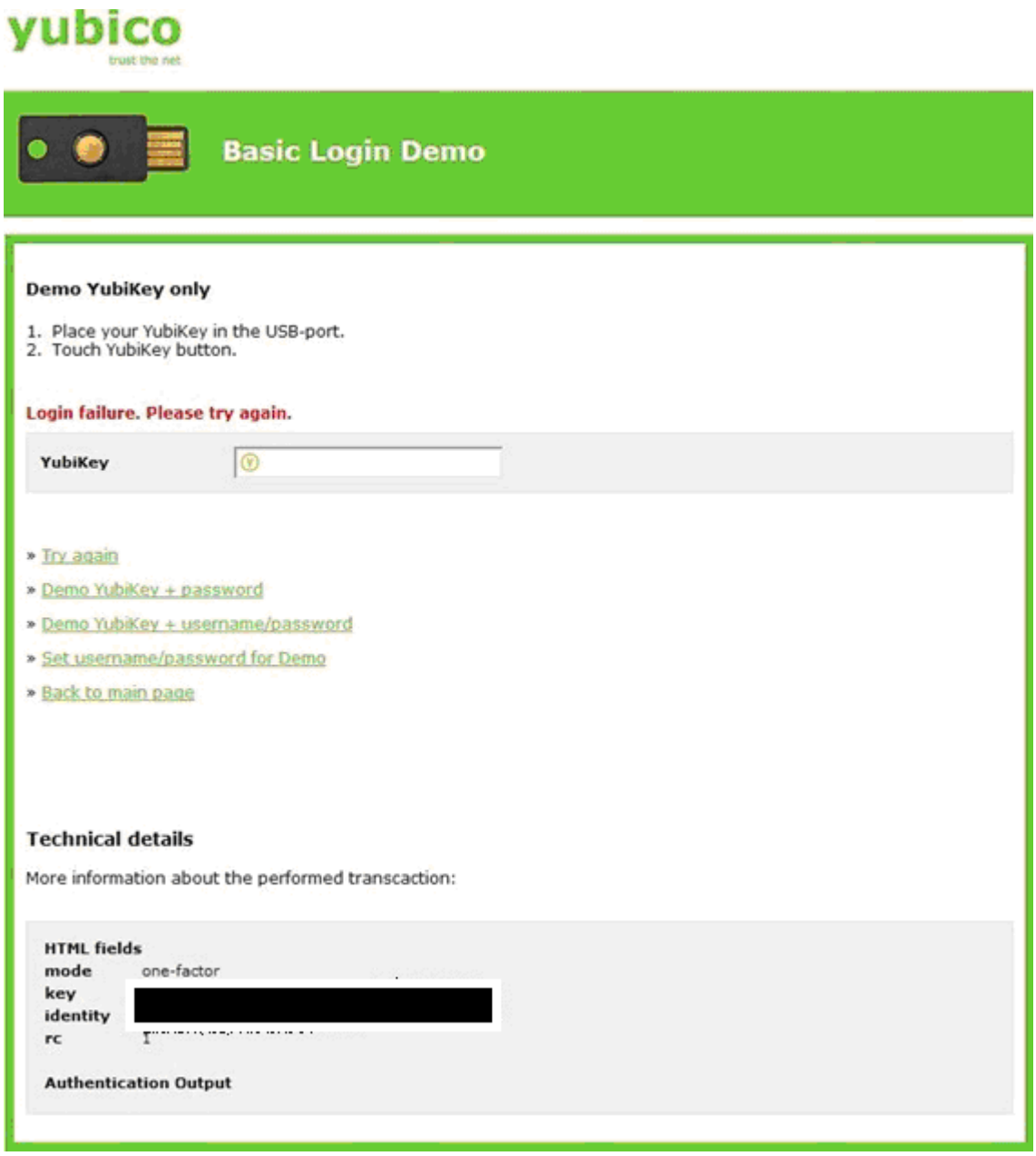
Kuva 28. Toisen vaiheen autentikointi Radius-autentikointipalvelimen kanssa

Toisen vaiheen autentikoinnin onnistuessa Juniper:n kuitenkin tulisi tarjota IP lokaalista DHCP-poolista, jonka jälkeen myös liikenne ohjataan VPN-tunnelin läpi.

8.4 Toiminta ja ongelmatilanteet

Radius-autentikointipalvelimella ilmenneiden ongelmien vuoksi kaksisuuntaisen autentikoinnin käyttöä VPN-tunnelin muodostukseen ei käytännössä täysin voitu saattaa toimintaan. OpenOTP-autentikointipalvelimen käyttöönotossa käytettiin valmistajan dokumentaatiota, jonka mukaan LDAP-testikäyttäjälle yritettiin määrittää Yubikey OTP:tä. Kokeiltiin vielä Radius-palvelimelle määritettyä AES-salaisuutta sekä OTP-identiteettiä ja ohjelmoida Yubikeytä näiden arvojen mukaisesti kuin myös Yubikey:n ohjelmointia useammille eri autentikointimääritteille, kuten pomminvarmaan staattiseen avaimeen. Tästä huolimatta palvelin ei hyväksynyt Yubikeyn generoimia OTP:ita missään muodossa. Palvelin ei myös suostunut luomaan lokitietoa kirjautumisen epäonnistumisista, joten tarkempi selvittely jätettiin ongelman osalta teknisen osuuden valitettavan tiukan aikataulun vuoksi.

Yubikeyn kanssa törmättiin ongelmiin muistipaikkojen Yubicloudin tunnistamispalvelussa sekä laitteen uudelleenohjelmoinnissa.



Kuva 29. Yubico-testaustyökalun epäonnistuminen

Ohjelmointia yritettiin molempiin muistipaikkoihin (Configuration Slot 1 ja 2). Koska tämä ei onnistunut, Yubikey ei voinut validoitua YubiCloudin kanssa, eikä sitä näin ollen myöskään voitu ohjelmoida autentikointipalvelimen paikalliselle OTP-validoinnille.

Pienoisen selvittelyn jälkeen kävi kuitenkin ilmi, että kyseinen Yubikey oli ohjelmoitu käyttämään vain erillistä validointipalvelua, ja molemmat muistipaikoista oli yksityisellä avaimella suojattu, joita ilman uudelleenohjelmointi ei onnistu. Puretaan suojaus ja ohjelmoidaan laite Yubico OTP -tilassa. Kun ohjelmointi on suoritettu, käytetään toi-

mintoa tietojen lähettämiseksi Yubicon palvelimille. Selaimeen avautuva lomake kysyy käyttäjän sähköpostia, jonka rekisteröitymisen jälkeen tulee ilmoitus, että Yubikey OTP määritetään YubiCloud-validointipalvelimille ja on käytössä noin 20 minuutin sisällä. Uudelleenautentikointi onnistuu, joten Yubikeyn toiminta todetaan. Aivan tavallisessa Yubico:n sivustolta hankitussa Yubikeyssä ei kuitenkaan aiemman kaltaisia ongelmia tulisi esiintyä.

Juniper:n VPN:n asetuksissa noudatettiin JunOS-version 11.4 teknisiä dokumenttejä dynaamisen VPN:n määritykseen käyttäen Radius-palvelinta autentikointipalvelimena. Toisen vaiheen Xauth:n haaste-vastaus -toiminnallisuutta Radius-palvelimen kanssa ei kuitenkaan onnistuttu todentamaan autentikointipalvelimen määritysongelmien vuoksi, eikä näin ollen myöskään lopullista tunnelin muodostusta. Autentikointi käyttäen pelkkää käyttäjätunnus - salasana-kombinaatiota käyttäen jätettiin myös todentamatta harmittavan kiireellisen aikataulun sekä toteutuksen alkuperäisen tarkoitusperän muuttumisen vuoksi.

9 Loppuyhteenveto

Mobiilin työntekijän tietoturva on loppujen lopuksi usean osatekijän summa: työntekijän laitteista huolehtiminen, yrityksen verkon määritykset, autentikointitavan- ja tietoturvallisen etäyhteyden määritykset ja niin edelleen. Yhdenkin osatekijän jättäminen pois yrityksen etäkäytön määrittelyissä voi toimia väylänä suuremmille tietoturvauhkille, mutta tarkkaan harkituilla turvatekijöiden valinnoilla minimoidaan uhkaa mahdollisimman pieneksi. Työn yhtenä tarkoituksista on osoittaa valintojen kautta, että etäkäyttöratkaisujen tietoturvallisuus ei vaadi verkon rakenteeseen massiivisia muutoksia eikä näin ollen myöskään suurempia investointeja – jo yrityksen olemassa olevat laitteistot sekä ohjelmistot voivat toimia pohjana ratkaisuille. Mahdollisimman kustannustehokas ratkaisu sekä yksinkertainen implementointi tarkoittaa myös sitä, että ratkaisu on toteutettavissa myös pienemmän yrityksen mittakaavassa.

Työn teknisen osuuden valitettava täysimittaisen toiminnallisuuden toteamisen puutteellisuus vaikuttaa, ettei toteutus toimi suorana oppaana etätyöntekijän tietoturvaratkaisuksi. Kuitenkin osatekijöiden valinta sekä toteutuksen läpikäyminen osatekijöiden kautta tuo esiin tärkeimmät parametrit, joiden pohjalta voidaan ratkaisua lähteä toteut-

tamaan. Toteutuksen mahdollisimman yksinkertainen topologia keskittyy vain olennaiseen, eli tietoturvan parantamiseen kuin myös sopivuuden osoittamiseen yksinkertaisempiin verkkototeutuksiin. Käytännön esimerkkinä muutoksia toteutukseen voisi tehdä esimerkiksi hankkimalla valmistajan oman Radius-palvelimen tai vaihtamalla toiseen OTP-pohjaiseen toteutukseen. Voi kuitenkin olla, että valitsemalla muita ratkaisuja, tarvitaan topologiaan lisätä komponentteja, kuten ulkoisen autentikointipalvelimen tai käyttäjätietokannan. Tätä kautta mitä luultavimmin myös ratkaisun kustannukset nousevat, ja sen käyttöönotto monimutkaistuu.

Sopivan tietoturvakombinaation valinta on tarkoitukseen ja yritykseen sidottu, mutta yleisillä ohjeistuksilla luodaan pohjaa ja helpotetaan osakomponenttien valintaa, joka tässäkin työssä pyritään osoittamaan. Mobiilin työntekijän kattava tietoturvaratkaisu ei ole siis enää kaukainen, monimutkainen ja tätä kautta lähes hyödytön ratkaisu – pikemminkin mahdollisuus uusiin työmahdollisuuksiin ja -tapoihin jatkuvasti mobilisoituvassa maailmassa.

Lähteet

Cronkhite, Cathy ja McGullough, Jack. 2001. Access denied – The Complete Guide to Protecting Your Business Online. USA: Osborne/McGraw-Hill.

Dubrawsky, Ido. 2007. How To Cheat At Securing Your Network. USA: Syngress Publishing, Inc.

IEEE 802.1X for Wired Networks and Internet Protocol Security with Microsoft Windows. Microsoft Corporation. 2008. Verkkodokumentti. <http://www.microsoft.com/en-us/download/confirmation.aspx?id=15249>. Luettu 20.5.2012.

JunOS-esittelysivu. Juniper Networks. Verkkodokumentti. <http://www.juniper.net/us/en/products-services/nos/junos/>. Luettu 20.5.2012.

Mobile workers still struggling with security. Matt Hines. 2007. Verkkodokumentti. <http://www.infoworld.com/d/security-central/mobile-workers-still-struggling-security-847>. Luettu 1.5.2012.

Radius Overview. Juniper Networks. Verkkodokumentti. <http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/Concepts2.html>. Luettu 18.5.2012.

RCdevs OpenOTP-esittelysivu. RCdevs. Verkkodokumentti. <http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/Concepts2.html>. Luettu 25.5.2012.

Safer Authentication with a One-Time Password Solution. Dan Griffin. 2008. Verkkodokumentti. <http://msdn.microsoft.com/en-us/magazine/cc507635.aspx>. Luettu 15.5.2012.

Setup Two-Factor Authentication using OpenOTP. Pradyumna Dash. 2011. <http://www.linuxforu.com/2011/08/setip-two-factor-authentication-using-openotp/>. Luettu 25.5.2012.

SRX-esittelysivu. Juniper Networks. Verkkodokumentti. <http://www.juniper.net/us/en/products-services/security/srx-series>. Luettu 20.5.2012.

SSL VPN – alternative Remote Access technology. NCP Network Communications Products engineering, Inc. 2012. Verkkodokumentti. <http://www.ncp-e.com/en/solutions/remote-access-technologies/ssl-vpn.html>. Luettu 6.5.2012.

What is 802.1X? Joel Snyder. 2010. Verkkodokumentti. <http://www.networkworld.com/news/2010/0506whatisit.html?page=1>. Luettu 13.5.2012.

Wikipedia-artikkeli IPSec. Verkkodokumentti. <http://en.wikipedia.org/wiki/IPSec>. Luettu 5.5.2012.

Wikipedia-artikkeli Juniper Networks. Verkkodokumentti. <http://en.wikipedia.org/wiki/Juniper_Networks>. Luettu 20.5.2012.

Yubikey-esittelysivu. Yubico. Verkkodokumentti. <http://www.yubico.com/yubikey>. Luettu. 23.5.2012.

Juniper SRX -konfiguraatiotiedosto

```
root@testilab-srx# show

## Last changed: 2012-05-31 14:43:59 UTC

version 11.4R2.14;

system {

    host-name testilab-srx;

    root-authentication {

        encrypted-password "$1$q.z63cgt$zmyrHfX.JZreY9OBNqDEM."; ## SECRET-DATA

    }

    name-server {

        10.95.254.252;

    }

    login {

        user testi {

            uid 2001;

            class super-user;

            authentication {
```

```
            encrypted-password "$1$I6k90eGo$be1QIeoFvrv8PrNWZp4LN/"; ## SE-
CRET-DATA
        }
    }
}
services {
    ssh;
    telnet;
    xnm-clear-text;
    web-management {
        http {
            interface vlan.0;
        }
        https {
            system-generated-certificate;
            interface [ vlan.0 ge-0/0/0.0 ge-0/0/1.0 ];
        }
    }
}
```

```
syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    file messages {
        any critical;
        authorization info;
    }
    file interactive-commands {
        interactive-commands error;
    }
}
max-configurations-on-flash 5;
max-configuration-rollbacks 5;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
```

```
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.5.1/24;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
```

```
fe-0/0/2 {
    unit 0 {
        family inet {
            address 10.95.0.52/23;
        }
    }
}
fe-0/0/3 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/4 {
    unit 0 {
```

```
        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/5 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/6 {
    unit 0 {
```

```
        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/7 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
vlan {
    unit 0 {
```

```
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
}
routing-options {
    router-id 192.168.1.1;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface ge-0/0/1.0;
            interface fe-0/0/2.0;
        }
    }
    stp;
```

```
}

security {

    ike {

        policy client1pol {

            mode aggressive;

            proposal-set compatible;

            pre-shared-key  ascii-text  "$9$zTE06/tyrvWLNApeW8Xwsmf5Qz6uORhclFnEy";
## SECRET-DATA

        }

        gateway client1gw {

            ike-policy client1pol;

            dynamic hostname example.com;

            external-interface ge-0/0/0.0;

            xauth access-profile radius-profile;

        }

    }

    IPSec {

        policy client1vpnpol {

            proposal-set compatible;
```

(19)

```
    }
    vpn client1vpn {
        ike {
            gateway client1gw;
            IPSec-policy client1vpnpol;
        }
    }
}
dynamic-vpn {
    access-profile radius-profile;
    clients {
        cfg1 {
            remote-protected-resources {
                192.168.1.0/24;
            }
            remote-exceptions {
                0.0.0.0/0;
            }
```

(19)

```
            IPSec-vpn client1vpn;
            user {
                testi;
            }
        }
    }
}
screen {
    ids-option untrust-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
```

(19)

```
            alarm-threshold 1024;
            attack-threshold 200;
            source-threshold 1024;
            destination-threshold 2048;
            timeout 20;
        }
        land;
    }
  }
}
policies {
  from-zone trust to-zone untrust {
    policy trust-to-untrust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
```

(19)

```
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy pol1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    policy client1-sec-policy {
        match {
```

(19)

```
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                tunnel {
                    IPSec-vpn client1vpn;
                }
            }
        }
    }
}
zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
```

(19)

```
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        vlan.0;
        ge-0/0/1.0;
        fe-0/0/2.0;
    }
}
security-zone untrust {
    screen untrust-screen;
    interfaces {
        ge-0/0/0.0 {
            host-inbound-traffic {
                system-services {
```

(19)

```
                ike;
                https;
                ping;
                ssh;
            }
            protocols {
                all;
            }
        }
    }
}
access {
    profile radius-profile {
        authentication-order radius;
        address-assignment {
```

(19)

```
        pool dyn-vpn-pool;
    }
    radius-server {
        192.168.1.254 {
            port 1812;
            secret "$9$4IZi.Qz6AtOQFCu0Byr"; ## SECRET-DATA
        }
    }
}
address-assignment {
    pool dyn-vpn-pool {
        family inet {
            network 192.168.2.0/24;
            range dyn-vpn-pool-range {
                low 192.168.2.1;
                high 192.168.2.254;
            }
        }
```

(19)

```
        }
    }
    firewall-authentication {
        web-authentication {
            default-profile radius-profile;
        }
    }
}
poe {
    interface all;
}
vlans {
    vlan-trust {
        vlan-id 3;
        l3-interface vlan.0;
    }
}
```

(19)

[edit]

root@testilab-srx