Risto Kuoppala

Kameravalvonnan suunnittelu ja toteutus kiinteistöön

Opinnäytetyö

Kevät 2012

Tekniikan yksikkö

Tietojenkäsittelyn koulutusohjelma

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Koulutusohjelma: Tietojenkäsittelyn Koulutusohjelma

Suuntautumisvaihtoehto: Verkkoliiketoiminta

Tekijä: Risto Kuoppala

Työn nimi: Kameravalvonnan suunnittelu ja toteutus kiinteistöön

Ohjaaja: Markku Lahti

Vuosi: 2012 Sivumäärä: 42 Liitteiden lukumäärä: 2

Tässä opinnäytetyössä kerrotaan kameravalvonnan suunnittelusta kohdeyritykseen. Suunnitelmassa tuodaan esille analogisen ja digitaalisen kameravalvontajärjestelmän erot. Lisäksi tutustutaan myös erilaisiin tallentimiin, tallenninohjelmiin, valvontakameroihin ja tietoturvaan.

Suunnitelma tehtiin, koska haluttiin selvittää millainen kameravalvontajärjestelmä olisi paras vaihtoehto kohdeyritykseen, jossa ei ollut aikaisempaa valvontajärjestelmää. Kameravalvontajärjestelmälle asetettiin tavoitteita, jotka olivat helppokäyttöisyys, etäkäyttö, hälytykset ja helppo ylläpito.

Opinnäytetyössä tutustaan myös kameravalvontaa koskeviin lakeihin ja perehdytään niihin.

Opinnäytetyön lopussa asennetaan ja kokeillaan kohdeyritykselle suunniteltua kameravalvontajärjestelmää. Ohjelman toiminteita käydään myös läpi ja käsitellään mahdollisia ongelmia.

Avainsanat: Kameravalvonta, IP-kamera, Videotallennin, Tietoturva

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Business Information Technology

Specialisation: Electric Business Development

Author/s: Risto Kuoppala

Title of thesis: Planning and implementing a property camera surveillance system

Supervisor(s): Markku Lahti

Year: 2012 Number of pages: 42 Number of appendices: 2

The aim of this thesis was to plan camera surveillance for a target company. The differences between analog and digital camera surveillance systems are explained and different kinds of recorders, recording software, surveillance cameras and data security is also made familiar.

The target of the surveillance plan was to define what kind of camera surveillance system would be best for the target company which did not have previous surveillance system. Goals were set for the camera surveillance system which was easy of use including-, remote access, alarms and easy maintenance.

The laws concerning camera surveillance were also introduced and made familiar in this thesis. The planned camera surveillance system for the target company was installed and tested in the end of the thesis. Features of the surveillance system software and its possible problems were worked out.

Keywords: Camera surveillance, IP-camera, Video recorder, Data security

SISÄLTÖ

Kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

APACHE	Apache on avoimeen lähdekoodin perustuva HTTP-palvelinohjelma. (Netcam Watcher Professional.)
CAT	Category, parikaapelissa käytetty laatuluokittelu standardi. (Sallinen 2010,72.)
CCD	Charge-Coupled Device, valoherkkä kenno, jota käytetään erilaisissa kameroissa. (Sallinen 2010,72.)
CMOS	Complementary Metal Oxide Semiconductor, kenno, jota käytetään erilaisissa kameroissa. (Sallinen 2010,72.)
DMZ	Demilitarized Zone, fyysinen tai looginen aliverkko. Tavallisesti internetin ja lähiverkon välissä oleva vyöhyke. (Sisäverkko-ohje 2010,25.)
DVR	Digital Video Recorder, digitaalinen videonauhuri, kuvamateriaali tallennettaan yleensä kiintolevylle. (Sallinen 2010,22.)
DVR-HYBRID	Digital Video Record-Hybrid, digitaalinen videonauhri, johon voidaan liittää analogsia ja digitaalisia kameroita. (Sallinen 2010,25.)
ETHERNET	Pakettipohjainen lähiverkko, yleisin lähiverkkotekniikka. (Sallinen 2010,72.)
FFMPEG	Kokoelma vapaita ohjelmistoja, joilla voi kääntää, tallentaa ja suoralähettää digitaalista ääntä ja videota. (Netcam Watcher Professional.)

IP Internet Protocol, protokolla, jota käytetään internetissä tiedonsiirtoon. Jokaisella lähiverkossa olevalla koneella on oma IP-osoite. (Sallinen 2010,72.)

MAC Media Access Control, verkkosovittimen ethernet verkossa yksilöivä osoite. (Sisäverkko-ohje 2010, 66.)

NODECT Zoneminder-ohjelmassa: liikkeen loppuessa tallennus käynnistyy. (Netcam Watcher Professional.)

MOCORD Zoneminder-ohjelmassa: jatkuva tallennus, liiketunnistukset listataan omana tiedostona. (Netcam Watcher Professional.)

MODECT Zoneminder-ohjelmassa: liikkeen loppuessa tallennus käynnistyy. (Netcam Watcher Professional.)

MONITOR Zoneminder-ohjelmassa: tarkkailutila, Ei tallennusta/liikkeentunnistusta käytössä. (Netcam Watcher Professional.)

MYSQL Relaatiotietokantaohjelmisto.

NTSC National Television System Committee, analoginen televisojärjestelmä Tyynen valtameren ympärysmaissa.

NVR Network Video Recorder, verkkotallennin jolla voidaan nauhoittaa IP-kameroiden digitaalista videokuvaa. (Sallinen 2010,72.)

PAL Phase Alternate Line, analoginen televisiojärjestelmä. Käytössä Euroopassa, Australiassa ja joissain Aasian, Afrikan ja Etelä-Amerikan maissa. (Sallinen 2010,20.)

PHP Hypertext Preprocessor, ohjelmointikieli, jota käytetään erityisesti web-palvelinympäristöissä.

POE Power over Ethernet, tekniikka jonka avulla voidaan syöttää käyttöjännite parikaapelissa. (IP-videovalvonta: vaatimukset, käyttöönotto, toiminta ja tulevaisuus 2010.)

PTZ Pan/Tilt/Zoom, liikulteltavasta ja tarkentavasta valvontakamerasta käytetty lyhenne. (Sallinen 2010,18.)

RECORD Zoneminder-ohjelmassa: jatkuva tallennus. (Netcam Watcher Professional.)

RESOLUUTIO Resoluutio on termi, jolla kuvankäsittelyssä ja tietotekniikassa tarkoitetaan kuvan erotuskykyä eli yksityiskohtien määrää. (Sallinen 2010,72.)

UPS Uninterruptible Power Supply, virransyöttöjärjestelmä, jolla voidaan taata tasainen virransyöttö sähkökatkojen ja sähköpiikkien aikana. (Sisäverkko-ohje 2010, 59.)

VLAN Virtual Lan, tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin. (Sisäverkko-ohje 2010, 19.)

WEB World Wide Web Internet-verkossa toimiva hypertekstijärjestelmä.

WLAN Wireless Local Area Network, langaton lähiverkko (Sallinen 2010,29.)

3G 3rd Generation, kolmannen sukupolven matkapuhelintekniikkaa, jonka avulla voidaan siirtää langattomassa tietoverkossa nopeasti kuvaa ja ääntä. (Sallinen 2010,20.)

802.1.X Port Based Authentication, Porttikohtaisen todentamisen standardi. Käytetään lähiverkoissa. (Sisäverkko-ohje 2010, 61.)

1 JOHDANTO

1.1 Työn tausta

Kameravalvontajärjestelmien yleistyminen alkoi 1980-luvun alkupuolella, jolloin markkinoille saapuivat CCD-kennolla varustetut mustavalkokamerat. Alussa kameroilla valvottiin pääasiassa suuren teollisuuden monimutkaisia prosesseja, esimerkiksi paperiteollisuus. (Kaikkonen 2007) Valvonnassa ei tuolloin tallennettu tietoa, vaan monitorien avulla lähinnä tarkkailtiin prosessien kulkua. Tämän jälkeen valvonta on lisääntynyt yksityis- ja viranomaiskäytössä.

Kameravalvontajärjestelmät ovat pitkään perustuneet analogiseen tekniikkaan, joka on asettanut niille erilaisia rajoituksia. Nykyaikainen digitaalinen kameravalvonta on kuitenkin mahdollistanut mm. kuvainformaation keskitetyn tallennuksen ja etävalvonnan.

Kohdeyritys on Seinäjoella sijaitseva maatalouskauppa, jonka liikepaikka sijaitsee vilkkaasti liikennöidyn tien varrella. Yrityksellä on pihamaalla paljon myynnissä olevaa kalustoa. Tätä aluetta olisi tarkoitus valvoa kameravalvonnalla. Ajatuksena on, että kameravalvonta toimisi pelotteena ja myös helpottaisi mahdollisen rikoksen selvittämistä jälkeenpäin. Yrityksellä ei ole tällä hetkellä käytössä minkäänlaista valvontaa. Liike-aluetta on aikaisemmin suunniteltu aidattavaksi, mutta sen katsottiin aiheuttavan tarpeetonta haittaa asiakkaille ja myös liiketoiminnalle.

1.2 Työn tavoite

Tarkoituksena on laatia suunnitelma kameravalvonnan käyttöönotosta tälle yritykselle. Siinä selvitetään paras mahdollinen kokonaisratkaisu yrityksen ja käyttäjien tarpeet huomioon ottaen. Järjestelmältä toivottavia ominaisuuksia ovat helppokäyttöisyys, etävalvonta, hälytykset ja järjestelmän helppo ylläpito. Tässä työssä käydään läpi myös lakiasiat, erilaiset kameravalvontatekniikat ja järjestelmään liittyvät tietoturva-asiat.

Opinnäytetyössä selvitetään, miten IP-valvontakamerat ja kameravalvontaohjelmistot palvelevat yrityksen tarpeita. Riittääkö pelkkä kameravalvonta yrityksen valvontaan?

2 KAMERAVALVONTA

2.1 Kameravalvonnan yleistyminen

Kameravalvonta lisääntyy jatkuvasti yleisillä paikoilla. Yhdeksänkymmentäluvulta lähtien kasvu on ollut nopeaa. Kasvua on ollut 10 - 15 prosenttia vuodessa kertoo Falck Securityn Timo Nordgren. Esimerkiksi Järvenpää, Imatra, Lappeenranta, Oulu ja Helsinki ovat rakentaneet kameravalvontaverkostoa viime vuosina. Kameravalvonnan lisääntymiseen on syynä laitteiden hintatason alentuminen, kaupunkien halu lisätä asukkaiden turvallisuutta ja tekninen kehitys, joka mahdollistaa hyvän kuvalaadun. (Julkisten tilojen kameravalvonta lisääntyy Suomessa 2006.)

Arvioidaan että Suomi kuuluu maailman kärkimaihin kameravalvonnassa. Yleisillä paikoilla yksityinen kuvaaminen on lisääntynyt ja se on myös herättänyt keskustelua asiasta. (Koskinen 2001.) Tutkimukset ovat kuitenkin osoittaneet, että kameravalvonta voi vähentää omaisuusrikoksien ja vahingontekojen määrä. Väkivaltarikollisuuteen sillä ei kuitenkaan näytä olevan ennaltaehkäisevää vaikutusta. (Kivivuori 2005.)

2.2 Valvontaan vaikuttavat lait

Kameravalvonta on laissa huomioitu ensimmäisen kerran vuonna 2004, kun laki yksityisyyden suojasta astui voimaan. Laissa määritellään kameravalvonta jatkuvasti kuvaa välittäväksi tai kuvaa tallentavaksi menetelmäksi. (L 13.8.2004/759.)

Kameravalvontaa varten ei ole olemassa yksittäistä sitä säätelevää lakia. Kameravalvonnan laillisuuteen vaikuttavia keskeisiä tekijöitä ovat: kuka kameravalvontaa suorittaa, missä henkilöä valvotaan ja myös se onko kyseessä pelkkä valvonta vai tallennetaanko samalla tapahtumat. Tällä hetkellä kameravalvontaa säätelee kolme eri lakia, näitä ovat: Henkilötietolaki (1999/523), Rikoslaki (1889/39) ja laki yksityisyyden suojasta työelämässä (2004/759). Seuraavissa luvuissa tuodaan esille keskeisimmät kohdat näistä kolmesta laista, koskien kameravalvontaa. (Koskinen 2001.)

2.2.1 Henkilötietolaki

Kameravalvonnassa tallennettu kuva ja ääni ovat henkilötietoja, jos henkilö on niistä tunnistettavissa. Tallenteiden säilytysajalla ei ole merkitystä siihen, voidaanko henkilötietolakia soveltaa. Kameravalvonnan omistaja on automaattisesti henkilötietolaissa tarkoitettu rekisterinpitäjä. Henkilötietolakia ei sovelleta silloin, kun kamerat ovat ainoastaan katselua varten. (Onko kameravalvonta henkilötietojen käsittelyä, [viitattu 31.1.2012.])

Tallentava kameravalvonta on henkilötietojen tallentamista. Tällöin täytyy olla asianmukainen perustelu kuvaamiselle. Tällaisia syitä voivat olla esimerkiksi rikollisuuden torjunta ja järjestyksen, sekä turvallisuuden ylläpito. (L 22.4.1999/523.)

Henkilötietolain 5 § velvoittaa, että kameravalvonnan omistaja eli rekisterinpitäjä käsittelee tallennettua materiaalia laillisesti ja pitää huolen siitä, ettei yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman perusteita. Tällä tarkoitetaan sitä, että materiaalia ei saa käyttää muuhun, kuin mihin laki antaa luvan. (L 22.4.1999/523.)

Henkilötietolain 8 § tarkoittaa kameravalvonnassa sitä, että tallenteita ei saa käsitellä ilman asianomistajan lupaa tai oikeudellista perustetta. Esimerkiksi rikos täyttää oikeudelliset vaatimukset niin, että tallennettu kuvamateriaali voidaan luovuttaa viranomaiselle. (L 22.4.1999/523.)

Henkilötietolain 24 § velvoittaa kameravalvontajärjestelmän omistajan luovuttamaan kuvatulle henkilölle tiedon siitä mihin kerättyä aineistoa käytetään ja kuka tietoja kerää. Lisäksi 26 § määrää käytännössä, että kameravalvonnasta on aina ilmoitettava asianomistajille. (L 22.4.1999/523.)

Henkilötietolain 32 § mukaan kameravalvonnan omistajan on huolehdittava siitä, että tietoja säilytetään asianmukaisella tavalla. Lisäksi 34 § edellyttää, että tallenteet on hävitettävä, jos ne eivät ole enää tarpeellisia. (L 22.4.1999/523.)

Henkilötietolain 33 § pykälän mukaan henkilötietojen käsittelyn (kameravalvonnan) suorittamiseen yhteydessä saadut tiedot esimerkiksi henkilön ominaisuudet, henki-

lökohtaiset olot tai taloudellista asemaa koskevia tietoja ei saa lainvastaisesti luovuttaa sivulliselle. (L 22.4.1999/523.)

2.2.2 Rikoslaki

Rikoslaissa on säädetty 6 § mukaan rangaistavaksi teoksi salakatselu tai kuvaaminen teknisen laitteen avulla kotirauhan alueella. Kotirauhan piiriin luetaan esimerkiksi kesämökki, hotellihuone, asuntovaunu ja auto. Salakatseluun ei vaikuta se missä tekninen välinen sijaitsee. Riittää, että salakatselu on tapahtunut. Myös salakatselun yritys on rangaistava teko. (L 9.6.2000/531.)

Yleisölle avoimissa paikoissa kuvaaminen on sallittua. Kuvaa ei saa kuitenkaan julkaista sellaisessa yhteydessä, jossa se loukkaa kuvattavan yksityisyyttä. (L 9.6.2000/531.) Nykyään monet kauppakeskukset kieltävät kuvaamiseen. Kielto ei tällöin perustu lakiin, vaan on lähinnä kehotus. (Julkisella paikalla saa kuvata 2008.)

2.2.3 Laki yksityisen suojasta työelämässä

Yksityisyyden suojasta työelämässä on säädetty lain 16 § kohdalla seuraavasti: Työnantaja saa kuvata ja tallentaa kameravalvonnalla tilojaan, jossa on työntekijöitä tai muita henkilöitä. Tämä perustuu siihen, että työantaja saa lain mukaan valvoa omaisuuttaan, tuotantoprosessin kulkua ja työntekijöidensä turvallisuutta työpaikalla. Työantaja ei saa kuitenkaan kohdistaa valvontaansa tiettyyn työntekijään tai tietyn ryhmän tarkkailuun työpaikalla. Työnantaja ei voi valvoa myöskään mm. työntekijän omaa työhuonetta, käymälöitä ja henkilöstön tiloja. (L 13.8.2004/759.)

Työantaja voi kuitenkin 1 momentin nojalla valvoa tiettyä työpistettä, jos valvonta on välttämätöntä (L 13.8.2004/759). Esimerkkejä valvonnasta ovat:

- Työhön liittyvä väkivallan uhka, turvallisuuden tai terveydellisen haitan ennaltaehkäisy.

- Omaisuusrikosten ehkäisyyn, jossa työntekijä on keskeisessä osassa. Työntekijä käsittelee rahaa tai muuta arvokasta omaisuutta.

- Varmistetaan työntekijän edut ja oikeudet. Tällöin lupa perustuu työantajan ja työntekijän väliseen sopimukseen.

Työpaikalla tapahtuvaa kameravalvontaa koskevat samat säädökset, kuin muitakin tiloja valvottaessa. Esimerkiksi 17 § edellyttää, että kameravalvonnasta on ilmoitettava näkyvästi niissä tiloissa, joihin se on asennettu. Työntekijän yksityisyyteen ei pidä puuttua enempää kuin mitä tarve vaatii ja kameravalvontatallenteet on hävitettävä heti, kun niitä ei katsota tarpeelliseksi. Kameravalvonnasta vastaa aina sen omistaja tai sen ylläpitäjä. (L 13.8.2004/759.)

3 KAMERAVALVONTATEKNIIKAT

3.1 Valvontakameroiden perusrakenne

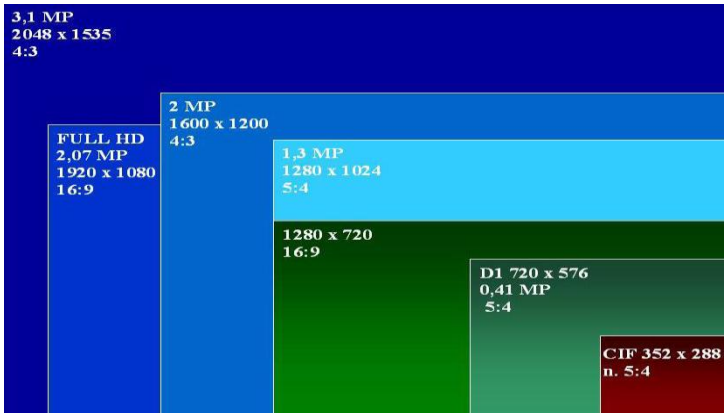
Valvontakameroita on saatavilla moneen eri käyttötarkoitukseen. Kameran perusrakenteeseen kuuluu runko, optiikka, virtalähde ja jalusta. Kameraan on myös saatavilla erilaisia lisävarusteita, joilla se voidaan suojata esimerkiksi pölyä, likaa, sää-tä ja ilkivaltaa vastaan. (Sallinen 2010,17.)

3.2 Valvontakameroiden tekniikka

Valvontakameroita on olemassa analogisia ja digitaalisia. Analogisen ja digitaalisen kameran eroja ovat erilainen kuvansiirtotekniikka ja erilainen kuvakenno.

Analoginen kamera käyttää CCD-kuvakennoa, joka siirtää suoraan kennolle tulevan valon sähköisenä signaalina eteenpäin esimerkiksi tallentimelle. Analogisen järjestelmän tarkkuus eli resoluutio on maksimissaan 720x576 tai 720x480. (Sallinen 2010,20.)

Digitaalisessa kamerassa eli IP-kamerassa valo tulee CMOS-kennolle, jonka jälkeen kuvavirta pakataan ja sitten lähetetään digitaalisena bittivirtana esimerkiksi tietoverkossa olevalle tallentimelle. Digitaalisen kuvansiirron etuna on kuvan häviämättömyys eli kuvanlaatu ei heikkene sitä siirrettäessä. Lisäksi CMOS-kuvakennon resoluutio voi olla erittäin suuri. Kennot kehittyvät jatkuvasti. (Sallinen 2010,20-21.) Kuviossa 1 havainnollistetaan resoluution vaikutus kuvan kokoon.



Kuvio 1. Resoluution vaikutus kuvan kokoon (Sallinen 2010,21)

CCD-kuvakennon etu CMOS-kuvakennoon on sen hyvä valoherkkyys ja värikylläisyys. Suurin haitta on kuitenkin sen suuri virrankulutus ja korkeammat valmistuskustannukset verrattuna CMOS-kennoon. Molemmilla kennoilla voidaan saavuttaa hyvä resoluutio, mutta analogisen järjestelmän tapa siirtää kuvaa eteenpäin kamerasta perustuu vanhoihin standardisoituihin televisiopohjaisiin järjestelmiin. Tällaisia järjestelmiä ovat PAL ja NTSC, joiden tarkkuus voi olla maksimissaan 720x480 (NTSC) ja 720x576 (PAL). (Sallinen 2010,11.) Digitaalisessa järjestelmässä tällaista rajoitusta ei ole.

3.2.1 Yökuvaus

Valvontakameroiden käyttö ympärivuorokautisessa valvonnassa vaatii kameroilta hyvää valoherkkyyttä. Valoherkkä kamerakaan ei riitä silloin, kun valon määrä laskee erittäin alhaiseksi. Yökuvaukseen on saatavilla kameroita, joilla voidaan kuvata myös täysin pimeässä. Kamerat käyttävät apuna ihmissilmälle näkymätöntä infrapunavaloa. Kamera valaisee kuvattavan kohteen infrapunavalolla. Kohteesta heijastuu takaisin valoa, jonka infrapuna-anturilla varustettu kamera tulkitsee kuvaksi. (What are infrared surveillance cameras used for, [viitattu 25.1.2012.]) Kuviossa 2 on infrapunaledeillä varustettu kamera.

Kuvio 2. Valvontakamera RL-2040H (Tuotteet Kameravalvonta, [viitattu 25.1.2012].)

3.2.2 Analogisen valvontakameran kaapelointi

Perinteinen analoginen valvontakamera käyttää tavallisesti koaksaalikaapelia, koska sillä saavutetaan yleensä riittävän pitkä siirtoyhteys ilman vahvistimia. Analogista signaalia voidaan myös tarvittaessa siirtää apulaitteilla valokuidussa tai parikaapelissa. (Aalto 2009,41.) Kuviossa 3 on koaksaalikaapeli BNC-liittimillä.

Kuvio 3. Koaksaalikaapeli Bnc-liittimillä (Vimdata Tuotteet, [viitattu 25.1.2012].)

Yleensä analoginen kamera vaatii kaksi erillistä kaapelia toimiakseen. Ensimmäinen kaapeli syöttää tarvittavan sähkön kameralle ja toinen kaapeli siirtää videosignaalin eteenpäin kamerasta. Lisäksi analogisen kameran mahdolliset lisäominaisuudet, esimerkiksi PTZ-toiminto eli liikuteltavuus, vaativat oman johdotuksen. (IP-videovalvonta: vaatimukset, käyttöönotto, toiminta ja tulevaisuus 2010.)

3.2.3 Digitaalisen valvontakameran kaapelointi

Digitaalinen IP-valvontakamera käyttää standardisoitua EN50173:n mukaista yleiskaapelointia. Yleiskaapeloinnissa käytetään parikaapelia. Parikaapeli luokitellaan laadun mukaan eri kaapeliluokkiin, jolloin puhutaan yleensä eri CAT-luokista. Parikaapeloinnissa voidaan hyödyntää Power over Ethernet -tekniikkaa eli PoE:ta, jossa voidaan siirtää samassa kaapelissa sähköä ja dataa. (Aalto 2009,41.)

IP-kameran kaapelointi voidaan toteuttaa yhdellä johdolla, mikäli kamera tukee PoE-virransyöttöä. PoE-virransyötössä kameran tarvitsema sähkö siirretään parikaapelointia pitkin, jossa on mahdollista siirtää sähköä ja dataa yhtäaikaisesti. PoE-kameroita varten täytyy olla Ethernet-kytkin, jossa on tuki virransyötölle. (IP-videovalvonta: vaatimukset, käyttöönotto, toiminta ja tulevaisuus 2010.) Kuviossa 4 on parikaapeli, jossa on RJ-45-liittimet.

Kuvio 4. Parikaapeli RJ-45 liittimellä (Ipcmax Tuotteet, [viitattu 26.1.2012].)

Sähkön ja virran syöttö samassa kaapelissa tuo merkittävän edun, sillä kameran virtalähde voidaan sijoittaa jopa 100 metrin päähän itse laitteesta. Tällöin kameroiden yhteisestä virransyötöstä voidaan huolehtia keskitetysti siihen tarkoitetulla varavoimalaitteella eli UPS:lla. UPS-laite huolehtii siitä, että videovalvonta on jatkuvaa, jopa sähkökatkosten aikana. (Network Camera Considerations 2012.)

3.2.4 Power Over Ethernet

PoE on tekniikka, jonka avulla voidaan syöttää päätelaitteiden tarvitsema käyttöjännite parikaapelissa. Käyttökohteita voivat olla esimerkiksi IP-valvontakamerat, IP-puhelimet ja WLAN-tukiasemat. Järjestelmä vaatii toimiakseen PoE-kytkimen tai erillisen PoE-sovittimen, joka syöttää jännitteen kaapeliin. (Lisää virtaa verkosta 2009.)

Ensimmäinen standardi PoE-virransyötölle oli 802.3af, joka määritteli virrankulutuksen neljään eri luokkaan. Ykkösluokkaan kuului laitteet, jotka saivat kuluttaa enintään 3,84 wattia. Viimeisessä luokassa tehonkulutus sai olla jopa 12,95 wattia.

802.3af-standardin sähkönkulutuksen yläraja tuli kuitenkin nopeasti vastaan, kun päätelaitevalmistajat toivat markkinoille yhä enemmän sähköä kuluttavia laitteita, kuten usealla radiolla varustetut WLAN-tukiasemat, värinäytölliset IP-videopuhelimet ja liikuteltavat videokamerat. Virrankulutuksen yhä kasvaessa julkaistiin uusi 802.3at-standardi, jossa päätelaitteiden teho voi olla melkein kaksinkertainen eli 25,5 wattia. (Lisää virtaa verkosta 2009.)

3.2.5 Langattomat valvontakamerat

Analogisia ja digitaalisia valvontakameroita on saatavana myös langattomina. Analogista videota voidaan siirtää langattomasti mikroaaltolinkin tai infrapunalinkin avulla. Mikroaaltolinkin kantomatka voi vaihdella 500 metristä aina 60 kilometriin saakka. Linkin pituuteen vaikuttaa pääasiassa siinä käytettävä taajuus. Esimerkiksi alle 10 Ghz:n taajuuksilla voi päästä 60 kilometriin. Suuremmilla taajuuksilla linkin kantomatka jää 500 metriin. Lisäksi jokaisen radiolinkin lähetykseen tarvitaan lupa viestintävirastolta. Infrapunalinkin kautta tapahtuva siirto ei ole luvanvaraista. Sillä voidaan saavuttaa jopa 500 metrin siirtomatka. Infrapunalinkin haittapuoli on, että sen käyttö edellyttää laitteilta näköyhteyttä. (Aalto 2009, 48-49).

Analogisessa järjestelmässä mikroaaltolinkin ja infrapunalinkin käytön suurin ongelma on, että tieto kulkee salaamattomana. Lisäksi niitä on myös mahdollisuus häiritä. (Sallinen 2010,29.)

Digitaaliset langattomat valvontakamerat käyttävät verkkopohjaista tiedonsiirtoa. Verkkopohjainen tiedonsiirto perustuu standardisoituun TCP/IP-protokollaan, joka on käytössä yleisesti koti- ja yritysverkoissa. Tällaisia valvontakameroita on saatavilla WLAN- ja 3G-tuella. (Aalto 2009, 59,61.)

WLAN perustuu standardisoituun 802.11 tekniikkaan. WLAN on paikallinen, yleensä kiinteän lähiverkon tukena oleva langaton yhteys. WLAN-verkon vahvuus on hyvä salaus ja nopeus. WLAN-verkon kantama voi olla hyvissä olosuhteissa jopa 100 metriä. (Aalto 2009, 11-12.)

3G-tekniikkaa käytetään matkapuhelinverkoissa ja se on kehitetty erityisesti nopeaa tiedonsiirtoa varten, koska matkapuhelinverkossa oleva dataliikenne kasvaa jatkuvasti (Granlund 2007, 417).

3.3 Erilaiset valvontakamerat

Kamera valitaan kohteeseen sen ominaisuuksien perusteella. Valintaan vaikuttavat ympäristön eri tekijät, joita voivat olla mm. valaistus, lämpötila ja pöly. Erilaisia olosuhteita ja käyttötarkoitusta varten valvontakamerat on jaettu seitsemään eri ryhmään. Seuraavissa luvuissa käydään jokainen ryhmä läpi (Sallinen 2010,17.)

Kiinteä sisäkamera. Kiinteä sisäkamera kuvaa aina samaa aluetta. Kamerassa on yleensä kiinteä tai vaihdettava objektiivi. Nykykameroissa on usein myös säädettävä objektiivi, jonka polttoväliä on mahdollista muuttaa tarvittavan kuva-alan saamiseksi. (Sallinen 2010,17.)

Kiinteä ulkokamera. Kiinteä ulkokamera eroaa sisäkamerasta oleellisesti sen koteloinnin osalta. Kamera on varustettu säänkestävällä koteloinnilla, joka on lämmitetty. Lämmitys ja tiivis kotelointi suojaa kameran tekniikkaa ulkoilmassa. (Sallinen 2010,17.)

Kiinteä kupukamera. Kiinteä kupukamera on pakattu nimensä mukaisesti kuvun sisälle. Kamera on huomaamattomampi kuin normaali sisä- tai ulkokamera. Kiinteää kupukameraa on saatavilla ulko- ja sisäkäyttöön. Kameraa on saatavilla myös vandaalisuojatulla kuvulla. (Sallinen 2010,18.)

PTZ-kamera. PTZ-kamera on kiinteä ulkokäyttöön suunniteltu säänkestävä valvontakamera. Siinä on moottoroitu kääntöpää, jolla saadaan 360 asteen kuva-ala kameraa kääntämällä. Kameralla valvotaan tavallisesti suuria ulko-alueita. (Sallinen 2010,18.)

Kupukamera. Kupukamera on tavallisen kiinteän kupukameran kaltainen valvontakamera, mutta se eroaa siitä moottoroidulla objektiivilla, jota voidaan kääntää haluttuun suuntaan. Lisäksi objektiivissa on moottoroitu zoom-toiminto, jolla voidaan tarkentaa kaukanakin olevaan kohteeseen. (Sallinen 2010,18.)

Megapikselikamera. Megapikselikamera on IP-kamera, joka on varustettu CMOS-kennolla. Kamera voi olla erityisen tarkka, koska sen kuvakennossa voi olla miljoonia kuvapisteitä eli megapikseleitä. Megapikselikameraa käytettäessä on otettava huomioon valaistus, sillä kamerassa oleva CMOS-kenno ei ole yhtä valoherkkä kuin perinteinen CCD-kenno. (Sallinen 2010,19.)

Harvinaiset kameratyypit. Harvinaisia kameratyyppejä ovat erilaiset erikoiskamerat, jotka on suunniteltu erityiskäyttöön. Tällaisia kameroita ovat:

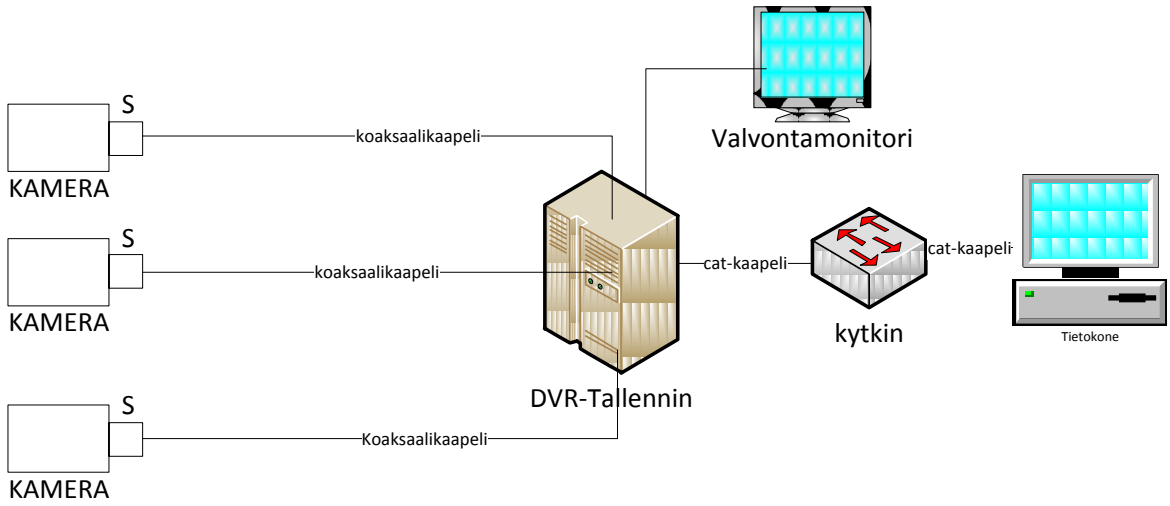
- EX-kamera eli räjähdysherkkien tilojen kamera
- vakoilukamera eli kamera, joka on naamioitu
- EMP-kamera eli kamera, joka on suojattu elektromagneettista säteilyä vastaan. (Sallinen 2010,19.)

3.4 Tallentimet

Tallentimia on olemassa kolmea eri luokkaa. Niiden perustoiminta ei ole muuttunut vuosien varrella, mutta tekninen kehitys on tuonut niille uusia vaatimuksia. Kehityksen kulussa ei yleensä voida siirtyä suoraan vanhasta tekniikasta uuteen, vaan on oltava sellaisia laitteita, joiden avulla siirtyminen voi tapahtua asteittain. Tallenninratkaisuja ovat DVR (Digital Video Recorder), NVR (Network Video Recorder) ja Hybrid DVR (Hybrid Digital Video Recorder). (Sallinen 2010,22.)

3.4.1 DVR-tallennin

DVR-tallentimeen voidaan liittää vain analogisia kameroita. Jokainen kamera on liitetty tallentimeen omalla koaksaalikaapelilla. Analogisen kameran kuva tuodaan tallentimelle, jossa se digitalisoidaan ja pakataan. Tämän jälkeen kuvainformaatio tallennetaan kiintolevylle. DVR-tallentimessa on katselua varten monitori ja myös mahdollisesti verkkokortti, jonka avulla tallennin voidaan liittää esim. yrityksen lähiverkkoon. (Sallinen 2010,22.) Kuviossa 5 jokainen kamera on liitetty omalla kaapelilla tallentimeen.

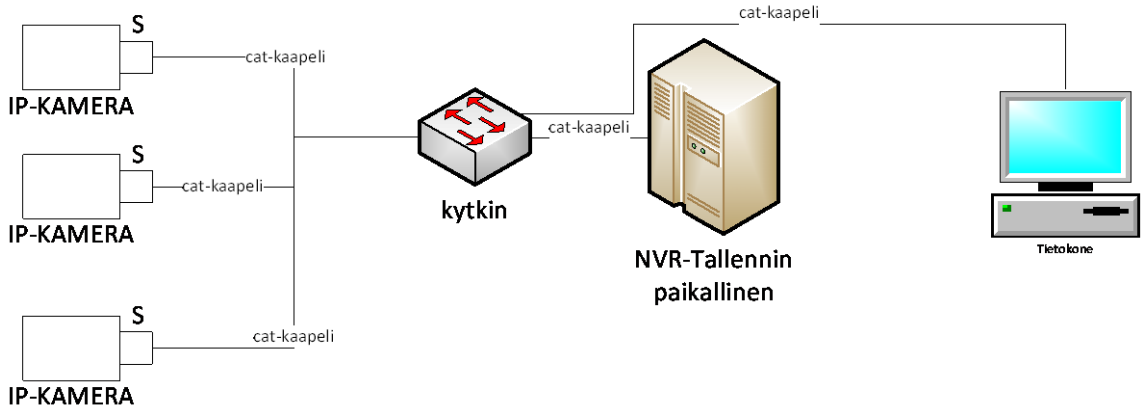


Kuvio 5. DVR-tallennin

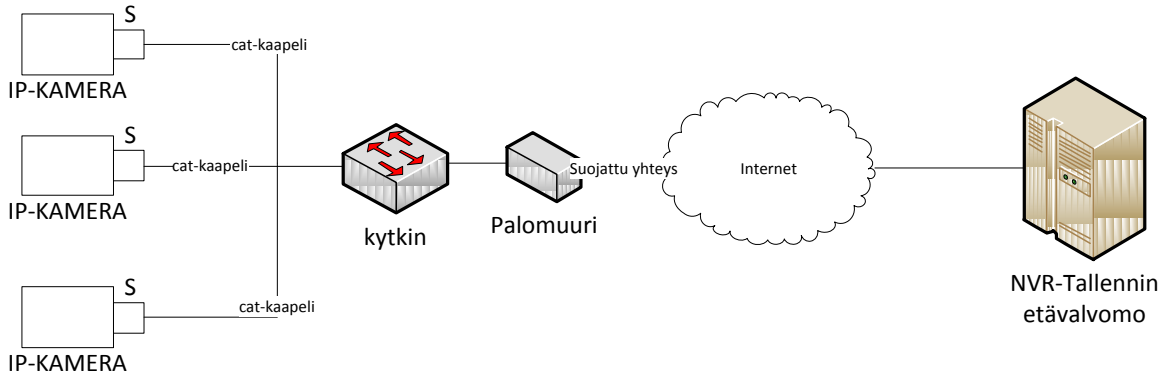
3.4.2 NVR-tallennin

NVR-tallenninta käytetään nykyaikaisessa IP-kameravalvonnassa. Tallennin perustuu useimmiten tavalliseen PC-tekniikkaan, johon käyttäjä voi hankkia tarvittavan ohjelmiston. (Sallinen 2010,24-25.)

IP-kameravalvonnassa kuvaa siirrettään kamerasta digitaalisesti lähiverkon välityksellä tallentimelle. Digitaalinen tiedonsiirto mahdollistaa tallentimen sijoittamisen verkon ulkopuolelle. Tällöin täytyy kuitenkin huomioida, että liikenne tulisi salata. (Sallinen 2010,24-25.) Kuviossa 6 on paikallinen tallennin ja kuviossa 7 on lähiverkon ulkopuolelle sijoitettu tallennin.



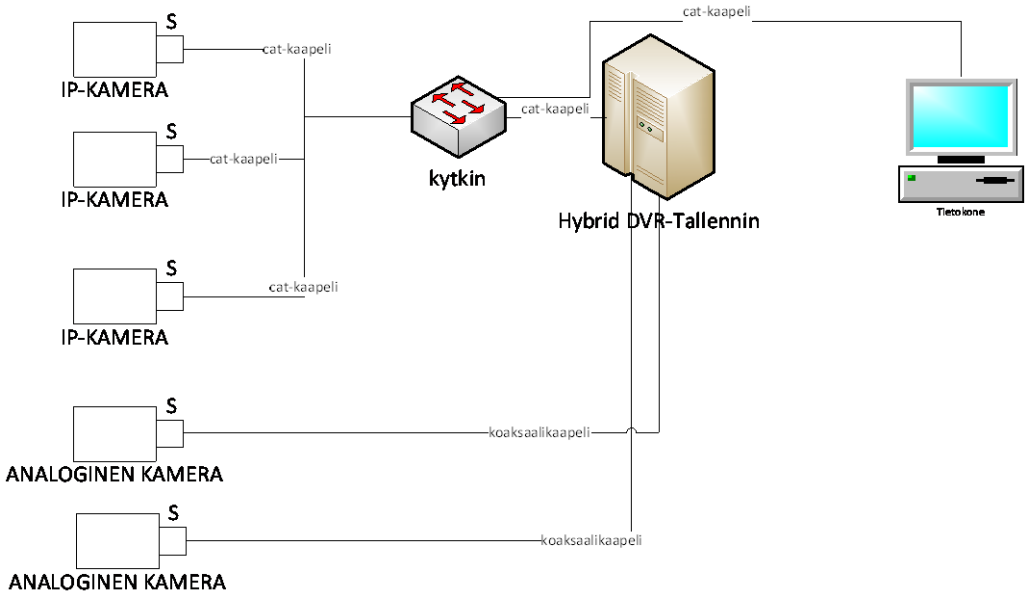
Kuvio 6. NVR-tallennin, paikallinen



Kuvio 7. NVR-tallennin, etävalvomo

3.4.3 Hybrid DVR -tallennin

Hybrid DVR-tallennin on joustava järjestelmä. Siinä on mahdollisuus yhdistellä vanhaa ja uutta tekniikka, koska laitteessa voidaan käyttää analogisia- ja digitaalisia kameroita. Tämä laskee kustannuksia, sillä vanhaa analogista järjestelmää ei tarvitse purkaa, vaan se voidaan liittää uuden Hybrid DVR-tallentimen yhteyteen. (Sallinen 2010,25-26.) Kuviossa 8 on kameravalvontaverkko, jossa on yhdistetty vanhaa ja uutta tekniikkaa. Analogiset kamerat kytketään palvelimeen koaksaalikaapelilla ja digitaaliset parikaapelilla.



Kuvio 8. Hybrid DVR -tallennin

3.5 NVR-tallenninohjelmistot

NVR-tallenninohjelmistoja on saatavilla tavallisille PC-tietokoneille, joissa on Windows tai Linux-käyttöjärjestelmä. Tallenninohjelmiston avulla voidaan hallita koko järjestelmää, sillä se käsittelee kameroilta tallennettua materiaalia ja järjestelmän toimintoja. (Sallinen 2010,22.)

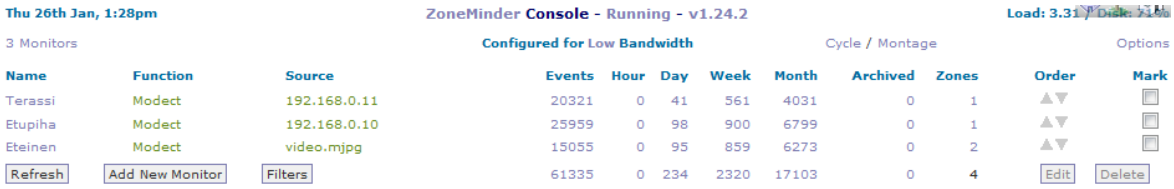
Ohjelmistoja tarjoavat useat eri valmistajat. Ohjelmistot edellyttävät tavallisesti maksullisen lisenssin. On olemassa kuitenkin myös täysin ilmaisia ohjelmistoja. Tällainen ohjelmisto on esimerkiksi Linux-käyttöjärjestelmälle suunniteltu Zoneminder. Seuraavissa kappaleissa tutustutaan ilmaiseen Linux-pohjaiseen Zoneminderiin ja maksullisen Netcam Watcher Pron perusominaisuuksiin.

3.5.1 Zoneminder-kameravalvontaohjelma

Zoneminder on suunniteltu Linux-käyttöjärjestelmälle. Se tarvitsee toimiakseen Linuxissa olevia lisäosia, kuten MySQL-tietokannan, PHP-tulkin, Apache Web-palvelimen ja ffmpeg-videomuuntimen. Käyttö ei vaadi erillistä valvontaohjelmaa, sillä se on rakennettu Web-alustalle. Ohjelmaa voidaan siis käyttää millä tahansa laitteella, jossa on internetselain. (Main Documentation, [viitattu 20.1.2012.])

Zoneminder-ohjelmisto tukee erittäin laajasti erilaisia kameroita. Siihen voidaan liittää mm. USB-kamera, IP-kamera ja analogikamera. Analogikamera vaatii tietokoneelta lisäkortin, johon voidaan tuoda analogisesta lähteestä videokuvaa. (Main Documentation, [viitattu 20.1.2012.])

Zoneminder-ohjelmisto tukee liikkeentunnistusta, jolla voidaan välttää turhaa kuvaamista. Se helpottaa myös tallenteiden selaamista, sillä jokainen liiketunnistettu video on tarkasti aikaleimattu. Liikkeentunnistuksessa voidaan myös rajata pois alueita, joita ei haluta huomioida. Ohjelmaan voidaan lisätä myös hälytys, jolloin ohjelma lähettää liiketunnistuksesta sähköpostia. (Main Documentation, [viitattu 20.1.2012.])

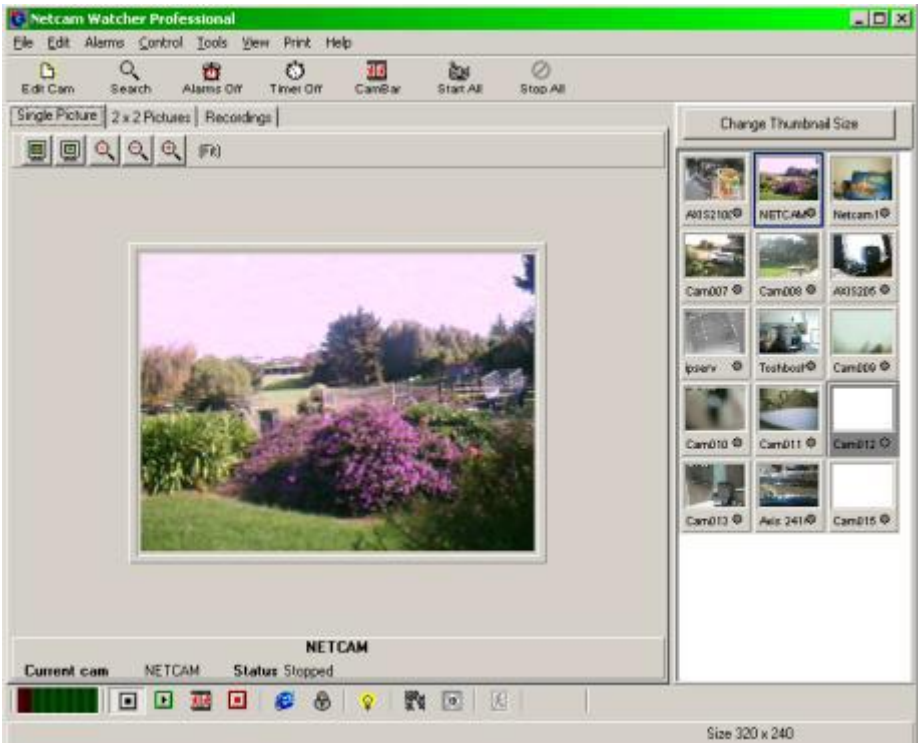


Kuvio 9. Zoneminder-ohjelman pääkäyttöliittymä

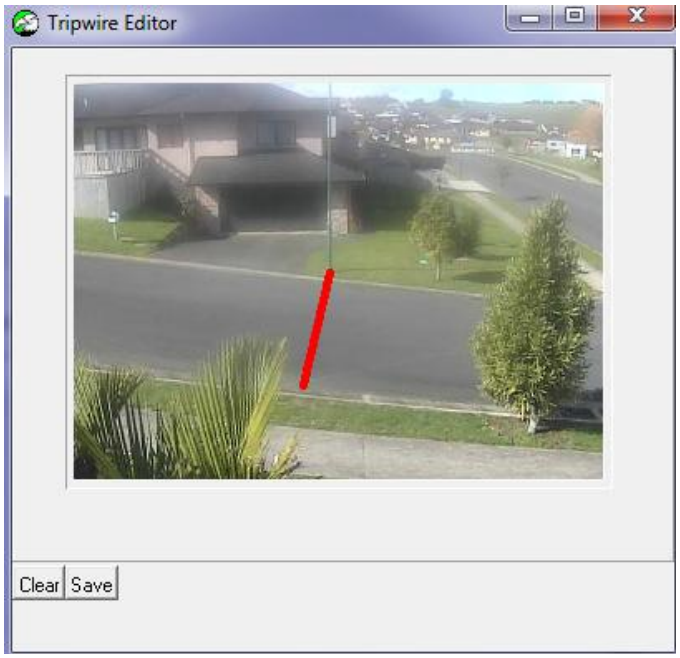
3.5.2 Netcam Watcher Professional

Netcam Watcher Professional on suunniteltu Windows-käyttöjärjestelmille. Sen käyttö tapahtuu omalla hallintaohjelmalla ja siinä on myös etäkäyttömahdollisuus. Etäkäyttötuki on saatavissa Windows-tietokoneille ja lisäksi myös Applen iPad/iPhone-laitteille. (Netcam Watcher Professional, [viitattu 21.1.2012.]) Kuviossa 10 on Netcam Watcher -ohjelman pääkäyttöliittymä.

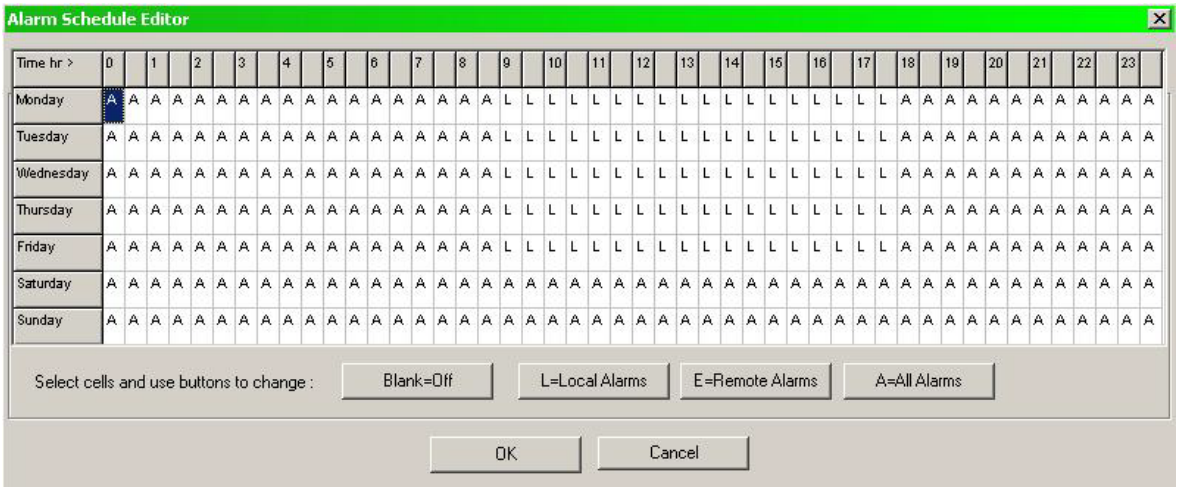
Netcam Watcher tukee vain digitaalisia kameroita, joten siihen voidaan liittää vain IP-kameroita. Ohjelmassa on kattavat säädöt erilaisille toiminnoille. Siihen voidaan asettaa esimerkiksi liikkeentunnistuksia ja hälytyksiä, joita käyttäjä voi määritellä melko vapaasti. Liiketunnistuksen kohteesta voidaan esimerkiksi poistaa kohteet, joiden liikkeeseen ei reagoida. Kuviossa 11 kohteeseen on viritetty ”ansalanka”, jolloin kuvaaminen tapahtuu vasta, kun jokin esine tai ihminen ylittää sen. Hälytysominaisuus voidaan liittää liikkeentunnistuksen yhteyteen, jolloin siitä lähtee käyttäjälle kuvallinen sähköpostiviesti tai jokin muu hälytys. Muu hälytys voi tarkoittaa käytännössä mitä tahansa toiminnetta, joka perustuu käyttäjän oman ohjelman ajamiseen hälytyksen yhteydessä. Käyttäjä voi esimerkiksi määritellä toiminnon, joka ohjaa tietokoneen USB- tai sarjaportissa olevaa relettä hälytyksen tapahtuessa. Näiden toimintojen lisäksi ohjelma sisältää kattavat ajastusmahdollisuudet. Liikkeentunnistus ja hälytys on mahdollista kytkeä pois ajastimella. Kuviossa 12 on esimerkki ajastimen hallintaikkunasta. Ajastimeen voidaan määritellä jokainen viikonpäivä erikseen. (Netcam Watcher Professional, [viitattu 21.1.2012.])



Kuvio 10. Netcam Watcher Professional -hallintaohjelma (Netcam Watcher Professional, [viitattu 21.1.2012]).



Kuvio 11. Netcam Watcher Professional -ansalangan käyttö (Netcam Watcher Professional, [viitattu 21.1.2012]).



Kuvio 12. Hälytysaikataulun valinta (Netcam Watcher Professional, [viitattu 21.1.2012]).

4 TIETOTURVA

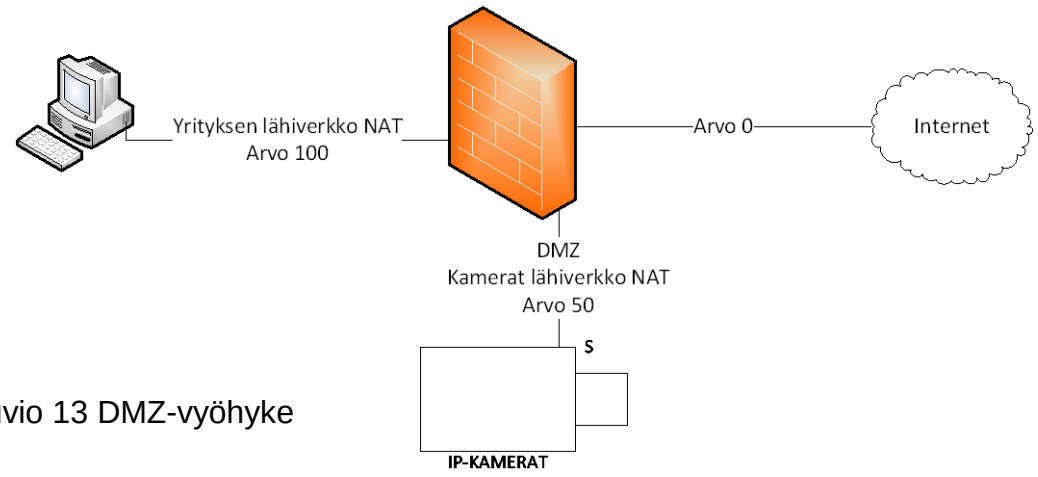
4.1 Erilaiset tietoturvavyöhykkeet

Koti- ja yritysverkko voidaan jakaa erilaisiin osiin tietoturvallisuuden perusteella. Tämä voidaan tehdä loogisesti käyttämällä VLAN-tekniikka, jossa yhteen kytkimeen voidaan luoda useampi virtuaalinen lähiverkko. Virtuaalisia verkkoja voivat olla esimerkiksi yrityksen oma lähiverkko, hallintaverkko ja palomuurin DMZ-alue. Nämä alueet voidaan eristää toisistaan palomuurilla tai reitittimen pääsylistoilla. (Sisäverkko-ohje 2010, 59.)

4.2 DMZ-vyöhyke palomuurissa

DMZ-vyöhyke on verkon alue, johon sijoitetaan tavallisesti laitteita, joihin on pääsy internetistä tai muusta riskipitoisesta vyöhykkeestä. Tällaisia laitteita voivat olla esimerkiksi erilaiset palvelimet, joihin on sallittu jokin tietty liikenne internetistä. DMZ-vyöhykkeen käyttö on hyödyllistä, sillä mahdollinen palvelimeen murtautuminen ei vaaranna lähiverkossa olevia koneita, sillä ne ovat eri verkoissa. (Sisäverkko-ohje 2010, 25.)

Ciscon palomuureissa käytetään eri verkkojen tietoturvan määrittelyyn turvallisuus arvoja. Kuvion 14 esimerkissä yrityksen lähiverkon arvo on 100, DMZ-alue on 50 ja ulkoliitännän eli internetin arvo on 0. Tämä tarkoittaa sitä, että ylimmästä arvosta pääsee verkon kaikkiin osiin, mutta alemmista arvoista ei pääse oletuksena ylöspäin. (Cisco Asa 5500 Series Configuration, [viitattu 27.1.2012], 72-73.)



Kuvio 13 DMZ-vyöhyke

4.3 Laitteen liittyminen lähiverkkoon

Laitteen liittyessä lähiverkkoon se voidaan tunnistaa MAC-osoitteen tai WLAN:sta tutun 802.1X-standardin avulla. MAC-osoite on laitevalmistajan asettama tunniste. Sen suojaustaso on heikko, sillä se on useimmiten helposti vaihdettavissa. 802.1x-menetelmässä voidaan käyttää monenlaista tunnistetta, kuten salasanaa tai bio-tunnistetta. Tuntemattomien laitteiden liittyminen verkkoon voidaan myös estää poistamalla käyttämättömät kytkennät, joko ohjelmallisesti tai poistamalla ne käsin. (Sisäverkko-ohje 2010, 66,78.)

4.4 VPN-tunnelointi palomuurilla

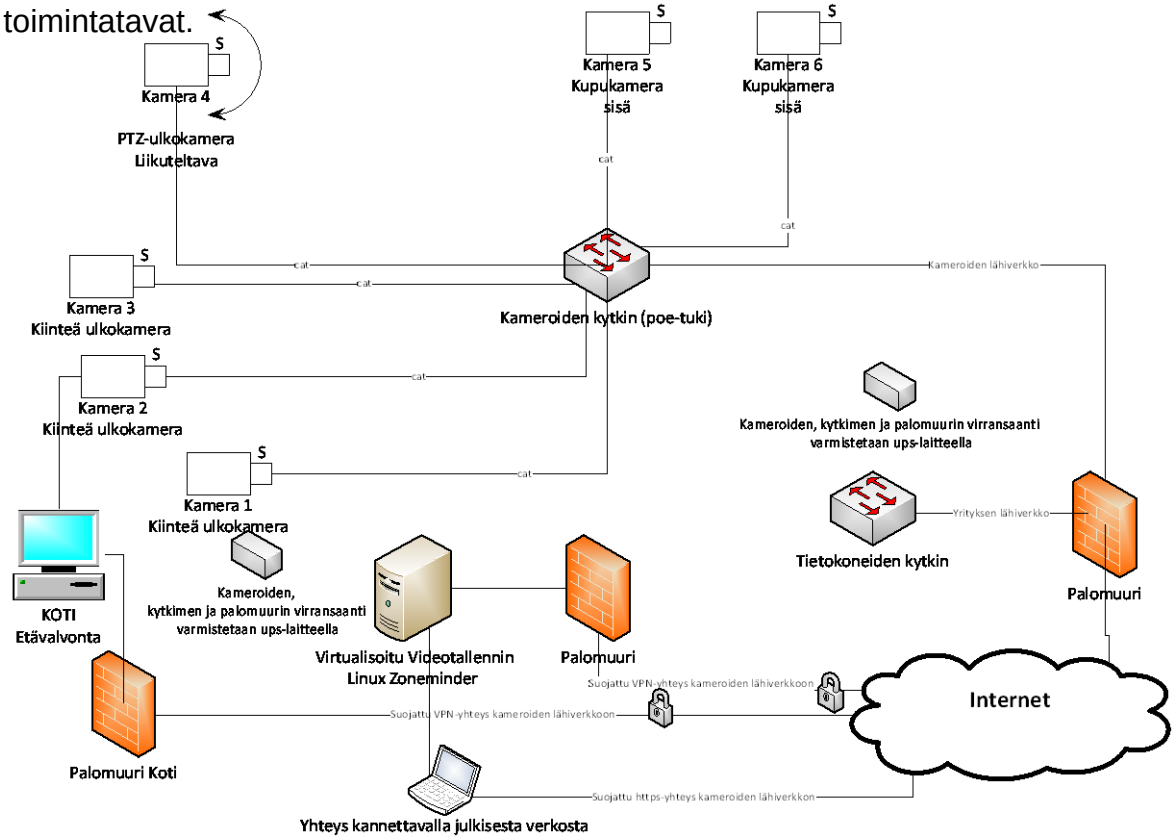
VPN (Virtual Private Networking) on menetelmä, jolla voidaan luoda salattu tunneli julkisen internetin läpi. VPN-ohjelmaa voidaan käyttää yksittäisissä koneissa, jolloin käyttäjä voi muodostaa esimerkiksi kotoa suojatun yhteyden yrityksen lähiverkkoon. Toinen mahdollisuus on liittää esimerkiksi kahden toimipisteen lähiverkot yhteen VPN:n avulla. Se mahdollistaa helpon ja turvallisen tiedonsiirron verkkojen välillä. (VPN-Palomuurit 2003, 1-3.)

5 SUUNNITELMA

5.1 Malli kohdeyrityksen valvontajärjestelmästä

Kohdeyrityksen suunnitelma aloitettiin kartoittamalla valvottavat kohteet. Valvottavia kohteita kertyi kuusi kappaletta, joista kaksi kohdetta on sisällä ja neljä ulkona. Tämän jälkeen selvitettiin voidaanko kiinteistön aikaisempaa kaapelointia hyödyntää kameravalvontaverkossa. Aikaisempaa kaapelointia ei ollut, joten rakennettiin uusi verkko. Verkoksi valittiin nykyaikainen yleiskaapelointi, jossa käytetään parikaapelia.

Parikaapelointia käytetään nykyään kaikissa lähiverkoissa. Erilaiset laitteet, kuten tietokoneet, tulostimet, kytkimet, IP-kamerat ja WLAN-tukiasemat toimivat lähiverkossa. Ympäristöön valittiin IP-kameravalvontajärjestelmä. Se on luonnollinen valinta, sillä se toimii saumattomasti yhteen muiden verkon laitteiden kanssa. Kuviossa 14 on verkkokuva suunnitellusta kameravalvontajärjestelmästä. Se on periaatekuva, josta selviää seuraavissa kappaleissa suunnitellut ratkaisut ja niiden toimintatavat.



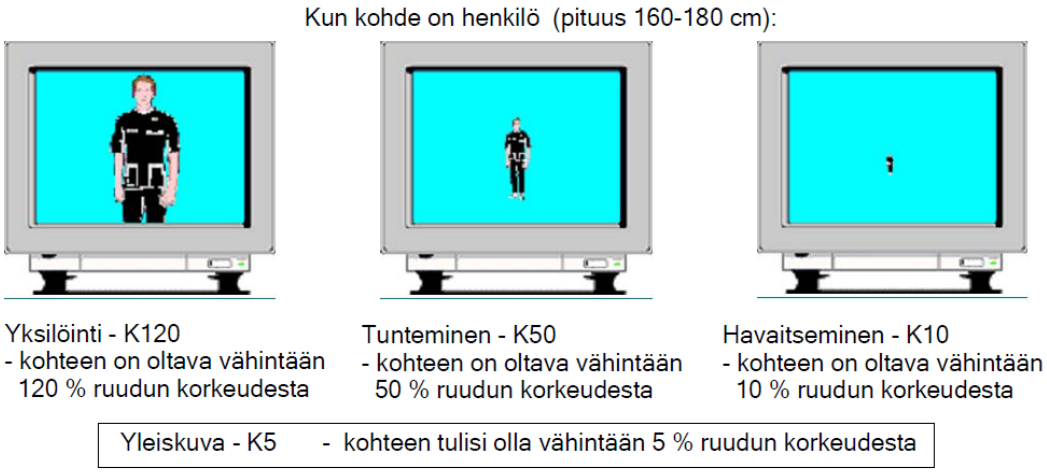
Kuvio 14. Kameravalvonnan verkkokuva.

5.2 Valvontakameroiden valinta

Kiinteistön parikaapelointi tuki IP-kameroiden valintaa. Valinta on ajanmukainen, sillä videovalvontateknologiassa on meneillään murros, jossa analogisia kameroita ja tallentimia päivitetään digitaaliseksi (IP-teknologia nostaa videovalvonnan uudelle tasolle, [viitattu 5.2.2012]).

Sisätiloihin päätettiin hankkia 2 kappaletta kiinteää PoE-virransyötöllä olevaa kupukameraa. Kameroiden läheinen sijainti uloskäynnin yhteydessä ohjasi kiinteän kupukameran valintaan, sillä kamera on huomaamaton ja se ei vaadi suurta asennustilaa.

Kameroilla on tarkoitus valvoa rakennuksen sisäänkäyntejä. Asennuspaikan määrityksessä käytettiin niin sanottua K-menetelmää, joka luokittelee kohteen kuvauksen kolmeen eri luokkaan. Kuviossa 15 havainnollistetaan näiden luokkien eroja. Kamerat kohdistettiin yksilöinti K-120-luokan mukaan, jossa kohde on vähintään 120 prosenttia ruudun korkeudesta.



Kuvio 15. K-menetelmä. (Kameravalvonnan K-menetelmä 2006, 5)

Ulkotiloihin valittiin neljä säänkestävää kameraa, joissa on PoE-tuki. Näistä kolme on kiinteitä ulkokameroita ja yksi on kääntöpäällä varustettu PTZ-kamera. Kolmella kiinteällä ja yhdellä PTZ-kameralla saatiin kattava valvonta koko piha-alueelle. PTZ-kameran 360 asteen katselukulmat ja zoom-toiminto mahdollistavat lisäksi pihamaan tarkemman tarkkailun.

Kiinteiden kameroiden asennuspaikan määrityksessä käytettiin menetelmää K-50, jossa kohde on vähintään 50 prosenttia ruudun korkeudesta. Tällä valinnalla valvontaan saatiin riittävän laaja alue, mutta myös samalla riittävän tarkka henkilön tunnistus.

PTZ-kamera on liikuteltava kamera, mutta sille voidaan myös asettaa vakioasento. Vakioasennon määrityksessä haettiin ensisijaisesti valvottavaksi pihaan saapuvaa liikennettä. Kameran asennuspiste tulee olemaan melko kaukana tieliittymästä. Se kuitenkin riittää tässä kohteessa, koska siinä käytetään K-10-menetelmää, jossa kohde on vähintään 10 prosenttia ruudun korkeudesta. K-10-menetelmän käyttö on perusteltua tässä kohteessa, sillä tallenninohjelmiston tukema liikkeentunnistus otetaan käyttöön. PTZ-kameran kohdalla se tarkoittaa, että esimerkiksi pihaan saapuva auto laukaisee liikkeentunnistuksen. Liikkeentunnistuksen käynnistyminen tässä kamerassa aloittaa tallennuksen jokaisessa kamerassa. Tämä ominaisuus voidaan tarvittaessa ottaa käyttöön myös muissa kameroissa.

5.3 Videotallenninohjelmiston valinta

Videotallenninohjelmistoa valittaessa tutkittiin kahden eri ohjelmiston ominaisuuksia. Nämä ohjelmistot olivat Windows-käyttöjärjestelmälle suunniteltu Netcam Watcher Pro ja Linux-käyttöjärjestelmälle toteutettu Zoneminder. Näistä molemmat ohjelmistot täyttivät vähimmäisvaatimukset, joita olivat liikkeentunnistus, hälytysomaisuus ja etäkäyttömahdollisuus.

Ohjelmistoksi valittiin Zoneminder tallenninohjelmisto. Valinta perustui ohjelman joustavampaan etäkäyttöön, ohjelman vakauteen ja sen ilmaiseen lisenssiin. Tässä tapauksessa koettiin, että selainpohjaisessa hallinnassa voitiin ohittaa erilaiset yhteensopivuusongelmat eri laitetyyppien välillä. Ohjelmaa voidaan käyttää erilaisilla laitteilla. Ainoa vaatimus on, että siihen on asennettu Web-selain.

5.4 Videopalvelinlaitteiston valinta

Videopalvelinlaitteiston hankintaa suunniteltaessa päädyttiin ratkaisuun, jossa koko videopalvelin ulkoistetaan kolmannelle osapuolelle. Tässä ratkaisussa ostetaan palveluntarjoajalta virtualisoitu palvelinratkaisu. Palvelimen virtualisoinnilla tarkoitetaan jonkin palvelinsovelluksen suorittamista virtuaalisessa ympäristössä. Yhdessä tehokkaassa palvelimessa voidaan ajaa useita virtuaalisia palvelimia yhtä aikaa. Etuja ovat mm. se, että käyttäjän ei tarvitse huolehtia ylläpidosta, vanhenevista laitteista ja tässä tapauksessa palvelin on turvallisessa paikassa. (Virtualisointi: Mitä se on ja onko siitä hyötyä minulle? 2010.)

5.5 Lähiverkon tietoturva ja etäkäyttö

Lähiverkon tietoturvaa suunniteltaessa otettiin huomioon turvallisen kameravalvontaympäristön vaatimukset. Siinä kamerat ja tallennin asetetaan omaan virtuaaliseen lähiverkkoon palomuurin DMZ-alueelle. Palomuurin DMZ-alueelta ei ole pääsyä yrityksen normaalin lähiverkkoon. Tämä antaa suojaa ulkoisia sekä paikallisia väärinkäyttöjä vastaan. Paikallisella suojalla tarkoitetaan esimerkiksi suoria tunkeutumisia fyysiseen kameroiden lähiverkkoon ja ulkoisella tarkoitetaan internetistä tapahtuvia hyökkäyksiä. Lisäksi täytyi huomioida myös verkon ulkopuolelle sijoitettu tallenninpalvelin ja videovalvonnan etäkäyttö. Näiden palvelujen toiminta mahdollistetaan palomuurin VPN-tunnelointiominaisuudella. VPN-tunneloinnilla saadaan turvallinen ja salattu yhteys näiden toimintojen välille.

5.6 Laitteiston sähkönsaanti sähkökatkoksen aikana

Valvontakameroiden täytyy toimia myös sähkökatkojen aikana. Tähän päätettiin varautua UPS-laitteella, jolla voidaan varmistaa sähkönsyöttö myös sähkökatkon aikana. Verkkopohjaisessa valvontakameraratkaisussa tämä onnistui helposti, sillä laitteiden virransaanti pystyttiin järjestämään keskitetysti. Tässä tapauksessa riitti, että varmistettiin kameroiden POE-kytkimen ja palomuurin virransyöttö.

6 JÄRJESTELMÄN KOKEILU TESTIYMPÄRISTÖSSÄ

6.1 Zoneminder-tallenninohjelmiston asennus Linux-käyttöjärjestelmään

Zoneminder-tallenninohjelmisto asennettiin Linux-palvelimelle, jossa oli käytössä Ubuntu 10.04 Lucid Lynx -käyttöjärjestelmä. Ohjelmisto ja sen vaatimat lisäosat asennettiin Linuxin komentoriviltä. Asennuksessa käytetyt komennot on lueteltu liitteessä 2. Liitteessä on myös kerrottu komentojen merkitykset.

Asennus aloitettiin Zoneminder-ohjelmiston lisäosien asennuksella, joita olivat Apache, Mysql, Php ja FFmpeg. Lisäosien asennus onnistui ilman ongelmia. Tämän jälkeen voitiin asentaa Zoneminder-ohjelmisto. Se ei kuitenkaan voi toimia suoraan asennuksen jälkeen, vaan siihen ja sen lisäosiin täytyy ensin tehdä tarvittavat asetukset.

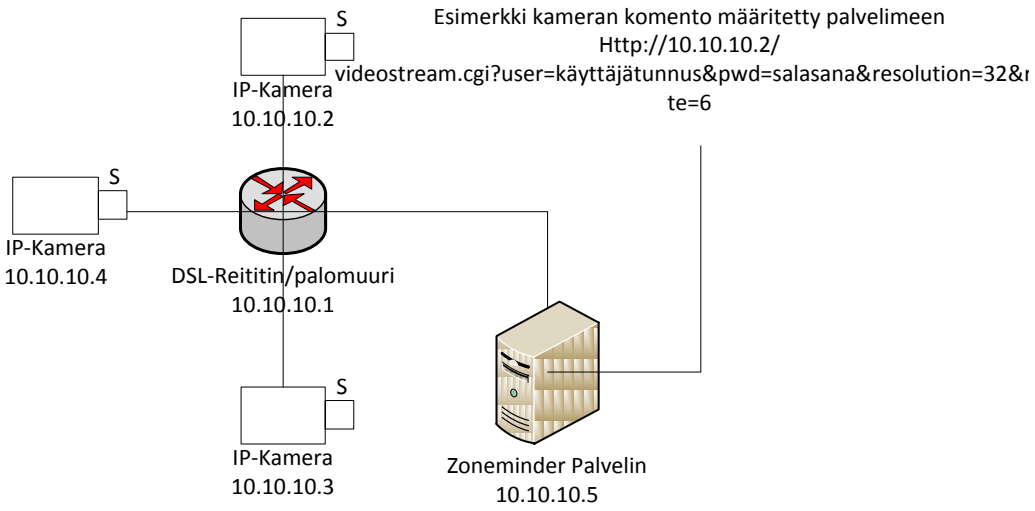
Seuraavaksi määriteltiin Mysql-tietokanta ja Apache Web-palvelin. Mysql-ohjelmaan vaihdettiin salasana, sekä viitattiin Zoneminderin tietokantaan. Tietokantaan määriteltiin myös tarvittavat oikeudet Zoneminder-ohjelmalle. Apache-palvelimeen lisättiin viittaus Zoneminder-ohjelmaan. Asetuksien saamiseksi käyttöön Apache-ohjelma käynnistettiin uudelleen.

Lopuksi palvelimeen asetettiin kiinteä IP-osoite ja järjestelmään lisättiin myös komennot, jotka vaikuttavat Zoneminder-ohjelman käyttöoikeuksiin ja muistinhallintaan.

6.2 IP-kameran määrittely Zoneminder-ohjelmalle

Jokaiselle kameralle asetettiin oma IP-osoite ja salasana. Kiinteitä osoitteita käytettiin, koska Zoneminder-videopalvelimeen on määritelty jokaisen kameran IP-osoite ja komento, jolla viitataan videolähteeseen eli kameraan. Zoneminder avaa käynnistyessään yhteyden kameraan IP-osoitteen ja erillisen komennon avulla. Kuviossa 16 havainnollistetaan lähiverkossa käytetyt IP-osoitteet ja komento, jolla Zoneminder avaa yhteyden kameraan.

Kameroihin ei ollut tarpeellista tehdä IP-osoitteiden ja salasanan määrittelyn lisäksi muita asetuksia, koska videotallenninympäristössä kameroiden kuva käsitellään videopalvelimella. Videopalvelinta varten selvitettiin komento, jota kamerat käyttivät. Komento löytyy yleensä kameran ohjekirjasta. Esimerkki kuviossa 16 mainittu komento sisältää kameran IP-osoiteen, videostream.cgi-tiedoston, käyttäjätunnuksen/salasanan ja videokuvalle määriteltävän resoluution.



Kuvio 16. Kameroiden IP-osoitteet lähiverkossa ja palvelimelle määritetty kameran IP-osoite ja komento

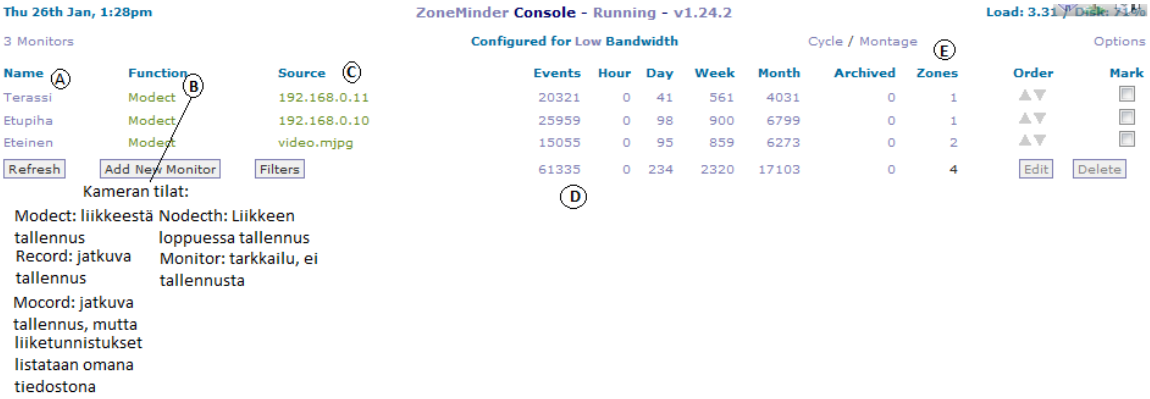
6.3 Zoneminder-ohjelmiston toiminteet

Zoneminder-ohjelman käyttäminen voitiin aloittaa avaamalla siihen yhteys internetselaimella. Selaimen osoiteriville kirjoitetaan videopalvelimen IP-osoite: 10.10.10.5, joka on mainittu kuviossa 16. Osoite koostuu HTTP:// etuliitteestä ja IP-osoitteesta.

Zoneminder-ohjelman tärkeimmät toiminteet löytyvät sen pääkäyttöliittymästä. Kuvion 18 kohdassa A on kerrottu kameran nimi. B-kohdassa määritellään kameran tilat, joita voivat olla Modect, Nodect, Monitor, Record ja Mocord. C-kohdassa kerrotaan kuvan lähde, joka on tässä tapauksessa IP-osoite. Lähteen tekstin väri paljastaa onko kamera käyttökunnossa. Tekstin ollessa vihreä kamera on toimintakunnossa. Kameran vikaantuessa teksti muuttuu punaiseksi. D-kohdassa on ker-

rottu hälytyksien kokonaismäärä, jota painamalla voidaan aukaista lista videoista, jotka kamera on kuvannut liiketunnistuksesta. Näitä voidaan tarkastella myös päivä-, viikko- tai kuukausitasolla. Kuvion 19 esimerkissä on yhden kameran päiväkohtaiset tallennukset. Aiheeseen palataan tarkemmin luvussa 6.5. E-kohdassa voidaan määritellä liikkeentunnistukselle erilaisia alueita, jotka voidaan rajata siitä pois. Kuviossa 17 on esimerkki rajauksen käyttämisestä. Esimerkissä on rajattu pois yksi alue. Ohjelmistossa on myös mahdollista rajata useita eri alueita.

Kuvio 17. Punaisen ulkopuolella olevat kohteet on rajattu kuvasta pois.



Kuvio 18. Zoneminder-ohjelman pääkäyttöliittymä.

6.4 Kameran lisääminen Zoneminder-ohjelmaan

Zoneminder-ohjelmaan asennettiin koekäyttöön kolme IP-kameraa. Kameran lisäämisessä täytyi selvittää sille asetettu IP-osoite, videolähteen komento ja käyttäjänimi/salasana, joihin on viitattu kuviossa 16. Ennen kameran lisäämistä ohjelmaan voidaan kameraan osoittavan linkin komennon toimivuus varmistaa selaimella. Se voidaan kokeilla yksinkertaisesti liittämällä selaimeen kuviossa 16 mainittu osoite. Toimiessaan selaimeen pitäisi avautua kameran kuva, joka päivittyy jatkuvasti. Kuviosta 18 voidaan todeta myös, että kaikki kolme asennettua kameraa ovat toiminnassa, sillä niiden osoitteet ovat vihreänä.

6.5 Tallenteiden tulkinta ja tehtävätyökalun käyttö Zoneminder-ohjelmassa

Kuvion 17 kohdassa D näkyy, että ohjelma on arkistoinut suuren määrän liiketunnistuksesta aiheutuneita videotallenteita. Videotallenteita on kerätty 120 päivän ajalta ja niitä on yhteensä 61335 kappaletta. Lukema on melko suuri, mutta siihen vaikuttaa monta muuttuvaa tekijää. Tällaisia muuttuvia tekijöitä voivat olla esimerkiksi valoisuuden vaihtelut, lumisade ja myrsky. Niiden aiheuttamaan turhaan kuvaamiseen ei pystytty vaikuttamaa merkittävästi, vaikka jokaiselle kameralle on määritetty vain tietyt liiketunnistusalueet ja lisäksi niiden herkkyyttä säädettiin pienemmälle. Tämä ei kuitenkaan tee liiketunnistuksella tapahtuvasta kuvaamisesta turhaa, sillä yhtä kameraa kohti tapahtumien määrä on vain noin 170 videota vuorokaudessa. Päivinä, jolloin häiriötekijöitä on vähemmän, tapahtumien määrä on huomattavasti pienempi. Kuviossa 19 on esimerkkikamera, joka on taltioinut tapahtumia 7 tunnin ajalta lumisateen aikana. Kuvasta voidaan päätellä aikaleimojen perusteella, että kamera on kuvannut paljon turhaa liikettä. Se johtuu kameran linssin ohittavista lumihiutaleista. Ohjelma kuitenkin kirjaa videot tarkasti päivämäärän perusteella. Se tekee videoiden selaamisesta melko helppoa. Riittää, että tietää tapahtuma-ajan muutaman päivän tarkkuudella. Muutaman päivän videomateriaali voidaan käydä vielä melko nopeasti läpi. Liiketunnistukseen vaikuttavat häiriötekijät estävät kuitenkin videovalvonnan käytön sähköpostihälytyksissä, koska se lähettäisi joka päivä useita tarpeettomia sähköpostihälytyksiä. Sähköpostihä-

lytyksen käyttö voi olla perusteltua ainoastaan tilassa, jossa aikaisemmin mainitut häiriötekijät ovat harvinaisia.

Kuviossa 20 on tapahtumien suodattamiseen liittyvä toimintoikkuna. Sillä voidaan esimerkiksi arkistoida tai tuhota tallennetut videot määrättyjen ehtojen perusteella. Toimintoikkuna on todella monipuolinen, mutta sen käyttö osoittautui melko vaikeaksi. Ohjelmassa saatiin kuitenkin testattua toiminto, joka helpottaa videopalvelimen ylläpitoa. Ohjelmassa otettiin käyttöön sääntö, jolla poistetaan kaikki yli kuukauden vanhat nauhoitukset. Tällä säännöllä myös täytetään lain vaatima velvoite siitä, että tarpeettomat videotallenteet tulisi hävittää välittömästi, kun niille ei ole enää perusteltua käyttöä.

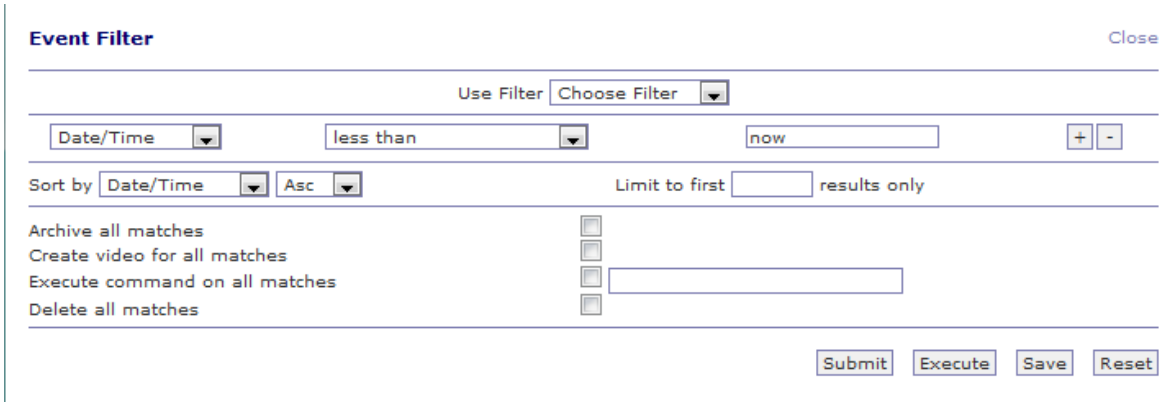
306 Events

View Paged Close

Refresh Show Filter Window Show Timeline

Id	Name	Monitor	Cause	Time(v)	Duration	Frames	Alarm Frames	Total Score	Avg. Score	Max. Score	
68246	Event-68246	Terassi	Motion	02/06 15:08:01	6.12	29	9	77	8	11	
68241	Event-68241	Terassi	Motion	02/06 11:37:19	4.27	22	2	14	7	8	
68236	Event-68236	Terassi	Motion	02/06 11:02:08	6.65	31	11	398	36	58	
68231	Event-68231	Terassi	Motion	02/06 10:08:05	5.62	27	7	122	17	32	
68228	Event-68228	Terassi	Motion	02/06 10:00:46	4.28	22	2	14	7	7	
68223	Event-68223	Terassi	Motion	02/06 09:28:19	5.91	28	8	67	8	12	
68220	Event-68220	Terassi	Motion	02/06 09:26:19	5.06	25	5	122	24	41	
68215	Event-68215	Terassi	Motion	02/06 09:10:26	6.27	29	9	299	33	57	
68210	Event-68210	Terassi	Motion	02/06 09:01:54	4.57	21	1	5	5	5	
68207	Event-68207	Terassi	Motion	02/06 08:53:08	6.32	28	8	224	28	54	
68193	Event-68193	Terassi	Motion	02/06 08:47:37	3.29	21	1	9	9	9	
68186	Event-68186	Terassi	Motion	02/06 08:42:44	5.74	30	10	419	41	63	
68183	Event-68183	Terassi	Motion	02/06 08:40:19	4.26	21	1	12	12	12	
68180	Event-68180	Terassi	Motion	02/06 08:38:16	4.62	22	2	12	6	6	
68177	Event-68177	Terassi	Motion	02/06 08:33:03	7.45	30	10	434	43	63	
68174	Event-68174	Terassi	Motion	02/06 08:26:43	5.56	21	1	5	5	5	
68171	Event-68171	Terassi	Motion	02/06 08:26:22	5.59	21	1	7	7	7	
68168	Event-68168	Terassi	Motion	02/06 08:21:03	6.10	21	1	5	5	5	
68165	Event-68165	Terassi	Motion	02/06 08:15:54	5.56	21	1	6	6	6	
68162	Event-68162	Terassi	Motion	02/06 08:15:09	5.60	21	1	5	5	5	
68159	Event-68159	Terassi	Motion	02/06 08:14:54	5.58	21	1	10	10	10	
68158	Event-68158	Terassi	Motion	02/06 08:04:26	6.62	24	2	19	9	10	
68155	Event-68155	Terassi	Motion	02/06 08:04:22	5.58	21	1	14	14	14	
68148	Event-68148	Terassi	Motion	02/06 08:02:05	5.57	21	1	9	9	9	
68145	Event-68145	Terassi	Motion	02/06 08:00:01	5.54	21	1	5	5	5	

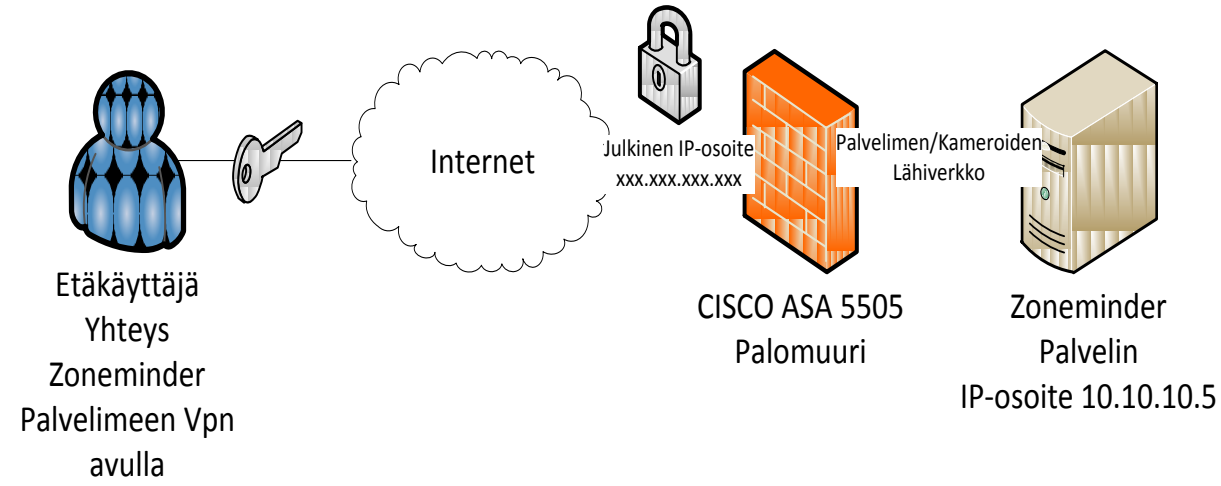
Kuvio 19. Zoneminderin tallentamat tapahtumat lumisateen aikana



Kuvio 20. Zoneminderin toimintoikkuna

6.6 Zoneminder-ohjelman etäkäyttö VPN-ohjelmalla

Zoneminder-ohjelmassa ei ole erillistä etäkäyttöohjelmaa, vaan sitä hallitaan jokaisessa tilanteessa selaimen avulla. Testiympäristössä Zoneminder toimii samassa lähiverkossa kameroiden kanssa. Käytössä oli Cisco Asa 5505 -palomuuri, johon määritettiin static-IP eli kiinteä IP-osoite. Palomuuriin määritettiin myös VPN-yhteys etäkäyttöä varten. Kuviossa 21 kuvataan VPN-yhteyden toimintaperiaate. Etäkäyttäjä avaa tietokoneellaan Cisco VPN-asiakasohjelman, jonka avulla otetaan yhteys valvontakameraverkon palomuuriin. Käyttäjän todennus palomuuriin on kaksinkertainen. Käyttäjä tarvitsee ryhmän salausavaimen lisäksi henkilökohtaisen salasanan. VPN-yhteyden ollessa toimintakunnossa etäkäyttäjä voi hallita Zoneminder-palvelinta samalla tapaa, kun olisi fyysisesti kytkeytynyt sen lähiverkkoon. Palvelin vastaa verkon ulkopuolelta kuviossa 21 mainitulla IP-osoittella (10.10.10.5). VPN-yhteyden avulla voidaan tarvittaessa myös hallita jokaista verkossa olevaa laitetta. VPN-yhteys täyttää tässä tapauksessa halutut ominaisuudet. Se on turvallinen ja sen avulla videopalvelinta pystytään hallinnoimaan etäisesti.



Kuvio 21. Etäkäyttäjä ja VPN-yhteys

7 JOHTOPÄÄTÖKSET

Kameravalvonnan suunnittelussa on hyvä tietää erilaiset kameravalvontajärjestelmät, sillä niitä on asennettu jo yli kaksi vuosikymmentä. Tuona aikana ne ovat kehittyneet paljon. Viimeisin muutos, jossa analogisista järjestelmistä siirrytään digitaalisiin, on suurin kameravalvonta-alalla koko aikana tapahtunut innovaatio.

Opinnäytetyössä kohdeyritykselle suunniteltu kameravalvonta täytti lähes kaikki vaatimukset, joita olivat helppokäyttöisyys, etäkäyttö, hälytykset ja helppo ylläpito. Ainoastaan hälytykset sähköpostin välityksellä jäivät saavuttamatta. Tämä johtui erilaisista häiriötekijöistä, jotka aiheuttavat paljon turhia hälytyksiä liiketunnistimessa. Kameravalvonta ei riitä siis ainoaksi valvontajärjestelmäksi. Sen avulla voidaan selvittää tehokkaammin mahdollisia rikoksia ja se voi myös toimia pelotteena.

Kameravalvontatekniikoihin tutustuminen on ollut opinnäytetyön tekijälle opettavaista. Se on laajentanut tietämystä eri laitteistoista ja tekniikoista, etenkin IP-kameroihin ja tallentimiin liittyvä tietämys on parantunut. Opinnäytetyön tekeminen on ollut mielenkiintoista, koska asioita on saanut toteuttaa myös käytännössä.

LÄHTEET

Aalto, S. 2009. Kameravalvontajärjestelmät. Espoo: Sähköinfo Oy.

Cisco ASA 5500 Series Configuration [Verkkosivu]. Cisco.com. [Viitattu:31.01.2012]. Saatavana: http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/asa_83_cli_cfg.pdf

Granlund, K. 2007. Tietoliikenne. Jyväskylä: Docendo.

IP-teknologia nostaa videovalvonnan uudelle tasolle.[Verkkosivu]. LANWAN. [Viitattu:5.2.2012]. Saatavana: http://www.lanwan.fi/filebank/173-hyvinkaa_videovalvonta.pdf

IP-videovalvonta: vaatimukset, käyttöönotto, toiminta ja tulevaisuus.16.11.2010. [Verkkosivu]. Mato78.com. [Viitattu:21.01.2012]. Saatavana: http://mato78.com/artikkelit/white-paper/10402-ip-videovalvonta-vaatimukset-kaeyttoeoenotto-toiminta-ja-tulevaisuus?start=1

Ipcmax Tuotteet [Verkkosivu]. Ipcmax.com. [Viitattu:26.01.2012]. Saatavana: www.ipcmax.com/product_info.php?products_id=1452

Julkisella paikalla saa kuvata. 17.1.2008.[Verkkosivu]. Suomen Tietotoimisto. [Viitattu:23.1.2012]. Saatavana: http://www.hs.fi/kotimaa/artikkeli/Julkisella+paikalla+saa+kuvata/1135233349499

Julkisten tilojen kameravalvonta lisääntyy Suomessa. 25.8.2006. [Verkkosivu]. MTV3 Uutiset. [Viitattu:31.01.2012]. Saatavana: http://www.mtv3.fi/uutiset/kotimaa.shtml/2006/08/465038/julkisten-tilojen-kameravalvonta-lisaantyy-suomessa

Kaikkonen, J. 2007. Henkilökohtainen tiedonanto 26.4.2007. Espoo: ASAN SecurityTechnologies.

Kameravalvonnan K-menetelmä 2006. Vakuutusyhtiöiden Keskusliitto. [Verkkosivu]. Finanssialan Keskusliitto. [Viitattu:1.2.2012]. Saatavana: http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kameravalvonnan_suunnitteluohje_K-menetelma_2006.pdf

Kivivuori, J. 2005. Perinteinen omaisuusrikollisuus vähentynyt nuorilla. [Verkkosivu]. Oikeusministeriö rikoksentorjuntaneuvosto [Viitattu: 25.1.2012]. Saatavana: http://www.haaste.om.fi/32933.htm

Koskinen, J. 24.01.2001. Kameravalvonnan oikeudellinen sääntely. [Verkkosivu]. Oikeusministeriö. [Viitattu: 25.1.2012]. Saatavana: http://www.om.fi/8156.htm

L 13.8.2004/759. Laki yksityisyyden suojasta työelämässä.

L 22.4.1999/523. Henkilötietolaki.

L 9.6.2000/531. Laki yksityisyyden, rauhan ja kunnian loukkaamisesta.

Lisää virtaa verkosta. 25.11.2009. [Verkkosivu]. Tietokone.fi. [Viitattu:17.01.2012]. Saatavana: http://www.tietokone.fi/lehti/tietokone_10_2009/lisaa_virtaa_verkosta_7957

Main Documentation. [Verkkosivu]. ZoneminderWiki [Viitattu: 20.1.2012]. Saatavana: http://www.zoneminder.com/wiki/index.php/Documentation

Netcam Watcher Professional. [Verkkosivu]. Netcam-Watcher.com [Viitattu: 21.1.2012]. Saatavana: http://www.netcam-watcher.com/userman.pdf

Network Camera Considerations. 2012. [Verkkosivu]. Video Surveillance [Viitattu: 8.2.2012]. Saatavana: http://www.videosurveillance.com/ip-video/network-camera-considerations.asp

Sallinen, P. 2010. Kameravalvontaopas. [Verkkokirja]. Sähköinfo Oy. [Viitattu: 23.1.2012]. Saatavana: http://www.niscayah.fi/70e1934b-4ffe-4c4d-978f-d753eb71a990.fodoc

Sisäverkko-ohje. 2010. [Verkkosivu]. Valtionvarainministeriö. [Viitattu: 1.2.2012]. Saatavana: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/Sisaeverkko-ohje.pdf

Tuotteet Kameravalvonta [Verkkosivu]. Aseko.fi. [Viitattu:25.01.2012]. Saatavana: http://www.aseko.fi/tuotteet/?group=00000633&mag_nr=3&prod_id=00002009

Vimdata Tuotteet [Verkkosivu]. Vimdata.fi. [Viitattu:25.01.2012]. Saatavana: http://vimdata.fi/kauppa/index.php?main_page=index&manufacturers_id=105&alpha_filter_id=75&page=1&sort=2a

Virtualisointi: mitä se on ja onko siitä hyötyä minulle? 25.05.2010. [Verkkosivu]. Mato78.com. [Viitattu:21.01.2012]. Saatavana: http://www.mato78.com/artikkelit/white-paper/2339-virtualisointi-mitae-se-on-ja-onko-siitae-hyoetyae-minulle

VPN-palomuurit.10/2003. [Verkkosivu]. MikroPC.net. [Viitattu:16.01.2012]. Saatavana: http://mikropc.net/nettilehti/pdf/0409200332.pdf

What are infrared surveillance cameras used for?[Verkkosivu]. Ehow.com. [Viitattu:25.01.2012]. Saatavana: http://www.ehow.com/info_8078848_infrared-surveillance-cameras-used.html

LIITTEET

LIITE 1 Cisco Asa 5505 VPN- ja Lähiverkkoasetukset

Palvelimen/kameroiden lähiverkkoasetukset Cisco 5505 palomuurissa:

```
interface Vlan12
 no forward interface Vlan1
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
interface Vlan1
 nameif inside
 security-level 100
 ip address julkinen 255.255.255.248
```

Sallitaan liikenne VPN verkosta kameroiden verkkoon.(tässä tapauksessa VPN-osoitteet jaetaan samasta verkosta)

```
access-list inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0 10.10.10.0 255.255.255.0
```

Etäkoneille jaettavat osoitteet

```
ip local pool vpnpool1 10.10.10.200-10.10.10.201 mask 255.255.255.0
```

Käytettävä salaus:

```
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
```

VPN-ryhmän tunnus ja käyttäjän/ryhmän salasanat:

```
default-group-policy testi2012
tunnel-group testi2012 ipsec-attributes
 pre-shared-key xxxxxxxxxxxxxxxxxxxxxx
```

```
username testi password xxxxxxxxxxxx encrypted privilege 1
```

LIITE 2 Linux Zoneminder asennus Linux-käyttöjärjestelmään

Ohjelmien asennus aptitude-ohjelman avulla

```
sudo aptitude install apache2 php5 apache2.2-common libapache2-mod-auth-mysql php5-mysql mysql-server ffmpeg
```

Zoneminder-ohjelman asennus

```
sudo aptitude install zoneminder
```

Salasanan luominen

```
mysqladmin -u root password oma_uusi_salasanasi
```

Viittaus Tietokantaan

```
sudo mysql -u root -p < /usr/share/zoneminder/db/zm.sql
```

Tietokannan oikeuksien määrittely

```
mysql -u root -p   grant select,insert,update,delete on zm.* to 'käyttäjänimi'@localhost identified by 'salasana';

flush privileges;
quit
```

```
Apachen määrittely ja uudelleen käynnistys:

sudo ln -s /etc/zm/apache.conf /etc/apache2/conf.d/zoneminder.conf

sudo /etc/init.d/apache2 force-reload
```

Kansion käyttöoikeuksien muutos

```
sudo chmod 4755 /usr/bin/zmfix

zmfix –a

Käyttäjän lisäys:

sudo adduser www-data video
```

Muistinhallinta:

```
sudo gedit /etc/sysctl.conf
```

```
kernel.shmall = 134217728

kernel.shmmax = 134217728
```

IP-osoitteen määrittely:

```
sudo gedit  /etc/network/interfaces

iface eth3 inet static

address 10.10.10.5

netmask 255.255.255.0

gateway 10.10.10.1
```