HAAGA-HELIA
ammattikorkeakoulu

# PK-yrityksen kokonaisvaltaisen tietoturvan käyttöönotto

Severi Sjöblom

Opinnäytetyö

13.12.2016

HAAGA-HELIA ammattikorkeakoulu

**Tiivistelmä**

Raportin palautuksen tai esityksen päivämäärä

Koulutusohjelma

| **Tekijä tai tekijät**<br>Severi Sjöblom | **Ryhmätunnus tai aloitusvuosi**<br>2010 |
|---|---|
| **Raportin nimi**<br>PK Yrityksen kokonaisvaltaisen tietoturvan käyttöönotto | **Sivu- ja liitesivumäärä**<br>34 |
| **Opettajat tai ohjaajat**<br>Juha Pispa | |


Opinnäytetyöni tarkoituksena on kuvata tietoturvan käyttöönotto vaihe vaiheelta. Käyttöönotto tehdään kuvitteelliselle PK-yritykselle, jolla on paljon erilaisia tietoturvatarpeita. Tavoitteena on, että työtä voidaan hyödyntää tulevaisuudessa oppaana asiakkaille.

Työni pohjautuu vahvasti teoriaan, jonka kautta lähestyn yrityksen kokonaisvaltaista tietoturvaa. Työssäni kerron tietoturvasta käsitteenä ja siitä miten se on muuttunut viime vuosien aikana. Työssä käydään läpi keskeisimmät aihealueet mitä tulee ottaa huomioon tietoturvaa suunniteltaessa. Aihealueita ovat hallinnollinen näkökulma tietoturvaa mietittäessä, huomioitava lainsäädäntö, henkilöstön merkitys tietoturvan suunnittelussa ja onnistumisessa, fyysinen tietoturva ja turvallisuus.

Raportissa käsitellään tietoturvan riskienhallintaa, erityisesti mitä osa-alueita tulee huomioida riskienhallinnan suunnittelussa ja seurannassa. Riskienhallintaan liittyy tiiviisti tietoturvan standardisointi.



**Asiasanat**
Tietoturva, Palomuuri, Riskien hallinta

HAAGA-HELIA
University of Applied Sciences

Degree programme

**Abstract**

Date of presentation

# Sisällys

# 1 Johdanto

Tietoturva on käsitteenä laaja ja alussa kerron mitä eri osa-alueita tulee huomioida. Työni keskittyy kuitenkin tietoturvan käyttöönottoon ja sen teknisiin osa-alueisiin, erityisesti palomuureihin. Raportin luvussa 2 keskityn tietoturva-käsitteeseen sekä siihen miksi sen on olennainen osa jokaisen yrityksen toimintaa. Luvussa 3 keskityn tietoturvan eri osa-alueisiin ja siihen mitä kaikkea tulee huomioida kattavaa tietoturvaa suunniteltaessa. Tässä luvussa käsittelen myös lyhyesti mitä eri lainsäädäntöjä tulee ottaa huomioon, menemättä näiden yksityiskohtiin. Luvussa 4 käsittelen tietoturvaan liittyvää riskienhallintaa, miten se voidaan luokitella ja mitä standardeja tähän on olemassa.

Alkupään lukujen jälkeen siirryn palomuureihin syvällisemmin ja kerron niiden yleisestä teknologiasta ja tarkoituksesta. Kerron, miten palomuuriteknologia on kehittynyt vuosien saatossa ja miltä se näyttää nyt. Teknologisen osion jälkeen, viimeisessä luvussa kuvaan vaihe vaiheelta palomuurin käyttöönoton kohdeyritykseni tarpeet huomioiden. Tämän työn tavoitteena on tarjota kokonaisvaltainen kuvaus tietoturvan merkityksestä, jossa lukijalle tarjotaan laajempi kuva tietoturvasta kokonaisuutena. Tämä kattaa kaiken teoriasta konkreettiseen käyttöönottoon.

# 2 Tietoturvan merkitys

Tietoturvan merkitys digitalisoituneessa yritysmaailmassa on kasvanut viime vuosien ajan. Tämä kehityssuunta jatkuu myös tulevaisuudessa ja kaiken kokoisten yritysten tulee kiinnittää siihen huomiota. Tietoturvan merkityksen muutosta voidaan miettiä esimerkiksi Internetin alkuaikojen kautta. Tavoitteena oli yhdistää tietokoneet toisiinsa, mutta pian huomattiin, että kaiken tiedon ei tule olla kaikkien saatavilla ja koneisiin tarvitaan suojausta ja hallintaa. (Hiltzik M. 2013) Myös media nostaa jatkuvasti esille tapauksia, joissa eri organisaatioihin tai järjestelmiin on tehty tietomurtoiskuja. Saatuja tietoja ovat muun muassa käyttäjätunnukset ja salasanat sekä organisaatioiden luottamukselliset asiakirjat. Suomessa esimerkiksi Viestintäviraston Kyberturvallisuus -sivusto tiedottaa verkkosivuillaan aktiivisesti tapahtuneista hyökkäyksistä ja havaituista järjestelmäheikkouksista. (www.viestintavirasto.fi)

## 2.1 Tietoturvan määrittely

Tietoturvalla tarkoitetaan kaikkia niitä toimia, joilla varmistetaan tietoaineistojen, -järjestelmien ja –palveluiden toimivuus ja suojaaminen. Tietoturva määritellään perinteisesti kolmen käsitteen avulla: luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuudella tarkoitetaan, että oikeilla henkilöillä on pääsy tarvittaviin tietoihin ja järjestelmiin. Luottamuksellisuus varmistetaan esimerkiksi salasanojen ja muiden todenteiden kautta. Eheys puolestaan tarkoittaa, että tiedot ovat luotettavasti saatavilla silloin kuin niitä tarvitaan. Eheyttä hoidetaan varmuuskopioilla ja tietoa korjaavilla koodeilla sekä varmistetaan, että tietoa ei voi muokata kuin valtuutetut tahot. Käytettävyys taas tarkoittaa, että jokaisella on mahdollisuus käyttää järjestelmiä eli käytännössä fyysisten laitteiden tulee olla toimivia ja mahdollistaa järjestelmien luottamuksellinen ja eheä käyttö. (Valtionhallinnon tietoturvasanasto 2008, s. 109; Karvi 2012, s.3)

## 2.2 Tietoturvan uudet lisämääritelmät

Nykyisin tietoruvassa kiinnitetään huomiota myös varmuuteen, autenttisuuteen sekä anonymiteettiin. Varmuudella tarkoitetaan sitä, että kaikki toimivat ja kaikki toimii, kuten on sovittu. Käytännössä tämä saavutetaan käyttösääntöjen, oikeuksien ja suojauksi-

en avulla. Autenttisuudella varmistetaan, että esimerkiksi komennot tulevat oikeilta tahoilta. Anonymiteetillä viitataan siihen, että käytössä olevaan dataa ei käytettä henkilökohtaisten tietojen keräämiseen ja näiden hyödyntämiseen (Karvi 2012, s. 4-5)

Uuden ajan tietoturva-ajatteluun voidaan lisätä myös maineenhallinta, joka osaltaan on luotettavuutta ja varmuutta. Esimerkkeinä maineeseen vaikuttavista tekijöistä voidaan mainita luottamuksellisten tietojen vuotaminen julkisuuteen ja virusten tarttuminen sivustolla käynnin jälkeen. Organisaatiot eivät välttämättä ymmärrä tai tiedosta tietoturvan merkitystä maineenhallinnassa ennen kuin jotain tapahtuu. Maineenhallinta voidaan nähdä myös osana riskienhallintaa, jota käsittelen luvussa 4. Ajankohtaisena esimerkkinä on suuri tietomurto, joka kohdistui asianajotoimisto Mossack Foncesan tietojärjestelmiin paljastaen miljoonittain luottamuksellisia ja arkaluontoisia asiakirjoja. (www.talouselmä.fi; www.yle.fi)

# 3 Tietoruvan osa-alueet

Perinteisesti tietoturva onkin jaoteltu eri osa-alueisiin, jotka yhdessä luovat tietoturva-kokonaisuuden. Nämä osa-alueet ovat:

- hallinnollinen tietoturva
- fyysinen turvallisuus ja suojausmekanismit
- henkilöstö
- käyttöturvallisuus
- tietoliikenne
- laitteistot
- ohjelmistot

(www.oph.fi)

Hallinnollinen tietoturva ja suojamekanismit ovat pohjana muille tietoturvan osa-aloille. Voidaan myös ajatella, että henkilöstö on vastuussa laitteiden, ohjelmien ja tietoliikenteen turvallisesta käytöstä. Tämä entisestään vahvistaa ajatusta siitä, että henkilöstön kouluttaminen tietoturva-asioissa on hyvin tärkeää. Tässä perinteisessä mallissa tuodaan esille myös välineistön ajantasaisuuden tärkeys eli vahvaa tietoturvaa on helpompi pitää yllä, kun laitteet ovat ajan mukaiset. (Laakso 2010, s. 9)

Tietoturva koostuu useasta eri tekijästä, kuten mainitsin yllä ja seuraavaksi käsittelen osa-alueittain miten ne vaikuttavat tietoturvakokonaisuuteen.

## 3.1 Hallinnollinen tietoturva

Kuinka tätä kaikkea hallinnoidaan ja kenen vastuulla on varmistaa, että aikaisemmin mainitut kriteerit luottamuksellisuus, eheys ja käytettävyys sekä varmuus, autenttisuus ja anonymiteetti toteutuvat. Hallinnan apuna voidaan käyttää PDCA-mallia, joka tulee englanninkielen sanoista Plan-Do-Check-Act. Vapaasti suomennettuna tämä tarkoittaa Suunnittele-Tee-Tarkasta-Toimi. Suunnitellessa määritellään yrityksen tietoturvatarpeet eli mitä kaikkea tulisi suojata ja millä tasolla. Tee –vaiheessa luodaan käytännössä määritelty tietoturva. Jo suunnitteluvaiheessa sekä itse toteutusvaiheessa organisaatio voi

käyttää apuna ulkoista asiantuntijaa, joka auttaa tarpeiden määrittelyssä sekä käytännön toteutuksessa. Tietoturvaongelmat saattavat johtua myös vääränlaisesta tietoturvaratkaisusta eli organisaatiossa ei ole ollut tarvittavaa asiantuntemusta määritellä minkälainen tietoturvakokonaisuus on tarpeen. Hallinnollinen tietoturva sisältää myös yleiset linjaukset henkilöstölle ja koulutus tietoturva-asioissa.

### 3.2 Fyysinen turvallisuus ja suojamekanismit

Fyysisellä turvallisuudella tarkoitetaan työskentelytilaa ja sen turvallisuutta, joka osaltaan vaikuttaa tietoturvaan esimerkiksi siten, että ulkopuolisissa ei ole pääsyä laitteisiin ja sitä kautta luottamukselliseen tietoon. Esimerkiksi tehokkaalla kulunhallinnalla voidaan edistää fyysistä turvallisuutta. Kulunhallinnalla voidaan seurata työntekijöiden liikkumista sekä luoda rajoituksia mihin kullakin työntekijällä on pääsy. Pienissä ja keskisuurissa yrityksissä kulunhallinta on yleensä vähäisempää ja seurataan lähinnä ulko-ovien käyttöä. Fyysinen turvallisuus sisältää myös tulipaloihin, vesivahinkoihin, sähkökatkoihin ja muihin vastaaviin tapaturmiin varautumisen.
Suojamekanismeilla tarkoitetaan esimerkiksi palomuureja ja virustentorjuntaohjelmistoja, varmuuskopiointia ja ohjelmistoturvallisuutta ja lisenssejä. 2010-luvulla puheenaiheeksi noussut todentaminen on myös olennainen osa suojausta. Todentaminen liittyy kiinteästi tietoturvan luotettavuuteen eli tällä varmistetaan keneltä käskyt tulevat ja minkälaiset oikeudet käyttäjällä on. Todentaminen voidaan hoitaa esimerkiksi salasanan tai PIN-koodin avulla. (Järvinen 2002, 24 – 27; Nietula 8 - 9)

### 3.3 Henkilöstö

Tietoruvalla ei tarkoiteta vain laitteita ja järjestelmiä vaan yrityksen henkilöstöllä on myös suuri rooli tietoturvan varmistamisessa. Varsinais-Suomen Yrittäjä –lehden tekemässä haastattelussa asiantuntija on todennut, että tietoturvasta n. 20 % tapahtuu teknisten ominaisuuksien kautta ja jäljelle jäävä 80 % tapahtuu hallinnollisten toimien kautta. (Laakso M. 2010.) Henkilöstön kouluttaminen onkin olennainen osa yrityksen tietoturvaa ja tulee luoda yhteiset pelisäännöt miten toimia. Esimerkiksi epäilyttävien linkkien klikkaaminen sähköpostista tai ohjelmistojen tietämätön lataaminen saattavat aiheuttaa vakaviakin tietoturvariskejä yrityksessä. (Kurittu 2015, s. 5-7, )

Henkilökunnan koulutuksessa voidaan tämän lisäksi keskustella vastuullisesta Internet-selailusta, vahvan salasanan luomisesta ja muista ajankohtaisista asioista. Kannattaa pitää mielessä, että tietoturva-alan ammattilaisille itsestään selvät asiat eivät välttämättä ole sitä tavalliselle työntekijälle. (www.andersinnovations.fi) Yle Savon teettämän tietoturvakyselyn perusteella henkilöstö nähtiin jopa suurimpana tietoturvauhkana yritykselle. (www.yle.fi) Henkilöstön lisäksi organisaation hallinnolliset toimet vaikuttavat tietoturvallisuuteen eli se miten järjestelmän autenttisuus on hoidettu ja sitä pidetään yllä jatkuvasti.

### 3.4 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan prosessien sujumista eli organisaation ydintoiminnot hoituvat saumattomasti tietoturvan kannalta. Tämä sisältää käyttäjätunnusten- ja salasanojen ja järjestelmien hallinnoinnin, varautumisen poikkeustiloihin, erinäiset palvelusopimukset sekä järjestelmän tilan seurannan. Käyttöturvallisuus nähdään yleisen luonteensa vuoksi ns. ylimääräisenä tietoturvan osa-alueena ja sen voikin nähdä tarkentavana ja kokoavana osana tietoturvaa. (Laakso M. 32; VAHTI ohje)

### 3.5 Tietoliikenne

Tietoliikenne osana tietoturvaa tarkoittaa, että taataan luotettava tiedon kulku eri toimijoiden välillä. PK-yrityksen arjessa tämä tarkoittaa, että verkko on suojattu riittävästi eikä ulkopuoliset tahot pääse siihen käsiksi. Tietoliikenneturvallisuutta voidaan edistää esimerkiksi ylläpitämällä laitteistoja, huolehtimalla verkonhallinnasta ja pääsynvalvonnasta. Tarkkaillaan tilannetta ja puututaan ongelmatilanteisiin heti niiden tultua ilmi. Tietoliikenteeseen kuuluu myös organisaation sisäiset dokumentit ja ohjeistus, miten informaatiota käsitellään, mihin se tallennetaan ja kenellä on oikeus tietoon. Apuna voidaan käyttää tietojen luokittelua. Tietoliikenneturvallisuuteen liittyy kiinteästi myös organisaatioon tuleva tieto. Laitteiden ja ohjelmistojen ajantasaisuus on tärkeää, jotta tuleva tieto tarkastetaan virusten varalta ja voidaan estää hyökkäykset. Tietoliikenneturvallisuuden varmistamisessa henkilöstöllä on suuri rooli kuten jo aikaisemmin mainitsin. (VAHTI-ohje)

### 3.6 Laitteistot

Tärkeä osa tietoturvaa on erilaiset suojausohjelmistot ja laitteet. Ensiksikin pitää identifioida yrityksen tarpeet, kuinka kattavaa tietoturvaratkaisua tarvitaan. Esimerkiksi sairaalat tarvitsevat tehokkaan ja kattavan tietoturvaratkaisun potilastietojen säilyttämistä varten kun taas ravintolalle saattaa riittää hieman kevyempi tietoturvaratkaisu. (Harju E. 2010) On myös tapauksia, joissa PK-yrityksen tietoturvan tarve voi olla samanlainen kuin suurellakin yrityksellä. Erottavana tekijänä näissä tapauksissa on usein budjetti, joka organisaatiolla on käytettävissä. Onneksi tietoturva-ala kehittyy jatkuvasti ja tarjolla on myös edullisempia, mutta hyviä, tietoturvaratkaisuja. Henkilökohtainen ammattilaisen mielipiteeni on, että tietoturva ei ole se asia, josta yrityksen kannattaa karsia kuluja. Luvussa 5.2 käsittelen tarkemmin oikeanlaisen tietoturvaratkaisun löytämistä ja keinoja siihen.

### 3.7 Ohjelmistot

Ohjelmistoturvallisuus kattaa kaikki käyttöjärjestelmät sekä muut ohjelmistot. Yleisimpiä ohjelmistoesimerkkejä ovat talous- ja henkilöstöhallinnon järjestelmät sekä toiminnanohjausjärjestelmät. Ajantasaiset ja ylläpidetyt ohjelmistot ovat myös oleellinen osa kokonaisvaltaista tietoturvaratkaisua. Tietoturva kehittyy jatkuvasti ja usein, jotta se voi toimia halutulla tavalla, se tarvitsee tuekseen ajanmukaiset ohjelmistot. Lisäksi ohjelmistojen tulee olla laadukkaita ja niitä tulee voida kehittää ja päivittää muuttuvien tarpeiden mukaan. Turvallisuuteen voidaan vaikuttaa muun muassa teknisillä turvakeinoilla. Käyttäjäoikeuksien hallinta on yksi käytetty keino, jolla rajoitetaan esimerkiksi ohjelmistojen asennusoikeuksia ja muita pääkäyttäjän toimintoja. (VAHTI-ohje)

### 3.8 Lainsäädäntö

Organisaation tietoturvaan liittyviä kysymyksiä saatetaan ohjata myös lainsäädännön kautta. Vaatimukset vaihtelevat toimialoittain ja yrityksen koon mukaan. Esimerkiksi henkilötietoja käsittelevillä organisaatioilla on tiukat vaatimukset. Lainsäädäntö voi myös koskea organisaation sisäistä toimintaa, kuten palkka- tai työsuhdetietoja. Lait, joita yritysten tulee huomioida ovat esimerkiksi:

- perustuslaki
- julkisuuslaki
- rikoslaki
- henkilötietolaki
- laki kansainvälisistä tietoturvavelvoitteista
- laki tietoyhteiskunnan palvelujen tarjoamisesta
- sähköisen viestinnän tietosuojalaki
- laki yksityisyyden suojasta työelämässä

(Laakso 2010, s.15; www.finlex.fi)

# 4 Riskienhallinta

Tietoturvaratkaisut ovat olennainen osa organisaation riskienhallintaa. Esimerkkinä saatetaan usein käyttää omaa kotia ja sitä miten pois lähtiessä varmistetaan, että kahvinkeitin on pois päältä. Eli ennakoidaan ja vältetään turhia riskejä. Tietoturvalla voidaan välttää turhia riskejä esimerkiksi virusten, väärinkäytösten tai tiedon hallinnan osalta. Riskienhallintaan kuuluu tiiviisti henkilöstön kouluttaminen, jälkitoimet henkilön lähdettyä organisaatiosta ja käyttöoikeuksien hallinta. (www.valtiokonttori.fi)

Riskienhallinnassa tärkeintä on tunnistaa mahdolliset riskit ja rakentaa näiden pohjalta juuri omalle organisaatiolle sopiva tietoturvaratkaisu. Kaikkien riskien tunnistaminen on toki mahdotonta ja siksi yhtäläisen tärkeää on varautua yllättäviin riskeihin ja poistaa ne havaitsemisen jälkeen. Yllättävät havaitut riskit siirtyvät tämän jälkeen tunnistetuiksi riskeiksi, joihin voidaan jatkossa varautua. Riskit voidaan jakaa karkeasti strategisiin, operatiivisiin, taloudellisiin ja vahinkoriskeihin sekä ulkoisiin ja sisäisiin riskeihin. (www.lahitapiola.fi; www.vtt.fi)

Taulukko 1. Riskienhallinnan eri tasot ja näiden ominaispiirteet.

| **Strategiset riskit** | **Operatiiviset riskit** | **Taloudelliset riskit** | **Vahinkoriskit** |
|---|---|---|---|
| Liikestrategia | Tuotteet | Investoinnit | Koneet ja laitteet |
| Yrityskulttuuri | Henkilöstö | Hinnoittelu | Tapaturmat |
| Asiakkaat | Hallinto | Tuottavuus | Turvallisuus |
| Yhteistyökumppanit | Tietotekniikka | Markkinoiden | Ympäristövahingot |
| Investoinnit | Tietoturva | muutos | Logistiikka |
| | Sopimukset | | |
| Ulkoinen | Sisäisiä | | |

Riskienhallintaan on olemassa erilaisia tietoturvastandardeja, joiden tarkoituksena on auttaa organisaatioita kehittämään tietoturvaansa ja arvioida omien järjestelmien toimivuutta. Eri standardit lähestyvät tietoturvallisuutta eri tavoilla. (Vahtiohje 2009) Alla lueteltu yleisimmät tietoturvastandardit, ISO/IEC 27000 ja CSA Cloud Control Matrix (CMM), sekä niiden ominaispiirteet.

### 4.1 ISO/IEC 27000

ISO/IEC 27000 on tietourvastandardi, joka on julkaistu vuonna 2013. Sen tarkoitus on varmistaa, että tietoturvan hallinta on tasalaatuista ja yhteismitallista. Siinä määritellään dokumentaatiomalli, viittausten muotoilu, organisationaalinen viitekehys ja sidosryhmien huomioiminen. Tämän lisäksi se antaa ohjeistuksen tietoturvan johtamiseen, tukeen ja tietoturvan hallinnan suunnitteluun. Standardi kattaa myös seurannan ja korjaustoimenpidesuunnitelman. (www.iso.org)

### 4.2 CSA Cloud Control Matrix (CCM)

CSA CMM on ohjeisto, joka on luotu tarjoamaan tietoturvaohjeistus pilvipalveluille. Ohjeistus on suunnattu jälleenmyyjille, jotka auttavat asiakkaitaan suojaamaan pilvipalvelunsa kokonaisvaltaisesti. Tämä malli tarjoaa yksityiskohtaiset ohjeet pilvipalvelun suojaamiselle. Malli turvautuu tiiviisti myös muihin olemassa oleviin strandardeihin ja yhteistyöhön näiden tuottajien välillä. Se kytkeytyy osaltaan myös ISO/IEC 27000 standardiin. Mallissa määritellään arviointikriteerit tietoturvalle, kontrollointitoimenpiteet sekä tuki tietoturvan hallinnalle. Pilvipalveluissa erityisesti riskien kartoitus ja niihin varautuminen on avain asemassa. Jatkuva seuranta ja kehittäminen on myös osa mallia, sillä pilvipalveluiden kenttä kehittyy ja muuttuu jatkuvasti.
(www.cloudsecurityalliance.org)

# 5 Palomuuriteknologiat

Palomuurit ovat tärkeä osa yrityksen kokonaisvaltaista tietoturvaa. Palomuureja on käytetty yrityksille kriittisen tietojen turvaamiseen internetin alkuajoista lähtien. Verkkorikolliset kehittävät uusia ja monimutkaisempia uhkia ja tietoturvan pitää pysyä näiden perässä. Palomuuriteknologia on mennyt huomattavasti eteenpäin viimeisien vuosien aikana ja samalla tietoturvan kokonaiskuva on muuttumassa. Internet ei enää koostu pelkästään tietokoneista ja mobiililaitteista vaan nykyisin verkkoon liitetään esimerkiksi jääkaappeja, autoja ja vaikka kokonaisia taloja. Puhutaan niin kutsutusta Internet of Things –ajattelusta (IoT). Se miten käytämme verkkoa mahdollistaa rikollisille myös uusia tapoja hyödyntää haavoittuvuuksia omiin tarkoituksiinsa.

## 5.1 Palomuurien evoluutio

Ensimmäiset palomuurituotteet tulivat markkinoille 1980-luvun lopulla. Kyseiset laitteet olivat reitittimiä, joihin pystyi tekemään filteröintisäännöstöjä. Näiden tehtävänä oli toimia niin kutsuttuina portinvartijoina, estämällä pääsy hyökkäyksiltä internetistä yrityksen sisäverkkoon. Yritykset luottivat omiin sisäisiin palveluihin sekä henkilöstöön, joten tästä syystä ulkoreunan palomuurit, perimeter firewall, olivat suosituimpia ratkaisuja palomuurien alkuaikoina. Perinteisen palomuurin yhtenä tarkoituksena oli luoda yksi piste, mihin kaikki tietoturva keskitetään ja näin ollen poistaa palomuuraustarve käyttäjien laitteista. Tämän suuntainen lähestymistapa oli riittävä 1990-luvulla sen aikaisilta uhilta suojautumiselle. Maailma on kuitenkin muuttunut ja tietoturvan tarve on kasvanut sen myötä, joten palomuurien täytyy myös muuntautua. (Forrest S & Ingham K, 2002, 3-4)

### 5.1.1 Pakettifilteröinti

Ensimmäiset palomuurit toimivat liikenteen ohjaajina joko kieltäen tai sallien liikenteen jostain päin verkkoa toiseen osaan verkkoa. Tämä tarkoittaa sitä, että esimerkiksi internetistä pääsy voidaan estää sisäverkon suuntaan. Tämän tyylinen liikenteen ohjaus tehtiin seuraavien kriteerien mukaisesti:

- Lähdeosoite (IP osoite mistä paketti on lähtenyt)

- Kohdeosoite (IP johon paketti lähetettiin)
- IP-protokolla sekä yhteystaso (Mitä yhteysprotokollaa käytetään ja mitä yhteystason porttinumero on käytössä)
- Rajapinta (Mistä rajapinnasta paketti on lähtenyt ja mihin rajapintaan se on lähetetty)

(Stallings, 2010, 378)

Pakettifilteröinti on yhdensuuntaista palomuurausta mikä tarkoittaa sitä, että kaikki palomuurin läpi kulkevat paketit joko sallitaan tai estetään. Tämä tehdään kumpaankin suuntaan, sisään- tai ulospäin meneville paketeille. Yksi suurimmista ongelmista tällaisella pakettifilteröinnillä on se, että palomuuri ei pysty tutkimaan paketin sisältöä. Kaikki paketinvälityspäätökset tehdään otsikkotason tiedoista ja siksi pakettifilteröinti ei ole tietoinen siitä mikä aplikaatio on kyseessä.

### 5.1.2 Tilallinen palomuuraus

Pakettifilteröinnin keskeisin ongelma on, että jokainen paketti tarkistetaan pääsylistasta. Tämänlainen liikenteen tarkastelu on raskasta ja siksi tilallinen palomuuraus kehitettiin ratkaisemaan tämä ongelma. Tilallinen palomuuri toimii kuten pakettifilteröinti, mutta tämän lisäksi se pitää kirjaa sessioista yhteystaulussa. Tällainen kirjanpito mahdollistaa sen, että palomuurin ei tarvitse sallia erikseen liikennettä kumpaankin suuntaan vaan se pitää yllä tietoa voimassaolevista yhteyksistä. Mikäli paketti kuuluu voimassaolevaan yhteyteen liikenne on sallittua niin sisään kuin ulos.

Palomuurissa joka käyttää vain pakettifilteröintiä tarkistetaan aina pääsylistalta onko liikenne hyväksyttyä. Tilallisella palomuurilla ensimmäinen tarkistus tehdään yhteystaulusta liittyykö paketti aikaisemmin hyväksyttyyn yhteyteen. Tämä parantaa tietoturvan tasoa, mutta myöskin nopeuttaa palomuurin toimintaa, koska palomuurin ei tarvitse käyttää niin paljon komponenttien tehoja paketin tarkastamiseen. Tilallisilla palomuureilla on kuitenkin heikkoutensa. Esimerkiksi nykyisin paljon uutisissa esiintyvillä palvelunestohyökkäyksillä voidaan täyttää yhteystaulu turhalla liikenteellä, joka vaikuttaa sal-

litulta. Kun yhteystaulu täytyy niin palomuuri ei pysty käsittelemään enempää liikennettä ja tällöin se kaatuu.

### 5.1.3 Proxy palomuurit

Proxy, eli sovellustason yhdyskäytävän palomuurit suodattavat liikennettä ohjelmistosovelluksen avulla. Palomuurina toimiva proxy-palvelin toimii tutkimalla läpikulkevaa liikennettä sisäisen verkon palveluihin. Proxy-palvelin tarjoaa korkeampaa suojausta sisäiselle verkolle, koska ratkaisussa pystytään hyödyntämään muun muassa käyttäjän autentikointia, datan salausta sekä tiedoston nimen ja kellonajan perusteella tapahtuvaa suodatusta. (www.netlab.tkk.fi, luettu 16.4.2016)

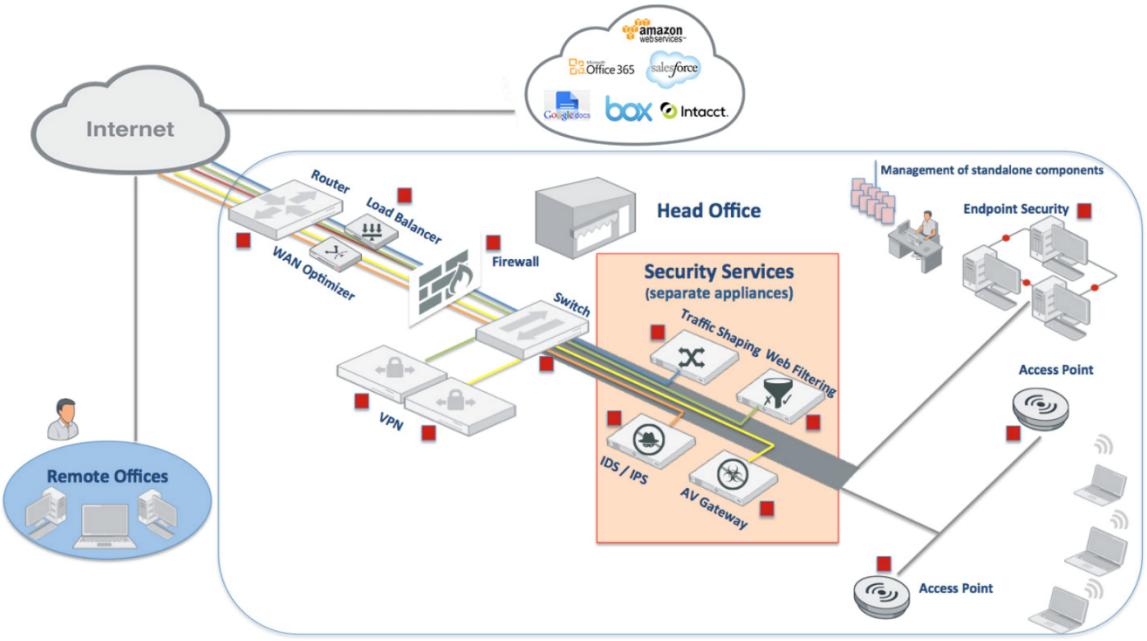
Proxy palomuuri toimii ulko- ja sisäverkon välissä olevana datan välittäjänä. Proxy palomuurin tehtävänä on luoda ja ylläpitää yhteyttä kumpaankin suuntaan lähdeosoitteen puolesta. Kaikki paketit pysäytetään ja tarkastetaan ja tämän jälkeen pakataan uudelleen, jolloin lähdeosoite muutetaan proxy palomuurin lähdeosoitteeksi ja toimitetaan edelleen kohteeseen. Näin ollen suoraa yhteyttä palvelimen ja palvelimen asiakkaan välillä ei ole jolloin saadaan parempaa tietoturvaa sisäverkolle, koska sisäverkko ei näy mitenkään ulkoverkon suuntaan.

## 5.2 Uuden ajan palomuurit

Vaikkakin edellä mainitut palomuurityypit ovat nykyisinkin käytössä on tietoturvan tarve yrityksissä kasvanut ja tätä myötä valmistajien on täytynyt vastata asiakkaidensa tarpeisiin. Palomuurit ovat nykyisin paljon tietoturvallisempia ja antavat näkyvyyden siihen mitä verkossa liikkuu. Tämä mahdollistaa verkon liikenteen analysoinnin, joka jo itsessään parantaa tietoturvaa, mutta auttaa yrityksiä myös keskittymään niille olennaisiin prosesseihin.

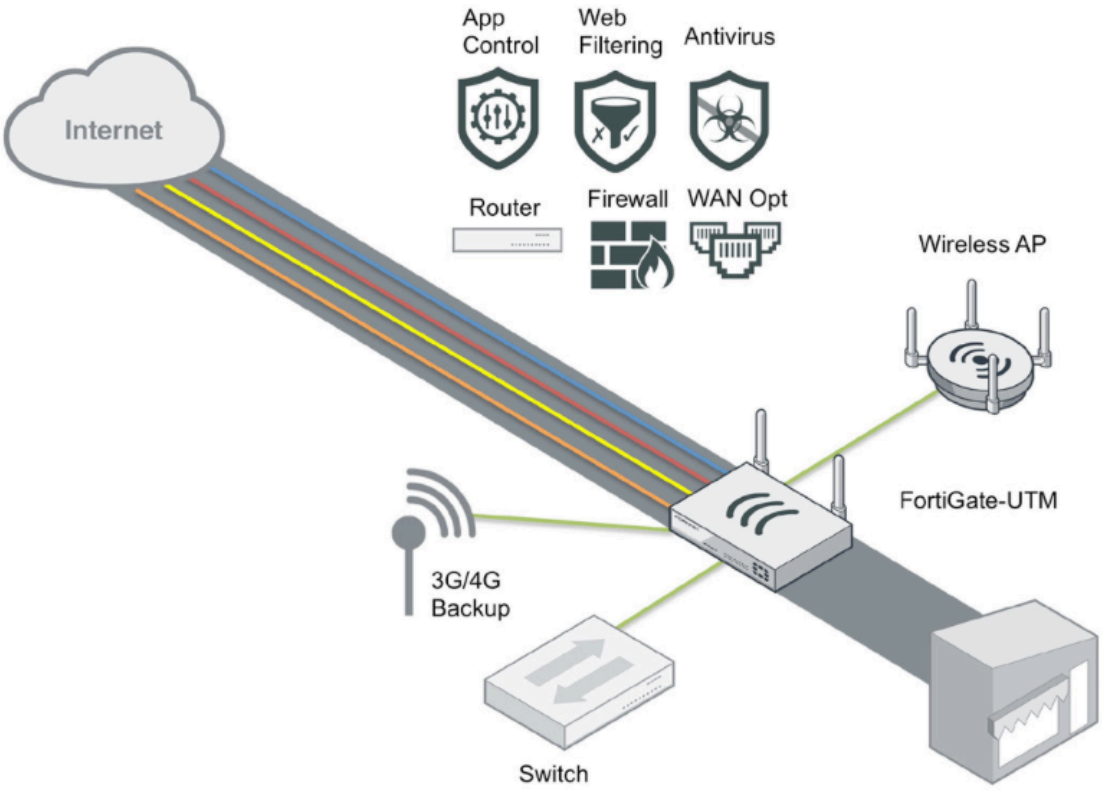
Teknologian kehittyminen ja komponenttien hintojen lasku on mahdollistanut sen, että valmistajat pystyvät tuottamaan laitteita jotka ovat tehoiltaan huomattavasti edeltäjiään parempia sekä konsolidoimaan tietoturvalaitteita ja ominaisuuksia. Konsolidoinnilla saadaan pienennettyä pakettien tutkimiseen käytettyä aikaa, koska tutkimista ei tarvitse

tehdä useammalla eri laitteella. Pakettien siirtämiseen käytetty aika laitteiden välillä siis poistuu.




Kuva 1. Perinteinen yrityksen tietoturvaratkaisu visuaalisesti kuvattuna. (Fortinet. White Paper – Simplify Your Small Business IT. 3/2016)

Perinteisesti yrityksen tietoturva koostui useista eri komponenteista, joita lisättiin verkkoon aina tarpeen mukaan. Hallinta tehtiin useasta pisteestä mikä oli hidasta ja jopa aiheutti jossain tilanteissa ongelmia tietoturvan kannalta, kun laitteet olivat kilpailevien toimijoiden ja niitä ei ollut rakennettu toimimaan yhdessä. Konsolidoinnilla saatiin hallinta yhden pisteen alle ja eri tietoturvakomponentit toimivat paremmin yhteen. Näin ollen tietoturvan tasoa saatiin kasvatettua ja vasteaikaa pienennettyä mahdollisissa ongelmatilanteissa. Tarpeet palomuuraukseen ja tietoturvaan ovat kasvaneet, mutta perinteisten palomuurien ominaisuuksien tarve ei ole poistunut. Palomuurit toimivat siis pohjimmiltaan samalla tavalla kuin aikaisemminkin, mutta näiden laitteiden päälle on tullut uusia ratkaisuja sekä helpotettu itse hallintaa. Esimerkiksi aplikaatiotason tunnistusta on kehitetty eteenpäin. Nyt pystytään näkemään verkkosivujen päällä pyörivät pelit, kuten facebook, sekä estämään näiden käyttö ilman koko sivuston käytön estämistä.




Kuva 2. Konsolidoitu tietoturvaratkaisu. (Fortinet. Solution Brief – Connected UTM. 2014)

### 5.3 Mihin tietoturva on kehittymässä?

Tietoturvamaailmassa suurimpana ongelmana on ollut aina, että valmistajien on pitänyt seurata verkkorikollisten toimia ja vastata heidän innovaatioihinsa uusilla suojausmenettelyillä. Siirtymä uuteen ajattelutapaan on jo käynnissä ja tulemme näkemään enemmän ja enemmän heurestiikkaan ja ohjelmien toiminnallisuuksiin perustuvaa suojautumista. Niin kutsutut sandbox-suojautumiset tutkivat mahdollisten uhkien prosesseja sekä mitä verkosta eristetyssä virtuaalikoneessa oikeasti tapahtuu, kun tiedosto avataan, ennen kuin paketti päästetään määränpäähänsä. Näin ollen sisäverkko ei saastu ja myös tuntemattomat uhkat, nollapäivähyökkäykset, saadaan kiinni, vaikka niistä ei olisi tunnistetietoja vielä tehty.

Perinteinen antivirus tulee jäämään pois päätelaitteilta ja tämän tilalle tulee uudenlaisia tapoja suojautua. Tästä hyvänä esimerkkinä on Palo Alto Networksin Traps-tuote. Traps on tarkoitettu varsinkin tuntemattomien uhkien ja kohdennettujen hyökkäysten torjuntaan. Kun Traps huomaa haitallisia tiedostoja tai haavoittuvuuksia hyväksikäyttäviä hyökkäyksiä se torjuu välittömästi hyökkäyksen ja suojaa laitteen myös tekniikalta

mitä hyökkäyksessä käytettiin. Sen ei siis tarvitse tietää etukäteen mahdollisista hyökkäyksistä, vaan myös aikaisemmin tunnistamattomat tavat saadaan kiinni, koska pakettien toimintaa tarkastellaan. Traps kerää tiedot hyökkäyksestä ja ilmoittaa löydöksistään eteenpäin. Näiden tietojen pohjalta pystytään tekemään tarkempaa tutkimusta ja kehittää uusia tapoja suojautua. (Palo Alto Networks. White Paper – Traps, Advanced Endpoint Protection. 2015)

Tietoturva on siis kehittymässä tilanteeseen missä valmistajien ei tarvitse enää harrastaa kissa-hiiri –leikkiä verkkorikollisten kanssa vaan he ovat rinta-rinnan vastaamassa uusiin uhkiin. Verkkorikolliset kuitenkin tekevät omaa tutkimustaan siitä miten uuden ajan tietoturvalaitteet ja sovellukset toimivat ja kehittävät omia hyökkäyksiään vastaamaan näihin. Tietoturvavalmistajien täytyy siis kehittää omia suojauksiaan vielä eteenpäin. Nyt puhutaan heurestisista eli oppivista suojausmenettelyistä, mutta jo muutamilla valmistajilla on uusi näkökulma siihen miten tietoturvaa tulisi kehittää. Esimerkiksi Lookout niminen valmistaja hakee omalla toiminnallaan ennustavaa tietoturvaa. Näin päästäisiin jopa tilanteeseen, missä verkkorikolliset olisivat jahtaavassa asemassa.

# 6 Tietoturvan käyttöönotto

Käyttöönoton jälkeen on tarpeen tarkastella hankittua tietoturvakokonaisuutta. PDCA-mallissa tämä vastaa tarkastusvaihetta eli vastaako hankittu kokonaisuus yrityksen tarpeita, onko siinä havaittu mahdollisia vikoja tai puutoksia ja onko tarve tehdä muutoksia. Mikäli tietoturvakokonaisuudesta löytyy korjattavia tai muutettavia osa-alueita, ryhdytään toimeen näiden hoitamiseksi. Tietoturva on myös alati muuttuva ja kehittyvä organisaation osa-alue. Ei voida ajatella, että kerran hankittu ja hyväksi todettu tietoturvaratkaisu olisi sitä aina. Eli aikaisemmin mainittu tehtävä –malli tulee toistaa tasaisin väliajoin. Seuranta on oleellinen osa ajantasaista tietoturvaa. (LÄHDE) + osia raportista

Tietoturvaratkaisua hankittaessa voidaan apuna käyttää alan ammattilaisia, joilla on kokonaisvaltainen kuva tarjonnasta ja sen sovittamisesta organisaation tarpeeseen. Asiantuntijan apua voidaan käyttää joko laite- ja sovellushankinnoissa tai kokonaisen tietoturvaratkaisun hankinnassa. (Rajapinta 1/2014)

## 6.1 PK yrityksen tilannekatsaus

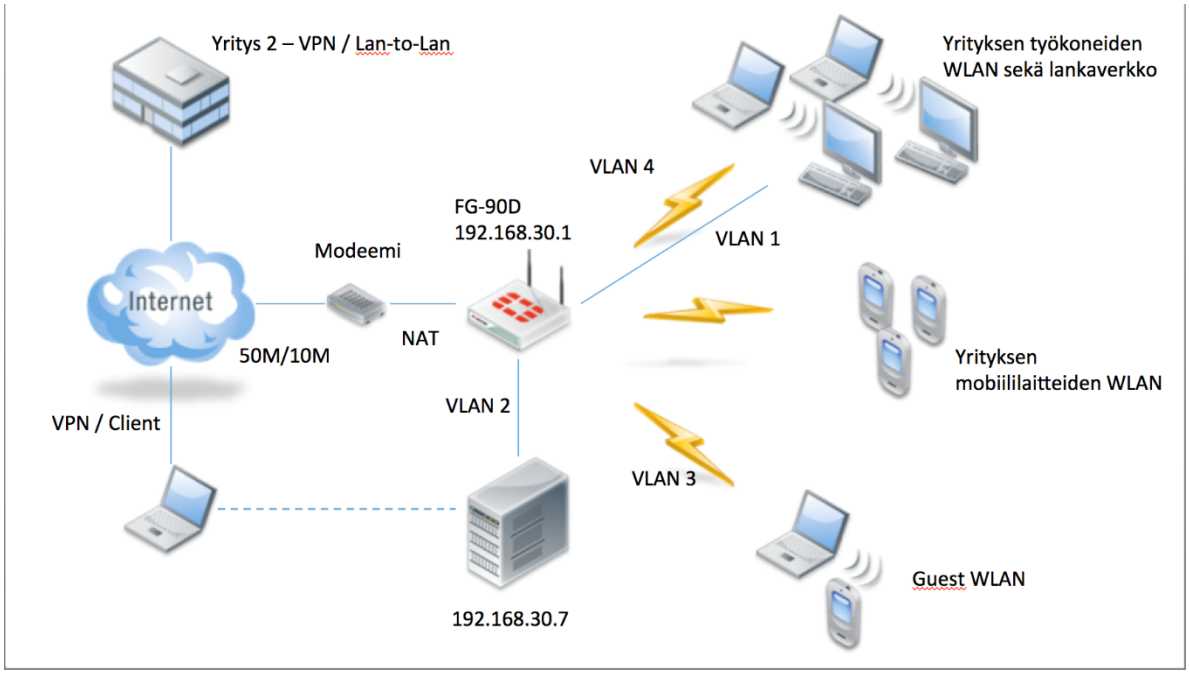
Kuvitteellisella yrityksellä on tarve tietoturvan parantamiseen. Yrityksessä toimii alle kymmenen työntekijää ja heillä on käytössä niin lankaverkkoon kuin langattomaan verkkoon liitettäviä päätelaitteita. Yrityksen oman henkilökunnan lisäksi he haluavat tarjota vierailijoille langattoman verkon, jonka tietoturvataso sekä pääsysäännöstöt ovat tiukemmat kuin oman henkilöstön. Työntekijät tarvitsevat myös VPN yhteyden yrityksen sisäverkkoon ja tätä kautta mahdollisuuden päästä yrityksen palvelimilla oleville työkaluille.

Yritys tarjoaa myös palveluita sisäverkkonsa ulkopuolelle kuvitteelliselle yritykselle numero kaksi omilta palvelimiltaan sekä samaiselta palvelimelta heillä on yrityksensä verkkosivut.

Yritys on asettanut IP-avaruudeksi seuraavat:

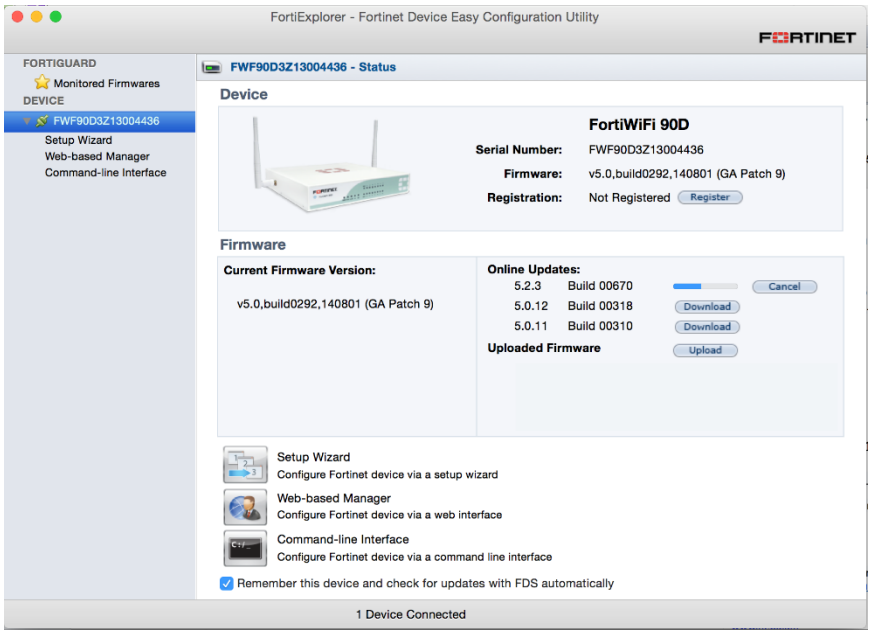
- hlok_koneet – 10.100.10.0/24
- palvelimet – 192.168.30.0/24
- Guest_wlan – 172.16.10.0/24
- hlok_wlan – 10.200.10.0/24

Tarpeen mahdollistajana käytetään Fortinet nimisen valmistajan FortiWiFi 90D palomuuria, jossa on integroituna langaton tukiasema. Laitteen UTM läpäisykyky on riittävä yrityksen 50M/10M liittymälle sekä käyttäjämääriin. Tämän lisäksi yrityksellä on käytössä oma modeemi.



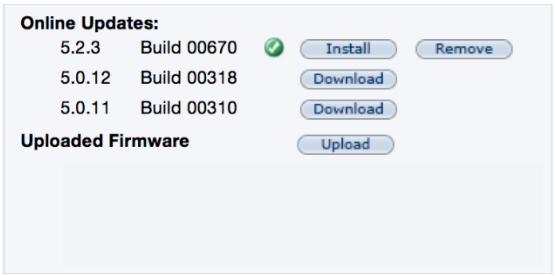
Kuva 3. Suunniteltu verkkokartta yrityksen tarpeista.

## 6.2 FortiWifi käyttöönotto



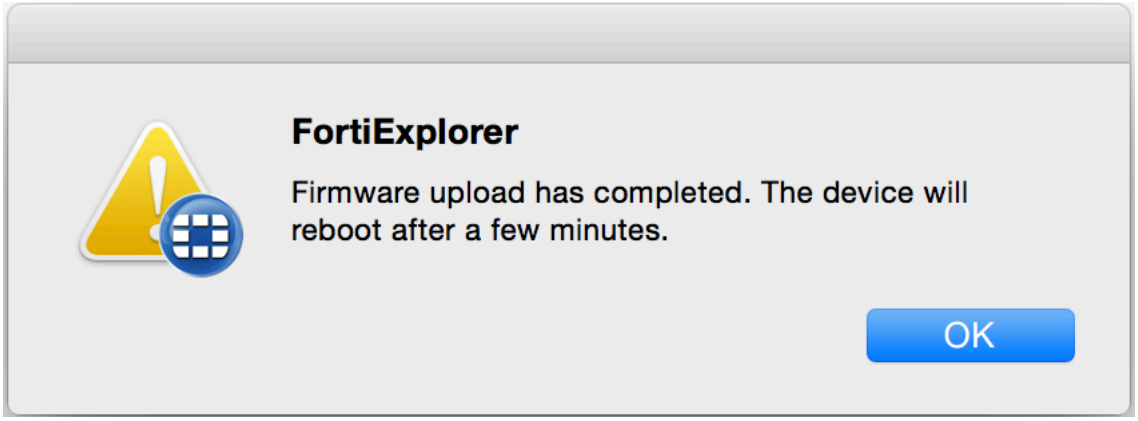

Kuva 4. FortiWifi 90D laitteen kirjaitumisikkuna.

FortiWiFi 90D laitteessa on käyttöjärjestelmänä Fortinetin tuottama FortiOS v5.0. Päivitimme käyttöjärjestelmän tuolloin uusimpaan versioon 5.2.3.



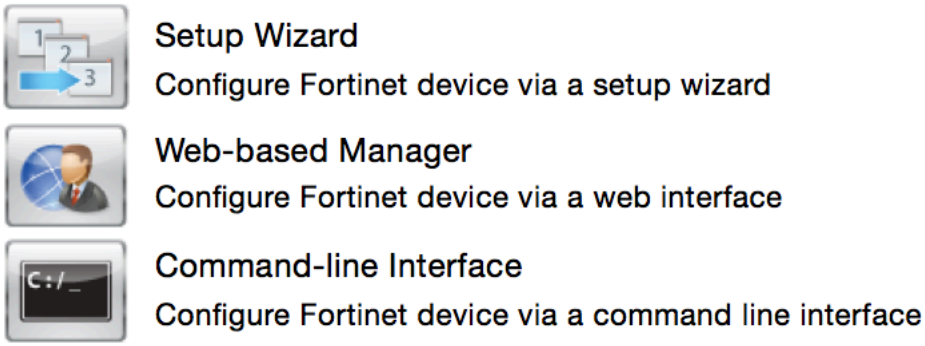

Kuva 5. FortiWifi 90D laitteen käyttöjärjestelmän päivitysvalikko.

Laite käynnistyy latauksen jälkeen automaattisesti sekä päivittyy uusimpaan käyttöjärjestelmäversioon.



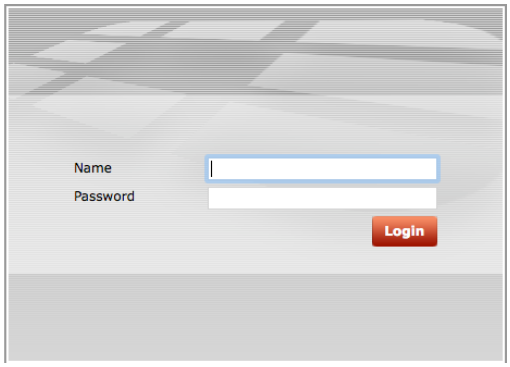

Kuva 6. FortiWifi 90D laitteen käyttöjärjestelmän päivityksen ilmoitusikkuna.

Käyttöönotto tehdään graafisen käyttöliittymän kautta, jota kutsutaan Web-based Manageriksi. Laitetta on myös mahdollista hallita komentoikkunan kautta, mutta Fortinetin graafinen käyttöliittymä on erittäin hyvä varsinkin pienten ja keskisuurten yritysten tarpeisiin.

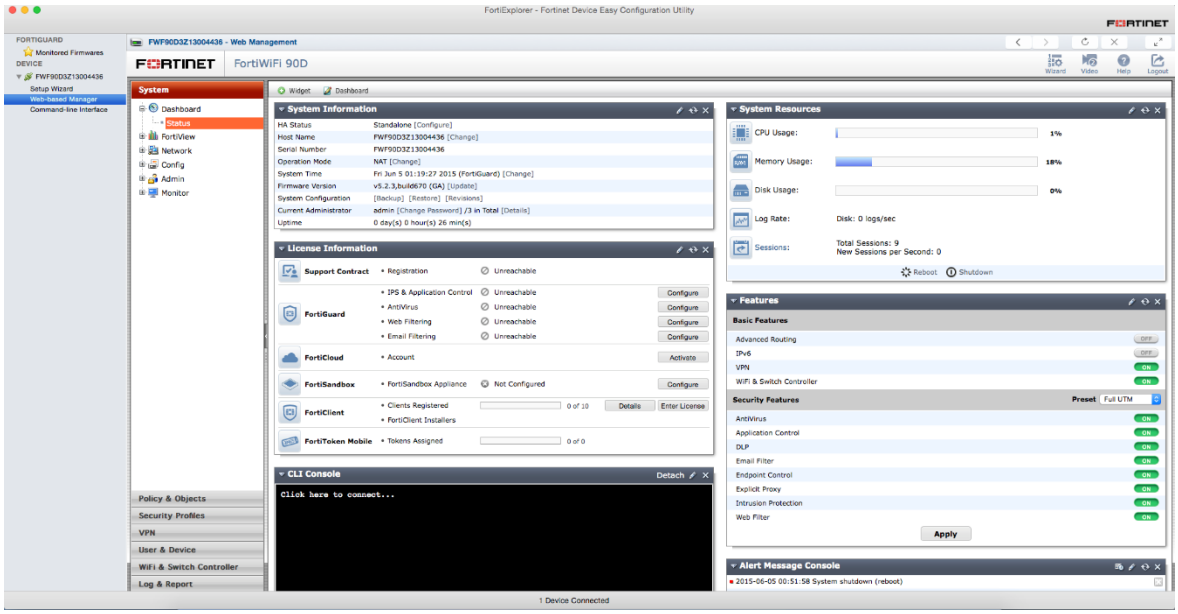



Kuva 7. FortiWifi 90D laitteen käyttöjärjestelmän hallintavalinnat.

Palomuuri on suojattu käyttäjätunnuksella ja salasanalla. Käyttäjätunnus on oletuksena ’admin’ ja salasana tyhjä. Nämä täytyy muuttaa laitteen asetuksista, jotta tietoturva ei vaarannu.



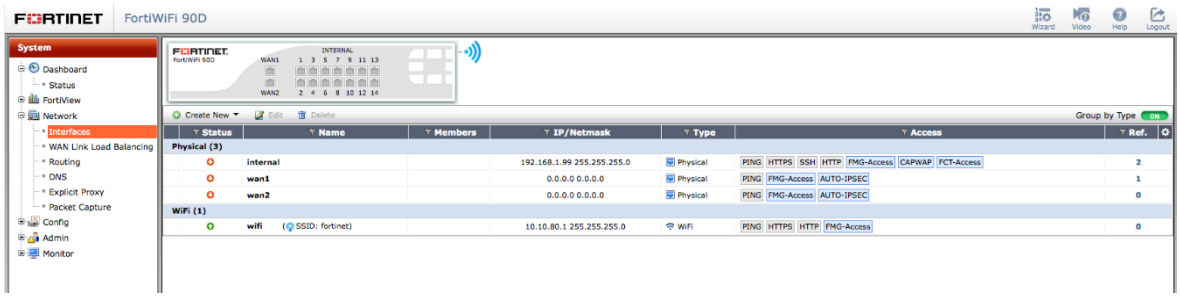

Kuva 8. FortiOS kirjautumisikkuna.




Kuva 9. FortiOS Dashboard.

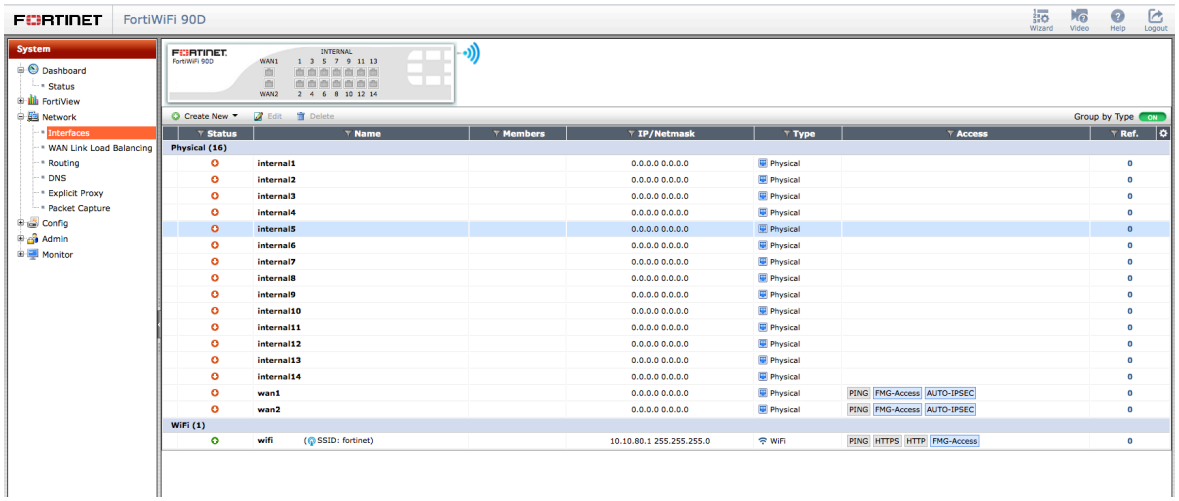
Dashboardilta näkee laitteen tukitilanteen sekä muita tarvittavia tietoja, kuten prosessorin, käyttömuistin sekä tallennustilan tilanteen. Laitteella on oletuksena myös tietoturva-asetuksia päällä.

Ensimmäisenä meidän täytyy ottaa käyttöön laitteen fyysiset portit vastaamaan yrityksen tarpeita. Laitteella on oletuksena kaikkiin portteihin väliltä 1-14 asetettu IP:ksi 192.168.1.99 sekä Netmask 255.255.255.0. Tämän lisäksi wan-portit ovat 0.0.0.0/0.0.0.0.




Kuva 10. FortiOS Interface asetusten yleisnäkymä

Asetamme tässä vaiheessa internal portit osoitteisiin 0.0.0.0/0.0.0.0.

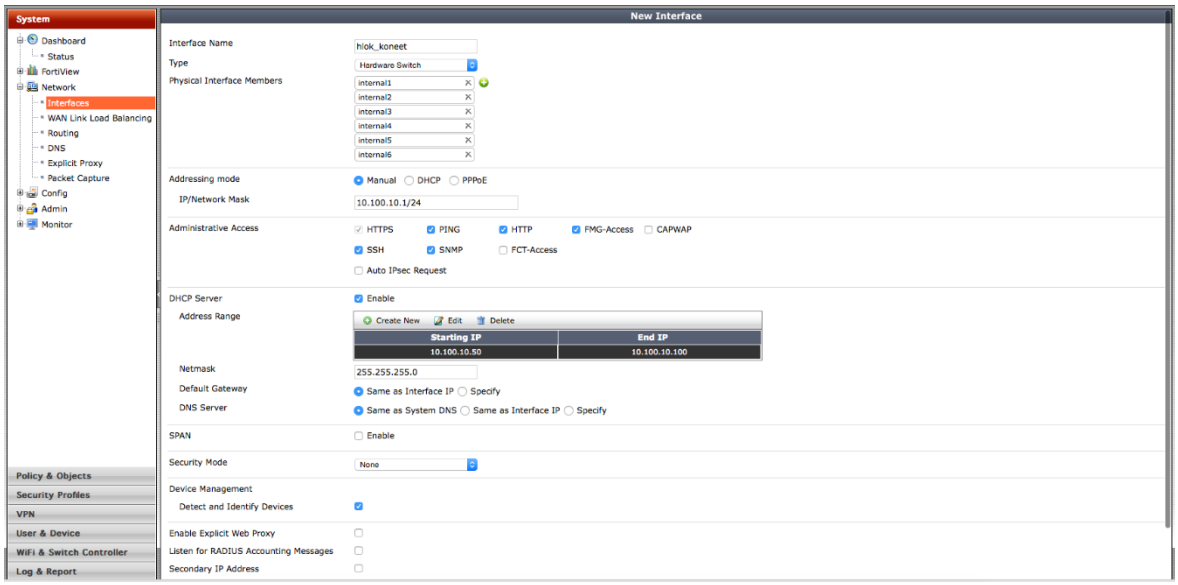



Kuva 11. FortiOS Interface asetusten yleisnäkymä, jossa on mukana internal portit.

Koska yrityksellä oli käytössä päätelaitteita, jotka liitetään suoraan verkkokaapelilla laitteeseen, asetamme portteihin 1-6 tarvitut IP osoitteet sekä Netmaskin (10.100.10.50 – 10.100.10.100 / 255.255.255.0. Tämän lisäksi näiltä osoitteilta pääsee tekemään seuraavia toimenpiteitä:

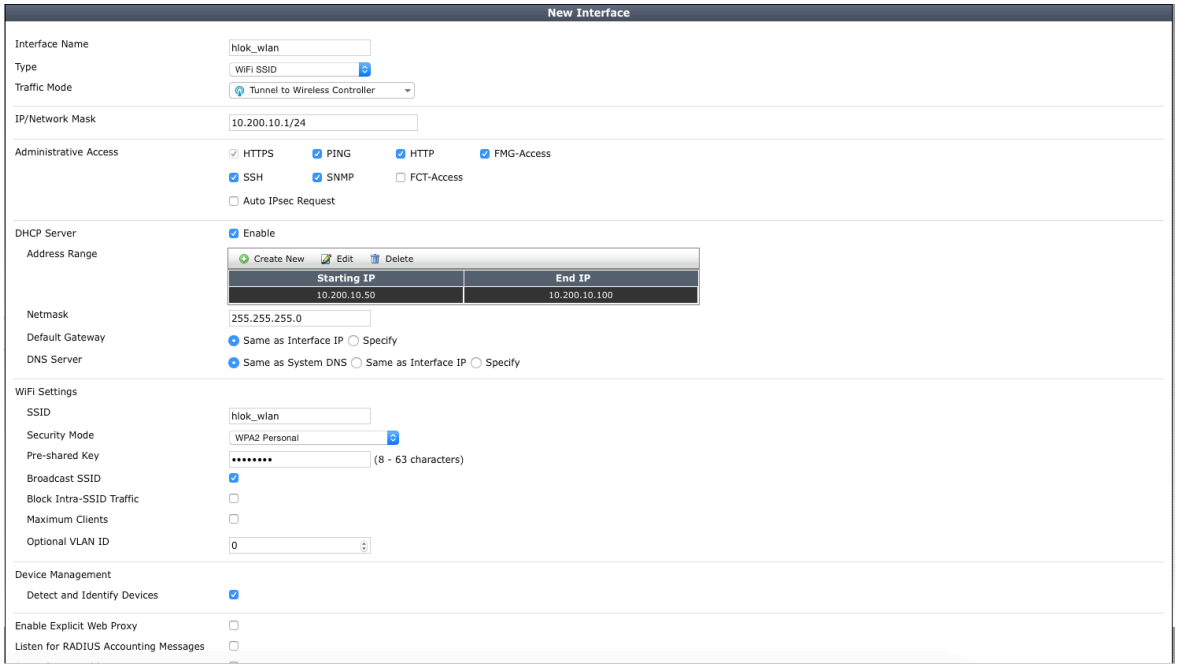
- ping
- http
- https
- FMG-Access (Fortinetin hallinta)
- SSH
- SNMP

Default Gateway sekä DNS-palvelin jätetään siihen tilaan kun ne automaattisesti ovat. Tämän lisäksi tutkimme mitä päätelaitteita verkossa on.



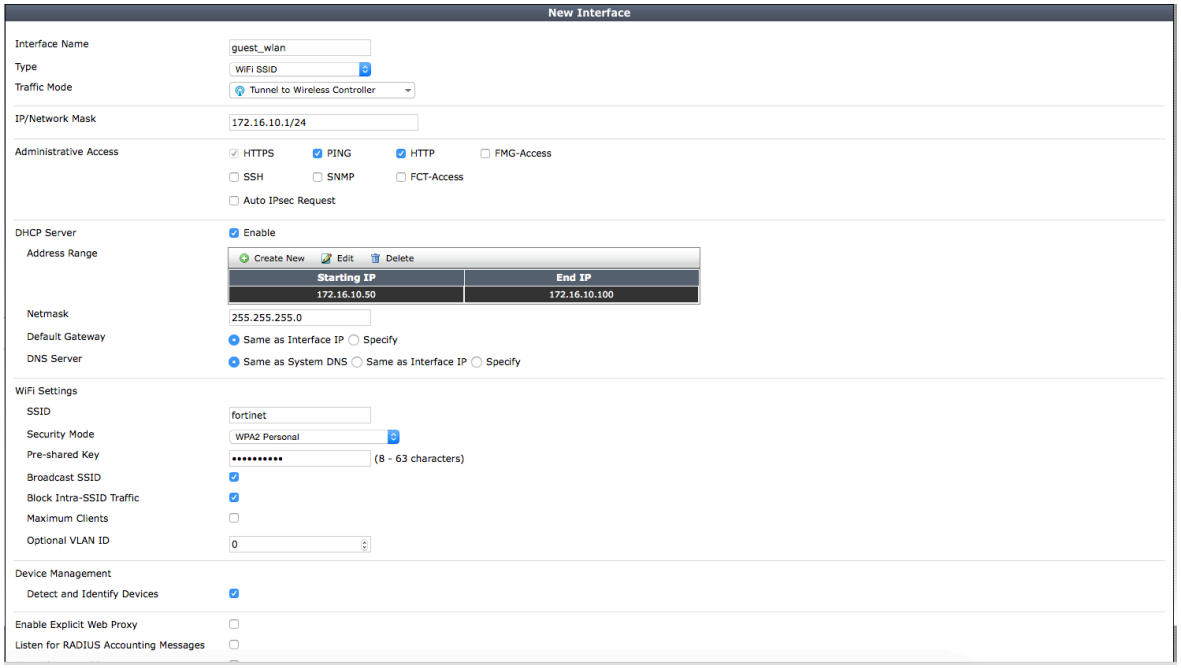

Kuva 12. FortiOS Interface konfigurointi-ikkuna, jossa konfiguroidaan hlok_koneet.

Henkilökunnalle tarvitaan myös wlan-verkko. Teemme samaiset asetukset hlok_wlan interfaceen. Asetamme SSID:ksi nimen hlok_wlan ja salasana on WPA2 Personal suojauksella tehty pre-shared avain. Salasana on kaikille henkilökunnasta sama. Kuulutamme myös SSID:tä, jotta tuon löytää ilman manuaalista hakua. IP ja Netmask asetetaan välille 10.200.10.50 – 10.200.10.100 / 255.255.255.0.



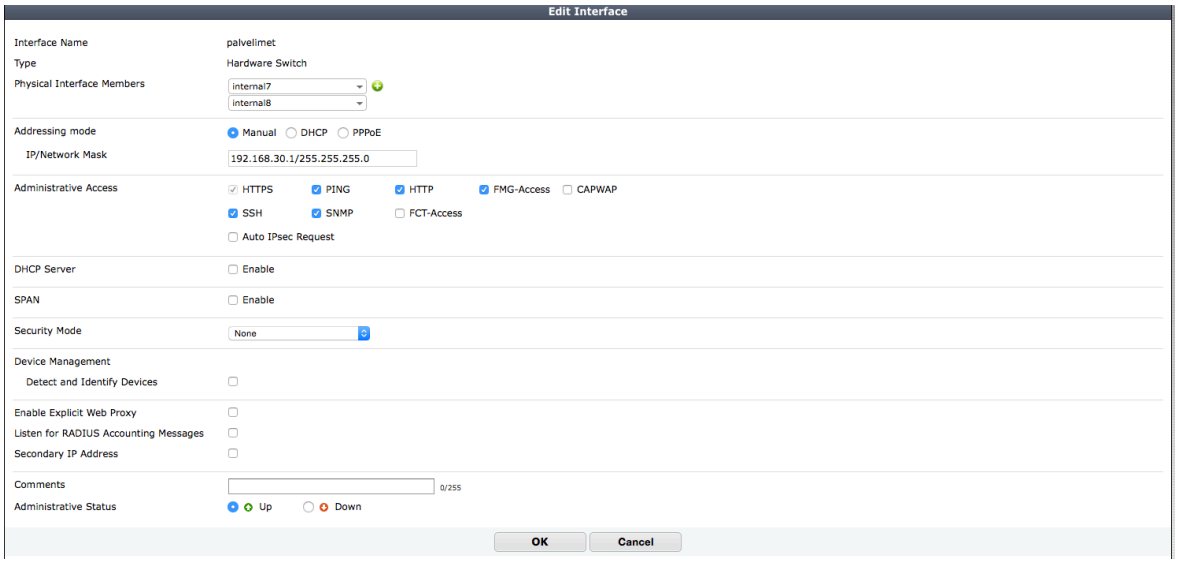

Kuva 13. FortiOS Interface konfigurointi-ikkuna, jossa konfiguroidaan hlok_wlan.

Vierailijoiden langaton verkko tehdään samalla tavalla kuin yrityksen oman henkilökunnan. Veirailijoille annetaan vähemmän oikeuksia verkon käyttöön. He pystyvät vai tekemään ping-pyyntöjä sekä käyttämään http:n ja https:n yli verkkoa. SSID:nä käytetään nimeä fortinet ja salaus tehdään WPA2 Personal menetelmällä. Veirailijoille on käytössä yksi yhteinen salasana. IP ja Netmask asetetaan välille 172.16.10.50 – 172.16.10.100 / 255.255.255.0.

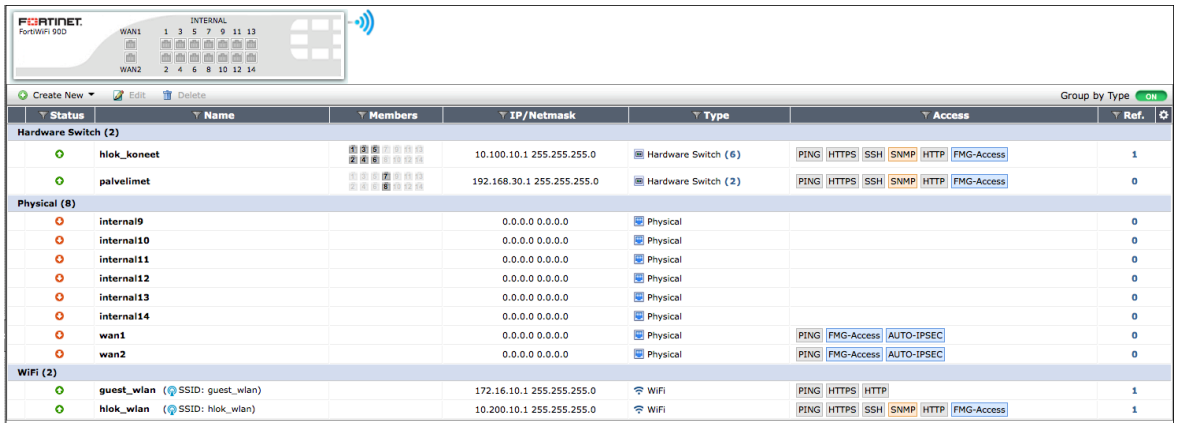



Kuva 14. FortiOS Interface konfigurointi-ikkuna, jossa konfiguroidaan guest_wlan.

Yrityksellä on myös käytössä palvelimia. Nämä liitetään portteihin seitsemän ja kahdeksan. IP/Network mask asetetaan manuaaliseksi osoitteeseen 192.168.30.1/255.255.255.0. DHCP server otetaan pois päältä.




Kuva 15. FortiOS Interface konfigurointi-ikkuna, jossa konfiguroidaan palvelimet.

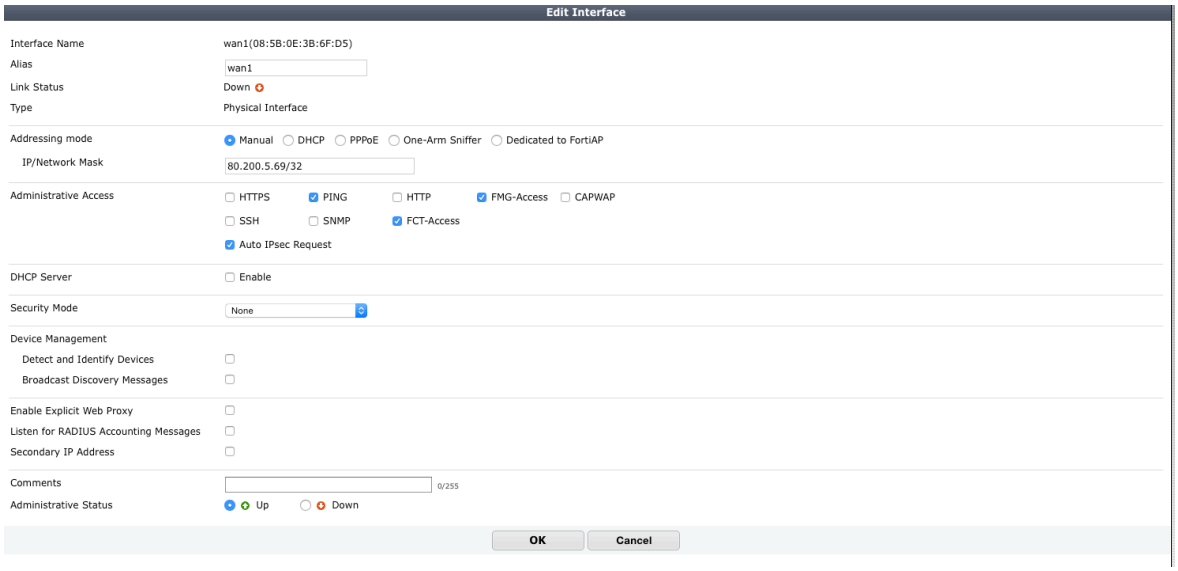



Kuva 16. FortiOS Interface asetusten yleisnäkymä, fyysisten porttien ja WiFi:n konfiguroinnin jälkeen.

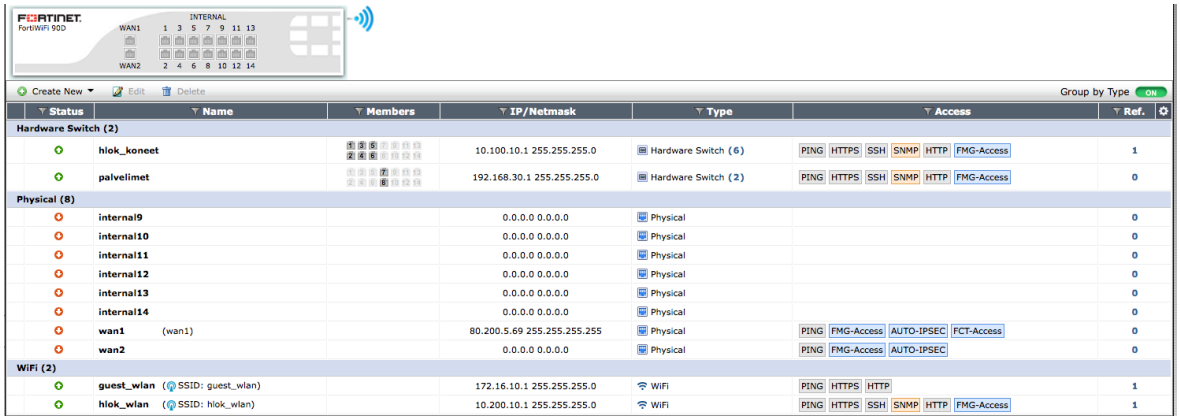
Lopputulos näiden toimenpiteiden jälkeen. Hlok_koneet ovat asetettu fyysisiin portteihin 1-6 ja palvelimet ovat porteissa 7-8. Portit 9-14 eivät ole käytössä ja wan1 ja wan2 portteihin ei ole vielä tehty säännöstöjä. WiFi-tiedot näkyvät myös tältä sivulta.

Seuraavaksi teimme reitin internetin suuntaan. Yrityksellä oli käytössä oma modeemi jonka IP osoite on 80.200.5.69/32. Teemme reitin wan1 portista modeemiin. Säänöstöjä asetetaan seuraavalla tavalla:

- Ping
- FMG-Access
- FCT-Access (FortiClientien päivitys)
- Auto IPSec Request (VPN yhteyttä varten)

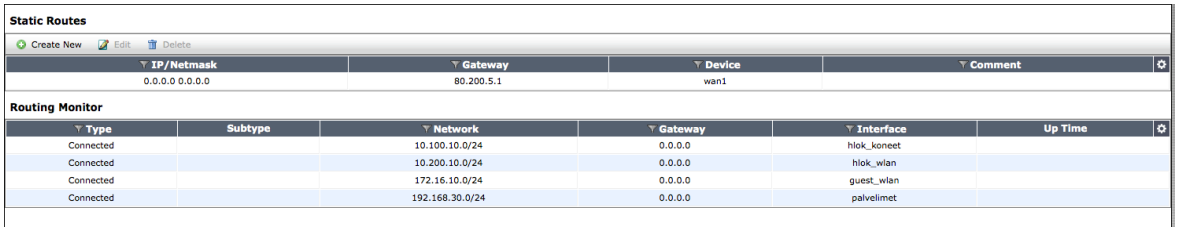



Kuva 17. Fyysisen wan1 -portin konfigurointi.




Kuva 18. Tilannekuva wan1 -portin konfiguroinnin jälkeen.

Pääsemme tässä tilanteessa wan1 portista internetin suuntaan, mutta sisäisestä IP-avaruudesta emme pysty ottamaan vielä yhteyttä wan1 porttiin. Teemme staattisen reitin hlok_koneet, hlok_wlan, guest_wlan ja palvelin interfaceista wan1:een.

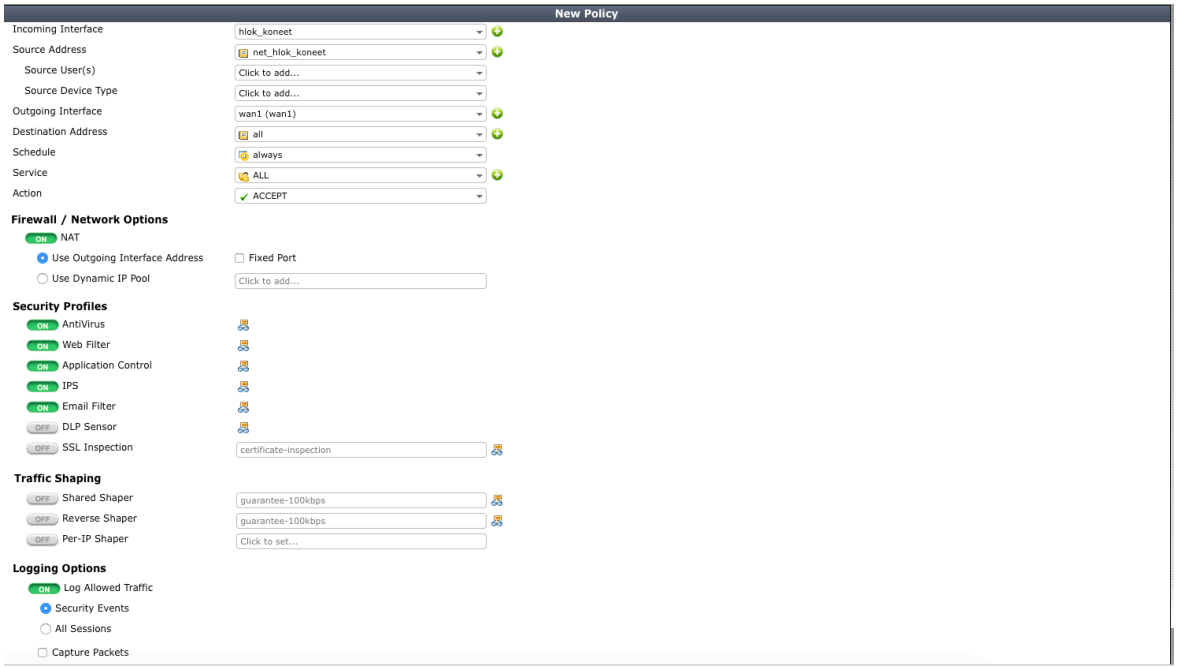



Kuva 19. Staattisen reitin konfigurointi.

Tässä vaiheessa meillä on verkon toiminta valmis. Yritys haluaa tietoturvansa myös ajan tasalle. Asetamme hlok_koneet, hlok_wlan ja palvelimet interfaceille seuraavat säännöstöt default profiililla:

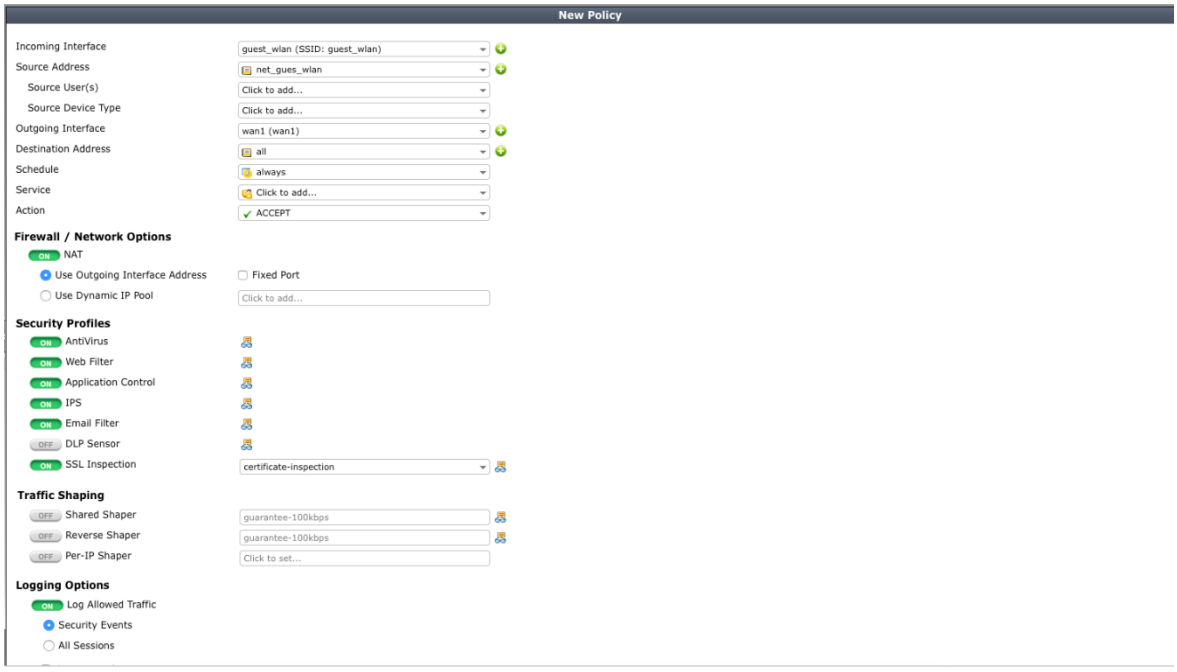
- NAT (Käytetään ulospäin menevän liikenteen interface osoitetta)
- Antivirus
- Web Filter
- Application Control
- IPS
- Email Filter

Näiden asetuksen lisäksi keräämme myös tietoja sallitusta liikenteestä.



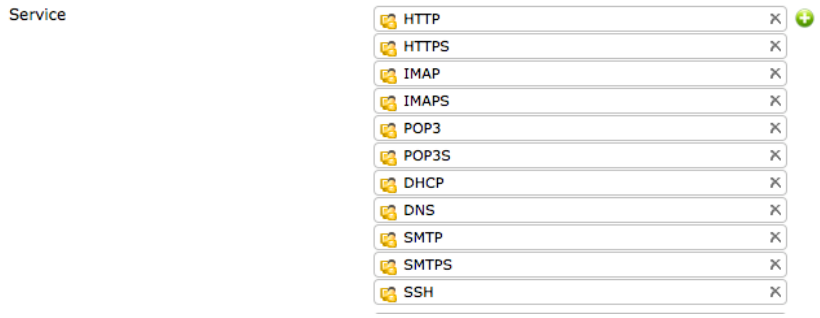

Kuva 20. Hlok_koneet tietotutva-asetusten konfigurointi.

Guest_wlanille asetamme samojen asetusten lisäksi myös SSL Inspectionin sertifikaatti-tasolla.




Kuva 21. Guest_wlan tietoturva-asetusten konfigurointi.

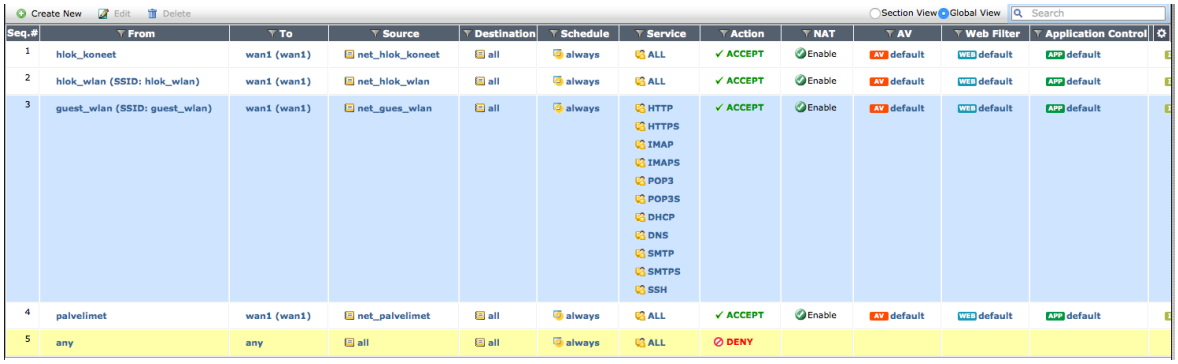
Rajoitamme myös vierailijoiden verkon käyttöä. Palvelut joita vierailijat saavat käyttää ovat listattuna kuvassa:




Kuva 22. Guest_wlan sallitut yhteysprotokollat.

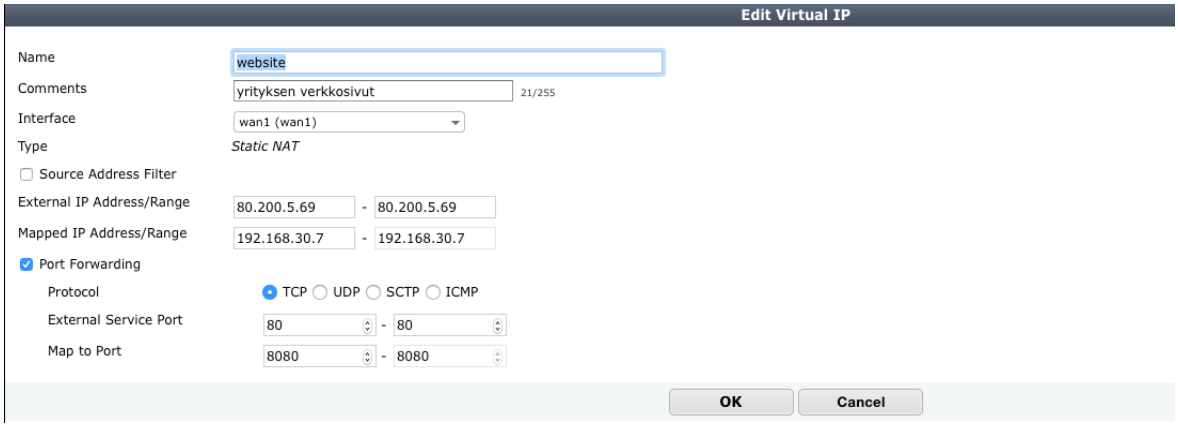

Kuva 23. Guest_wlan liikenteen rajoittamisen konfigurointi.

Vierailijoiden verkon käyttö asetetaan pienemmälle prioriteetille, jolloin yrityksen omat toiminteet menevät ruuhkatilanteissa ulkopuolisten verkon käytön edelle.




Kuva 24. Tilannekuva tietoturva-asetusten jälkeen.

Jotta saamme yrityksen verkkosivut julkaistua verkkoon, meidän täytyy tehdä säännöstö myös palomuurille. Asetamme verkkosivut nimen website alle interface wan1:een. IP osoitteet asetetaan sisäisesti palvelimen osoitteesta 192.168.30.7 osoitteeseen 80.200.5.69, joka menee ulkomaailmaan. Port forwarding asetetaan TCP protokollaan porttiin 80 sekä mappaus porttiin 8080. Säännöstön tyyppinä on staattinen NAT.

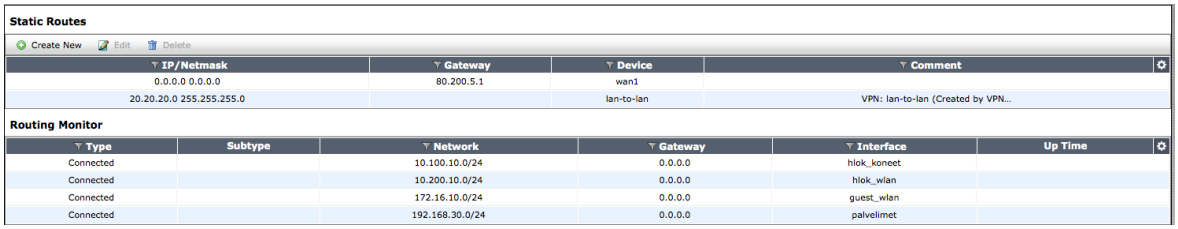



Kuva 25. Yrityksen verkkosivujen yhteyksien konfigurointi.

Asetimme myös VPN yhteydet etäkäyttäjille, jotka ottavat yhteyden sisäverkkoon käyttäen FortiClient-työkalua, sekä site-to-site yhteyden yritys kahdelle. Etäkäyttäjille on asetettu salasana, jonka he syöttävät ensimmäisen kerran verkkoon kirjautuessa ja tämän jälkeen yhteydenotto on automaattinen. Yritysten välinen yhteys on koko ajan päällä ja tämä on myös suojattu salasanalla.


Kuva 26. VPN-yhteyksien konfiguroinnin yleisnäkymä.

Staattiset reitit näyttävät näiden toimenpiteiden jälkeen tältä:




Kuva 27. Staattisten reittien yleisnäkymä.

Kun etäkäyttäjät ottavat yhteyden verkkoon, heidän tietonsa ja käyttäjänimensä tallentuvat palomuurille.


Kuva 28. VPN-asiakkaiden yleisnäkymä.

Yrityksen verkko on täten verkkokartan mukainen ja tietoturvataso toivotulla tasolla. Palomuuri lataa automaattisesti Fortinetin FortiGuard palvelusta tietoturvapäivityksiä sekä tunnisteita, jolloin tietoturvan taso ei laske missään kohdassa.

# 7 Lähteet


Anders Innovations. 2013. Tietoturvan perusasiat pk-yrityksessä. Luettavissa: https://www.andersinnovations.com/fi/blogi/tietoturvan-perusasiat-pk-yrityksessa. Luettu: 29.3.2016

Cloud Security Alliance. 2016. Cloud Controls Matrix. Luettavissa: https://cloudsecurityalliance.org/group/cloud-controls-matrix//. Luettu 12.12.2016

Fortinet. 2015. White Paper – SMB Connected UTM.

ISO. 2016. ISO/IEC 27000:2016(en). Luettavissa: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en. Luettu 12.12.2016

Järvinen, Petteri. 2002. Tietoturva & yksityisyys. Porvoo: Docendo Finland Oy.

Karvi, T. 2012. Tietoturvan perusteet. Luettavissa: https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf. Luettu: 29.3.201)

Kurittu, Antti. 2015. TIKKA Tietoturvallisuus tilanteen kartoitustyökalu pienille yrityksille. Luettavissa: http://ek.fi/ajankohtaista/uutiset/2015/06/22/kaytannonlaheinen-tietoturvaopas-pk-yritysten-arkeen. Luettu: 29.3.2016.

Laakso M. 2010. PK-yrityksen tietotuvasuunnitelman laatiminen. Luettavissa: https://publications.theseus.fi/handle/10024/20793. Luettu: 29.3.2016.

Los Angeles Times. 2013. Today in history: The internet is born. Luettavissa: http://www.latimes.com/business/hiltzik/la-fi-mh-internet-20131029-story.html. Luettu: 29.3.2016.

Nykänen, Pirkko. 2014. Tietoturva – tietosuoja tietojärjestemien suunnittelussa. Luettavissa:

http://www.uta.fi/sis/tie/tjsum/index/TJSUM_Luento6_2014_PirkkoNyk%C3%A4nen.pdf. Luettu: 29.3.2016.

Opetushallitus. 2012. Tietoturvan peruskäsitteitä. Luettavissa: http://www.oph.fi/opetustoimen_turvallisuusopas/turvallisuuden_osa-alueita/tietoturva/tietoturvan_peruskasitteita. Luettu: 29.3.2016.

Palo Alto Networks. 2015. White Paper – Traps, Advanced Endpoint Protection.

Talouselämä. 2015. Johtaja ei kehtaa tunnustaa olevansa pihalla tietoturvasta. Luettavissa: http://www.talouselama.fi/uutiset/johtaja-ei-kehtaa-tunnustaa-olevansa-pihalla-tietoturvasta-3473418. Luettu 29.3.2016.

Teknillinen korkeakoulu. 2000. Palomuurityypit. Luettavissa: http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/30/ptyypit.shtml. Luettu: 20.5.2016.

Valtionhallinnon tietoturvasanasto. Luettavissa: https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto. Luettu: 29.3.2016

Valtiovarainministeriö. 2016a. Vahti-ohjeet. Luettavissa: https://www.vahtiohje.fi/web/guest/riskienhallinnan-keinot. Luettu: 29.3.2016.
Lähitapiola. Yrityksen riskienhallinta. Luettavissa: http://www.lahitapiola.fi/yritys/palvelut/yrityksen-riskienhallinta/yritystoiminnan-riskit. Luettu: 29.3.2016.

Valtiovarainministeriö. 2016b. Vahti-ohjeet. Luettavissa: https://www.vahtiohje.fi/web/guest/kayttoturvallisuus1. Luettu: 29.3.2016.

Valtiovarainministeriö. 2016c. Vahti-ohjeet. Luettavissa: https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus. Luettu: 29.3.2016.

Valtori. 2014. Laadun kaava: riskienhallinta + tietoturvallisuus + varautuminen + seuranta. Luettavissa: http://www.valtiokonttori.fi/vuosikertomukset/public/download.aspx?ID=89486&GUID=%7B7D9791B4-F77E-4F88-865F-0EF70668F50D%7D. Luettu: 29.3.2016.

Varsinaisuomen Yrittäjät. 2010. Luettavissa: http://www.y-lehti.fi/arkisto/artikkeli/3192/Tietoturvasta+huolehtiminen+on+elinehto+. Luettu: 29.3.2016.

Viestintävirasto. Kyberturvallisuus. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus.html. Luettu: 29.3.2016.

VTT Oy. 2009. Pk-yrityksen riskienhallinta. Luettavissa: http://virtual.vtt.fi/virtual/pkrh/riskilajit.html. Luettu: 29.3.2016.

YLE. 2013. Työntekijät ovat suurin tietoturvauhka yrityksille – Henkilöstön ohjoistusta aiotaan tiukentaa. Luettavissa: http://yle.fi/uutiset/tyontekijat_ovat_suurin_tietoturvauhka_yrityksille__henkiloston_ohjeistusta_aiotaan_tiukentaa/6941588. Luettu 29.3.2016.

YLE. 2016. Panamalainen asianajotoimisto syyttää tietovuodosta ulkopuolista tahoa. Luettavissa: http://yle.fi/uutiset/panamalainen_asianajotoimisto_syyttaa_tietovuodosta_ulkopuolista_tahoa/8790419. Luettu 20.5.2016.