jamk.fi

CISCO TRUSTSEC KÄYTTÖÖNOTTO JYVSECTEC -YMPÄRISTÖSSÄ

Joni Honkanen

Opinnäytetyö
Elokuu 2014

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) Honkanen Joni	Julkaisun laji Opinnäytetyö	Päivämäärä 25.08.2014
	Sivumäärä 115 + 24	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)
Työn nimi Cisco TrustSec käyttöönotto JYVSECTEC -ympäristössä		
Koulutusohjelma Tietotekniikan (Tietoverkkotekniikan) koulutusohjelma		
Työn ohjaaja(t) Saharinen Karo Kotikoski Sampo		
Toimeksiantaja(t) Jyväskylä Security Technology (JYVSECTEC) Vatanen Marko		

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Jyväskylä Security Technology (JYVSECTEC)-hanke, joka toimii Jyväskylän ammattikorkeakoulun tiloissa. JYVSECTEC kehittää ja ylläpitää kyberturvallisuuden kehitysympäristöä tutkimus, kehitys ja koulutuskäyttöön. Tavoitteena työssä oli toteuttaa identiteettipohjainen tietoturva-ratkaisu käyttäen hyväksi Cisco TrustSec-komponentteja. Työ koostui suunnittelu-, testaus- ja todennusosioista sekä ohjeesta ympäristöä tulevaisuudessa hyödyntäville.

Työn verkkoympäristö koostui Cisco Systemsin laitteista, jotka tukivat TrustSec-toiminnallisuuksia. Näitä laitteita olivat mm. C3750X- ja C3560X-kytkimet, ASA-palomuuri, sekä WLC 2504. Pääkomponenttina työssä toimi Cisco Identity Services Engine (ISE), jolla hallinnoitiin mm. verkkoon pääsyä autentikoimisen ja valtuuttamisen muodossa. Ympäristössä hyödynnettiin SGA-arkkitehtuuria, johon sisältyi mm. verkkolaitteiden välinen NDAC-autentikointi, liikenteen merkkaamista SGT/SXP-menetelmillä, palomuurin SGFW-ominaisuuden testaamista ja päätelaitteiden autentikoimista 802.1X-protokollalla. Päätelaitteen ja kytkimen välillä toteutettiin myös L2-tason salaus 802.1AE (MACsec)-protokollan avulla. Samaa salausta käytettiin myös kytkinten välillä NDAC-autentikoinnin päätteeksi.

Opinnäytetyön tuloksena syntyi ympäristö, jossa tutkittiin useita TrustSec-ominaisuuksia. Tulevaisuudessa ympäristöä voidaan hyödyntää jatkokehityksessä ja koulutuspalveluissa.

Avainsanat (asiasanat)
TrustSec, ISE, 802.1X, SGA, NDAC, SGT, SXP, MACsec

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
Honkanen Joni	Bachelor´s Thesis	25.08.2014
	Pages 115 + 24	Language Finnish
		Permission for web publication (X)

Title
Cisco TrustSec implementation in JYVSECTEC-environment

Degree Programme
Information Technology

Tutor(s)
Saharinen Karo
Kotikoski Sampo

Assigned by
Jyväskylä Security Technology (JYVSECTEC)
Vatanen Marko

Abstract

The Bachelor's thesis was assigned by Jyväskylä Security Technology (JYVSECTEC) project which operates in the JAMK University of Applied Sciences (JAMK) environment. JYVSECTEC develops and maintains closed cyber security infrastructure for research, development and training-services. Goal of the thesis was to create identity-based network solution by using components of Cisco Trusted Security (TrustSec). Thesis conducted from design, testing- and verifying parts along with creating a manual for future use.

The network environment in the thesis included TrustSec-capable devices manufactured by Cisco Systems, among others C3750X and C3560X switches, ASA-5515X firewall and WLC 2504. The main component was Cisco Identity services Engine (ISE) which was used to handle mainly policies in terms of authentication and authorization in network. The environment utilized SGA architecture which included authenticating network devices with NDAC procedure, handling traffic with SGT/SXP and testing firewall SGFW feature. The endpoints were authenticated with 802.1X protocol by using EAP-FAST chaining method. After authentication the L2 link between endpoint and switch was secured with 802.1AE (MACsec) protocol. The same encryption was also used between switches.

The result of the thesis is a network environment including several TrustSec components. The solutions and features were tested and verified. In future the environment will be used in training services and further development.

Keywords
TrustSec, ISE, 802.1X, SGA, NDAC, SGT, SXP, MACsec

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AD	Active Directory
AES-GCM	Advanced Encryption Standard - Galois Counter Mode
ASA	Adaptive Security Appliance
CTS	Cisco TrustSec
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAP-FAST	EAP- Flexible Authentication via Secure Tunneling
FTP	File Transfer Protocol
ISE	Identity Services Engine
MAB	MAC Authentication Bypass
MACsec	Media Access Control Security
MKA	MACSec Key Agreement
NAM	Network Access Manager
NDAC	Network Device Admission Control
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial In User Service
RGCE	Realistic Global Cyber Environment
PAC	Protected Access Credential
SAP	Security Association Protocol
SGA	Security Group Access
SGT	Security Group Tag
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SXP	SGT Exchange Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Työn lähtökohdat

1.1 Tehtävä ja tausta

Tietoverkot ja niiden monimutkaisuus ovat kasvaneet viime vuosikymmenen aikana räjähdysmäisesti. Tämä on luonnollisesti vaikuttanut siihen, että myös tietoturvan tarve on kasvanut kaiken muun ohella. Erilaisia hyökkäystapoja on lukuisia ja varsinkin sisäverkkojen tietoturvan toteuttaminen sekä ylläpitäminen on nykyaikana vaatinut eri yrityksiltä ja organisaatioilta paljon ammattitaitoa ja päänvaivaa. Aiemmin työntekijät saattoivat istua vakituisen tietokoneen eteen työpäiväksi, mutta nykyään tilanne on täysin toisenlainen. Käytössä on työntekijöiden omia laitteita tableteista älypuhelimiin, mikä on muuttanut merkittävästi vaatimuksia tietoturvan suunnittelussa yrityksissä.

Keräämällä tietoa verkosta käyttäjien ja laitteiden osalta, voidaan verkkoon luoda identiteettipohjainen tietoturva-arkkitehtuuri. Kyseisen menetelmän avulla mahdollistetaan mm. se, että laitteet ja käyttäjät tunnistetaan pelkän IP-osoitteiden sijasta niiden identiteetin perusteella. Uudet tekniikat pyrkivät tuomaan verkkoon lisää tietoisuutta ja yksinkertaisuutta parantaen samalla tietoturvaa. Opinnäytetyön tarkoituksena oli tutustua Cisco Systems:in ratkaisuun nimeltä Cisco TrustSec.

Työssä pyrittiin paneutumaan pääsääntöisesti käyttäjien ja laitteiden autentikointiin ja valtuuttamiseen käyttäen hyväksi TrustSec-ratkaisun menetelmiä. Työ koostui suunnitteluosasta, toteutuksesta sekä testaamisesta ja ohjeen luomisesta ympäristöä tulevaisuudessa käyttäville.

1.2 JAMK ja tietotekniikan koulutusohjelma

Jyväskylän Ammattikorkeakoulu (JAMK) on vetovoimainen ja kansainvälinen korkeakoulu, jonka toimipisteet sijaitsevat Jyväskylän eri puolilla ja Saarijärven Tarvaalassa. JAMK tarjoaa perinteisen korkeakoulututkinnon lisäksi mm. ammatillista opettaja-

koulutusta, avoimia ammattikorkeakouluopintoja ja täydennyskoulutusta. Tällä hetkellä opiskelijoita on 8500, jotka jakautuvat usean eri koulutusalan kesken. (Tutustu JAMKiin 2013.)

Tietotekniikan koulutusohjelma (Insinööri/AMK) on keskittynyt tietoverkkojen osa-alueelle. 240 opintopisteen laajuinen koulutus pitää sisällään mm. laajakaista, ja eri operaattoritason teknologioita. (Opintojaksot, 2010). Opinnoissa keskitytään myös verkkojen suunnitteluun ja ylläpitoon, sekä toteuttamaan tietoverkkojen palveluita uusia tekniikoita hyväksikäyttäen. (Tietotekniikan koulutusohjelma 2010.)

Opinnot koulutusohjelmassa jakautuvat perusopintoihin (100 op), ammattiopintoihin (80 op), vapaasti valittaviin opintoihin (15 op), harjoitteluun (30 op) ja opinnäytetyöhön (15 op). Pääasiassa opinnot koostuvat luennoista, tenteistä ja ryhmätyötehtävistä nykyaikaisissa laiteympäristöissä. (Tietotekniikan koulutusohjelma 2010.)

1.3 JYVSECTEC

JYVSECTEC on Jyväskylän ammattikorkeakoulun tiloissa toimiva kyberturvallisuusteknologian kehittämishanke, joka mm. kehittää ja ylläpitää kyberturvallisuuden kehitysympäristöä nimeltä RGCE (Realistic Global Cyber Environment). RGCE:n avulla voidaan mallintaa suljetussa ympäristössä oikean maailman verkkoympäristöä siihen kuuluvine palveluineen. Tämä verkko koostuu niin fyysisistä - kuin virtuaalisista laitteista ja alustoista, joiden tarkoituksena on mallintaa oikean internetin toimintaa. (JYVSECTEC-RGCE 2014.)

Hankkeen tarkoituksena on tuottaa erilaisia kehitys-, testaus ja koulutuspalveluita yhteistyöverkoston käyttöön. Toiminta sisältää mm. verkottunutta yhteistoimintaa, koulutusta ja erilaista palvelutoimintaa ja näiden yhdistämisen yhdeksi kokonaisuudeksi. (JYVSECTEC 2014.)

JYVSECTEC 2011-2013 -projekti alkoi syyskuussa 2011. Projektin tavoitteena on olla Suomen johtavimpia kyberturvallisuuden kehittämis- ja koulutuskeskuksista ja luoda Keski-Suomeen yhteistyöverkosto turvallisuusalan yritysten, sekä toimijoiden käyt-

töön. Projektin toteuttamisella pyritään edistämään mm. yritysten turvallisuuden tietämystä, riskien hallintaa sekä parantamaan turvallisuuden ylläpitoa. (JYVSECTEC 2014.)

Osarahoittajina projektissa toimivat Keski-Suomen Liitto ja Euroopan aluekehitysrahasto. Rahoitusta projektille on päätetty jatkaa kesään 2014 saakka. Yhteistyökumppaneille JYVSECTEC tarjoaa erilaisia verkostoitumismahdollisuuksia kansallisten ja kansainvälisten toimijoiden kanssa sekä lisää tietoisuutta Keski-Suomen kybertoimiala-mahdollisuuksista. (JYVSECTEC 2014.)

1.4 Tavoitteet ja toimeksianto

Opinnäytetyön tavoitteena oli luoda Cisco TrustSec-tietoturva-ratkaisu JYVSECTEC-ympäristöön. Tarkoituksena oli, että työn valmistuttua kasassa olisi identiteettipohjainen tietoturva-arkkitehtuuri, jossa käytettäisiin hyväksi edellä mainitun Cisco TrustSec-ratkaisun komponentteja ja menetelmiä.

Toimeksianto oli melko vapaamuotoinen, joka tarkoitti sitä, että käytetyt menetelmät olivat pääsääntöisesti opinnäytetyön tekijän suunnitelmassa esitettyjä ja hyväksytettyjä. Pyydettyjä ominaisuuksia työhön kuitenkin tuli myös. Näitä olivat mm. MACSec-salauksen toteuttaminen L2-tasolla ja erilaisten käyttäjäkohtaisten tilanteiden (*Use Case*) miettiminen ja toteuttaminen. Näiden osalta tuli miettiä muun muassa miten yrityksen työntekijän pääsyä hallitaan ja kontrolloidaan, kun

- Työntekijä kirjautuu yrityksen hallitsemalla työasemalla kiinteään verkkoon
- Työntekijä kirjautuu yrityksen hallitsemalla työasemalla langattomaan verkkoon (WLAN)
- Yrityksen työntekijä kirjautuu omalla laitteellaan (esim. puhelin tai tablet)
- Yrityksen työntekijä kirjautuu verkkoon VPN-yhteyden kautta.

Ympäristössä tuli suorittaa myös erilaisia testauksia ominaisuuksien toimivuuden todentamiseksi. Testaukset olivat pääsääntöisesti kirjautumisia eri tavoilla verkkoon ja sen seurauksena määritettyjen oikeuksien todentamista.

Työ toteutettiin verkkoympäristöön, jonka pohja oli rakennettu työharjoittelun aikana kesällä 2013. Ympäristöä muutettiin hieman aikaisemmasta kuitenkaan puuttumatta pohjan perusratkaisuun. TrustSec-ominaisuuksia varten verkkoon lisättiin myös uusia laitteita, jotta ympäristöstä saataisiin mahdollisimman kattava erilaisia tilanteita silmällä pitäen.

Henkilökohtaisina tavoitteina oli kasvattaa omaa tietämystä nykyaikaisista tietoturvaratkaisuista sekä kehittää jo opittuja taitoja. Lähtökohdat kokemuksen suhteen TrustSec-ratkaisuun liittyen olivat erittäin minimaaliset, joten henkilökohtaisella tasolla lähes kaikki tuli uutena asiana.

2 Tunnistautuminen tiedonsiirtoverkoissa

2.1 AAA

AAA on arkkitehtuurimalli, jota käytetään hyväksi tietoverkkojen tietoturvassa. Se koostuu kolmesta erillisestä osasta, joita ovat autentikointi (authentication), valtuutus (authorization) ja tilastointi (accounting). AAA-malli on itsessään vain prosessi, jonka tarkoituksena on todentaa kuka olet, mitä pystyt tekemään ja mitä teit tuona aikana. (Carrol, Banga & Santuka 2011.)

Yleisesti käytettyjä protokollia AAA-arkkitehtuurimallissa ovat Remote Authentication Dial-In User Service (RADIUS) ja Terminal Access Controller Access Control System Plus (TACACS+). Suurin ero RADIUS- ja TACACS+ -protokollan välillä on se, että RADIUS ei erittele autentikointi- ja valtuutusprosesseja erillisiksi toiminnoiksi, vaan hoitaa ne samanaikaisesti. Tilastointi on kuitenkin RADIUS-protokollassa myös erillinen prosessi. (Carrol, Banga & Santuka 2011.)

Authentication

Autentikoinnin (authentication) tarkoituksena on tunnistaa käyttäjä tai laite. Arkielämässä on myös monia tilanteita, joilla autentikointia voidaan kuvata. Esimerkkinä on tilanne, jossa henkilö on menossa elokuviin. Ovella henkilön on esitettävä pääsylippu päästäkseen sisällä. Tässä tilanteessa henkilö autentikoidaan perustuen siihen, mitä hän omistaa. Tietoverkkomaailmassa vastaavanlainen tapahtuma olisi esimerkiksi tilanne, jossa verkkoon pääsyä varten tarvittaisiin erillinen asiakassertifikaatti. (Carrol, Banga & Santuka 2011.)

Toinen arkielämän tilanne on, jossa henkilö on menossa tilaisuuteen, johon päästäkseen hänen tulee esittää salasana. Tällä kertaa autentikointi perustuu siihen, mitä henkilö tietää. Kyseinen esimerkki on rinnastettavissa tilanteeseen, jossa henkilö haluaa kirjautua verkon reitittimeen Secure Shell (SSH)-protokolla. Päästäkseen sisään

tulee hänen syöttää kirjautumisikkunaan oikea käyttäjätunnus/salasanapari. (Carrol, Banga & Santuka 2011.)

Verkkomaailmassa tilanne autentikoinnin suhteen voi käydä monimutkaiseksi, sillä laitteille, esim. kytkimille, tulee kertoa täsmälleen, mitä tehdä. Yhteensopivuus ongelmiakin voi esiintyä esimerkiksi erilaisten protokollien kanssa, ja jopa pienetkin ”väärinymmärrykset” voivat aiheuttaa sen, ettei autentikointiprosessi toimi oikealla tavalla tai ei ollenkaan. (Geier 2008.)

Autentikointi voi siis perustua siihen, mitä omistat, mitä tiedät tai mitä olet. Verkkomaailmassa autentikointitapahtuma tapahtuu yleensä ennen, kuin käyttäjälle sallitaan pääsy verkon resursseihin. (Carrol, Banga & Santuka 2011.)

Authorization

Valtuuttamisella (Authorization) tarkoitetaan menetelmää, jolla henkilölle tai laitteelle jaetaan tiettyjä oikeuksia perustuen autentikoinnin tulokseen. Arkielämässä valtuuttaminen voidaan kuvata tilanteena, jossa henkilö astuu lentokoneeseen näytettyään virkailijalle tarvittavat henkilötiedot. Koneessa olisi ensimmäisen luokan paikkoja, joissa on paremmat oltavat, mutta henkilön lippu oikeuttaa vain huonoimmille paikoille. Henkilöllä ei ole siis valtuuksia kyseisiin paikkoihin. (Carrol, Banga & Santuka 2011.)

Verkkomaailmaan yhdistettynä valtuuttaminen on menetelmä taata käyttäjälle tiettyjä oikeuksia pyytämiinsä palveluihin. Esimerkkinä on tilanne, jossa yrityksen laskutusosaston henkilö kirjautuu verkkoon ja häneltä pyydetään käyttäjätunnus sekä salasana. Tässä vaiheessa käytössä on kuitenkin ollut vasta autentikointiprosessi. Tämän jälkeen henkilö pääsee kirjautumaan ainoastaan laskutusosaston palvelimille. Tämä vaihe käsittelee siis valtuutusosiota. (Geier 2008.) Huomioitavaa on myös, että käyttäjä tulee autentikoida, ennen kuin voidaan määritellä se, mitä käyttäjä valtuutetaan tekemään (Carrol, Banga & Santuka 2011.).

Accounting

Tilastoinnin tarkoituksena on kerätä tietoa siitä, mitä autentikoitu teki autentikoinnin jälkeen. Viitaten valtuuttamisosion lentokone esimerkkiin henkilöstä tilastoitiin tietoa hänen astuessaan koneeseen ja näyttäessään lentolippunsa tarkastajalle. Tarkastaja skannaa lipun, ja tämän jälkeen on tilastoitu, että kyseinen henkilö on astunut koneeseen. (Carrol, Banga & Santuka 2011.)

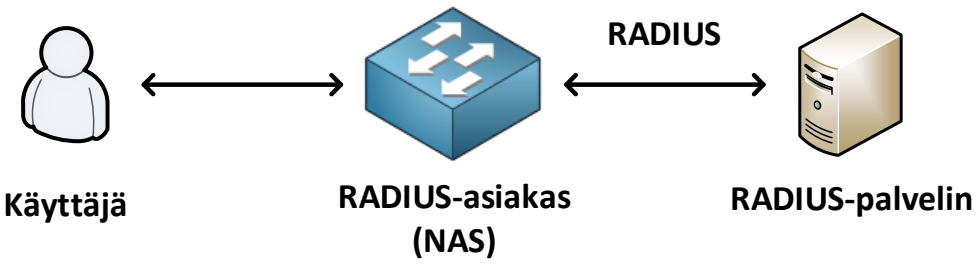
AAA:n tilastoinnin avulla voidaan kerätä monenlaista tietoa verkkomaailmassa. Tällaisia tietoja ovat mm. yhteyden kesto, siirretyn datan määrä, käytetty yhteys jne. Kerättyä tietoa voidaan syöttää esimerkiksi erilaisiin monitorointityökaluihin ja säilöä moniin eri paikkoihin. Näitä tietoja voidaan käyttää esimerkiksi tilanteessa, jossa asiakkaita laskutetaan käytetyn yhteysajan tai käytettyjen resurssien mukaan. (Carrol, Banga & Santuka 2011.)

2.2 RADIUS

2.2.1 Yleistä ja komponentit

Remote Authentication Dial-In User Service (RADIUS) on Internet Engineering Task Forcen (IETF) määrittelemä standardi, joka tukee kaikkia AAA-arkkitehtuurin komponentteja. Protokollan autentikointia ja valtuutusta varten on virallisesti määritetty portti 1812 (IETF RFC 2865, 2000, 1) sekä tilastointia varten portti 1813 (IETF RFC 2866, 2000, 1). RADIUS- protokollan autentikointi- ja valtuutusosiot on määritelty IETF:n standardissa RFC 2865 ja tilastointi standardissa RFC 2866 (Carrol, Banga & Santuka 2011).

RADIUS toimii asiakas-palvelin -periaatteen mukaisesti (IETF RFC 2866, 2000 1). Kuviossa 1 on havainnollistettu RADIUS-protokollassa toimivat komponentit ja niiden kytkeytyminen toisiinsa.



Kuvio 1. RADIUS-komponentit

Asiakkaana RADIUS-protokollassa toimii Network Access Server (NAS)-laite, joka vastaa käyttäjätietojen välittämisestä RADIUS-palvelimelle (IETF RFC 2865, 2000, 3). NAS on laite, joka hallitsee edes jollain tasolla pääsyä suurempaan verkkoon. Tyypillisesti tällainen laite on langattoman verkon liityntäpiste tai verkon liityntätasolla toimiva 802.1X-protokollaa tukeva kytkin. Huomioitavaa on, että RADIUS-asiakas ei ole esimerkiksi normaali asiakastietokone. RADIUS-asiakkaana voi olla myös erillinen RADIUS-proxy, joka keskustelee erillisen RADIUS-autentikointipalvelimen kanssa toimien asiakasroolissa. (RADIUS-Client 2012).

RADIUS- palvelimen tehtävänä on vastaanottaa RADIUS-pyyntöjä, autentikoida käyttäjä ja palauttaa RADIUS-asiakkaalle tarvittavat parametrit, jotta käyttäjälle voidaan sallia tarvittavat palvelut. Joustavuutta protokolla tuo palvelimen kohdalla siinä, että itse palvelin tukee monia erilaisia autentikointi-mekanismeja ja uusia ominaisuuksia voidaan lisätä häiritsemättä olemassa olevaa toteutusta. (IETF RFC 2865, 2000, 4).

RADIUS-asiakas ja palvelin autentikoituvat keskenään käyttäen hyväksi jaettua salaisuutta. Tätä kyseistä salaisuutta ei lähetetä koskaan verkon yli. Muita tietoturvaominaisuuksia ovat mm. se, että kaikki käyttäjän syöttämät salasanat salataan asiakkaan ja palvelimen välillä. Tällä pyritään estämään se, ettei turvattomassa verkkoympäristössä pystytä esimerkiksi monitoroimaan käyttäjien salasanoja. (IETF RFC 2865, 2000, 4).

RADIUS käyttää kuljetusprotokollanaan UDP:tä TCP:n sijaan. UDP on valittu puhtaasti teknillisistä syistä, ja tämän selventämiseksi on hyvä ymmärtää seuraavia seikkoja. UDP:n käyttö vaatii kuitenkin yhtä toiminnallisuutta, joka on rakennettu TCP:hen valmiiksi. Tämä toiminnallisuus on uudelleenlähetysajastimen käyttö samalle palve-

limelle, jota joudutaan hallinnoimaan keinotekoisesti UDP:n kanssa. Tämä on kuitenkin vain pieni ongelma verrattuna UDP:n tuomiin hyötyihin protokollan kanssa. (IETF RFC 2865, 2000, 10-11.)

2.2.2 RADIUS-pakettityypit

RADIUS-paketti enkapsuloidaan UDP-paketin data-osioon. Huomioitavaa on, että RADIUS-paketteja voidaan sisällyttää ainoastaan yksi jokaisen UDP-paketin data-kenttää kohti. (IETF RFC 2865, 2000, 13.)

Kuviossa 2 on esitetty RADIUS-paketin rakenne.

Kuvio 2. RADIUS-paketti

Paketin alussa oleva *Code*-kentän pituus on yksi oktetti (8 bittiä). Kyseinen kenttä ilmoittaa minkä tyyppisestä RADIUS-viestistä on kyse(IETF RFC 2865, 2000, 14). Taulukossa 1 on esitetty *Code*-kentän arvot desimaalimuodossa sekä niitä vastaavat viestityypit.

Taulukko 1. RADIUS-paketit

CODE-KENTÄN ARVO	**PAKETTITYYPPI**
1	RADIUS-Access-Request
2	RADIUS-Access-Accept
3	RADIUS-Access-Reject
4	RADIUS-Accounting-Request
5	RADIUS-Accounting-Response
11	RADIUS-Access-Challenge
12	Status-Server (kokeellinen)
13	Status Client (kokeellinen)
255	Reserved

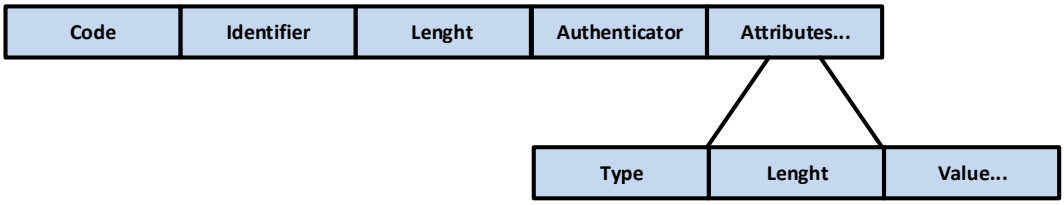
Jos *Code*-kentän arvona on jokin muu kuin taulukossa 1 listattuna olevat arvot, tulee paketti tiputtaa ilman muita toimenpiteitä (IETF RFC 2865, 2000, 14).

Seuraavana RADIUS-paketissa oleva oktetin pituinen *Identifier*-kenttä on tarkoitettu pyyntö- ja vastausviestien yhteensovitukseen keskenään. Kyseinen kenttä mahdollistaa myös päällekkäisten pyyntö-viestien huomaamisen RADIUS-palvelimella. Tämä perustuu siihen, että palvelin huomaa asiakkaalta tulevan pyyntö-paketteja (Access-Request) lyhyen ajan sisään, joissa on sama lähde-IP-osoite, lähde-UDP-portti sekä *Identifier*-kentän arvo. (IETF RFC 2865, 2000, 14.)

Kahden oktetin pituinen *Length*-kenttä ilmaisee nimensä mukaisesti paketin pituuden. Kyseisessä arvossa ovat mukana kentät *Code*, *Identifier*, *Length*, *Authenticator* ja *Attributes*. Oktetit, jotka eivät kuulu *Length*-kentässä määriteltyyn arvoon, tulee kohdella ns. täytebitteinä ja jättää huomioimatta. Huomioitavaa on myös tilanne, jossa paketti on lyhyempi kuin *Length*-kentässä ilmoitettu arvo. Tällaisessa tilanteessa paketti tulee tiputtaa ilman muita toimenpiteitä. (IETF RFC 2865, 2000, 15.)

Authenticator-kenttä on 16 oktetin pituinen, ja sitä käytetään autentikoimaan RADIUS-palvelimen vastausviesti. Kentän tiedot lähetetään eniten merkitsevä oktetti ensin. *Authenticator*-kenttiä on kahdenlaisia ja niiden sisältö riippuu käytetystä RADIUS-pakettityypistä. (IETF RFC 2865, 2000, 15-16.)

Attributes-kenttä sisältää tietoa autentikointiin, valtuuttamiseen ja erilaisiin konfiguraatioihin liittyen pyyntö- ja vastauspaketeissa (IETF RFC 2865, 2000, 22). Yksittäisen *Attribute*-kentän sisältö ja sen kytkeytyminen RADIUS-pakettiin on esitetty kuviossa 3.



Kuvio 3. TLV-kenttä RADIUS-paketissa

Attribuutit on sisällytetty RADIUS-pakettiin TLV (Type Lenght Value)-muodoissa. *Type* -kenttä ilmaisee sen, minkälaisesta attribuutista on kyse. Attribuuttityyppejä ovat mm. ”*User-Name*”, ”*User Password*” ja ”*NAS-IP-Address*”, joille kullekin on määritelty omat arvot (IETF RFC 2865 2000, 23 -24). Yleisesti käytetty attribuutti on myös *Vendor Specific Attribute* (VSA). Tämä attribuutti mahdollistaa valmistajakohtaisten laajennettujen attribuuttien käytön, jotka eivät ole yleisesti määriteltyjä. Kyseisten valmistajakohtaisten attribuuttien käyttö ei saa vaikuttaa RADIUS-protokollan yleiseen toimintaan (IETF RFC 2865, 2000, 47).

Seuraavana oleva oktetin pituinen *Length*-kenttä määrittelee yksittäisen attribuutin pituuden ja koostuu TLV-kentän arvojen yhteenlasketusta pituudesta (IETF RFC 2865, 2000, 25).

Value-kenttä on 0 tai useamman oktetin pituinen ja sisältää attribuuttikohtaista tietoa. Kyseisen kentän pituus ja muoto määräytyy edellä olevien *Type*- ja *Length*-kenttien arvojen mukaan. Itse arvo kentässä voi olla yksi viidestä eri tyypistä, jotka ovat *”text”, ”string”, ”address”, ”integer” tai ”time”.* (IETF RFC 2865, 2000, 25.)

Access-Request-paketti

Access-Request-paketit lähetetään RADIUS-palvelimelle ja ne sisältävät tietoa, josta määritellään onko käyttäjällä oikeus päästä tiettyyn RADIUS-asiakaslaitteeseen. Samaan viestiin myös sisällytetään tiedot mahdollisista palveluista, joihin käyttäjä pyytää pääsyä. (IETF RFC 2865, 2000, 47). Kuviossa 4 on esitetty RADIUS-Access-Request-paketin sisältö.

Kuvio 4. RADIUS-Access-Request

Access-Request-paketit lähetetään aina *Code*-kentän arvolla 1 taulukon 1 mukaisesti. Paketin *Authenticator*-kenttä on nimeltään Request-Authenticator. Kyseinen kenttä on 16 oktettia pitkä sattumanvarainen numero. Asiakkaan ja RADIUS-palvelimen kanssa jaettu salaisuus, sekä Request-Authenticator-kentän arvo ajetaan MD5-

tiivistealgoritmin läpi. Tähän tiivisteeseen käytetään XOR-loogista operaatiota käyttäjän syöttämällä salasanalla. Arvo syötetään tämän jälkeen *"User-Password"*-attribuuttiin Access-Request-paketissa. (IETF RFC 2865, 2000, 14.)

Access-Accept/Access-Challenge/Access-Reject-paketti

Kuviossa 5 on esitetty Access-Accept/Access-Challenge/Access-Reject-pakettien rakenne.

Kuvio 5. Access-Accept -, Access-Reject- tai Access Challenge -paketti

Access-Accept-, Access-Reject- ja Access-Challenge –paketeissa olevan *Authenticator*-kentän arvoa kutsutaan nimellä *Response-Authenticator*. Se sisältää MD5-tiivisteen asiakkaalta saadusta RADIUS-Access-Request-paketista. MD5-tiiviste muodostetaan Access-Request-paketin neljästä ensimmäisestä kentästä, vastauksena lähetettävistä attribuuteista, sekä jaetusta salaisuudesta eli

MD5 (Code + ID + Length + RequestAuth + Attributes + jaettu salaisuus)

Access-Accept-paketit lähetetään RADIUS-palvelimen toimesta ja niiden tarkoitus on ilmoittaa erityisistä konfiguraatioista, jotta käyttäjälle voidaan taata haluttua palvelua. RADIUS-palvelimen tulee lähettää Access-Accept-viesti jos attribuutit Access-Request-viestissä ovat hyväksyttäviä. RADIUS-Access-Accept -viestit lähetetään aina *Code*-kentän arvolla 2 taulukon 1 mukaisesti. (IETF RFC 2865, 2000, 18.)

RADIUS-palvelimen tulee lähettää Access-Reject-viesti, jos mikään saaduista attribuuteista ei ole hyväksyttävä. Access-Reject-viestit lähetetään aina *Code*-kentän arvolla 3 taulukon 1 mukaisesti. (IETF RFC 2865, 2000, 20.)

Halutessaan RADIUS-palvelin voi lähettää käyttäjälle haasteen *(challenge)* vastauksena Access-Request-pakettiin saadakseen lisää tietoa käyttäjästä. Tällaisessa tilanteessa palvelin lähettää Access-Challenge-paketin, jonka *Code*-kentän arvo on 11 taulukon 1 mukaan. Asiakkaan kanssa voi tulla tilanne, jossa laite ei tue *challen-*

ge/response–menetelmää. Tällaisessa tilanteessa asiakas kohtelee Access-Challenge-pakettia kuin olisi saanut Access-Reject-paketin. (IETF RFC 2865, 2000, 21.)

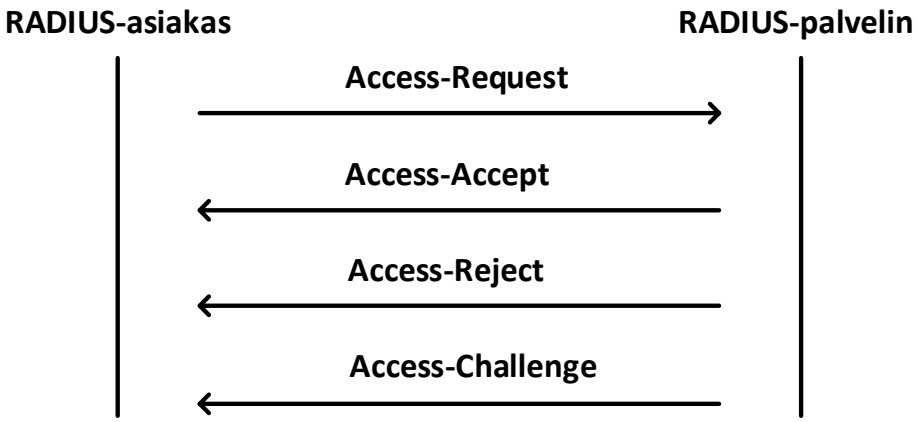
Accounting-Request ja Accounting-Response-paketti

RADIUS-Accounting(tilastointi)-Request- ja RADIUS-Accounting-Response paketit ovat rakenteeltaan samanlaisia, kuin aiemmin kuvioissa 4 ja 5 esitetyt Request- ja Response-paketit.

Accounting-Request lähetetään muodossa, jossa *Code*-kenttään on asetettu arvo 4. Kyseinen paketti sisältää tietoa käyttäjälle tarjotusta palvelusta ja se lähetetään RADIUS-tilastointipalvelimelle. (IETF RFC 2866 2000, 8). Accounting-Response-paketti lähetetään aina *Code*-kentän arvolla 5, ja sen tarkoitus on vastata vastaanotettuun Request-pakettiin. (RFC 2866 2000, 9). RADIUS-tilastointipakettien tyypillisin attribuutti on*"Acct-Status-Type"*, joka ilmaisee käyttäjälle myönnetyn palvelun alkamis - ja/tai loppumiskohdan (Start/Stop). (IETF RFC 2866, 2000, 12).

2.2.3 RADIUS-Autentikoinnin- ja valtuuttamisen toimintaperiaate

RADIUS-autentikointi- ja valtuuttaminen on esitelty seuraavaksi. Kuviossa 6 on esitetty viestien kulkusuunta RADIUS-asiakkaan- ja palvelimen välillä autentikoinnin kohdalla:



Kuvio 6. RADIUS-viestit

RADIUS-prosessi alkaa tilanteesta, kun asiakas(NAS) on konfiguroitu käyttämään RADIUS-protokollaa. Tämän jälkeen kaikki käyttäjät voivat esittää autentikointiin liitty-

viä tietoja asiakkaalle. Tiedot, esimerkiksi käyttäjätunnus ja salasana, voidaan syöttää käyttäjälle näkyvässä sisäänkirjautumisruudussa. Huomioitavaa on, että autentikointiin liittyvät tiedot voivat siirtyä myös monella muulla tavalla asiakkaalle (IETF RFC 2865, 2000, 5).

Seuraavaksi asiakas voi autentikoida halutessaan käyttäjän käyttäen saatuja kirjautumistietoja hyväkseen. Tehdäkseen niin, tulee asiakkaan luoda Access-Request–viesti, jonka sisällä ovat juuri käyttäjän syöttämät autentikointiin liittyvät tiedot erillisissä attribuuteissa (IETF RFC 2865, 2000, 5).

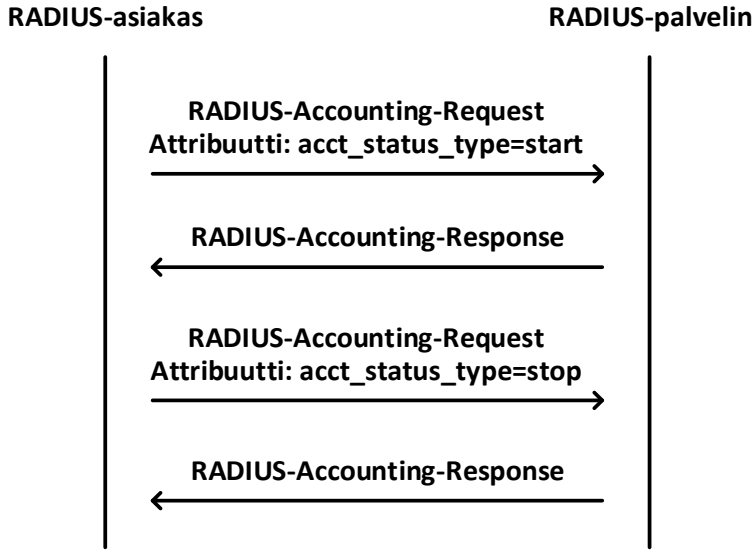
Access-Request- paketti lähetetään verkon yli RADIUS-palvelimelle. Paketteja lähetetään uudestaan tietyn määrän verran, jos vastausta RADIUS-palvelimelta ei tule tietyn ajan kuluessa. Vaihtoehtoisesti asiakas voi välittää Access-Request-paketin vaihtoehtoiselle palvelimelle, jos vastausta ensisijaiselta palvelimelta ei tule. RADIUS-palvelin tutkii paketin saatuaan lähettäjän, eli asiakkaan tiedot, ja tarkistaa sen oikeellisuuden. Paketit, jotka tulevat asiakkailta joiden kanssa RADIUS-palvelimella ei ole samaa jaettua salaisuutta, tulee tiputtaa pois ilman muita toimenpiteitä. Jos asiakkaan oikeellisuus voidaan taata, tutkii RADIUS-palvelin tämän jälkeen määritetystä tietokannasta vastaavuutta Access-Request–paketissa olevalle käyttäjänimelle. Tietokannassa käyttäjänimeen on yhdistettynä tiettyjä vaatimuksia, joiden pitää täyttyä, jotta käyttäjälle voitaisiin sallia pääsy palveluun. Vaatimuksina voivat olla salasanan lisäksi esimerkiksi tietyt asiakaslaitteet tai portit, joihin käyttäjillä on pääsy sallittu. (IETF RFC 2865, 2000, 6.)

RADIUS-palvelin lähettää asiakkaalle Access-Reject-paketin, jos vaaditut vaatimukset eivät täyty. Viestin tarkoitus on ilmaista asiakkaalle, että pyyntö oli viallinen. Halutessaan palvelin voi sisällyttää Access-Reject–pakettiin tekstipohjaisen viestin attribuuttina. Mitään muita attribuutteja, lukuunottamatta Proxy-State, ei lähetetä kyseisessä viestissä asiakkaalle päin. (IETF RFC 2865, 2000, 6.)

Access-Accept- paketti lähetetään asiakkaalle RADIUS-palvelimen toimesta, jos kaikki vaatimukset täyttyvät. Tähän pakettiin liitetään lista konfiguraatioista, joita käyttäjä tarvitsee päästäkseen käsiksi haluttuun palveluun (IETF RFC 2865, 2000, 7.)

2.2.4 RADIUS- Tilastoinnin toimintaperiaate

RADIUS-Tilastointi (RADIUS-Accounting) toimii autentikoinnin tapaan asiakas/palvelin-periaatteen mukaisesti. Tilastoinnin tarkoituksena on kerätä tietoa autentikoinnissa muodostettavasta istunnosta. Tällaisia tietoja voivat olla esimerkiksi käytetty aika, lähetetty pakettien määrä jne. (Carrol, Banga & Santuka 2011). Kuviossa 7 on esitettytyypillinen tilanne RADIUS-tilastoinnin toiminnasta, sekä viestien kulkusuunta:



Kuvio 7. RADIUS-tilastoinnin viestit

Tilastointi alkaa asiakkaan, yleisesti NAS-laiteen tai sen välityspalvelimen, toimesta. Asiakas lähettää Accounting-Request–paketin tilastointipalvelimelle, johon on sisällytettynä tietoa käyttäjälle toimitetusta palvelusta. Palvelin lähettää vastauksena Accounting-Response–paketin, jos se pystyy onnistuneesti tallentamaan Accounting-Request – paketin sisältämät tiedot. (IETF RFC 2866, 2000, 8). Attribuutteina voidaan käyttää esimerkiksi *Acct-Status-Type*–attribuuttia. Tällä attribuutilla merkataan tietty Accounting-Request–paketti ilmoittamaan esimerkiksi käyttäjän palvelun alkamisesta (*start)* tai loppumisesta *(end).* (IETF RFC 2866, 2000, 12). Kuvion 7 mukaan RADIUS-palvelin vastaa *stop*-viestiin Accounting-Response-viestillä hyväksymisen merkiksi.

2.3 802.1X

2.3.1 Yleistä

IEEE:n standardoima 802.1X, eli porttikohtainen todentaminen, on suunniteltu hallitsemaan verkkoon pääsyä langallisissa ja langattomissa lähiverkoissa. Protokollan avulla pystytään mm. estämään ja sallimaan käyttäjän tai laitteen kytkeytyminen verkkoon ja asettamaan liikennöintisääntöjä. Termi ”porttikohtainen todentaminen” tulee siitä, että laite tai käyttäjä tunnistetaan, ennen pääsyn sallimista verkon liityntäpisteen, eli portin kautta. (Carrol, Banga & Santuka 2011.)

Portit ovat porttikohtaisessa todentamisessa L2-tason (Siirtoyhteyskerros) yhteyksiä verkkoympäristöön. Langallisissa verkoissa sana ”portti” viittaa porttikohtaisessa todentamisessa kytkimen ethernet-porttiin. Langattomissa verkoissa (802.11) sana portti viittaa assosiaatioon langattoman verkon liityntäpisteen (Access point) kanssa. (Geier 2008.)

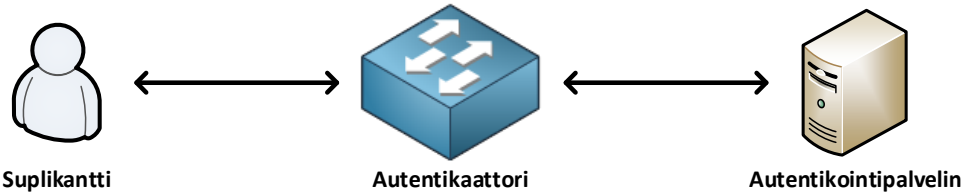
802.1X koostuu useasta eri protokollasta ja niiden yhteistoiminnasta, joita ovat mm. EAPOL, EAP, EAP-Methods ja RADIUS. Näitä kyseisiä protokollia standardoidaan myös eri organisaatioiden, kuten IEEE:n ja IETF:n toimesta. Tämä aiheuttaaa luonnollisesti monimutkaisuutta, sillä pelkän yksittäisen standardin ymmärtäminen ei kerro yhtään porttikohtaisen todennuksen kokonaismekanimista. Näiden protokollien ymmärtäminen on kuitenkin pakollista, sillä mikään yksittäinen standardi ei määrittele miten kaikki edellä mainitut protokollat toimivat yhdessä. (Geier, 2008.)

Käytännössä voidaan sanoa, 802.1X-protokolla on itsessään vain pieni osa porttikohtaista todentamisprosessia. Tarkemmin sanottuna, vain yksi protokolla on yhtä kuin 802.1X ja tämä on EAPOL (Brown 2007, 5.)

2.3.2 Komponentit

802.1X toimii asiakas-palvelin -periaatteen mukaisesti. Standardissa on määritelty, että 802.1X sisältää kolme komponenttia, joiden avulla verkkoon pääsyä hallitaan. Nämä komponentit ovat asiakas/suplikantti (Client/Supplicant), autentikaattori (Aut-

henticator) ja autentikointipalvelin (Authentication Server). Kuviossa 8 on esitetty komponenttien suhde toisiinsa.



Kuvio 8. 802.1X-komponentit

Asiakkaalla tai suplikantilla tarkoitetaan laitetta, joka pyrkii pääsemään langattomaan tai langalliseen lähiverkkoon. Tällaisen laitteen tulee sisältää erillinen asiakasohjelmisto, joka tukee 802.1X-protokollaa ja tietynlaisia EAP-Method:eja. Asiakaslaite voi olla esimerkiksi kiinteästi kytkimeen yhdistetty tietokone tai langattomasti WLAN-tukiasemaan yhdistyvä kannettava tietokone. (Geier 2008.)

Autentikaattori on L2-tason laite, esimerkiksi ethernet kytkin tai WLAN-liityntäpiste. Sen tehtävänä on toimia välittäjänä asiakaslaitteen ja autentikointipalvelimen välillä. Autentikaattori on lopulta se laite, joka avaa portin, jotta suplikantti pääsee liikennöimään verkkoon. (Geier 2008.)

Autentikointipalvelimen tehtävä on taata autentikointi-palvelu autentikaattorille. Tälläinen palvelu määrittää sen, onko asiakkaalla oikeutta päästä pyytämiinsä palveluihin. Huomionarvoista on myös se, että autentikointipalvelin ja autentikaattori voivat sijaita myös yhdessä ja samassa laitteessa.(IEEE 802.1X-2010, 6.)

Nämä edellämainitut komponentit käyttävät hyväkseen kolmea erilaista loogista keskustelua suplikantin, autentikaattorin ja autentikointipalvelimen välillä. Suplikantin ja autentikaattorin, sekä autentikaattorin ja autentikointipalvelimen välinen liikenne voidaan kuvata fyysisinä keskusteluina. Molemmat edellämainituista voidaan nähdä pakettikaappauksissa. Fyysiset keskustelut mahdollistavat keskustelun ja pääsynhallintaan liittyvien tietojen vaihtamisen suplikantin ja autentikointipalvelimen välillä. Tämä on täysin looginen keskustelu. Ideana on, että suplikantti voi keskustella aino-

astaan autentikaattorin kanssa ja autentikaattori toimii välikätenä autentikointipalvelimen ja suplikantin välillä. (Brown 2007, 4-5.)

2.3.3 EAP

EAP (Extensible Authentication Protocol) on eräänlainen viitekehys, jota käytetään hyväksi mm. 802.1X -autentikoinnissa. Sen avulla määritetään ainoastaan mekanismit, joita itse autentikoinnissa käytetään. Tällaisia mekanismeja ovat mm. käyttäjätunnus/salasana-parit, Kerberoksen ja sertifikaattien käyttö. (IEEE 802.1X-2010, 48). Käytännössä EAP mahdollistaa kahden laitteen välisen tiedonsiirron, jossa käydään läpi menetelmä, joita laitteet haluavat käyttää tunnistautumiseen. Tämä on yksi EAP-arkkitehtuurin vahvoja puolia, sillä se on joustava ja skaalautuva. Autentikaattoria ei tarvitse päivittää tukemaan erilaisia tai uusia autentikointitapoja, sillä ainoastaan suplikantti ja autentikointipalvelin voivat ottaa käyttöön eri autentikointitavan. (Carrol, Banga & Santuka 2011). Suunnittelussa on otettu huomioon myös se, että autentikaattori on erotettu autentikointipalvelimesta, jotta voitaisiin yksinkertaistaa tunnistustietojen hallintaa (IETF RFC 3748, 2004, 8).

EAP-paketti muodostuu neljästä eri osasta, jotka on esitetty kuviossa 9.

Kuvio 9. EAP-paketti

Yhden oktetin(8 bittiä) pituinen *Code* -kenttä on tarkoitettu EAP-paketin tunnistamiseen. (IETF RFC 3748, 2004, 20). Taulukossa 2 on listattu *Code*-kentän arvot desimaalimuodossa, sekä niitä vastaavat EAP-viestit.

Taulukko 2. EAP-pakettityypit

CODE-KENTÄN ARVO	PAKETTITYYPPI
1	EAP-Request
2	EAP-Response
3	EAP-Success
4	EAP-Failure

Seuraavana oleva yhden oktetin pituinen *Identifier*-kenttä on tarkoitettu täsmäämään oikeat pyyntö- ja vastausviestit keskenään. Kahden oktetin pituinen *Lenght*-kenttä sisältää tiedon paketin kokonaispituudesta. Viimeisenä oleva *Data*-kenttä on pituudeltaan 0 tai useampi oktetti ja sen sisältö määräytyy *Code*-kentässä olevan arvon mukaan. (IETF RFC 3748, 2004, 20.)

EAP-Request -ja Response-paketti

EAP-Request –pakettia käytetään lähettämään viesti autentikaattorilta suplikantille ja EAP-Response:a viestien lähettämiseen suplikantilta autentikaattorille (IETF RFC 3748, 2004, 20). Kuviossa 10 on esitetty kyseiset pakettityypit.

Kuvio 10. EAP-Request -ja Response-paketti

Code-kentän arvo on Request viesteissä 1 ja Response viesteissä 2 taulukon 2 mukaisesti. Yhden oktetin pituisen *Type*- kentän tarkoitus on ilmaista se minkä tyyppisestä Request- tai Response-viestistä on kyse. Kentän jälkeen tulee vaihtelevanmittainen *Data*-kenttä, jonka sisältö riippuu edellä olevan *Type*-kentän arvosta. (IETF RFC 3748, 2004, 22-23.)

EAP-Success ja EAP-Failure

Kuviossa 11 on esitetty EAP-Success ja EAP-Failure-paketit.

Kuvio 11. EAP-Success-ja EAP-Failure-paketti

EAP-Success–paketteja lähetetään autentikaattorin toimesta EAP-autentikoinnin jälkeen onnistumisen merkiksi *Code*-arvolla 3. Vastaavasti EAP-Failure paketteja lähetetään *Code*-arvolla 4 ilmoittamaan, että autentikointi epäonnistui. *Lenght*-kenttä on aina 4 oktetin mittainen. (IETF RFC 3748, 2004, 24-25.)

2.3.4 EAPOL

EAP-viestit itsessään eivät vielä määrittele, miten viestit välittyvät verkossa. Tätä varten on kehitetty erityinen protokolla, jolla EAP-viestit enkapsuloidaan verkossa. Tätä kyseistä protokollaa kutsutaan nimellä EAP over LAN (EAPOL) ja sen tärkeimpänä tehtävänä on saada EAP-viestit välitettyä juuri supplikantin ja autentikaattorin kesken. (Carrol, Banga & Santuka 2011.)

EAPOL-paketin rakenne on esitetty kuviossa 12.

Kuvio 12. EAPOL-paketti

Paketin alussa oleva yhden oktetin pituinen *Version*-kenttä ilmaisee sen, mikä EAPOL-protokollan versio paketin lähettäjällä on käytössään. Seuraavana vuorossa oleva oktetin pituinen *Type*-kenttä ilmaisee sen, minkätyyppisestä EAP-paketista on kyse. (IEEE 802.1X-2010, 90.) Taulukossa 3 on listattu käytössä olevat EAP-pakettityypit.

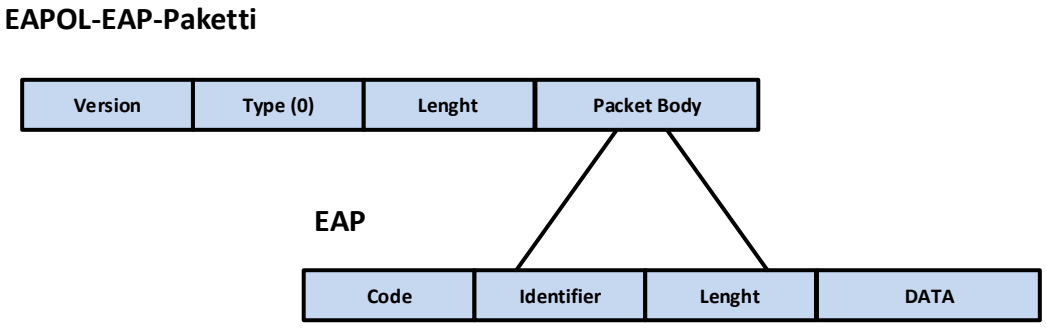
Taulukko 3. EAPOL-pakettityypit

TYPE-KENTÄN ARVO	PAKETTI-TYYPPI
0	EAPOL -EAP
1	EAPOL -Start
2	EAPOL -Logoff
3	EAPOL -Key
4	EAPOL -Encapsulated -ASF-Alert
5	EAPOL -MKA
6	EAPOL -Announcement (Generic)
7	EAPOL -Announcement (Specific)
8	EAPOL -Announcement-Req

Muita kuin taulukossa 3 esitettyjä *Type*-kentän arvoja ei tule käyttää, sillä ne ovat varattu tulevaisuudessa ilmestyviin laajennuksiin (IEEE 802.1X-2010, 90).

Seuraavana oleva *Length*-kenttä ilmaisee *Packet Body*-kentän pituuden. Kyseinen kenttä on kahden oktetin pituinen. Viimeisenä oleva *Packet Body*-kentän arvo ja pituus riippuu käytettävästä pakettityypistä. (IEEE 802.1X-2010, 91.)

Kuviossa 13 on esitetty yleisin EAPOL-paketti nimeltä EAPOL-EAP ja kuinka EAP on kytkeytynyt kyseiseen pakettiin.



Kuvio 13. EAP-paketti EAPOL-paketissa

Supplikantti voi käynnistää autentikoinnin halutessaan EAPOL-Start-viestillä, jotta sen ei tarvitse odottaa autentikaattorin lähettävän ensin EAP-Identity/Request-viestiä. EAPOL-Logoff-viestiä käytetään ilmoittamaan, että suplikantti on lopettanut verkon käytön ja portti voidaan palauttaa takaisin suljettuun tilaan. EAPOL-Key-viestejä käytetään erilaisten salausavainten vaihtamiseen. (IEEE 802.1X-2010, 91.)

2.3.5 EAP-Method

EAP itsessään on vain viitekehys autentikoinnissa eikä mikään tietty autentikointitapa. Se mahdollistaa kuitenkin erilaisten autentikointimenetelmien käytön. Näitä menetelmiä kutsutaan nimellä *EAP-Methods*. EAP Method:it tukevat monenlaisia autentikointityyppejä kuten mm. token card:eja, one-time-password:eja, sertifikaatteja ja PKI-menetelmiä. Nykypäivänä käytössä on monia standardoituja EAP-autentikointimenetelmiä kuten EAP-MD5, EAP-OTP, EAP-TLS, EAP-FAST ja myös valmistajakohtaisia ratkaisuja kuten PEAP ja EAP-TTLS. (Carrol, Banga & Santuka 2011.)

EAP-FAST

Extensible Authentication Protocol Flexible Authentication via Secure Tunneling (EAP-FAST) on EAP- menetelmä, joka mahdollistaa turvallisen tiedonsiirron peer-laitteen ja palvelimen välillä käyttäen hyväksi suojattua tunnelia. Suojatun tunnelin muodostamiseen käytetään hyväksi TLS (Transport Layer Security)- menetelmää. Kyseisen tunnelin sisällä voidaan käyttää erilaisia mahdollisesti heikoimpia autentikointitapoja, jotka voivat perustua esim. salasanoihin jne. (IETF-RFC 4851, 2007, 3-6.)

EAP-FAST:n suunnittelussa on pyritty huomioimaan mm. seuraavia seikkoja. EAP-palvelimen täytyy tunnistaa peer-laitteen aitous ja vastaavasti peer-laitteen täytyy tunnistaa EAP-palvelimen aitous. Protokolla estää myös liikenteen salakuuntelun autentikoinnin yhteydessä, sillä tunnistetiedot (esim. salasanat) lähetetään suojatun tunnelin sisällä. Tärkeitä piirteitä suunnittelussa olivat myös joustavuus ja suorituskyky. Joustavuus tarkoittaa EAP-FAST:issä sitä, että autentikoinnissa voidaan käyttää hyväksi monia eri tunnistautumistapoja, joista esimerkkeinä mainittakoon Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Lightweight Directory Access Protocol (LDAP) jne. (IETF RFC 4851, 2007, 3.)

EAP-FAST jakautuu käytännössä kahteen vaiheeseen jotka ovat

- Tunnelin muodostaminen (Phase 1)
- Tunneloitu autentikointi (Phase 2)

Ensimmäisessä vaiheessa palvelin käynnistää EAP-FAST-keskustelun EAP-FASt/Start-paketin muodossa. Tämän jälkeen laite vastaa ja keskustelee palvelimen kanssa käytettävästä versiosta ja TLS-tunnelin muodostamisesta. Tämä vaihe jatkuu siihen asti kunnes TLS-tunneli on täysin muodostettu. Tämän jälkeen siirrytään vaiheeseen kaksi, jossa itse autentikointi tapahtuu. Tämä tapahtuu välittömästi vaiheen 1 jälkeen. Tunnelin sisällä voi tapahtua nolla tai useampi EAP-Method-autentikointi. Esimerkiksi EAP-TLS:ää voidaan käyttää tunnelin sisällä kaksi kertaa autentikoiden ensin laitteen ja tämän jälkeen käyttäjän. Viimeisen viestin jälkeen tunneli puretaan, jonka jälkeen palvelin palauttaa selkokielisenä EAP-Success- tai EAP-Failure-viestin autentikointituloksen mukaan.(IETF RFC 4851, 2007, 9-13). Huomioitavaa on, että EAP-FAST:issa on myös ns. vaihe 0 (Phase 0), jolla tarkoitetaan tilannetta, jossa Protected Access Credential (PAC)-tiketti myönnetään supplikantille (TrustSec Arch Over 2012).

Protected Access Credential (PAC)

Protected Access Credential (PAC) –tikettiä käytetään muodostamaan suojattu TLS-tunneli (IETF-RFC 4851 2007, 11). PAC-tikettejä on erilaisia, joista yleisimmät ovat tunnelointia varten käytettävä PAC (Tunnel PAC), laiteautentikointi PAC (Machine Authentication PAC) ja käyttäjäkohtainen valtuutus PAC (User Authorization PAC) (IETF-RFC 5422 2009, 13). PAC muodostuu enimmillään kolmesta eri osasta (IETF RFC 4851 2007, 11). Nämä osat ovat:

- PAC-Key
- PAC-Opaque
- PAC-Info

PAC-Key on 32 oktetin pituinen avain, jota käytetään muodostamaan EAP-FAST protokollan vaiheen 1 (Phase 1) tunneli. Kyseinen avain luodaan EAP-palvelimella ja se tulee säilöä turvallisesti asianmukaisilla tavoilla. (IETF RFC 4851, 2007, 11.)

PAC-Opaque on vaihtelevanpituinen kenttä, joka lähetetään palvelimelle EAP-FAST–phase 1 vaiheessa, jossa suojattua tunnelia muodostetaan. PAC-Opaque kentän sisältö voidaan selvittää vain palvelimen toimesta. Sisällön perusteella voidaan vahvistaa peer-laitteen identiteetti ja autentikointi. Sisältö voi koostua mm. PAC-Key:stä ja

esimerkiksi PAC:ia hyödyntävän laitteen identiteetistä. PAC-Opaque:sta itsessään ei voi saada hyödyllistä tietoa. PAC-Opaquen luonnista vastaava palvelin on vastuussa myös siitä, että PAC-Opaque suojataan vahvoilla salausavaimilla ja algoritmeilla. (IETF RFC 4851, 2007, 11.)

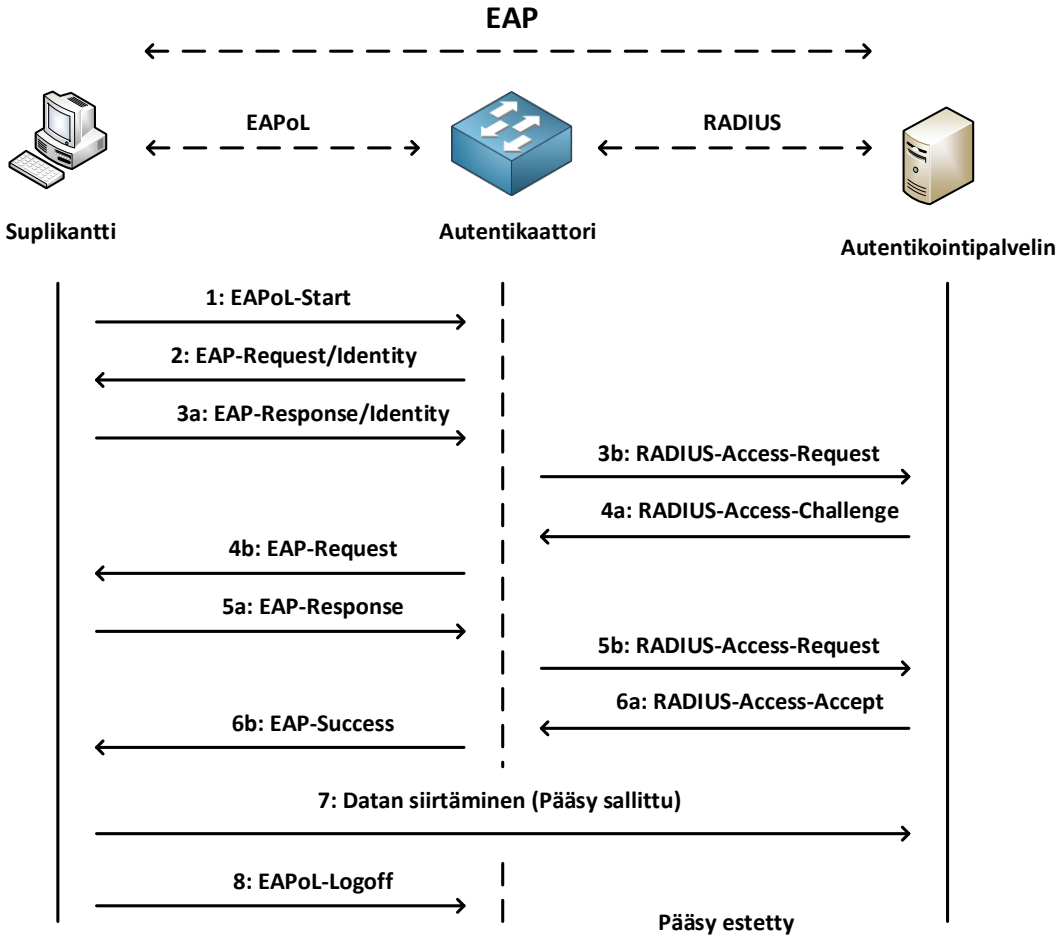
PAC-Info on vaihtelevanpituinen kenttä, joka minimissään antaa tietoa PAC:n luojan identiteetistä. Muuta hyödyllistä, mutta ei pakollista tietoa, ovat esim. PAC-elinaika. (IETF RFC 4851, 2007, 11.)

PAC-voidaan jakaa laitteille dynaamisesti ns. anonyymin tunnelin sisällä. Tällaisessa tapauksessa luodaan Phase 1 vaiheessa anonyymi suojattu Diffie-Hellman-pohjainen TLS-tunneli, jonka jälkeen autentikointi tapahtuu sisäisellä EAP-methodilla (Phase 2) (esimerkiksi EAP-MSCHAPv2). Onnistuneen autentikoinnin jälkeen autentikointipalvelin antaa laitteelle/käyttäjälle PAC-tiedoston. Tämän jälkeen palvelin voi konfiguraatioista riippuen päästää laitteen verkkoon tai ohjeistaa katkaisemaan yhteyden ja aloittamaan uuden EAP-FAST-keskustelun. Uudessa EAP-FAST-keskustelussa käytetään dynaamisesti saatua PAC-tiedostoa uudelleen autentikointiin. (IETF RFC 5422, 2009, 5-11.)

Tällainen PAC-tikettien jakaminen voi mahdollistaa myös MitM-hyökkäykset verkossa, sillä palvelinta ei ole vielä autentikoitu tikettien jakamistilanteessa. On myös mahdollista jakaa manuaalisesti PAC-tiketit laitteille tai käyttää esimerkiksi. sertifikaatteja valmistamaan palvelimen aitous. (IETF RFC 5422, 2009, 6-7.)

2.3.6 802.1X –toimintaperiaate

Yleisen 802.1X-tunnistautumisen vaiheet on esitetty kuviossa 14. Kuvioon on sisällytetty numerot eri viestien kohdalle, joiden avulla esitettyä tilannetta on selkeämpi tarkastella.



Kuvio 14. 802.1X-tunnistautumisen vaiheet

Tyypillinen 802.1X–tunnistautuminen alkaa yleisesti autentikaattorin toimesta. Autentikaattori lähettää suplikantille EAP-request-paketin (2), jonka avulla se pyytää suplikantin identiteettiä. Suplikantti voi myös aloittaa kyseisen prosessin lähettämällä itse EAPOL-Start-paketin(1). Suplikantin aloittaessa prosessin, tulee autentikaattorin lähettää EAP-Request/Identity-paketti(2) vastauksena suplikantin EAPoL-start-pakettiin. Vastauksina edellämainittuihin tilanteisiin suplikantti lähettää tietonsa EAP-Response/Identity-kehyksessä(3a). Autentikaattori vastaanottaa paketin ja purkaa EAPoL-kapsuloinnin paketista.

Seuraavaksi autentikaattori välittää EAPoL-paketista saadun EAP-tiedon autentikointipalvelimelle RADIUS-Access-Request-viestin(3b) yhteydessä. RADIUS-palvelin neuvottelee suplikantin kanssa lähettämällä RADIUS-Access-Challenge–viestin (4a) autentikaattorille, joka enkapsuloi EAP-tiedon EAPoL-kehykseen. Tämän jälkeen autentikaattori välittää kyseisen paketin suplikantille EAP-Request-paketissa(4b).

Suplikantti vastaa EAP-Request-pakettiin lähettämällä autentikaattorille EAP-Response-paketin (5a), joka jälleen purkaa EAP-tiedon EAPoL-kehyksestä ja välittää sen autentikointipalvelimelle RADIUS-Access-Request-viestissä (5b). Tässä vaiheessa lähetetään useita EAP-Response/RADIUS-Access-Request -ja RADIUS-Access-Challenge/EAP-Request- pareja, kunnes autentikointipalvelin lähettää autentikaattorille RADIUS-Access-Accept-viestin (6a). Kyseisellä viestillä ilmaistaan, että suplikantti autentikoitiin onnistuneesti. Autentikaattori välittää tiedon onnistumisesta suplikantille EAP-Success-viestissä (6b).

Suplikantti on tässä vaiheessa autentikoitu onnistuneesti porttiin ja voi siirtää dataa verkossa(7). Datan siirtämisen päätteeksi suplikantti lähettää EAPoL-Logoff viestin (8)autentikaattorille ilmoittaakseen poistumisestaan, jotta portti voidaan laittaa estävään*(blocking)* tai ei-valtuutettuun *(unauthorized)*–tilaan. Tämän jälkeen liikennettä ei mene portista läpi ennen prosessin uudelleenkäynnistymistä.

3 Cisco TrustSec

3.1 SecureX ja TrustSec

SecureX

Secure X on Cisco System:sin kehittämä arkkitehtuurimalli, jonka pääasiallinen tarkoitus on tehdä tietoverkkojen tietoturvasta dynaamisempia. Malli kehitettiin erityisesti silmälläpitäen nykyaikana ilmentyneitä muutoksia tietoverkoissa, joita ovat mm. virtualisoinnin ja erilaisten pilvipalveluiden lisääntynyt käyttö. SecureX on keskittynyt juuri edellämainittujen ratkaisujen tietoturvan kehittämiseen ja ylläpitämiseen. (Velte & Velte, 2014.)

SecureX arkkitehtuuri koostuu kolmesta komponentista, jotka ovat listattuna seuraavassa:

- Cisco Security Intelligence Operations (SIO)
- Context-aware policy and enforcement
- Integrated network and security management

SIO mahdollistaa reaaliaikaisen käsityksen luomisen tietoturvauhkista. Se ylläpitää myös useassa maassa tietokantoja, joihin kerätään tietoja erilaisista uhkista ja niihin liittyvistä tiedoista. Tietoja voidaan päivittää reaaliajassa esimerkiksi IPS-sensoreille jne. (Velte & Velte, 2014.)

Organisaatiotasolla SecureX pyrkii luomaan tietoturvakäytäntöjä perustuen mm. käyttäjien identiteetteihin, sovelluksiin ja käytettäviin laitteisiin. Siinä missä SIO:n tarkoitus on tarjota globaalisti tietoturvaa asiakkaille, keskittyy TrustSec paikallisen tietoturvan parantamiseen. (Velte & Velte 2014.)

3.2 TrustSec

Cisco TrustSec on älykäs korkean turvatason pääsynhallintajärjestelmä. Se antaa näkyvyyden siitä, kuka tai mikä on liittymässä verkkoon ja vähentää riskejä kontrolloimalla resursseja, joihin käyttäjät tai laitteet voivat päästä. (TrustSec Products 2014.)

Määritelmänä ”TrustSec” voi olla sekava. Yleisesti määritettynä TrustSec on monia osa-alueita kattava termi, joka kattaa kaikkea jolla on jotain tekemistä identiteetin kanssa. Identiteetti tässä tapauksessa tarkoittaa ymmärtämistä siitä kuka, mikä, missä, milloin ja miten kytkeytyy verkkoon. TrustSec ei kuitenkaan ole terminä yhtä kuin identiteetti vaan pikemminkin identiteetteihin perustuva järjestelmä tai ratkaisu, johon kuuluu useita erilaisia komponentteja. (BRKSEC-1022 2011, 7-8). Näitä komponentteja ovat mm.

- IEEE 802.1X, MAB
- Profiling Technologies
- Posture Assessment
- Guest Services
- Security Group Access (SGA)
- MACSec (802.1AE)
- Identity Services Engine (ISE)
- Access Control Server (ACS)

TrustSecin ominaisuudet on sisällytetty lukuisiin eri Ciscon järjestelmiin. Näitä ovat mm. reitittimet, kytkimet, WLC:t ja palomuurit. TrustSec:n tarkoituksena on kategorioida liikennettä päätelaitteiden identiteetin mukaan pelkän IP-osoitteen sijaan, joka mahdollistaa aikaisempaa joustavamman pääsynhallinnan dynaamisiin verkkoympäristöihin ja datakeskuksiin. (TrustSec Overview 2014, 6.)

Cisco TrustSec-ratkaisun tarkoituksena on yksinkertaistaa tietoturvan luomista ja hallintaa. Perinteinen pääsynhallinta perustuu verkon topologiaan, mutta TrustSec ottaa tähän käyttöön erilaisen lähestymistavan. Se käyttää pääsynhallinnassaan hyväksi loogisia ryhmiä, jolloin korkean tietoturvan pääsynhallintaa voidaan ylläpitää,

vaikka erilaisia resursseja siirrettäisiin verkossa paikasta toiseen. (TrustSec Overview 2014, 6.)

3.3 Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine (Cisco ISE) on seuraavan sukupolven identiteettiin- ja pääsynhallintaan keskittyvä alusta, jonka tarkoituksena on mm. vahvistaa verkon infrastruktuurin tietoturvaa ja nykyaikaistaa palvelujen toimintaa. ISE:n ainutlaatuinen arkkitehtuuri mahdollistaa mm. reaaliaikaisen tiedon keräämisen niin verkosta, laitteista kuin käyttäjistäkin. Näitä tietoja voidaan käyttää sitomalla identiteetit verkon laitteistoon, kuten kytkimiin, WLC:ihin, VPN Gateway:hin jne. (ISE User Guide-1.2 2014.)

ISE mahdollistaa monien eri ominaisuuksien toteuttamisen. Se yhdistää AAA-palvelut yhteen alustaan. Autentikointi voidaan suorittaa käyttämällä hyväksi monia standardoituja autentikointiprotokollia kuten Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Protectec Extensible Authentication Protocol (PEAP) jne. ISE määrittelee sallittavat protokollat, joita verkkolaitteiden kanssa käytetään sekä identiteettilähteen, josta käyttäjän autentikointitiedot tarkistetaan. (ISE User Guide-1.2 2014.)

Cisco ISE:n identiteetteihin perustuva hallinta mahdollistaa mm. sen, että käyttäjä kirjautuu verkkoon sallitulla ja verkon tietoturvapolitiikkaa noudattavalla laitteella. Käyttäjän identiteetistä, sijainnista ja kirjautumisista kerätään myös tietoa, jota voidaan myöhemmin käyttää erilaisissa raporteissa ja valvonnassa. Palveluita voidaan myös määritellä mm. roolin, ryhmän, laitetyypin, politiikan jne. mukaan. Yleisesti ISE sallii autentikoiduille käyttäjille pääsyn sovelluksiin ja palveluihin perusten autentikointituloksiin. (ISE User Guide-1.2 2014.)

Perustasolla ISE tukee 802.1X-, MAC Authentication Bypass (MAB)- ja selainpohjaista Web Authentication (WebAuth)-menetelmiä autentikoinnissa niin langallisissa kuin langattomissakin verkoissa. ISE määrittelee autentikointipyynnön saapuessa ovatko kyseiset protokollat sallittuja kyseiseen pyyntöön. Tätä kutsutaan ns. ”ulommaksi

osaksi". Tämän jälkeen ns. "sisäinen osa"määrittelee sen, mitä identiteettilähdettä käytetään autentikoinnin yhteydessä. Autentikoinnin onnistuessa sessio siirtyy valtuutuspolitiikkaan. ISE:n valtuutuspolitiikan tulos on valtuusprofiili ja sisältää esimerkiksi ladattavan pääsylistan (dACL). (ISE User Guide-1.2 2014.)

Profiler Service

Profilointipalvelu (Profiler Service) mahdollistaa kaikkien päätelaitteiden tunnistamisen, paikallistamisen ja ominaisuuksien päättelemisen verkossa riippumatta laitteen tyypistä. Profilointipalvelu käyttää hyväkseen useita tunnistimia (probe), jotka keräävät attribuutteja verkon kaikilta päätelaitteilta. Näitä tietoja käytetään ISE:llä määrittelemään päätelaitteet oikeisiin ryhmiin. ISE mahdollistaa laitteiden profiloinnin mm. SNMP:n, NetFlown, HTTP:n, DHCP:n, RADIUS ja DNS avulla. Esimerkkinä mainittakoon RADIUS-ilmaisin joka kerää RADIUS-viesteistä attribuutteja profilointia varten autentikoinnin yhteydessä. (ISE User Guide-1.2 2014.)

Posture Assessment

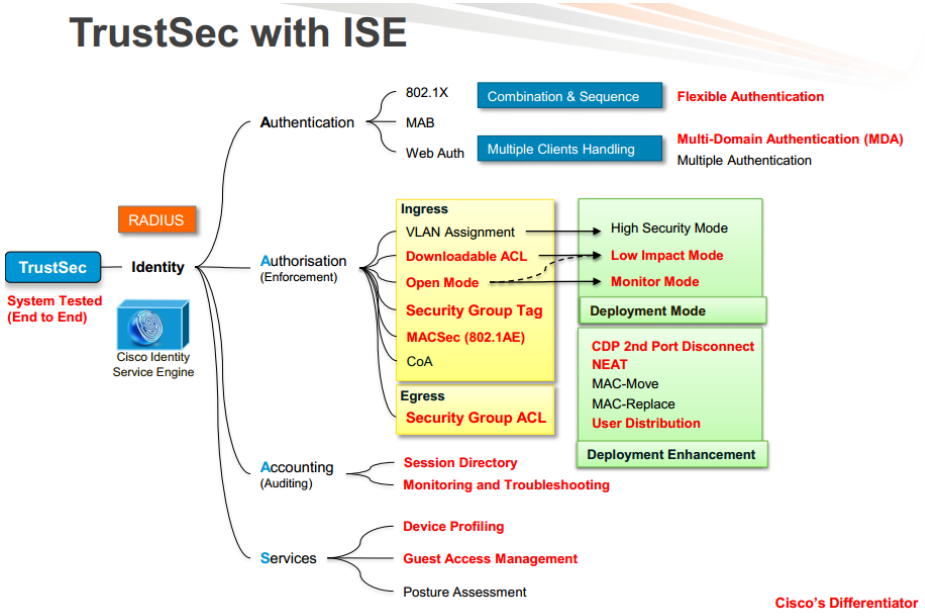
ISE:n avulla pystytään vahvistamaan ja ylläpitämään jokaisen asiakaslaitteen tietoturvaominaisuuksia jotka liittyvät suojattuun verkkoon. Erityiset *"posture policies"* mahdollistavat sen, että asiakaslaitteilla on ajantasalla olevat tietoturva-asetukset ja ohjelmistot. Posture-ominaisuus voidaan toteuttaa kahdella erilaisella asiakaslaitteille asennettavilla sovelluksella: Cisco NAC Web Agent:lla tai Cisco NAC Agent:lla. Erona näiden kahden välillä on, että NAC Web Agent asentuu vain väliaikaisesti sisäänkirjautumisen yhteydessä laitteelle, jonka jälkeen se ei enää näy. NAC Agent taasen jää asentuneeksi laitteelle. (ISE User Guide-1.2 2014.)

Guest Services

ISE mahdollistaa myös erityisten vierastilien luonnin väliaikaisesti joiden avulla voidaan määrätä esimerkiksi vierailijoiden, konsulttien ja asiakkaiden pääsy verkossa. Näillä tileillä on myös erityiset aikarajoitukset, joten vieraiden pääsyä voidaan hallita esimerkiksi päivään, aikarajaan jne. perustuen. ISE:n järjestelmävalvojat voivat luoda

myös erityisiä tilejä, joilla on oikeus luoda vierailijoille väliaikaisia tunnuksia. (ISE User Guide-1.2 2014.)

Kuviossa 15 on havainnollistettu ISE:n rooli TrustSec-ympäristössä



Kuvio 15. ISE:n rooli TrustSec-ympäristössä (BRKSEC-1022 2011, 106.)

ISE sisältää lukuisia eri ratkaisuja ja ominaisuuksia profiloinnista AAA-palveluihin. ISE toimiii myös pääkomponenttina TrustSec:n SGA-ratkaisussa.

3.4 SGA

Cisco Security Group Access (SGA)-ratkaisun tarkoituksena on luoda turvallinen verkkoympäristö käyttämällä hyväksi luotetuista laitteista koostuvaa toimialuetta. Jokainen uusi laite autentikoidaan toisten vertaisten laitteiden kanssa. Toimialueen sisällä kommunikaatio pyritään turvaamaan mm. salaamalla liikenne, turvaamalla viestien eheys ja käyttämällä erilaisia toistinhyökkäyksiä estäviä mekanismeja. SGA käyttää hyväkseen autentikoinnin aikana saatuja käyttäjä- ja laitetunnistetietoja määrittääkseen paketit eri Security Group (SG)-ryhmiin. Luotettuun toimialueeseen saapuvat paketit merkitään tunnisteilla, jotta niihin voidaan tarvittaessa sijoittaa erilaisia tietoturvaparametreja. (ISE User Guide-1.2 2014.)

SGA:n ominaisuuksia ja komponentteja listattuna:

- Security Group (SG)
- Security Group Tag (SGT)
- SGT Exchange Protocol (SXP)
- Network Device Admission Control (NDAC)
- Endpoint Admission Control (EAC)
- Security Group Access Control List (SGACL)
- Security Group Firewall (SGFW)
- Environment Data Download

Huomioitavaa on, että identiteettipohjainen pääsynhallinta vaatii myös muitakin komponentteja toimiakseen. Näitä ovat mahdollisesti Active Directory (AD), certificate authority (CA)-palvelin, Domain Name Server (DNS)-palvelin ja Dynamic Host Configuration Protocol (DHCP)-palvelin. (ISE User Guide-1.2 2014.)

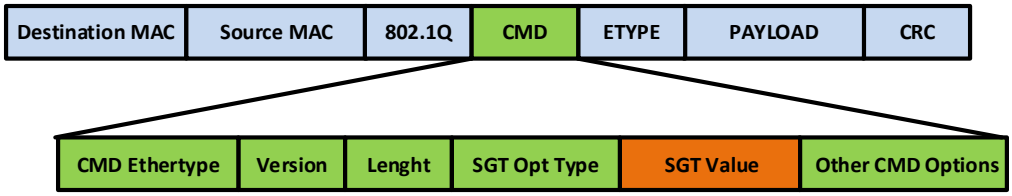
SG

Security Group (SG)-menetelmällä tarkoitetaan käyttäjien, päätelaitteiden ja resurssien liittämistä ryhmiin jotka jakavat samat pääsynhallintapolitiikat. Uudet laitteet ja käyttäjät voidaan liittää oikeisiin SG-ryhmiin näiden liittyessä SGA:ta tukevaan toimialueeseen. (ISE User Guide-1.2 2014.)

SGT

Security Group Tag (SGT) on 16-bittinen arvo, joka verkkoon liittyville laitteille ja/tai käyttäjille annetaan kirjautumisen yhteydessä. Verkon infrastruktuuri näkee SGT-leiman erillisenä attribuuttina joka istuntoihin liitetään. Verkon laitteet liittävät tämän L2-leiman kaikkeen liikenteeseen jota kyseisestä istunnosta lähetetään. Kullekin päätelaitteelle tai käyttäjille voidaan määrätä vain yksi SGT-leima. (TrustSec Overview 2014, 6-7.)

Kuviossa 16 on esitetty SGT-leima (Kuviossa oranssilla) Ethernet-kehyksessä.



Kuvio 16. SGT Ethernet-kehyksessä.

Päätelaitteet eivät ole itse tietoisia niille määrätystä SGT-leimasta vaan se on tiedossa ainoastaan verkkolaitteilla. Ainoastaan verkon luotetut tai autentikoidut verkkolaitteet voivat määrätä SGT-leiman. Laitteiden tulee myös tukea SGT-leimoja, jotta niitä voidaan käyttää. (TrustSec Overview 2014, 7.)

SXP

SXP on TCP-pohjainen protokolla, jota käytetään lähettämään IP-osoite-SG-kytköksiä protokollaa tukevien laitteiden välillä. Protokolla on kehitetty laitteille jotka eivät tue rautatasolla SGT-leimoja. Kyseistä protokollaa tukevat laitteet voivat kuulua joihinkin seuraavista tiloista: ”Speaker”, ”Listener” tai molempiin edellämainituista. Näistä Speaker määritellään laitteeksi, joka lähettää eteenpäin IP-osoite-SG-kytköksiä. Listener on vastaavasti laite, joka vastaanottaa edellämainittuja kytköksiä. (TrustSec Overview 2014, 21.)

EAC

Endpoint Admission Control (EAC) tarkoittaa autentikointiprosessia päätelaitteelle tai käyttäjälle, joka on yhdistymässä SGA-ympäristöön. EAC tapahtuu tyypillisesti verkon liityntätasolla sijaitsevalla kytkimelle. Onnistuneen autentikointi -ja valtuutusprosessin jälkeen päätelaitteelle määrätään SGT-leima. Pääsymenetelmiä EAC:issa ovat 802.1X, MAB ja WebAuth. (ISE User Guide-1.2 2014.)

NDAC ja Environment Data

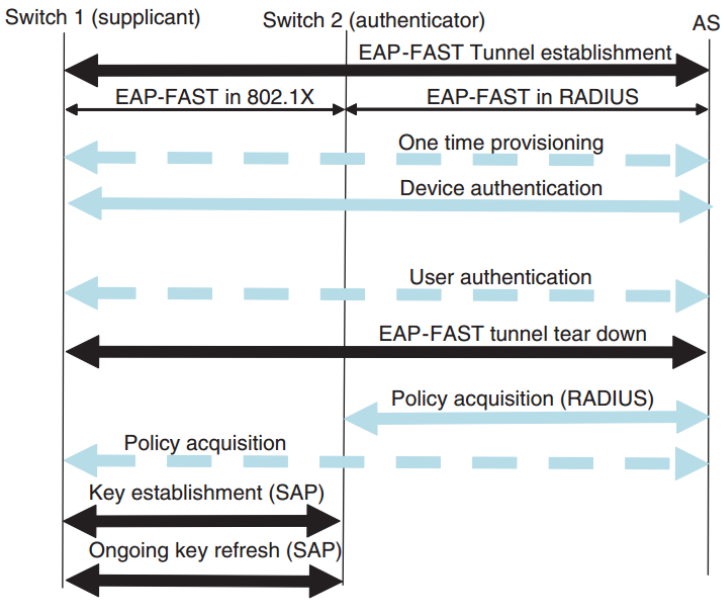
Cisco TrustSec-ratkaisu autentikoi verkkolaitteen, ennen kuin se sallii sen pääsyn verkkoon. Tähän käytetään hyväksi Network Device Admission (NDAC)- menetelmää, jossa verkkolaitteet (esim.kytkin) autentikoituvat keskenään käyttäen hyväksi 802.1X-protokollaa Extensible Authentication Protocol Flexible Authentication via

Secure Tunnel (EAP-FAST) kanssa. EAP-FAST–metodia käytetään mm. siitä syystä, että tunnistautumisessa voidaan käyttää useita eri menetelmiä (esim. MSCHAPv2) käyttäen hyväksi autentikoinnin aikana luotua suojattua tunnelia (EAP-FAST tunnel). (Cisco TrustSec Arch 2011.)

NDAC:issa on tyypillisesti kolme vaihetta, jotka ovat

- Autentikointi
- Valtuutus
- Security Association Protocol (SAP)-keskustelu

Kuviossa 17 on havainnollistettu kokonaista prosessia.



Kuvio 17. NDAC-vaiheet (Cisco TrustSec Arch 2011.)

Autentikoinnilla tarkoitetaan tilannetta, jossa supplikantti autentikoidaan autentikointipalvelimen toimesta. Samassa tilanteessa autentikaattori toimii välikätenä. Suplikantilla (non-seed) tarkoitetaan laitetta, joka on kytkeytyneenä jo-tunnistautuneeseen laitteeseen Trustsec-ympäristössä ja pyrkii liittymään verkkoon. Autentikaattori on taasen laite (seed), joka on jo liittynyt osaksi TrustSec–toimialuetta. TrustSec mahdollistaa myös ns.roolinvalinta-algoritmin käytön, joka automaattisesti päättelee, kumpi kytkimistä toimii autentikaattorina ja kumpi suppli-

kanttina. Autentikaattoriksi valitaan kytkin, jolla on IP-yhteys autentikointipalvelimeen. Eteen voi tulla myös tilanne, jossa molemmilla kytkimillä on tieto palvelimesta ja ovat seed-laitteita. Tällaisessa tilanteessa kytkimestä, joka saa ensimmäisenä vastauksen RADIUS-palvelimelta, tulee autentikaattori. (Cisco TrustSec Arch 2011.)

Valtuutusvaiheessa laitteiden identiteetin perusteella autentikointipalvelin määrää valtuutuspolitiikat, kuten SG-ryhmän tai ACL:n kummallekin linkin osapuolelle. Samassa tilanteessa autentikointipalvelin antaa molemmille osapuolille (supplikantille ja autentikaattorille) tiedon toistensa identiteeteistä, jolloin molemmat osaavat asettaa linkille oikeat politiikat. Viimeisessä vaiheessa käydään SAP-keskustelu. Autentikaattori ja supplikantti keskustelevat vaadittavista parametreista linkin salaamiseen, jos molemmat tukevat kyseistä menetelmää. (Cisco TrustSec Arch 2011.)

Kaikkien vaiheiden jälkeen autentikaattori vaihtaa linkin tilan estävästä valtuutetuksi ja supplikantista tulee TrustSec-toimialueen jäsen. (Cisco TrustSec Arch 2011).

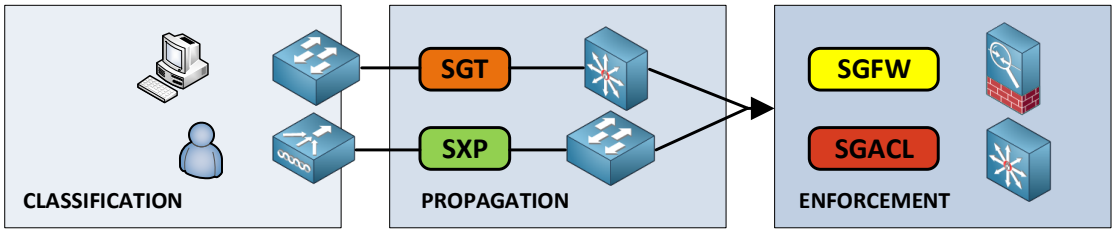
Environment Data Download vaiheessa laite saa ympäristöön liittyvää tietoa ISE:ltä. Kyseistä tietoa voidaan myös manuaalisesti konfiguroida laitteelle tarvittaessa. Kyseiset tiedot sisältävät mm. listan palvelimista (Server Lists), joita asiakas voi käyttää tulevissa RADIUS-pyynnöissä autentikointiin ja valtuuttamiseen. Lisäksi laite saa laitepohjaisen SG-ryhmän tiedon, johon se itse kuuluu ja tiedon ajasta, jonka välein edellämainitut tiedot tulee päivittää. (ISE User Guide-1.2 2014.)

3.5 TrustSec:in pääsynhallinnan vaiheet

Yleisesti TrustSec:in pääsynhallinta voidaan jakaa kolmeen eri vaiheeseen, jotka ovat (TrustSec Overview 2014, 3.):

- Classification
- Propagation
- Enforcement

Kuviossa 18 on esitetty loogisesti TrustSec:n vaiheet pääsynhallinnassa.



Kuvio 18. TrustSec vaiheet pääsynhallinnassa

SGT voidaan ”määritellä” (Classification) laitteille dynaamisesti tai staattisesti. Laitteiden tulee myös tukea SGT-leimoja. Dynaaminen määrittely tapahtuu autentikointitapahtuman jälkeen. Näitä tapahtumia ovat esimerkiksi 802.1X, MAB tai Web Authentication. Staattisessa määrittely tapahtuu tilanteessa, jolloin autentikointi ei ole mahdollinen tai käytössä on topologiaan pohjautuvia politiikkoja. Yleisesti staattisia määrityksiä käytetään esimerkiksi datakeskuksien palvelimille. Tällöin määrittely tapahtuu siten, että SGT yhdistetään esimerkiksi IP-osoitteeseen, VLAN:iin tai rajapintaan. Edellämainitut esimerkit määrittelyssä, jossa SGT asetetaan, kuljetetaan syvemmälle verkkoon. (TrustSec Overview 2014, 11-12.)

Tässä vaiheessa SGT on määritelty laitteille/käyttäjille, joten seuraava askel on siirtää tieto leimasta upstream-suuntaan TrustSec-laitteille, jotka voivat asettaa politiikkoja SGT-leimojen mukaan. Tätä kommunikointiprosessia kutsutaan nimellä ”eteneminen” (Propagation). TrustSec sisältää kaksi tapaa siirtää SGT-leimoja eteenpäin jotka ovat ”inline” ja SXP. Inline-leimaaminen on perimmäisenä tavoitteena. Tällaisella lähestymistavalla liityntäkerroksen laitteet voivat asettaa SGT-leiman suoraan L2-kehyksiin ja kuljettaa tätä eteenpäin upstream-laitteille. Tällainen natiivileimaaminen mahdollistaa tekniikan skaalautuvan käytännössä rajattomasti, sillä se ei ole riippuvainen mistään L3-tason protokollasta. Toisinsanoen sillä ei ole merkitystä onko liikenne IPv4- vai IPv6–liikennettä, sillä leima on yksilöllinen. Natiivia leimausta käytettäessä SGT välitetään hyppy-hypyltä menetelmällä koko verkon infrastruktuurissa. Menetelmä mahdollistaa sen, että liikennettä voidaan hallita missä tahansa verkon osassa. (TrustSec Overview 2014, 14-16.)

Täydellisessä maailmassa kaikki verkon laitteet tukisivat inline-leimaamista. Tämä ei ole todellisuutta, sillä laitteet tarvitsevat erikseen räätälöityjä piirejä. Tätä varten

kehitettiin SXP, jotta verkossa voidaan mainostaa IP-SGT-kytköksiä. SXP:tä käytetään ”etenemisvaiheessa” pääasiallisesti kahdesta syystä. Toinen on se, että laite ei pysty inline-leimaamiseen. Tällainen laite on esimerkiksi vanhempi WLC, joka voi toimia vain SXP-speaker-tilassa. Toinen tilanne on, että viereinen laite ei ole kykeneväinen mihinkään SGT-ominaisuuksiin. Tällöin IP-SGT-kytkökset voidaan mainostaa kyseisen laitteen/laitteiden yli L2-tai L3-tasolla. (TrustSec Overview 2014, 21-22.)

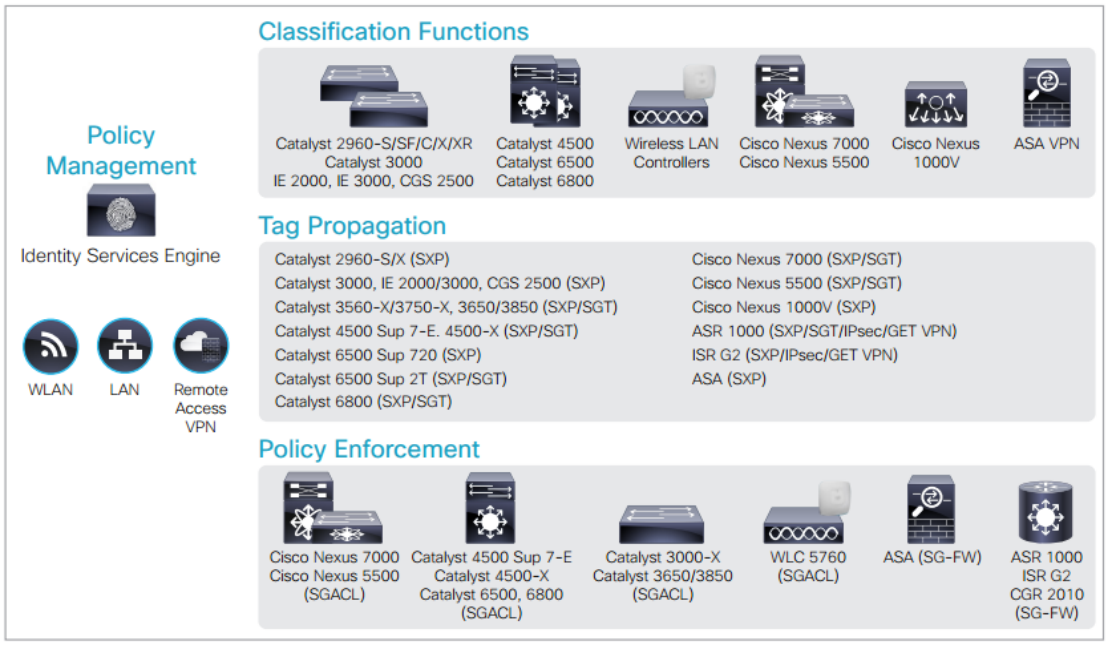
Tässä vaiheessa laitteille on määritelty (Classification)leimat ja niitä pystytään siirtämään verkossa (Propagation). Tämän jälkeen on vuorossa toimeenpanovaihe (Enforcement). Liikennöintiä voidaan hallita usealla tavalla, mutta yleisesti nämä voidaan jakaa kahteen ryhmään, jotka ovat:

- Security Group Access Control List (SGACL)
- Security Group Firewall (SGFW)

Security Group Access Control List (SGACL) mahdollistaa pääsynhallintaa perustuen määrättyihin SGT-leimoihin. Ne rajaavat sitä, mitä käyttäjä voi tehdä perustuen rooliin pelkän IP-osoitteen sijaan. (ISE User Guide-1.2 2014). Tyypillinen tilanne on, että pääsyä hallitaan IP-pohjaisten pääsylistojen avulla, mutta ongelmaksi tulee näiden jatkuva ylläpitäminen. Yksinkertaisessa tilanteessa tämä ei ole ongelma, mutta erilaisten roolien kasvaessa kasvaa myös pääsylistojen hallitsemisen määrä. Tämän takia SGACL-menetelmä on yksinkertainen hallita, sillä listat pitävät sisällään vain lähde- ja kohde roolit (SG) sekä palvelujen portit. SGACL-listat ladataan dynaamisesti ISE:ltä, joten mitään muutoksia listoihin koskien ei tarvitse tehdä verkkolaitteilla suoraan. (TrustSec AAG 2013).

Jotkin organisaatiot haluavat keskittää liikenteen suodattamisen yhteen palomuuriin. Cisco on lisännyt palomuureihinsa ominaisuuden nimeltä Security Group Firewall (SGFW). Olemassa on kahdentyyppisiä SGFW:ja, jotka ovat ASA-pohjainen SGFW ja reititinpohjainen SGFW. ASA:n SGFW pohjautuu yksinkertaiseen konseptiin. Palomuurin säännöt sisältävät nyt mahdollisuuden lähde- ja kohde-SG:eille. Huomioitavaa on, että SGFW ei pysty hyödyntämään ISE:llä luotuja SGACL:iä. (TrustSec Overview 2014, 45-46.)

Kuviossa 19 on esitetty Ciscon laitteiden ominaisuudet SG-pohjaisessa TrustSec-ympäristössä.



Kuvio 19. TrustSec laitteisto (TrustSec AAG 2014.)

3.6 802.1AE (MACsec)

3.6.1 Media Access Control Security (802.1AE)

Media Access Control Security (MACSec) on L2-tason salaukseen käytettävä protokolla lähiverkoissa. Sen tarkoituksena on salata liikenne autentikoitujen lähiverkon päätelaitteiden välillä niin, ettei fyysisellä linjalla liikkuvaa dataa pystytä monitoroimaan tai muokkaamaan. MACsec on määritelty IEEE-standardissa 802.1AE. (MACsec Deploy Guide 2011, 4.)

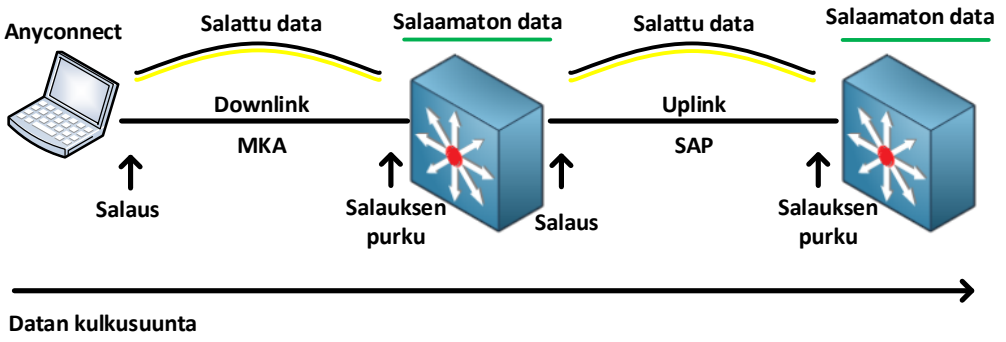
MACsec suunniteltiin pääpuoleisesti käytettäväksi 802.1X-protokollan kanssa. Ennen vuoden 2010 versiota IEEE:n 802.1X-standardista ei ollut menetelmää olla varmoja lähetetyn datan eheydestä ja luotettavuudesta autentikoinnin jälkeen. Data lähetettiin selkokielisenä ilman eheystarkistuksia, joten fyysisen pääsyn autentikoituun porttiin omaavat pystyivät monitoroimaan, muokkaamaan ja lähettämään liikennettä.

Tämä pystyttiin toteuttamaan esimerkiksi käyttämällä hyväksi väärennettyjä MAC-osoitteita. (MAC Address Spoofing). (MACsec Deploy Guide 2011, 5.)

MACsec sisältää myös haittapuolia. Näistä kenties merkittävin on mahdollisten kustannusten kasvu verkkolaitteiden päivittämisen kohdalla, sillä läheskään kaikki laitteet eivät tue kyseistä protokollaa. Kustannukset kasvavat esimerkiksi tilanteessa, jossa kytkimen rautaa joudutaan päivittämään. Protokollan käyttöönotto voi myös vaikuttaa jo olemassa olevien teknologioiden toimintaan. (MACsec Deploy Guide 2011, 4.)

MACsec on hyödyllisin verkon liityntätasolla, jossa käyttäjillä on suora yhteys kytkinten portteihin. Tämän tyyppistä liityntätapaa kutsutaan nimellä downlink-MACSec. Myös uplink suuntaan olevat linkit liityntä- ja jakelukerroksen välillä voidaan suojata MACsec-protokollan avulla. MACSec:n ollessa käytössä uplink -ja downlink-suuntaan samanaikaisesti tulee huomioida se, että molemmat istunnot ovat täysin itsenäisiä. Liikenne on salattua kytkimen porteista ulospäin, mutta selkokielistä kytkimen sisällä. Tätä termiä voidaan myös kutsua nimellä hop-by-hop-encryption eli hyppy-hypyltä-salaus. Tämän tarkoituksena on mahdollistaa mm. se, että kytkin voi tarvittaessa monitoroida liikennettä ja liittää verkkokohtaisia sääntöjä (esim. QoS) paketteihin kuitenkaan vaarantamatta tietoturvaa fyysisellä linjalla. (MACsec Deploy Guide 2011, 6.)

Kuviossa 20 on havainnollistettu MACsec salaus hyppy-hypyltä-periaatteella.



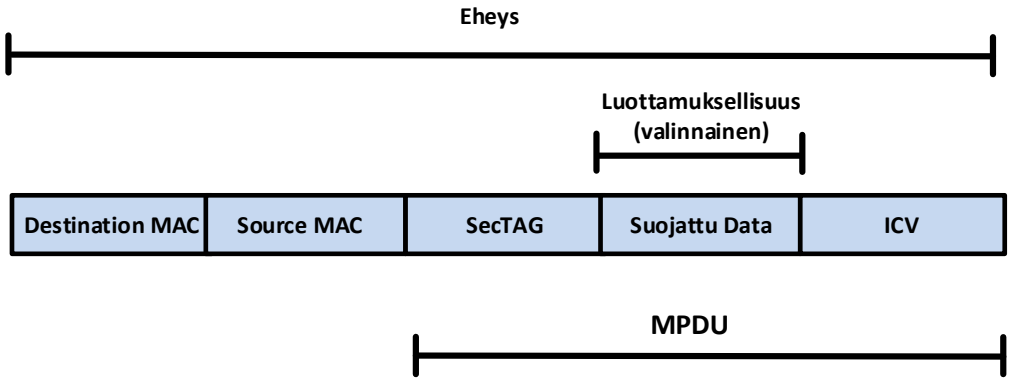
Kuvio 20. MACsec hop-by-hop

Kuviosta voidaan tarkastella periaatetta hyppy-hypyltä salauksessa. Linkki AnyConnect-suplikantin ja kytkimen välillä on salattuna ja selkokielistä kytkimen sisällä. Kytkinten välinen linkki on kuitenkin uudelleen salattu uplink-suuntaan.

Kuviosta voidaan myös havaita käytettyt avaintenhallintaprotokollat. Cisco Security Association Protocol (SAP) on tarkoitettu avaintenhallintaan kytkinten väliselle linkille ja tätä ei tueta päätelaitteisiin kytkeytyvissä porteissa, joiden takana on esimerkiksi PC tai IP-puhelin. Tätä varten on kehitetty MACSec Key Agreement (MKA) protokolla. Molemmat tukevat 802.1AE:n mukaisesti pakettien salaamista ja autentikointia MACsec-protokollaa tukevien laitteiden välillä. (MACsec Switch Guide.)

MACsec-paketti

Kuviossa 21 on esitetty MACsec-paketti.



Kuvio 21. MACsec-paketti

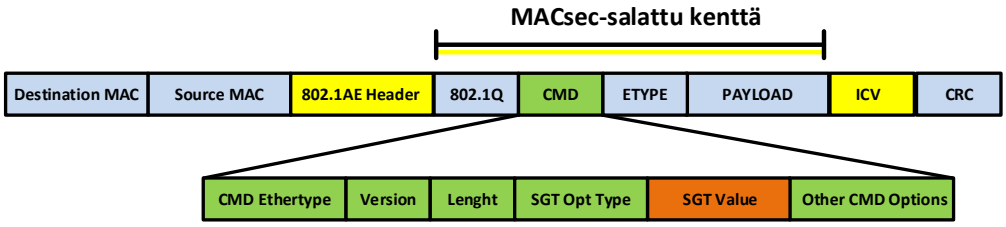
Jokainen MACsec-protocol Data Unit (MPDU) koostuu kolmesta osasta, jotka ovat

- Security TAG (SecTAG)
- Suojattu Data
- Integrity Check Value (ICV)

SecTAG (tai 802.1AE-Header) sisältää tiedot mm. MACsec protokollan EtherTypestä (0x88E5), Association Numberista (AN), Packet Numberista(PN). AN tarkoitus on tunnistaa turvatun linkin osapuolet yksilöllisesti. PN mahdollistaa toistohyökkäysten estämisen yksilöimällä kaikki lähetetyt MPDU:t. Suojatun datan kenttä käsittää koko

osan SecTAG- ja ICV-kentän välissä. ICV suojaa koko pakettia MAC-osoitteita myöten (802.1AE-2006, 41-42). Arvoa käytetään varmistamaan ettei paketin data ole muuttunut (802.1AE-2006, 6).

Kuviossa 22 on vielä havainnollistettu MACsec-suojattu paketti, johon on avattu MACsec-salattu kenttä TrustSec SGT-leiman kanssa.



Kuvio 22. MACsec-paketti SGT:n kanssa

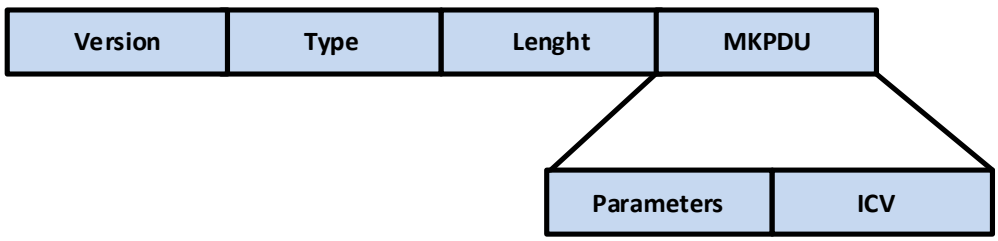
Kuviosta voidaan havaita myös, että mahdollinen VLAN-leimakin kulkee salattuna paketin sisällä.

3.6.2 MKA

MACsec Key Agreement (MKA) on protokolla, joka mahdollistaa protokollaa tukevien laitteiden keskinäisen tunnistamisen ja huolehtii käytettävistä avaimista MACsec-salauksen luomista varten. Protokolla on määritelty standardissa IEEE 802.1X-2010. (MACsec Deploy Guide 2011, 8.)

MKA käyttää hyväkseen EAPOL-MKA pakettityyppiä. Näitä paketteja kutsutaan nimellä EAPOL-MKPDU (MACsec Key Agreement Protocol Data Unit). (802.1X-2010, 95.)

Kuviossa 23 on esitetty EAPOL-MKA-paketti.



Kuvio 23. MKPDU-paketti

Version-kenttä ilmaisee lähettäjän EAPOL-version. *Type*-kentän arvona on 5 taulukon 3 mukaisesti. Lenght-kenttä ilmaisee MKPDU:n pituuden. (802.1X-2010, 90). Parametreihin (Parameters) liitetään tietoa mm. siitä, onko osapuoli kykeneväinen MACsec-protokollaan, onko MACsec-käytössä, käytetäänkö eheystarkistuksia jne. (802.1X-2010, 69).

Jokaisessa MKA-instanssissa valitaan ns. *"Key Server"*, jonka tehtävänä on mm. päättää MACsec:n käytöstä, valita käytettävä salausmenetelmä ja luoda sekä jakaa SAK-avain.

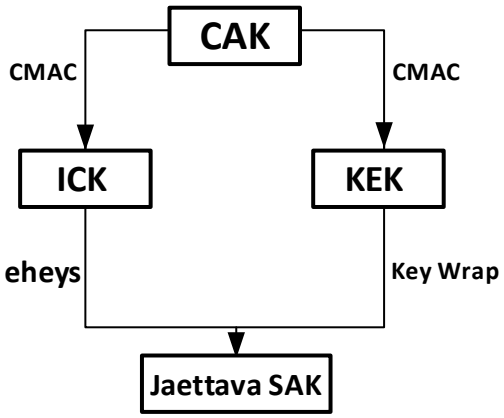
MKA sisältää monia avaimia, joita ovat mm.

- CAK
- KEK
- ICK
- SAK

Connectivity Association Key (CAK) on jokaisen MKA-instanssin juuriavain, joka on jokaisella linkin osapuolella. Jokainen CAK tunnistetaan Connectivity Association Key Name (CKN) avulla. CAK-avainta ei koskaan käytetä suoraan MKA:ssa. Johdettavat avaimet sidotaan CAK:hon, joten niitä ei voida käyttää minkään muun CAK-avaimen kanssa. (802.1X-2010, 62-63.)

CAK:sta johdetaan myös kaksi muuta avainta AES-CMAC-menetelmän avulla. Nämä ovat Key Encrypting Key (KEK) ja Integrity Check Value Key (ICK). (802.1X-2010, 63).

Kuviossa 24 on havainnollistettu avainhierarkiaa.



Kuvio 24. MKA Perus-hierarkia

Key encypting key (KEK) on avain, jota käytetään AES- Key Wrapin kanssa suojaamaan Security Association Key (SAK)-avainta (802.1X-2010, 64). SAK taasen on salainen avain, jota käytetään salaamaan liikenne linkkivälillä. Kyseinen avain johdetaan muiden tavoin CAK-avaimesta ja se tulee olla molemmilla osapuolilla, jotta liikennettä voidaan salata. (MACsec-Deploy-Guide 2011, 9). Key Server on vastuussa SAK luomisesta, sekä jakamisesta. Key Server myös päättää mahdollisesti käytettävästä salausmenetelmästä, joka oletuksena on AES-GCM 128 bit. SAK lähetetään jokaisessa MKPDU-paketissa, kunnes vastapuoli ilmoittaa SAK-avaimen asennuksen onnistuneen. (802.1X-2010, 69-70).

Jokainen MKPDU:n eheys suojataan 128 bittisellä Integrity Check Valuella (ICV). ICV luodaan AES-CMAC:n avulla avaimesta ICK käyttämällä hyväksi mm. osapuolten MAC-osoitteita ja ICK-avainta. ICK avainta ei jaeta suoraan minkään protokollan mukana, sillä se vain johdetaan CAK:sta. Tämän ansiosta ICV arvon todentaminen takaa sen, että MKPDU:iden sisältö ei ole muuttunut, kuten myös sen, että kyseisen paketin on luonut järjestelmä jolla on CAK hallussaan. (802.1X-2010, 65.)

MACsec -ja 802.1X-komponentit

Liityntätasolla MACSec sisältää 802.1X:n tavoin kolme komponenttia, jotka ovat suplikantti, autentikaattori ja autentikointipalvelin. Suplikantti tai asiakas on laite, johon on asennettu MACSec-salausta tukeva ohjelmisto. Sen tehtävänä on välittää tunnistautumistiedot eteenpäin autentikointia varten ja kyetä lähettämään MACSec-

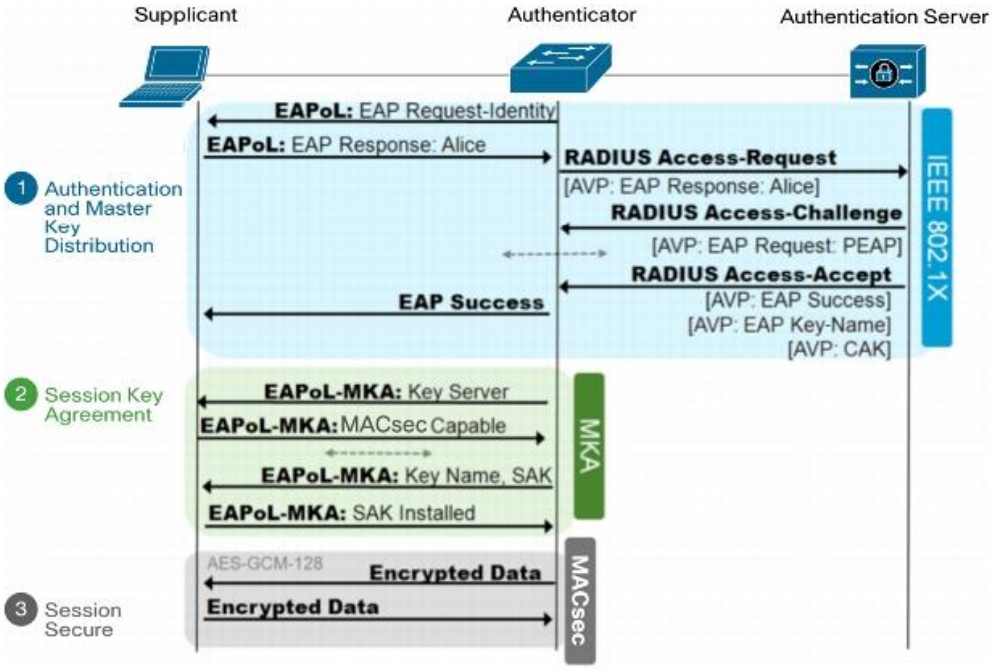
salattua liikennettä, sekä hallitsemaan protokollan avaimenluonti-mekanismia. (MACsec-Deploy-Guide 2011, 7.)

Autentikaattorin tehtävänä on mm. välittää eteenpäin suplikantin tunnistautumistiedot autentikointipalvelimelle ja kyetä hallitsemaan MACsec:in salausavaimen luominen ja pakettien salaaminen. (MACsec-Deploy-Guide 2011, 7.)

Autentikointipalvelimen tehtävänä on tarkistaa suplikantin tunnistautumistiedot ja määritellä millaiset oikeudet tunnistettavalle osapuolelle luovutetaan. MACSec-salauksen muodostamisessa autentikointipalvelimella on myös tärkeä rooli, sillä se luo vaadittavat avain-materiaalit salauksen luomiseen suplikantin ja autentikaattorin välille.(MACsec-Deploy-Guide 2011, 7.)

802.1X ja MACSec-salauksen muodostumisen vaiheet

Kuviossa 25 on esitetty MACsec:in toiminta 802.1X-protokollan kanssa.



Kuvio 25. 802.1X ja MACsec (MACsec Deploy Guide 2011, 8.)

MACSec- salauksen muodostuminen voidaan jakaa kolmeen eri vaiheeseen, jotka ovat:

- ”Master Key Distribution”
- ”Session Key Agreement”
- ”Session Secured”

MACSec-salauksen muodostaminen päätelaitteelta autentikaattorille alkaa onnistuneen 802.1X-tunnistautumisen seurauksena. Tämänjälkeistä vaihetta kutsutaan Master Key distribution-vaiheeksi. Tunnistautumisvaiheessa suplikantti ja autentikaattorikytkin saavat tarvittavat salausavainmateriaalit MACSec-salauksen muodostamista varten. Suplikantti ja autentikointipalvelin käyttävät hyväkseen EAP-methodia, joka tukee salausavaimien muodostamista. Tämän avulla ne luovat saman MSK-avaimen, jonka avulla luodaan CAK-avain suplikantille ja autentikointipalvelimelle. (MACsec-Deploy-Guide 2011, 9.)

802.1X-autentikointivaiheessa kytkin ei ole tietoinen suplikantin ja autentikointipalvelimen välissä tapahtuvan EAP-istunnon yksityiskohdista, jonka takia laite ei voi suoraan muodostaa salaukseen tarvittavia MSK- ja CAK-avaimia. Sen sijaan kytkin saa CAK-avaimen 802.1X -tunnistautumisen lopussa olevassa RADIUS-Access-Accept –viestin VSA attribuuteista MS-MPPE-Send-Key ja MS-MPPE-Recv-Key autentikointipalvelimelta. Näiden lisäksi palvelin palauttaa Eap-Key-Name Attribuutin. (MACsec-Deploy-Guide 2011, 9.)

Session Key Agreement-vaiheessa autentikaattori ja suplikantti mainostavat toisilleen tietojaan ja johtavat kaikki parametrit MACsec-salauksen muodostamiseen. Nämä toiminnot saadaan MKA-protokollasta. Jos molemmat ovat kykeneväisiä muodostamaan MACsec-salauksen, tulee autentikaattorista automaattisesti *”Key server”*. *Key Server* luo SAK:n CAK-avaimesta. Juuri SAK-avainta käytetään salauksen muodostamiseen linkkivälille. SAK avain ei ole pitkäaikainen avain vaan se voidaan uudistaa tietyin väliajoin tarvittaessa. Suplikantin täytyy myös omistaa SAK-avain, jotta liikennettä voidaan salata. Kyseinen avain salataan kytkimellä CAK:sta johdetuilla avaimilla

sekä AES Key Wrap-ominaisuudella ja lähetetään suplikantille. (MACsec-Deploy-Guide 2011, 9.)

Session Secured-vaiheessa suplikantti ja kytkin ovat asentaneet SAK-avaimen ja pystyvät lähettämään sekä vastaanottamaan salattua liikennettä. Yleisesti ottaen, liikenne, jota ei ole salattu, pudotetaan. (MACsec-Deploy-Guide 2011, 9.)

4 Toteutusympäristö

Opinnäytetyössä käytetty ympäristö pohjautui työharjoittelussa kesällä 2013 suunniteltuun ympäristöön. Tarkoituksena oli, että Cisco TrustSec- ominaisuudet tuotaisiin jo olemassa olevaan ympäristöön ja tätä kautta saataisiin tietoa käyttöönoton haastavuudesta tai helppoudesta. Uutena lisänä verkkoon tuotiin WLAN-liikennöinnin mahdollistavat laitteet, sekä lisää kytkimiä mm. SGT-testauksia silmälläpitäen.

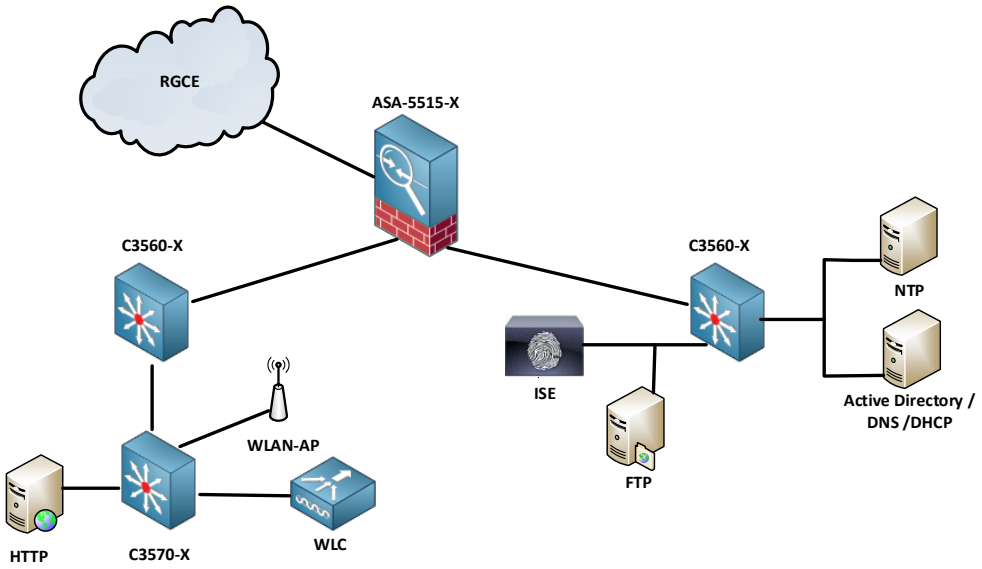
Opinnäytetyössä käytetty laitteisto koostui pääosin Cisco Systems:in laitteista. Taulukossa 4 on esitetty työn verkkoympäristön laitteisto kappalemäärineen, sekä ohjelmistoversioineen.

Taulukko 4. Ciscon laitteisto työssä

LAITE	KPL	Versio
Cisco C3560-X	2	IOS 15.2
Cisco C3570-X	1	IOS 15.2
Cisco ASA-5515-X	1	ASDM (7.1)/ ASA (9.1)
Cisco ISE	1	1.2 (Patch 7)
Cisco AIR-LAP1131	1	7.4
Cisco 2504 WLC	1	7.4

Palveluista käytössä olivat vain oleellisimmat. Nämä palvelut olivat Active Directory, DNS, DHCP, NTP ja FTP. Active Directory, DNS, sekä DHCP oli sijoitettu Windows Server 2008 R2 – palvelimelle ja NTP/FTP CentOS 6.3 –palvelimille. Sisäverkon NTP ja DNS yhdistettiin RGCE:ssä oleviin vastaaviin palveluihin. FTP- palvelinta käytettiin konfiguraatioiden varmuuskopioimiseen, palomuurisääntöjen kohteenasekä mm. PAC-tiedostojen siirtämiseen ASA:lle. Sisäverkossa oli myös HTTP-palvelin, jota käytettiin SGFW-ominaisuuksien testaamiseen.

Opinnäytetyön verkkoratkaisu palveluineen on esitetty kuviossa 26. Uusina laitteina verkkoon liitettiin Cisco Aironet AP, Cisco WLC 2504 , Cisco Catalyst 3750X–L3-kytkin ja Cisco ISE.



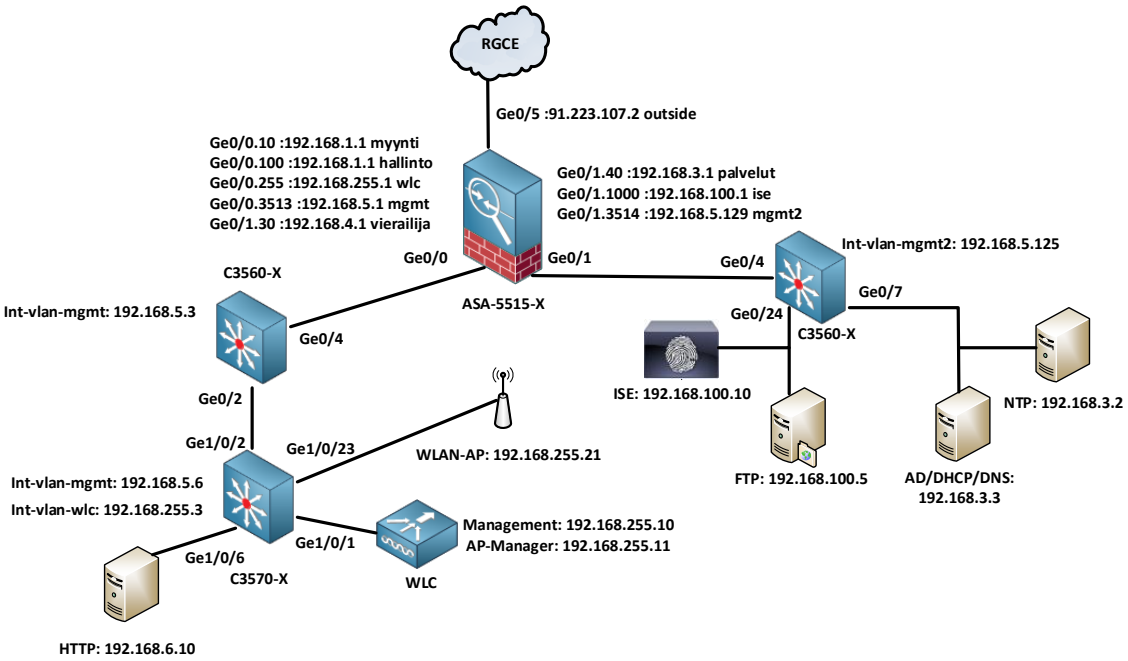
Kuvio 26. Opinnäytetyön verkkoratkaisu

Verkkoympäristössä oli käytössä myös eri VLAN:eja, jotka jätettiin verkkoon kesällä 2013 tehdyn ympäristön ratkaisusta. Uusina VLAN:eina verkkoon lisättiin WLC- ja ISE. Taulukossa 5 on listattu verkossa olevat VLAN:it, sekä niiden osoiteavaruudet.

Taulukko 5. VLAN:it ja osoiteavaruudet

VLAN	NIMI	OSOITEAVARUUS
10	MYYNTI	192.168.1.0 /25
30	VIERAILIJA	192.168.4.0 /24
40	PALVELUT	192.168.3.0 /24
100	HALLINTO	192.168.6.0 /24
255	WLC	192.168.255.0 /24
1000	ISE	192.168.100.0 /24
3513	MGMT	192.168.5.0 /25
3514	MGMT 2	192.168.5.128 /25

Kuviossa 27 on esitetty fyysinen kuva sekä toiminnan kannalta oleelliset palvelut.



Kuvio 27. Verkkoympäristön fyysinen kuva

Verkkoratkaisussa ei otettu huomioon vikasietoisuutta, sillä se ei vaikuttanut ominaisuuksien testaamiseen. ASA-5515X toimii verkon liitospisteenä RGCE-ympäristöön, joten sillä toteutettiin myös osoitemuunnokset (PAT) ”julkiseen” osoitteeseen. Palvelut olivat alkuperäisillä paikoillaan lukuun ottamatta Centos FTP-palvelinta ja HTTP-palvelinta.

5 Työn toteutus

5.1 Toteutuksen vaiheet ja TrustSec-ominaisuudet verkossa

Työ oli järkevää jakaa erilaisiin vaiheisiin, sillä erilaisia toiminnallisuuksia oli useita, joiden kytkeminen päälle tulisi väistämättä aiheuttamaan ongelmia muiden toiminnallisuuksien kanssa. Karkeasti katsoen työn toteutus jakautui seuraaviin vaiheisiin:

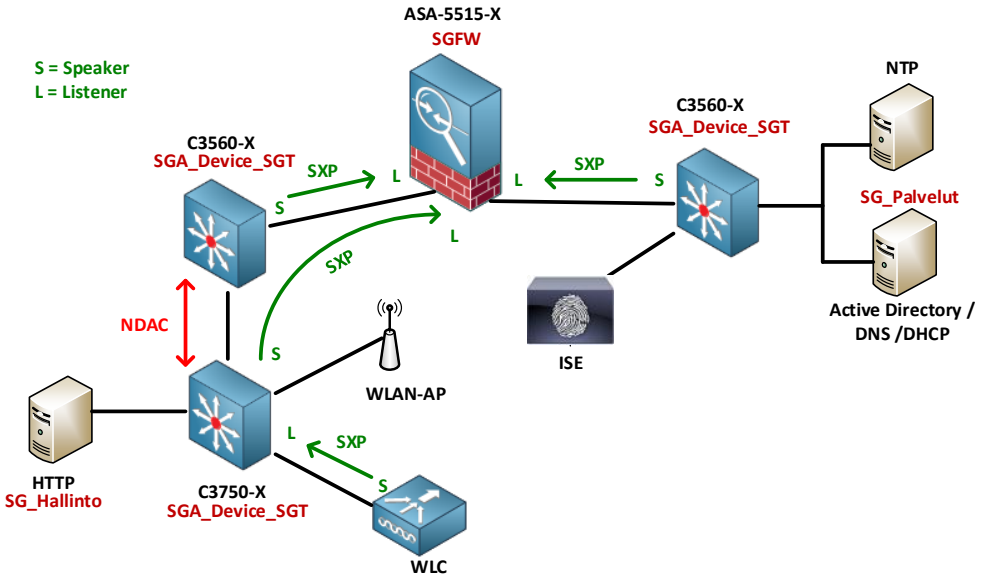
- Suunnittelu ja mahdollisten rajoituksien selvittäminen, sekä uusiin laitteisiin tutustuminen
- Verkon rungon toiminnan testaaminen
- Testausten suorittaminen ja todentaminen TrustSec-ominaisuuksilla

Työ aloitettiin tutustumalla TrustSec-ratkaisun komponentteihin, sekä niitä mahdollisesti koskeviin rajoituksiin. Komponentteja ratkaisussa on erittäin paljon, joten niiden yhteistoimintaan tuli kiinnittää erityisen paljon huomiota. Ratkaisussa päädyttiin testaamaan NDAC-ominaisuutta, 802.1X-autentikointia, SXP:tä, SGFW:ia ja VPN-kirjautumista ladattavan pääsylistan kanssa. Oleellisena osana olivat SGT-leimat, jotka on esitetty taulukossa 6.

Taulukko 6. SGT-leimat verkossa

NIMI	SGT
SGA_Device_SGT	2
SG_Palvelut	3
SG_Hallinto	4
SG_WLAN	8
SG_WLC	7
Unknown	0

Kuviossa 28 on esitetty TrustSec-ominaisuudet verkkoratkaisussa NDAC:n, SGT-leimojen ja SXP:n osalta.



Kuvio 28. TrustSec-ominaisuudet ympäristössä

Kytkimien C3560X-Upper ja C3750X-stack välillä suoritettaisiin NDAC-autentikointi ja MACsec-salaus. SXP konfiguroitiin myös kytkinten, WLC:n ja ASA:n välille kuvion mukaisesti. Palveluille liitettiin staattinen SGT (SG_Palvelut) kuten myös HTTP-palvelimelle (SG_Hallinto). ASA:lla käytettiin hyväksi SGFW-ominaisuutta.

Rajoitusten tutkimisen ja suunnittelun jälkeen vuorossa oli uusiin laitteistoihin ja alustoihin tutustuminen. Tämä oli kaikista eniten aikaa vienyt vaihe, sillä varsinkin ISE:n politiikoiden luominen oli täysin uutta, kuten myös WLC:n konfiguroiminen.

Työn toteutus alkoi palauttamalla pohjakonfiguraatiot kytkimiin ja ASA:an, jonka jälkeen testattiin yhteyksien toimiminen verkon sisällä, sekä ulos RGCE-ympäristöön. Tämän jälkeen alkoi ISE:n konfigurointi TrustSec-ominaisuuksia varten. Konfiguroitavana oli mm. SGA-komponentit, verkkolaitteet ja erilaisia sääntöjä AAA:han liittyen.

Testauksia suoritettiin myös työasemalta langallisesti ja langattomasti, joista tapahtumat kirjattiin ylös. Tässä käytettiin hyväksi mm. Anyconnect Secure Mobility Client–suplikanttia, jonka avulla autentikoitiin laite/käyttäjä verkkoon. Langallisessa 802.1X-testauksessa suoritettiin myös MACsec-salaus päätelaitteelle asti.

Toteutukseen kuului myös VPN-kirjautuminen ASA:n ulkorajapintaan AnyConnect-VPN-moduulilla. Kyseisessä tilanteessa ei pystytty vielä käyttämään SGT-leimoja, sillä

ominaisuus ei ollut vielä mahdollinen työn toteutuksen aikana. Kirjautuminen käsitti siis ainoastaan autentikointipyynnön siirtämisen ISE:lle ja ladattavan pääsylistan avulla liikenteen kontrolloinin sisäverkossa.

Testattavana oli myös ASA:n SGFW-ominaisuus, jossa liikennettä estettiin ja sallittiin perustuen SGT-leimoihin. Testauksia suoritettiin yksinkertaisesti mm. estämällä HTTP-liikenne tietyllä SGT-leimalla varustettuun palvelimeen. Sääntöjä muutettiin perustuen siihen, kirjautuuko käyttäjä esimerkiksi langallisesti tai langattomasti yrityksen verkkoon.

5.2 Konfigurointi

5.2.1 Yleistä, verkon runko ja ISE:n liittäminen AD-palvelimeen

Työn toteutus aloitettiin verkon rungon muodostavien laitteiden, eli ASA:n ja kytkinten peruskonfiguraatioista. Näihin lukeutuivat mm. fyysisten- ja alirajapintojen konfigurointi, VLAN:ien luominen, laitteiden nimeäminen jne. Kyseiset konfiguraatiot on esitetty liitteessä 1. Seuraavissa konfiguraatioissa on esitetty toimeksiantajan pyynnöstä pääsääntöisesti TrustSec-ominaisuuksiin vaikuttavat konfiguraatiot. Konfiguraatioissa ei ole esitelty esimerkiksi ISE:n rajapintojen konfiguroimista, AD-ryhmien luomista, VPN:n konfiguroimista ASA:lla jne. Laitekohtaiset konfiguraatiot on esitetty liitteessä 4. Huomioitavaa on, että liitteen 4 konfiguraatioissa esiintyy myös profilointia varten olevia komentoja. Näitä käytettiin työn aikana vain verkon näkyvyyden parantamiseen käyttäjälle keräämällä tietoa verkkolaitteista. Kattavampi profilointiominaisuuksien testaaminen ja todentaminen päätettiin siirtää jatkokehityksen osa-alueeksi.

WLC ja AP

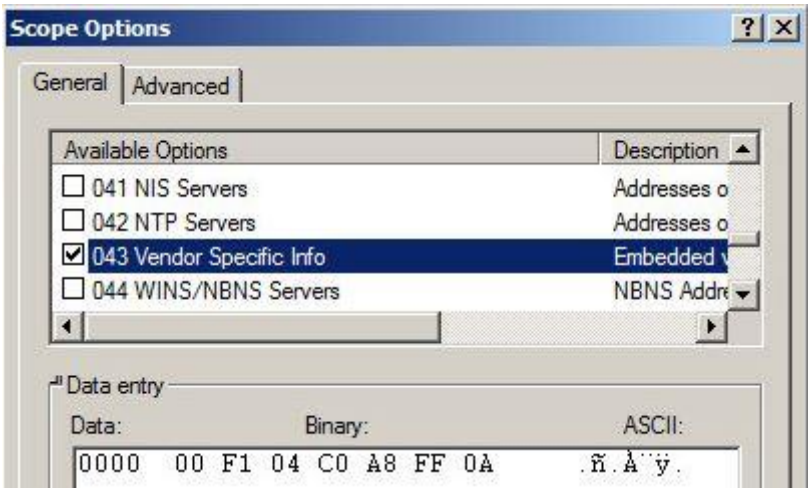
WLC:lle asetettiin staattinen IP-osoite 192.168.255.10 VLAN:sta 255 management-rajapintaan. Samasta VLAN:sta asetettiin myös osoite 192.168.255.11 AP-manager-rajapinnalle.

Ciscon Aironet AP:tä varten AD:lla sijaitsevalle DHCP-palvelimelle tuli tehdä muutoksia. DHCP-paketteihin tuli sisällyttää DHCP optio 43 (*Vendor Specific Info*). Ilman tätä optiota AP ei saa tietoa verkossa olevan WLC-laitteen management-rajapinnasta, eikä voi ottaa yhteyttä kyseiseen rajapintaan.

Optio määritetään DHCP-palvelimelle halutun jaettavan osoitealueen asetuksiin. Tässä tapauksessa käytettiin DHCP-osoiteavaruutta ”*wlc”. ”Scope Options”*-kohdasta valitaan kohta *”043 Vendor Specific Info”*. Kyseiseen optioon lisätään seuraavaksi tieto WLC:n IP-osoitteesta seuraavalla tavalla TLV-arvoksi:

- Type = 0xF1 (ei vaihdu)
- Lenght = 4 x management-rajapintojen lukumäärä hex-arvona
- Value = management-rajapinnan IP-osoite hex-muodossa

Kuviossa 29 on esitetty kuvakaappaus DHCP-palvelimelta, johon on syötetty edellämainituin toimenpitein arvot optioon 43.



Kuvio 29. DHCP-asetukset Aironet AP:ta varten

Cisco ISE ja AD-integraatio

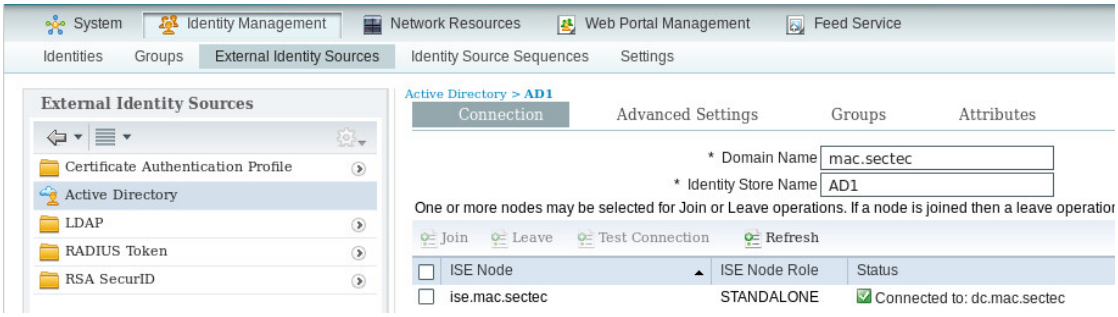
Cisco ISE liitettiin olemassa olevaan AD-ympäristöön seuraavaksi. Tarkoituksena oli, että Active Directoryn- käyttäjäkanta synkronoitaisiin ISE:n kanssa ns. ulkoiseksi iden-

titeettilähteeksi. AD: lle luotiin käyttäjä ”ciscoise”, jonka avulla ISE kirjautui toimialueeseen. Liittäminen tapahtui ISE:n käyttöliittymästä kohdasta:

> *Administration -> Identity Management -> External Identity Sources -> Active Directory -> Connection*

Liittyminen toimi-alueeseen on yksinkertaista. ”*Domain Name*”- kohtaan määritellään toimialue, jonka jälkeen asetetaan nimi ISE:lle luotavalle identiteettikannalle. Tässä tapauksessa käytettiin nimeä ”AD1”.

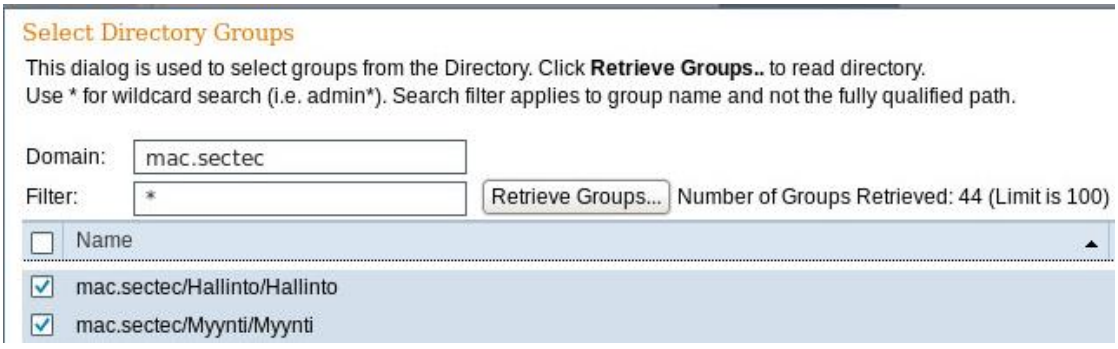
Kuviossa 30 on esitetty näkymä ISE:ltä, kun laite on liitetty onnistuneesti työssä käytettävään mac.sectec-toimialueeseen.



Kuvio 30. ISE:n onnistunut liittyminen toimialueeseen

Tämän jälkeen ”*Groups*”-välilehdeltä voidaan hakea halutut ryhmät AD-palvelimelta. Kuviossa 31 on esitetty näkymä kyseiseltä välilehdeltä. ”*Retrieve Groups*”-painikkeesta saadaan listattua ryhmät AD-palvelimelta. Jos ryhmiä on suuri määrä, voidaan hakutulokset suodattaa ”*Filter*”- laatikkoon syötettävien parametrien avulla.

Kuviossa 31 on esitetty AD-ryhmien valitseminen.



Kuvio 31. AD-ryhmien valitseminen

Haettavia ryhmiä olivat mm. ”Hallinto”, ”Myynti”, ”Domain Admins” ja ”Domain computers”. Kyseisiä ryhmiä tullaan käyttämään testauksien identiteettiryhminä.

5.2.2 SGA

ISE

Security Group Access-ominaisuuksien konfigurointi aloitettiin luomalla ryhmä verkkolaitteille. Ryhmä luodaan ISE:llä kohdasta

Administration -> Network Resources -> Network Device Groups

Kuviossa 32 on esitetty kuvakaappaus *“TRUSTSEC”*-ryhmän luomisesta.

Kuvio 32. Network Device Group luonti

Tämän ryhmän alle luodaan toiset kaksi ryhmää painikkeesta *”Add”*. Luotava ryhmä on *”TRUSTSEC-Device”*, jonka tyypiksi valitaan *”TRUSTSEC”*. Kyseistä ryhmää tullaan käyttämään NDAC-valtuutussäännössä myöhemmin.

Kaikki verkkolaitteet tulee lisätä ISE:lle, jotta halutut TrustSec-ominaisuudet saadaan käyttöön. Laitteiden lisääminen tapahtuu kohdasta:

Administration -> Network Devices

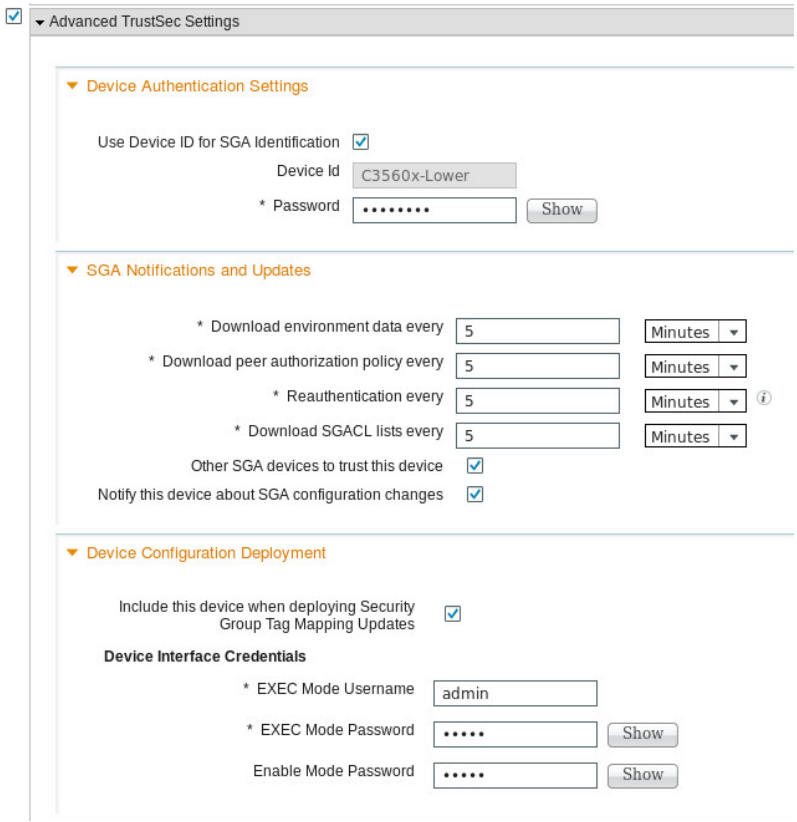
Uusi laite lisätään *”Add”*-kohdasta. Laitteen perustietoihin määritellään nimi, sekä laitteen IP-osoite. *”Network Device Group”*-kohdasta määritellään halutessa laitteen

tyyppi ja sijainti. Samassa asetetaan laite myös kuuluvaksi aiemmin luotuun *”TRUSTSEC-Devices”*-ryhmään.

Seuraavaksi *”Authentication Settings”*-kohdasta määritellään RADIUS-autentikointia koskevat asetukset. *”Shared Secret”*-kohtaan asetetaan käytettävä jaettu salaisuus. Tämä asetus määritellään WLC:lle, joka ei tue PAC-tiedostoja.

Verkonvalvonnan kohdalla käytössä oli myös SNMP. Laitekohtaisesti SNMP-asetukset määriteltiin kohtaan *”SNMP Settings”.* Versioksi valittiin 2c ja *”SNMP RO Community”*-asetukseen laitettiin käytettävä salasana. SNMP:n avulla laitteilta voidaan myös kerätä tietoa profilointiin liittyen mm. CDP:n muodossa.

Viimeisenä verkkolaitteen asetuslistassa on *”Advanced TrustSec Settings”*. Nämä asetukset mahdollistavat TrustSec-ominaisuuksien käyttämisen niitä tukevien verkkolaitteiden kohdalla. Kuviossa 33 on esitetty näkymä *”Advanced TrustSec Settings”*-kohdasta:



Kuvio 33. Advanced TrustSec Settings verkkolaitteilla

”Device Authentication Settings”-alavalikosta voidaan määrittää, käytetäänkö TrustSec -tunnistautumiseen aiempana *”Name”*-kohdassa määritettyä nimeä vai valitaanko käytettäväksi jokin muu. Käytettäessä aiemmin määriteltyä nimeä, laitetaan ruksi kohtaan *”Use Device ID for SGA Identification”.* Kyseinen *”Device ID”* ja *”Password”*-pari mahdollistaa laitteen tunnistamisen TrustSec-ympäristössä sekä PAC-tiedoston lataamisen. Kytkimille tulee asettaa myös samat tiedot, jotta keskustelu ISE:n kanssa onnistuisi ja tarvittavat SGA-parametrit saadaan kytkimille. Tämä on esitetty myöhemmin.

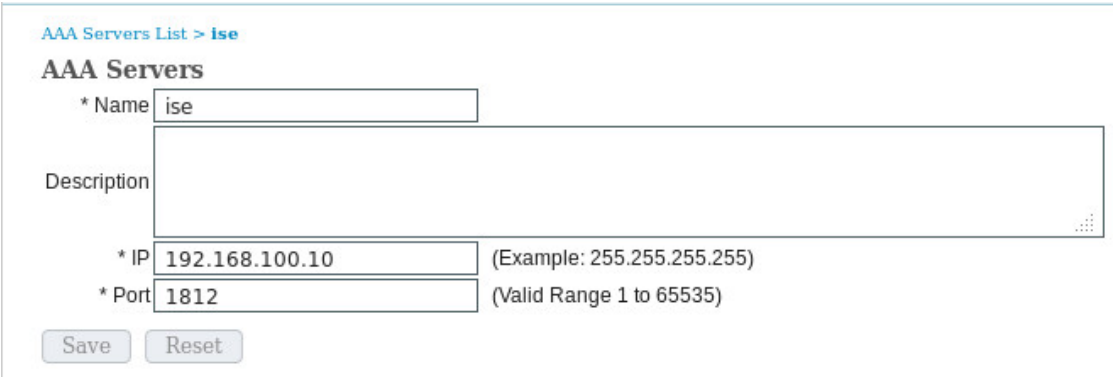
”SGA Notifications and Updates”-kohdasta määritetään asetukset, jotka määrittelevät mm. kuinka usein laite lataa SGA:han liittyvän datan ISE:ltä, luottavatko muut SGA-laitteet kyseiseen laitteeseen jne. Testaustarkoituksessa arvoiksi asetettiin 5 minuuttia, jotta mahdolliset muutokset nähtäisiin laitteilla pikimmiten. *”SGACL”*-asetusta ei tarvita, sillä kyseistä ominaisuutta ei käytetä.

ISE:ltä voidaan myös mm. päivittää SGT-mapping-tietoja suoraan kytkimille. Tätä varten määritetääm ISE:lle kytkimen *”EXEC-mode”* –käyttäjätunnus ja salasana, sekä salasana *”Enable”*- tilaan. Ominaisuutta varten kytkimille tulee myös kytkeä SSH-päälle, jonka konfigurointi on esitetty myöhemmin.

SGA:ta varten tulee määritellä lista AAA-palvelimista, joihin autentikoituneet verkkolaitteet ottavat yhteyttä RADIUS-viestien kanssa. Tämä lista sisältää tiedot kaikista käytettävistä AAA-palvelimista, jotka tukevat SGA-komponentteja. Työssä oli käytössä vain yksi palvelin, joka määriteltiin listalle kohdasta:

Administration -> Network Resources -> SGA AAA Servers

Kuviossa 34 on esitetty näkymä ISE-palvelimelta kyseiseltä välilehdeltä.



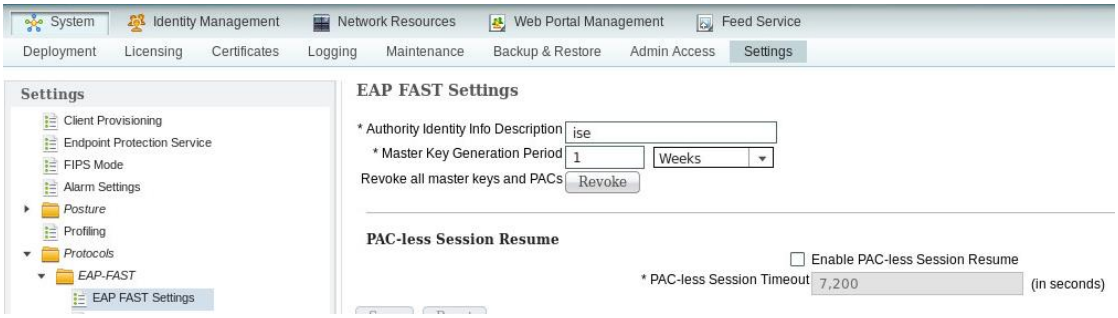
Kuvio 34. SGA-AAA-palvelimet

Välilehdeltä määritetään palvelimen nimi, valinnainen kuvaus, sekä palvelimen IP-osoite ja portti.

EAP-FAST:ia ja PAC-tiedostojen luontia varten ISE:ltä muutetaan protokollakohtaisia asetuksia. Asetuksiin pääsee kohdasta:

> *Administration -> System ->Settings ->Protocols -> EAP-FAST ->EAP-FAST Settings*

Kuviossa 35 on esitetty näkymä EAP FAST-asetussivulta:



Kuvio 35. EAP-FAST asetukset ISE:llä

”Authority Identity Info Description”-kohtaan asetetaan helposti tunnistettava nimi, joka mm. näkyy ladatuissa PAC-tiedostoissa. Nimeksi asetettiin ”ise”. Muut asetukset jätettiin oletusarvoille.

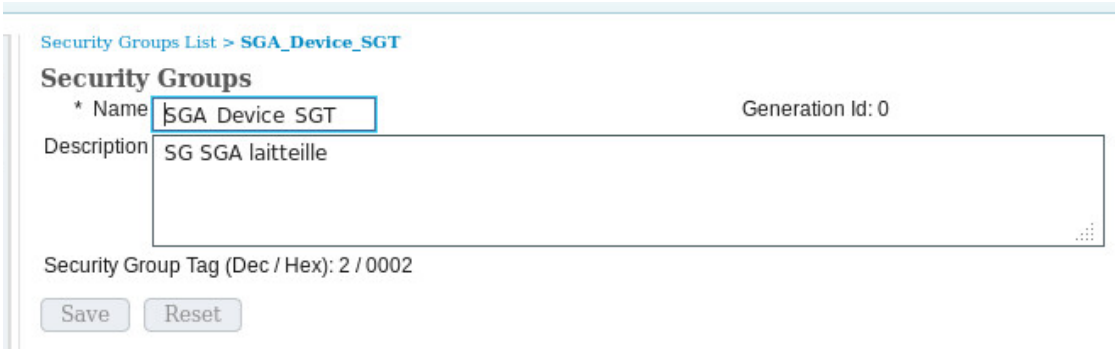
Tämän jälkeen luotiin käytettävät Security Groupit ja niitä vastaavat SGT-arvot. Arvot SGT-leimoille voidaan asettaa manuaalisesti tai niin, että ISE asettaa automaattisesti

arvon uudelle luodulle ryhmälle. Työssä käytettiin jälkimmäistä vaihtoehtoa. Huomioitavaa on, että SGT arvolla 0 on varattu ryhmälle *”Unknown”*.

SGT luonti tapahtuu ISE:llä kohdasta:

Policy -> Policy Elements -> Results -> Security Group Access -> Security Groups

”Add”-painikkeesta voidaan lisätä uusi ryhmä. Huomioitavaa on, että numerointi on aina ylöspäin kasvava, joten ryhmän poistaminen ei vapauta käytössä ollutta SGT-arvoa. Kuviossa 36 on esitetty SG-ryhmän luonti verkkolaitteille.



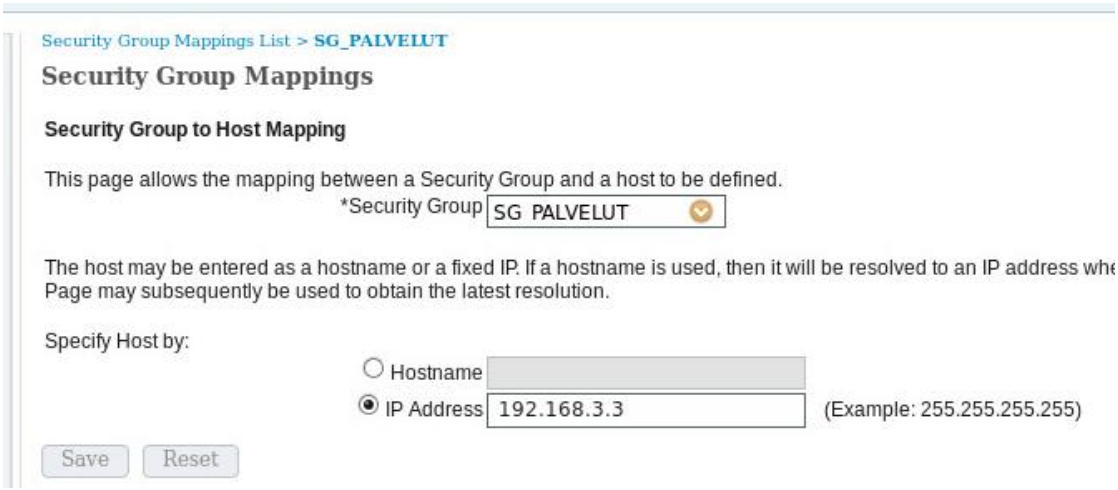
Kuvio 36. SGT luonti verkkolaitteille

Ryhmää luodessa määritetään nimi, sekä valinnainen kuvaus.

Työssä käytettiin myös staattisesti määrättyjä SGT-leimoja. Staattiset arvot määriteltiin kohdasta

Policy -> Policy Elements -> Results -> Security Group Mappings

Kuviossa 37 on esitetty kuvakaappaus staattisten SGT leimojen määrittelemisestä IP-osoitteen mukaan.



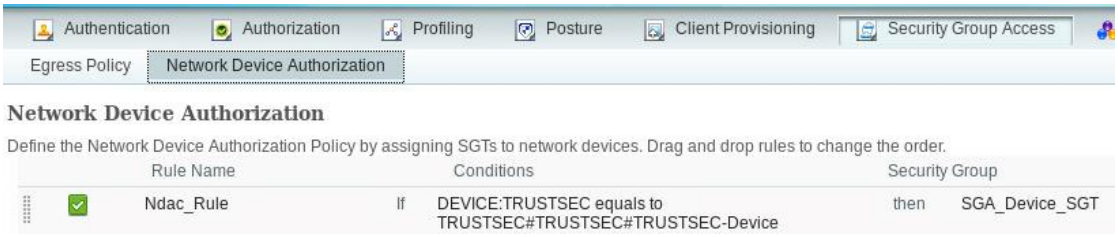
Kuvio 37. staattinen SGT määritelmä

Staattiset SGT-arvot luodaan lisäämällä haluttu SG sekä IP-osoite. Staattisia määrityksiä käytettiin mm. palvelut VLAN:issa sijaitsevalla AD:lla ja NTP-palvelimella sekä hallinto VLAN:issa sijaitsevalla http-palvelimella. Painikkeesta *”Deploy”* voidaan asettaa ISE päivittämään staattiset tiedot verkkolaitteille SSH:n avulla.

NDAC-autentikointia varten määritetään valtuutussääntö, jolloin autentikoituvalle verkkolaitteelle annetaan aiemmin luotu SGT (SGA_Device_SGT)

Policy -> Security Group Access -> Network Device Authorization

Kuviossa 38 on esitetty kuvakaappaus kyseisestä säännöstä.

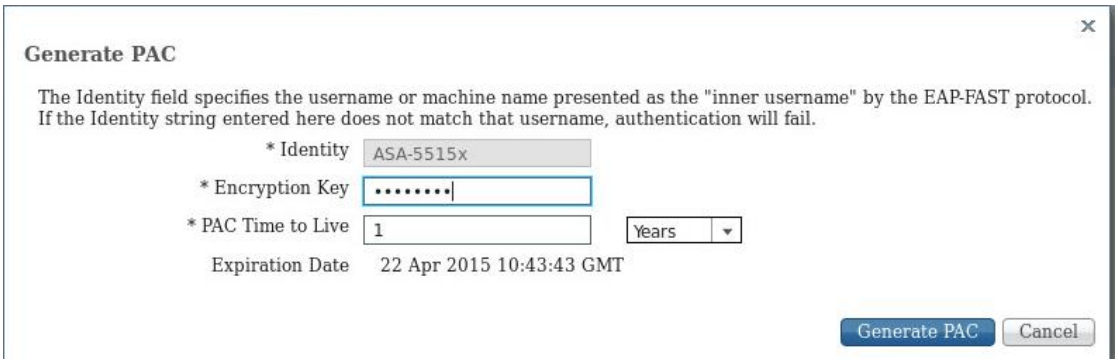


Kuvio 38. NDAC-valtuutus-säännön luominen

”Conditions”-kohdasta määritellään laitteen tyypiksi aiemmin luotu ryhmä *”TrustSec-Device”*. Tämän jälkeen *”Security Group”* kohtaan asetetaan verkkolaitteille tarkoitettu SGT-leima nimeltä *”SGA_Device_SGT”.* Tämän jälkeen onnistuneen NDAC-autentikoinnin päätteeksi verkkolaitteelle määrätään oikea SGT-leima.

ASA:n liittäminen Trustsec-ratkaisuun

ASA ei voi saada dynaamisesti PAC-tiedostoa ISE:ltä, joten se joudutaan siirtämään muulla tavalla. PAC-luodaan ASA:lle *”Network Devices”* –valikosta. Kuviossa 39 on esitetty ASA:n PAC-luonti.



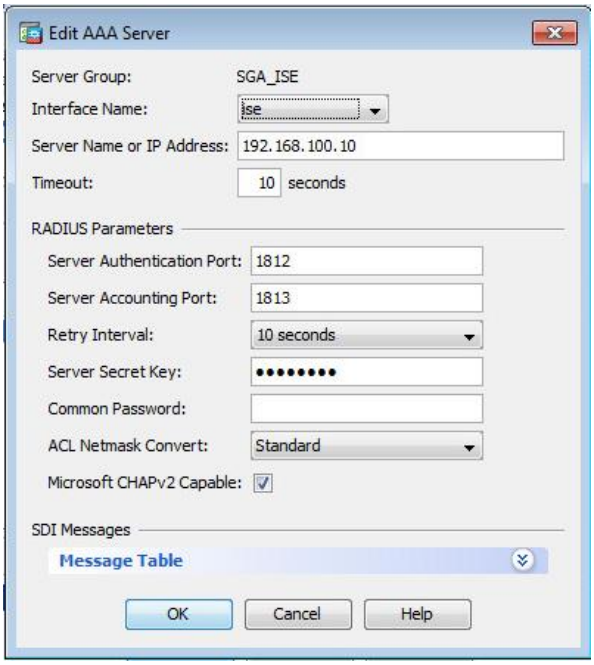
Kuvio 39. ASA:n PAC-tiedoston luonti

Määriteltävänä on mm. salausavain ja PAC-:n elinaika.

ASA:n puolelta täytyy määrittää ISE käytettäväksi RADIUS-palvelimeksi SGA-toimintoja varten. Tämä tapahtuu kohdasta

Configuration -> Firewall -> Identity by TrustSec -> Server Group Setup

”Manage”-painikkeesta lisätään uusi AAA-palvelinryhmä oletusasetuksilla kohdasta *”AAA Server Groups”*. Kyseiseen ryhmään lisätään tämän jälkeen tiedot ISE:stä. Kuviossa 40 on esitetty kuvakaappaus ASDM:ltä kyseisestä kohdasta.



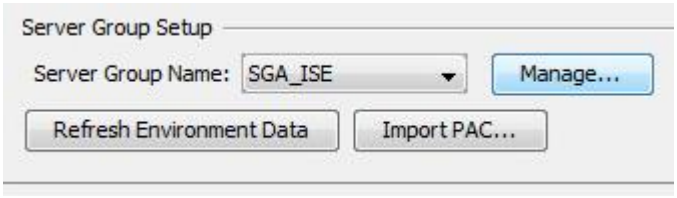
Kuvio 40. AAA-palvelimen lisäys ASA:lla

Määritettävänä on mm. rajapinnan nimi, jonka takana ISE sijaitsee, käytettävät portit (1812 ja 1813) sekä salainen avain.

PAC-tiedosto siirretään seuraavaksi ASA:lle. Siirtämiseen käytettiin FTP-palvelinta, josta PAC-voidaan helposti ladata käytettäväksi. Tiedosto siirrettiin ASA:n ASDM-hallintaan käytettävän Win7-virtuaalityöaseman työpöydälle FTP-palvelimelta. Tämän jälkeen PAC-asennus suoritetaan ASDM –kohdasta

Configuration -> Firewall -> Identity by TrustSec -> Server Group Setup -> Import PAC

Kuviossa 41 on esitetty näkymä kyseisestä kohdasta.



Kuvio 41. PAC asennus ASA:lle

Tämän jälkeen PAC-siirretään ASA:lle työasemalta. Asennus vaatii salaukseen käytettävän salasanan syöttämisen. Onnistunut PAC-tiedoston asennus tulostaa ASDM:llä

ilmoituksen *”PAC Imported successfully”*. Tämän jälkeen PAC-asennus voidaan todentaa esimerkiksi ASA:n CLI:stä komennolla:

cisco-asa# show cts pac

Kuviossa 42 on esitetty ASA:n tuloste kyseiselle komennolle.

```
cisco-asa# show cts pac

  PAC-Info:
    Valid until: Apr 22 2015 10:54:24
    AID:         4f8c92d489446f6c4ded974104dd721d
    I-ID:        ASA-5515x
    A-ID-Info:   ise
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b800030001000400104f8c92d489446f6c4ded974104dd721d0006009c000301
    00d235871cc933a27340e21ad3d085978e00000001534f905c00093a80a384aeb11185
    333d025574d4f08d55758d2f17bd9a5e904021ac1fe5325945968f4d41d5053df74722
    98a531c6118ae065042a0c9e82a98d020144004068a771f7d410d7cc10bc8c06610e87
    2b59d076a1d22202860dc7df21de814697a06238cd30a167e97307fc300ec11efe296e
    2278b296e9f1ac0e1496583489
```

Kuvio 42. PAC-tiedosto ASA:lla

Kuviosta voidaan havaita mm. aiemmin ISE:llä määritelty *”Authority Info Description (A-ID-Info)”* näkyy tulosteessa oikein nimellä *”ise”. ”I-ID”* – kohdassa on ISE:llä ASA:lle luotu identiteetti (ASA-5515X) TrustSec-ratkaisuun.

5.2.3 SXP:n konfigurointi

SXP konfiguroitiin käytettäväksi kytkimille, WLC:lle ja ASA:lle kuvion 28 mukaisesti. Seuraavassa esimerkissä on esitetty C3560X-Lower:in ja ASA:n välisen SXP-yhteyden muodostamisen konfiguraatiot.

Alussa SXP kytketään päälle komennolla:

C3560X-Lower(config)# cts sxp enable

Oletussalasana SXP-yhteydelle asetettiin seuraavaksi. Tätä salasanaa käytetään muodostamaan yhteys SXP-laitteiden välillä. Salasana ei ole pakollinen, mutta luonnollisesti tietoturvasyistä salasana on hyvä asettaa laitteisiin luvattoman yhteydenmuodostuksen estämiseksi.

C3560X-Lower(config)# cts sxp enable default password ciscocts

Seuraavaksi määritellään vastakkaisen laitteen(peer) asetukset SXP-yhteyden muodostamista varten. Tässä tapauksessa määriteltiin ASA:n IP-osoite, käytettävä salasana, sekä ASA:n rooli SXP yhteydessä. Rooliksi asetettiin ”listener”, sillä ASA vastaanottaa SGT-tiedot kytkimeltä. Edellä mainitut toimenpiteet asetettiin komennoilla:

C3560X-Lower(config)# cts sxp connection peer 192.168.100.1 password default mode peer listener

ASA:lle asetettiin vastaavasti kytkimen C3560X-Lower rooliksi *”Speaker”*.

Tämän jälkeen konfiguroidut laitteet muodostavat keskenään SXP-yhteyden. Seuraavalla komennolla voidaan tarkastaa SXP-yhteyden tiedot:

C3560X-Lower# show cts sxp connections

Kuviossa 43 on esitetty yhteyden muodostumisen todennus C3560X-Lower–kytkimeltä.

```
C3560X-Lower#show cts sxp connections
 SXP                : Enabled
 Highest Version Supported: 3
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP           : 192.168.100.1
Source IP         : 192.168.100.125
Conn status       : On
Conn version      : 2
Local mode        : SXP Speaker
Connection inst#  : 1
TCP conn fd       : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:11:09 (dd:hr:mm:sec)

Total num of SXP Connections = 1
```

Kuvio 43. SXP-todennus kytkimellä C3560X-Lower

Kuviosta voidaan havaita, että yhteys muodostui onnistuneesti sillä *”Conn status”* kohdassa lukee *”On”*. Jos yhteys olisi muodostumisvaiheessa, kyseinen kohta ilmoittaisi *”Pending”*. Muita tietoja ovat mm. IP-osoitteet, käytetty SXP-versio ja paikallisen laitteen SXP-rooli.

WLC:n kohdalla SXP:n konfiguroiminen tapahtui graafisen käyttöliittymän kautta. SXP konfiguroitiin käyttöön kohdasta

Security -> TrustSec SXP

Kuviossa 44 on esitetty kuvakaappaus kyseisistä asetuksista

Kuvio 44. WLC SXP konfigurointi

Asetuksiin määritellään mm. käytettävä salasana, lähdeosoite ja peer-laitteen IP-osoite. SXP tulee myös kytkeä päälle kohdasta *”SXP State”*. Roolia laitteella ei voi muuttaa, koska WLC on kykeneväinen vain toimimaan Speaker-roolissa.

5.2.4 Kytkinten konfiguraatiot TrustSec-ratkaisuun

Verkon kytkimet liitettiin TrustSec-ratkaisuun seuraavalla tavalla. NDAC-autentikointi suoritettiin kytkinten C3560X-Upper ja C3750X-stack välillä, joten ainut *”non seed”*-laite verkossa oli C3750X-stack.

Kaikkiin kytkimiin asetettiin SSH-päälle, jotta ISE:ltä voidaan tarvittaessa ottaa yhteys laitteisiin tarkastamaan esim. konfiguraatioita tai päivittämään dynaamisesti SG-taulut. Samoja tunnuksia käytetään myös kytkimeen kirjautumisessa.

```
C3560X-Lower(conf)# username admin privilege 15 password cisco
C3560X-Lower(conf)# crypto key generate rsa modulus 1024
```

Kytkimille luotiin erityiset CTS-käyttäjätiedot, joita käytetään mm. PAC-tiedoston lataamiseen dynaamisesti. Kyseiset tiedot tulee määritellä täsmälleen samalla taval-

la, kuin ISE:lle määriteltiin kyseisen laitteen *”Advanced TrustSec Settings”*-kohdassa. Seuraavassa on esitetty esimerkkinä C3560x-Lower–kytkimen konfigurointi edellä mainittuun toimenpiteeseen.

```
C3560X-Lower# cts credentials id C3560X-Lower password ciscocts
```

Kytkimen paikallista kirjautumista varten määritellään käytettäväksi paikalliset tunnukset. Samalla aktivoidaan myös AAA-palvelu käyttöön komennolla *”aaa new-model”*.

```
C3560X-Upper(config)# aaa new-model
C3560X-Upper(config)# aaa authentication login default local
```

Tämän jälkeen laitteelle määritellään 802.1X-autentikointia varten mm. käytettäväksi protokollaksi RADIUS. Samalla kytketään päälle valtuuttaminen verkkoon liittyvien pyyntöjen kohdalla. Tilastointi 802.1X:n kohdalla asetetaan start-stop-muotoon. CTS-valtuuttaminen kytketään myös päälle.

```
C3560X-Upper(config)# aaa authentication dot1x default group radius
C3560X-Upper(config)# aaa authorization network default group radius
C3560X-Upper(config)# aaa authorization network ise group radius
C3560X-Upper(config)# aaa accounting dot1x default start-stop group radius
C3560X-Upper(config)# cts authorization list ise
```

”Seed”-laitteelle määritellään tiedot käytettävästä RADIUS-palvelimesta. Määritettävänä on mm. IP-osoite, käytettävä PAC-avain ja portti autentikointia varten. Lopuksi kytkimelle asetetaan päälle VSA-attribuutit tilastointia ja autentikointia varten.

```
C3560X-Upper(config)# radius-server host 192.168.100.10 pac key ciscocts
C3560X-Upper(config)# radius-server host 192.168.100.10 auth-port 1812
C3560X-Upper(config)# radius-server vsa send accounting
C3560X-Upper(config)# radius-server vsa send authentication
```

”Non-Seed” laitteelle ei tarvitse konfiguroida AAA-asetuksista kuin seuraavat.

```
C3750X-stack(config)# aaa new-model
C3750X-stack(config)# aaa authentication login default local
C3750X-stack(config)# aaa authentication dot1x default group radius
C3750X-stack(config)# aaa authorization network default group radius
C3750X-stack(config)# aaa accounting dot1x default start-stop group radius
```

Molemmille kytkimille tulee myös kytkeä 802.1X globaalisti päälle. Tämä tapahtuu komennolla

C3560X-Upper(config)# dot1x system-auth-control

Trunk-linkille määritellään molemmalle puolelle komento, joka kytkee 802.1X ominaisuuden kytkinten välille NDAC:ia varten.

C3560X-Upper(config-if)# cts dot1x

Tässä vaiheessa konfiguraatiot ovat NDAC:ia varten valmiita. Rajapinnat tulee vielä asettaa ylös-tilaan komennolla

C3560X-Upper(config-if)# no shutdown

5.2.5 ISE:n policy EAP-FAST-Chaining-autentikointiin

EAP-Chaining-metodia varten ISE:lle luodaan erityiset säännöt, joiden avulla autentikointia ja valtuutusta kontrolloidaan. Ensin määritellään EAP FAST Chaining protokollakohtaisen asetukset ISE:llä kohdasta

Policy -> Policy Elements -> Results -> Authentication -> Allowed Protocols -> Add

Luodaan protokollakohtainen profiilit nimeltä *”EAP-FAST_EAP-Chaining”*. *”Allowed Protocols”*-kohdasta määritellään EAP-FAST –parametrit kohdasta:

Allowed Protocols -> Authentication Protocols -> Allow EAP-FAST

”MS-CHAPv2” kohdasta määritellään sisäiseksi tyypiksi EAP-MSCHAPv2. PAC-tiedostoa varten kytketään päälle kohdat *”Use PACs”, ”Allow Anonymous In-Band PAC Provisioning ja ”Allow Authenticated In-Band PAC Provisioning”.*

“Allow Authenticated In-Band PAC Provisioning”-kohdan alavaihtoehdoista asetetaan päälle *”Server Returns Access-Accept After Authenticated Provisioning”* ja *“Accept client Certificate For Provisioning”.*

Lopuksi valitaan *“Allow Machine Authentication” ja “Enable Stateless Session Resume”, sekä “Enable EAP Chaining”*-aktiiviseksi. Asetusten tallentamisen jälkeen luotu-

na on profiili, joka mahdollistaa käyttäjän ja laitteen tunnistamisen EAP Chaining menelmällä. Myös PAC-tiedostot saadaan päätelaitteelle autentikoinnin yhteydessä.

Tämän jälkeen voidaan ISE:lle luoda autentikointi-säännöt käyttäen hyväksi edellä-luotua protokolla-profiilia. Säännöt luodaan kohdasta:

Policy -> Authentication Policy

”Edit” -painikkeesta lisätään uusi sääntö, johon määritellään seuraavat asetukset. Nimeksi langalliselle 802.1X-autentikoinnille annettiin *”MACsec_EAPChaining_wired”*. *”If”*-kohdan alasvetovalikosta lisätään sääntö viittaamaan 802.1X-autentikointiin kohdasta

Condition Name -> Compound Condition -> Wired_802.1X

Seuraavaksi valitaan aiemmin luotu autentikointi-protokolla-profiili säännön kohdasta

Allow Protocols -> Allowed Protocols -> EAP-FAST_EAP-Chaining

Viimeiseksi liitetään vielä käytettävä identiteettivarasto(AD1) autentikointia varten. Tämä tapahtuu kohdasta

Use -> Identity Source -> AD1

Tallennuksen jälkeen sääntö on valmis. Tässä vaiheessa luotuna on siis sääntö autentikointia varten ISE:lle, joka mahdollistaa EAP-Chaining-käytön langallisessa 802.1X –autentikoinnissa. Käyttäjää ja laitetta verrataan myös aiemmin luotuun identiteetti varastoon *”AD1”*.

Samantyylinen autentikointi-sääntö tehdään myös langattomalle yhteydelle. Ainoana erona on käytettävä *”Compound Condition”*, johon asetetaan arvo *”Wireless_802.1X”*.

Kuviossa 45 on esitetty kuvakaappaus *”Authentication Policy”*-kohdasta, johon käytettävät säännöt on luotu.

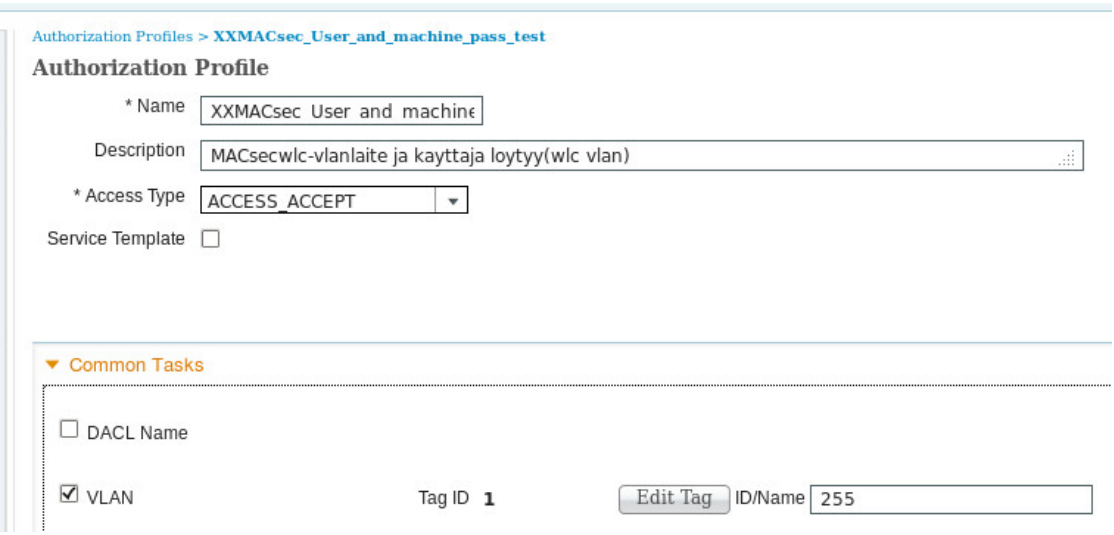
Kuvio 45. ISE Authentication Policy

Luotuna on langattomassa verkossa käytössä oleva EAP-Chaining-autentikointi-profiili, jonka identiteettilähteenä on AD1. Langallista kirjautumista varten on myös luotu samanlainen profiili, jonka identiteettilähde on sama kuin langattomassakin.

Seuraavaksi ISE:lle luodaan valtuutusprofiili langalliseen ja langattomaan 802.1X-tunnistautumiseen, johon määritellään onnistuneen autentikoinnin jälkeen kytkimelle/WLC:lle asetettavat parametrit kyseiseen autentikointitilanteeseen. Valtuutus-profiilit luodaan kohdasta:

Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles

Kuviossa 46 on esitetty kuvakaappaus profiilin luomisesta.



Kuvio 46. Valtuutusprofiilin luonti

Profiiliin lisätään testaustilanteessa käytettävät parametrit, joita ovat mm. VLAN 255, MACsec-politiikka (*Must Secure*). Nimeksi profiilille asetettiin *”XXMACsec_User_and_machine_pass”. ”Access Type”*-kohtaan määritellään tieto siitä, että käytettävä profiili kuuluu tilanteeseen, jossa ISE palauttaa autentikoinnin

seurauksena RADIUS-Access Accept-viestin. *”Common Tasks”*, kohdasta valitaan mm. VLAN arvoksi 255 ja käytettävä MACsec- politiikka arvolla *”must secure”.*

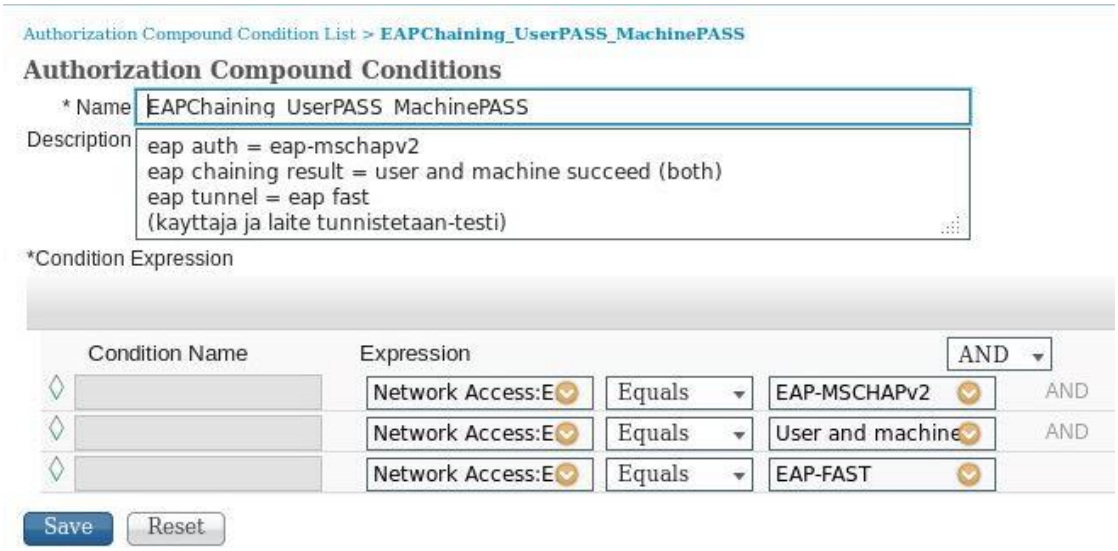
Langattomaan verkkoon kirjautumisen valtuutusprofiili luodaan vastaavalla tavalla. Nimeksi asetettiin *”User_and_machine_pass_auth”* ja VLAN-arvoksi 70. MACsec-salausta langattomassa verkossa ei voida käyttää.

Edellämainitut asetukset luovat profiilin, joka onnistuneen autentikoinnin jälkeen asennetaan kytkimen porttiin. VLAN-arvoksi määritellään 255 ja liikenne salataan MACsec-protokollalla päätelaitteelle asti langallisessa verkossa. Langattomassa verkossa laite asetetaan VLAN:iin 70.

Seuraavaksi luodaan valtuutukseen liittyvä *”Authorization Compound Condition”*, joka määrittelee edellytykset, joiden tulee täyttyä esimerkiksi EAP-Chaining-autentikoinnin kohdalla.

Kuviossa 47 on esitetty kuvakaappaus ISE:ltä kohdasta

> *Policy -> Policy Elements -> Conditions -> Authorization -> Compound Conditions -> Create Compound Condition*



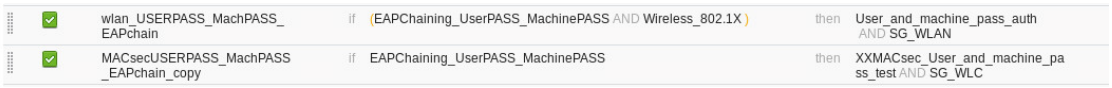
Kuvio 47. EAP Chaining Condition-määrittely

”Expression” kohtaan luodaan kolme eri määritelmää, joiden tulee täyttyä valtuutusvaiheen yhteydessä. Ensin asetetaan EAP-autentikoinnin tyypiksi *”EAP-MSCHAPv2”* kohdasta *Network Access -> EAP-Authentication.* Tämän jälkeen uuteen *”Expression”*-kohtaan määritellään vaadittava EAP-Chaining tulos. Tähän kohtaan asetetaan arvo *”User and Machine Both Succeed”*. Viimeiseen *”Expression”*-kohtaan valitaan EAP-tunnelin tyypiksi *”EAP-FAST”*. Huomioitavaa on, että operaattorin tulee olla *”AND”*, jolloin kaikkien määritelmien tulee täyttyä. Tässä vaiheessa on määriteltynä tarvittavat parametrit EAP-Chaining-menetelmää varten.

Tämän jälkeen luodaan itse valtuutuspolitiikka langallista kirjautumista varten ISE:llä kohdasta

Policy -> Authorization

Kuviossa 48 on esitetty kuvakaappaus kyseiseltä sivulta.



Kuvio 48. Valtuutussäännöt

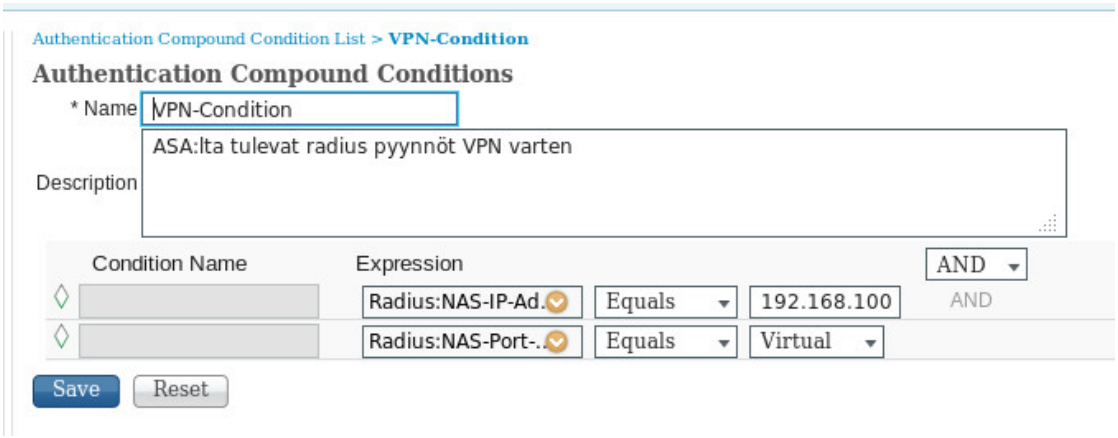
Oikealta luodaan uusi sääntö painikkeesta *”Edit”*. Nimeksi säännölle asetettiin *”MACsecUSERPASS_MachPASS_EAPChain”. ”Conditions”* kohdasta valitaan luotu määrittely *”EAPchaining_UserPASS_MachinePASS”. ”Permissions”* kohtaan valitaan luotu valtuutusprofiili *”XXMACsec_user_and_machine_pass_test”*, sekä SGT *”SG_WLC”*. Vastaavanlaisesti luotiin myös sääntö WLAN-kirjautumista varten. Eroina ovat säännön nimi, *”Conditions”*-kohdan *”Wireless_802.1X”,* valtuutusprofiili *”User_and_machine_pass_auth”*, sekä SGT *”SG_WLAN”*. Tässä vaiheessa kaikki on valmista myös valtuutuksen osalta. Valtuutusvaiheessa sääntö tarkastaa, että määritelmät EAP-Chainingia varten toteutuvat, jonka jälkeen kirjautuvalle laitteelle asetetaan oikea valtuutusprofiili sekä SGT.

5.2.6 ISE:n policy VPN:ää varten

VPN-kirjautumista varten ISE:lle luodaan myös omat säännöt, jotta ASA:lta tulevia viestejä osataan käsitellä oikein. Ensin luodaan käytettävä autentikointimääritelmä kohdasta

Policy -> Policy Elements -> Conditions -> Authentication -> Compound Conditions

Kuviossa 49 on esitetty kuvakaappaus kyseisestä sivusta.



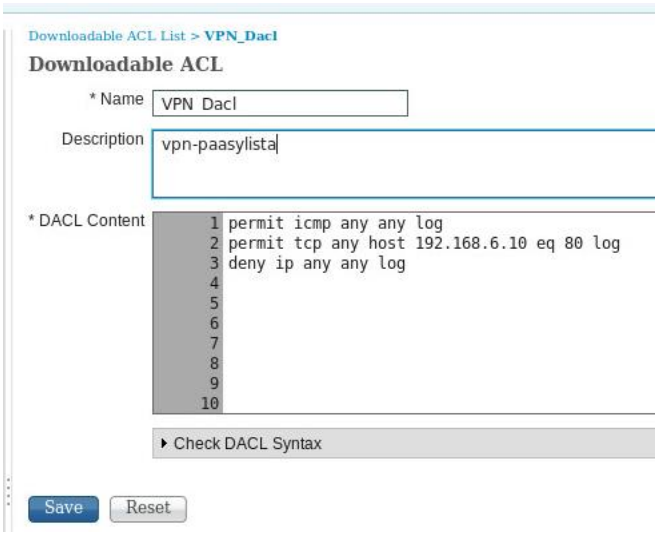
Kuvio 49. VPN määritelmät

”Add” painikkeesta luodaan uusi määritelmä. Nimeksi tulee *”VPN-Condition”*. *”Expression”* kohtaan lisätään kaksi parametria jotka ovat *”RADIUS:NAS-IP-Address equals 192.168.100.1” ja RADIUS:NAS-Port Type equals Virtual”.* Tässä vaiheessa autentikointisääntö osataan yhdistää tulevaksi ASA:lta sekä siihen, että portin tyyppi on *”Virtual”* VPN-kirjautumisen takia.

VPN-kirjautumista varten luotiin myös ladattava pääsylista (DACL), joka ASA:lle lähetetään RADIUS-Access-Accept viestin yhteydessä. Pääsylista luodaan kohdasta

Policy -> Policy Elements -> Results -> Authorization ->Downloadable ACLs”

”Add”-painikkeesta luodaan uusi pääsylista. Kuviossa 50 on esitetty kuvakaappaus pääsylistan luomisesta.



Kuvio 50. DACL-luonti

Pääsylistalle annettiin nimeksi *”VPN_Dacl”*. sisältöön määritettiin yksinkertaisia sääntöjä. Kuviossa esiintyvät säännöt sallivat ICMP-viestit mihin tahansa osoitteeseen, http-yhteyden sisäverkon palvelimeen ja kieltävät kaiken muun. Jokaiseen sääntöön on lisätty myös lokitus. Pääsylistan oikeinkirjoitus voidaan tarkistaa painikkeesta *”Check DACL Syntax”*. Huomioitavaa on, että lista ei toimi, jos säännöt on kirjoitettu väärin.

VPN-kirjautumista varten luotiin myös oma valtuutusprofiili. Valtuutusprofiilin luonti tapahtui kohdasta

Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles

Kuviossa 46 on esitetty kuvakaappaus profiilinluontisivusta. Profiiliin määritettiin nimi *”VPN_auth_success”* ja *”Access Type” ”Access Accept”.* DACL-kohtaan asetettiin luotu ladattava pääsylista nimeltä *“VPN_Dacl”*.

Tämän jälkeen luodaan autentikointi- ja valtuutussäännöt kuvioiden 44 ja 47 mukaisesti. Autentikointisäännön nimeksi asetettiin *”VPN”*, sekä *”Conditions”* määrittelyiksi *VPN-Condition”*. Identiteettilähteenä on *”AD1”*. Valtuutussääntöön asetettiin nimi *”VPN”*, sekä *”Conditions”*-kohtaan *”VPN-Authorization”*. valtuutusprofiiliksi *”Permissions”*-kohtaan asetettiin *”VPN_auth_success”.* Tässä vaiheessa VPN-kirjautumista

varten olevat säännöt ovat kunnossa. ISE osaa vastaanottaa VPN-pyynnöt ASA:lta sekä määrätä normaalin pääsyn verkkoon yksinkertaisella profiililla.

5.2.7 Anyconnect Secure Mobility Client NAM-konfigurointi

Verkkoon kirjautumiseen käytettiin hyväksi Cisco Anyconnect Secure Mobility Client-suplikanttia, johon oli asennettuna Network Access Manager-moduuli. NAM-moduulin hallintaa varten käytettiin NAM-profile editor-ohjelmaa, jolla suplikanttiin saadaan tehtyä erilliset profiilit langallista ja langatonta autentikointia varten. Kuvakaappaukset NAM profile editorista on esitetty liitteessä 2.

NAM profile editorin välilehdeltä *”Client Policy”* määritellään asetukset, joita profiilin käyttäjä voi itse muuttaa. Testauksen takia asetukset jätetään oletusarvoilleen, joten käyttäjä voi vapaasti muokata asetuksia tarvittaessa. *”Authentication Policy”*-välilehdeltä asetetaan autentikointityypit langattomiin ja langallisiin yhteyksiin, joita profiilin käyttäjä voi käyttää kirjautuessaan. Tässä kohtaa tulee varmistaa, että aktiivisena ovat EAP-FAST ja EAP-MSCHAPv2 *”Allowed Authentication Modes”*-kohdassa sekä *”802.1x with MacSec” ”Allowed Wired Security”*-kohdassa.

Tämän jälkeen *”Networks”*-välilehdeltä lisätään autentikointi-asetukset käyttäjälle lisättyihin verkkoprofiileihin. Langallista 802.1X-autentikointia varten luodaan verkko nimeltä *”EAPChaining”*, jonka tyypiksi valitaan *”Wired”* kohdasta *”Choose Your Network Media”.*

Seuraavaksi *”Security Level”*-kohdasta valitaan käyttöön *”Authenticating Network”*. Tämä asetus asettaa käyttöön autentikoinnin, sillä verkkoon ei pääse sisään ilman onnistunutta autentikointia. *”Security”*-kohdasta valitaan käyttöön avaintenhallintaan MKA-protokolla ja salaustyypiksi *”MACsec: AES-128-GCM”*. Nämä asetukset mahdollistavat MACsec-salauksen luomisen suplikantin puolella kirjautumisen yhteydessä.

”Connection Type” määrittelee käytettävän liittymistyypin verkkoon. Tässä tapauksessa käyttäjä ja laite autentikoidaan, joten valinta on *”Machine and User Connection”. ”Machine Auth”*-kohdasta valitaan käytettävä EAP-Method yhteydelle, joka täs-

sä tapauksessa on *”EAP-FAST”. ”EAP-FAST-Settings”*-kohdasta otetaan valinnat pois asetuksista *”Validate Server Identity”* ja *”Enable Fast Reconnect”*. Sisäiseksi EAP-methodiksi laitteen autentikoinnille käytetään EAP-MSCHAPv2-protokollaa ja PAC-tiedostoja. Tämän takia valitaan aktiivisiksi *”Inner Methods based on Credentials Source”*-kohdan *“Authenticate using a Password”*-asetusten kohdat *“EAP-MSCHAPv2”* ja *“If Using PACs, allow unauthenticated PAC provisioning”.* Lopuksi sivun alalaidasta valitaan kohta *“Use PAC’s”*.

“PAC Files”-välilehti jätetään oletusarvojen mukaisesti tyhjäksi, sillä PAC-tiedosto ladataan ISE:ltä dynaamisesti kirjautumisen yhteydessä. *”Credentials”*-välilehdeltä määritetään yhteys käyttämään laiteautentikointiin laitteen nimeä. Tämä asetus määritellään *Machine Credentials”*-kohdan valinnalla *”Use Machine Credentials”*. Muut asetukset sivulta jätetään oletusmuotoon.

”User Auth”-välilehdeltä määritetään asetukset käyttäjän autentikointiin liittyen. Nämä asetukset ovat samanlaiset kuin *”Machine Auth”*-välilehden asetukset. Vastaavasti myös seuraavan *”PAC Files”*-välilehden määritykset jätetään tyhjäksi aiemman *”PAC Files”* määritysten tapaan.

”Credentials”-välilehdeltä valitaan *”User Credentials”*-kohdasta asetus *”Use Single Sign On Credentials”*, jolloin käyttäjän ei yhteyden katketessa tarvitse syöttää salasanaa joka kerta uudestaan.

Tämän jälkeen profiili langallista yhteyttä varten on valmis. Seuraavaksi luodaan asetukset langatonta yhteyttä varten. Lisätään uusi verkko *”Networks”*-välilehdeltä. Asetukset ovat vastaavat langallisen yhteyden kanssa lukuun ottamatta muutamaa asetusta. *”Media Type”*-kohdasta määritellään nimeksi *”EAPChainingwireless”.* Saman sivun *”Choose Your Network Media”*-kohdasta valitaan käytettäväksi langaton Wi-Fi-yhteys. Asetuksiin määritetään langattoman verkon SSID-tunnus, joka tässä tapauksessa on *”ciscocts”*. Verkko on piilotettu, joten valitaan myös asetus *”Hidden Network”*. Lopuksi langattoman profiilin asetuksista muutetaan vielä *”Security Level”*-kohdasta käytettävä WPA-tila, johon asetetaan *”WPA Enterprise (AES)”*.

Lopuksi konfiguraatio-profiili tallennetaan vielä polkuun

C:\Programdata\Cisco\Cisco Anyconnect Secure Mobility Client\Network Access Manager\newConfigfiles

Huomioitavaa on, että tallennettavan XML-tiedoston nimi tulee olla nimetty *”configuration.xml”* ilman heittomerkkejä. Mikään muu tiedoston nimi ei käy. Asetukset tulevat voimaan vasta, kun Anyconnect-Clientin hallitsemat verkkorajapinnat käynnistetään uudestaan. Tämä suoritetaan helpoiten Windowsin tehtäväpalkin ilmaisinalueen Anyconnect-ikonista painamalla hiiren oikeaa painiketta ja valitsemalla *”Network Repair”*.

Tässä vaiheessa konfiguraatiot ovat suplikantin osalta valmiit. Luotuna on profiilit niin langalliselle, kuin langattomallekkin yhteydelle ja joissa molemmissa on käytössä EAP-FAST-Chaining. Molemmissa tapauksissa laite ja käyttäjä autentikoidaan EAP-FAST-tunnelin sisällä.

5.2.8 Kytkimen ja WLC:n konfiguroiminen 802.1X autentikointeja varten

Kytkimen konfiguroiminen langallista autentikointia varten on esitetty seuraavassa.

```
C3750X-stack(config)# interface GigabitEthernet 1/0/10
C3750X-stack(config-if)# switchport mode access
C3750X-stack(config-if)# authentication order dot1x
C3750X-stack(config-if)# authentication port-control auto
C3750X-stack(config-if)# macsec
C3750X-stack(config-if)# mka default-policy
C3750X-stack(config-if)# dot1x pae authenticator
C3750X-stack(config-if)# spanning-tree portfast
```

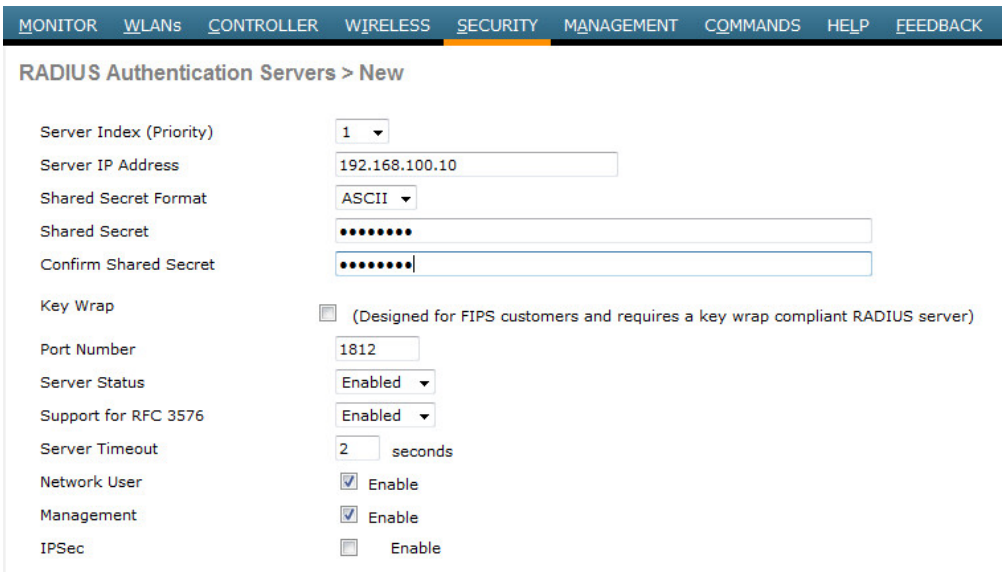
Rajapinta konfiguroitiin access-portiksi, jonka jälkeen määriteltiin käytettäväksi vain 802.1X-autentikointi. Tämän jälkeen 802.1X kytketään päälle *”authentication port control auto”*-komennolla. MACsec-politiikka saadaan ISE:ltä, mutta esille voi tulla myös tilanne jolloin kytkin ei saa määrättyä tietoa ja voi palata oletuspolitiikkaan *”mka default policy”*. Lisäksi määritellään portin tyypiksi autentikaattori komennolla *”dot1x pae authenticator”*.

Huomioitavaa on myös, että 802.1X tulee olla globaalisti kytkettynä päälle. Testaustilanteessa kytkin C370X-stack toimi seed-laitteena verkossa, jolloin käytössä oli normaalisti RADIUS-palvelin PAC tiedoston avulla.

Langatonta autentikointia varten WLC:lle lisätään tiedot ISE:stä, jotta RADIUS-viestit pystytään ohjaamaan autentikointia varten oikeaan paikkaan. WLC:llä tämä tapahtuu kohdasta

Security -> AAA -> RADIUS -> Authentication

"New"-painikkeesta lisätään uusi RADIUS-palvelin. Kuviossa 51 on esitetty näkymä WLC:llä RADIUS-palvelimen lisäämisestä.



Kuvio 51. RADIUS-palvelimen lisääminen WLC:lle

Määriteltävänä ovat mm. osoite, portti ja jaettu salaisuus. Tilastointia varten konfigurointi tapahtuu vastaavanlaisesti kohdasta

Security -> AAA -> RADIUS -> Accounting

Tämän jälkeen RADIUS-palvelin liitetään WLAN:iin *"ciscocts"*. Tämä tapahtuu kohdasta

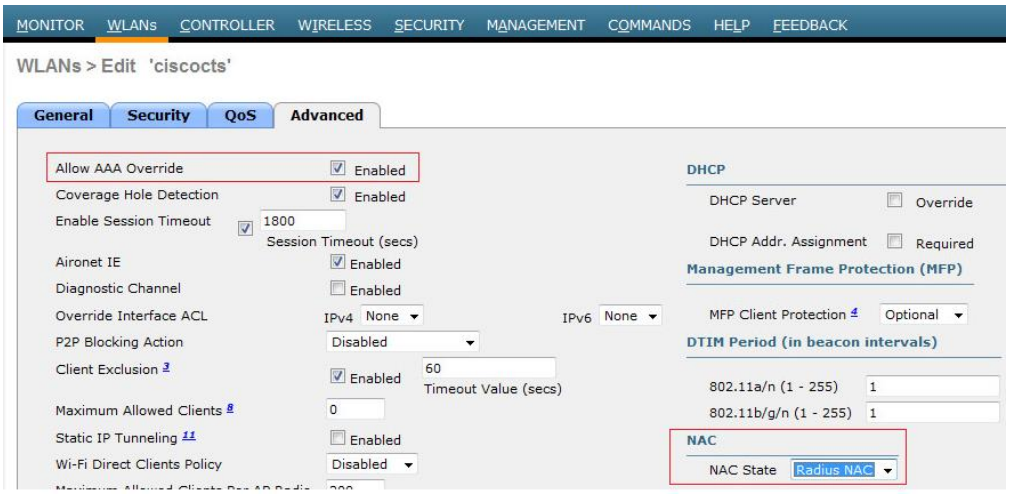
WLAN -> ciscocts -> Security -> AAA Servers

Kuviossa 52 on esitetty kuvakaappaus palvelimen lisäämisestä.

Kuvio 52. RADIUS-palvelimen lisääminen WLAN:iin

”Authentication Servers” kohtaan lisätään luotu palvelin kuten myös *”Accounting Servers”*-kohtaan. Molemmat tulee myös olla *”Enabled”* tilassa.

”Advanced”-välilehdeltä muutetaan vielä asetuksia. Kuviossa 53 on esitetty WLC:n Advanced-välilehden asetukset.



Kuvio 53. WLC Advanced-välilehti

”Allow AAA override” asetus tulee kytkeä päälle, jotta WLC pystyy asettamaan asiakkaille ISE:ltä saatavat RADIUS-attribuutit kuten VLAN:in ja SGT-leiman. *”NAC State”*-kohtaan asetetaan parametriksi *”RADIUS NAC”*, jotta ISE pystyy ilmoittamaan mm. autentikoinnin onnistumisesta.

5.2.9 ASA:n palomuurisääntöjen konfigurointi

Testaustilanteita varten ASA:lle luotiin palomuurisääntöjä perustuen SGT-leimoihin. Säännöt luodaan ASDM-kohdasta

Configuration -> Firewall -> Access Rules

Kuviossa 54 on esitetty esimerkkinä langallisen testaustilanteen säännöt, jossa käytettiin hyväksi ISE:llä määriteltyjä SG-tietoja

#	Enabled	Source Criteria:			Destination Criteria:		Service	Action
		Source	User	Security Group	Destination	Security Group		
wlc (5 incoming rules)								
1	☑	any		SG_WLC	any	SG_PALVELUT	ip	Permit
2	☑	any		SG_WLC	any	SG_Hallinto	http	Permit
3	☑	any		SG_WLC	192.168.100.5		ftp	Permit
4	☑	any		SG_WLC	any		ip	Deny

Kuvio 54. ASA:n LAN-säännöt

Rajapinnan *”wlc”* alle lisätään säännöt *”Add”*-painikkeesta. Luodaan esimerkkinä sääntö (Kuviossa toisena), joka sallii http-protokollan SG_WLC-ryhmästä SG_Hallinto-ryhmään. *”Action”* kohtaan laitetaan *”Permit”* sallimisen merkiksi. *”Source Criteria”*-kohtaan määritetään *”Source”*-arvoksi *”Any”* ja *”Security Group”* kohtaan *”SG_WLC”. ”Destination Criteria”*-kohtaan määritellään *”Destination”* arvoksi *”Any”* ja *”Security Group”* arvoksi *”SG_Hallinto”*. Lopuksi määritetään vielä haluttu palvelu (http) kohdasta *”Service”*.

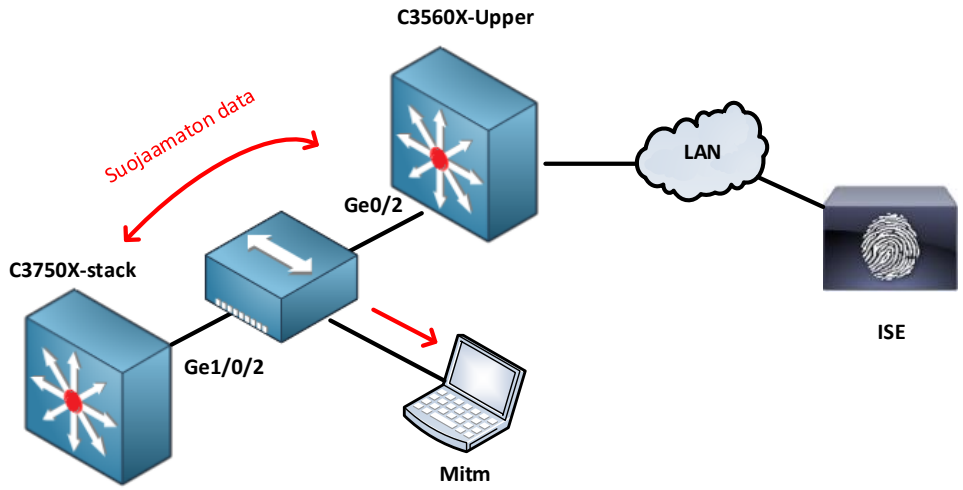
Kyseinen sääntö sallii kaikki SG_WLC-ryhmään kuuluvan http-liikenteen wlc-rajapinnasta kaikkiin SG_Hallinto-ryhmän SGT-leimalla oleviin laitteisiin.

Sääntö tehtiin myös testimielessä FTP-palvelimelle, jossa käytettiin pelkästään IP-osoitetta. Tarkoituksena oli esittää, että sääntöjä voi luoda myös pelkkiin IP-osoitteihin perustuen joko SGT-leimojen kanssa tai ilman. Lopussa on vielä sääntö, joka estää kaiken IP-liikenteen mihin tahansa kohteeseen. Konfiguraatioiden hyväksymisen jälkeen ASA luo pääsyryhmän kyseiseen rajapintaan nimellä *”wlc_in”*.

5.3 Testaukset ja todennukset

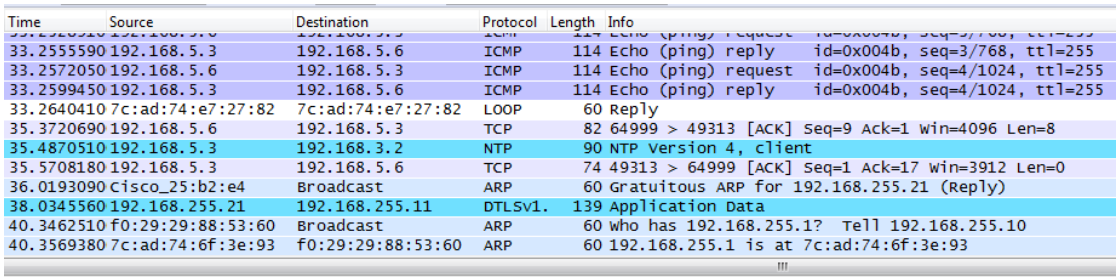
5.3.1 NDAC

NDAC-testaaminen suoritettiin C3560X-Upper- ja C3750X-stack –kytkinten välillä. MACsec salauksen testaamista varten lisättiin kytkinten väliin toistin, johon kytkettiin Wireshark–ohjelmalla varustettu kannettava tietokone kiinni. Toistimen asentamisen tarkoituksena oli todentaa mm. se, että normaali L2–liikenne ei ole kytkinten välillä oletuksena salattua millään tavalla. Toistimen toiminnallisuus perustuu siihen, että se lähettää vastaanotetut paketit jokaisesta portista ulos. Kytkimet eivät myöskään ymmärrä toistimen olemassaoloa niiden välissä. Kuviossa 55 on havainnollistettu testaustilanne ilman NDAC-autentikointia ja MACsec-salausta.



Kuvio 55. NDAC-testauksen alkutilanne

Kaikki liikenne trunk-linkillä porttien Ge1/0/2 ja Ge0/2 välillä välittyy siis myös Man in the Middle (Mitm)-koneelle. Liikenteen kaappaaminen on yksinkertaista Wireshark-ohjelman avulla. Kuviossa 56 on esitetty Wireshark kuvakaappaus alkutilanteessa, jossa NDAC–autentikointia tai linkin suojaamista MACsec:illä ei ole tapahtunut.



Time	Source	Destination	Protocol	Length	Info
33.2555590	192.168.5.3	192.168.5.6	ICMP	114	Echo (ping) reply id=0x004b, seq=3/768, ttl=255
33.2572050	192.168.5.6	192.168.5.3	ICMP	114	Echo (ping) request id=0x004b, seq=4/1024, ttl=255
33.2599450	192.168.5.3	192.168.5.6	ICMP	114	Echo (ping) reply id=0x004b, seq=4/1024, ttl=255
33.2640410	7c:ad:74:e7:27:82	7c:ad:74:e7:27:82	LOOP	60	Reply
35.3720690	192.168.5.6	192.168.5.3	TCP	82	64999 > 49313 [ACK] Seq=9 Ack=1 Win=4096 Len=8
35.4870510	192.168.5.3	192.168.3.2	NTP	90	NTP Version 4, client
35.5708180	192.168.5.3	192.168.5.6	TCP	74	49313 > 64999 [ACK] Seq=1 Ack=17 Win=3912 Len=0
36.0193090	Cisco_25:b2:e4	Broadcast	ARP	60	Gratuitous ARP for 192.168.255.21 (Reply)
38.0345560	192.168.255.21	192.168.255.11	DTLSv1.	139	Application Data
40.3462510	f0:29:29:88:53:60	Broadcast	ARP	60	Who has 192.168.255.1? Tell 192.168.255.10
40.3569380	7c:ad:74:6f:3e:93	f0:29:29:88:53:60	ARP	60	192.168.255.1 is at 7c:ad:74:6f:3e:93

Kuvio 56. Suojaamatonta liikennettä Wiresharkissa ennen MACsec-salausta

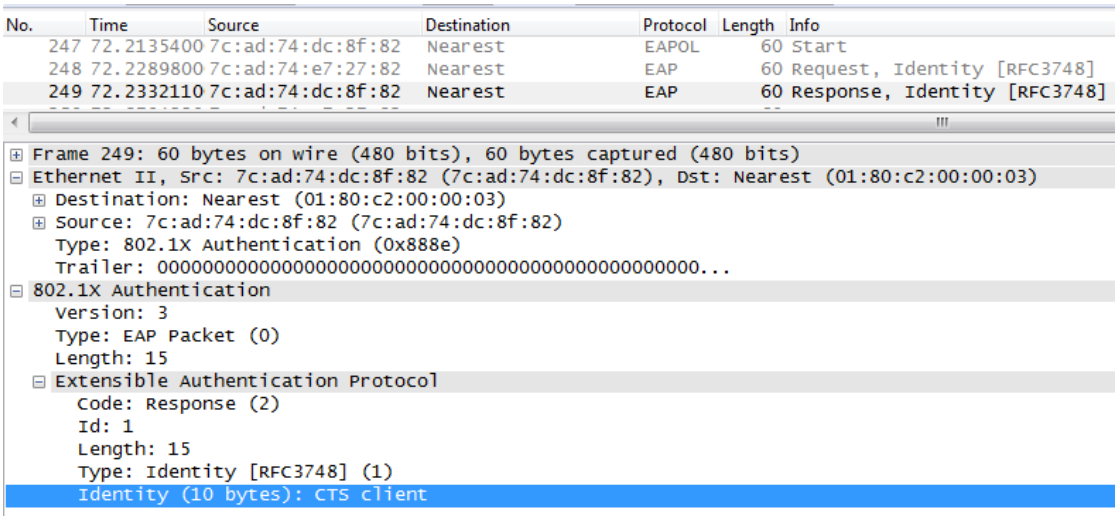
Esimerkkiviesteissä näkyvät kytkinten välillä kulkevat viestit laitteiden välissä olevalle Wireshark-koneelle.

Itse NDAC-prosessi käynnistyy heti, kun komennot on syötetty kytkimiin. Kytkimistä autentikaattorin roolin 802.1X-autentikoitiin ottaa C3560X-Upper, sillä C3750X-stack-kytkimellä ei ole tietoa RADIUS-palvelimesta. C3560X-Upper on liitetty CTS-toimialueeseen *”seed”* -laitteeksi etukäteen. Myöskään PAC-tiedostoa ei löydy kytkimeltä C3750X-stack.

Vaiheet koko prosessiin on listattu seuraavassa

- PAC-tiedoston lataus C3750X-stack-kytkimelle (EAP-FAST)
- C3750X-autentikointi (EAP-FAST)
- *”Peer policy”*-lataus
- SAP
- *”Environment Data”*-lataus

Kuviossa 57 on esitetty ensimmäiset 802.1X-viestit (EAPOL ja EAP Req/Resp-Identity)



Kuvio 57. Ensimmäiset EAP-viestit

Kuvion avatusta *”EAP-Response Identity”*-paketista voidaan havaita kytkimen C3750X-stack lähettämä identiteettityyppi. Arvona on kuviossa korostettu *”CTS client”*, joka välitetään ISE:lle RADIUS-Access-Request-paketissa *”username”* -attribuuttina C3560X-Upper-toimesta. Tämän jälkeen ISE:n ja C3750X-stack-kytkimen välille muodostuu EAP-FAST:n avulla TLS-tunneli, jota käytetään hyväksi PAC-tiedoston lataamiseen ISE:ltä. Tunneli on tässä vaiheessa vielä anonyymi, sillä PAC-tiedosto ei ole vielä siirtynyt. Tunnelin sisällä välittyvät ISE:lle kytkimelle C3750X-stack aiemmin syötetyt CTS-käyttäjätiedot MSCHAPv2-sessiossa.

Kuviossa 58 on esitetty ISE:n loki PAC-tiedoston lataamistilanteen onnistumisesta.

Policy Server	ise
Event	5206 PAC provisioned
Failure Reason	
Resolution	
Root cause	
Username	C3570-stack
User Type	
Endpoint Id	7C:AD:74:E7:27:82
Endpoint Profile	
IP Address	
Identity Store	Internal CTS Devices
Identity Group	
Audit Session Id	C0A80503000002C04C779420
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)
Service Type	Framed
Network Device	C3560x-Upper

Kuvio 58. NDAC PAC-lataus onnistuu

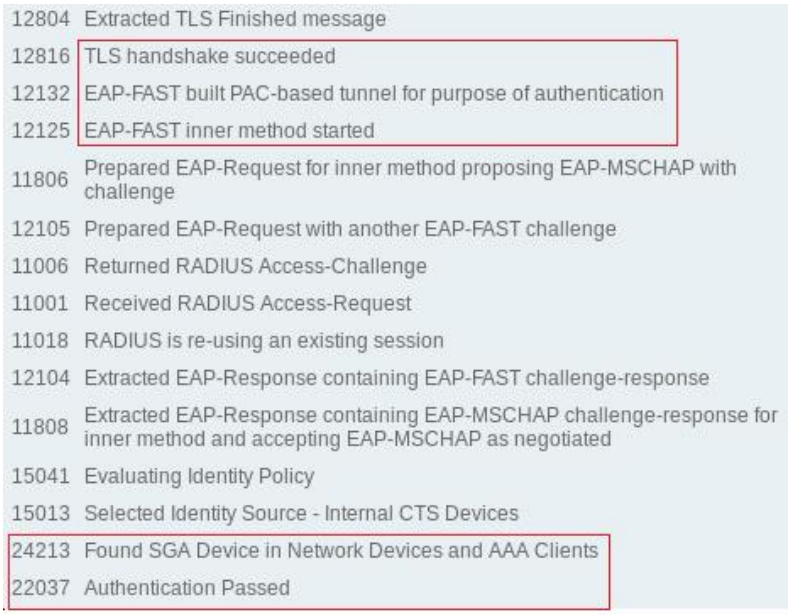
Kuviosta voidaan havaita, että PAC saatiin onnistuneesti siirrettyä C3750X-stack-kytkimelle. RADIUS-käyttäjätunnuksena on käytetty oikeaa arvoa, sillä se on löytynyt identiteetti-varastosta *”Internal CTS Devices”*. Lopuksi ISE palauttaa RADIUS-Access Reject–viestissä EAP-Failure ilmoituksen, sillä PAC on onnistuneesti siirretty ja kyseinen istunto voidaan purkaa ja aloittaa uusi autentikoiminen. Kuviossa 59 on esitetty Wireshark-kaappaus kyseistä tilanteesta.

```
No.   Time          Source              Destination   Protocol  Length  Info
  533 343.0145990(Cisco_e7:27:82          Nearest       TLSv1       77 Application Data
  534 343.0390310(Cisco_dc:8f:82          Nearest       EAP         60 Failure
  535 343.0516490(Cisco_e7:27:82          Nearest       EAPOL       60 Logoff
  537 348.0447750(Cisco_dc:8f:82          Nearest       EAPOL       60 Start
  538 348.0779510(Cisco_e7:27:82          Nearest       EAPOL       60 Start
  539 348.0918380(Cisco_dc:8f:82          Nearest       EAP         60 Request, Identity
  540 348.0936710(Cisco_e7:27:82          Nearest       EAP         60 Response, Identity
  541 348.1057430(Cisco_dc:8f:82          Nearest       TLSv1       60 Ignored Unknown Record
  542 348.1189560(Cisco_e7:27:82          Nearest       TLSv1      274 Client Hello

⊞ Frame 542: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface 0
⊞ Ethernet II, Src: Cisco_e7:27:82 (7c:ad:74:e7:27:82), Dst: Nearest (01:80:c2:00:00:03)
⊟ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 256
  ⊟ Extensible Authentication Protocol
      Code: Response (2)
      Id: 247
      Length: 256
      Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)
    ⊞ EAP-TLS Flags: 0x01
    ⊞ Secure Sockets Layer
```

Kuvio 59. EAP-Failure ja uusi autentikointi

Kuviosta voidaan havaita, että EAP-Failure viestin jälkeen alkaa uusi EAPOL-keskustelu kytkinten välillä. Avatussa paketissa voidaan myös huomioida käytössä olevan EAP-FAST uudelleen.

Tämän vaiheen EAP FAST – prosessin tarkoituksena on autentikoida C3750X-stack. Autentikointi tapahtuu suojatun tunnelin sisällä saadulla PAC-tiketillä. ISE kuitenkin tuottaa lokia kyseisestä tapahtumasta. Kuviossa 60 on esitetty ISE:n loki käydystä EAP-FAST-keskustelusta.

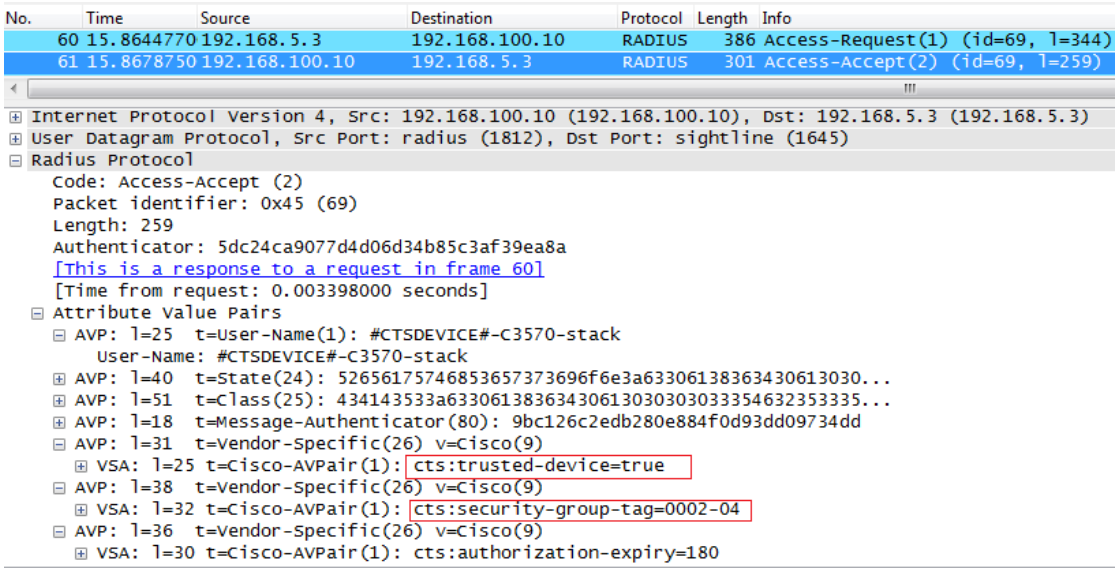


Kuvio 60. Toinen EAP-FAST-autentikointi

Kuviosta voidaan havaita, että TLS-kättelyn onnistumisen jälkeen EAP-FAST muodostaa tunnelin autentikointia varten. Käytettäväksi sisäiseksi metodiksi valitaan MSCHAPv2. Tämän jälkeen laitteet käyvät usean viestin EAP-Challenge-Response-keskustelun. Lopussa ISE tarkastaa identiteettivarastostaan *”Internal CTS Devices”* kytkimen tiedot, jonka jälkeen autentikointivaihe päättyy.

Onnistuneen 802.1X-autentikoinnin jälkeen kytkimet lataavat ISE:ltä ns. *”peer policyn”*, jolla kytkimet muodostavat luottamussiteen toisiinsa. Tässä tilanteessa kytkimet keskustelevat RADIUS-protokollan avulla sisällyttäen *”Username”*-attribuuttiin viereisen kytkimen tiedot.

Kuviossa 61 on esitetty C3560X-Upperin vastaanottama RADIUS-Access Accept –paketti.



Kuvio 61. RADIUS-Access-Accept ja CTS avp

C3560X-kytkin on pyytänyt ISE:ltä tietoa C3750X-stack-kytkimestä. *”User name”*- attribuutti ilmoittaa, että ladattava *”policy”* viittaa laitteeseen C3750X-stack. Punaisella merkityt *”cts:trusted-device=true”* ja *”cts:security-group-tag=0002-04”* kertovat kytkimelle, että C3750X-stack laitteelta tulevat SGT-paketit ovat luotettuja ja leimattu SGT-arvolla 2. ISE:ltä voidaan vielä tarkastaa tieto säännön osumisesta oikeaan valtuutusprofiiliin. Kuviossa 62 on esitetty tilanne kyseisestä kohdasta.

Kuvio 62. NDAC-Rule ISE:n lokissa

Kuviosta voidaan havaita mm. , että autentikointi C3750X-Stack-kytkimen kohdalla osui luotuun *”NDAC_Rule”*-sääntöön.

Tämän jälkeen kytkimet keskustelevat SAP-istunnon luomisesta. Kuviossa on esitetty C3560X-Upperin debug tilanteesta komennolla

C3560X-Upper#debug cts sap events

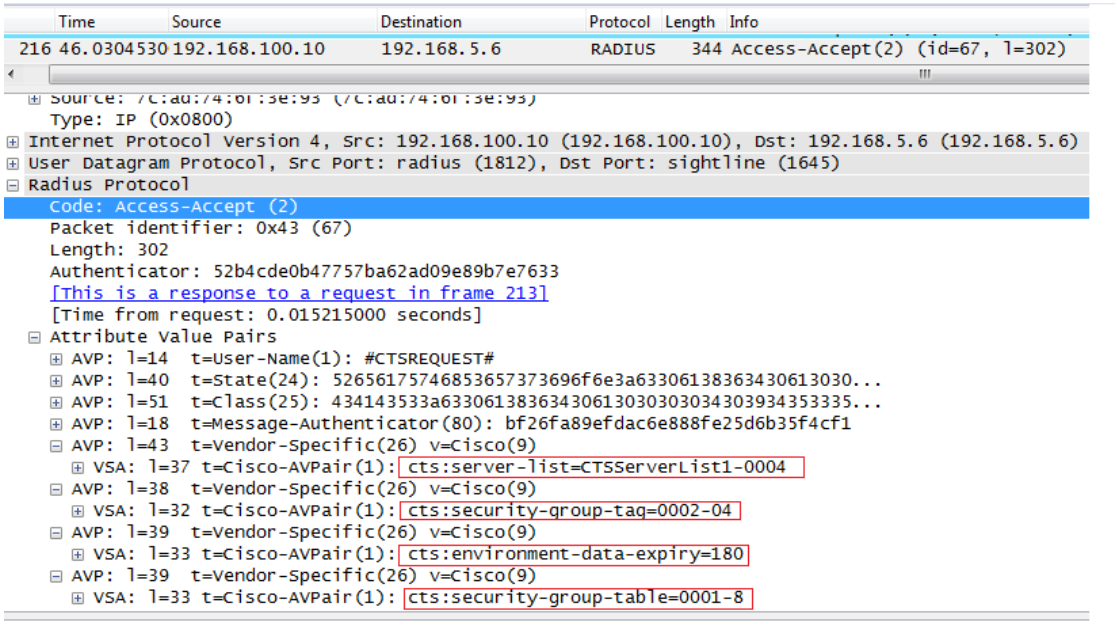
Kuviossa 63 on esitetty kyseisen komennon tuloste kytkimeltä C3560X-Upper.

```
C3560X-Upper# 22 12:16:25.756: CTS SAP ev (Gi0/2): Session started (new).
Aug 22 12:16:25.756: cts_sap_session_start CTS SAP ev (Gi0/2) peer:7cad.74e7.278
2 055DF99B88629F8074C8DEBD21353BBFAEFA516AF2E72E368AF16674E5501C2C
Aug 22 12:16:25.756: cts_sap_generate_pmkid_and_sci CTS SAP ev (Gi0/2) auth:7cad
.74dc.8f82 supp:7cad.74e7.2782, 055DF99B88629F8074C8DEBD21353BBFAEFA516AF2E72E36
8AF16674E5501C2C
Aug 22 12:16:25.756: CTS SAP ev (Gi0/2): Old state: [determining role],
  event: [change to authenticator], action: [send
C3560X-Upper#message #1] succeeded.
  New state: [waiting to receive message #2].
Aug 22 12:16:25.756: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (7ca
d.74e7.2782) on Interface Gi0/2 AuditSessionID C0A805030000018E58EE1765
Aug 22 12:16:25.790: CTS SAP ev (Gi0/2): EAPOL-Key message from 7CAD.74E7.2782.
Aug 22 12:16:25.790: CTS SAP ev (Gi0/2): EAPOL-Key message #0 parsed and validat
ed.
Aug 22 12:16:25.798: CTS SAP er (Gi0/2): Resent message #1.
Aug 22 12:16:25.823: CTS SAP ev (Gi0/2): EAPOL-Key message f
C3560X-Upper#rom 7CAD.74E7.2782.
Aug 22 12:16:25.823: CTS SAP ev (Gi0/2): New keys derived:
  KCK = CEAFD89E 483791EC 011FC455 AEEE5FCB,
  KEK = 7E5AA020 D0A8DCCA 447044C9 F039436E,
  TK = B37FC557 402A2A1B DB130FAF 356F2B15,
Aug 22 12:16:25.823: CTS SAP ev (Gi0/2): EAPOL-Key message #2 parsed and validat
ed.
Aug 22 12:16:25.823: CTS-SAP ev: cts_sap_action_program_msg_2: (Gi0/2) GCM is al
lowed.
Aug 22 12:16:25.848: CTS SAP ev (Gi0/2): Old state: [waiting to receive message
#2],
  event: [received message #2], ac
C3560X-Upper#tion: [program message #2] succeeded.
  New state: [waiting to program message #2].
Aug 22 12:16:25.848: CTS SAP ev (Gi0/2): Old state: [waiting to program message
#2],
  event: [data path programmed], action: [send message #3] succeeded.
  New state: [waiting to receive message #4].
Aug 22 12:16:25.865: CTS SAP ev (Gi0/2): EAPOL-Key message from 7CAD.74E7.2782.
Aug 22 12:16:25.865: CTS SAP ev (Gi0/2): EAPOL-Key message #4 parsed and validat
ed.
Aug 22 12:16:25.865: CTS-SAP ev: cts_sap_sync_sap_info:
C3560X-Upper# incr sync msg sent for Gi0/2
Aug 22 12:16:25.865: CTS SAP ev (Gi0/2): Old state: [waiting to receive message
#4],
  event: [received message #4], action: [establish] succeeded.
  New state: [established].
Aug 22 12:16:27.567: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state
 to up
Aug 22 12:16:29.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthe
rnet0/2, changed state to up
```

Kuvio 63. CTS SAP Debug-tuloste

Kuviosta voidaan havaita SAP-keskustelun alkaneen määritetyssä rajapinnassa. Toisessa punaisessa merkityllä kohdassa nähdään, että kytkin on luonut uudet avaimet, esimerkiksi KEK-avaimen. Tämän jälkeen kytkin ilmoittaa, että GCM on mahdollinen, joten keskustelu käytettävästä salausmenetelmästä on mahdollinen. Viimeisenä on ilmoitus vielä keskustelun onnistumisesta, jonka jälkeen portti nousee ylös.

C3750X-stack osaa tässä vaiheessa ladata itse *”Environment data”*-tiedot ISE:ltä RADIUS-protokollan avulla. Kuviossa 64 on esitetty Access-Accept-paketti ISE:ltä vastauksena C3750X-stack-kytkimen pyytämiin CTS-tietoihin.



Kuvio 64. C3750X-stack environment data-lataus

Punaisella merkityistä kohdista voidaan havaita, että paketti sisältää mm. *”CTSServer-list1”*-attribuutin, joka sisältää tiedot käytössä olevasta SGA-palvelimesta. *”Security-group-tag =0002-04”* on ISE:lle määritetty SGA_Device_SGT –SGT, joka luotiin annettavaksi TrustSec-ympäristön luotetuille verkkolaitteille. *”environment-data-expiry=180”* asettaa kytkimen päivitysvälin *”environment data”*:lle 180 sekuntiin.

Kytkin on siis saanut ISE:lle määritellyt SGA-tiedot onnistuneesti ja NDAC on päättynyt. Onnistuneen NDAC-autentikoinnin- ja rajapintakohtaiset CTS-tiedot voidaan tarkastaa kytkimellä komennolla:

C3750X-stack # show cts interface GigabitEthernet 1/0/2

Kuviossa 65 on esitetty edelläoleva komento C3750X-stack -kytkimellä

```
C3750X-stack#sh cts interface gigabitEthernet 1/0/2
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/2:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "C3560x-Upper"
        Peer's advertised capabilities: "sap"
        802.1X role:         Supplicant
        Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
        Peer SGT:            2:SGA_Device_SGT
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE

    Statistics:
        authc success:              1
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   0
        authz success:              3
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/2
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 3
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

Kuvio 65. CTS-rajapinnan tuloste NDAC:n-jälkeen

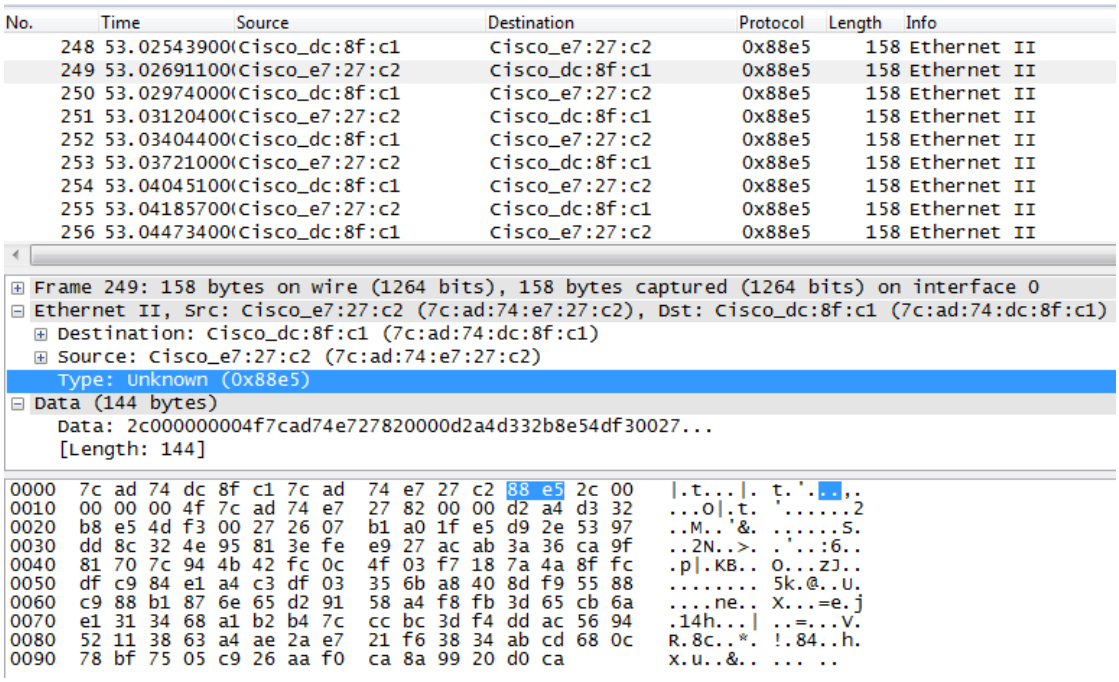
Kuviosta voidaan havaita autentikoinnin onnistuneen. Tämä voidaan todeta kohdasta *”Authentication Status”*, jonka perässä lukee *”SUCCEEDED”*. Tämän alla olevista kohdista saadaan tietoa mm. toisen kytkimen identiteetistä sekä siitä, että kytkimen kykynä on MACsec-salauksen muodostaminen SAP-protokollan avulla. *”Authorization Status”*-kohdasta voidaan havaita C3560X-upper:in SGT-arvo (SGA_Device_SGT), sekä myös luottamuksen muodostuneen kyseiselle SGT:lle (Peer SGT Assignment: Trusted).

”Authorization Status”-kohdasta nähdään, että valtuutus toteutui onnistuneesti. Samasta kohdasta voidaan myös huomata, että kytkimellä on tieto *”peer”*-laitteen SGT-

leimasta. Viimeinen kohta ilmoittaa, että C3750X-stack luottaa C3560X-Upper kytkimen SGT-arvoon (SGA_Device_SGT) ISE:ltä saadun tiedon mukaisesti.

”SAP Status SUCCEEDED” merkintä ilmoittaa SAP-protokollan onnistumisen, joten MACsec on toiminnassa kytkinten välillä. Alempana on myös ilmoitus käytössä olevasta salaustavasta, joka on AES-GCM. Tulosteen alhaalta voidaan todeta lisäksi mm. kytkimen C3750X-stack rooli tapahtuneessa 802.1X –autentikoinnissa. Kyseinen kytkin toimi suplikanttina kuten kohta *”PAE = SUPPLICANT”* ilmaisee.

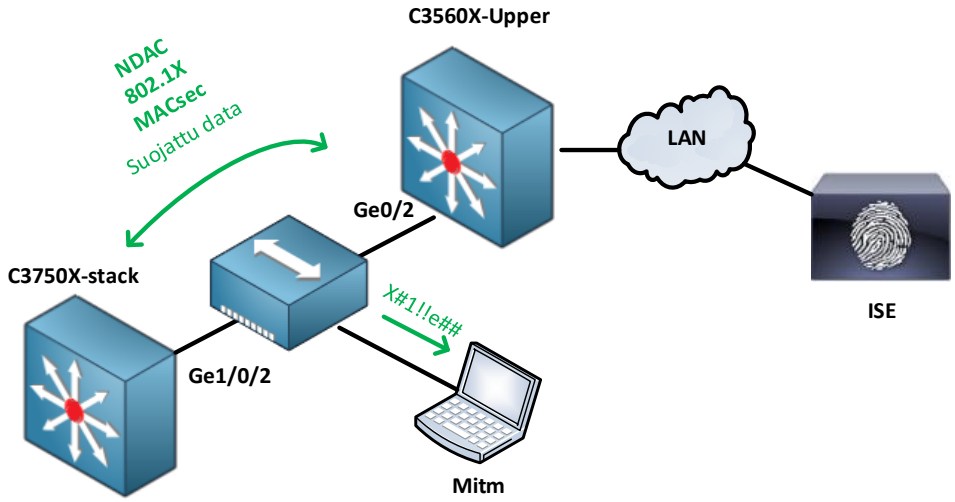
Tässä vaiheessa kytkinten välinen liikenne on salattua. Todentamiseksi on esitetty kuvion 66 mukainen MitM-laitteen WireShark-kaappaus NDAC-autentikoinnin jälkeen.



Kuvio 66. MACsec-salattu liikenne NDAC:n jälkeen

Kuviosta voidaan huomata, että viimeisen EAPOL-viestin jälkeen *”protocol”*-kenttä sisältää vain ethertype arvon *”0x88e5”.* Tämä arvo on käytössä MACsec-paketeilla. Opinnäytetyön aikana WireSharkiin ei löytynyt päivitystä, joka tunnistais paketit muuna kuin *”Unknown”*-tyyppinä.

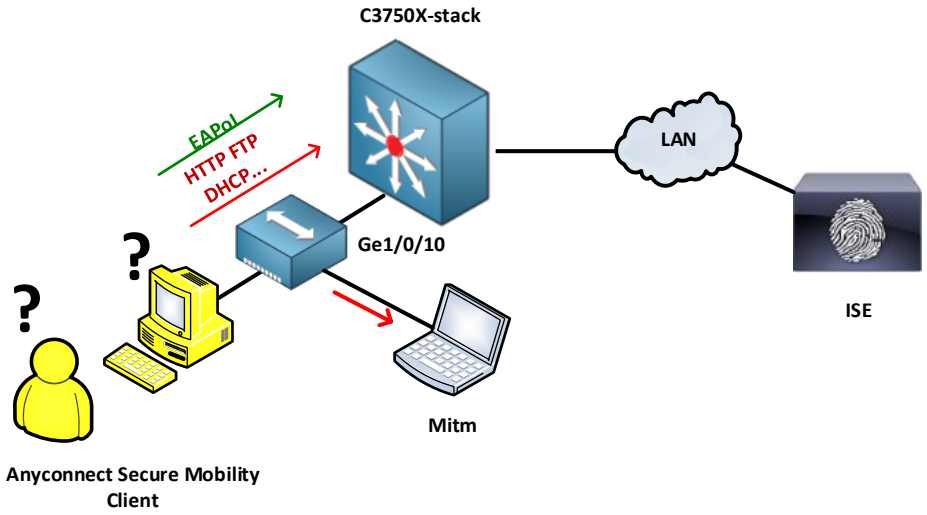
NDAC-autentikointi ja liikenteen salaus on tässä vaiheessa toiminnassa kytkimillä. Kuviossa 67 on havainnollistettu lopullinen tilanne.



Kuvio 67. Lopputilanne NDAC autentikoinnin jälkeen

5.3.2 EAP-FAST -Chaining Anyconnect-suplikantilla

Toinen testaustilanne oli 802.1X – tunnistautuminen kytkimen porttiin. Testaukseen käytettiin suplikantin roolissa HP-kannettavaa, johon oli asennettu Anyconnect Secure Mobility Client ohjelmisto NAM-moduulilla. Kannettava oli myös lisätty AD:lle *”Domain Computers”*-ryhmään. Autentikaattorina toimi C3750X-stack ja RADIUS-palvelimena ISE. Kuviossa 68 on esitetty alkutilanne testaustapahtumasta.

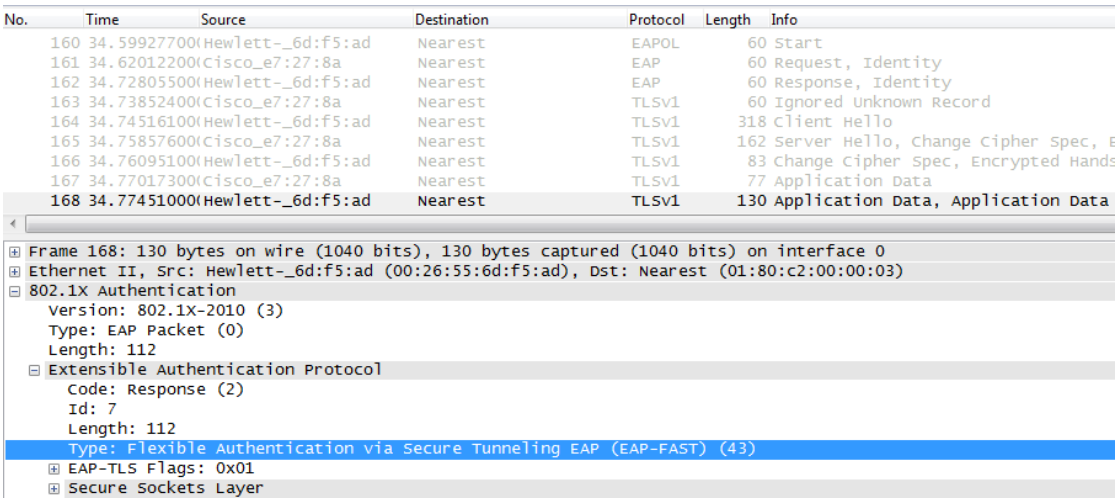


Kuvio 68. Anyconnect LAN alkutilanne

Testaustilanteessa käytettiin myös kuvion mukaisesti toistinta, johon oli liitetty Wireshark-varustetta kannettava monitoroimaan liikennettä.

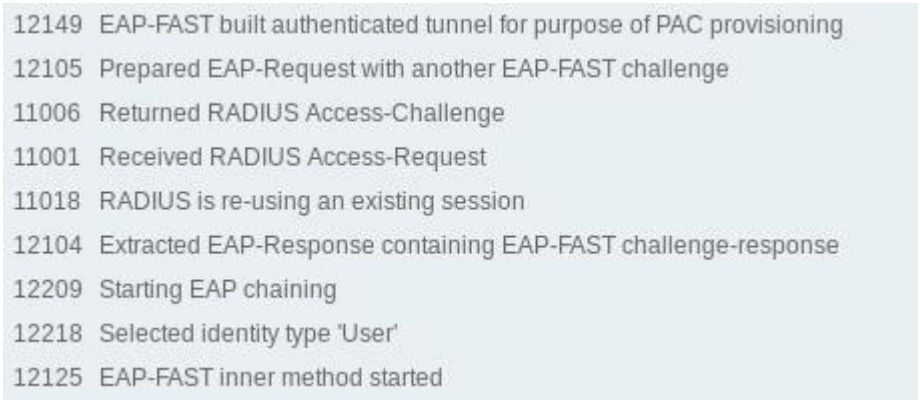
Alkutilanne on normaalin 802.1X-autentikoinnin mukainen, eli kytkin ei vastaanota portista muita kuin EAPoL-paketteja. Tässä vaiheessa luonnollisesti käyttäjää ja/tai laitetta ei ole tunnistettu, joten autentikointi alkaa kytkimen tai suplikantin toimesta EAPOL-paketilla.

Kuviossa 69 on esitetty ensimmäiset viestit autentikoinnin aikana.



Kuvio 69. EAPOL-Start

HP-kannettava aloittaa keskustelun EAPOL-start paketilla, jonka jälkeen kytkin pyytää protokollan mukaisesti tietoa identiteetistä EAP-Request-Identity-paketin muodossa. Tämän jälkeen HP vastaa EAP-Response-Identityllä. Seuraavana on vuorossa TLS-tunnelin muodostus, jonka sisällä PAC-tiedosto siirretään HP:lle. Tilannetta voidaan tarkastella ISE:n lokista, sillä tunneli on suojattu. Kuviossa 70 on esitetty alkutilanne PAC-Provision-kohdasta.



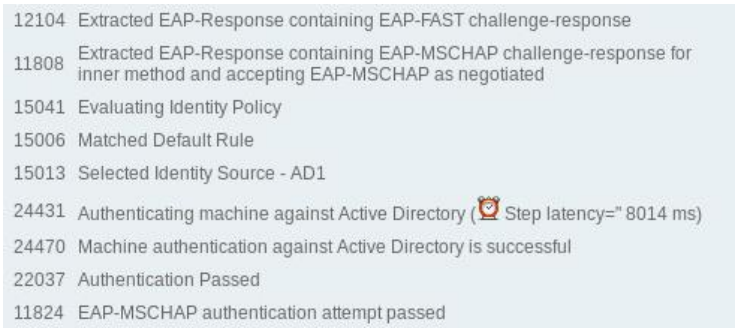
Kuvio 70. PAC Provision

Kuviosta voidaan havaita, että EAP-FAST muodostaa autentikoidun tunnelin PAC-tiedoston lataamista varten. Tunnukset tullaan tarkistamaan tunnelin sisällä, jonka jälkeen PAC-tiedostot latautuvat supplikantille ja pääsy verkkoon tapahtuu samalla. Kolmanneksi viimeisestä viestistä voidaan havaita, että EAP-Chaining-metodi alkaa. Ensin etsitään käyttää sisäisenä metodina. Tämän jälkeen autentikointipalvelin ja supplikantti keskustelevat käytettävästä sisäisestä metodista käyttäjän kohdalla, joka on EAP-MSCHAPv2. Kuviossa 71 on esitetty käyttäjän autentikoinnin onnistuminen.

Kuvio 71. Käyttäjän autentikointi onnistuu

Kuvion ensimmäisestä punaisesta laatikosta voidaan havaita, että käyttäjän autentikointi AD:tä vastaan onnistui. Tässä vaiheessa ensimmäinen autentikointi onnistui ja laitteelle voidaan palauttaa EAP-Success-viesti. Tämän jälkeen keskustelu jatkuu tunnelin sisällä. Kuvion alempi punainen laatikko ilmoittaa, että RADIUS-käyttää käynnissä olevaa istuntoa.

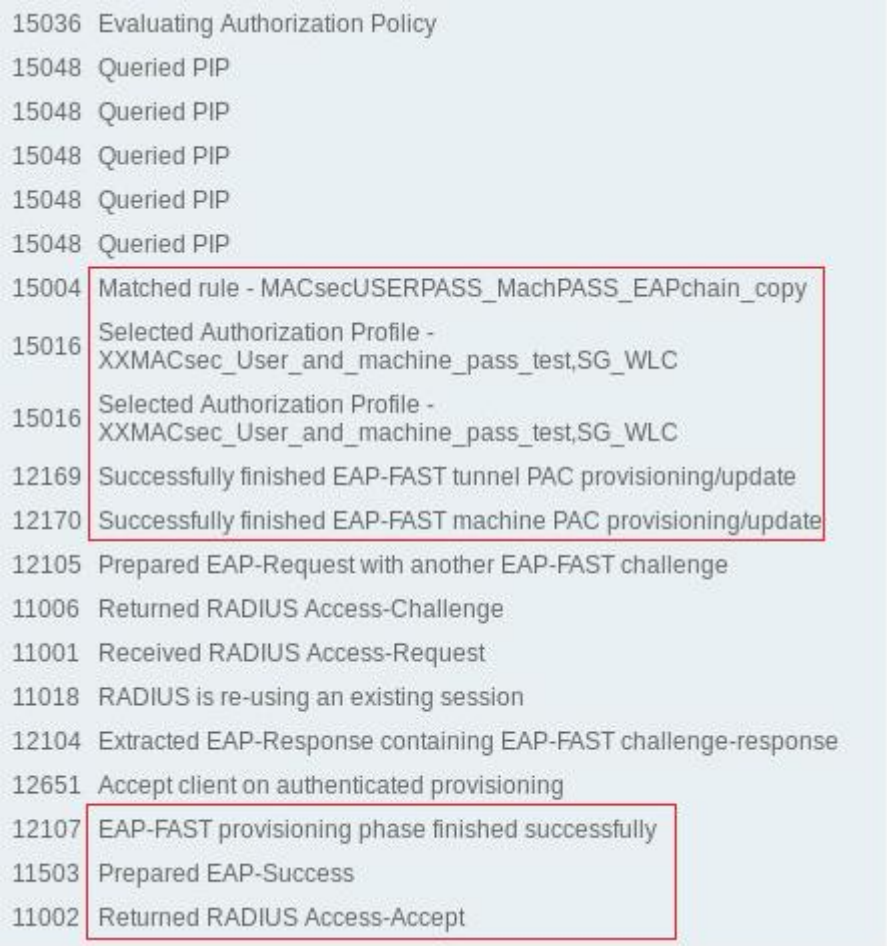
Tämän jälkeen autentikoidaan laite (CTSADMIN-PC) EAP-FAST:in avulla. Kuviossa 72 on esitetty ISE:n loki autentikoinnin onnistumisesta.



Kuvio 72. Laitteen autentikointi onnistuu

Kuviosta voidaan havaita, että laite käyttää samaa EAP-metodia autentikointiin. Samalla huomataan, että autentikointi AD:ta vasten onnistui myös laitteen kohdalla.

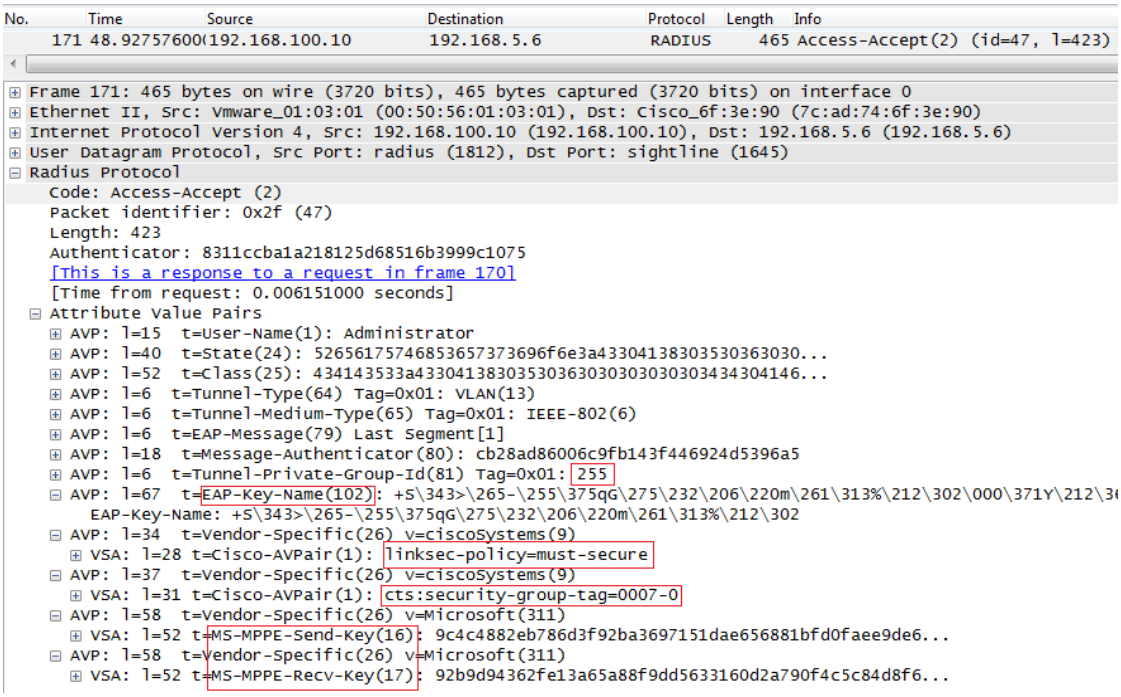
Tunnistautumisen loppuvaiheessa valitaan laitteelle määritetty valtuutuspolitiikka. Kuviossa 73 on esitetty kuvakaappaus ISE:ltä tunnistautumisen lopun vaiheista.



Kuvio 73. Autentikoinnin loppu ja valtuutuspolitiikan valinta

Kuviosta voidaan havaita mm. oikean valtuutuspofiilin valinta kohdassa *”Selected Authorization Profile”*(Kuviossa ensimmäisenä punaisena). Samassa on ilmoiteuttu laitekohtaisen PAC-ja tunneli-PAC-tiedostojen myöntämisen onnistuneen. Autentikoinnin lopputuloksena kytkimelle annetaan parametrit, jotka tunnistautuvalle käyttäjä/laitteelle kuuluu asettaa. Lopussa on ilmoitettu ISE:n palauttavan EAP-Success viestin RADIUS-viestin yhteydessä (Kuviossa alhaalla punaisella).

Kuviossa 74 on esitetty WireShark-kuvakaappaus viimeisestä RADIUS-Access-Accept-viestistä.

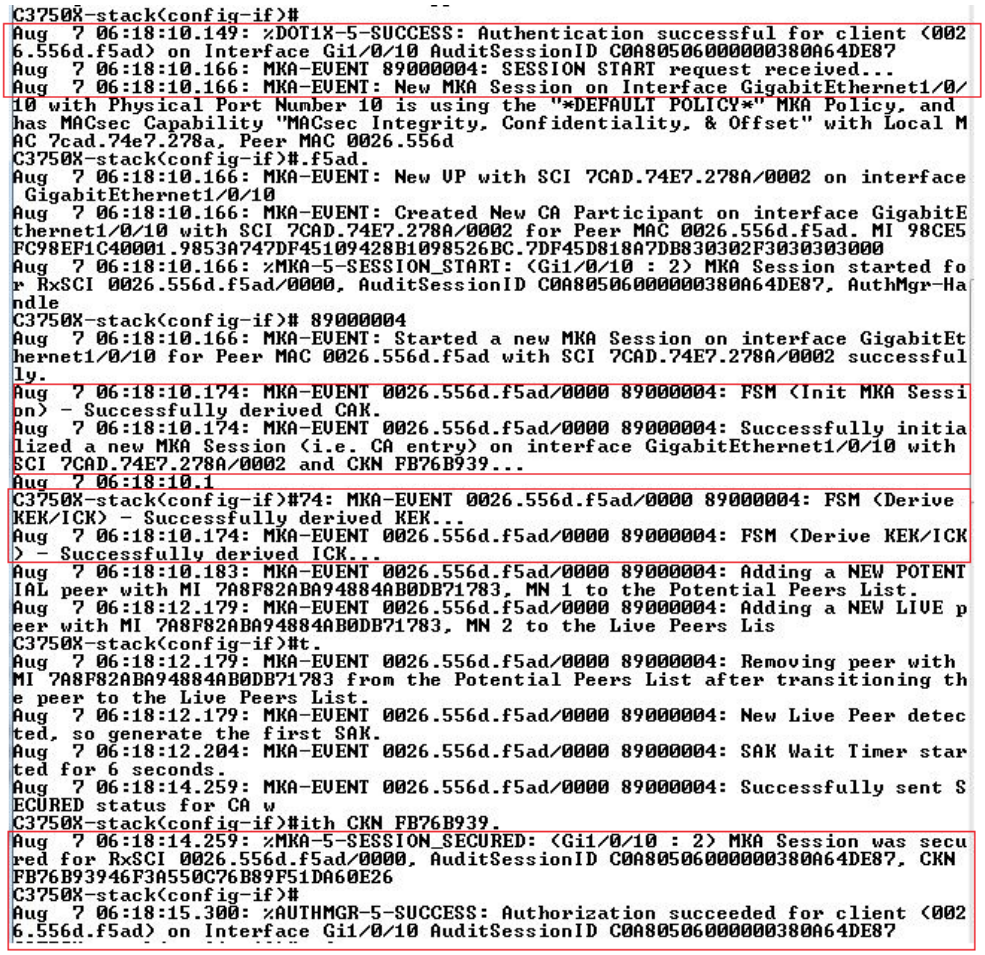


Kuvio 74. RADIUS-Access-Accept ja attribuutit

Kytkin saa viimeisessä viestissä mm. VLAN-tiedon, EAP-Key-Name-attribuutin, MACsec-politiikan ja SG-ryhmän. Lopussa olevia MS-MPPE-avaimia käytetään CAK:n muodostamiseen kytkimelle. Tässä vaiheessa supplikantilla on tiedossa jo käytettävä CAK-avain.

Kuviossa 75 on esitetty kytkimen tuloste MKA-tapahtumista komennosta

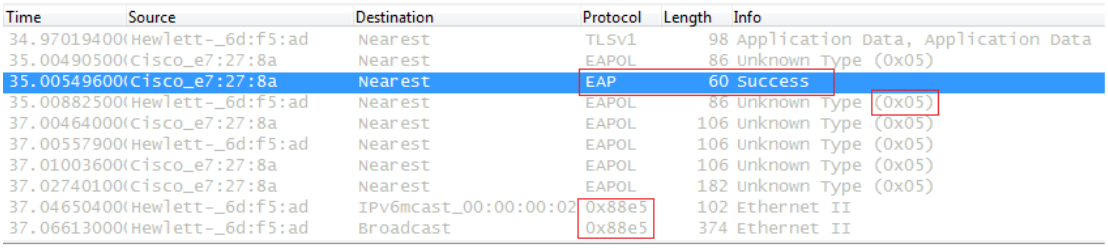
C3750X-Stack# debug mka events



Kuvio 75. MKA-tapahtumat

Kuvion ensimmäisestä punaisesta laatikosta voidaan huomata autentikoinnin onnistuneen ja MKA-istunnon alkaminen. Toisesta kohdasta nähdään, että key-serverinä toimiva kytkin pystyi onnistuneesti johtamaan CAK-avaimen. Kolmannesta kohdasta havaitaan, että kytkin loi onnistuneesti myös ICK-avaimen, ja KEK-avaimen SAK:n salaamista varten. Tämän jälkeen kytkin ilmoittaa luoneensa SAK:n. Viimeiset punaiset laatikot ilmoittavat istunnon suojauksen ja valtuutuspolitiikan määräämisen onnistuneen.

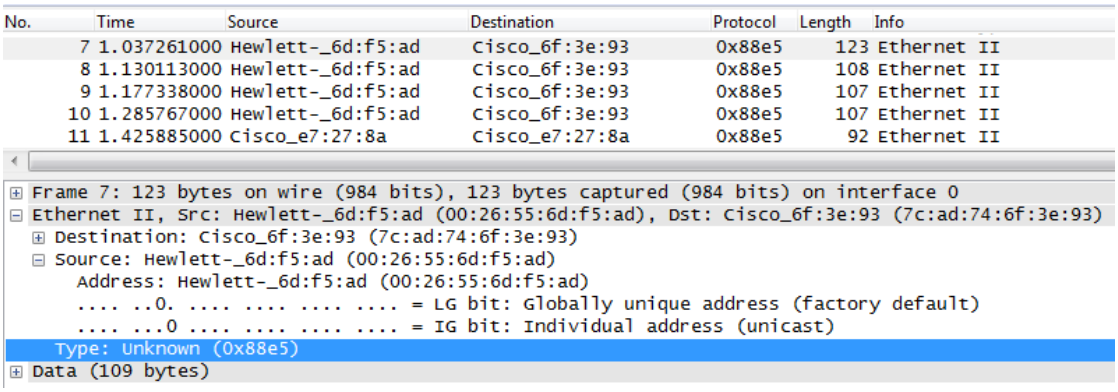
Kuviossa 76 on esitetty supplikantin ja kytkimen välillä viimeiset EAPOL-viestit ennen salauksen muodostumista WireSharkista.



Kuvio 76. Viimeiset EAPOL-viestit ennen salausta

Paketeista voidaan havaita, että EAP-Success-viestin jälkeen lähetetään useampi EAPOL-paketti, jonka tyyppinä on arvo 5. WireShark ei osaa näyttää paketin tyyppiä, mutta protokollan mukaan type 5 EAPOL-viestit ovat EAPOL-MKA-paketteja. Tässä vaiheessa tapahtuu kuvion 59 mukaisestikin esitetty salauksen muodostaminen. Viimeisenä punaisella oleva laatikko ilmoittaa ethertype arvolla *”0x88e5”* olevien pakettien liikkuvan linkillä.

Kuviossa 77 on esitetty WireSharkista lisää MACsec-paketteja.



Kuvio 77. MACsec-salattu liikenne autentikoinnin jälkeen

Kytkimen puolelta tilannetta voidaan tarkastella rajapinnasta GE 1/0/10 komennolla:

> *C3750X-stack# show authentication sessions interface gigabitEthernet 1/0/10 details*

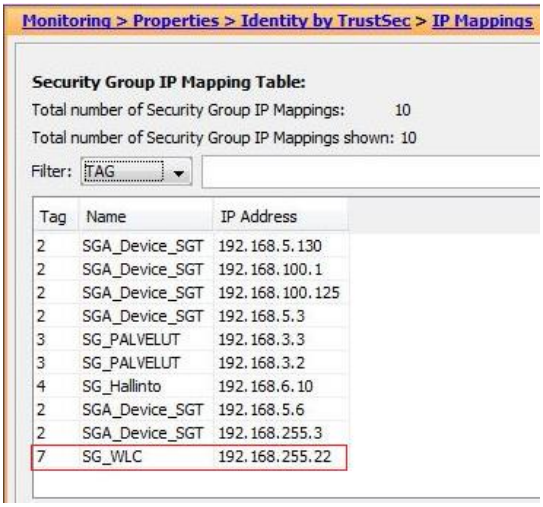
Kuviossa 78 on esitetty kuvakaappaus kyseisen komennon tulosteesta kytkimellä.

```
C3750X-stack#$tication sessions interface gigabitEthernet 1/0/10 details
            Interface:  GigabitEthernet1/0/10
          MAC Address:  0026.556d.f5ad
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.22
            User-Name:  Administrator
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  C0A805060000002A849111DD5
     Acct Session ID:  0x0000029F
              Handle:  0xD2000145
      Current Policy:  POLICY_Gi1/0/10

Local Policies:
       Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 255
      Security Policy:  Must Secure
      Security Status:  Link Secured
            SGT Value:  7

Method status list:
       Method            State
       dot1x             Authc Success
```

Kuvio 78. Kytkimen portin tuloste autentikoinnin jälkeen

Tulosteesta voidaan havaita mm. ISE:ltä saadut parametrit kohdasta *”Server Policies”*. VLAN:iksi on asetettu testin WLC–VLAN (VLAN 255), jonka osoiteavaruudesta laite on myös saanut IP-osoitteen kohdan *”IPv4 Address”* mukaisesti. *”Security Policy”* ilmaisee käytettävän MACSec-politiikan, joka oli ISE:llä määritelty arvolle *”Must Secure”.* MACSec -salauksen onnistuminen on tässä tapauksessa välttämätöntä. *”Security Status”* kohta ilmaisee myös linkkivälin PC:lle olevan suojattu onnistuneesti. Lopuksi kytkin on määrittänyt portista tulevalle liikenteelle SGT-arvon 7 ISE:llä määritetyn valtuutussäännön mukaisesti.

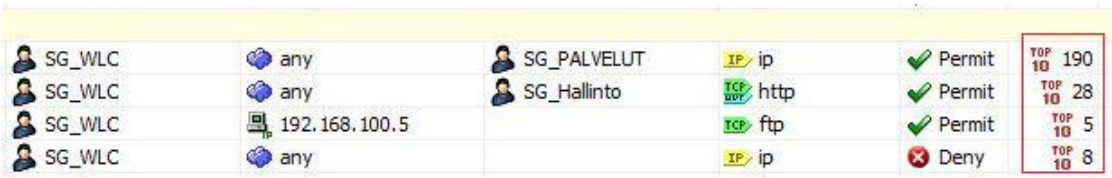
Tässä vaiheessa autentikointi, valtuutus ja salaaminen on suoritettu loppuun. Tämän jälkeen tarkastetaan palomuurisääntöjen toiminta ASA:lla. C3750X-Stack on siirtänyt tiedon kirjautuneesta kannettavasta ASA:lle SXP:n avulla. Kuviossa 79 on esitetty ASA:n SG-taulu autentikoinnin jälkeen.



Kuvio 79. ASA IP-Mappings LAN

Kuviosta voidaan havaita ASA:n saaneen tiedon kirjautuneesta laitteesta. Punaisella merkityssä kohdassa huomataan SGT-leiman numero 7 (SG_WLC) kuuluvan IP-osoitteelle 192.168.255.22. Tässä vaiheessa rajapintaan wlc luodut muurisäännöt tulevat voimaan laitteen osalta.

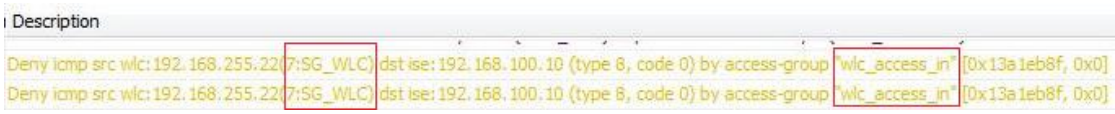
Kuviosta 80 voidaan tarkastella ASA:n sääntöjä liikenteen generoimisen jälkeen.



Kuvio 80. ASA:n säännöt SG_WLC:lle

Kuvion punaisella merkitystä sarakkeesta voidaan havaita, että kukin sääntö oli käytössä. Liikennettä generoitiin kunkin säännön mukaisesti esimerkiksi käyttämällä FTP-protokollaa IP-osoitteessa 192.168.100.5 sijaitsevalla palvelimella.

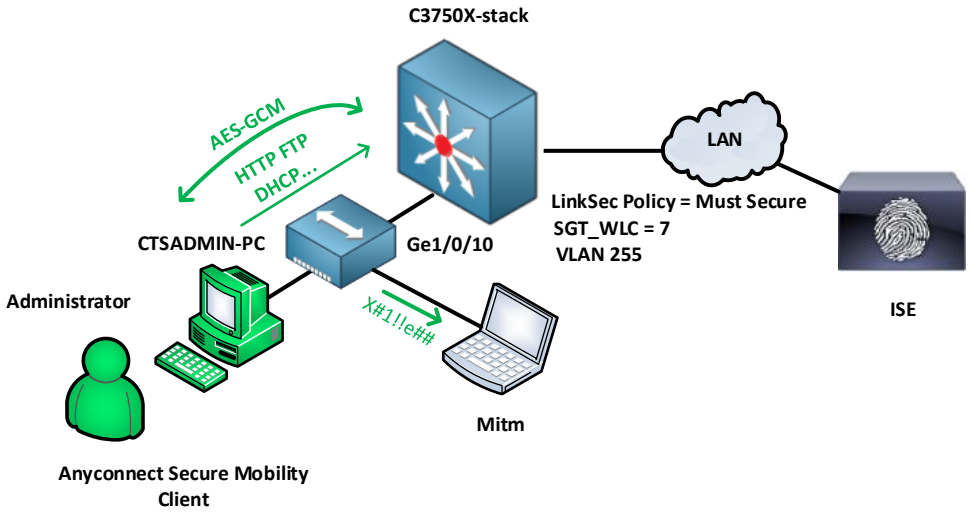
Viimeinen sääntö kieltää kaiken muun liikenteen mihin tahansa osoitteeseen. Tätä testattiin lähettämällä ICMP-viestejä kannettavalta ISE:lle. Kuviossa 81 on esitetty ASA:n Syslog-ilmoitus kyseisestä tilanteesta.



Kuvio 81. ASA:n Syslog wlc_access_in

Kuviosta voidaan havaita, että ICMP-kielletään rajapinnasta wlc. Vasemmalla punaisella merkityllä alueella on myös tieto, että IP-osoitteelle 192.168.255.22 kuuluu SG 7. Oikealla on havaittavissa myös aiemmin luotu sääntöryhmä *”wlc_access_in”.*

Kuviossa 82 on havainnollistettu lopullinen tilanne 802.1X autentikoinnin jälkeen.

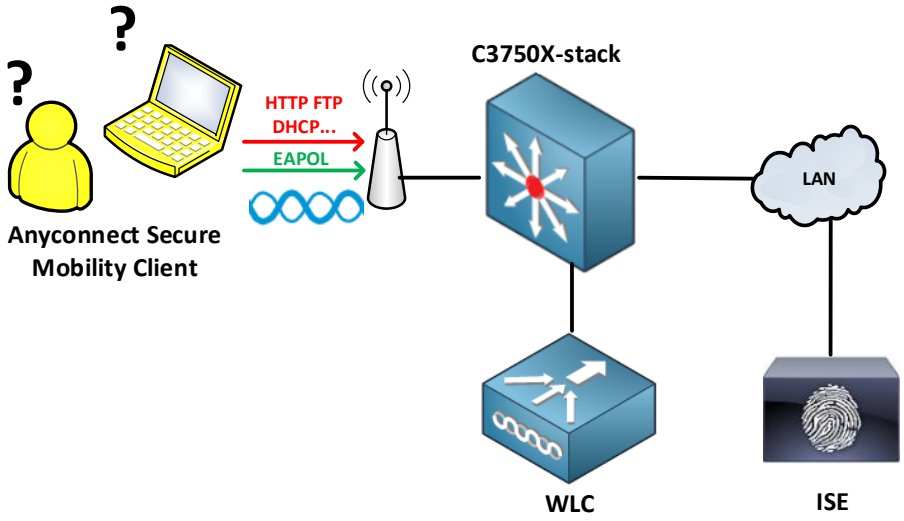


Kuvio 82. 802.1X Lopputilanne

5.3.3 WLAN-kirjautuminen EAP-FAST-Chaining-metodilla

Seuraava testi oli kirjautuminen WLAN:iin EAP-FAST:n avulla. Kirjautuminen on samankaltainen langallisen kanssa. Anyconnect-supplikanttiin on asetettu langaton yhteys päälle ja valittu konfiguroinneissa esitetty profiili *”EAP-FAST-Chaining-Wireless”.*

Kuviossa 83 on esitetty alkutilanne WLAN-kirjautumistilanteesta.



Kuvio 83. WLAN-kirjautumisen alkutilanne

Autentikointitapahtuma on vastaavanlainen langallisen kirjautumisen kanssa, joka on esitetty kappaleessa 5.3.2. Suurimpana erona on valtuutusprofiili, joka ISE:ltä myönnetään kirjautuvalle laitteelle. Kuviossa 84 on esitetty loki ISE:ltä kirjautumisen loppuvaiheesta.

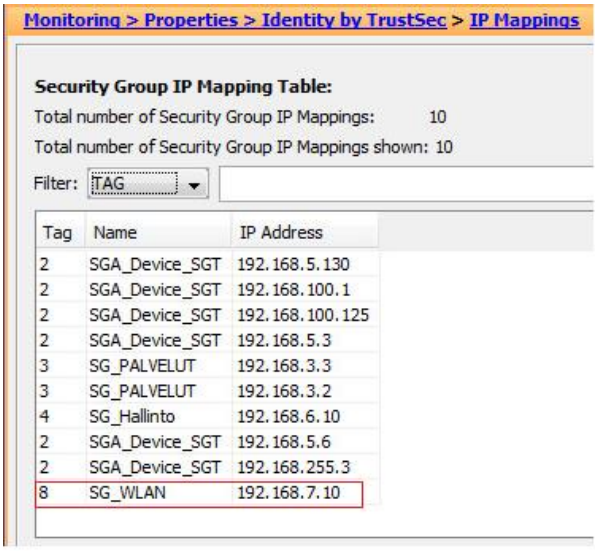
15036	Evaluating Authorization Policy
15048	Queried PIP
15048	Queried PIP
15048	Queried PIP
15048	Queried PIP
15048	Queried PIP
15004	Matched rule - wlan_USERPASS_MachPASS_EAPchain
15016	Selected Authorization Profile - User_and_machine_pass_auth,SG_WLAN
15016	Selected Authorization Profile - User_and_machine_pass_auth,SG_WLAN
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12106	EAP-FAST authentication phase finished successfully
11503	Prepared EAP-Success
11002	Returned RADIUS Access-Accept

Kuvio 84. WLAN valtuutuspolitiikka

Kuviosta voidaan havaita valtuutuspolitiikan olevan oikea. Kuvion lopussa on todennus autentikointivaiheen onnistumisesta. Tämän jälkeen WLC osaa asettaa autenti-

koituneelle laitteelle konfiguroinneissa määritetyn VLAN:in (70) ja SGT-arvon 8. VLAN:in perusteella laite saa myös IP-osoitteen halutusta aliverkosta 192.168.70.0/24.

Kirjautumisen jälkeen ASA saa SXP:n kautta tiedon kannettavalle myönnetystä IP-osoitteesta, sekä SG-ryhmästä SXP:n avulla. Kuviossa 85 on esitetty ASA:n SG-taulu WLAN-kirjautumisen jälkeen.



Kuvio 85. ASA IP-Mappings WLAN

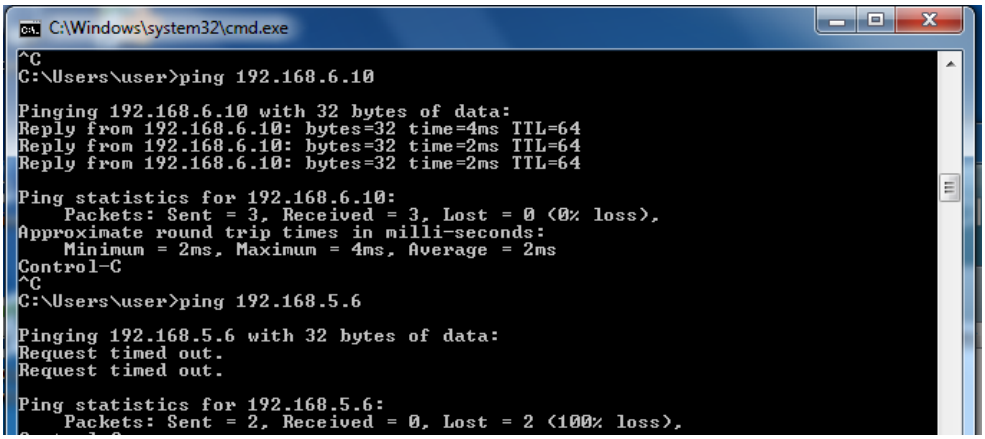
Kuviosta voidaan havaita ASA:n saaneen oikein tiedot WLAN:iin kirjautuneesta laitteesta. Punaisella merkityssä kohdassa näkyy IP-osoitteelle 192.168.7.10 myönnetty SGT 8.

Seuraavana vuorossa oli ASA:n SGFW-ominaisuuden testaaminen WLAN-tilanteessa. Palomuurisääntöinä käytettiin yksinkertaisia sisäverkkoon kohdistuvia sääntöjä. Kuviossa 86 on esitetty palomuurisäännöt, jotka astuvat voimaan WLAN-kirjautumisen jälkeen.

	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits
wlan-tyontekijat (6 incoming rules)									
1	☑	any		SG_WLAN	any	SG_PALVELUT	ip	Permit	TOP 10 267
2	☑	any		SG_WLAN	any	SG_Hallinto	icmp http	Permit	TOP 10 46
3	☑	any		SG_WLAN	192.168.100.5		ftp	Deny	3
4	☑	any		SG_WLAN	any	SGA_Device_SGT	icmp	Deny	3
5	☑	any		SG_WLAN	any		ip	Deny	TOP 10 58

Kuvio 86. WLAN-muurisäännöt

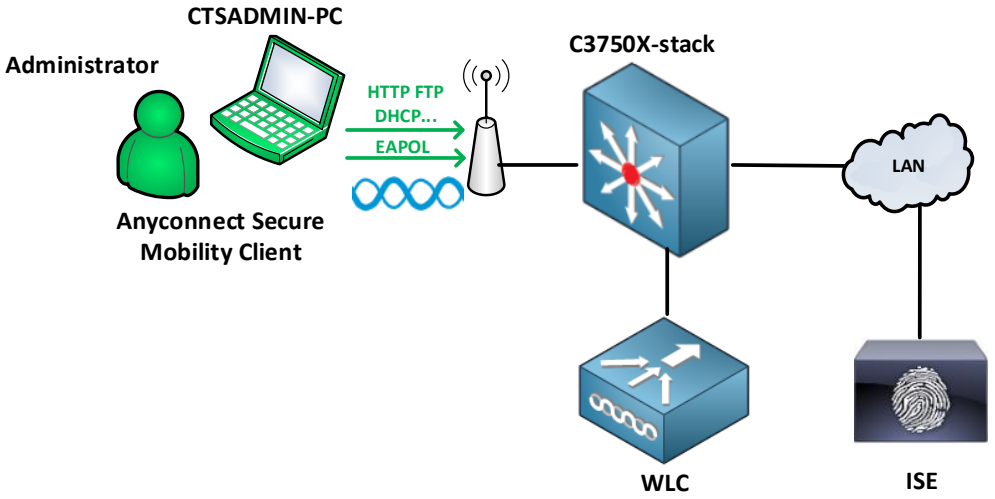
Liikennettä generoitiin kaikkiin sääntöihin. Kuviossa punaisella merkitystä kohdasta voidaan todeta osumat kuhunkin sääntöön. Testimielessä ICMP sallittiin SG_Hallinto-palvelimelle ja estettiin SGA_Device_SGT-laitteille. Kuviossa 87 on esitetty ping http-palvelimelle (SG_Hallinto), sekä C3750X-Stack-kytkimelle (SGA_Device_SGT).



Kuvio 87. Ping-testaus autentikoinnin jälkeen

Tulosteesta voidaan huomata, että ping onnistui http-palvelimelle ja epäonnistui kytkimelle palomuurisäännön mukaisesti.

Tässä vaiheessa WLAN-kirjautumisen testaaminen on päättynyt. Kuviossa 88 on havainnollistettu lopputilanne.

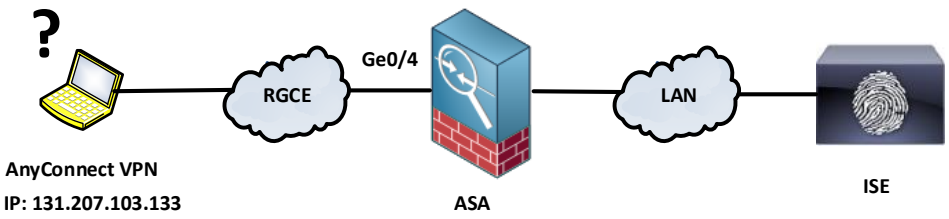


Kuvio 88. WLAN kirjautumisen lopputilanne

5.3.4 VPN-kirjautuminen Anyconnect VPN-moduulilla

Viimeisenä testitilanteena oli VPN-kirjautuminen RGCE-verkosta Anyconnectin VPN-moduulilla. VPN-yhteyden terminointipisteenä toimi ASA:n Ge 0/4 rajapinta, johon virtuaalikoneella otettiin yhteys. Virtuaalikoneelle oli aiemmin asennettu Anyconnect-VPN-moduuli joten yhdistäminen tapahtui yksinkertaisesti määrittelemällä ASA:n IP-osoite. Tämän jälkeen tulee syöttää käyttäjätunnus/salasanapari.

Kuviossa 89 on esitetty VPN-testauksen alkutilanne.



Kuvio 89. VPN-testauksen alkutilanne

Kuviossa 90 on esitetty RADIUS-tapahtumat ja käyttäjän autentikoiminen AD:tä vasten.

Kuvio 90. VPN-käyttäjän autentikointi

Kuviosta voidaan havaita, että autentikointi käytettyä identiteetti-lähdettä vastaan onnistui.

Tämä jälkeen kirjautumiseen liitetään luotu valtuutusprofiili. Kuvioss 91 on esitetty tapahtuma ISE:n lokissa.

Kuvio 91. VPN Auth-Policy

Valtuutus onnistui halutulla tavalla. ISE osasi yhdistää autentikoinnin oikeaan sääntöön *”VPN”* ja palautti valtuutusprofiilin *”VPN_auth_success”* (Kuviossa punaisella). Lopussa ISE palauttaa ASA:lle RADIUS Access-Accept-viestin autentikoinnin onnistumisen merkiksi. Viestiin on sisällytetty myös luotu DACL, jonka ASA liittää VPN-yhteyteen. ASA:n puolelta voidaan tarkastaa pääsylistan asentuminen komennolla

cisco-asa#show vpn-sessiondb detail anyconnect

Kuviossa 92 on esitetty kyseisen komennon tulosteesta SSL-tunnelia, koskeva osa.

```
SSL-Tunnel:
  Tunnel ID    : 6.2
  Assigned IP  : 10.10.10.10            Public IP    : 131.207.103.133
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Src Port : 49240
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.05152
  Bytes Tx     : 544927                 Bytes Rx     : 84552
  Pkts Tx      : 863                    Pkts Rx      : 720
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-VPN_Dacl-53e9f721
```

Kuvio 92. DACL ASA:lla

Kuviosta voidaan havaita mm. VPN-laitteelle määrätty IP-osoite (10.10.10.10), sekä laitteen julkine osoite (131.207.103.133). Kuvion jälkimmäisestä punaisella merkitystä osasta huomataan, että suodattimeksi on valittu ISE:ltä saatu pääsylista *”VPN_Dacl”*.

DACL:ää testattiin lähettämällä ICMP-viestejä sisäverkkoon ISE:lle, sekä ottamalla http yhteys palvelimelle 192.168.6.10. Kuviossa 93 on esitetty ASA:n Syslog-viestit kyseisestä tilanteesta.

```
access-list #ACSACL#-IP-VPN_Dacl-53e9f721 permitted tcp for user 'Administrator' outside/10.10.10.10(49243) -> hallinto/192.168.6.10(80) hit-cnt 1 first hit [0xe64015cd, 0x0]
Built inbound TCP connection 62796 for outside:10.10.10.10/49242 (10.10.10.10/49242)(LOCAL\Administrator) to hallinto:192.168.6.10/80 (192.168.6.10/80)(4:SG_Hallinto) (Administrator)
access-list #ACSACL#-IP-VPN_Dacl-53e9f721 permitted tcp for user 'Administrator' outside/10.10.10.10(49242) -> hallinto/192.168.6.10(80) hit-cnt 1 first hit [0xe64015cd, 0x0]
access-list #ACSACL#-IP-VPN_Dacl-53e9f721 permitted icmp for user 'Administrator' outside/10.10.10.10(3) -> ise/192.168.100.10(2) hit-cnt 1 first hit [0x9a816a15, 0x0]
Built inbound ICMP connection for faddr 192.168.100.10/0 gaddr 10.10.10.10/1 laddr 10.10.10.10/1(LOCAL\Administrator)
access-list #ACSACL#-IP-VPN_Dacl-53e9f721 permitted icmp for user '<unknown>' ise/192.168.100.10(0) -> outside/10.10.10.10(0) hit-cnt 1 first hit [0x9a816a15, 0x0]
```

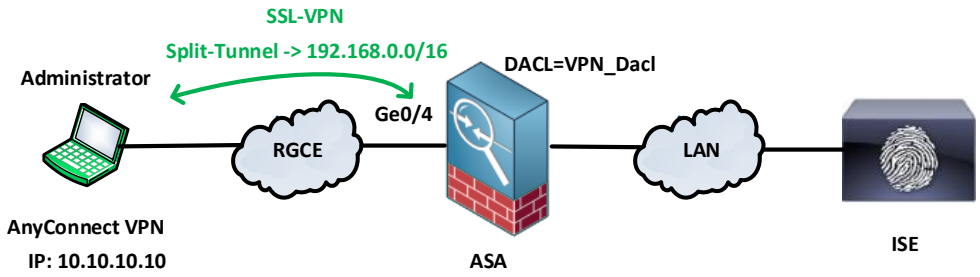
Kuvio 93. ASA:n Syslog viestit pääsylistasta

Kuvion ensimmäisellä punaisella merkitystä alueesta voidaan huomata pääsylistan nimi VPN_Dacl, joka liikenteeseen ottaa kiinni. Jälkimmäisestä punaisella merkitystä alueesta huomataan, että ASA sallii http-liikenteen palvelimelle, ISE:llä määritetyn DACL:n mukaisesti. Kuvion muista kohdista huomataan saman säännön pätevän myös sallittuihin ICMP-viesteihin.

Tässä vaiheessa SSL-VPN yhteys on toiminnassa halutulla tavalla. ASA:lla oli määritelty tunnelin yhteyteen myös Split-Tunnel-ominaisuus, joka ohjaa tunnelin läpi liiken-

teen ainoastaan sisäverkkoon. Kaikki muu liikenne menee VPN-koneelta laitteen oletusyhdyskäytävää pitkin RGCE-verkkoon. Kyseisen ominaisuuden kuin myös muun VPN-konfiguraation voi tarkastaa liitteessä olevasta ASA:n konfiguraatioista.

Tässä vaiheessa testaaminen on päättynyt VPN osalta. Kuviossa 94 on havainnollistettu lopullinen tilanne.



Kuvio 94. Lopputilanne VPN-kirjautumisen jälkeen

6 Pohdinta

Opinnäytetyön toteuttaminen oli haastavaa. Tavoitteena oli toteuttaa identiteetteihin pohjautuva verkkoympäristö, jossa hyödynnettäisiin TrustSec-komponentteja mahdollisuuksien mukaan. Ympäristön pohjana käytettiin opinnäytetyön tekijän edellisellä kesällä suunnittelemaa ympäristöä palveluineen. Vapaat kädet TrustSec-ominaisuuksien toteuttamisessa toivat omat haasteensa, jotta tilaajaan vaatimukset täyttyisivät.

Oikeaan ympäristöön työssä testattujen ominaisuuksien lisääminen olisi haastavaa jo yksinään siitä syystä, että palveluja olisi paljon enemmän. Yhteensopivuusongelmia jouduttaisiin ratkomaan laitekohtaisesti ja transitio pitäisi jakaa useaan vaiheeseen. Ongelmana ratkaisussa on myös, että kattava toteutus vaatisi Cisco-pohjaisen ympäristön, jotta mahdollisimman monia ominaisuuksia saataisiin toteutettua.

Suurimmat ongelmat työssä liittyivät erilaisiin ohjelmistovikoihin, jotka estivät haluttujen ominaisuuksien toimimisen. Verkkolaitteita liittäessä SGA-ympäristöön mikään laitteista ei pystynyt lataamaan *”Environment dataa”*, vaikka PAC-tiedoston lataus onnistui ongelmitta. Tämä esti mm. sen, etteivät laitteet saaneet SG-tauluja tai SGA-palvelimen osoitetta ISE:ltä. Ongelma ratkesi lähes kokonaan asentamalla viimeisin ohjelmistopaikkaus ISE:lle.

Autentikointitapahtumat onnistuivat odotetulla tavalla lukuunottamatta käyttäjän autentikoimista langattomassa verkossa oman laitteen kanssa. Tässä oli tarkoitus käyttää hyväksi Apple IPad:in natiivia EAP-FAST-metodia tukevaa supplikanttia, mutta tarkempi tutkiskelu osoitti, että konfiguroiminen olisi vaatinut erillisen ohjelman lataamisen kyseiseen laitteeseen. JYVSECTEC:llä ei ollut omaa laitetta testausta varten, joten tämä toi ongelmia. Toimeksiantajan päätöksestä testauksesta päätettiin luopua ja siirtää se myöhempään vaiheeseen.

Verrattaessa aikaisempiin palomuurisääntöihin, oli konfiguroiminen SGFW-ominaisuuden avulla yksinkertaisempaa. Sääntöjä ei tarvitse sitoa tiettyihin aliverkkoihin tai yksittäisiin osoitteisiin. Testausympäristön pienuus ei kuitenkaan anna täyt-

tä kuvaa siitä, miten ominaisuudet toimisivat kun laitteita on suurempi määrä. Tilanne kuitenkin antoi hyvän kuvan siitä miten sääntöjen luominen pienenee huomattavasti, koska käytettävät politiikat perustuvat SG-ryhmiin.

Opinnäytetyöhön olisi voinut lisätä vielä runsaasti ominaisuuksia varsinkin ISE:n avulla, mutta tämä olisi tehnyt työstä liian laajan. Tästä päätettiin jo suunnitteluvaiheesta. Jatkokehitysmahdollisuuksia ympäristössä on useita, joista osan toteuttamisesta on sovittu. Cisco Prime Infrastructure liitetään ympäristöön ja integroidaan ISE:n kanssa, jotta saadaan tietoa mm. autentikoinneista ja langattoman verkon toimivuudesta. Ympäristön käyttöä voidaan myös helpottaa mahdollistamalla 802.1X-autentikointi virtuaalikoneilla, joka ei toiminut opinnäytetyön tekemisen aikana. Ympäristöön voisi lisätä myös useita eri autentikointi-menetelmiä mm. sertifikaatteihin perustuen, jotta esimerkiksi koulutustilanteessa näiden toteuttaminen ja esitteleminen olisi yksinkertaista. Ympäristöön liitetään myöhemmin kattavammat profilointimenetelmät, kuten myös posture-check-ominaisuus.

LÄHTEET

Brown, E L. 2007. 802.1X Port Based Authentication. Boca Raton: Auerbach Publications.

Carrol, B., Banga, P. & Santuka, V. 2011. AAA Identity Management Security. http://www.jamk.fi/fi/Palvelut/kirjasto/Etusivu/ , Nelli-portaali, Books24x7.

Cisco Arch Over. TrustSec arkkitehtuuri. 2011. Viitattu 14.1.2014. http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.pdf

Cisco Live-BRKSEC-1022. 2011. Introduction to TrustSec-PDF. Viitattu 17.7.2014. https://www.ciscolive.com/online/connect/publicDashboard.ww

Geir, J. 2008. Implementing 802.1X Security Solutions for Wired and Wireless Networks. http://www.jamk.fi/fi/Palvelut/kirjasto/Etusivu/ , Nelli-portaali, Books24x7.

IEEE 802.1X-2010. Viitattu 14.3.2014
http://www.jamk.fi/fi/Palvelut/kirjasto/Etusivu/ , Nelli-portaali, IEEE Xplore

IEEE 802.1AE-2006. Viitattu 21.8.2014
http://www.jamk.fi/fi/Palvelut/kirjasto/Etusivu/ , Nelli-portaali, IEEE Xplore

IETF RFC 2865. 2000. Viitattu 16.4.2014
http://www.ietf.org/rfc/rfc2865.txt

IETF RFC 2866. 2000. Viitattu 16.4.2014
http://tools.ietf.org/html/rfc2866

IETF RFC 3748. 2004. Viitattu 16.4.2014.
http://tools.ietf.org/html/rfc3748

IETF RFC 4851. 2007. Viitattu 16.4.2014.
http://tools.ietf.org/html/rfc4851

IETF RFC 5422. 2009. Viitattu 16.4.2014.
http://tools.ietf.org/html/rfc5422

ISE User Guide 1.2 .15.7.2014. ISE:n käyttöopas PDF. Viitattu 4.8.2014
http://www.cisco.com/en/US/docs/security/ise/1.2/user_guide/ise_ug.pdf

JYVSECTEC. 2014 .JYVSECTEC-hankkeen kotisivut. Viitattu 14.4.2014.
http://www.jyvsectec.fi/

JYVSECTEC-RGCE. 2014 .JYVSECTEC-RGCE-ympäristö. Viitattu 15.8.2014.
http://www.jyvsectec.fi/rgce/

MACSec Deploy Guide. 2011. MACSec-yleiskatsaus PDF. Viitattu 6.8.2014 http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/deploy_guide_c17-663760.pdf

MACSec Switch Guide. MACSec-konfigurointiohje PDF. Viitattu 15.8.2014 http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_1_e/configuration/guide/scg3750x/swmacsec.html

RADIUS-Client. 29.3.2012. Viitattu 13.2.2014. http://technet.microsoft.com/en-us/library/cc754033.aspx

Tietotekniikan koulutusohjelma. 2010. JAMKin tutkintokuvaus. Viitattu 14.3.2014 https://asio.jamk.fi/pls/asio/asio_rakenne_julkaisu.rakenne_osaamisalue?ckohj=IIT&csuunt=99999&cvuosi=0S&caste=N&cark=2010-2011

Tutustu JAMKiin. 2013. JAMKin kotisivut. Viitattu 21.1.2013 http://www.jamk.fi/fi/Tietoa-JAMKista/Tutustu-JAMKiin/

TrustSec-AAG. Cisco TrustSec-esite PDF. 2014. Viitattu 4.8.2014 http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec_aag.pdf

TrustSec Products. TrustSec 5.0 tuotteet-PDF. 2014. Viitattu 24.8.2014 http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/c96-731479-00-secure-access.pdf

Velte, Anthony T., Velte, Toby J, .2014. Cisco: A Beginner's Guide, Fifth Edition. http://www.jamk.fi/fi/Palvelut/kirjasto/Etusivu/ , Nelli-portaali, Books24x7.

LIITTEET

Liite1. Verkkolaitteiden peruskonfiguraatiot

Cisco ASA, C3560X ja C3750X nimeäminen ja VLAN:ien luonti

```
Switch# configure terminal
Switch (conf)# hostname 3560X-Lower
3560X-Lower#
```

VLAN:ien luonti kytkimille tapahtui komennolla:

```
3560X-Lower(conf)#vlan 1000
3560X-Lower(conf-vlan)# name ise
```

Kytkimien rajapinnat konfiguroitiin seuraavalla tavalla riippuen käyttötarkoituksesta. Seuraavassa on esitetty trunk-portin konfigurointi 3560X-Lower-kytkimellä.

```
3560X-Lower(conf)# interface GigabitEthernet 0/4
3560X-Lower(conf-if)# switchport mode trunk
3560X-Lower(conf-if)# switchport trunk encapsulation dot1q
3560X-Lower(conf)# description link to ASA
3560X-Lower(conf-if)# no shutdown
```

VLAN-rajapinnat luotiin hallintaa varten kytkimille komennoilla:

```
3560X-Lower(conf)# interface vlan 3513
3560X-Lower(conf-if)# ip address 192.168.5.125 255.255.255.128
```

ASA:n ali-rajapinnat luotiin seuraavalla tavalla. Määritettävänä oli IP-osoitteiden ja VLAN:nien lisäksi mm. Security Levelit, joilla verkon eri osa-alueille voidaan asettaa ”luottamustasot”.

```
cisco-asa(conf)# interface GigabitEthernet 0/0.255
cisco-asa(conf-if)# description wlc-vlan
cisco-asa(conf-if)# nameif wlc
cisco-asa(conf-if)# security-level 100
cisco-asa(conf-if)# ip address 192.168.255.1 255.255.255.0
```

Laitteet lisättiin mac.sectec-toimialueeseen, määritettiin NTP-palvelin ja DNS-palvelin seuraavalla tavalla:

C3560X-Lower(conf)# ip domain-name mac.sectec
C3560X-Lower(conf)# ip name-server 192.168.3.3
C3560X-Lower(conf)# ntp-server 192.168.3.2

SNMP konfiguroitiin kytkimille ja ASA:lle RO-tilaan komennolla.

C3560X-Lower(conf)# snmp server community ciscocts RO

WLC

Rajapinnat WLC:lle luodaan kohdasta

Controller -> Interfaces

”New”-painikkeesta lisätään uusi rajapinta, johon määritetään mm. nimi, portti, VLAN, IP-osoite jne.

WLAN luodaan kohdasta

WLAN’s

”Create New”-painikkeesta luodaan uusi WLAN, johon määritetään mm. profiilin nimi ja SSID. Kyseiseen WLAN:in asetuksista *”General”*-kohdasta valitaan haluttu rajapinta tai rajapintaryhmä ja asetaan *”Status”*- kohdan tilaksi *”Enabled”*. *”Security”* välileh-deltä asetetaan halutut L2-politiikat.

ASA-VPN peruskonfigurointi

ASA:n VPN-yhteyttä varten konfiguroitiin VPN-seuraavasti. Ensin luodaan DHCP-pool josta osoitteet laitteille jaetaan.

cisco-asa# ip local pool VPN_pool 10.10.10.10-10.10.10.20 mas 255.255.255.0

Split-tunnelointi mahdollistaa ainoastaan halutun liikenteen kuljettamisen VPN:yhteyden läpi. Tunnelia varten luotiin ensin pääsylista, joka ottaa huomioon sisäverkkoon kohdistuvan liikenteen.

cisco-asa# access-list VPN_split standard permit 192.168.0.0 255.255.0.0

VPN kytketään päälle seuraavasti. määritettävänä on rajapinta, johon yhteydet luodaan sekä mahdollisesti ladattava Anyconnect-sovellus. Lopuksi VPN kytketään päälle.

```
cisco-asa (config)# webvpn
cisco-asa(config-webvpn)# webvpn
cisco-asa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
cisco-asa(config-webvpn)# anyconnect enable
```

Oletusyhteys-profiilin (Default WEBVPNGroup Policy) lisätään luotu DHCP-pool, sekä autentikointipalvelimeksi ISE.

```
cisco-asa (config)#tunnel-group DefaultWEBVPNGroup general attributes
cisco-asa (config-tunnel-general)# address-pool VPN_pool
cisco-asa (config-tunnel-general)# authentication-server-group SGA_ISE
```

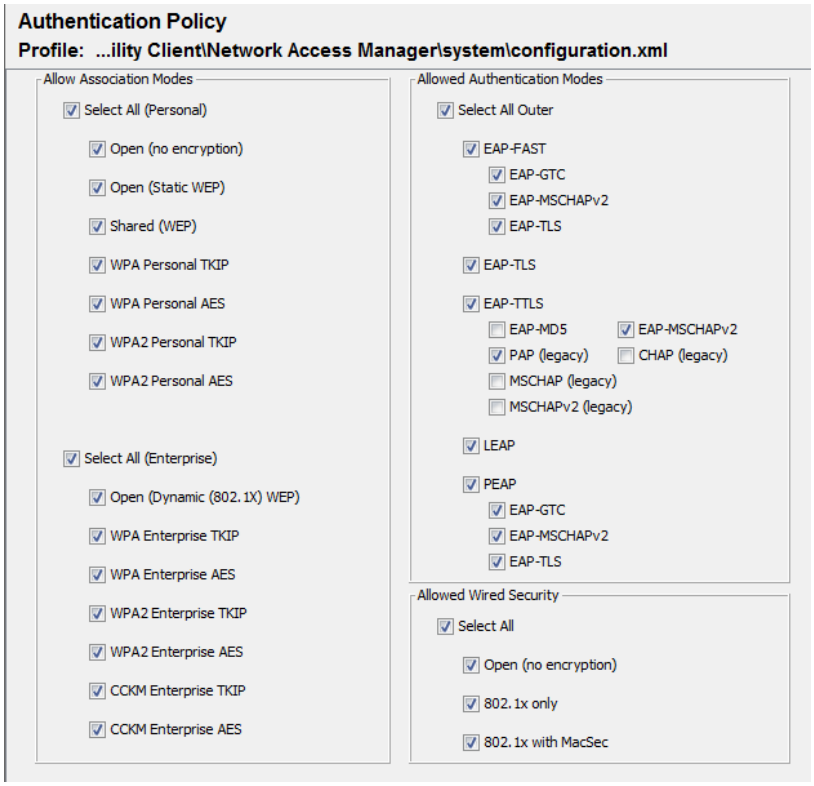
Split-tunnelointia varten luodaan standardi pääsylista, jossa määritellään osoitealue, johon kohdistuva liikenne ohjataan tunneliin.

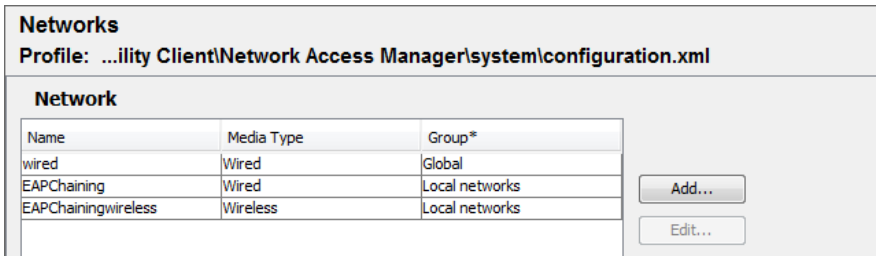
```
cisco-asa(config)# access-list VPN_split standard permit 192.168.0.0 255.255.0.0
```

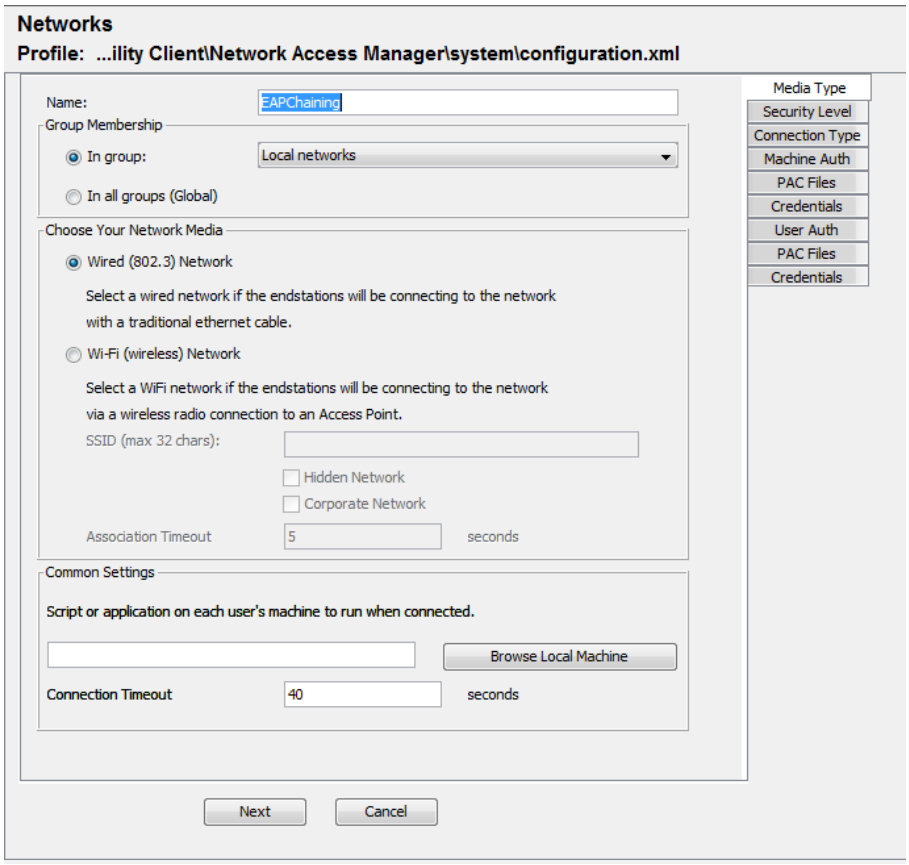
Oletus Group policyyn (DfltGrpPolicy) lisätään mm. tunnelointiprotokollat ja Split-tunnelin tiedot.

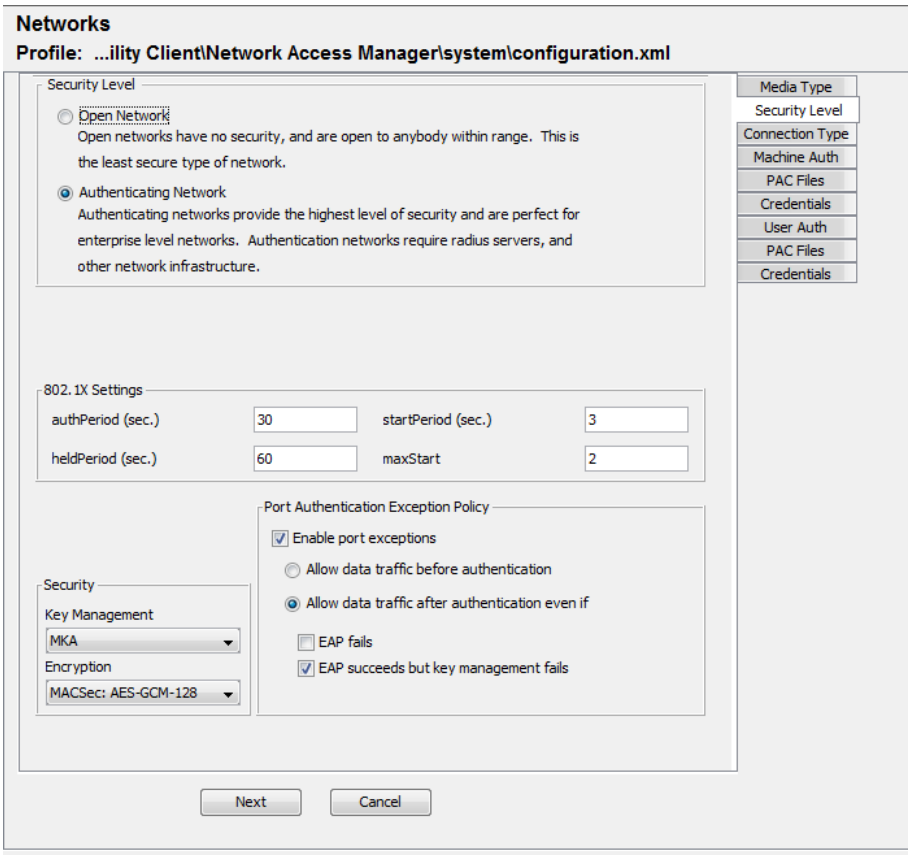
```
cisco-asa(config)#group-policy DfltGrpPolicy attributes
cisco-asa(config-group-policy)#vpn-tunnel-protocol ssl-client ssl-clientless
cisco-asa(config-group-policy)# split-tunnel-policy tunnelspecified
cisco-asa(config-group-policy)# split-tunnel-network-list value VPN_split
cisco-asa(config-group-policy)#default-domain value mac.sectec
```

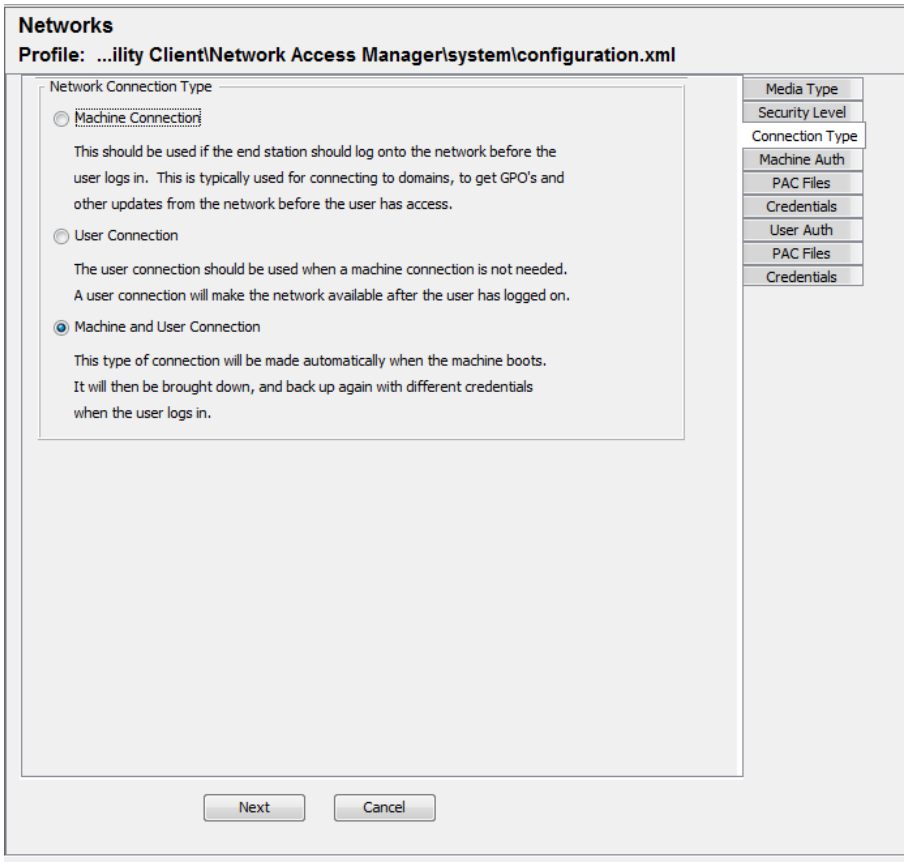
Liite 2: Anyconnect Secure Mobility Client NAM-profiilin luonti

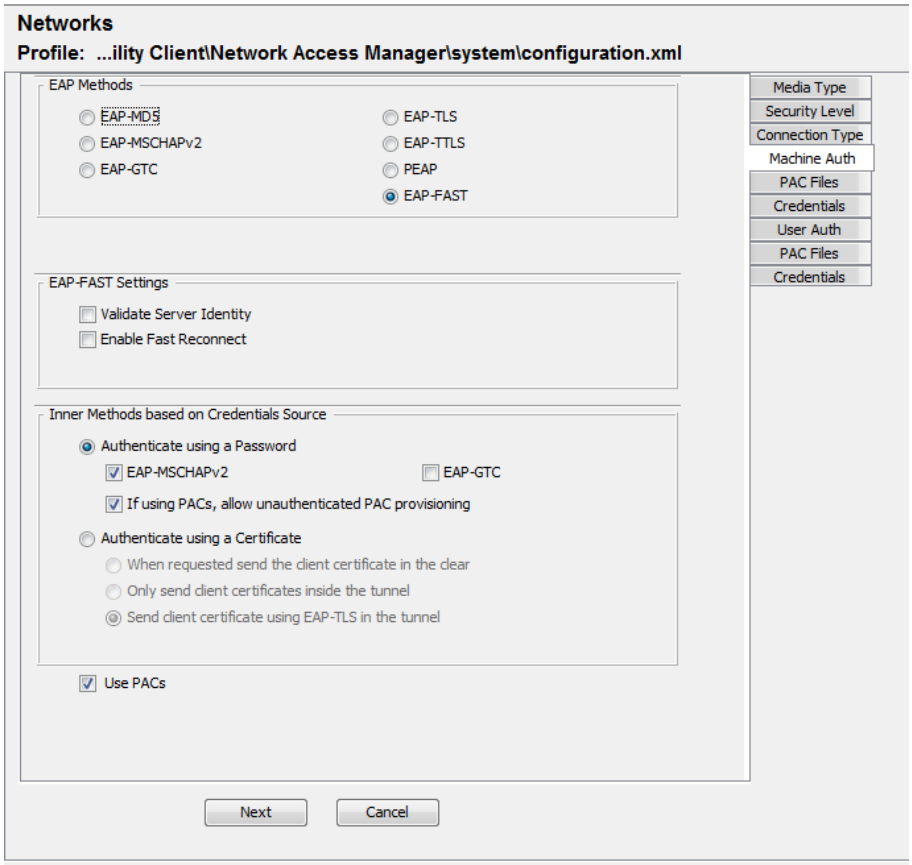


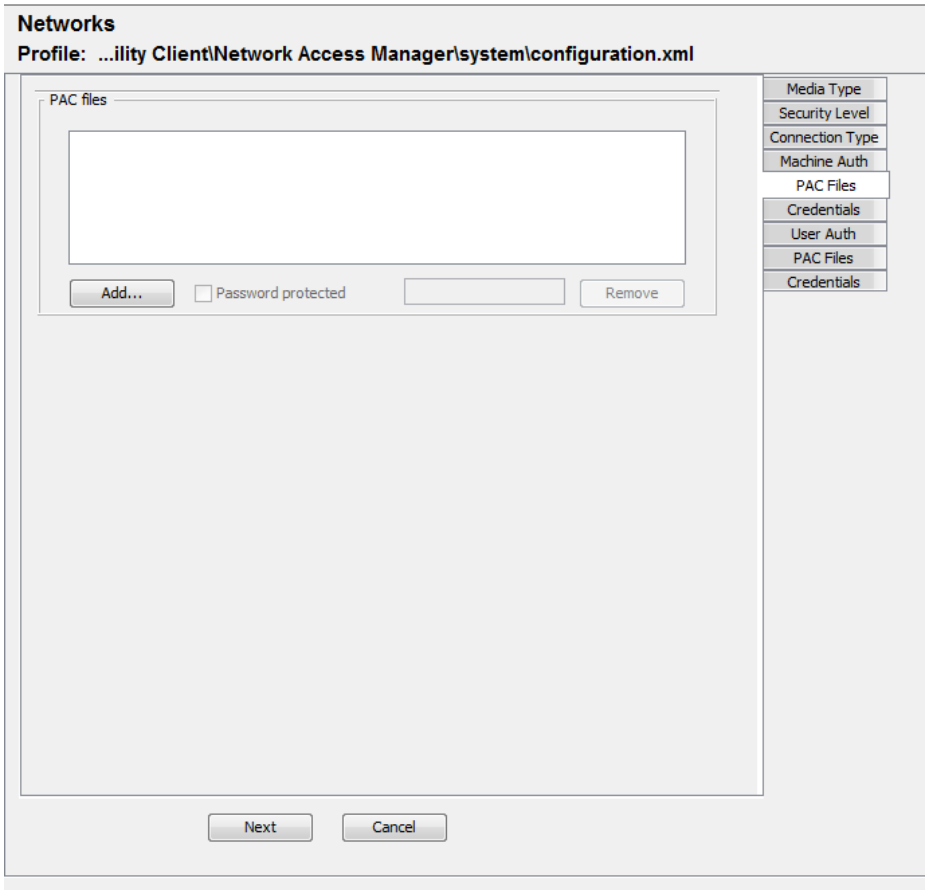


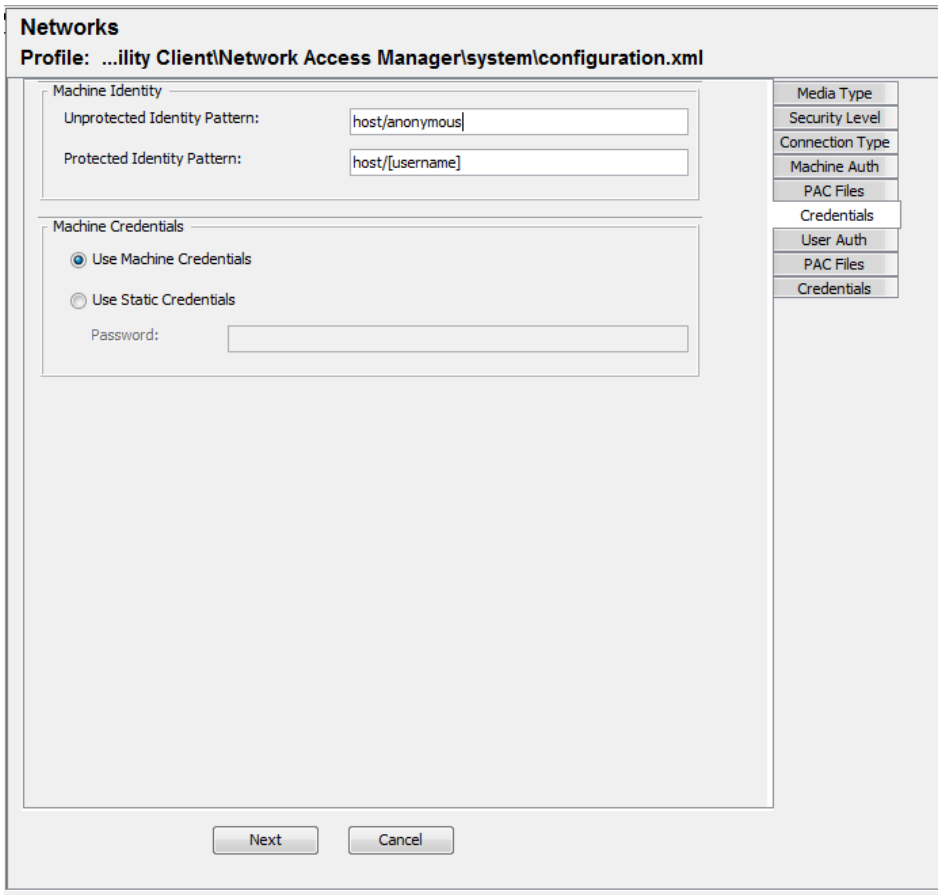

Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Name:
EAPChaining
Group Membership
In group:
Local networks
In all groups (Global)
Choose Your Network Media
Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.
Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.
SSID (max 32 chars):
Hidden Network
Corporate Network
Association Timeout
5
seconds
Common Settings
Script or application on each user's machine to run when connected.
Browse Local Machine
Connection Timeout
40
seconds
Next
Cancel
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials

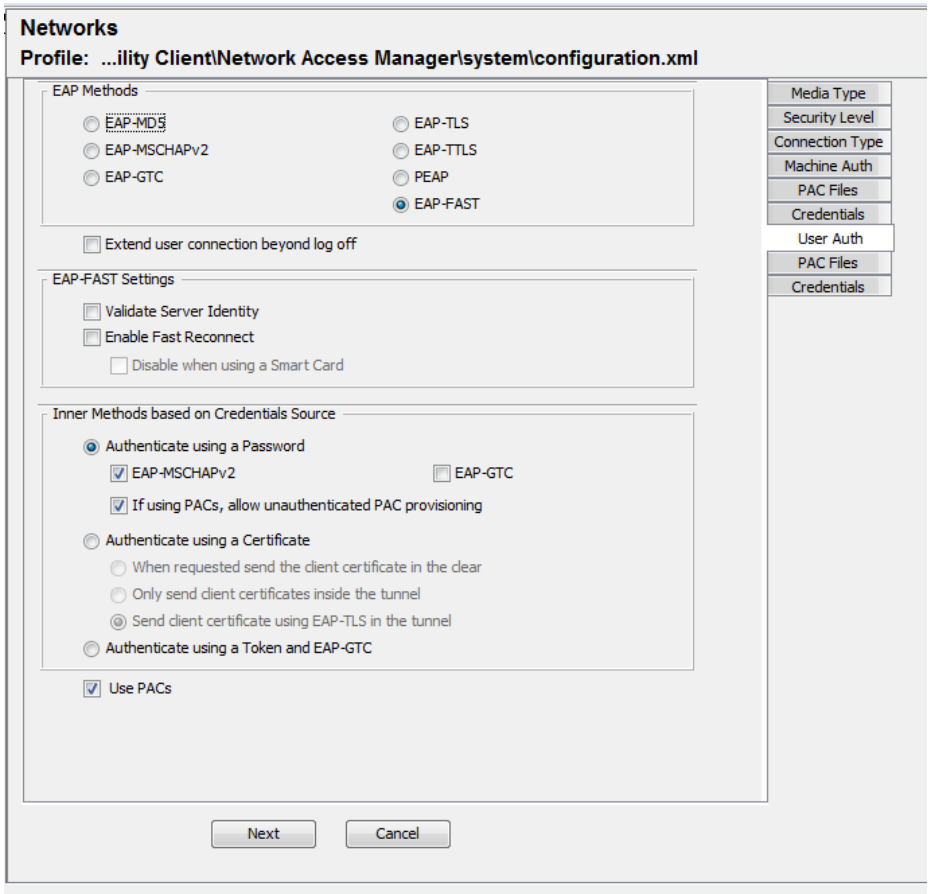

Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Security Level
Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.
Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.
802.1X Settings
authPeriod (sec.)
30
startPeriod (sec.)
3
heldPeriod (sec.)
60
maxStart
2
Port Authentication Exception Policy
Enable port exceptions
Allow data traffic before authentication
Allow data traffic after authentication even if
EAP fails
EAP succeeds but key management fails
Security
Key Management
MKA
Encryption
MACSec: AES-GCM-128
Next
Cancel
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials

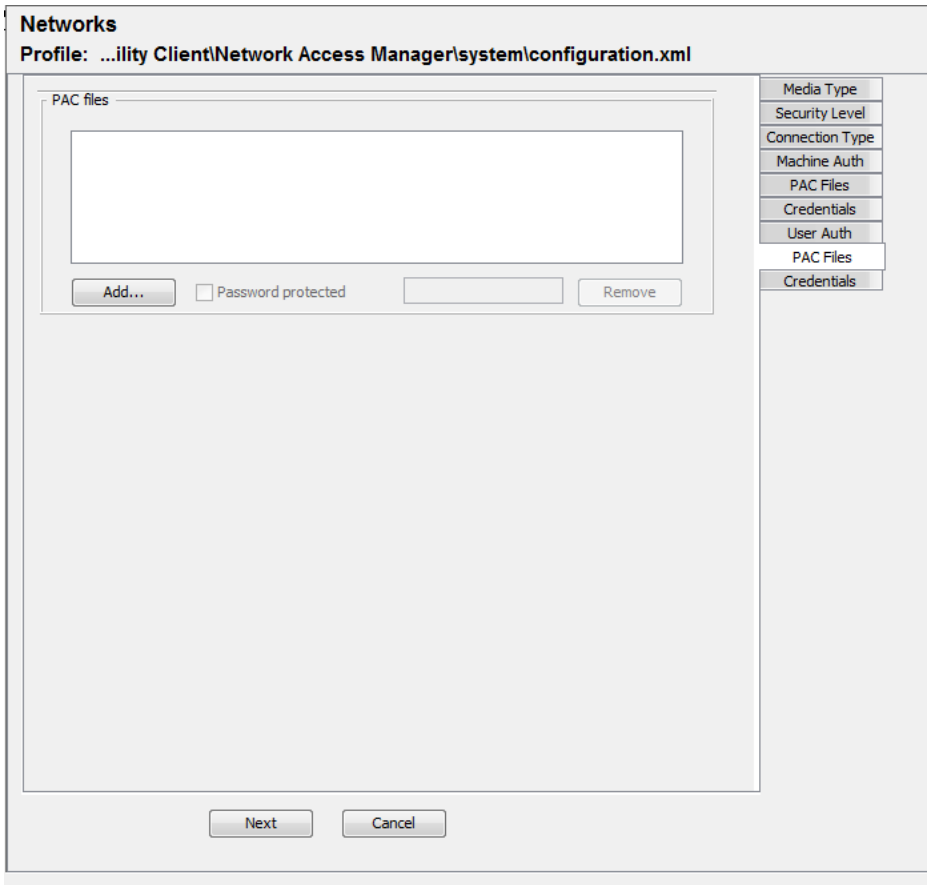

Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Network Connection Type
Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.
User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.
Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Next
Cancel

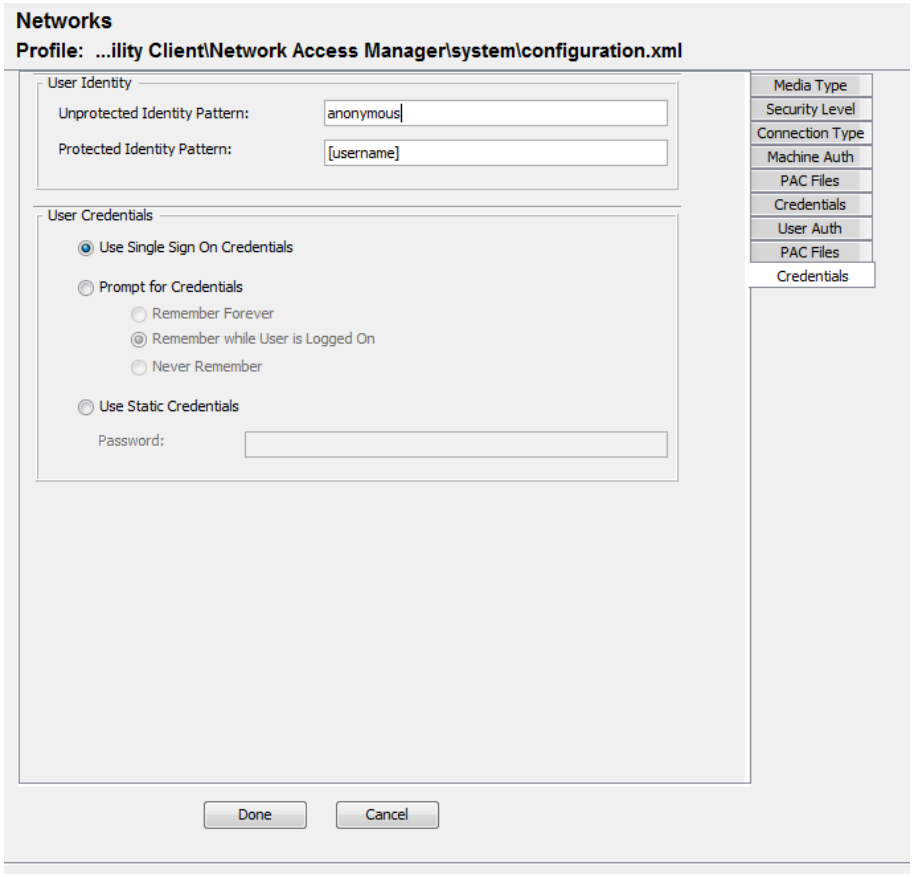

Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
EAP Methods
EAP-MD5
EAP-MSCHAPv2
EAP-GTC
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
EAP-FAST Settings
Validate Server Identity
Enable Fast Reconnect
Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
EAP-GTC
If using PACs, allow unauthenticated PAC provisioning
Authenticate using a Certificate
When requested send the client certificate in the clear
Only send client certificates inside the tunnel
Send client certificate using EAP-TLS in the tunnel
Use PACs
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Next
Cancel


Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
PAC files
Add...
Password protected
Remove
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Next
Cancel


Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Machine Identity
Unprotected Identity Pattern:
host/anonymous
Protected Identity Pattern:
host/[username]
Machine Credentials
Use Machine Credentials
Use Static Credentials
Password:
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Next
Cancel


Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
EAP Methods
EAP-MD5
EAP-MSCHAPv2
EAP-GTC
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
Extend user connection beyond log off
EAP-FAST Settings
Validate Server Identity
Enable Fast Reconnect
Disable when using a Smart Card
Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
EAP-GTC
If using PACs, allow unauthenticated PAC provisioning
Authenticate using a Certificate
When requested send the client certificate in the clear
Only send client certificates inside the tunnel
Send client certificate using EAP-TLS in the tunnel
Authenticate using a Token and EAP-GTC
Use PACs
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Next
Cancel


Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
PAC files
Add...
Password protected
Remove
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Next
Cancel


Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
User Identity
Unprotected Identity Pattern:
anonymous
Protected Identity Pattern:
[username]
User Credentials
Use Single Sign On Credentials
Prompt for Credentials
Remember Forever
Remember while User is Logged On
Never Remember
Use Static Credentials
Password:
Media Type
Security Level
Connection Type
Machine Auth
PAC Files
Credentials
User Auth
PAC Files
Credentials
Done
Cancel

Liite 3: Pikaopas TrustSec-ympäristöön

Tämän ohjeen tarkoitus on esitellä peruskonfigurointi TrustSec-ominaisuuksiin liittyen. Tarkemmat selvitykset löytyvät opinnäytetyöstä.

Verkkolaitteiden lisääminen

Verkkolaitteet lisätään ISE:llä kohdasta

Administration -> Network Resources -> Network Devices

Kyseisiin asetuksiin määritellään IP-osoitteet ja tapauskohtaisesti RADIUS-ja SGA-asetukset.

SG-ryhmien luominen

SG-ryhmät luodaan ISE:llä kohdasta

Policy -> Policy Elements -> Results -> Security Group Access -> Security Groups

Luotuja ryhmiä voidaan käyttää valtuutuspolitiikassa kohdassa

Policy -> Authorization -> Permissions

SXP:n konfigurointi

SXP:n konfiguroiminen tapahtuu kytkemällä toiminto päälle ja luomalla oletus-salasana. Tämän jälkeen määritetään yhteydelle vastapuolen IP-osoite sekä rooli.

```
Switch (config)# cts sxp enable
Switch (config)# cts sxp default password  “WORD”
Switch (config)# cts sxp connection peer “IP-osoite” password default mode peer
“speaker/listener”
```

Yhteyden muodostumisen voi tarkastaa komennolla:

```
C3560X-Lower# show cts sxp connections
```

Kytkimen perus 802.1X-komennot (NDAC ja 802.1X)

Rajapinnan komennot suplikantille päin:

Switch(config)# interface “rajapinta”
Switch(config-if)# switchport mode access
Switch(config-if)# authentication order dot1x
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast

AAA-komennot (NDAC-seed-laitteelle ja 802.1X).

Switch (config)# aaa new-model
Switch (config)# aaa authentication dot1x default group radius
Switch (config)# aaa authorization network default group radius
Switch (config)# aaa authorization network ise group radius
Switch (config)# aaa accounting dot1x default start-stop group radius
Switch (config)# cts authorization list ise
Switch (config)# dot1x system-auth control

RADIUS-palvelimen lisääminen (PAC).

Switch (config)# radius-server host [ISE-IP] pac key ciscocts
Switch (config)# radius-server host [ISE-IP] auth-port 1812
Switch (config)# radius-server vsa send accounting
Switch (config)# radius-server vsa send authentication

Trunk-rajapintaan asetaan 802.1X-autentikointi (NDAC) toimintaan komennolla

Switch (config-if)# cts dot1x

Rajapinnat tulee molemminpuolin käyttää mahdollisesti alhaalla ja ylhäällä. Rajapinnat ja SAP:n onnistuminen voidaan tarkastaa komennolla:

Switch# show cts interfaces ”rajapinta”

Ongelmatilanteissa voidaan käyttää mm. seuraavia debug-komentoja

Switch# debug cts sap events
Switch# debug radius
Switch# debug cts environment-data [aaa, all, events]

ISE antaa myös yksityiskohtaista tietoa kaikkeen autentikointiin liittyen kohdasta

Operations -> Authentications

Liite 4: Laitteiden konfiguraatiot

ASA-5515X

```
ASA Version 9.1(4)
!
hostname cisco-asa
domain-name mac.sectec
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool VPN_pool 10.10.10.10-10.10.10.20 mask 255.255.255.0
!
interface GigabitEthernet0/0.10
 description myynti VLAN
 vlan 10
 nameif myynti
 security-level 100
 ip address 192.168.1.1 255.255.255.128
 dhcprelay information trusted
!
interface GigabitEthernet0/0.30
 description vierailija vlan
 vlan 30
 nameif vierailija
 security-level 100
 ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet0/0.70
 vlan 70
 nameif wlan-tyontekijat
 security-level 100
 ip address 192.168.7.1 255.255.255.0
 dhcprelay information trusted
!
interface GigabitEthernet0/0.100
 description Hallinto VLAN
 vlan 100
 nameif hallinto
 security-level 100
 ip address 192.168.6.1 255.255.255.0
 dhcprelay information trusted
!
interface GigabitEthernet0/0.255
 vlan 255
 nameif wlc
 security-level 100
 ip address 192.168.255.1 255.255.255.0
 dhcprelay information trusted
!
interface GigabitEthernet0/0.3513
```

```
 description MGMT VLAN
 vlan 3513
 nameif mgmt
 security-level 100
 ip address 192.168.5.1 255.255.255.128
 dhcprelay information trusted
!
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.40
 description palvelut VLAN
 vlan 40
 nameif palvelut
 security-level 100
 ip address 192.168.3.1 255.255.255.0
 dhcprelay server 192.168.3.3
!
interface GigabitEthernet0/1.1000
 description ISE-VLAN
 vlan 1000
 nameif ise
 security-level 100
 ip address 192.168.100.1 255.255.255.0
 dhcprelay information trusted
!
interface GigabitEthernet0/1.3514
 description mgmt2 vlan
 vlan 3514
 nameif mgmt2
 security-level 100
 ip address 192.168.5.129 255.255.255.128
 dhcprelay information trusted
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 description Link to RGCE
 nameif outside
 security-level 0
 ip address 91.223.107.2 255.255.255.0
!
interface Management0/0
 management-only
 nameif management
 security-level 0
 ip address 192.168.10.1 255.255.255.0
!
boot system disk0:/asa914-smp-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name mac.sectec
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network sisaverkko
 subnet 192.168.0.0 255.255.0.0
object network vpn-net
```

```
 subnet 10.10.10.0 255.255.255.0
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
object-group service DM_INLINE_SERVICE_1
 service-object icmp
 service-object tcp-udp destination eq www
access-list wlc_access_in extended permit ip security-group name SG_WLC any secu
rity-group name SG_PALVELUT any
access-list wlc_access_in extended permit object-group TCPUDP security-group nam
e SG_WLC any security-group name SG_Hallinto any eq www
access-list wlc_access_in extended permit tcp security-group name SG_WLC any hos
t 192.168.100.5 eq ftp
access-list wlc_access_in extended deny ip security-group name SG_WLC any any
access-list wlc_access_in extended permit ip any any
access-list wlan-tyontekijat_access_in extended permit ip security-group name SG
_WLAN any security-group name SG_PALVELUT any
access-list wlan-tyontekijat_access_in extended permit object-group DM_INLINE_SE
RVICE_1 security-group name SG_WLAN any security-group name SG_Hallinto any
access-list wlan-tyontekijat_access_in extended deny tcp security-group name SG_
WLAN any host 192.168.100.5 eq ftp
access-list wlan-tyontekijat_access_in extended deny icmp security-group name SG
_WLAN any security-group name SGA_Device_SGT any
access-list wlan-tyontekijat_access_in extended deny ip security-group name SG_W
LAN any any
access-list wlan-tyontekijat_access_in extended permit ip any any
access-list vpn_ftp standard permit host 192.168.100.5
access-list VPN_split standard permit 192.168.0.0 255.255.0.0
pager lines 24
logging enable
logging asdm informational
mtu management 1500
mtu myynti 1500
mtu vierailija 1500
mtu wlan-tyontekijat 1500
mtu hallinto 1500
mtu wlc 1500
mtu mgmt 1500
mtu palvelut 1500
mtu ise 1500
mtu mgmt2 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any hallinto
icmp permit any wlc
icmp permit any mgmt
icmp permit any palvelut
icmp permit any ise
icmp permit any mgmt2
asdm image disk0:/asdm-715-100.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (outside,any) source static vpn-net vpn-net
!
object network sisaverkko
 nat (any,outside) dynamic interface
access-group wlan-tyontekijat_access_in in interface wlan-tyontekijat
access-group wlc_access_in in interface wlc
route outside 0.0.0.0 0.0.0.0 91.223.107.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server SGA_ISE protocol radius
aaa-server SGA_ISE (ise) host 192.168.100.10
 key *****
 authentication-port 1812
 accounting-port 1813
cts server-group SGA_ISE
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 192.168.100.1
cts sxp connection peer 192.168.100.125 password default mode peer speaker
cts sxp connection peer 192.168.5.3 source 192.168.5.1 password default mode pee
r speaker
cts sxp connection peer 192.168.5.6 source 192.168.5.1 password default mode pee
r speaker
user-identity default-domain LOCAL
http server enable
http 192.168.10.0 255.255.255.0 management
http 192.168.100.0 255.255.255.0 ise
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcprelay server 192.168.3.3 palvelut
dhcprelay enable wlan-tyontekijat
dhcprelay enable hallinto
dhcprelay enable wlc
dhcprelay enable ise
dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.3.2
webvpn
 enable outside tls-only
 anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
 anyconnect enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value VPN_split
 default-domain value mac.sectec
username asa password aZ7OAJ42v6iRcnMu encrypted
tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool VPN_pool
 authentication-server-group SGA_ISE
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
```

```
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DD
CEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 9
  subscribe-to-alert-group configuration periodic monthly 9
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

WLC

```
cdp advertise-v2 enable
 country FI
 cts sxp enable
 cts sxp connection peer 192.168.255.3
 cts sxp connection default password ****
 cts sxp retry period 120
 cts sxp sxpversion 2
 database size 2048
 dhcp proxy disable
 dhcp opt-82 remote-id ap-mac
 local-auth method fast server-key ****
interface create ap-manager 255

interface create wlan_tyontekija 70
interface address dynamic-interface ap-manager 192.168.255.11 255.255.255.0 192.
168.255.1
interface address management 192.168.255.10 255.255.255.0 192.168.255.1
interface address virtual 1.1.1.1
interface address dynamic-interface wlan_tyontekija 192.168.7.5 255.255.255.0 19
```

```
2.168.7.1
interface dhcp management primary 192.168.3.3
interface vlan ap-manager 255
interface vlan management 255
interface vlan wlan_tyontekija 70
interface port ap-manager 1
interface port management 1
interface port wlan_tyontekija 1
wlan apgroup add default-group
wlan apgroup interface-mapping add default-group 1 ctsgroup
wlan apgroup nac-snmp disable default-group 1
snmp version v2c enable
snmp version v3 enable
snmp community create ciscocts
snmp community accessmode ro ciscocts
snmp community ipaddr 192.168.100.10 255.255.255.0 ciscocts
sysname Cisco_WLC
stats-timer realtime 5
stats-timer normal 180
time ntp interval 6000
time ntp server 1 192.168.3.2
wlan create 1 ciscocts ciscocts
wlan nac snmp disable 1
wlan nac radius enable 1
wlan interface 1 ctsgroup
wlan multicast interface 1 disable
wlan aaa-override enable 1
wlan security wpa akm  802.1x enable 1
wlan security wpa akm cckm timestamp-tolerance  1000 1
wlan security wpa wpa1 enable 1
wlan security wpa wpa1 ciphers aes enable 1
wlan enable 1
```

C3560X-Lower

```
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3560X-Lower
!
boot-start-marker
boot-end-marker
!
!
logging monitor informational
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
aaa new-model
!
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
!
```

```
!
aaa session-id common
system mtu routing 1500
device-sensor accounting
device-sensor notify all-changes
!
!
!
ip dhcp snooping vlan 1000
no ip dhcp snooping information option
ip dhcp snooping database flash:snoopingdatabase.txt
ip dhcp snooping
ip domain-name mac.sectec
ip name-server 192.168.3.3
ip device tracking
epm logging
vtp mode off
!
!
crypto pki trustpoint TP-self-signed-1960113152
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1960113152
 revocation-check none
 rsakeypair TP-self-signed-1960113152
!
cts authorization list ise
cts role-based sgt-map 192.168.3.2 sgt 3
cts role-based sgt-map 192.168.3.3 sgt 3
cts role-based sgt-map 192.168.6.10 sgt 4
cts role-based sgt-map 192.168.100.1 sgt 2
cts sxp enable
cts sxp default source-ip 192.168.100.125
cts sxp default password ciscocts
cts sxp connection peer 192.168.100.1 source 192.168.100.125 password default mo
de peer listener hold-time 0
!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 20
 name Tuotanto
!
vlan 30
 name Vierailijat
!
vlan 40
 name Palvelut
!
vlan 1000
 name ise-vlan
!
vlan 3514
 name MGMT2
!
lldp run
!
interface GigabitEthernet0/2
 description Link to c3750x-stack ge1/1/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 shutdown
!
interface GigabitEthernet0/3
 shutdown
!
interface GigabitEthernet0/4
 description Link to ASA
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface GigabitEthernet0/5
 description Palvelut
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet0/6
 description Win7-mgmt-pc
 switchport access vlan 1000
 switchport mode access
!
interface GigabitEthernet0/7
 description Palvelut
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet0/24
 description ISE
 switchport access vlan 1000
 switchport mode access
!
interface Vlan1000
 description ISE-MGMT
 ip address 192.168.100.125 255.255.255.0
 no ip route-cache
!
interface Vlan3514
 description mgmt2 vlan
 ip address 192.168.5.130 255.255.255.128
 no ip route-cache
!
ip default-gateway 192.168.5.129
ip forward-protocol nd
!
ip http server
ip http secure-server
!
snmp-server community ciscocts RO
snmp-server trap-source Vlan3513
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host 192.168.100.10 version 2c ciscocts

!
radius-server host 192.168.100.10 auth-port 1812 acct-port 1813 pac key ciscocts
radius-server vsa send authentication
radius-server vsa send accounting
!
line con 0
 logging synchronous
line vty 5 15
!
!
```

```
monitor session 1 source interface Gi0/24
monitor session 1 destination interface Gi0/10 encapsulation replicate
ntp server 192.168.3.2
mac address-table notification change
mac address-table notification mac-move
end
```

C3750X-Stack

```
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3750X-stack
!
boot-start-marker
boot-end-marker
!
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
aaa new-model
!
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
switch 1 provision ws-c3750x-24
switch 2 provision ws-c3750x-24
system mtu routing 1500
device-sensor accounting
device-sensor notify all-changes
!
ip domain-name mac.sectec
ip name-server 192.168.3.3
ip device tracking
epm logging
vtp mode off
!
crypto pki trustpoint TP-self-signed-1961305984
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1961305984
 revocation-check none
 rsakeypair TP-self-signed-1961305984
!
cts authorization list ise
cts role-based sgt-map 192.168.3.2 sgt 3
cts role-based sgt-map 192.168.3.3 sgt 3
cts role-based sgt-map 192.168.6.10 sgt 4
cts role-based sgt-map 192.168.100.1 sgt 2
cts sxp enable
cts sxp default password ciscocts
cts sxp connection peer 192.168.255.10 source 192.168.255.3 password default mod
e peer speaker hold-time 0 0
cts sxp connection peer 192.168.5.1 source 192.168.5.6 password default mode pee
```

```
r listener hold-time 0
!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 70
 name wlc-tyontekijat
!
vlan 100
 name hallinto
!
vlan 255
 name wlc
!
vlan 3513
 name mgmt
!
lldp run
!
interface GigabitEthernet1/0/1
 description link to wlc
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 description Link to 3560x-upper
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
!
interface GigabitEthernet1/0/10
 switchport mode access
 shutdown
 authentication order dot1x
 authentication port-control auto
 macsec
 mka default-policy
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 spanning-tree portfast
!
interface GigabitEthernet1/0/23
 description link to hp-aironet
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet1/1/2
 description Link to c3560x-lower ge0/2
 switchport trunk encapsulation dot1q
!
interface Vlan255
 ip address 192.168.255.3 255.255.255.0
 ip helper-address 192.168.3.3
!
interface Vlan3513
```

```
 ip address 192.168.5.6 255.255.255.128
 no ip route-cache
!
ip default-gateway 192.168.5.1
ip forward-protocol nd
!
ip http server
ip http secure-server
!
snmp-server community ciscocts RO
snmp-server trap-source Vlan3513
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host 192.168.100.10 version 2c ciscocts
!
radius-server host 192.168.100.10 auth-port 1812 acct-port 1813 pac key ciscocts
radius-server vsa send authentication
radius-server vsa send accounting
!
line con 0
 logging synchronous
line vty 5 15
!
ntp server 192.168.3.2
end
```

C3560X-Upper

```
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3560X-Upper
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
aaa new-model
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
system mtu routing 1500
device-sensor accounting
device-sensor notify all-changes
!
ip dhcp snooping vlan 100
ip dhcp snooping database flash:snoopingdatabase.txt
ip domain-name mac.sectec
ip name-server 192.168.3.3
```

```
ip device tracking
epm logging
vtp mode off
!
!
crypto pki trustpoint TP-self-signed-1960611712
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1960611712
 revocation-check none
 rsakeypair TP-self-signed-1960611712
!
cts authorization list ise
cts role-based sgt-map 192.168.3.2 sgt 3
cts role-based sgt-map 192.168.3.3 sgt 3
cts role-based sgt-map 192.168.6.10 sgt 4
cts role-based sgt-map 192.168.100.1 sgt 2
cts sxp enable
cts sxp default source-ip 192.168.5.3
cts sxp default password ciscocts
cts sxp connection peer 192.168.5.1 source 192.168.5.3 password default mode pee
r listener hold-time 0
!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
 name Myynti
!
vlan 70
 name wlan_tyontekijat
!
vlan 100
 name Hallinto
!
vlan 255
 name wlc
!
vlan 3513
 name mgmt
!
interface GigabitEthernet0/2
 description Link to 3750x-ge1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
!
interface GigabitEthernet0/4
 description link to ASA
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/6
 description http-palvelin
 switchport access vlan 100
 switchport mode access
!
interface Vlan3513
 ip address 192.168.5.3 255.255.255.128
 no ip route-cache
!
```

```
ip default-gateway 192.168.5.1
ip forward-protocol nd
!
ip http server
ip http secure-server
!
snmp-server community ciscocts RO
!
radius-server host 192.168.100.10 auth-port 1812 acct-port 1813 pac key ciscocts
radius-server vsa send authentication
radius-server vsa send accounting
!
line con 0
 logging synchronous
line vty 5 15
!
ntp server 192.168.3.2
end
```