VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Olli Majapuro

YRITYKSEN LANGATTOMAN VERKON TIETOTURVA

Tekniikka ja liikenne

2011

SISÄLLYS……..2

VAASAN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Olli Majapuro
Opinnäytetyön nimi	Yrityksen langattoman verkon tietoturva
Vuosi	2011
Kieli	suomi
Sivumäärä	58
Ohjaaja	Kalevi Ylinen

Monet yritykset ovat epätietoisia siitä, millainen tietosuoja on yhtiölle paras. Ostaja vertailee laitteita ja hintoja ja valitsee usein edullisimman ja helppokäyttöisimmän. Tutkimuksen tehtävä on kertoa, mitä asioita on selitettävä käyttäjälle valintatilanteessa parhaan ratkaisun tekemiseksi.

Tutkimuksessa on esitetty WLAN-tekniikkaa, Internet-yhteyden palomuuria ja erilaisia tietoturvalaitteita. Lisäksi on käsitelty tietoturvan laajentamista.

Eri valmistajien laitteita ja järjestelmiä on vertailtu käyttäjän näkökulmasta. Edelleen on tutkittu tietoturvan laajentamista jo hankittuihin laitteisiin.

Yhä useammat ostajat ovat kiinnostuneita tietoturvan laajentamisesta. Nykyisin arvostetaan helppokäyttöisyyttä ja laitteen varmaa toimintaa. Hinta ei ole aina ratkaiseva tekijä. Tuloksena voidaankin todeta tietoturvan, luotettavuuden ja laajennettavuuden olevan tärkeimpiä tekijöitä hankintaa tehdessä.

Avainsanat WLAN-tekniikka, tietoturvalaitteet, tietoturvan laajentaminen

VAASAN AMMATTIKORKEAKOULU

UNIVERSITY OF APPLIED SCIENCES

Tietotekniikan koulutusohjelma

ABSTRACT

Author	Olli Majapuro
Title	The Company´s Wireless Network Security
Year	2011
Language	Finnish
Pages	58
Name of Supervisor	Kalevi Ylinen

Many companies are unaware of what kind secure of data is the best for their company. The buyer compares equipments and prices, and often chooses the cheapest and easiest to use. The role of research is to describe what things have to explain to the user for the best choice.

The study is presented in WLAN technology, the Internet Connection Firewall, and a variety of security devices. In addition, security is treated with the extension.

Different manufacturers of devices and systems, is compares the user's point of view. Continued expansion of security has been studied already purchased equipment.

More and more buyers are interested in the extension of security. Currently valued at ease and secure operation of the device. Price is not always the deciding factor. As a result it can be said for security, reliability and expandability of the most important factors when making the purchase.

Keywords Wireless technology, security equipment, expansion of security

KÄYTETYT MERKIT JA LYHENTEET

ADSL	asymmetric digital subscriber line,	epäsymmetrinen yhteys
AES	Advanced Encryption Standard,	salausstandardi
AP	access point,	liityntäpiste
ATM	asynchronous transfer mode,	asynkroninen tiedonsiirto
CCX	Cisco compostible extensions,	Cisco-laajennus
CD	compact disc,	digitaalinen tallennusmedia
CF	certainty factor,	varma tuotanto
DMZ	demilitared zone,	demilitarisoitu alue
DSL	digital subscriber line,	digitaalinen linja
EAP	Extensible Authentication Protocol,	laajennettu autentikointi
ETSI	European Telecommunication Standard Institute	
GHz	gigahertz,	gigahertzi
GSM	Global System for Mobile communication, matkapuhelin järjestelmä	
IEEE	Institute of Electrical and Electronics Engineers	
IMPI	International Microwave Power Institute	

IMSI	international mobile subscriber identification,	tilaajan tunnistus
IP	internet protocol,	internet-protokolla
IPSec	Internet protocol Security Architecture,	turvaamisprotokolla
ISM	industrial, scientific, medical,	teollisuus, tiede, lääketiede
ISP	internet service provider,	palvelun tarjoaja
LAN	local area network,	paikallinen verkko
MAC	Media Access Control,	sijaintiosoite
Mb/s	speed unit,	megabitti sekunnissa
MIC	Message Integrity Check,	tarkastusprotokolla
MIMO	Multiple-Input and Multiple-Output,	moniantenni
NSA	National Security Agency	
OEM	Original Equipment Manufacturer,	lisenssi
OSPF	Open Shortest Path First Protocol,	reititysprotokolla
PCI	Peripheral Component Interconnect,	tietokoneväylä
PCMCIA	Personal Computer Memory Card International Association	
PK- yritykset		pienet ja keskisuuret yritykset

PMK	Pairwise Master Key,	salausavain
PPPoE	Point-to-Point Protocol Over Ethernet,	yhteysprotokolla
RADIUS	Remote Authentication Dial In User Service,	autentikointi
RC4	Rivest cipher 4,	salausalgoritmi
SIP	Single Inline Package,	tietoliikenneprotokolla
SSID	Service Set Identifier,	verkkotunnus
TKIP	Temporal Key Integrity Protocol,	tietoturvaprotokolla
UKK		usein kysytyt kysymykset
UMTS	universal mobile telecommunications system	
USB	Universal Serial Bus,	sarjaväyläarkkitehtuuri
UTM	Unified threat management,	tietoturvalaite
VPN	Virtual Private Network,	etäyhteys
WAN	wide area network,	tiedonsiirtoverkko
WCS	Wireless Control System,	langaton kontrolleri
WEB		selain
WEP	Wired Equivalent Privacy,	salausmenetelmä

WES	World Educations Services,	portaali
Wi-Fi	Wireless Fidelity,	langaton yhteys
WISP	Wireless Internet service provider,	palvelun tarjoaja
WLAN	Wireless Local Area Network,	langaton verkko
WLAN, oWLAN, OWLAN		operaattorin langaton verkko
WPA, WPA2	Wi-Fi Protected Access,	salausavain
WWAN	Wireless Wide Area Network,	laaja langaton verkko
3G	UMTS,	yhteys

/6/

1 JOHDANTO

Valittu aihe on tärkeä yleisestä näkökulmasta siksi, että on havaittu tietoturvarikoksien lisääntyvän ja sekä ostajia että käyttäjiä halutaan auttaa kyllin kattavan tietoturvan valitsemisessa. Työssä on kiinnitetty huomiota myös siihen, kuinka jo olemassa olevaan järjestelmään voidaan yhdistää mahdollisia lisälaitteita ja –palveluja.

Työn toimeksiantajaorganisaatio on nimeltään Fin-LAN. Yrityksen toimipaikkoja on Vaasan lisäksi Tampereella, Lahdessa, Kuopiossa, Helsingissä ja Turussa. Henkilökuntaa on kaikkiaan 107. Aruba-koulutus (Aruban oma certifiointi, joka on vaadittu jälleenmyyntisopimuksessa) on saanut kaikki 27 asentajaa. Yrityksen perustaja hallituksen puheenjohtaja pitää tärkeänä henkilökunnan koulutusta. Fin-LAN myy erilaisia puhelinjärjestelmiä ja niihin liittyviä laitteistoja. Erityisesti yritys kiinnittää huomiota tietoturvan lisäämiseen.

Aihe on tärkeä toimeksiantajalle siksi, että kilpailu asiakkaista ja heidän valinnoistaan kiihtyy. Tämän vuoksi yritys pyrkii entistä paremmin palvelemaan sekä suuryrityksiä että pieniä elinkeinonharjoittajia. Ostotilanteessa käyttäjälle kerrotaan erilaisista vaihtoehdoista ja verrataan niitä keskenään.

Työssä on esitelty langatonta lähiverkkoa. WLAN-kytkimistä on mukana kuusi erilaista laitetta, joita on vertailtu keskenään. Taulukossa näkyvät myös hintaerot. Selvitys verkon asentamisesta on otettu mukaan siksi, että se saattaa lisätä ostajan tietoisuutta yksityiskohtien merkityksestä. Asentajia on kehotettu tarkistamaan jokaikinen yksityiskohta ennen työn lopullista luovuttamista. Palomuurikohdassa on esitelty tietoturvalaitteita ja vertailtu niitä. Lopuksi on kiinnitetty huomiota tietoturvan laajentamiseen. Vertailussa on mukana neljä eri laitetta.

2 LANGATON LÄHIVERKKO

2.1 Standardit

Langaton lähiverkko käyttää radioaaltoja tiedonsiirtoon. Se on esimerkiksi sisätilojen lähiverkko ja antaa kaikille langattoman verkon piirissä oleville käyttäjille mahdollisuuden kirjautua verkkoon. Runkoverkkona langaton lähiverkko käyttää kaapeleita. Nykyään suosituin on standardiksi muodostunut WLAN eli Wireless Local Area Network.

WLAN on tärkeä yhteysmuoto monessa liiketoiminnassa. Markkinoiden arvellaan kasvavan, kun WLANin hyödyt huomataan. Suuria kasvunäkymiä odotetaan terveydenhuoltoon, opetustiloihin ja toimistoihin. Yritykset, tapaamispaikat, julkiset alueet ja sivutoimipaikat olisivat ihanteellisia paikkoja WLAN-käyttöön. Yhdysvalloissa on 2000-luvun alun innostuksen jälkeen todettu, että julkisten tilojen ilmaiset langattomat verkot ovat karsiutumassa.

WLAN on kaapeleilla toteutetulle lähiverkolle vaihtoehto paikoissa, joissa kaapelointi on vaikeaa tai mahdotonta. Sellaisia paikkoja voisivat olla vanhat suojellut rakennukset tai koulutilat. WLAN-asennukset ovat myös edullisia, koska ne koostuvat ainoastaan tukiasemista ja runkoverkkoasennuksista. Viimeinen osa verkosta kulkee ilmassa.

Langattomien lähiverkkojen alkuvaiheessa oli olemassa suljettuja protokollia ja eri verkkoja eri käyttötarkoituksiin. 1990-luvun lopussa protokollat korvautuivat standardeilla, jotka olivat pääasiassa toimistokäyttöön soveltuva IEEE 802.11 (2 Mb/s), kotikäyttöön tarkoitettu HomeRF (2 Mb/s) ja IEEE 802.11b (11 Mb/s). Viimeisin standardoitiin myöhään vuonna 1999, ja suuria määriä edullisia tuotteita eri valmistajilta alkoi saapua myyntiin vuoden 2000 puolivälissä. Standardi toimii lupa vapaalla ISM-taajuusalueella taajuudella 2,45 GHz. Tätä standardia noudattavia tuotteita on otettu käyttöön nopeaan tahtiin toimistoissa,

kodeissa ja julkisissa asennuksissa, kuten kahviloissa, yliopiston kampuksilla ja kirjastoissa.

Edullisten ja lupavapaiden verkkotuotteiden saatavuus on aikaansaanut uusien yhteisöverkkojen perustamisen. Toimivasta yhteisöstä hyvänä esimerkkinä on avoimeen standardiin perustuva SparkNet.

IEEE 802.11a-standardi, joka toimii myös lupavapaalla ISM-alueella 5 GHz:n taajuudella, mahdollistaa jopa nopeuden 54 Mb/s. Vaihtoehtona sille on eurooppalainen ATM-tyylinen 5 GHz:n teknologia HiperLAN, joka ei ole menestynyt poliittisten ja markkinasyiden takia.

WLAN on langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita. Useimmiten WLAN-termiä käytetään tarkoittamaan IEEE 802.11-standardia, mutta myös ETSIin HiperLAN-standardi on langaton lähiverkko. HiperLAN-standardin eri versiot eivät kuitenkaan ole kovin suosittuja, joten yleisessä kielenkäytössä termeillä WLAN, 802.11 ja Wi-Fi tarkoitetaan samaa asiaa, vaikka tarkkaan ottaen nämä termit eivät olekaan synonyymejä. Tavallisin käytössä oleva versio on 802.11g, jonka radiorajapinnan maksimisiirtonopeus on 54 Mb/s.

WLAN-tuotteista käytetään usein nimitystä Wi-Fi. Se on kaupallinen nimitys. Wi-Fi on Wi-Fi Alliancen tavaramerkki, jota jäsenet käyttävät määritellyn laatutason symbolina. Wi-Fi Zone -logolla merkityssä paikassa on tarjolla lähiverkko, johon voi liittyä Wi-Fi-yhteensopivalla päätelaitteella. Vastoin yleistä luuloa, Wi-Fi ei ole lyhenne sanoista ”Wireless Fidelity”. Se on vain tavaramerkki.

IEEE 802.11 on IEEE:n standardi langattomille WLAN-lähiverkoille. Varsinkin alkuaikoina käytettiin usein nimitystä langaton Ethernet, koska tekniikka on läheistä sukua Ethernetille (802.3). Nykyisin suosituimmat IEEE 802.11 -sarjan

standardit ovat 802.11b, nopeus 11 Mb/s ja 802.11g, nopeus 54 Mb/s. /9, 71-73,84/,/6 ,304,587/,/13/

2.2 Käyttötavat

Jatkossa esitellään erilaiset käyttöympäristöt. Lisäksi vertaillaan myös niiden teknisiä eroavaisuuksia.

2.2.1 Kotitaloudet

Kotitalouksissa WLAN:a käytetään muun muassa verkottamaan langallinen Internet-yhteys langattomaksi, jottei asuntoihin tarvitse kaapeloida erillistä sisäverkkoa. Asuntoon tulevaan kiinteään tietoliikenneyhteyteen liitettyyn modeemiin kytketään langaton tukiasema. Lisäksi asennetaan tukiaseman kanssa radioteitse kommunikoiva lähetin-vastaanotin tietokoneeseen. Se voi olla esimerkiksi PCI-verkkokortti pöytätietokoneeseen, PCMCIA-kortti yleensä kannettavaan tietokoneeseen tai USB:llä molempiin kytkettävissä oleva erillinen lähetin-vastaanotin. Kannettavissa tietokoneissa on nykyään lähes aina WLAN-lähetin-vastaanotin sisäänrakennettuna. Samoin monissa ADSL-modeemeissa on sisäänrakennettu WLAN-tukiasema, joskin näiden kuluttajahintaisten yhdistelmälaitteiden toimivuutta pidetään heikkona.

2.2.2 Kunnat, kaupungit ja elinkeinonharjoittajat

WLAN-tukiaseman liittäminen jo olemassa olevaan kiinteään tietoliikenneverkkoon on yksinkertaista ja edullista. Useat ravintolat ja kahvilat ovat alkaneet tarjota maksutta asiakkailleen WLAN-palvelua käytettäväksi esimerkiksi kannettavilla tietokoneilla, kämmentietokoneilla ja älymatkapuhelimilla. Myös kunnat ovat avanneet avoimia verkkoja, jotka voivat kattaa kunnan taajamat, kirjastot tai oppilaitokset. Näitä Wi-Fi tai WLAN-

hotspoteiksi kutsuttuja yhteyspisteitä tarjotaan jatkuvasti lisää, ja kokeilut myös julkisissa kulkuneuvoissa ovat käynnissä, mm. Muuramen kunnassa.

2.2.3 Operator WLAN

Operator WLAN eli oWLAN tai OWLAN on järjestelmä, joka yhdistää esimerkiksi GSM:n matkapuhelinverkon tilaajatunnisteen IMSIn WLAN-tekniikkaa käyttäviin verkkoihin. Tämä mahdollistaa verkkovierailun sekä laskutuksen hallinnoinnin. Englanniksi puhuttaessa verkkovierailusta käytetään sana Roaming. Teleoperaattorit tutkivat 2000-luvun alussa OWLAN-järjestelmien kaupallista hyödyntämistä, mutta se ei koskaan osoittautunut kannattavaksi liiketoimintamalliksi. OWLANn sijasta kuluttajat useimmiten yhdistävät matkapuhelimensa tietoverkkoon joko nopealla 3G-yhteydellä tai ilmaisella WLAN- hotspot-yhteydellä. /6, 587/

2.3 Tietoturvallisuus

WLAN-verkoista osa on avoimia ja osa on suojattu erilaisilla salasanoilla. Yksi melko yleinen ja nykyään jo tehottomaksi muodostunut salausprotokolla on WEP eli Wired Equivalent Privacy. Kun WEP tuli helposti murrettavaksi, kehitettiin TKIP eli Temporal Key Integrity Protocol ja sen jälkeen uusi tekniikka WPA.

Erilaisia ohjelmia on kehitetty salasanojen vahvuuden kokeilemiseen. Ohjelmia ovat AirSnort, Kismet, Kismat ja Elcomsoftin Wireless Security Auditor. /9, 77-78/

2.4 Kirjautuminen verkkoon

Service Set ID, SSID, on korkeintaan 32 merkkiä pitkä, muutettavissa oleva tunnus, jonka perusteella asiakkaat kytkeytyvät haluamaansa langattoman verkon tukiasemaan eli Access Pointiin.

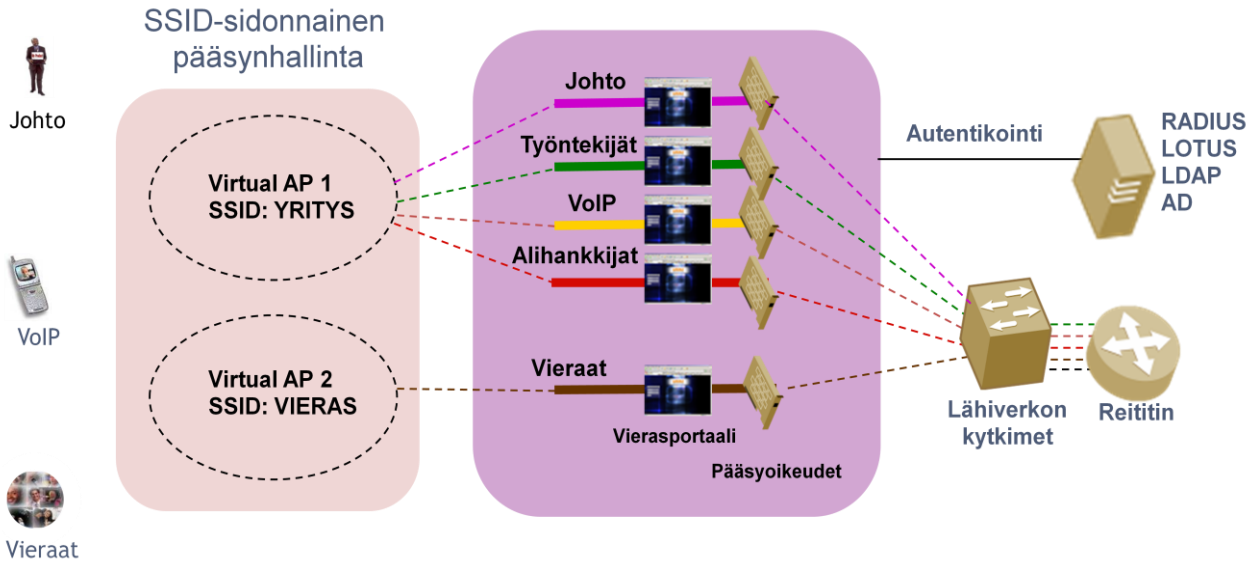
Access Point –laite on yleensä mahdollista asettaa lähettämään SSID-tietoa ilmatielle, ja monessa laitteesa tämä ominaisuus on oletuksena päällä. Näin asiakkaan ei tarvitse tietää SSID:tä kytkeytyäkseen kyseiseen verkkoon.

Kyseisestä ominaisuudesta on hyötyä, jos esimerkiksi yrityksessä tai oppilaitoksessa halutaan antaa vierailijoiden käyttää jotain osaa verkosta tai jos verkko on muuten tarkoitettu julkiseksi. Jos kuitenkin halutaan vaikeuttaa asiattomien henkilöiden pääsyä verkkoon, on suositeltavaa kytkeä tämä ominaisuus pois käytöstä tai valita ns. hidden-SSID–toiminto.

Uusiin AP-laitteisiin on tavallisesti asetettu valmiiksi jokin SSID, joka on yleensä saman valmistajan tuotteissa sama. Heti käyttöönoton yhteydessä SSID kannattaa muuttaa, jotta vältetään sekaantuminen esimerkiksi naapurin verkon kanssa.

On kuitenkin huomattava, että yllä mainitut varotoimenpiteet estävät ainoastaan satunnaiset verkkoskannaukset. Uuden asiakkaan kirjautuessa langattomaan lähiverkkoon, SSID-tieto kulkee salaamattomana asiakkaan ja Access Pointin välillä. Tarpeeksi kauan verkkoa kuuntelemalla on mahdollista saada SSID selville. /6, 10/

Seuraavalla sivulla kuvassa numero 1 esitellään malli vierasverkon toteuttamisesta.



Kuva 1. SSID:llä toteutettu vierasverkko

2.5 Pääsylistat

Access Pointissa voidaan käyttää listaa, jossa määritellään ne asiakaslaitteiden MAC-osoitteet, joilla on lupa päästä verkkoon. Tämä järjestelmä rajoittaa ulkopuolisten henkilöiden pääsyä verkkoon. Järjestelmä lisää verkon ylläpitäjän työtaakkaa, koska jokainen MAC-osoite on lisättävä manuaalisesti jokaisen verkon tukiaseman pääsylistaan. Jotkut tukiasemavalmistajat tarjoavat tuotteilleen ohjelmistoja, joilla voidaan toteuttaa listojen hallinta koostetusti.

Kovinkaan tehokkaana tapana verkkoon pääsyn rajoittamiseksi ei tule pitää verkkoon pääsyn suodattamista MAC-osoitelistalla. Listan osoittet kulkevat selväkielisinä paketeissa, vaikka niissä itse data olisikin salakirjoitettu. Tunkeutuja voi vähällä vaivalla selvittää verkkoliikenteen kuunteluohjelmalla jonkin verkossa käytettn MACin ja muuttaa oman MAC-verkkokorttinsa vastaamaan tätä. Menetelmä ei ole erityisen sopiva lähiverkkoihin, joissa käy paljon vierailijoita tai joissa tietokoneet vaihtuvat nopeasti. Tällaisessa tilanteessa täydellisen MAC-rekisterin ylläpitäminen voi olla hankalaa.

2.6 Autentikointi

Autentikoinnilla tarkoitetaan käyttäjän tunnistautumista kyseiseen verkkoon. Tunnistautumistapoja on erilaisia ja erivahvuisia.

2.6.1 WEP tunnistautuminen

WEP tarjoaa rajoitetun tavan verkossa tunnistamiseen. Asiakkaan laitteistopohjainen tunnistaminen voi olla joko avoin tai perustua jaettuun avaimeen AP:n ja asiakkaan välillä. Jos käyttäjän tunnistaminen on tarpeen, se voidaan toteuttaa RADIUS eli Remote Authentication Dial In User Service –protokollaa käyttäen. RADIUS-palvelin voi toimia monen erityyppisen tunnistamisen perustana, joten sitä voidaan käyttää esimerkiksi VPN eli Virtual Private Network -asiakkaiden tunnistamiseen. /9, 78-79/

2.6.2 WPA ja WPA2

WPA- ja WPA2-standardeissa molemminpuolinen autentikointi alkaa asiakkaan yrittäessä kirjautua tukiaseman piirissä olevaan verkkoon. Tukiasema, tiedostettua asiakkaan läsnäolon, estää tältä pääsyn verkkoon, kunnes asiakas saadaan tunnistettua. Käyttäjä antaa tunnistetiedot, jotka tukiasema toimittaa autentikointi-palvelimelle. Tunnistautuminen verkkoon tehdään käyttäen IEEE 802.IX/EAP -rajapintaa. Sekä asiakas että autentikointipalvelin tunnistautuvat toisilleen tukiaseman kautta. Molemminpuolinen tunnistautuminen lisää verkon turvallisuutta huomattavasti, koska myös palvelin tunnistautuu asiakkaalle. Näin käyttäjä tietää tunnistautuvansa oikealle autentikointipalvelimelle, eikä ole vaaraa joutua ns. evil twin -hyökkäyksen kohteeksi. Evil twin on luotettavaksi tekeytyvä rinnakkaistukiasema, jonka lähetysteho on korkeampi. Tämä mahdollistaa phishingin, eli kalastelun.

Kirjautumispalvelimen hyväksyessä asiakkaan tämä liitetään WLAN-verkkoon. Jos tunnistamista ei tapahdu, asiakkaan on mahdotonta päästä verkkoon. Kun asiakas tunnistetaan, asiakaskone ja palvelin luovat samanaikaisesti PMK eli Pairwise Master Key –avainparin.

Kun kirjautumispalvelin on hyväksynyt asiakkaan verkkoon käyttäjäksi, kirjautuminen saatetaan loppuun tukiaseman ja asiakkaan välillä. Tähän kuuluu salausavainten muodostaminen ja asentaminen asiakkaalle. Käytetty protokolla on WPA-standardissa TKIP eli Temporal Key Integrity Protocol ja WPA2-standardissa AES eli Advanced Encryption Standard. /6, 44/

2.7 Salausprotokollat

Salausprotokollilla tarkoitetaan avainta, jolla viesti salataan. Salauksella voidaan estää verkkohyökkäykset.

2.7.1 WEP

WEP on WLAN-tekniikan alkuperäinen, vanhentunut ja verkkohyökkäyksille alttiiksi osoittautunut salausprotokolla. WEP käyttää 40-, 104- tai 232-bittistä salausta. Sen RC4-salausprotokollassa olevan puutteen vuoksi joidenkin pakettien kehyksissä lähetetään salaamattomia bittejä, alustusvektoreita (initialization vector IV) ja niiden perusteella voidaan helposti laskea käytetty salausavain. Monet uudemmista WLAN-korteista sisältävät tekniikkaa, jolla pystytään vähentämään näiden tietojen lähettämistä.

Tehokkaampaa salausta käytettäessä AirSnort-ohjelman UKK-sivun mukaan 16 miljoonasta lähetetystä paketista keskimäärin 9000 sisältää ohjausvektoritietoa. Salausavaimista useimmat pystytään selvittämään noin 2000 ”heikon paketin” perusteella. Mitä enemmän tietoa verkossa liikkuu, sitä nopeammin salausavain

saadaan selvitettyä. WEP-salausta ei suositella käytettäväksi, koska se on purettavissa melko helposti.

2.7.2 WPA eli TKIP

WPAn uusi salausmetodi poistaa kokonaan WEP-salauksen tunnetut ongelmakohdat, jotka johtuvat WEPin käyttämästä staattisesta salausavaimesta. TKIP korvaa WEPin käyttämän tukiaseman ja asiakkaalle manuaalisesti syötetyn 40-bittisen staattisen avainparin 128-bittisellä pakettikohtaisella salausavaimella. WEPin purkamisessa oleellisena osana oleva salausavaimen ennustettavuus poistuu TKIP-avainta käytettäessä, koska avainparit luodaan pakettikohtaisesti. WPA-salaus sisältää myös pakettien eheyttä valvovan MIC eli Message Integrity Check –toiminnon, joka tarkistaa jokaisen paketin. Tällöin mahdollinen hyökkääjä ei pysty ottamaan paketteja ja muuttamaan niiden tietoja. WPA toimii verkon fyysisellä MAC- kerroksella.

Sen jälkeen kun käyttäjä on autentikoitu verkkoon käyttäjäksi jonkin edellä mainitun tavan mukaisesti, joko kirjautumispalvelin tai tukiasema luo uniikin pääavainparin PMK:n käyttäjälle tapahtuman ajaksi. TKIP-protokolla toimittaa avaimen käyttäjälle, eli luo avainhierarkian ja dynaamisten avainten hallintajärjestelmän. Tämän avaimen mukaan TKIP luo pakettikohtaiset avaimet jokaisen verkkoon toimitetun paketin salaamiseksi.

Kyseinen tekniikka korvaa WEP-salauksen staattisen, manuaalisesti syötetyn avainparin, noin 280 triljoonalla mahdollisella avaimella. Kyseisiä avaimia voidaan käyttää jokaisen paketin salaamiseen.

MIC estää hyökkääjää muuttamasta verkossa liikkuvien pakettien sisältöä vahvan matemaattisen funktion avulla. Tässä sekä lähettäjä että vastaanottaja laskevat jokaisesta paketista tarkistussumman. Näitä verrataan keskenään pakettien eheyden takaamiseksi. Jos MIC-toiminnot eivät täsmää, paketin katsotaan olevan

muutettu, ja se jätetään huomioimatta. MICissä on myös ylimääräinen turvallisuustoiminto. Siinä havaittaessa virheellinen paketti, kaikki verkon asiakkaat autentikoidaan uudelleen ja kaikki uudet tunnistuspyynnöt estetään minuutin ajaksi.

2.7.3 WPA2 eli AES

AES:a vastaan ei ole yhtään tunnistettua hyökkäystä. Kansallinen turvallisuusvirasto eli NSA on hyväksynyt kaikki AES-protokollaa käyttävät tekniikat salaamaan Yhdysvaltojen hallituksen ”non-classified”-luokiteltua tietoa. Siviileillä ei ole ollut pääsyä salaustekniikkaan, jonka NSA on hyväksynyt salaamaan TOP SECRET –luokittelemaansa aineistoa. /8, 242-244/

2.8 Tietomurron havaitseminen

Useat WLAN-kortit on mahdollista asettaa kuuntelutilaan. Tällöin ne eivät lähetä tietoa, vaan vastaanottavat verkossa liikkuvaa tietoa. Tässä tilassa tehtyä verkkokuuntelua ja pakettien keräystä salausavaimien purkamiseksi on mahdotonta havaita.

Täysin laillisesti tätä ominaisuutta on mahdollista käyttää myös oman verkon valvomiseen. Kuuntelemalla verkkoa voidaan nopeasti havaita yhteydenottoyritykset tuntemattomilla tai väärennetyillä MAC-osoitteilla. Varoittavaa on esimerkiksi se, jos jonkun oman koneen verkkokortin MAC-osoitteella näyttäisi olevan liikennettä aikana, jolloin kone ei ole varmasti käytössä. Tällaisten tietojen perusteella voi harkita, onko syytä nostaa langattoman lähiverkkonsa tietoturvaa. Salauksessa voisi esimerkiksi ottaa tehokkaamman algometrin käyttöön.Verkkokuunteluun ja WEP-salauksen murtamiseen sopivia ohjelmia ovat esimerkiksi seuraavat: AirSnort, Kismet ja KisMAC.

3 WLAN-KYTKIMET

Wireless Local Area Network –kytkimet mahdollistavat signaalin ohjaamisen eri tukiasemiin. Seuraavassa esitellään kuusi erilaista mallia.

3.1 Aruba 200 Mobility controller

Aruba 200 on malliston pienin laite. Se tarjoaa kuusi power over Ethernet –porttia tukiasemille ja tukee enintään sataa käyttäjää. Suurin käytössä oleva malli tukee peräti 512 tukiasemaa ja 800 käyttäjää. Kalifornialaisen Aruba Networksin ratkaisut skaalautuvat suuryrityksiin ja operaattoreihin asti. Huomattavin referenssiasiakas on Microsoft.

Hallintaohjelmistot asennetaan selaimella hallittavaan kytkimeen eikä erillistä hallintapalvelinta tarvita. Vertailussa oleva malli on varustettu kaikilla optioilla, joiden hinnat ovat kuitenkin melko kohtuulliset. Aruban ratkaisu on vertailun monipuolisin. Suunnittelussa otetaan huomioon laitteiden sijainti. Käyttäjien oikeuksia ja asetuksia voidaan määritellä paitsi WLAN- myös rooli- ja politiikkapohjaisesti.

Forte Netservices edustaa Arubaa Suomessa. Se keskittyy laitemyynnin sijasta hallittujen verkko- ja tietoturvapalvelujen tarjoamiseen. Arubaa kannattaa harkita palveluna, koska sen hallintaohjelmisto on vertailun vaikeimmin hahmotettava. Näyttöruudut muodostavat loogisen puurakenteen sijasta hajanaisesti kytketyn verkon. Seikkailtaessa verkossa yksittäisten asetusten merkitys hämärtyy helposti, varsinkin kun opastustoiminto puuttuu kokonaan. Pystyvä ja monipuolinen WLAN-verkkojen hallintaratkaisu vaatii pääkäyttäjältään paljon. /1/,/16/

3.2 Cisco WLC2006

Pitkään Cisco luotti perinteisiin älykkäisiin Aironet-tukiasemiinsa ja niitä varten kehittämäänsä SWAN-arkkitehtuuriin, structured wireless aware nework. Keväällä 2005 yhtiö osti WLAN-kytkimiin erikoistuneen Airespace-yhtiön. Cisco on onnistunut integroimaan hankkimansa teknologian tuotelinjaansa runsaassa vuodessa.

Cisco tarjoaa nyt WLAN-kytkimiä vertailuun saadun mallin tapaan erillislaitteina, mutta myös moduuleina Ethernet-kytkimiinsä ja haarakonttorireitittimiinsä. Vanhat Aironet-tukiasemat voidaan päivittää WLAN-kytkimellä hallittaviksi. Näin niitä ei tarvitse vaihtaa Airespacen tukiasemateknologiaksi. Yhtiö on myös lisännyt kytkimiin tuen WLAN-sovitintensa CCX-tekniikalle. CCX tulee sanoista cisco compatible extensions. Näin pystytään mm. tukemaan langatonta multimediakäyttöä. Erillinen WCS-hallintapalvelin on saatavissa WLAN-kytkinten hallintaan ja verkon suunnitteluun. Yksittäisen laitteen perushallinnassa WEB-käyttöliittymä riittää hyvin.

Jalometallien mukaan nimettyjä yhteyden laatusanoja on neljä. Niiden merkitys käy selväksi tyyliin platina IP-puheelle, pronssi taustaliikenteelle. Osa asioista on esitetty selkeästi, vaikka opasteissa onkin puutteellisuuksia. Takuuaika on 3 kk. Cisco WLAN 2006 on ajanmukainen WLAN-kytkin, joka sopii pk-yrityksen ratkaisuksi yhtä hyvin kuin ison Cisco-verkon osaksi. /2/,/16/

3.3 HP Procurve 5304xl + Wes xl

HP Procurve Networking pitää ratkaisussaan WLANin roolina olla korostetusti lankaverkon jatke. WES xl eli wireless edge services on procurve 5300xl-sarjan kytkimiin asennettava moduuli, johon langattoman verkon äly keskitetään WLAN-kytkinten tapaan.

WES-moduulissa ei ole itsessään liitäntäportteja. Tukiasemat, joita kutsutaan radioporteiksi, liitetään joko samaan tai toiseen kytkimeen eri moduuleilla. Nämä tarjoavat niille virransyötön Ethernet-portin kautta.

WES tukee vain omia radioporttejaan. Edes HP:n omat vanhat tukiasemat eivät sovellu kytkimellä hallittaviksi. Testissä (3.11.2010) laite havaitsi vieraista tukiasemista vain Symbolin mallit. Yhtiöt eivät ole vastanneet kysymykseen mahdollisesta OEM-sopimuksesta, Original Equipment Manufacturer, joka tarkoittaa alkuperäistä laitevalmistajaa.

Java-pohjainen selainhallinta tapahtuu Procurve-tyyliin, mutta kehikolla ja WES-moduulilla on omat IP-osoitteensa. WES integroituu muihin HP:n hallintaohjelmiin, kuten Procurve Manager plussaan, Mobility manageriin sekä päävalvontaa helpottavaan Identity driven manageriin. Laitteilla on ikuinen takuu, kuten muillakin Procurve-tuotteilla. Ratkaisu on selkeä, mutta se vaatii Procurve-ympäristön. Toiminnot ovat suppeat. WLAN-kytkin on asiallinen HP:n Procurve-verkkoinfraan sovitettu, muttei kovin edistynyt. /5/,/16/

3.4 Nortel WLAN Security Switch 2360

Nortelin ratkaisu perustuu Trapeze networks –nimisen, WLAN-kytkimiin erikoistuneen yhtiön tekniikkaan. Kakkos- ja kolmoskerroksilla toimivia kytkimiä voidaan joustavasti liittää yhteen nortel mobility domain –hallinnan avulla. Näin järjestelmä skaalautuu helposti suuriinkin verkkoihin. Rajoituksin kytkinhallinnan piiriin voidaan tuoda myös muita kuin Nortelin omia tukiasemia.

Vertailun tuotteista Aruban jälkeen toiminnoiltaan monipuolisin on Nortelin WLAN-kytkin. Avainkäsitteenä ovat palvelut, joita kytkimeen määritellyt WLAN-tekniikat tarjoavat. Käyttäjät saavat käyttöönsä kyseisiä palveluja kirjauduttuaan verkkoon.

Pääkäyttäjä voi myös luoda virtuaalisia palveluryhmiä. Näille voidaan asettaa omat tietoturva- ja todennusmenettelynsä, portaalinsa ja liikennemäärittelynsä. Täten Nortelin ratkaisu soveltuu yrityspuistojen ja muiden moniasiakasympäristöjen WLAN-verkkojen rungoksi.

Suoraviivaisella ja kankealla selainhallinnalla voidaan tehdä kytkimen asetuksia. Laitteen monipuolisuuden vuoksi erillisen WLAN Management –option hankinta on erittäin suositeltavaa. Se on tämän vertailun selkeimmin dokumentoitu ja pystyvin WLAN-kytkinten hallintaohjelmisto. Vaikka selainhallinta onkin kankea, laaja toiminnallisuus, skaalautuvuus ja dokumentointi takaavat käyttäjien arvostuksen. Nortel WLAN Security Switch 2360 on monipuolinen, mutta selkeä WLAN-kytkin, jonka ominaisuudet eivät heti lopu. /10/,/16/

3.5 Siemens Hipath Wireless Controller C10

Siemensillä on vahva tausta puhelinvalmistajana. Se näkyy yhtiön WLAN-kytkintarjonnassa. Yhtiö toimitti ainoana valmistajana vertailuun kytkimensä kanssa yhteensopivia, 802.11g-verkossa toimivia SIP-puhelimia (optipoint w12 professional). IP-puhetta välittävien WLAN-kytkinten luonti ja hallinta on helppoa.

WLAN-kytkin on Siemensin arkkitehtuurissa täysiverinen ospf-reititin. Tukiasemat asennetaan verkon taakse. Kytkimen rooli on vahvemmin hallinnassa kuin tosiaikaisessa ohjauksessa. Tukiasemiksi käyvät muutkin kuin Siemensin valmistamat. Ne voivat liikennöidä lankaverkkoon joko suoraan tai WLAN-kytkimen kautta.

Kytkin ei tue työasemien siirtymistä toisen kytkimen hallitsemalle tukiasemalle eikä tarjoa laajennettavuutta. Sitä ja järeämpiä rinnakkaismalleja voidaan kuitenkin konfiguroida keskitetysti. Toiminnot löytyvät kytkimen

selainkäyttöisestä hallintaohjelmistosta helposti. Erillistä graafista hallintaohjelmaa ei ole tarjolla.

Siemensin ratkaisu tukee 30 tukiasemaa, mutta tarjoaa suppeahkot toiminnot. Käyttäjien pääsynvalvonnasta tai tunkeilijoiden torjunnasta sekä radioverkon suunnittelun ja hallinnan apuvälineistä kiinnostunut löytää vertailun tuotteista helposti Siemensiä kehittyneempiä ratkaisuja. Vaikka Siemensin arkkitehtuuri on selkeä ja puheratkaisu kattava, käyttäjiä hillitsevät korkea hinta ja rajallinen toiminnallisuus. Siemens on suunnitellut erityisesti IP-puheelle WLAN-ratkaisun. /11/,/16/

3.6 Symbol WS2000

Symbol pitää itseään koko tuoteryhmän keksijänä, koska se toi ensimmäisen WLAN-kytkimen markkinoille jo vuonna 2002. WS2000 poikkeaa vertailun muista tuotteista siinä, että se on selkeästi pienyritys- tai sivukonttorikäyttöön.

Internet-liityntään sopivan, PPPOE-tuella varustetun WAN-portin ohella muovikuorinen pikkukytkin tarjoaa puoli tusinaa porttia tukiasemia tai palvelimia varten. Osoitteenmuutoksen tekevä tilallinen palomuuri on integroitu laitteeseen. Lisäksi laitteessa on IPSEC-tuki sekä RADIUS-palvelin käyttäjien todennusta ja laskutustietojen keruuta varten.

Symbol tukee muiden kytkintoimittajien tapaan myös IP-puhetta. WS2000 on erityisesti optimoitu SIP-puheluiden hallintaan. Tukiasema voidaan haluttaessa asettaa toimimaan sensorina, joka kuuntelee jatkuvasti radiotietä luvattomien tukiasemien hallitsemiseksi. Saatavissa on myös optiona WIPS-ohjelmisto, joka tulee sanoista wireless intrusion protection system. Tukiasema voidaan palauttaa normaalikäyttöön, kun tietoturvaongelma on torjuttu.

CF-korttipaikka on laitteen erikoisuutena. Sitä voidaan käyttää esimerkiksi ohjelmistopäivitysten jakeluun. Kokonaisuus kaikkineen on järkevä rajalliseen käyttöön, mutta laajennusvaraa ei ole. Symbolin ratkaisu on pienyrityskäyttöön suunniteltu helppokäyttöinen WLAN-kytkin. /14/,/16/

Taulukossa 1 esitellään erilaisia WLAN kytkimiä. Hintoja on vertailtu hankintamielessä.

Taulukko 1. WLAN-kytkinten kontrollereita

Laite	Hinta	Arviointi
Aruba 200 Mobility controller	4937 €	monipuolisin
Cisco WLC2006	4860 €	8,2
HP Procurve 5304xl + Wes xl	9963 €	7,9
Nortel Wlan Security Switch 2360	4230 €	8,2
Siemens Hipath Wireless Controller C10	14064 €	7,3
Symbol WS2000	3084 €	7,9

Taulukossa olevat tiedot perustuvat Tietokonelehden asiantuntijoiden vertailun tuloksiin.

Laitteet ovat taulukossa selvityksessä olevassa järjertyksessä. Hinnat ovat valmistajien antamia. Arubasta on itse laitteen hinta, mutta vertailun kokoonpanon hinnaksi tulee 7594 €. HP Procurven hinta alkaen 9963 €:a sisältää kytkinkehikon.

Siemensin arkkitehtuurin selkeys ja puheratkaisun kattavuus nostavat hinnan muita korkeammaksi.

Asiantuntijat ovat arvioineet laitteet ja antaneet arvosanan kullekin. Aruballe ei ole annettu varsinaisesti arvosanaa, mutta se oli arvioinnissa monipuolisin. Vaikka Siemensin laite on kallein, sai se alhaisimman arvosanan. Ciscoa pidetään yleisesti melko laadukkaana. Se menestyy myös hintavertailussa.

3.7 Vertailu ostajan näkökulmasta

Ostajaa kiinnostaa yleensä hinta, mutta se ei välttämättä ole ainoa ratkaisuun vaikuttava tekijä kaupantekotilanteessa. Keskitetyn hallinnon kontrollereista valittaessa asiakas vaatii usein selkeyttä, johon liittyy myös helppokäyttöisyys. HP Procurven tarjoama ratkaisu on selkeä, mutta se vaatii Procurve-ympäristön. Vaikka toiminnot ovat suppeat, saattaa ostajaa kiinnostaa se, että laitteilla on ikuinen takuu.

Ciscon ratkaisussa osa asioista on esitetty selkeästi, vaikka opasteissa onkin puutteellisuuksia. Ostajaa saattaa arveluttaa takuuaika, joka on vain 3 kk. Jos asiakas on PK-yritys, on hyvä tietää, että ajanmukainen Cisco WLAN 2006 sopii hyvin ratkaisuksi. Kytkin sopii yhtä hyvin myös ison Cisco-verkon osaksi.

Nortel Wlan Security Switch 2360:n selainhallinta on kankea. Siitä huolimatta ostaja arvostaa laitteen toiminnallisuutta, skaalautuvuutta ja dokumentointia. Nortelin tarjoama laite on monipuolinen, mutta selkeä WLAN-kytkin. Sen ominaisuudet eivät lopu heti.

Symbolin ratkaisu kaikkineen on järkevä rajalliseen käyttöön. Helppokäyttöinen WLAN-kytkin on suunniteltu pienyrityskäyttöön. Ostajan on kuitenkin hyvä tietää, ettei laajennusvaraa ole. Symbol WS2000 on erityisesti optimoitu SIP-puheluiden hallintaan.

Siemensin tarjoamassa ratkaisussa tukiasemiksi käyvät muutkin kuin Siemensin valmistamat. Käyttäjien pääsynvalvonnasta tai tunkeilijoiden torjunnasta kiinnostunut ostaja löytää helposti vertailuun otetuista tuotteista Siemensiä kehittyneempiä ratkaisuja, korkeasta hinnasta ja rajoittuneesta toiminnallisuudesta huolimatta, Siemensin arkkitehtuuri on selkeä ja puheratkaisu kattava.

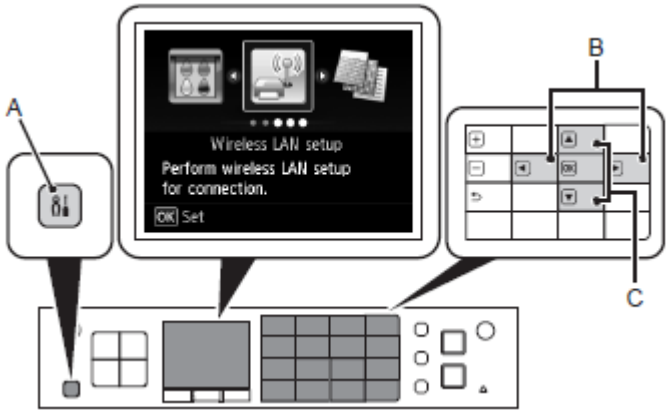
Suomessa Arubaa edustava Forte Netservices keskittyy laitemyynnin sijasta hallittujen verkko- ja tietoturvapalvelujen tarjoamiseen. Vaikka Aruban ratkaisu on vertailun monipuolisin, ostajan on hyvä tietää, että opastustoiminto puuttuu kokonaan. Pääkäyttäjältä vaaditaan paljon monipuolisen WLAN-verkkojen hallintaratkaisun äärellä.

4 VERKON ASENTAMINEN

4.1 Fyysinen liitäntä verkkoon tai laajakaistamodeemiin

Tietokoneessa on oltava verkkosovitin asennettuna ja verkkokaapeli kytkettynä, ennen kuin tietokone liitetään langattomaan verkkoon. Verkkokaapeli kytketään tietokoneen takana olevaan verkkosovittimen liittimeen. Kaapeliliitin työnnetään oikeaan kohtaan, kunnes se napsahtaa paikalleen. Kaapelista voidaan vetää kevyesti ja varmistaa sen olevan kiinni tiukasti. Verkkokaapelin toinen pää kiinnitetään verkkoyhteyslaitteeseen tai seinässä olevaan verkkoliittimeen. On varottava kytkemästä verkkokaapelia seinässä olevaan puhelinliittimeen.

Kuvassa 2 esitellään kytkentäpaneeli.



Kuva 2. Liitäntä verkkoon tai laajakaistamodeemiin.

4.2 Ohjattu verkon asennus

Microsoft Windows XP –käyttöjärjestelmä sisältää ohjatun verkon asennuksen. Se antaa ohjeita tiedostojen jaosta, tulostimien ja kotona tai toimistossa olevien tietokoneiden välisistä verkkoyhteyksistä.

Ensin valitaan **Käynnistä** –> **Ohjelmat** -> **Apuohjelmat** –> **Tietoliikenneyhteydet** –> **Ohjattu verkon asennus**. Sitten valitaan Tervetuloa-ikkunassa **Seuraava**. Lopuksi napsautetaan **Verkon luomisen tarkistuslista**.

Jos valitaan väite **Tästä tietokoneesta on suora yhteys Internetiin**, kytkeytyy päälle integroitu palomuuri, joka toimitetaan Windows XP Service Pack 2:n (SP2) mukana.

Seuraavaksi täydennetään tarkistuslista. Viimeiseksi palataan Ohjatun verkon asennukseen ja seurataan näytön ohjeita.

WLAN-yhteyden asentamista varten tarvitaan nopea Internet-yhteys, kuten kaapeli tai DSL, kytketty ja toimiva laajakaistamodeemi sekä langaton reititin tai tukiasema. Lisäksi tarvitaan langaton verkkokortti jokaiselle tietokoneelle, joka halutaan liittää WLAN-verkkoon, ja verkkoliittimellä (RJ-45) varustettu verkkokaapeli. /8, 81-85/

4.2.1 Langattoman verkkokortin tarkistus

On syytä varmistaa, että tietokoneessa on langaton verkkokortti ja määrittää kortin tyyppi. Varmistaminen onnistuu menetelmällä, josta käytetään nimitystä **Käynnistä**-painike ja **Yhdistä**-vaihtoehto. Ensin painetaan **Käynnistä**-painiketta. Sitten valitaan **Yhdistä** ja lopuksi **Näytä kaikki yhteydet**.

Jos langaton verkkoyhteys ei ilmaannu LAN- tai nopea Internet-yhteyskohdan alle, koneessa ei ole langatonta verkkokorttia. Jos Langaton verkkoyhteys ilmaantuu, koneessa on langaton verkkoyhteys. Langattoman verkkokortin tarkkoja tietoja tarkastellaan valitsemalla hiiren kakkospainikkeella **Langaton verkkoyhteys**. Sen jälkeen valitaan **Ominaisuudet**. **Langattoman verkkoyhteyden ominaisuudet** –ikkuna tulee esiin.

Jos tietokone on asetettu **Klassinen käynnistys** –valikkovaihtoehtoon, verkkoyhteyksiä voi tarkastella napsauttamalla **Käynnistä**-painiketta, valitsemalla **Asetukset** ja lopuksi valitsemalla **Verkkoyhteydet**. Koneessa ei ole langatonta verkkoyhteyttä, jos **Langaton verkkoyhteys** ei tule esiin. /7, 54-56/ , /5, 50-53/

4.2.2 Uuden WLAN-yhteyden asetus

Langattoman reitittimen ja laajakaistamodeemin liittämisessä on hyvä ottaa yhteyttä Internet-palveluntarjoajaan (ISP), jotta saadaan tarkat tiedot laajakaistamodeemin yhteysvaatimuksista. On varmistettava, että koneessa on langallinen Internet-yhteys, ennen kuin yritetään asettaa langaton Internet-yhteys.

Seuraavaksi asennetaan langattoman reitittimen vaatimat ohjelmistot. Langaton reititin on mahdollisesti toimitettu CD-asennuslevyn kanssa. Tällainen CD-levy sisältää yleensä asennus- ja vianmääritystiedot. Vaaditut ohjelmistot asennetaan valmistajan ohjeiden mukaisesti. Tietokone sammutetaan, samoin muut mahdolliset lähietäisyydellä olevat langatonta toimintaa tukevat tietokoneet **Käynnistä**-valikon kautta. Laajakaistamodeemin virtajohto on irrotettava sähköpistorasiasta, samoin verkkokaapeli tietokoneesta ja modeemista.

On hyvä odottaa 5 min laajakaistamodeemin irrotuksen jälkeen, ennen kuin jatketaan verkkoasennusta. Sen jälkeen on irrotettava verkkolaitteen johto reitittimestä, jotta varmistetaan, ettei reitittimeen tule virtaa. Verkkokaapeli liitetään virrattomassa laajakaistamodeemissa olevaan verkkoliittimeen (RJ-45) ja verkkokaapelin toinen pää kiinnitetään virrattomassa langattomassa reitittimessä olevaan Internet-verkkoliittimeen (RJ-45).

On varmistettava, ettei yksikään verkko- tai USB-kaapeli, muut kuin modeemin ja langattoman reitittimen liittävä verkkokaapeli, ole liitettynä laajakaistamodeemiin.

Langattomat laitteet käynnistetään uudelleen alla kuvatussa järjestyksessä, jotta estetään mahdollinen yhteysongelma.

Päälle kytketään vain laajakaistamodeemi ja odotetaan vähintään 2 min, jotta laajakaistamodeemin toiminta vakiintuu. Tämän jälkeen työtä jatketaan. Langaton reititin kytketään päälle ja odotetaan vähintään 2 min, jotta langaton reititin vakiintuu. Työtä jatketaan odotteluajan jälkeen. Tietokoneen käynnistämisen jälkeen odotetaan, kunnes käynnistys on valmis. Langattoman reitittimen asentamiseksi on muodostettava yhteys tietokoneen ja langattoman reitittimen välille. Seuraavaksi on määritettävä langaton reititin kommunikoimaan laajakaistareitittimen kanssa. Lisäksi on otettava selville langattoman reitittimen lähetysnimi. Tekninen termi reitittimen lähetysnimelle on Service Identifier SSID tai verkkonimi. Tarvittaessa on hyvä määrittää langaton verkkokortti yhteyden muodostamiseksi langattomaan verkkoon.

Ennen WLAN-verkkoon kytkeytymistä on varmistettava, että on noudatettu langattomasta lähiverkosta annettuja ohjeita. Langaton verkkokortti vaatii erityiset ohjelmistot ja ohjaimet verkkoon liittymiseen. Jos ohjelmisto on poistettu tai se on viallinen, on seurattava käyttöoppaassa olevia ohjeita langattomasta verkkokortista. On hyvä varmistaa tietokoneelle asennetun langattoman verkkokortin tyyppi.

4.2.3 Langattoman verkon laitehallinnan määrittäminen

Erilaiset langattomat määritysapuohjelmat tietokoneelle asennetusta ohjelmistosta riippuen voivat hallita verkkolaitteita. Nämä voivat olla esimerkiksi langattoman verkkokortin määritysapuohjelma tai Windows XP –käyttöjärjestelmä.

Langattoman verkkokortin määritysapuohjelman määrittämisessä edetään seuraavasti:

- Valitaan **Käynnistä** – **Asetukset** – **Ohjauspaneeli**.
- Kaksoisnapsautetaan **Verkkoyhteydet**-kohtaa.
- Napsautetaan hiiren kakkospainikkeella **Langaton verkkoyhteys** -kuvaketta ja lisäksi napsautetaan **Tarkastele seuraavana olevia langattomia verkkoyhteyksiä**.

Jos **Valitse langaton verkko** –ikkuna ilmoittaa, että **Windows ei voi määrittää tätä yhteyttä**, langatonta verkkokorttia hallitsee langattoman verkkokortin määritysapuohjelma. Jos **Valitse langaton verkko** –ikkuna ilmoittaa, että **Napsauta alla olevan luettelon kohtaa langattoman verkkoyhteyden luomiseksi tai lisätietojen etsimiseksi**, langatonta verkkoa hallitsee Windows XP –käyttöjärjestelmä.

WLAN-yhteyden muodostamisen loppuun saattamisessa on hyvä noudattaa ohjeita. Kun käynnistetään tietokone ja alueella havaitaan verkko, jolle tietokonetta ei ole määritetty, ponnahdusikkuna avautuu Langaton signaali –kuvakkeen viereen Windows-työpöydän oikeaan alakulmaan. Tulee ilmoitus, että langaton verkko on havaittu. On hyvä noudattaa näyttöön tulevien apukehotteiden ohjeita.

Kun tietokone on määritetty valittua langatonta verkkoa varten, toinen ponnahdusikkuna ilmoittaa, että tietokone on kytketty verkkoon. Aina kun kirjaudutaan tietokoneelle valitun langattoman verkon kantama-alueella, sama ponnahdusikkuna ilmoittaa langattomasta verkkoyhteydestä.

Jos valitaan suojattu verkko, on kirjoitettava WEP- tai WPA-tunnus vaadittaessa. Verkon suojausasetukset ovat verkkokohtaisia. Tietokoneelta voi kestää verkkoyhteyden muodostamiseen jopa minuutti. Jos langattomaan verkkoon ei

saada yhteyttä, on varmistettava, että on olemassa kaikki WLAN-yhteyden muodostamiseen vaadittavat komponentit.

Tämän jälkeen on tarkistettava, että langaton verkkokortti on otettu käyttöön painamalla <Fn><F2>. Tietokoneen langattoman verkkotoiminnan voi kytkeä päälle ja pois päältä painamalla <Fn><F2>-näppäinyhdistelmää. Jos langaton verkkotoiminto on kytketty päälle, tulee painaa <Fn><F2> sen poiskytkemiseksi. Langattoman toiminnan ilmaisin osoittaa, onko tietokoneen langattomat laitteet otettu käyttöön vai poistettu käytöstä. Kun kytketään langaton verkkotiminto päälle tai päältä pois, langattoman toiminnan ilmaisin muuttuu näyttämään tilan.

4.3 Mobile Broadband

Mobile Broadband –verkko, tunnetaan myös nimellä WWAN eli Wireless Wide Area Network, on paljolti samanlainen kuin WLAN-verkko. Se muodostuu joukosta yhteenkytkettyjä tietokoneita. Nämä kommunikoivat toistensa kanssa langattomalla verkkotekniikalla. Matkapuhelintekniikkaa käyttävä Mobile Broadband –verkko tarjoaa siten Internet-yhteyden siellä, missä matkapuhelinverkkokin toimii. Niin kauan kuin tietokone pysyy matkapuhelinpalvelun tarjoajan palvelualueella, tietokone voi ylläpitää Mobile Broadband –verkkoyhteyttä sen fyysisestä sijainnista huolimatta.

Mobile Broadband –yhteyden tarjoamiseen tietokone tukee 34 mm:n ExpressCard-korttia. Ohjeet koskevat vain Mobile Broadband ExpressCard- tai Mini-Card-kortteja. Ne eivät koske sisäisiä kortteja, joissa on langaton Bluetooth-tekniikka, tai WLAN Mini-kortteja.

Ennen kuin otetaan yhteys Internetiin, on aktivoitava Mobile Broadband –palvelu matkapuhelinpalvelun tarjoajan kautta. Dell Mobile Broadband Card apuohjelmaa käytetään muodostamaan ja hallitsemaan Mobile Broadband –verkkoyhteyttä Internetiin. Ensin on napsautettava apuohjelman suorittamiseksi

Dell Mobile Broadband Card –apuohjelman kuvaketta, joka on Windowsin tehtävärivillä. Seuraavaksi valitaan painike **Yhdistä**. Kyseinen painike muuttuu **Katkaise yhteys** –painikkeeksi. Lopuksi on seurattava näytöllä näkyviä ohjeita verkkoyhteyden hallitsemiseksi apuohjelmalla.

5 PALOMUURI

5.1 Internet-yhteyden palomuuri

Internet-yhteyden palomuuri tarjoaa tietokoneen luvatonta käyttöä vastaan perussuojan, kun tietokone on kytketty Internetiin. Kun Ohjattu verkon asennus toteutetaan, palomuuri otetaan automaattisesti käyttöön. Palomuurikuvake ilmaantuu punaisella taustalla Ohjauspaneelin Verkkoyhteyden-osioon, kun palomuuri on otettu käyttöön verkkoyhteyttä varten. On hyvä tietää, että Internet-yhteyden palomuuri ei vähennä viruksentorjuntaohjelmiston tarvetta.

Monipuolisissa UTM-tietoturvalaitteissa yhdistyvät virusten, hyökkäyksien ja roskapostin torjunta sekä etäyhteydet, langaton verkko ja WEB-selailun suodatus. UTM Unified Threat Management. Markkinatutkijat ovat arvioineet, että tietoturvan yhdistelmälaitteita myydään jo nyt enemmän kuin perinteisiä palomuuri- ja etäkäyttölaitteita.

Asiantuntijoiden vertailussa huomattiin, että UTM-laitteista on kasvanut hyvä tuoteryhmä. Laadussa ja ominaisuuksissa on eroja, mutta suuria suorituskykyongelmia on enää harvoin. Vertailussa olivat mukana Fortinetin, Sonicwallin, Watchguardin ja Zyxelin utm-laitteet. Laitteiden suorituskyvyn, tiedonsiirtonopeuden viidellä eri tavalla sekä virrankulutuksen mittasi Tietokone-lehden tutkimuslaboratorio TK Labs. Vertailussa arvioitiin lisäksi laitteiden turva- ja verkko-ominaisuudet sekä etäkäyttöominaisuudet. Lisäksi arvioitiin hallinta ja käyttöönotto. /8, 105-111/,/3, 56-57/

5.2 Tietoturvalaitteet

Työssä esitellään fyysiset tietoturvalaitteet, jotka eroavat ohjelmistoversioista.

5.2.1 Fortinet Fortigate 60

Fortinet on umt-laitteiden edelläkävijä. Toteutuksessa laite on rakennettu fortiasic-kiihdytinpiirin ympärille. Tulos rasitusmittauksissa (Tietokonelehti) oli vertailun paras. Kyseessä on kevyehkö malli, mutta Fortigate pystyy suojaamaan liikennettä hidastamatta varsin tehokkaankin laajakaistayhteyden antiviruksen kera.

Fortinet tuottaa tietoturvapalvelunsa itse. Suojaukset vaikuttavat melko kattavilta. Myös muut laitteen ominaisuudet ovat kelvolliset, aina sääntöpohjaista kahden nettiyhteyden reititystä myöten.

Seuraavassa kuva laitteesta.

Kuva 3. Fortinet Fortigate 60

Hallinnassa näkyy se, että Fortinet on alusta alkaen suunniteltu umt-laitteeksi. Kokonaisuus on toimiva ja helppokäyttöinen, ei kuitenkaan ihan Sonicwallin tasoinen. Fortinetin hinnoittelu sopii hyvin utm-laitteelle. Hankintahinta on kohtuullinen, ja kaikki muu turva tulee yhdessä paketissa vertailun toiseksi edullisimpaan vuosihintaan. Vaikka hinta onkin edullinen, laite on suorituskykyinen ja kattava. Dmz-liittymien määrä on riittävä. Dmz Demilitarized zone. /4/,/17/

5.2.2 GTA GB-800

Global technology associates eli GTA on lähtöisin Floridasta. Yhtiö on tunnettu Gnat box –palomuureistaan. Laitteita on myyty kymmenisen vuotta. Yhtiön UTM-laite perustuu samaan palomuuri/VPN-yhdistelmään, johon on lisätty kokonaistietoturvan lisäosat, VPN Virtual private network.

Päivityspalvelut GTA toimittaa itse. Se on paketoinut lisäosat omiksi Sentinel-palveluikseen. Tekniikat ostetaan alan erikoisyhtiöiltä. Virustorjunta hankitaan Kasperskyltä, roskapostitorjunta Mailshelliltä ja sisällönsuojaus SurfControllilta. Virustorjunta rajoittuu vain sähköpostiin, ja hyökkäyksien eston toiminnot ovat vaatimattomammat.

Kuvassa 4 laitteesta.

Kuva 4. GTA GB-800

Käyttöönotto ja hallinta on hankalaa. WEB-hallinta on sekava ja vaikea. Ohjeita ei ole hyvin saatavilla. Pahimmillaan asetusten etsintä on arpapeliä. Laitteen suorituskyky palomuuritoiminnoissa on varsin hyvä. Täyden virustorjunnan puute poistaa suurimmat suorituskykyvaateet. GTA GB-800 on tehokas, mutta hallinnaltaan vaikea tietoturvalaite. Virustorjunta on vain sähköpostille. /12/,/17/

5.2.3 Juniper Netscreen-5GT

Netscreen on tunnettu suorituskykyisistä palomuureistaan. Sen osti muutama vuosi sitten reititinjätti Juniper. Laajentuminen UTM-yhdistelmälaitteisiin on

onnistunut mainiosti. Tekniikkaa on lisensoitu erikoistuntijoilta, esimerkiksi laitteen tuholaistorjunnasta huolehtii Trend micro. Ominaisuudet on saatu sovitettua hallintaan hyvin. Laitteen ylläpito on selkeää ja loogista. Ominaisuudet ovat myös kohtuullisen kattavat, erikoisesti palomuuri- ja hyökkäyksen estotoiminnoissa.

Kuvassa 5 laitteesta.

Kuva 5. Juniper Netscreen-5GT

Juniperin erikoisuus on laitteen viiden verkkoliitännän hallinta. Valikossa on seitsemän erilaista yhdistelmää sisäverkon, ulkoverkon ja Dmz-alueen portteja. Joissakin on otettu huomioon jopa sarjaportin tietoturva. Netscreenin perussuorituskyky on melko hyvä. Kun käyttöön otetaan kaikki tietoturvaominaisuudet, jää alkuperäisestä läpäisystä jäljelle 8 %:a. Juniperin hinnoittelu on melko edullinen vuosipalveluiden kokonaispaketin ansiosta. Juniper Netscreen-5GT on ominaisuuksiltaan tasapainoinen tietoturvalaite, erityisesti virustorjuntaa pidetään hyvänä. VPN-yhteyksien määrää pidetään suurena. /12/,/17/

5.2.4 Sonicwall Totalsecure 25

Vasta vuonna 2005 UMT-markkinoille tullut Sonicwall on nykyisin noussut jo markkinoiden kärkeen. Totalsecure-laite antaa tähän mahdollisuuden, sillä kyseessä on viimeistellyn ja ominaisuuksiltaan laadukkaantuntuinen tuote. Sonicwallissa on hyvää erityisesti toimiva hallinta. Käyttöönotto hoituu helpoimmillaan vain parissa minuutissa, esimerkiksi avustetoiminto neuvoo heti

esillä olevan kohdan ongelmien ratkaisemiseen. Ominaisuuksia laitteessa on paljon, niin tietoturvassa kuin verkko-ominaisuuksissakin. Myös raportointiin on muita parempia välineitä. Heikkoutena on suorituskyky. Sonicwall on pitkäaikaisessa käytössä vertailun edullisin.

Kuvassa 6 laitteesta.

Kuva 6. Sonicwall Totalsecure 25

Sonicwall Totalsecure 25 on monipuolinen ja laadukkaasti toteutettu UMT-laite, jossa hyviä puolia ovat ominaisuudet, hallinta ja käyttöönotto. Suorituskykyä on moitittu. /12/,/17/

5.2.5 Watchguard Firebox X500

Se että Watchguaed on joutunut kirimään UTM-laitteiden kehittelyssä, näkyy valitettavasti vielä tuotteen viimeistelyssä. UTM-laite perustuu Fireboxin perinteiseen palomuuri/VPN-yhdistelmään, jonka perusominaisuudet tässä käytössä ovat hyvät. Yhdistelmään on lisätty roskapostisuodatusta, hyökkäyksien torjuntaa ja sisällönsuodatusta. Virustorjunta koskee vain sähköpostiliikennettä, mikä vähentää laitteen käyttöarvoa.

Peruskäytössä suorituskyky on erinomainen, eikä siitä ilman täyttä virustorjuntaa voisikaan tulla ongelmaa. Valmistaja lupaa täyden virustorjunnan, samoin kuin esimerkiksi sääntöpohjaisen reitityksen laitteen seuraavaan versioon.

Kuvassa 7 laitteesta.

Kuva 7. Watchguard Firebox X500

Käyttäjät toivovat, että lisäyksien yhteydessä korjataan myös hallinnan ongelmia. Watchguardia ohjataan erillisestä hallintaohjelmasta, joka soveltyy hyvin palomuurisäätöihin. Tarkasteltaessa UTM-ominaisuuksia ei voi välttyä epäilykseltä, että lisäominaisuudet on vain kiireessä lisätty valikkoihin.

Korkeaa hankintahintaa selittää osin se, että Watchguardissa on mahdollisuus kasvattaa laite järeämmäksi vain lisenssiavaimen avulla. Tätä pidetään hyvänä ominaisuutena. Watchguard Firebox X500 vaikuttaa vielä hieman keskeneräiseltä, mutta suorituskyvyltään lupaavalta UTM-laitteelta. Vajaata virustorjuntaa pidetään puutteena. /15/,/17/

5.2.6 Zyxel Zywall 35 UTM

Zyxel on ratkaissut yhdistelmätietoturvan suorituskykyongelmat innovatiivisesti. Mallia on otettu Fortinetilta ja sen Fortiasic-kiihdytinpiiristä. Nykyisien Zywall-laitteiden lisäominaisuudeksi Zyxel on tuonut oman Secuasic-piirinsä. Se asennetaan alun perin langattomalle lisäkortille tarkoitettuun PC-card-paikkaan. Zyxelin laite on teholtaan hyvin vaatimaton, mutta UTM-toiminnoissa tulos on hyvä. Mittausten perusteella idea toimii. On syytä miettiä, kannattaako Zyxelin varaan rakentaa kovin laajassa mitassa VPN-tunneleita.

Zyxelin ominaisuudet ovat laajat ja hyvin toteutetut. Runsaasti toimintoja on vikasietoisuuteen, verkkoyhteyksien hallintaan ja tietoturvaan. Myös web-pohjainen hallinta on toteutettu hyvin.

Kuvassa 8 laitteesta.

Kuva 8. Zyxel Zywall 35 UTM

Eri tietoturvatoiminnot löytyvät loogisesti. Zyxel Zywall 35 UTM on tasaisen laadukas laite, jonka suorituskyvystä vastaa erillinen UTM-kortti. Edullinen hankintahinta miellyttää kuluttajia. /17/,/18/

Taulukko 2. Tietoturvalaitteiden hinnat ja asiantuntijoiden arviot.

Laite	Hinta	Arvosana
Fortinet Fortigate 60	1650 €	8,6
GTA GB-800	3412 €	6,9
Juniper Netscreen-5GT	1621 €	8,0
Sonicwall Totalsecure 25	1751 €	8,1
Watchguard Firebox x500	4175 €	7,6
Zyxel Zywall 35 UTM	1544 €	7,4

Taulukossa 2 olevat tiedot perustuvat Tietokonelehden asiantuntijoiden vertailun tuloksiin.

Laitteet ovat taulukossa selvityksen mukaisessa järjestyksessä. Tuottajien antamat hinnat ovat hyvin tarkkoja. Niistä puhuttaessa olisi ilmeisesti parempi käyttää sanaa hintaluokka. Todennäköisesti 1 €:n lisäys tai vähennys lopulliseen hintaan ei vaikuta ostopäätökseen. Testi on tehty maaliskuussa 2010.

Asiantuntijat ovat arvioineet ja verranneet laitteita sekä niiden käytettävyyttä ja antaneet kullekin laitekokonaisuudelle arvosanan. GTA GB-800 on saanut vertailussa arvosanaksi 6,9, ja kuitentin sen hinta on toiseksi korkein.

Tietoturvalaite Fortinet Fortigate 60 on saanut arvosanaksi 8,6. Hinta on muihin laitteisiin verrattuna melko kohtuullinen. Juniperin hintaa asiantuntijat pitävät edullisena, etenkin kun otetaan huomioon kaikki tietoturvaominaisuudet. /4/,/17/

5.2.7 Ostopäätökseen vaikuttavia tekijöitä

Vanha sanonta ”Asiakas on aina oikeassa” on myyntipiireissä otettu vakavasti. Ostajan mielipiteitä ja toivomuksia pyritään nuodattamaan tarkasti. Tietoturvalaitteita myytäessä voisi joskus sanoa leikkimielisesti ”Asiakas on aina väärässä”.

Usein ostaja tarkkailee vain hintaa ja toimintojen selkeyttä sekä helppokäyttöisyyttä. Laitteen laajennettavuus ja tietoturvaominaisuudet jäävät sivuseikoiksi. Myyjän on hyvä mainita kaupantekotilanteessa myös laitteen suorituskyvystä. Samoin on sopivaa kertoa, mitä virustorjunta kattaa.

Jos ostaja päättää valita laitteen, joka on hallinnaltaan toimiva ja käyttöönotoltaan nopea, valinta saattaa olla Sonicwall Totalsecure 25. Se on viimeistelty ja laadukkaasti toteutettu. Laitteessa on sekä tietoturvassa että verkkojärjestelyissä paljon hyviä ominaisuuksia. Asiakkaalle on kuitenkin hyvä kertoa suorituskyvyn heikkoudesta. Hinta kokonaisuuteen nähden on hyvin edullinen.

Joskus ostaja pitää tärkeänä sitä, että laite on ollut markkinoilla jo useita vuosia ja vakiinnuttanut paikkansa. GTA GB-800 on tunnettu Gnat box –palomuureistaan. Laitteita on ollut myynnissä yli kymmenen vuotta. Näin ollen laitteen suorituskyky palomuuritoiminnoissa on hyvä. Kyseinen tietoturvalaite on tehokas, mutta hallinnaltaan vaikea. Myyntitilanteessa on hyvä kertoa, että virustoiminta rajoittuu vain sähköpostiin. Ohjeita ei ole hyvin saatavilla.

Vaikka Zyxel Zywall 35 UTM on teholtaan hyvin vaatimaton, UTM-toiminnoissa tulos on hyvä. VPN-tunneleita ei ehkä kannata rakentaa Zyxelin varaan kovin laajassa mitassa. Ostajaa miellyttää edullinen hankintahinta ja laitteen laajat ja hyvin toteutetut ominaisuudet.

Watchguard Firebox x500:n suorituskyky peruskäytössä on erinomainen, vaikka hallinnassa onkin ongelmia. Hyvänä ominaisuutena pidetään sitä, että Watchgardissa on mahdollisuus kasvattaa laite järeämmäksi vain lisenssiavaimen avulla. Myyntitilanteessa pitäisi ehdottomasti kertoa, että virustorjunta on vain sähköpostiliikenteessä. Se vähentää laitteen käyttöarvoa. Asiantuntijoiden mielestä Watchguard Firebox x500 on hieman keskeneräinen.

Juniper Netscreen-5GT on tunnettu suorituskykyisistä palomuureistaan. Kun käyttöön otetaan kaikki tietoturvaominaisuudet, jää jäljelle alkuperäisestä läpäisystä vain 8 %:a. Myyjän on helppo suositella laitetta, varsinkin kun hinta on edullinen ja laitteen ylläpito selkeää ja loogista. VPN-yhteyksien määrää pidetään suurena.

Fortinet Fortigate 60 tuottaa tietoturvapalvelunsa itse. Laite on toimiva ja helppokäyttöinen. Tuote on asiantuntijoiden arvioinnissa paras. Edullinen hankintahinta vetoaa ostajiin. Laite on suorituskykyinen ja kattava. Dzm-liittymien määrä on suuri.

Jos asiakas kysyy myyjän suositusta, on hyvä kertoa erilaisista ominaisuuksista ja vertailla niitä keskenään. Yleensä tietysti kartoitetaan ostajan käyttötarpeet.

Sonicwall on asiantuntijoiden arvioinnissa toiseksi paras vertailtujen tuotteiden joukossa. Edullinen hankintahinta tietysti kiinnostaa asiakasta, jolle kannattaa mainita, että pitkäaikaisessa käytössä Sonicwall on vertailun edullisin.

6 TIETOTURVAN LAAJENTAMINEN

6.1 n-standardi

Aiempiin standardeihin, kuten IEEE 802.11a:han ja 801.11g:hen verrattuna n-laajennuksen tarkoituksena on parantaa WLAN:n suorituskykyä. Yhteensopivuustilassa nopeus on sama kuin vanhan standardin, mutta laajennus on yhteensopiva joko jommankumman tai molempien aiempien standardien kanssa.

802.11n määrittää suurimmaksi bruttonopeudeksi 600 Mbit/s. Todellisuudessa luvataan nopeutta noin 100 – 200 Mbit/s, jolloin nopeus olisi samaa luokkaa kuin perinteisellä Ethernet-kaapelilla, 100 Mbit/s. Samalla n-määritelmä tukee MIMO-tekniikkaa eli multiple-input, multiple output, jossa käytetään useampaa antennia ja useampaa ilmatien kanavaa samanaikaisesti. Uusi MIMO-tekniikka antaa tasaisemman kantaman ja mahdollistaa useat ilmakanavat. IEEE standardoi 802.11n:n syyskuun 11. päivänä 2009.

Kuluttajien näkökulmasta 802.11n parantaa eniten WLAN-verkkojen tiedonsiirto-nopeuksia ja luotettavuutta, kuten aiemmat 802.11-standardit. Suurin teoreettinen tiedonsiirtonopeus 802.11n-standardissa on 600 Mbit/s, ja käytännössä nopeudet ovat noin 100 Mbit/s. Tämä on aiempaan 802.11g-standardiin verrattuna selvä parannus. Siellä vastaavat luvut ovat 54 Mbit/s ja 20 Mbit/s.

Nettisurfailussa lisänopeus ei yleensä näy, nopeuslisästä on kuitenkin hyötyä erityisesti kotiverkoissa, joissa siirretään runsaasti dataa eri laitteiden välillä. Esimerkiksi Blu-ray-elokuvia voi jatkossa toistaa suoraan WLAN-verkon ylitse parempien nopeuksien myötä, eikä niitä tarvitse kopioida katselulaitteen kiintolevylle katselua varten.

Nykyisin markkinoilla on satoja 802.11n-yhteensopivia laitteita, koska laitevalmistajat ovat parin viimeisen vuoden aikana myyneet kuluttajille ns. Draft N -yhteesopivia laitteita. Näiden toteutukset perustuvat 802.11n:n silloiseen luonnostelmaan. Parin viime vuoden aikana varsinaiset muutokset 802.11n-standardiin ovat olleet vähäisiä. Näin monet kuluttajat voivat päivittää laitteensa 802.11n-yhteensopiviksi firmware-päivityksellä.

Laitevalmistajilta saadun tiedon mukaan lähes kaikki Draft N -yhteensopivat laitteet voidaan päivittää firmware-päivityksellä WLAN-laitteiden yhteensopivuutta mittaavan WI-FI Alliancen mukaan vastamaan lopullisen standardin vaatimuksia.

6.2 UTM-tietoturvalaitteet

Yhä vähemmän käytetään perinteistä palomuuria. Nykyisin yritysverkko suojataan monitoimisella UTM- eli unified treat management tietoturvalaitteella. Samassa laiteessa on virusten, hyökkäyksien ja roskapostin torjunta, etätyö, langaton verkko ja nettiselailun suodatus.

Aikaisemmin tietokoneelle ostettiin virustutka, joka etsi pelkästään viruksia. Nykyään on syytä hankkia laaja tietoturvaohjelmisto, jossa on toistakymmentä erilaista turvatoimintoa. Ennen käytössä ollut palomuuri sulki yritysverkon ulkopuolisilta ja avasi etätyöyhteydet. Nyt yritykset siirtyvät tietoturvan monitoimilaitteisiin, joista käytetään myös nimityksiä UTM.

Verkkoliikennettä tarkemmin tutkiva UTM-laite pyrkii poistamaan hyökkäykset, haittaohjelmat ja roskapostin jo ennen kuin ne pääsevät verkon koneille. Laitteella voi myös vähentää turhaa surffailua ja estää pääsyn asiattomille nettisivuille. Tutkijoiden arvioiden mukaan monitoimilaitteita myydään jo enemmän kuin perinteisiä palomuuri- ja etäkäyttölaitteita.

Useimmat palomuurivalmistajat innostuivat asiasta, kun UTM-laiteet ilmestyvät markkinoille vuoden 2004 tienoilla. Alkuaan UTM-laite oli kehitelmä, jossa palomuurin päälle oli lisätty virustorjuntaa ja muita turvaominaisuuksia. Laitteen teho ei riittänyt turvamoottorien käyttämiseen, ja laitteen käyttö oli monimutkaista.

Tässä työssä vertailuun on otettu seuraavat UTM-laitteet:

-Fortinet Fortiwifi – 80CM
- Sonicwall TZ 200
- Watchguard Firebox Edge X55e-W
- Zyxel Zywall UGS 100.

Mukaan on otettu laitteita, joissa on myös langaton lähiverkko. Pieni yritys voi tällaisella laitteella hoitaa periaatteessa kaikki lähiverkon, etätyön ja verkon tietoturvan tarpeet. Mukaan vertailuun saatiin utm-valmistajista tutut Fortinet, Sonicwall, Zyxel ja Watchguard. Ciscolls ja Check Pointilla olisi ollut myös tähän ryhmään sopivan kevyet tuotteet, mutta yhtiöt päättivät jäädä pois vertailusta. Yhtiöt eivät ehtineet saada viimeistä releasiaan valmiiksi ennen testiä. /3, 56-57/

6.3 Yhdistelmälaitteen säästöt ja kulut

Erikokoisissa yrityksissä on erilaisia syitä ostaa tietoturvan monitoimilaite. Suurissa yrityksissä tietoturva halutaan varmistaa, ja yhtiö on aiemmin hankkinut erillislaitteita, esimerkiksi hyökkäyksien ja virusten torjuntaan. UTM-laite on nyt entistä edullisempi ja yksinkertaisempi vaihtoehto. Enää ei tarvitse opetella eri valmistajien laitteita eikä niiden hallintatapoja. Yhdistelmälaite säästää ylläpidon kustannuksia. Lisäksi tilaa ja sähköä kuluu vähemmän.

Koska tehoa tarvitaan paljon, suurin ongelma on suorituskyvyn riittävyys. Suorituskyky on noussut nopeasti, ja turvatarkastuksiin pystytään nykyään jopa gigabittiluokan nopeuksilla.

UTM-laitteiden käyttö suuryrityksissä on kasvussa. Pienissä yrityksissä käytössä on ehkä jonkinlainen palomuuri. UTM-laite on palomuuria kalliimpi vaihtoehto, sillä turvaominaisuuksista täytyy maksaa vuosimaksuja. Kuluista huolimatta turvaominaisuuksista kannattaa maksaa, sillä UTM-laite puhdistaa suuren osan viruksista ja muista turvauhkista jo ennen kuin ne pääsevät tietokoneille. Ylimääräinen turvakerros parantaa kokonaissuojaa ja vähentää hälytyksiä käyttäjien koneilla. Jos tähän lisätään etäyhteyksien ja esimerkiksi 3G-varayhteyden mahdollisuus, on kokonaispaketti hyvä. Juuri pienet yritykset ovat innokkaimmin ostaneet UTM-laitteita .

Suurin syy UTM-laitteiden suosioon on ilmeisesti hintojen reipas lasku. Ostajan on hyvä tietää, että mukana on piilokustannuksia. Lähinnä palomuuritoiminnot sisältyvät itse laitteen hintaan. Muista turvatoiminnoista täytyy yleensä maksaa vuosihinta. Turvapalvelujen yhteispaketti eli bundle on niin edullinen, ettei muuta kannata harkita.

Uusia turva- ja verkkotekniikoita tulee jatkuvasti. Jotkut valmistajat käyttävät jo uutta termiä extended threat management eli xtm. Se viittaa ominaisuuksien laajentamiseen. Sovellusten valvonnalla voi estää esimerkiksi p2p-vertaisverkko-ohjelmien käytön. Työasemia voidaan valvoa myös nac- eli network access control-tekniikalla. Konetta ei päästetä verkkoon ennen päivitystä, jos siltä puuttuu esimerkiksi ajantasainen tietoturvaohjelma.

Salatun nettiliikenteen turvatarkastukset, esimerkiksi https ja tietokonehyökkäyksiä poistavat suojaukset ovat uutta alalla. Perinteisen IPsec-tekniikan rinnalle on tullut SSL –VPN -etäyhteyksissä. IPsec-yhteydet ovat tehokkaita, mutta ne vaativat oikein säädetyn asiakasohjelman. SSL –VPN -

yhteyden kautta yritysverkkoon pääsee vaikka lentokentän nettikioskista tai toiselta koneelta. /4/, /12/,/15/,/17/,/18/

6.4 Laitteiden vertailua

Suorituskyky on utm-laitteiden suurin haaste. Vertailun kaikkiin muihin laitteisiin kuuluu langattoman WLAN-verkon tukiasema. Tutkimuksen aikana huomattiin, että utm-laitteiden langattomat ominaisuudet ovat vaatimattomampia kuin WLAN-tukiasemien. Monipuolisin oli Sonicwall, joka valmistaa myös WLAN-tukiasemi.

Varsinkin virustorjunnassa UTM -laitteiden suorituskyky havaittiin puutteelliseksi. Käyttäjän on hyvä miettiä tehotarpeensa ja valita ostotilanteessa riittävän suorituskykyinen malli. Testeissä vain Zyxel pystyi ilmoittamaansa suorituskykyyn. Muut jäivät jälkeen. Sonicwallin tulos oli puolet luvatusta.

Suurin tuntematon tekijä on tietoturvan taso. On hyvä tietää, ettei UTM-laite ole tarkoitettu korvaamaan tietoturvaohjelmia, vaan täydentämään niitä. Nykyisin Fortinet ja Sonicwall tekevät kaikki turvatekniikat itse. Zyxelkin tarjoaa omaa virusturvaansa. UTM -laitteen mukana kannattaa ostaa samalla laitteen asennus ja säätäminen.

Useilla erilaisilla turvamoottoreilla avataan ja tarkastetaan melkein kaikki netti-liikenne. Viime vuosina laitteiden suorituskyky on parantunut. Se ei kuitenkaan riitä. Fortinet oli vertailun ylivoimainen ykkönen suorituskyvyssä. Sen tulos virustorjunnassa oli 35 Mbit/s. Se riittää nopeimmillekin ADSL -liittymille, mutta sadan megabitin valokuituyhteys vaatisi järeämpää mallia. Fortinetin suorituskyky etäkäytössä (IPsec-VPN) on vielä ylivoimaisempi.

Edullisemmat Zyxel ja Sonicwall pystyivät hyviin tuloksiin hintaansa nähden. Kun tehtäviin lisättiin etäkäyttö, Zyxelin tulos putosi puoleen. Watchguardilla oli

suuria ongelmia. Virustarkastuksiin se pystyi noin kolmen megabitin nopeudella. Etäkäyttö pudotti nopeuden megabittiin. Laitteesta ilmestyy lähiaikoina tehokkaampi versio.

Turva- ja verkko-ominaisuudet ovat melko samankaltaisia. Kaikki ovat asiallisella tasolla. Molemmilla alueilla Fortinet ja Sonicwall ovat muita edellä. Etäkäyttöominaisuuksissa otettiin huomioon IPsec-VPN ja sen asiakasohjelma sekä uudempi SSL –VPN -tekniikka. Toteutuksissa oli suuria eroja.

6.4.1 Fortinet Fortiwifi – 80CM

Fortinet-yhtiö loi tavallaan UTM-laitteiden luokan, ja se jatkaa edelläkävijänä. Yhtiö on keskittynyt salatun liikenteen puhdistamiseen ja tietokantoihin suunnattujen hyökkäysten poistoon. Fortinetillä on nac-ominaisuuksia, joilla voidaan estää puutteellisesti suojattujen koneiden pääsy verkkoon. VPN -ohjelmaan on liitetty palomuuri ja sama virusten ja hyökkäyksien torjunta kuin itse laitteeseen.

Hyvä suorituskyky perustuu yhtiön kehittämiin asic-piireihin. Laitteen nopeus oli vertailussa paras. Virrankulutus kertoi laitteiden suorituskyvystä. Fortinetin sähkölasku oli lähes kolminkertainen muihin nähden. Vertailussa laite oli kallein.

6.4.2 Sonicwall TZ 200

Sonicwall on yhdysvaltalainen utm-laitteiden valmistaja varsinkin pieniä yrityksiä varten. Vertailussa hallinta todettiin helpoimmaksi ja selkeimmäksi. Yritys valmistaa myös langattomia tukiasemia, toisin kuin muut vertailun kohteena olleet valmistajat. Sonicwallin langatonta verkkoa voi laajentaa Sonicpoint-tukiasemilla. Tällöin verkko muodostaa yhden kokonaisuuden. Vaikka suorituskyky tuotti pienen pettymyksen, sitä voidaan pitää riittävänä.

SSL –VPN -etäkäytössä on tarjolla vain yksi yhteys, ei WEB-sivuilla olevia palveluja. Kaikki turvaominaisuutensa Sonicwall tekee itse. Saatavana on myös Websensen-versio nettisuodatuksesta. Hintaa ja helppokäyttöisyyttä pidetään hyvinä, samoin WLAN-ominaisuuksia.

6.4.3 Zyxel Zywall UGS 100

Taiwanilainen Zyxel tekee monenlaisia kotien ja yritysten verkkolaitteita. Zywall-utm-laite jatkaa Zyxelin perinteitä. Laitteet ovat melko eleettömiä, mutta laadukkaita ja edullisia. Zywallin langaton verkko on toteutettu PC-card-paikkaan laitettavalla WLAN-kortilla.

Laitteessa ei ole erikoisuuksia, muttei myöskään heikkouksia. UTM-ominaisuudet ovat keskitasoa. Zyxelin suorituskyky on melko hyvä hintaan nähden. Virustorjunnan yritys tekee itse, mutta tarjoaa rinnalle Kasperskyn turvamoottoria. WEB-suodatus on ostettu Blue Coat –yrityseltä. WLAN-ominaisuudet ovat vertailun suppeimmat.

6.4.4 Watchguard Firebox Edge X55e-W

Seattlesta kotoisin oleva Watchguard on jättämässä UTM-nimityksen. Pian myyntiin televissa laitteissa käytetään termiä xtm eli extended treat management. Vertailussa vanhan sarjan laitteen suorituskyky nousi ongelmaksi. Uusille laitteille odotetaan 18-40 megabitin nopeuksia, mikä olisi hyvä parannus.

Sinänsä asiallisella tasolla olevat ominaisuudet ovat vertailun kevyemmästä päästä. Langattomassa verkossa käytetään vielä hitaampaa g-tekniikkaa. Muuten sen ominaisuudet ovat erinomaiset. Laitteen hallinta onnistuu erillisellä ohjelmalla

tai WEB-hallintaliittymällä. Monimutkainen ohjelma on osaavalle käyttäjälle näppärämpi. Hidas WEB-hallinta on asiallinen.

7 LOPPUPÄÄTELMÄT

Selvityksessä on esitelty ja vertailtu WLAN-kytkimiä, tietoturvalaitteita ja tietoturvan laajentamiseen tarvittavia uudempia laitteita. Kaupantekotilanteessa ostajalle on syytä kertoa erilaisista vaihtoehdoista ja myöhemmistä laajennusmahdollisuuksista.

Joskus käyttäjä saattaa pitää ”nippelitietona” verkon asentamiseen liittyviä yksityiskohtia. On kuitenkin esimerkkejä siitä, että jonkin yksityiskohdan laiminlyönti on tuonut kilpailijalle asiatonta hyötyä. Myyjän on kerrottava ostajalle kaikki mahdolliset uhkatekijät. Mahdollisimman suuren hyödyn saavuttamiseksi on hyvä tarkistaa käyttäjän jo olemassa oleva laitteisto ja miettiä siihen yhdistettäviä lisälaitteita ja –palveluja.

Yrityksen langattoman verkon tietoturvan suunnittelussa voidaan todeta, kuten aikaisemmin, ettei asiakas ole aina oikeassa. Selvityksen tekijänä uskallan väittää, että hyvällä tiedottamisella ja laitteiden vertailemisella saadaan jokaiselle ostajalle hänen tarpeisiinsa paras mahdollinen tietoturva.

Turhan usein asiakas kuitenkin vaihtaa ”munan munaan” taitavan myyntimiehen edessä. Kokonaisuutta ajatellen tulisi vanha infra ottaa huomioon ja järjestelmän skaalautuvuus juuri kyseiselle asiakkaalle huomioiden olisi tarkistettava, tulevaisuuden tarpeet. On vältettävä tekemästä niin sanottua pakkokauppaa ensimmäisen kaupan jälkeen, eli asiakas on pakotettu ostamaan lisää kytkimiä tai muuta sellaista perusinfraa. Tällöin budjetointi menettää merkityksensä eikä pysy kehyksissään. Ostovaiheessa myös niin sanottu ”right sizing” on hyvin tärkeää loistavan toimituksen ja tyytyväisen asiakkaan kannalta.

LÄHTEET

/1/ Aruba Networks Inc., 2009, EMEA HQ, Watford. (viitattu 24.3.2011) Available form Internet: www.arubanetworks.com.

/2/ Cisco Systems, (viitattu 24.3.20011) saatvilla Internetissä: www.cisco.com.

/3/ Data Leakage For Dummies, Sophos Special Edition. Publishing by Wiley Publishing, Inc., Indianapolis Indiana 2009.

/4/ Fortinet-palomuuri, (viitattu 25.3.2011) saatavilla Internetissä: www.fortinet.com.

/5/ HP Procurve Networking, (viitattu 24.3.2011) saatavana Internetissä: www.procurve.com.

/6/ Jaakonhuhta, Hannu (2003). IT-Ensyklopedia. 2. painos Helsinki. Edita.

/7/ Järvinen, Petteri (2002). Tietoturva & yksityisyys. 1. painos. Porvoo. Docendo Finlad Oy.

/8/ Järvinen, Petteri (2006). Paranna tietoturvaasi. 1. painos. Porvoo Docendo Finland Oy.

/9/ Kontio, Tervo, Jääskeläinen, Arokoski, Vierimaa, Raatikainen ja Köykkä (2002). 1. painos. Mobiiliteknologiat. Helsinki. Edita.

/10/ Nortel, (viitattu 24.3.2011) saatavana Internetissä: www.nortel.com.

/11/ Siemens, enterprise.usa.siemens.com, (viitattu 24.3.2011) saatavana Internetissä: www.siemens.fi.

/12/ Sonicwall TZ 200 -palomuuri, (viitattu 3.5.2011) saatavana Internetissä: http://www.tietokone.fi.

/13/ Stallings, William (2005). Wireless communications and Network. 2. ed. Cranbury, NJ 08512.

/14/ Symbol Technologies, (viitattu 24.3.2011) saatavana Internetissä: www.symbol.com.

/15/ Watchguard Firebox Edge X55e-W –palomuuri, (viitattu 3.5.2011) saatavana Internetissä: http://www.tietokone.fi.

/16/ www.tietokone.fi/lehti/tietokone_13_2006/

/17/ www.tietokone.fi/lehti/tietokone_4_2010/

/18/ Zyxel Zywall UGS 100 -palomuuri, (viitattu 3.5.2011) saatavana Internetissä: http://www.tietokone.fi.