BCP WLAN-verkon infrastruktuuri

Tämän sivun sisältö:

Tunniste	Funetin Parhaat käytännöt-dokumentti
Versio	1.0
Tila	Funetin työvaliokunnan hyväksymä
Päiväys	13.5.2011
Otsikko	WLAN-verkon infrastruktuuri
Työryhmä	MobileFunet
Laatijat	Wenche Backman/CSC, Ville Mattila/CSC, Tanda Tuovinen/HY, Matti Saarinen/HY Juha Nisso/TTY, Siiri Sipilä/Aalto, Mikko Laiho/aiemmin JYU, nyt HY, Thomas Backa/ÅA, Miika Räisänen/OY
Vastuutaho	Wenche Backman/CSC
Tyyppi	suositus

Parhaat käytännöt-dokumenttiin WLAN-verkon infrastruktuuriin kuuluvat myös seuraavat liitteet:

- Ciscon WLAN-kontrollerin konfigurointi
- HPn WLAN-kontrollerin konfigurointi
- FreeRADIUS:en konfigurointi

Liitteet sisältävät ainoastaan konfigurointiohjeita eikä varsinaisia suosituksia.

WLAN-verkon infrastruktuuriin liittyvät elementit

WLAN-verkon infrastruktuuriin voidaan laskea WLAN-tukiasemat, WLAN-kontrolleri sekä autentikointiin liittyvät ohjelmistot ja palvelut, kuten RADIUS-palvelin ja suplikantit. Muussa mielessä WLAN-verkolla on samantyyppiset vaatimukset kun kiinteä lähiverkko. Tukiasemien ja kontrollerin välille voidaan tarvittaessa rakentaa erillinen lähiverkko, jos esim. halutaan käyttää kytkimiä, jotka tukevat Power over Ethernet (!PoE)-standardia. !PoE:n avulla tukiasemien virransyöttö ja kytkeminen verkkoon voidaan hoitaa yhdellä ja samalla Ethernet-kaapelilla, jos tukiasemat pärjäävät !PoE:n antamalla maksimiteholla. Jos WLAN-verkko käyttää sama lähiverkkoinfrastruktuuri kun muu(t) lähiverkko(t), WLAN-verkon liikenteeseen voidaan kuitenkin käyttää eri VLAN. Näin tehdään useassa isossa organisaatiossa. Lisäksi voidaan myös erottaa eri WLAN-verkkojen liikennettä niin, että eri SSID:ssä olevinen WLAN-klienttien liikennettä siirretään kiinteässä lähiverkossa eri VLAN:illa.

WLAN-verkon ja Internetin välillä on lisäksi usein palomuuri. WLAN-verkon säännöt ovat tavallisesti joko samat kuin muiden lähiverkkojen säännöt, jos käytetään sama palomuuri kaikkiin verkkoihin, tai hieman kevyemmät. Jos erotetaan eri WLAN-verkkojen liikennettä kiinteässä lähiverkossa eri VLAN:ien avulla voidaan myös toteuttaa eri palomuurisääntöjä eri verkoille. Näin esim. avoimpien verkkojen säännöt voivat olla tiukempia kuin käyttäjätunnistusta vaativien verkkojen säännöt.

WLAN-verkon kontrollerin konfigurointi

WLAN-verkon kontrolleri kutsutaan suomeksi myös nimellä WLAN-radiokytkin. Aikaisemmin WLAN-verkon peittoa saavutettiin ainoastaan autonomislla (stand-alone) tukiasemilla mutta nykyään yhä useampi verkko rakennetaan kontrolleripohjaiseksi. Tällöin kontrolleri ohjaa tukiasemien toiminnot, kuten viestinvälitys ja signaalitaso. Kontrollerin avulla saadaan yhdenmukaisempi ja helpommin hahmottavissa oleva verkko. Myös ylläpitotyö helpottuu.

Konfiguroinnin kannalta jokaisen valmistajan ratkaisu on hieman erilainen, mutta perustoimenpiteet ovat samat. Alhaalla olevissa dokumenteissa esitetään eri valmistajien parhaaksi käytännöksi nähdyt konfiguroinnit.

Eri valmistajien kontrollerien konfigurointiohjeet:
* Ciscon WLAN-kontrollerin konfigurointi
* HP-kontrollerin konfigurointi

Ciscon konfigurointiohjeissa esitetään miten kontrolleri konfiguroidaan niin, että liikenne aina kulkee tukiasemista kontrollerin kautta ja vasta sitten reitittimen kautta Internettiin. Toinen vaihtoehto olisi viedä liikenne suoraan tukiasemasta lähimpään reitittimeen. Tätä voidaan saavuttaa H-REAP-toimintojen (Hybrid Remote Edge Access Point) avulla. H-REAP-toimintojen avulla voidaan varmistaa että WLAN-klientit pystyvät liikennöimään vaikka kontrolleri olisi vähän aikaa alhaalla. Toisaalta, käyttäjäkohtainen tunnistus, joka BCP WLAN-verkon tietoturva Parhaat käytännöt-dokumentissa suositellaan, toimii ainoastaan kontrollerin kautta, vaikka liikenne vietäisiinkin tukiasemasta lähimpään reitittimeen. H-REAP-toimintojen avulla voidaan myös varmistua siitä, että kontrolleri ei koskaan toimi WLAN-klienttien yhteyksien pullonkaulana, mutta toisaalta kontrollerin prosessointiteho ja porttien nopeudet ovat käytännössä aina tarpeeksi suuret, ainakin vielä tänä päivänä. Lisäksi multicast kontrollerin ja tukiasemien välillä verkon kapasiteetin säästämiseksi ei voida toteuttaa jos liikennettä ei viedä kontrollerin kautta. Lisätietoja H-REAP-toimintojen käyttöönottamisesta löytyy Ciscon sivuilta. Lyhyesti liikenteen vieminen suoraan lähimpään reitittimeen vaatii sen, että sekä tukiasemaan että WLAN-verkkoon (SSID:hen), johon käyttäjä liittyy, on määritelty H-REAP-moodiin.

HP:n kontrollerissa on myös mahdollista valita kulkeeko liikenne aina kontrollerin kautta tai viedäänkö se suoraan tukiasemasta lähimpään reitittimeen. Ohjeissa ei ole otettu kantaa tapaan, jolla käyttäjien liikenne hoidetaan kiinteässä LAN-verkossa. HP:n ohjeissa mainitaan kuitenkin, että verkon rakenne yksinkertaistetaan viemällä kaikki liikenne kontrollerin kautta.

Suosituksia

WLAN-verkon infrastruktuuriin liittyen suositellaan, että

- Uudet verkot rakennetaan aina koostumaan WLAN-kontrollerista ja kontrolleripohjaisista tukiasemista.

Kontrollerien konfigurointiin liittyen suositellaan, että

- Lähekkäin sijaitseville, esim. samassa rakennuksessa tai samalla kampuksella sijaitseville tukiasemille laitetaan sama peruskonfiguraatio, vaikka kontrolleri mahdollistaisi eri parametrien asettamista eri tukiasemille. Näin ylläpito helpottuu.
- Sallitaan kaikkialta kontrollerin ja/tai tukiasemien pingaaminen läpipääsylistoissa.
- Mikäli mahdollista, konfiguroidaan tukiasemat liikennöimään sekä 5 GHz:n että 2,4 GHz:n taajuudella.
- Jos yhdessä kampuksessa on käytössä enemmän kuin yksi kontrolleri, kontrollerit konfiguroidaan kommunikoimaan toistensa kanssa. Näin käyttäjä voi siirtyä tukiasemasta toiseen (handover) ilman katkoja, vaikka tukiasemat olisivat liittyneet eri kontrolleriehin. Ciscon kontrollereissa tähän käytetään mobility-group -määritelmää.

Autentikointimenetelmät ja verkkovierailun huomiointi verkon infrastruktuurissa

WLAN-verkon kontrollerin konfiguroinnin yhteydessä määritellään myös palvelin, joka on liitetty organisaation käyttäjätietokantaan ja joka näin hoitaa käyttäjien autentikoinnin. Palvelimena toimii yleensä RADIUS-palvelin ja eri organisaatioiden RADIUS-palvelimet voidaan liittää yhteiseen juureen, jos halutaan jakaa verkkoa toisten organisaatioiden kanssa. Menetelmä kutsutaan verkkovierailuksi.

Verkkovierailun avulla käyttäjät saavat verkkoyhteyttä nopeasti ja vaivattomasti heidän vieraillessaan eri korkeakouluissa ja yliopistoissa. Verkkovierailu perustuu organisaatioden väliseen vastavuoroisuuteen. Tämä tarkoittaa, että jos organisaatiot A ja B ovat mukana verkkovierailussa, organisaation A käyttäjät voivat käyttää organisaation B julkisen pääsyn verkkoa ja päinvastoin.

Verkkovierailuun on helppo liittyä mutta tietyt federaatiot asettavat tietynlaiset vaatimukset verkkoon, jotka on hyvä huomioida aikaisessa vaiheessa, jopa verkon suunnitteluvaiheessa.

Funet-verkossa tarjolla olevat verkkovierailujärjestelmät ***eduroam*** ja ***Funet-verkkovierailu*** perustuvat RADIUS-hierarkiaan. Käyttäjätunnus ja salasana lähetetään tunnuksen realmin perusteella kotiorganisaatiolle, joka vertaa näitä tietokantaan tallennettuihin tietoihin. Shibboleth-verkkovierailu on kolmas verkkovierailumenetelmä ja se voidaan ottaa käyttöön Haka-infrastruktuuriin liittyneissä organisaatioissa. Liittyminen eduroamiin tai Funet-verkkovierailuun vaatii organisaatiolta oman RADIUS-palvelimen pystyttämisen ja käyttäjien autentikointia tätä RADIUS-palvelinta hyväksikäyttäen. Verkon tukiasemat täytyy myös tukea RADIUS-autentikointia.

eduroam on Funet-verkkovierailua tietoturvallisempi koska käyttäjien autentikointi on hoidettava 802.1x-standardia soveltaen. Tämä tarkoitta, että verkon tukiasemat täytyy tukea kyseistä standardia. Lisäksi liikenne on salattava käyttäen WPA:ta tai WPA2:ta, katso tarkemmin WLAN-verkon tietoturvasta. Funet-verkkovierailussa web-autentikointi on sallittu ja liikenne voi olla salaamaton. eduroamin ja Funet-verkkovierailun erot on esitetty taulukossa 1.

Taulukko 1. eduroamin ja Funet-verkkovierailun erot

eduroam	Funet-verkkovierailu
kansainvälinen	kansallinen
turvallinen autentikointi (802.1x) ja salaus (WPA/WPA2)	web-autentikointi sallittu
yksi SSID (eduroam)	käytetään organisaatioiden omat SSIDt

vain ylemmille oppilaitoksille ja tutkimuslaitoksille	kaupallisia toimijoita sallitaan

RADIUS-palvelimet

Tavallisimpiin RADIUS-palvelimiin kuuluvat Radiator ja !FreeRADIUS, joista ensimmäinen on kaupallinen ja jälkimmäinen perustuu avoimeen lähdekoodiin. Muita kaupallisia RADIUS-palvelimia ovat Microsoftin IAS/NPS ja Ciscon ACS.

RADIUS-palvelimet voidaan asettaa seuraavaan paremmusjärjestykseen Funet-jäsenten kokeilujen perusteella:

- **Radiator** on helppokäyttöisin ja sisältää monipuolisimmat toiminnot. Tuote on kuitenkin kaupallinen
- **FreeRADIUS** on avoimeen lähdekoodinsa takia saavuttanut laajan suosion. Palvelimen versio 2 on selvästi helpommin konfiguroitavissa kuin versio 1.
- **Microsoft IAS/NPS** -palvelimesta puuttuu toimintoja, esim. realmien riisuminen. Realmin riisuminen on kätevä kun halutaan välittää tietokannalle vain käyttäjätunnus ja salasana.

Monipuolisia RADIUS-palvelimien konfigurointiohjeita löytyy eduroam cookbookista. Yksityiskohtaisia FreeRADIUS-konfigurotintiohjeita löytyy FreeRADIUSen konfigurointi-sivulta.

Organisaatiot, jotka ovat liittyneet verkkovieriluun ennen helmikuuta 2010 tulisi tarkistaa, että he ovat liittäneet RADIUS-palvelinsa molempiin Suomen juuripalvelimiin, fltr.funet.fi:hin ja ftlr2.funet.fi:hin. Jos on käytössä Radiator, suositellaan käytettäväksi Dead Realm Marking-menetelmä. Lisätietoja saat Funetilta.

IEEE 802.1x

eduroam-verkkovierailussa autentikointi on hoidettava 802.1x-standardin avulla. IEEE 802.1x -standardi on otettava huomioon konfiguroidessa WLAN-kontrolleria ja RADIUS-palvelinta. Lisäksi standardi on otettava huomioon käyttäjien opastuksen yhteydessä, koska verkkoon liitytään selaimen sijasta suplikantin avulla. IEEE 802.1x käytetään porttikohtaiseen todentamiseen. 802.1x määrittelee kolme osapuolta: suplikantti eli asiakas (käyttäjän päätelaite/ohjelmisto), autentikaattori (verkon liityntäpiste, esim. tukiasema) ja autentikointipalvelin.

802.1x -pohjaisessa todentamisessa käytetään ilmarajapinnassa EAP over LANs (EAPOL)-protokollaa. Tukiaseman ja autentikointipalvelimen välillä EAP-viestit välitetään RADIUS-paketeissa. Varsinainen todentaminen suoritetaan Radius-Access-Request-paketeilla, joissa käyttäjän antamat tiedot välitetään autentikointipalvelimelle sekä autentikointipalvelimen vastauksena lähettämillä Radius-Access-Challenge-paketeilla, jotka käytetään käyttäjän identiteetin tarkistamiseen. Pääsy verkkoon sallitaan Radius-Access-Accept-paketilla, jonka jälkeen tukiasema lähettää suplikantille tarvittavat kryptausavaimet. Tarvittavat kryptausavaimet määräytyy verkon salaustason mukaan, katso BCP WLAN-verkon tietoturva Parhaat käytännöt-dokumenttia. Jos kryptausavaimet halutaan vaihtaa tietyllä aikavälillä, joudutaan usein autentkoimaan käyttäjä uudelleen.

Toisin kuin web-autentikoinnissa, 802.1x:ssä käyttäjälle ei anneta IP-osoitetta ennen autentikointia ja paketteja lähetetään vain pyydettäessä. Pyytämättömiä paketteja autentikoimattomilta käyttäjiltä ei esiinny ilmarajapinnassa.

EAP-menetelmät ja autentikointi

802.1x perustuu EAPiin (Extensible Authentication Protocol) ja EAP-metodissa on määritelty sääntöjä siitä, miten autentikointi hoidetaan. Sääntöihin kuuluu mm. miten käyttäjän identiteetti pyydetään ja lähetetään sekä miten todentamiseen liittyvät haasteet (challenge) hoidetaan. EAPissa on sekä ulompi menetelmä että sisempi menetelmä. Riittävän vahvaa kryptausta tarjoaa käytännössä vain seuraavat ulommat EAP-menetelmät:

- EAP-TLS (Transport Layer Security), joka perustuu molemminpuoliseen todentamiseen varmentimien vaihdon kautta. Vaatii kuitenkin varmennen asentamista jokaiselle päätelaitteelle.
- PEAP (Protected EAP) ja TTLS (Tunneled TLS) ovat kaksivaiheisia ja hyvin samankaltaisia. Ensimmäisessä vaiheessa avataan TLS-tunneli, jonka kautta palvelimen varmenne lähetetään ja hyväksytään. Tämän jälkeen TLS-tunneli käytetään käyttäjän todentamiseen sisäisellä autenitkointimenetelmällä. Tunnetuimmat sisemmät autentikointimenetelmät ovat:
    - MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2), jossa salasana lähetetään Windowsin käyttämässä hash-muodossa.
    - PAP (Password Authentication Protocol), jossa salasana kulkee verkossa selväkielisenä. Toimii vain TTLS:n kanssa koska siinä sisempi autentikointimenetelmä ei tarvitse olla EAP-tyyppinen.

Autentikoinnissa käytetty RADIUS-palvelin voidaan liittää mihin tahansa tietokantaan, mutta salasanan säilytysmuoto määrittelee mitkä EAP-menetelmät infrastruktuurissa voidaan ottaa käyttöön. Jos RADIUS-palvelin liitetään AD:hen, salasana on varastoitu MSCHAPv2:n käyttämässä hash-muodossa (NTHASH) ja kaikki päätelaitteiden omat suplikantit, jotka yleensä tukevat MSCHAPv2:ta, voidaan käyttää. MSCHAPv2 on tuettu mm. Linuxeissa, Windowsissa, Nokian puhelimissa ja Maceissa. Jos käytetty RADIUS-palvelin ja AD eivät ole yhteensopivia, joudutaan käyttämään domain kontrolleria tai muita ratkaisuja. RADIUS-palvelin voidaan myös liittää muista hasheista koostuvaan tietokantaan, esim. MD5-hashesta koostuvaan tietokantaan, mutta tässä tapauksessa käyttöjärjestelmien omat suplikantit eivät välttämättä voida hyödyntää vaan joudutaan käyttämään kolmannen osapuolen suplikanttia. Kattava lista hash-muotojen ja autentikointimenetelmien yhteensopivuudesta löytyy täältä.

Käytettävät EAP-menetelmät määritellään kotiorganisaation RADIUS-palvelimen konfiguroinnin yhteydessä ja määritettyjen menetelmien avulla käyttäjä autentikoidaan sekä kotiorganisaation verkossa että vierailijaorganisaation verkossa. On siis huomattava, että käytettävät EAP-menetelmät määräytyvät kukin käyttäjän kotiorganisaation mukaan. Vieraillessa muualla käytetään aina samat EAP-menetelmät kuin kotiorganisaatiossa.

Varmenne

WLAN-verkon autentikointia hoitavalle RADIUS-palvelimelle on ehdottomasti hankittava varmenne. Varmenne voi olla joko itse-allekirjoitettu (self-signed) tai julkisen CA:n varmistama. Kun organisaation RADIUS-palvelimelle hankitaan varmenne on otettava huomioon seuraavat seikat:

- Jos hankitaan kaupallinen CA-varmenne, olisi hyvä valita mahdollisimman tunnettu toimittaja, jonka juurivarmenne löytyy valmiiksi asennettuna useimmista päätelaitteista.
- Jos luodaan palvelimelle oma varmenne (self-signed certificate) on kehitettävä käyttötukiprosessia niin, että oman organisaation loppukäyttäjien päätelaitteisiin saadaan varmenetta vastaava viittausvarmenne (reference certificate) asennettua turvallisesti.

Jotta saavutettaisiin varmenteen kanssa turvallinen autentikointi, suplikantin asetuksiin on kiinnitettävä tarkkaa huomiota. Jos hankittu varmenne on julkisen CA:n allekirjoittama, ei riitä että käyttäjä suplikantissaan määrittelee CA:n luotuksi toimittajaksi vaan tämän lisäksi käyttäjän on määriteltävä palvelimen nimi, jolle varmenne on allekirjoitettu, esim. auth.csc.fi. Jos käytetään itse-allekirjoitettua (self-signed) varmennetta on houlehdittava siitä, että varmenne saadaan jaettua käyttäjille helposti ja turvallisesti. Varmenne on asennettava käyttäjien päätelaitteille ennen kuin niillä liitytään verkkoon.

Suosituksia

Autentikoinnin ja verkkovierailun huomiointiin infrastruktuurissa liittyen suositellaan, että:

- kaikki Funet-jäsenet liittäisivät langattomat verkkonsa ainakin Funet-verkkovierailuun ja mahdollisuuksien mukaan myös eduroamiin.
- Funet-jäsenet panostaisivat verkkovierailun tiedottamiseen ainakin seuraavalla tavalla:
    - Kotisivuilta löytyisi tietoa Funet-verkkovierailun ja/tai eduroamin käyttömahdollisuuksista jäsenen kampuksilla
    - Vierailijoiden saapuessa kampuksille tai oman organisaation henkilökunnan tai opiskelijan matkustamisen yhteydessä huomioitaisiin ensisijaisesti eduroam ja Funet-verkkovierailu. Vasta tämän jälkeen yritettäisiin järjestää langaton verkkoyhteys muulla tavalla.
- Funet-jäsenet varmistaisivat, että he ovat liittäneet RADIUS-palvelinsa molempiin Suomen juuripalvelimiin, fltr.funet.fi:hin ja ftlr2.funet.fi:hin. Jos on käytössä Radiator, käytetään tässä yhteydessä Dead Realm Marking-menetelmä.
- Funet-jäsen käyttäessään julkisen CA:n allekirjoittettua varmennetta kiinnittäisi tarkkaa huomiota siihen, että käyttäjien suplikantissa käytetty CA on valittu luotuksi toimittajaksi ja ennen kaikkea siihen, että myös palvelimen nimi on määritelty.

Käyttäjän liittyminen verkkoon

Kun WLAN-verkko on pystytetty ja RADIUS-palvelin on liitetty käyttäjätietokantaan sekä mahdollisesti myös verkkovierailun RADIUS-hierarkiaan, käyttäjät voivat liittyä verkkoon määriteltyjen menetelmien avulla. Funet-verkkovierailussa tämä tarkoittaa web-autentikointia mutta eduroamissa liittyminen tapahtuu käyttöjärjestelmän oman suplikantin tai kolmannen osapuolen suplikantin avulla.

Selainpohjainen autentikointi

Web-autentikointia käytettävissä verkoissa, mm. Funet-verkkovierailun piirissä olevissa verkoissa, käyttäjälle aukeaa sisäänkirjautumissivu hänen avatessaan selainta. Autentikointia varten päätelaitteessa tarvitaan ainoastaan selain. Funet-verkkovierailussa olevat organisaatiot voivat konfiguroida sisäänkirjautumissivuaan sisältämään listan kaikista mukana olevasta organisaatioista, jotta käyttäjä heti tietää onko hänellä mahdollisuus päästä verkkoon omilla käyttäjätunnuksillaan. Käyttäjätunnus syötetään muodossa tunnus@kotiorganisaatio.fi

Funetin ylläpitämä lista mukana olevista organisaatioista:

- Verkkovierailuyhteistyössä mukana olevat suomalaiset organisaatiot

Suplikantit

802.1x-standardia soveltavissa verkoissa, mm. eduroamissa, käyttäjät liittyvät verkkoon kotiorganisaation määrittelemää EAP-menetelmää käyttäen. Tarvittava suplikantti löytyy useammista käyttöjärjestelmistä sekä ulkoisista verkkokorteista. Linuxista löytyy WPA-suplikantti ja Windowsilla on myös omansa. Nokian uusimmat puhelimet ja iPhone sisältävät myös 802.1x-suplikantin. On myös mahdollista käyttää kolmannen osapuolen suplikanttia, joista mm. SecureW2 on suosittu. Suplikanttien konfigurointi voi olla epätriviaali, jonka takia on tuotettu runsaasti opastusmateriaalia. Alhaalla muutama esimerkki.

Windows XP:n konfigurointi eduroamia varten:

- Windows XP:n suplikantin konfiguroini (video suomeksi)

Windows XP:n, Intelin ja !SecureW2:n suplikanttien konfigurointiohjeita eduroamia varten:

- Suplikanttien konfigurointi (video englanniksi)

Windows XP:n, WPA-suplikantin, Nokian E51-sarjan suplikantin sekä Lenovon !ThinkVantage Access Connections -suplikantin konfigurointiohjeita eduroamia varten esimerkkinä:

- Suplikanttien konfigurointi (tekstimuodossa suomeksi)

Windows Vistalle ja Windows 7:lle voidaan luoda asentajan (installer) joka laatii WLAN-verkon tietojen pohjalta xml-tiedoston. Tiedoston avulla asetukset viedään suplikantille ja konfigurointi on valmis. Lisätietoja EduroamAsennusohjelma-sivulta.

Useaan suplikanttiin voidaan määritellä sekä ulompi että sisempi identiteetti. Ulommassa identiteetissa (outer identity) käyttäjätunnus voi olla mikä tahansa mutta realm on oltava oikein, esim. anonymous@csc.fi. Sisempi identiteetti (inner identity) on sisältävä sekä oikea käyttäjätunnus että realm, esim. wbackman@csc.fi. Käyttämällä anonyymi ulompi identiteetti voidaan verkkovierailussa välttyä siitä, että henkilöllisyys tallentuu vierailevan organisaation lokeihin. Sisempi identiteetti on tiedossa ainoastaan kotiorganisaatiolla. Linuxin suplikantti, Nokian puhelimien suplikantti sekä SecureW2 tukevat eri sisäisen ja ulkoisen identiteetin määrittelemisen, mutta Windowsin sisäänrakennettu suplikantti ei tue tätä.

Suosituksia

Suplikantteihin liittyen suositellaan, että

- käyttäjiä olisi hyvä opastaa käyttämään anonyymi ulompi identiteetti aina kuin se on mahdollista. Jos autentikointiyritys jostain syystä epäonnistuu, olisi hyvä virheselvitystä varten tehdä ainakin yksi yritys sellaisella ulommalla identiteetillä, joka muistetetaan jälkikäteen. Näin virheselvitystyö helpottuu.

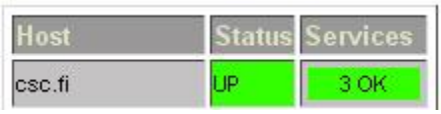
Infrastruktuurin valvonta

Verkkovierailuinfrastruktuuria on syytä valvoa, jotta ongelmatilanteet voidaan havaita ja ratkaista ennen kuin käyttäjät turhautuvat. Nagios soveltuu hyvin tähän tarkoitukseen ja CSC/Funet valvoo Suomen juuripalvelimien, ftlr.funet.fi ja ftlr2.funet.fi sekä oman RADIUS-palvelimensa lähettämällä autentikointipyyntöjä ja tarkistamalla että autentikointi onnistuu. Valvonta tehdään useampaa reittiä pitkin:

- @csc.fi-tunnus lähetetään ftlr.funet.fi:lle ja ftlr2.funet.fi:lle
- paikallisessa tietokannassa olevan käyttäjätunnuksen autentikointia testataan ftlr.funet.fi:ssa ja ftlr2.funet.fi:ssa
- @csc.fi-tunnus lähetetään suoraan CSC:n RADIUS-palvelimelle
- Lisäksi testataan vierailijatunnuksen autentikointia sekä valvotaan ping-viive, pakettihävikkiä ja SSH-yhteyden avaamista.

Kehittyneimpiin valvontamenetelmiin kuuluu valvonnan hoitaminen vastaavalla viestinvälityksellä kuin käyttäjän suplikantti. Toinen vaihtoehto on käyttää tähän tarkoitukseen pelkkiä RADIUS-autentikointipyyntöjä, mutta tässä tapauksessa mm. varmenteen tiedot jää tarkistamatta. Palvelimen toiminnan tarkistaminen suplikantin näkökulmasta voidaan hoitaa WPA-suplikantin eapol_test -ohjelmalla. eapol_test -ohjelma voidaan liittää ainakin Nagiokseen sekä Helsingin Yliopistossa käytettyyn valvontaohjelmistoon Big Sisteriin. Ohjelman avulla voidaan toteuttaa mm. PEAP-MSCHAPv2, TTLS-MSCHAPv2 sekä TTLS-PAP -menetelmien valvonta.

Funet-verkon verkkovierailun reaaliaikaisen tilanteen havaitsemiseksi on kehitetty eapol_test -ohjelmaan perustuva valvonta, jonka tulokset esitetään [[https://info.funet.fi/cgi-bin/funet-services-roaming-availability][info.funet.fi:ssa]]. Valvonnassa ovat organisaation toteutuneista menetelmistä riippuen yksi tai useampi seuraavista menetelmistä: PEAP-MSCHAPv2, TTLS-MSCHAPv2 ja/tai TTLS-PAP. Lisää palvelimia liitetään mielellään palveluun, mutta tätä varten Funet tarvitsee voimassa olevan käyttäjätunnuksen ja salasanan sekä tietoa palvelimen varmenteesta. Kun kaikkien kolmen menetelmän avulla toteutettu autentikointi onnistuu, tulos on kuvan 1 mukainen.



Kuva 1. Verkkovierailun valvonta. Esimerkkinä CSC:n autentikointipalvelimen tulokset.

Funet-jäseniä kehoitetaan valvomaan omia palvelimia vähintään RADIUS-autentikointipyynnöillä mutta mielellään WPA-suplikantin eapol_test-ohjelman avulla. eapol_testin installointiohjeet (EAP)autentikointimenetelmien konfigurointitietoineen löytyvät netistä. CSC/Funet on eapol_test-ohjelman ympärille kehittänyt tarkistusskripti nimellä check_eapauth, jonka Debian/Ubuntu- ja RHEL/CentOS-paketit löytyvät liitteestä. check_eapauth -skriptille on parametreina annettava kaksi tiedostoa, joista toinen on eapol_testin installointiohjeista löytyvä .conf-tiedosto, esimerkiksi peap-mschapv2.conf. Toinen on tiedosto, missä on verkkovierailussa käytettävän palvelimen IP-osoite ja jaettu salaisuus seuraavassa muodossa:

```
radius-server <palvelimen IP-osoite>
radius-secret <jaettu salaisuus>
```

Valvontapalvelimen IP-osoite ja jaettu salaisuus on myös luonnollisesti lisättävä verkkovierailussa käytettävän palvelimen klienttinä.

Suosituksia

Verkkovierailuinfrastruktuurin valvontaan liittyen suositellaan, että:

- Organisaatio valvoo oman RADIUS-palvelimensa käyttäen voimassa olevaa käyttäjätunnusta, joka on määritelty valvontaa varten. Valvonta on vähintään hoidettava RADIUS-autentikointipyynnöillä mutta suositeltavaa olisi käyttää WPA-suplikantin eapol_test -ohjelmaa valvontaan, jotta myös EAP-menetelmien toimivuutta voitaisiin valvoa.

Verkkovierailuinfrastruktuuriin liittyen huomautetaan seuraavista:

- Mikäli käytännössä mahdollista, olisi hyvä järjestää Funetille voimassaolevan käyttäjätunnuksen verkkovierailun reaaliaikaisen tilanteen visualisoimiseen info.funet.fi:ssä. Tästä hyötyisivät sekä IT-tuki että viime kädessä myös loppukäyttäjät.

Muutama yleinen huomautus

- PAP-menetelmällä salasana lähetetään kryptaamattomana mutta tämä ei kuitenkaan estä sitä, ettei käyttäjätietokanta voisi sisältää salasana kryptatussa muodossa.
- FreeRADIUS ei toimi joidenkin puhelimien suplikanttien kanssa
- Isolla kampusalueella RADIUS-palvelimia saattaa olla useampia ja eri käyttötarkoituksiin hankittuja. Niiden yhdistäminen voisi helpottaa ylläpitoa mutta yhteisymmärryksen aikaansaaminen saattaa olla vaikea.

Funet-jäsenten autentikointi- ja verkkovierailuratkaisut

Tämän otsikon alla esitetään lyhyesti eri Funet-jäsenten autentikointi- ja verkkovierailuratkaisut esimerkkeinä.

Helsingin yliopisto

Helsingin yliopistolla on käytössä PEAP-MSCHAPv2, TTLS-MSCHAPv2 ja TTLS-PAP. Autentikointipyyntö ohjataan kampusten sisäisen RADIUS-hierarkian avulla oikeeseen tietokantaan realmin perusteella. Esimerkiksi @ad.helsinki.fi-käyttäjätunnukset ohjataan AD:hen, jossa salasanat on varastoitu NTHASH-muodossa ja EAP-menetelmät PEAP-MSCHAPv2 sekä TTLS-MSCHAPv2 voidaan tukea.

Helsingin yliopistolla on käytössä Radiatorin RADIUS-palvelimia. FreeRADIUS v1:stä on huonoja kokemuksia mutta FreeRADIUS v2 pitäisi toimia paremmin.

Suplikanttien suhteen ei ole rajoituksia, vaan kaikki vaihtoehdot tuetaan.

Teknillinen korkeakoulu / Aalto yliopisto

Aallon yliopistolla on tällä hetkellä FreeRADIUSv2-palvelin liitettynä NPS-palvelimeen, joka vuorollaan on liitetty AD:hen. FreeRADIUSv2-palvelin ei ole liitetty suoraan AD:hen johtuen samban tämänhetkisistä puutteista. EAP-menetelmistä tuetaan PEAP-MSCHAPv2. Realmina käytetään org.aalto.fi aalto.fi:n sijasta koska domain controller on konfiguroitu tälle realmille eikä autentikointi toisella realmilla onnistu. NPS-palvelimesta puuttuu realmin riisuminen ja tästä syystä pelkää käyttäjätunnusta ja salasanaa ei voida välittää tietokannalle.

Åbo Akademi

Åbo Akademilla on Sparknet-verkossaan käytössä FreeRADIUS v1 liitettynä LDAPiin. Vaasassa on käytössä IAS.

Lisäksi Åbo Akademilla on verkkouudistus meneillään ja tämän yhteydessä on mm. eduroamia varten pystytetty FreeRADIUSv2-palvelin ja liitetty se LDAP-tietokantaan.

Tampereen teknillinen yliopisto

Tampereen teknillisellä yliopistolla on käytössä Radiator, joka on liitettynä LDAPiin. Tuetut EAP-menetelmät ovat PEAP-MSCHAPv2, TTLS-MSCHAPv2 sekä TTLS-PAP. Salasanat on LDAP-tietokannassa tallennettu useampaan eri muotoon kuten NTHASH ja SHA-hash. Salasanoja ei kuitenkaan ole tallennettu selväkielisinä.

Windowsin ja puhelimien suplikanteille tarjotaan käyttöohjeistusta ja tukea.

Jyväskylän yliopisto

Jyväskylän yliopistolla on käytössä FreeRADIUS-palvelimia. Tuetut EAP-menetelmät ovat PEAP-MSCHAPv2 ja TTLS-PAP. Salasana, joka käytetään PEAP-MSCHAPv2-autentikoinnin yhteydessä, on vaihdettava kahden viikon välein. SecureW2 tuetaan ja esikonfiguroimiseen tarvittava lisenssi on hankittu.

Myös Shibboleth-verkkovierailu on jonkun verran käytössä.

Oulun yliopisto

Oulun yliopisto käyttää !FreeRADIUSv2 palvelimia, jotka ovat liitetty kahteen eri aktiivihakemistoon. Freeradiuksella tehdään mm. realmien uudelleenkirjoitus ja ntlm_auth –ohjelman ajoa eri parametrein, jotta käyttäjät voivat käyttää helpommin muistettavaa tunnusmuotoa (~sähköpostiosoite).

Oulun yliopiston tukiasemissa henkilökuntatunnuksella kirjautuneelle annetaan eri VLAN kuin opiskelijoille ja vierasorganisaatioista tuleville. Näin saadaan poistettua erillisen henkilökuntaverkon SSID ja käytön *pitäisi* olla helpompaa.

Windows XP, Vista ja 7 –käyttäjille on tehty eduroam-asennuspaketti, joka asentaa työasemaan oulu.fi CA –varmenteen ja tekee eduroam-verkkoprofiilin. Käyttäjän tarvitsee vain syöttää käyttäjätunnus ja salasana käyttöjärjestelmän sitä kysyessä. Asennuspaketti on

toteutettu NSIS:lla.

EAP-menetelmistä tuetaan PEAP-MSCHAPv2 ja suplikanteista käyttöjärjestelmien mukana tulevat. Muiden suplikanttien käyttöä ei ole ohjeistettu.

Turun yliopisto

Turun yliopistolla on kahdennettu FreeRADIUSv2 RHEL6-alustalla. Tuettuna EAP-menetelmänä on PEAP-MSCHAPv2. Eduroamin EAP-autentikoinnit ohjataan Active Directoryyn, Sparknetin ja Funet-verkkovierailun RADIUS-autentikoinnit LDAP:iin. AD-salasana synkronoidaan automaattisesti LDAP:iin ja syyskuusta alkaen myös toiseen suuntaan. EAP-varmenne hankittiin DigiCertiltä Entrustin juurella allekirjoitettuna, joka kelpaa ainakin tuoreille Symbian-puhelimille suoraan.

Arcada

Arcadassa on FreeRadius v2 liitettynä OpenLDAP-kantaamme jossa salasanat on salattu md5:lla. Tuettu EAP-menetelmä on TTLS-PAP. Realm-ittomat ja @arcada.fi realmilliset ohjataan suoraan LDAP:iin suffix() jälkeen, muut ftlr:ään. radius.arcada.fi-palvelimen varmenteen on allekirjoittanut AddTrust External CA Root.

Arcada tarjoaa käyttäjilleen valmiita SecureW2-paketteja sekä MacOSX mobileconfig tiedostoja helpottamaan mukaantuloa. Tätä kirjoitettaessa eduroam-tukitiedostot on vielä tekemättä. Arcadassa on rakennettu kokonaan uusi langaton kaikenkattava verkko syksyllä 2011. Vielä on ratkaisematta miten saadaan klientit siirtymään 5 GHz:in puolelle jos SSID on sama "eduroam" myös 2.4 GHz:in puolella.

Lisätietoja

Esite eduroamista

- eduroam-esite

Lisätietoja Funet-verkossa tarjolla olevista verkkovierailujärjestelmistä:

- http://www.eduroam.fi

Teknisiä tietoja ja ohjeita eduroamista

- eduroam.org-ohjeet

NIST Special Publication 800-120, "Recommendation for EAP Methods Used in Wireless Network Access Authentication:"

- NIST_EAP_recommendations

Kommentteja

Shibboleth-verkkovierailu on kai käytännössä mahdollista vain Helsingin yliopiston HUPNetissä, jossa HAKA-infrastruktuuriin liittyneiden organisaatioiden henkilöt voivat tunnistautua oman organisaationsa tunnuksilla ja päästä käyttämään verkkoa. Shibboleth myös vaatii tuen WWW-pääsynvalvojalta ja tätä tukea ei taas kaupallisissa WWW-pääsynvalvojissa ole. Osittain tästä syystä Shibbolethiin pohjautuvaa verkkovierailua ei siis juuri ole käytössä muissa HAKA-infrastruktuuriin liittyneiden organisaatioiden langattomissa verkoissa. -- Karri Huhtanen

Shibboleth-verkkovierailu pitäisi olla mahdollista Helsingin yliopistossa (Hupnet), Turun yliopistossa (Sparknet) ja Jyväskylän AMK:ssa. (http://www.csc.fi/hallinto/haka/luottamusverkosto/palvelut). --Wenche Backman