HAAGA-HELIA
ammattikorkeakoulu

Verkonvalvonta ja -hallintasovelluksen valinta, Case: Neste Oil

Tapio Naumanen

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2014

HAAGA-HELIA ammattikorkeakoulu

Tiivistelmä

Päiväys 28.11.2014

Tekijä(t)
Tapio Naumanen

Koulutusohjelma
Tietojenkäsittely

Opinnäytetyön otsikko
Verkonvalvonta ja -hallintasovelluksen valinta, Case: Neste Oil

Sivu- ja liitesivumäärä
33+3

Opinnäytetyön otsikko englanniksi
Choosing a network monitoring software, Case: Neste Oil

Suurten yritysten kasvavat tietoverkot ja niiden ylläpitäjät tarvitsevat tuekseen verkonvalvonta ja -hallintajärjestelmän. Kyseisillä järjestelmillä voidaan ehkäistä verkossa ilmenevien vikatilanteiden syntyminen ja pystytään reagoimaan nopeasti verkkovikoihin. Lisäksi verkonvalvontasovelluksilla saadaan kerättyä verkosta tietoa, jota voidaan hyödyntää esimerkiksi verkon optimoinnissa tai laitehankinnoissa.

Opinnäytetyön tehtävänä on kartoittaa Neste Oilille sopivin vaihtoehto ennalta valituista sovelluksista. Työssä vertaillut sovellukset olivat Nagios XI, WhatsUp Gold ja PRTG Network Monitor. Sopivan sovelluksen tulee täyttää toimeksiantajan määrittämät kriteerit, kuten esimerkiksi mahdollisuus valvoa useampaa erillistä verkkoa ja vähintään tuhatta erillistä laitetta, tullakseen valituksi. Työ rajoittui ainoastaan sovelluksen valintaan.

Opinnäytetyön teoriaosuudessa pohjustetaan verkonvalvontaa ja -hallintaa käsitteenä sekä käsitellään yleisimpiä käytössä olevia valvontaprotokollia ja -tekniikoita. Valituista sovelluksista käydään läpi toimeksiantajan kannalta tärkeimmät ominaisuudet ja perehdytään niiden toimintaan. Sovelluksien toimintaa ja ominaisuuksia vertaillaan toisiinsa tekstissä ja kahdessa taulukossa.

Sovellukseksi valittiin PRTG Network Monitor. Tulokseen päädyttiin sovelluksen monipuolisuuden, lisensoinnin ja yksinkertaisuuden johdosta. Toinen varteenotettava vaihtoehto oli WhatsUp Gold, joka on Neste Oilin nykyinen sovellus. Lopullinen valinta näiden kahden välillä voidaan suorittaa, kun molemmat sovellukset on testattu käytännössä toimeksiantajalla.

Asiasanat
verkonhallinta, nettivalvonta, protokollat, TCP/IP, verkkoympäristö

HAAGA-HELIA
University of Applied Sciences

Abstract

Date 28.11.2014

Author(s)
Tapio Naumanen

Degree programme
Degree Programme in Business Information Technology

Report/thesis title
Choosing a network monitoring software, Case: Neste Oil

Number of pages and appendix pages
33+3

Corporations' growing networks require a monitoring system to support their networks and network administrators. Modern monitoring systems may prevent network faults, and enable administrators to react quickly when there are errors and difficulties. In addition, network monitoring programs can be used to gather information on the network. That information can be, for example, utilized for network optimizing or for future hardware equipment purchases.

The goal of the study was to map out the best possible option for Neste Oil from pre-selected applications. The applications were Nagios XI, WhatsUp Gold and PRTG Network Monitor. To be accepted, application must meet criteria defined by the client, such as an option to monitor multiple subnetworks and an option to monitor, at least, a thousand different devices. The scope of the study was limited to choosing the application only.

The theoretical part of the study deals, with the concept of network monitoring and the most common monitoring protocols and techniques. With applications, the main focus is on functions which are important to client, and how those work in that application. The mode of work and the functions of the application which are crucial for the client are compared to each other descriptively and with the help of two tables.

The PRTG Network Monitor application was selected. The study has ended up with this conclusion because the application is versatile, it is simple and it has simple licensing. WhatsUp Gold, which is Neste Oil's current application, was a worthy alternative. The final selection between these two can be performed when both applications have been tested in practice.

Keywords
network monitoring, network management, protcols, TCP/IP, network enviroment

Sisällys

Sanasto

.NET on Microsoftin vapaaseen lähdekoodiin perustuva ohjelmistokomponenttikirjasto pääasiassa Microsoft Windows -käyttöjärjestelmälle.

AES, Advanced Encryption Standard, on toistaiseksi murtamaton lohkosalausmenetelmä tiedon salaamiseen. Avaimen pituudelle on kolme vaihtoehtoa 128, 192 ja 256 bittiä.

API, Application Programming Interface, ohjelmointirajapinta, määritelmä tietojen vaihtamiseen ohjelmien välillä.

CIM, Common Information Model, avoin standardi, joka määrittelee kuinka hallittavat elementit IT-ympäristöissä ovat esitetty yleisinä objekteina sekä eri elementtien väliset suhteet.

Flow käsittää eri valmistajien kehittämät Flow-tekniikat, kuten NetFlow, Jflow, NetStream, Cflow, sFlow ja niin edelleen. Flow-tekniikka mahdollistaa IP liikennettä koskevan tiedon keräämisen talteen reitittimestä tai kytkimestä.

ICMP, Internet Control Message Protocol, protokolla IP yhteyksiä käyttävien laitteiden viestien välittämiseen.

IP, Internet Protoocol, internetprotokolla, joka huolehtii IP-pakettien siirrosta Internetverkossa.

ITU-T, International Telecommunication Union, lopussa oleva T tarkoittaa televiestintäsektoria. ITU on YK:n alainen kansainvälinen televiestintäverkkoja ja -palveluja koordinoiva järjestö.

LLDP, Link Layer Discovery Protocol, on linkkikerroksen protokolla, jota verkkolaitteet käyttävät itsestään tai ominaisuuksistaan ilmoittamiseen sekä ilmoittavat mahdollisista viereisistä laitteista paikallisverkossa.

MAC-osoite, Media Access Control, valmistajan määrittelemä laitteen verkkosovittimen yksilöivä osoite, joka koostuu kuudesta kaksinumeroisesta heksadesimaalisesta luvusta.
MIB, Management Information Base, SNMP protokollan hallintatietokanta, se määrittelee verkonhallintaobjektit.

Ping, TCP/IP-protokollan työkalu, jolla voidaan mitata laitteen saatavuutta. Se lähettää laitteelle ICMP echo request -paketin, johon sen vastaanottama laite vastaa echo reply –paketilla, mikäli laite on tavoitettavissa.

Proxy, proxy server, eli välityspalvelin, tietokonejärjestelmä tai ohjelma, joka varastoi, suodattaa ja välittää verkossa siirrettävää dataa.

RMON, Remote Network Monitoring, ohjelmisto tai laite, joka kerää tietoja verkon laitteista ja tallentaa ne omaan tiedostoonsa tai lähettää isäntäohjelmalle.

RSA on julkisen avaimen salausalgoritmi, jota käytetään tiedon salaamiseen. Se perustuu julkiseen ja yksityiseen avaimeen.

SMI, Structure of Management Information, MIB-taulukon hierarkkisen rakenteen ja objektien määrittelemiseen käytettävä tietorakenne.

SNMP, Simpe Network Management Protocol, yleinen TCP/IP-verkkojen verkonvalvontaprotokolla.

TCP, Transmission Control Protocol, tietoliikenneprotokolla, jonka avulla luodaan yhteyksiä laitteiden välillä.

TCP/IP, Transmission Control Protocol / Internet Protocol, on kahden tietoverkkoprotokollaan yhdistelmä. TCP-protkolla vastaa kahden laitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja uudelleenlähettämisestä. IP-protokolla vastaa, että paketit löytävät oikeisiin osoitteisiinsa.

Telnet on yhteysprotokolla jolla voidaan muodostaa pääteyhteys Internetin yli esimerkiksi reitittimeen tai kytkimeen. Telnet tunnetaan myös telnet-protokollaa käyttävänä ohjelmana, jolla muodostetaan pääteyhteyksiä.

UDP, User Datagram Protocol, tiedonsiirtoprotokolla, yhteydetön protokolla joka ei vaadi jatkuvaa yhteyttä laitteiden välille mutta mahdollistaa tietojen siirron.

WMI Windows Management Instrumentation, Windowsin kehittämiä laajennuksia, joilla mahdollistetaan hallintatietojen välitys laitteiden välillä ja esimerkiksi skriptien suorittaminen.

1 Johdanto

Verkon hallintaan ja valvontaan on kehitetty useita erilaisia sovelluksia, jotka hyödyntävät erillisiä laitteita ja tekniikoita, kuten Internet-protokollia. Verkko on alati muuttuva kokonaisuus eikä se pitkään pysy sellaisena kuin se on alun perin suunniteltu. Verkkoon tehdään muutoksia kun halutaan uusia palveluita, lisätään päätelaitteita tai poistetaan vanhoja ja rikkinäisiä laitteita. Mitä suuremmaksi verkko kasvaa, sen haasteellisemmaksi sen ylläpitäminen muuttuu.

Tämä opinnäytetyö käsittelee verkonvalvonnassa ja -hallinnassa yleisimmin käytettyjä tekniikoita, joita siihen tarkoitetut sovellukset käyttävät. Ennalta valitut kolme sovellusta käydään myös näiltä osin läpi ja arvioidaan, kuinka ne vastaavat määritettyjä kriteereitä. Työn tehtävänä oli valita toimeksiantajalle kolmesta markkinoilla olevasta kaupallisesta sovelluksesta paras mahdollinen kriteerit täyttävä sovellus. Työ ei käsittele sovelluksen asennusta, testausta tai tuotantoon saattamista.

Yleisimmin käytetyt tekniikat käytiin yksityiskohtaisesti läpi. Sovellusten toiminnassa keskityttiin erityisesti niihin ominaisuuksiin, jotka olivat toimeksiantajalle tärkeimpiä. Liitteenä olevassa taulukossa vertailtiin toimeksiantajana asettamia kriteereitä sovelluksiin. Sovelluksen valintaan vaikutti kuinka se vastaa annettuja kriteereitä, lisenssien ominaisuudet, helppous ajatellen sovelluksen ostoa ja hinta.

Toimeksiantaja Neste Oil Oyj on jalostus- ja markkinointiyhtiö, joka keskittyy korkealaatuisiin puhtaamman liikenteen polttoaineisiin ja valmistaa kaikkia tärkeimpiä öljytuotteita. Liikevaihto vuonna 2013 oli 17,5 miljardia euroa, ja sen palveluksessa työskentelee noin 5 000 henkilöä. (Neste Oil 2014a.)

Porvoon jalostamo keskittyy korkealaatuisiin ja puhtaisiin liikenteen polttoaineisiin. Jalostamo aloitti toimintansa vuonna 1965. Neljä tuotantolinjaa ja yli 40 prosessiyksikköä muodostavat jalostamoalueen. Lähes miljardin euron investointeina 2000-luvulla jalostamolle on rakennettu ja käynnistetty kolme uutta prosessiyksikköä: dieseliä tuottava tuotantolinja 4 ja uusiutuvaa dieseliä tuottavat NEXBTL-yksiköt 1 ja 2. Raakaöljyn jalostuskapasiteetti noin 200 000 barrelia päivässä; koko tuotanto on noin 12,5 miljoonaa tonnia vuodessa. Raakaöljyn ja öljytuotteiden varastointitilaa on maan päällä kuin alla noin 7 miljoonaa kuutiometriä. Porvoon jalostamo sijaitsee Kilpilahden teollisuusalueella, noin 30 kilometriä Helsingistä itään päin Porvoon suuntaan. Koko teollisuusalueella työskentelee noin 3500 henkilöä, joista Nesteoililaisia noin 1900. (Neste Oil 2014a.; Neste Oil 2014b.)

2 Verkonvalvonta ja -hallinta

2.1 Käsitteenä

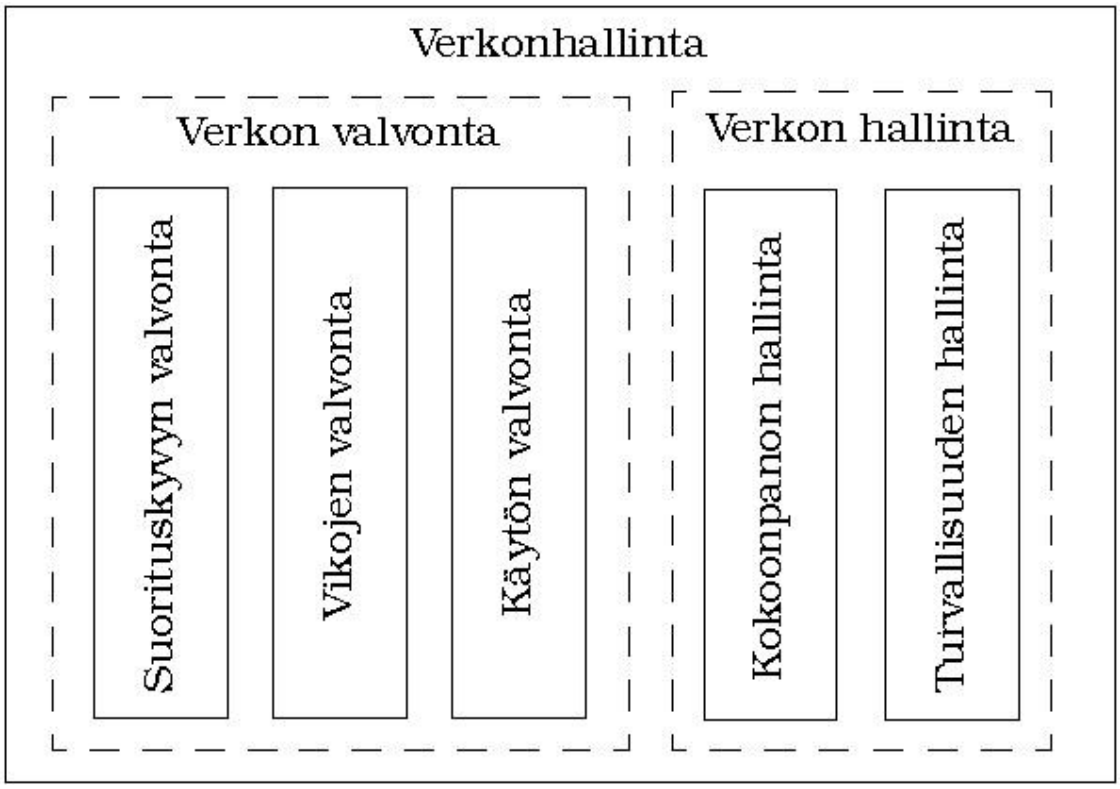
Verkonvalvonta ja -hallinta ovat kriittisiä IT-toimintoja laajoissa sekä tärkeissä yritys- ja tuotantoverkoissa. Parhaimmillaan tehokas valvonta sekä hallinta säästävät prosessin ja verkon kokonaiskustannuksia, lisäävät työntekijöiden ja prosessien tehokkuutta sekä antavat paremmat lähtökohdat vikatilanteiden ja ongelmien varalle. Ajatellaan esimerkiksi, että kuvitteellisen yrityksen verkossa on verkkovika, joka pysäyttää koko verkkoliikenteen. 1000 hengen organisaatiossa 2 % käyttökatkokset tarkoittavat 35 000 työtunnin menetystä vuodessa ja tähän lisäksi epäluotettavan toimittajan maine ja muut verkkovioista johtuvat ongelmat mahdollisille asiakkaille (Puska 2000, 306). Tilannetta helpottamaan on luotu verkonvalvonta ja -hallintasovellukset. Ne antavat kriittistä tietoa siitä, kuinka verkon eri osa-alueet, laitteet ja käyttäjät toimivat ja käyttävät verkkoa. Mitä tahansa verkkoa voidaan valvoa ja hallita, eikä laitteilla tai käyttöjärjestelmillä ole merkitystä. (Nash & Behr 2008.)

2.2 Osa-alueet

Puhuttaessa verkonhallinnasta tarkoitetaan sekä verkonhallintaa, että verkonvalvontaa (kuva 1). Valvonta ja hallinta ovat laajoja käsitteitä, joiden yleisiksi osa-alueiksi ITU-T:n verkonhallintastandardi X.700 määrittelee:

- Vikatilanteiden hallinta (Fault Management)
- Määrittelyjen hallinta (Configuration Management)
- Suorituskyvyn hallinta (Performance Management)
- Käytön ja laskutuksen hallinta (Accounting Management)
- Turvallisuuden hallinta (Security Management)

(Puska 2000, 306.)



Kuva 1. Verkonhallinta jaettuna osa-alueisiin (Hautaniemi 1994, 3)

Vikatilanteiden ennaltaehkäisy ja ennenaikainen havaitseminen ovat verkonvalvonnan ja -hallinnan yksi tärkeimmistä osa-alueista. Viat voivat aiheuttaa käyttökatkoksia tuotannon vaiheissa ja jo lyhyilläkin katkoksilla on taloudellisia vaikutuksia. Tästä syystä nopea reagointi ja ennaltaehkäisy ovat elintärkeitä. Vioista ja vikatilanteista kerättävien vikalokien tietoa voidaan hyödyntää kun verkkoa suunnitellaan, tehdään ostopäätöksiä tai harkitaan palveluiden ulkoistusta. (Puska 2000, 306.)

Verkkoelementtien määrittelytietoja seurataan määrittelyjen hallinnalla, jonka määrittelykantaa käytetään hyväksi vianeristyksessä, vianhaussa ja verkon suunnittelussa. Verkon elementtien ja komponenttien määrittelyllä on myös merkitystä tietoturvan kannalta. (Puska 2000, 306.)

Suorituskyvyn hallinnalla pyritään säilyttämään ja ylläpitämään verkon suorituskyky optimaalisella tasolla. Suorituskyvyn mittaamiseen käytetään usein helposti mitattavia suureita kuten verkon kapasiteettia eli onko verkko riittävän kyvykäs siltä vaadittuihin toimintoihin ja verkon kuormitusastetta. Käyttäjän kannalta on tärkeintä, kuinka nopeasti verkko vastaa, eli niin sanottu vasteaika. (Puska 2000, 306.)

Käytön hallinta on oleellinen osa verkonhallintaa lähiverkoissa. Lähiverkon käyttötietoja voidaan hyödyntää kapasiteettisuunnittelussa tai käyttäjäkohtaisien rajoitusten toteuttamisessa (kuten levytilarajoituksissa tai oikeuksien määrittelyssä). (Puska 2000, 307.) Käytön hallintaan olennaisesti liittyvän turvallisuuden hallinnan tarkoituksena on kontrolloida verkkoresurssien käyttöä; tietyillä henkilöillä on pääsy tiettyyn materiaaliin. Esimerkkinä yrityksen Internetsivut ovat kaikkien käytettävissä, sisäinen Intranet sivusto on vain yrityksen työntekijöiden käytössä, mutta laskutuksen tai henkilöstöhallinnon salaisiin tietoihin on pääsy vain tarkasti rajatuilla henkilöillä. (Puska 2000, 307.)

X.700-standardi kattaa verkot laidasta laitaan. Lähiverkkojen hallinnassa on painotus eri osa-alueilla (vian-, suorituskyvyn-, turvallisuuden- ja määrittelyjen hallinta) kuin esimerkiksi yleisen puhelinverkon operoinnissa, jossa laskutuksen- ja käytön hallinta ovat suuressa roolissa. Standardi kuvaa kattavasti kaikki osa-alueet. On selvää, ettei kaikkia osa-alueita voida toteuttaa yhdellä järjestelmällä tai sovelluksella. Tosin tällä hetkellä markkinoilla olevat verkonvalvonta ja -hallintasovellukset ovat kyvykkäitä valvomaan monia eri osa-alueita ja osittainen verkon määritysten hallinta on myös mahdollista. (Puska 2000, 307.)

2.3 Verkonvalvonta

Verkonvalvontaan sisällytetään verkonhallinnan osa-alueista suorituskyvyn hallinta, vikojen hallinta ja käytönhallinta. Näistä keskeisimmät ovat verkonvalvonnan kannalta suorituskyvyn hallinta ja vikojen hallinta. Verkonvalvonnan tärkeimpiä ominaisuuksia on varautua ennaltaehkäisemään ja havaitsemaan ongelmat riittävän ajoissa. Tästä syystä verkkoa monitoroitaessa ja valvoessa tulee keskittyä verkon suorituskyvyn mittaamiseen, laitteiden käyntiaikaan ja palveluiden saatavuuteen. Mittaamalla suorituskykyä on mahdollista kiinnittää huomiota ajoissa, jos jokin verkon osa-alue ruuhkautuu tai jokin verkkolaite on ylikuormittunut. Näin siihen voidaan reagoida ennaltaehkäisevästi, ennen kuin tilanteesta aiheutuu suurempia ongelmia, jotka mahdollisesti haittaa työntekoa. Esimerkiksi palvelin, joka on ollut pitkään yhtäjaksoisesti päällä, saattaa aiheuttaa verkkoon hidastumista tai palvelukatkoksia. Näin ollen käyntiaikaa on syytä tarkkailla. Verkonvalvontaohjelmalla voidaan suorittaa testejä eri palveluita tai resursseja vastaan ja näin todentaa niiden toiminta. Mikäli jokin palvelu ei vastaa, ohjelma ilmoittaa siitä. On myös mahdollista esimerkiksi seurata palvelimen tietoja tarkemmin, kuten palvelimen työmuistin (RAM muisti) tai kiintolevyn tilankäyttöä. Ohjelmiin voidaan asettaa resursseille erilaisia ”liipaisuarvoja” eli rajoja. Rajan ylittyessä ohjelma informoi muutoksista hälytyksellä tai raportilla. (Feldman 1999, 362.)

3 Yleisimmin käytetyt tekniikat

Verkonvalvonta ja -hallinta tulee toteuttaa niin, että sitä voidaan soveltaa useaan eri teknologiaan ja sen rakenne on avoin. Näin mahdollistetaan useiden järjestelmien ja erilaisten laitteiden välinen toiminta. Kuitenkin toteutukseen liittyy kolme keskeistä tekniikkaa: SNMP–protokolla (Simple Network Management Protocol), RMON (Remote Monitoring) ja MIB-tietokannat (Management Information Base). (Jaakohuhta 2002, 312, 314.)

Verkonvalvontasovellukset valvovat sovelluskerrokseen kuuluvia internet-protokollia. Yleisin TCP/IP-verkkojen valvonnassa käytössä oleva tietoliikenneprotokolla on SNMP. Protokolla mahdollistaa kyselyjen välittämisen yksittäisille laitteille valvontasovelluksen avulla tai laite voi itsenäisesti antaa tietoja itsestään. SNMP protokolla hyödyntää MIB tietokantaa, joka sisältää MIB objekteja, jotka sisältävät tiedon esimerkiksi siitä, mitä tietoa jokin laite vastaa tai välittää. Tämä opinnäytetyö perehtyy sovelluksiin, jotka pystyvät valvomaan TCP/IP-verkkoja käyttäen SNMP protokollaa, joka on yksi tärkeimmistä toimeksiantajan määrittämistä kriteereistä. (DenHartog 2010; Cisco 2002, 1.)

3.1 SNMP

3.1.1 Yleisesti

SNMP verkonhallintakäytäntö on valmistajariippumaton. Sen ensisijainen tehtävä on määritellä verkonvalvonta ja -hallintaohjelmiston toiminnot ja selittää raporttien määrittelyt sekä miten ne on lähetetty. Lisäksi käytäntö määrittelee lähetettävän laitteen viestin muodon sekä yrittää korjata, että välttää virheitä. (Jaakohuhta 2002, 312.)

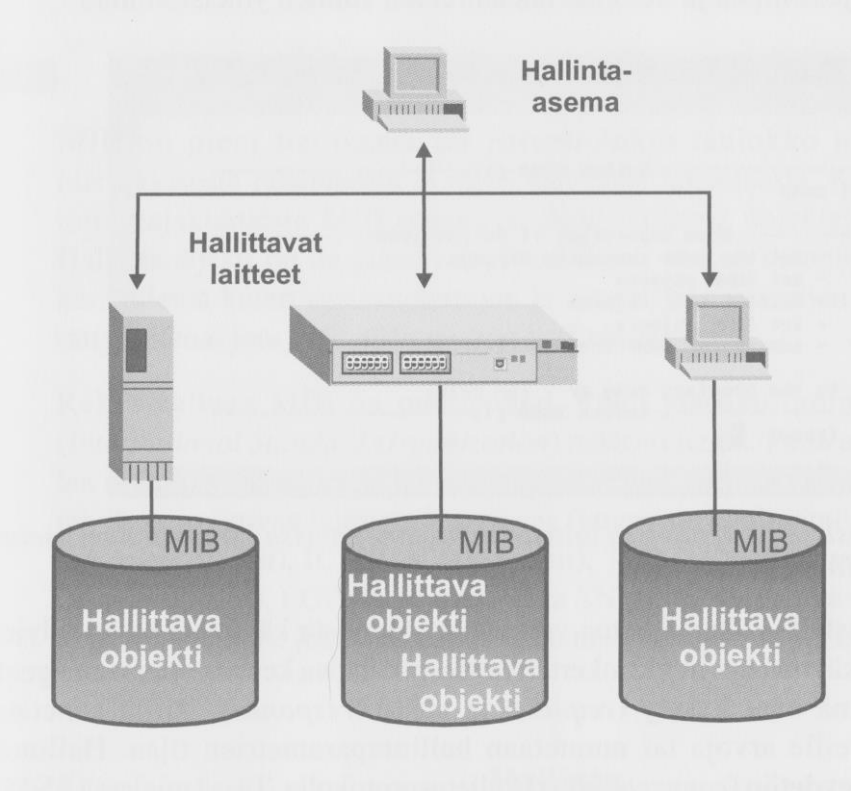
SNMP kehitettiin jo vuonna 1988 Yhdysvalloissa yhteistyössä DoD:n (United States Department of Defense), teollisuuden ja akateemisten yhteisöjen kanssa. Siitä on kehitetty kolme versiota. Ensimmäinen SNMPv1 on vuodelta 1990, toinen SNMPv2 on vuodelta 1993 ja kolmas eli uusin versio SNMPv3 vuodelta 2002. Uusin SNMPv3 on yleistymässä edellisiä versioita paremman tietoturvan ansiosta. (Jaakohuhta 2002, 312.)

3.1.2 Toiminta

TCP/IP-protokollaperheen sovelluskerroksen SNMP on keskeisin verkonvalvonnassa ja -hallinnassa käytettävä protokolla. Seuraavat komponentit määrittelevät tyypillisen SNMP käyttöympäristön:

- Agentti, joka kerää tietoja valvottavista ja hallittavista laitteista, kuten kytkimistä ja reitittimistä. Laitteiden toiminnasta kerätty tieto välitetään SNMP protokollaa käyttäen hallintatyöasemalle (management console).
- Hallintajärjestelmä kerää valvottavien ja hallittavien laitteiden agenteilta tiedot.
- SNMP protokolla, joka sisältää kyselykielen ja sen tehtävä on välittää laitteiden agenteilta saatu tieto hallintatyöaseman hallintajärjestelmään käyttäen UDP (User Datagram Protocol) protokollaa.
- Laitteet jotka eivät sisällä omaa agenttia tarvitsevat proxy-agentin. Se on erillinen laite, joka sisältää agentin ja tuen SNMP:lle.
- Asiakas-palvelin (client-server) arkkitehtuurissa agentti on palvelin ja hallintasovellus on asiakas.

(Jaakohuhta 2002, 312-313.)



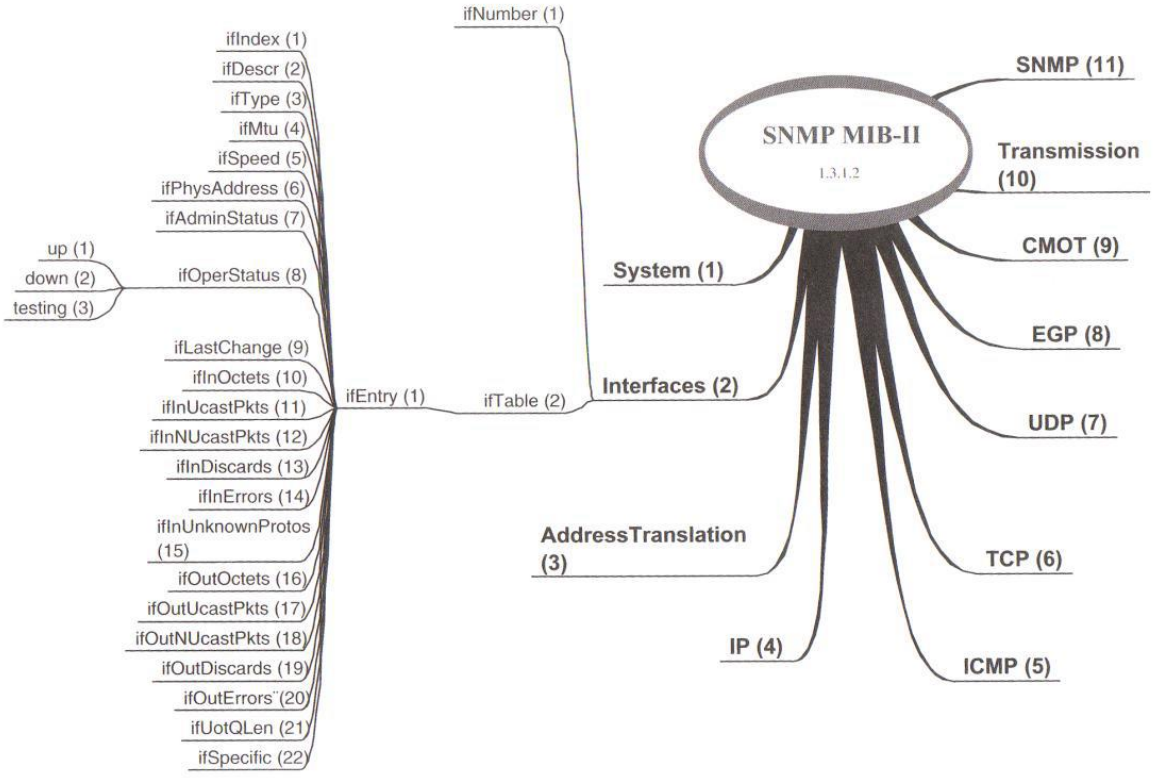
Kuva 2. SNMP ympäristön rakenne (Jaakohuhta 2002, 313.)

SNMP:n tarkoitus on toimia taustalla huomaamattomasti ja kerätä käyttäjän määrittelyjen mukaan tietoja verkosta. Viestintätekniikka, jolla se keskustelee agenttien kanssa, on hyvin yksinkertainen kysely (request) ja vaste (response) tekniikka. Protokollana SNMP on yhteydetön (connectionless) kuljetusprotokolla, jonka seurauksena se on tehokas ja pystyy toimimaan vaikka verkossa olisi huomattavaa kuormaa. (Jaakohuhta 2002, 314.)

3.2 MIB

MIB on hierarkkinen pieni tietokanta hallittavien objektien rakenteesta ja hallinnan rakenteesta. Kannassa esiintyviä rekisteröityjä yleisiä ja toimittajakohtaisia MIB-objekteja tunnetaan yli 1000. Hallintaobjekti kuvaa loogisesti todellisen verkon rakennetta. Objekti kerää tietoa esimerkiksi vastaanotettujen ja lähetettyjen pakettien määrää sekä ylläpitää tietoa. Näitä objektien keräämiä tietoja välitetään SNMP:n avulla hallintatyöasemalle. (Jaakohuhta 2002, 315.)

Kannan rakenne on puumainen ja sen yläosan ominaisuudet ovat ISO:n (International Standard Oraganization) määrittelemiä. Alemmat tasot määrittelevät eri organisaatiot ja laitetoimittajat. ISO:n määrittelemä ylin taso sisältää objektiryhmiä system (laitteet), interface (verkkoliitäntöjen liikenne), IP (IP-pakettien tilastot), ICMP (ICMP-viestit), TCP (TCP-liikennetilastot), UDP (UDP-liikennetilastot), EGP (EGP-tilastot) ja SNMP (SNMP-liikennetilastot). (Jaakohuhta 2002, 315.)



Kuva 3. Puumainen MIB tietokanta, jossa objektit ja SMI rakenne (Puska 2000, 310.)

MIB:en liittyy olennaisesti SMI (Structure Management Information) –tietorakenne. Se tunnistaa tietotyyppejä ja datan esitystapoja. Lisäksi se määrittelee hierarkkisen nimirakenteen, jolla hallittavat objektit tunnistetaan. MIB puu sisältää useita yksittäisiä tietoja laitteesta eli objekteja. SMI määrittää siis säännöt, kuinka MIB objektit rakennetaan, kuva-

taan ja järjestetään. Se mahdollistaa toisistaan eriävien laitteiden kommunikoinnin varmistamalla, että ne käyttävät universaalia esitystapaa hallintatiedoille. (Jaakohuhta 2002, 316; Kozierok 2005.)

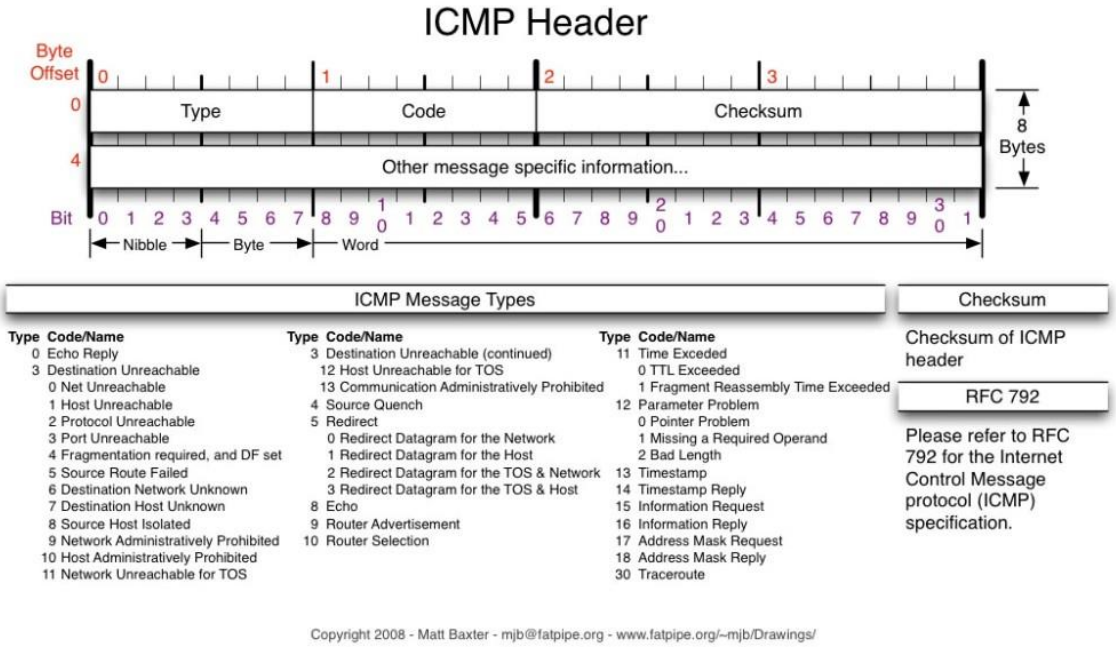
3.3 RMON

RMON kehitettiin alun perin korvaamaan SNMP:n puutteita, mutta nyt niitä käytetään yhdessä. Suuri ongelma SNMP:tä käytettäessä on, että se ruuhkauttaa ja pahimmassa tapauksessa ylikuormittaa verkkoa jatkuvilla kyselyillään. Tämä seikka tulee ottaa huomioon, kun ajatellaan toimeksiantajan suuria verkkokokonaisuuksia. Turha liikenne verkossa saattaa aiheuttaa jonkin kriittisemmän tiedon välittymisen vaaraan. Sekä RMON, että SNMP käyttävät molemmat agentteja eli yleisesti keruuyksiköitä (probe). RMON on erillinen laite tai ohjelmisto, joka on asetettu verkon laitteeseen keräämään ja tallentamaan tietoa verkkoliikenteestä MIB tiedostoon/kantaan. Kun SNMP hallinta-aseman on jatkuvasti käytävä tutkimassa agenttejaan niin RMON mahdollistaa, että kerättyä tietoa voidaan tarkastella myöhemmin historiaan perustuen. Näin tiedon keruu ei ruuhkauta verkkoa ja kerätty tieto voidaan välittää kokonaisuutena hallinta-asemalle. (Jaakohuhta 2002, 316-317.)

Yleisimmin RMON sijoitetaan verkossa osaksi kytkintä, reititintä tai jakajaa. Hallinta-asema ei jatkuvasti tutki keruuyksiköitä eli agentteja. vaan vasta sitten kun yksiköillä on jotain kerrottavaa. Keruuyksiköt ovat palvelimia ja hallinta-asemat asiakkaita, jos asiaa ajatellaan asiakas-palvelin -suhteessa. SNMP:n tehtävä on siis välittää tietoa RMON agenttien ja hallinta-aseman välillä. (Jaakohuhta 2002, 317.)

3.4 ICMP

ICMP-protkolla on tarkoitettu välittämään verkkoon kytkettyjen laitteiden välisiä virhe-, ohjaus- ja muita viestejä. Toimeksiantajan laajoissa prosessiverkoissa esimerkiksi tilanne jossa paketti ei välity sille määrättyyn kohteeseen tai verkossa on ruuhkaa ja kapasiteettia ei ole on erittäin kriittistä. ICMP on osa IP-protokollaa ja esiintyy kaikissa IP-moduuleissa. ICMP-sanomilla on oma rakenne ja jotta sanomat voidaan erottaa toisistaan, kaikkien sanomien alussa on kahdeksan bittiä pitkä tyyppikenttä. Tämän kentän arvolla kerrotaan mistä sanomassa on kyse. Kaikkiaan ICMP-sanoma sisältää tyypin, koodin, tarkistussumman ja yleisen kentän. Koodikenttä tarkentaa viestityypille ominaisia määrittelyjä, tarkistussummaa käytetään tarkistamaan paketin eheys ja yleisessä viestikentässä määritellään muu viestiin liittyvä informaatio. (RFC792 1981,1-5.)



Kuva 4. ICMP-sanoman rakenne (Baxter 2008.)

3.5 NetFlow

NetFlow on Cisco Systemsin kehittämä protokolla, jota käytetään keräämään IP liikenteestä tietoa ja monitoroimaan verkon liikennettä. NetFlowsta on tullut käsite ja standardi, mutta monet muut valmistajat käyttävät vaihtoehtoisia vastaavanlaisia tekniikoita, kuten esimerkiksi Juniper Jflow:ta, 3Com/HP, Dell ja Netgear Sflow:ta, Huawein NetStreamia, Alcatel-Lucenta Cflow:ta ja Ericsson Rflow:ta. (Hale 2012.)

NetFlow esiteltiin ensimmäisen kerran vuonna 1990 ja on sen jälkeen saanut yhdeksän uuta versiota. Ensimmäinen versio on nykypäivänä vanhentunut ja rajattu ainoastaan IPv4:n käyttöön ilman IP maskeja ja AS numeroita. Seuraavat versiot aina neljänteen asti olivat Ciscon omia sisäisiä versioita, joita ei koskaan julkaistu. Viides ja yleisin käytössä oleva NetFlow versio julkaistiin vuonna 2009 ja se on käytössä monilla eri reititin valmistajilla, mutta se on rajattu vain IPv4:lle. Versioita on kaiken kaikkiaan kymmenen ja jokainen tuo hieman lisää ominaisuuksia. Käytetyimmät kaksi versiota ovat kuitenkin edelleen viisi ja yhdeksän, yhdeksäs versio toi tuen IPv6:lle. (Hale 2012.)

Reitittimet ja kytkimet, jotka tukevat ja käyttävät NetFlow tekniikkaa, keräävät IP liikenteen tietoja kaikista käyttöliittymistä, joissa NetFlow on kytkettynä päälle. Myöhemmin ne välittävät tiedot NetFlow tallenteina vähintään yhdelle NetFlow kerääjälle. Kerääjänä yleisimmin on serveri, joka tekee varsinaiset analyysit tiedoille ja esittää ne käyttäjäystävällisessä muodossa. Kerääjät voivat olla rautapohjaisia, luotain tyyppisiä tai sovelluspohjaisia. (Hale 2012.)

NetFlown avulla valvominen ja tiedon analysointi antaa arvokasta tietoa verkon käyttäjistä ja sovelluksista, ruuhka-ajoista ja liikenteen reitittymisestä. Tämä on erityisen tärkeää, kun ajatellaan toimeksiantajan verkkoja ja niiden optimointia, sekä suorituskyvyn parantamista. Tavalliseen SNMP tekniikkaan verrattuna NetFlow mahdollistaa tietyn sovelluksen tai käyttäjän käyttämän verkkoliikenteen tunnistamisen. Se ymmärtää millaisia kaavoja verkossa tapahtuva liikenne noudattaa sekä tarjoaa kokonaisvaltaisen kuvan verkon käyttämästä kaistasta ja WAN (Wide Area Network) liikenteestä. NetFlow tukee myös CBQoS (Class Based Quality of Service) vahvistusta ja suorituskyvyn valvontaa. Lisäksi sitä voidaan hyödyntää verkkoliikenteen ongelmien selvittämisessä ja sisäisen valvonnan raporteissa. (Hale 2012.)

3.6 Packet Sniffing

Packet sniffer eli paketinhaistelija on ohjelma, jolla pystytään havaitsemaan ja keräämään paketteja, jotka liikkuvat yli sen verkon, johon ohjelma on liitetty. Paketit sisältävät erilaisia tietoja liikenteestä. Tarvittaessa ohjelma purkaa paketin pienemmiksi osiksi ja kertoo yksityiskohtaisemmin sen sisällön. Näitä havaittuja ja analysoituja tietoja voidaan käyttää verkon tiedonsiirto-ongelmien ratkaisemiseen, väärien verkkoasetusten havaitsemiseen tai haittaohjelmia sisältävien koneiden havaitsemiseen. Toimeksiantajan verkoissa on tärkeää pystyä havaitsemaan väärät verkkoasetukset, koska ne saattavat vaikuttaa koko prosessiverkon toimintaan negatiivisesti. Lisäksi verkoissa on liitettynä monia työasemia, jolloin haittaohjelmien mahdollisuus lisääntyy ja niiden välittämä liikenne kuormittaa verkkoja turhaan. (Crenshaw 2008.)

Toimiakseen oikein sen tietokoneen verkkokortti, jossa paketinhaistelijaohjelma on, tulisi olla asetettu ”umpimähkäisyys -tilaan” (promiscuous mode). Tämä tarkoittaa siis sitä, että verkkokortti kerää kaiken tiedon joka verkossa liikkuu, eikä vain niitä jotka ovat osoitettu sen MAC-osoitteelle (Media Access Control). Paketinhaistelijaohjelmat eivät toimi verkoissa, joissa tieto kulkee kytkimien välityksellä. Jotkin kytkimet tosin voidaan huijata peilaamaan kaikki niihin tuleva liikenne, jolloin tiedot on mahdollista havaita ohjelman avulla. (Crenshaw 2008.)

3.7 WMI

WMI (Windows Management Instrumentation) on Windows pohjaisille käyttöjärjestelmille kehitetty hallintatietojen ja operaatioiden infrastruktuuri. WMI:llä on mahdollista kirjoittaa komentosarjoja tai luoda ohjelmia, joilla voidaan ajaa hallinnollisia tehtäviä etäkoneilla. WMI:tä voidaan hyödyntää verkonvalvontatietoja keräämisessä Windows-pohjaisilta etä-

koneilta. Pääasiassa sitä käytetään kuitenkin erilaisten yrityssovelluksien komentosarjojen ja hallinnollisten komentosarjojen luomisessa. WMI käyttää CIM (Common Information Model) standardia määrittäessään järjestelmien, ohjelmien, verkkojen, laitteiden ja muita valvottavia komponentteja. Toimeksiantajan verkoissa esiintyy paljon Windows pohjaisia laitteita, joita ei välttämättä käytä tai valvo yhtäjaksoisesti kukaan. Mahdollisuus tarkkailla ja hallita laitteita etänä on elintärkeää, kun ajatellaan vikatilanteiden ennaltaehkäisyä ja vikatilanteiden selvittämistä. (Microsoft 2014.)

WMI mahdollistaa verkonhallintatietoihin käsiksi pääsemisen määrittelemällä ohjelmassa valvottavan Windows koneen kirjautumistiedot. Koneeseen, johon etäyhteys on luotu, kerätään hallintatietoja, jotka on erikseen määritelty käytettävässä ohjelmassa. WMI:tä hyödyntävässä ohjelmassa voidaan lisäksi toteuttaa hallinnollisia tehtäviä, esimerkiksi käynnistää etähallittava laite uudestaan tai sammuttaa se.
(Microsoft 2014.)

3.8 WBEM

Kaikki nykyaikaiset verkonvalvonnassa ja -hallinnassa käytettävät työkalut perustuvat HTTP-protokollaan (Hypertext Transfer Protocol). Nämä työkalut käyttävät Internet-protokollia ja tunnettuja web-tekniikoita kuten HTML, JavaScript, PHP ja niin edelleen. Nykyaikaiset hallittavat älylliset laitteet sisältävät web-palvelimen, joka välittää tiedot käyttäjän työkalulle, joka toimii selainohjelmalla. Selaimen avulla toteutettu hallinta tunnetaan nimellä WBEM (Web-Based Enterprise Management). WBEM on kehitetty yhteistyössä yli 60 merkittävän laite- ja ohjelmistovalmistajan toimesta. Sen tavoitteena on ollut täydentää SNMP:tä ja DMI:tä (Desktop Management Interface). Kaiken selainpohjaisen, kuten myös WBEM-hallinnan ongelmana on haasteellinen tietoturva. Mahdolliset välimieshyökkäykset ja väärinkäytökset pystytään kuitenkin eristämään pois riittävillä palomuuriratkaisuilla, tiukalla käyttäjäpolitiikalla ja mahdollisesti eristämällä verkko. Nykyaikaiset työkalut ovat myös kehittyneet tietoturvan osalta niin, että monet sovellukset pystyvät salaamaan välitetyt tiedot esimerkiksi SSL:llä (Single Socket Layer) ja RSA-salauksella. Tieturvan tärkeyttä tärkeissä prosessiverkoissa ei voi väheksyä. Tietoturva onkin tästä syystä tärkeä ominaisuus toimeksiantajalle valitussa sovelluksessa. (Jaakohuhta 2002, 321.)

4 Sovellusten vertailu

4.1 Kohde

Opinnäytetyön kohteena oli Neste Oilin Porvoon jalostamon verkonvalvonta ja hallintasovellus. Nykyisen sovelluksen käyttöikä oli tullut tiensä päähän ja suunnitteilla oli ollut jo pitkään uuden sovelluksen hankinta. Nykyinen WhatsUp Gold sovelluksen versio ei pystynyt enää palvelemaan tarpeita, joita suuren lähiverkon ja lukuisten erillisverkkojen valvonta ja hallinta vaativat. Nykyaikaiset verkonvalvonta ja -hallintasovellukset ovat pitkälle automatisoituja ja helposti käyttöön otettavia suurissakin kokonaisuuksissa.

4.2 Kriteerit

Sovelluksille määritetyt vaatimukset voidaan jakaa karkeasti kahteen osaan; toiminnallisiin ja ei-toiminnallisiin vaatimuksiin. Toiminnalliset vaatimukset kuvaavat millaisia toimintoja sovellukselta halutaan ja mitä vaatimuksia sen olisi täytettävä. Ei-toiminnalliset vaatimukset liittyvät suorituskykyyn, kuten vaste- ja käyttöaikaan, lisenssien ominaisuuksiin ja helppokäyttöisyyteen.

Toimeksiantajan laatima määrittely valittavan sovelluksen ominaisuuksista määritti tietysti suurimmaksi osaksi lopullisen ohjelman valinnan. Heidän tarve oli hankkia nykyaikainen verkonvalvonta ja -hallintaohjelmisto, jonka olisi kyettävä valvomaan verkon suorituskykyä ja havainnoimaan vikoja. Sen tuli lisäksi mahdollistaa erilaisten näkymien luonti eri käyttäjille ja käyttäjäryhmille heidän omasta valvottavasta verkostaan. Syitä tähän oli, että erillisverkoille saatiin parempaa vasteaikaa ja asiakastyytyväisyyttä, kun mahdolliset viat ja liikenteen pullonkaulat havaittaisiin välittömästi tai jopa etukäteen. Porvoon jalostamon valvottava ja hallittava verkko koostuu b-luokan osoiteavaruudesta aliverkkoineen, mutta sovellusta tuli myös pystyä käyttämään privaattiverkoissa. Lisäksi sovelluksen tuli myös olla laajennettavissa myöhemmin muihin toimipaikkoihin, kuten Naantaliin tai ulkomaiden toimipaikoille. Haluttuja ominaisuuksia oli myös mahdolliset valmiit kielivaihtoehdot englannin lisäksi, käyttäjäryhmien ja profiilien luonti, web-pohjainen käyttöliittymä, raportointityökalut, sähköposti ja tekstiviesti hälytykset sekä riittävä tietoturva. Sovellukseen tuli myös pystyä lisäämään noin tuhat laitetta / valvottavaa määrettä ja sen tuli olla myös laajennettavissa tältä osin. Näiden haluttujen kriteerien lisäksi, listasin liitteeseen laatimaani vertailuun joitain kriteereitä, jotka mielestäni olivat tärkeitä sovellusta valittaessa.

Ennalta annettujen kriteerien ja silmämääräisen tarkastelun pohjalta valitsin tarkasteluun kolme erilaista, mutta samantyylistä verkonvalvontaan ja -hallintaan tarkoitettua sovellusta. Paesslerin PRTG Network Monitor, Ipswitchin WhatsUpGold ja Nagios Enterprisesin

Nagios XI edustavat kaikki kaupallisia suurien yritysten luomia sovelluksia, jotka ovat tarkoitettu suurten ja keskisuurten yritysten käyttöön. Jokainen toimittaja tarjoaa täyden asiakastuen, kattavat dokumentaatiot ja jatkuvan ylläpidon sovelluksilleen. Sovelluksien toimittajat tarjoavat pienempiä ja yksinkertaisempia ratkaisuja sovelluksistaan pienyrityksille ja yksityisille henkilöille sekä myös ilmaisia kokeiluversioita.

WhatsUp Gold edusti Neste Oilin nykyisen sovelluksen uusinta versiota, joka sinällään oli riittävä syy siihen miksi se otettiin mukaan opinnäytetyöhön. Nagios XI pohjautui vapaaseen lähdekoodiin, joka on räätälöity suurille yrityksille suunnatuksi kaupalliseksi ratkaisuksi. Mielestäni on aina hyvä tarkastella vapaaseen lähdekoodiin pohjautuvia vaihtoehtoja. PRTG edusti suurille yritykselle suunnattua ratkaisua, joka on saanut hyviä arvosteluja ja positiivista julkisuutta verkonvalvontaa ja -hallintaa käsittelevillä sivustoilla ja artikkeleissa.

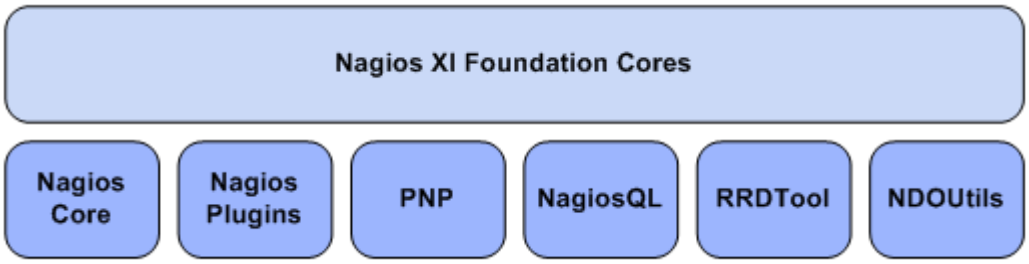
4.3 Menetelmä

Näistä sovelluksista paras valittiin puhtaasti tutkimustyyppisesti vertailemalla niitä keskenään liitteenä olevassa taulukossa (Liite 1). Se, joka vastasi parhaiten toimeksiantajan asettamia kriteereitä, tuli valituksi. Lisäksi valintaan vaikutti sovelluksen hinta, lisensointi ja käyttöönoton helppous.

4.4 Nagios XI

Nagios XI on tehokas yritystason IT infrastruktuurin valvontaan ja hallintaan käytettävä sovellus. Nagios XI hyödyntää Nagioksen avoimen lähdekoodin komponentteja tarjoillakseen parhaan ja monipuolisen valvonta ja hallinta ratkaisun tämän päivän vaativille organisaatioille ja ympäristöille. Se on suunniteltu skaalautuvaksi ja joustavaksi sovellukseksi, jonka tarkoitus on pitää ongelmalliset IT valvonta tehtävät yksinkertaisina, samalla kuitenkin säilyttäen monet sen ominaisuudet käytettävissä. Nagios XI voidaan yhdistää saumattomasti Nagios Network Analyzer, Incident Manager ja Fusion sovelluksiin. Näin pystytään luomaan kaiken kattava tietojärjestelmien valvonta ja verkonvalvonta ja -hallinta ympäristö. (Nagios 2014a.)

Kuten jo aikaisemmin on sanottu, sovelluksen perusta koostuu muutamista hyvin tunnetuista ja arvostetuista vapaan lähdekoodin Nagios komponenteista ja lisäosista.



Kuva 5 Nagios XI:n ytimen koostuminen. (Nagios 2014e.)

- Nagios Core hoitaa valvonta toimintoja.
- Nagios Plugins hoitaa sovelluksien, palveluiden ja mittarien valvonnan.
- PNP tuottaa RRD työkalu pohjaisia kuvaajia valvonta datasta.
- NagiosQL on pohja kehittyneelle web-konfiguroinnin graafiselle käyttöliittymälle.
- MRTG valvoo yhdessä RRD työkalun kanssa käyttöliittymän kaistaa.
- NDOUtils käsittelee valvonta toimintojen tietokannan backendiä

(Nagios 2014f.)

4.4.1 Ominaisuudet

Ominaisuuksiltaan Nagios XI vastaa hyvin toimeksiantajan määrittelemiä kriteereitä. Alla on listattuna sovelluksen vahvimmat osa-alueet ja ominaisuudet, jotka tuovat sille lisäarvoa. Määritetyissä kriteereissä ei ollut tuotu esille laajennettavaa arkkitehtuuria, mutta sovellukset tarjoamat useat ohjelmointirajapinnat (API) tarjoavat yksinkertaisen integraation sisäisten- ja kolmansien osapuolien sovelluksien kanssa. Sadat yhteisön luomat lisäosat sekä laajentavat valvonta- ja hälytystoimintoja, että mahdollistavat sovelluksen räätälöimisen paremmin organisaatiolle. (Nagios 2014a; Nagios 2014b.)

- Kattava IT infrastruktuurin valvonta:
  Mahdollistaa kaikkien kriittisten komponenttien valvonnan, kuten esimerkiksi sovellusten, palveluiden, käyttöjärjestelmien, verkkoprotokollien, järjestelmätietojen ja verkon infrastruktuurin. Sadat kolmansien osapuolien tuottamat lisäosat mahdollistavat lähes minkä tahansa sisäisen sovelluksen, palvelun tai systeemin valvonnan.
- Näkyvyys:
  Kyvykäs pääkonsoli antaa hyvän näkymän koko verkosta, palveluista, prosesseista ja laitteista. Tehokas konsoli ja erilliset näkymät mahdollistavat nopean pääsyn valvontatietoihin ja dataan.
- Hälytykset:
  Hälytykset voidaan välittää yksilöidyille käyttäjille sähköpostilla tai tekstiviesteillä.

- Ennakoiva suunnittelu:
  Automaattiset kehityssuunnan ja kapasiteetin arvioinnin grafiikat tarjoavat mahdollisuuden suunnitella etukäteen laite- ja systeemipäivitykset ennen kuin ne vanhenevat yllättäen.
- Muunneltavuus:
  Graafinen käyttöliittymä mahdollistaa näkymien, asettelujen ja tietojen määrittämisen yksilökohtaisesti jokaiselle käyttäjälle.
- Helppokäyttöisyys:
  Integroitu web-pohjainen konfigurointi käyttöliittymä antaa pääkäyttäjille mahdollisuuden jakaa valvonta-asetusten, systeemiasetusten ja muiden asetusten oikeuksia loppukäyttäjille. Ohjatut asennukset opastavat käyttäjää uuden laitteen, palvelun tai sovelluksen valvonnan lisäämisessä ilman, että käyttäjän tarvitsee ymmärtää monimutkaisia valvontakonsepteja ja asetuksien määrittelyjä.
- Käyttäjien ja näkymien hallinta:
  Käyttäjien pääsy webnäkymään tarjoaa nopeasti informaatiota verkon tilasta. Käyttäjäkohtaiset näkymät varmistava, että käyttäjät näkevät vain heille tarkoitetut näkymät. Kehittynyt käyttäjähallinta yksinkertaistaa käyttäjien ja roolien hallinnan ja tekee siitä helppoa. Uusien käyttäjien määrittämiseen vaaditaan vain muutama klikkaus ja käyttäjät saavat automaattisesti sähköpostissa kirjautumistiedot.

(Nagios 2014a; Nagios 2014b.)

Nagios XI:n monipuolisuus ja laajennettavuus ovat sen vahvuus, mutta samalla sen heikkous toimeksiantajan kriteerien valossa. Jotta sovelluksesta saadaan kaikki hyöty irti, on siihen asennettava erilaisia lisäosia. Monet lisäosat ovat kolmansien osapuolien laatimia ja ne eivät välttämättä toimi uusimpien versioiden kanssa. Kriittisissä verkoissa on pystyttävä luottamaan, että sovellus toimii moitteetta.

4.4.2 Toiminta

Asetusvelhot helpottavat käyttäjää ottamaan käyttöön koko infrastruktuurin ja sen kriittisimpien osien valvontaan tarvittavia komponentteja ja työkaluja. Uusien asetusvelhojen asentaminen on helppoa ja niitä on monia erilaisia esimerkiksi juuri tietylle kytkintyypille omansa. Velhon tarkoitus on siis asentaa sovellukseen uusi elementti, jolla pystytään valvomaan ja hallitsemaan haluttua ominaisuutta tai laitetta. (Nagios 2010d; Scott 2014.)

Jonkinlaiseen käyttöjärjestelmään pohjautuvissa laitteissa valvonnan käyttöönotto on kuitenkin hankalaa. Erilaiset valvonta- ja hallintaelementit vaativat tietynlaisia esiasennuksia ennen kuin ne voidaan asettaa käyttöön. Näille tulee asentaa NCPA (Nagios Cross Plat-

form Agent), jonka tehtävänä on olla linkki isäntä laitteen ja valvottavan laitteen välillä. Agentti välittää halututut tiedot valvottavalta laitteelta sovellukseen. NCPA:ta voidaan käyttää niin Windows käyttöjärjestelmään pohjautuvissa laitteissa kuin Linux RPM (Red-Hat Package Manager) ja DEB (Debian package management) pakettienhallintajärjestelmän omaavissa käyttöjärjestelmissä ja tarball tiedostoarkistoja käyttävissä käyttöjärjestelmissä. NCPA voidaan asentaa myös Mac OS X:lle mutta se ei ole täysin vakaa. Tämä hidastaa ja vaikeuttaa sovelluksen hyödyntämistä. (Nagios 2014c; Scott 2014.)

Sovelluksella on mahdollista valvoa laitteita sekä aktiivisilla, että passiivisilla tarkistuksilla, vaikka ne olisivat palomuurin takana. (Nagios 2014c.)

4.4.3 Kyselyjen ja web-sovelluksen tietoturva

Nagios XI:n etäagenttien turvaaminen on tärkeää, sillä esimerkiksi NRPE agentilla pystytään esittämään kyselyjä jotka tarkastavat järjestelmän kuorman ja levynkäytön. Agentit voidaan määritellä niin, että ainoastaan tietty IP osoite pystyy suorittamaan kyselyn tietyllä asiakkaalla. Agentteja ei tulisi myöskään koskaan suorittaa pääkäyttäjänä. Aina, kun liikennöidään verkkojen yli, tulisi miettiä kuinka siitä saadaan turvallisempaa. Useimmat agentit sallivat SSL salauksen. Jotta sovelluksen monitorointi serveri ja itse ympäristö voidaan suojata riittävän hyvin, joudutaan siihen asentamaan erillisiä lisäosia. Eikä varsinaisesti sovellus itse tarjoa suoraan mahdollisuutta parantaa web-sovelluksen tietoturvaa, vaan se on riippuvainen web-palvelimen tietoturva-asetuksista. (Keys 2014; Nagios 2014h.)

Suurin web-sovelluksen tietoturvaan vaikuttava asia on yksittäisille käyttäjille ja käyttäjäryhmille määritetyt oikeudet. Sovellus mahdollistaa erilaisten turvallisuustasojen luomisen ja ainoastaan pääkäyttäjä tasolla on mahdollista ottaa yhteys tai lisätä laitteita, lisätä tai muokata käyttäjiä, palveluja, komponentteja ja turvallisuus määrittelyjä. User-tason käyttäjätileillä on vakiona ainoastaan näkymä ja oikeus muokata isäntiä sekä palveluja, joihin heillä on suora kontakti. (Nagios 2014g.)

4.4.4 Versiointi

Sovelluksesta on kaksi eri versiota: Enterprise ja Standard. Enterprise versio sisältää lisättyjä toiminnallisuuksia ja ominaisuuksia, jotka on suunniteltu helpottamaan suuria konfiguraatioita, ennaltaehkäisyä sekä suunniteltua raportointia. Versioiden hinnoittelu määräytyy valvottavien ”nodejen” eli isäntiä mukaan. Valvottavien palveluiden määrää ei ole rajoitettu. Yhdessä isännässä voi olla siis useampi valvottava palvelu. Hinnoittelu alkaa molemmissa versioissa sadasta isännästä, seuraava on 200 isäntää ja kolmas vaihtoehto on

rajoittamaton määrä valvottavia isäntiä. Lisäksi Enterprise versiot vaativat vuotuisen huolto- ja tukisopimuksen tai vain jommankumman. (Nagios 2014f.)

Yhdellä Nagios XI lisenssillä voidaan valvoa vain yhtä verkkoa. Jos tarvitaan valvoa useampaa verkkoa, joudutaan hankkimaan useampi lisenssi. Lisensseillä on niin sanottu paljous alennus. Kahdesta neljään lisenssin ostaja saa kymmenen prosentin alennuksen, viidestä kymmeneen lisenssiin tuo 20 % alennuksen ja yli kymmenen lisenssiä antaa 30 % alennuksen. Tämä hinnoittelutyyli ei vastaa toimeksiantajan toivetta, sillä tarkoitus on päästä mahdollisimman yksinkertaisella ja helpolla ratkaisulla. Nagios XI:n tapauksessa erillisiä lisenssejä jouduttaisiin hankkimaan todella useita, sillä erillisverkkoja pelkästään Porvoon jalostamon alueella on useita. Tähän jos ajatellaan lisäksi Naantali ja vielä ulkomaiden toimipisteet kasvaa lisenssien määrä todella suureksi. (Nagios 2014f.)

4.5 WhatsUp Gold

WhatsUp Gold on ohjelmistoyritys Ipswitchin valmistama verkonvalvonta ja -hallintasovellus. Ensimmäinen versio sovelluksesta julkaistiin jo vuonna 1996. Se on suunnattu aina pienistä yrityksistä suuryrityksiin. Sovellus pystyy käsittelemään ja monitoroimaan jopa yli 20 000 laitetta, niin langallisia kuin langattomia verkkoja, järjestelmiä ja sovelluksia. Yhtenäinen kojelauta tarjoaa täyden näkymän infrastruktuurista helposti ja nopeasti. (Ipswitch 2014a.)

4.5.1 Ominaisuudet

Sovelluksen ominaisuudet vastaavat hyvin ajatellen toimeksiantajan määrittämiä kriteereitä. Erityisesti uusien laitteiden havaitseminen ja kartoittaminen verkosta on pitkälle automatisoitu. Se pystyy rakentamaan tarkan kuvan verkon laitteista, järjestelmistä ja niiden internetyhteyksistä käyttäen Layer 2 ja 3 verkkoteknologioita. Sovellus hyödyntää laitteiden havaitsemisessa aikaisemmin mainittuja yleisimpiä protokollia ja ARP-, SSH- sekä LLDP-protokollia. Valvonnassa sovellus hyödyntää suurimmaksi osaksi SNMP-protokollaa. Hälytyksille suunniteltu erityinen hälytyskeskus tarjoaa yhden kojelaudan näkymän, josta näkee koko infrastruktuurin hälytykset. Monitasoinen eskalointi helpottaa priorisoimaan ongelmiin reagointia. Hälytyskeskuksesta selviää laitteiden, palveluiden ja ohjelmien omistajuudet, se näyttää tila päivitykset ja sen avulla ongelman selvitys prosessin hallinta on tehokasta. Erilaisia raportointipohjia ja raportteja on yli 200. Raportit antavat kokonaiskuvan infrastruktuurin tilasta ja suorituskyvystä. Lisäksi web-käyttöliittymän avulla raportteja voidaan räätälöidä tiettyjä tarpeita tai kohderyhmiä varten. Raportit mahdollistavat verkon, servereiden ja sovellusten suorituskykytietojen vertailun vierekkäin verkkoliikenne- ja konfiguraatiotietojen kanssa. (Ipswitch 2014a; Ipswitch 2014b.)

4.5.2 Toiminta

Whatsup Gold kartoittaa verkon laitteet käyttäen ping (ICMP-protokolla) toimintoa tai skannaamalla avoimia TCP-portteja. Jos verkon laite ei vastaa pingiin, tai sillä ei ole avoimia portteja, ei sovellus voi sitä havaita. Näin ollen sitä ei voida myöskään monitoroida. Havaittuaan laitteen sovellus kyselee siltä valmistajan, mallin, komponenttien (prosessorit, tuulettimet, kiintolevyt) tiedot, käyttöjärjestelmän ja tarkemmat palvelut kuten HTTP tai DNS palvelut. Näiden tietojen keräämiseen käytetään SNMP-protokollaa tai WMI:tä. Verkon laitteiden havainnointiin ja kartoittamiseen on erilaisia vaihtoehtoja, kuten SNMP Smart Scan, jolle annetaan kriteereiksi pääreitittimen IP osoite ja jokaisen sivu reitittimen IP osoite sekä skannaussyvyys. Vaihtoehtona on myös käyttää ominaisuutta jossa anne-

taan kartoitettavaksi halutun verkon IP avaruus, esimerkiksi 10.0.0.1 – 10.0.0.100. (Ipswitch 2014c, 5-10.)

Kerätäkseen tietoja reitittimistä ja kytkimistä WhatsUp Gold tarvitsee Flow Monitor lisäosan. Lisäksi laitteesta, josta tietoja halutaan kerätä, tulee asettaa Flow ominaisuus päälle. Tämän jälkeen sovellus kerää automaattisesti verkkoliikenteen käyttöä koskevia tietoja, jotka kulkevat laitteiden lävitse. (Ipswitch 2014c, 5-10.)

WhatsUp Gold käyttää kolmen tyyppisiä monitoreja kerätäkseen ja raportoidakseen tietoja verkkolaitteista. Laitteiden havainnoinnin yhteydessä lisättyjen laiteroolien vakio monitoreiden lisäksi voidaan lisätä laitteelle seuraavia lisämonitoreja:

- Aktiivimonitorit kyselevät kohdelaitteelta tietoja, kuten ping saavutettavuus tai laitteen palvelut, kuten esimerkiksi web- tai sähköpostipalvelin. Näiden monitoreiden tehtävä on säännöllisesti kysellä laitteilta haluttua tietoa ja odottaa vastausta.
- Passiivimonitorit kuuntelevat laitteiden tapahtumia. Ne eivät aktiivisesti kysele laitteilta palveluiden tilaa ja näin ollen käyttävät vähemmän kaistaa. Passiivimonitorit kuuntelevat monimutkaisempia tapahtumia laitteissa verrattuna aktiivimonitoreiden yksinkertaisiin päällä ja pois kyselyihin. Esimerkiksi passiivimonitori voidaan asettaa kuuntelemaan epäonnistuneita kirjautumisyrityksiä verkkolaitteelle. Apuna käytetään SNMP ansaa joka tallentaa SNMP Trap lokitiedostoon kaikki epäonnistuneet kirjautumisyritykset laitteelle ja lähettää niistä halutessa ilmoituksen käyttäjälle.
- Suorituskykymonitorit keräävät tietoja verkon laitteiden komponenteista, kuten prosessorin ja muistin käytöstä. Kerättyjä tietoja käytetään esimerkiksi raporttien luontiin, joista voidaan tarkkailla laitteiden käytettävyyttä ja saatavuutta.

(Ipswitch 2014c, 13.)

Sovellus vaatii toimiakseen Microsoft SQL tietokannan. Tietokanta voidaan asentaa sovelluksen kanssa samaan paikkaan, jolloin verkkoliikennettä pystytään minimoimaan tai se voidaan asentaa erilliselle palvelimelle. Tämä kasvattaa sovelluksen kustannuksia, koska tarvitaan erillinen lisenssi tietokantaratkaisulle. (Ipswitch 2014e, 3.)

WhatsUp Gold vaatii Central Site ja Remote Site lisäosien asennuksen, jotta sillä voidaan hallita erillis- ja etäverkkoja. Central Site ominaisuutta käytetään keräämään etäverkoista kerätty data ja esittämään se käyttäjälle sovelluksessa. Remote Site komponentti asennetaan fyysisesti etä- tai erillisverkkoon tietokoneelle ja se raportoi toimintaansa Central Site asennukselle. Ratkaisu täyttää toimeksiantajan vaatiman kriteerin erillisverkkojen valvomiselle, mutta samalla se vaikeuttaa ja hidastaa käyttöönottoa. (Ipswitch 2014f, 1-2.)

Sovellus on hyvin perusteellinen ja automaattinen toiminnassaan sekä se on ominaisuuksiltaan todella monipuolinen. Huonona puolena voidaan kuitenkin pitää samaa monipuolisuutta. Se tarvitsee paljon erikseen ostettavia lisäosia toimiakseen mahdollisimman hyvin ja tehokkaasti. Ominaisuuksiltaan ja tehokkuudeltaan WhatsUp Gold olisi erinomainen valinta, mutta erityisesti helpon käyttöönoton puolesta se ei vastaa toimeksiantajan määrittelemiä kriteereitä.

4.5.3 Versiointi

Sovelluksesta on neljä eri versiota Standard, Premium, Distributed ja MSP (Managed Service Providers). Jokainen versio tuo lisäominaisuuksia ja Distributed on näistä kehittynein. Neljäs MSP versio on tarkoitettu verkonvalvonta ja -hallintapalveluita tarjoaville yrityksille. Se sisältää kaikki samat ominaisuudet kuin Distributed versio, mutta valvonta ja hallinta ominaisuudet voidaan hyödyntää kolmansille osapuolille. (Ipswitch 2014d.)

Jokaiselle versiolle valitaan valvottavien laitteiden määrä, alkaen 25 laitteesta yli 500 laitteeseen. Lisäksi versioille voidaan valita seitsemän lisätoiminnallisuutta:

- Sovellusten ja niiden suorituskyvyn sekä saatavuuden valvonta
- Yksityiskohtainen verkkoliikenteen käytön seuranta, joka mahdollistaa yksittäisten sovelluksien käyttäjien ja sivustojen liikenteen seurannan.
- Automaattinen verkkolaitteiden konfigurointi manageri poistaa turhat manuaaliset ja toistuvat konfigurointitehtävät.
- Tuki VMware virtuaali servereille.
- Mahdollisuus tarkkailla valvonnan alla olevaa infrastruktuuria kun varsinaisen valvonta serverin suorituskyky tai yhteydet ovat uhattuna.
- Tietoliikenteen luokittelu ja priorisointi mahdollisuus esimerkiksi IP puheluiden laadun takaamiseen.
- Mahdollisuus tarkkailla, kerätä, analysoida ja raportoida laitteiden verkkoliikennettä käyttäen NetFlow, sFlow, Jflow ja IPFIX protokollia.

Lisäominaisuudet nostavat hintaa ja näiden ominaisuuksien lisäksi tarjolla on useita muita pienempiä ominaisuuksia. (Ipswitch 2014d.)

4.5.4 Kyselyjen ja web-sovelluksen tietoturva

WhatsUp Gold tarjoaa useita tärkeitä turvallisuusominaisuuksia, jotka tulisi asettaa parantamaan ja ehkäisemään luvattomia kirjautumisia servereille ja laitteille. Sovellus tallentaa arkaluontoiset käyttäjätiedot ja järjestelmätietueet kryptattuna AES 256-bittisellä salauk-

sella. Yksittäiset käyttäjätilit ja käyttäjät on mahdollista jakaa ryhmiin ja ryhmille tai käyttäjille on mahdollista määrittää oikeudet vain tiettyihin valvottaviin ja hallittaviin laitteisiin. (Ipswitch 2014c, 18-21.)

Sovellus mahdollistaa FIPS (Federal Information Processing Standards) 140-2 standardin ja 128 bittisen SSL salauksen käyttämisen. FIPS salausta voidaan käyttää Microsoft serverin IIS (Internet Information Server) kanssa sekä .NET yhteydessä. IIS käsittelee ulkoisten web-käyttöliittymän käyttäjien ja sovelluksen välistä liikennettä. .NET yhteyttä käytetään käsittelemään lisäanturien ja sovelluksen välistä liikennettä sekä WhatsUp Goldin vara serverin ja sovelluksen liikennettä. Silloin, kun käytössä oleva käyttöjärjestelmä on asetettu toimimaan FIPS140-2 tilassa, myös WhatsUp Gold mahdollistaa FIPS tilan käyttämisen. Tämä mahdollistaa aktiivisessa ja suorituskyky valvonnassa käytettävien monitorien käyttämään FIPS algoritmia kun ne keskustelevat verkkolaitteiden kanssa. WhatsUp Gold mahdollistaa myös HTTPS (SSL ja TLS), SNMPv3 ja SNMPv2-protokollien käytön niin paikallisessa kuin etävalvonnassakin ja niitä suositellaan käytettäväksi aina kun on mahdollista. (Ipswtich 2014c, 22-23.)

4.6 PRTG Network Monitor

PRTG on vuonna 1997 perustetun Paesslerin kehittämä verkonvalvonta ja -hallintasovellus. Sovellus on tarkoitettu kaiken kokoisille yrityksille ja on lisensoitu niin, että kaikki ominaisuudet ovat aina käytössä. Kahdeksan lisenssiä erottaa toisistaan ainoastaan sensorien määrä. PRTG toimii Windows käyttöjärjestelmän päällä keräten ja tallentaen statistiikkaa verkosta, tietokoneista, ohjelmista ja laitteista. Käyttöliittymä on web-pohjainen ja se toimii kaikilla alustoilla sekä se on helposti konfiguroitavissa. Sovellusta on myös mahdollista käyttää kaikilla mobiililaitteilla. Sovelluksella voi helposti jakaa tietoja, tuottaa live grafiikkaa ja kustomoituja raportteja. (Paessler 2014a.)

4.6.1 Ominaisuudet

PRTG Network Monitor sisältää yli 200 sensorityyppiä ja niitä voidaan hyödyntää reitittimien, kytkimien, servereiden, raudan, käyttöjärjestelmien, sovellusten, virtuaaliympäristöjen, internetsivujen, sähköpostipalvelimien, tietokantojen, VoIP-palveluiden (Voice over IP) ja QoS-palveluiden (Quality of Service), IP-SLA:n (Internet Protocol Service Level Agreement), lokien, tapahtumien, suorituskykyjen, Flow tekniikoiden, pakettihaistelijoiden, SNMP:n, WMI:n, lämpötilojen, kosteuden ja monen muun valvontaan. Lisäksi sillä voidaan valvoa kaikkia yleisiä verkkopalveluita kuten esimerkiksi HTTP:tä ja FTP:tä. Sensori on yksi tietty yksittäinen valvontakokonaisuus. Sovelluksen konfigurointi on nopeaa ja helppoa käyttäen automaattista laitteiden havainnointia, joka luo sensorit automaattisesti. Mahdollisuutena on myös valita manuaalinen laitteiden ja sensorien asennus haluttaville laitteille. (Paessler 2014a; Paessler 2014b.)

Käyttöliittymänä on mahdollisuus käyttää internetselaimessa toimivaa täysiveristä hallintasivustoa, joka pohjautuu AJAX tekniikkaan tai vaihtoehtona HTML kieleen pohjautuva minimalistinen, ominaisuuksiltaan rajoitettu, vanhemmille selaimille ja mobiililaitteille tarkoitettu käyttöliittymä. Kolmantena vaihtoehtona on paikallinen Windows asennus, joka on tarkoitettu suurille yritysympäristöille. Se mahdollistaa valvontatietojen tarkastelun useista PRTG asennuksista samanaikaisesti. PRTG:tä voi käyttää myös mobiililaitteissa jotka ovat iOS tai Android pohjaisia. (Paessler 2014b; Paessler 2014c.)

Monipuolisilla hälytysvaihtoehdoilla on käytössä yhdeksän erilaista teknologiaa: sähköposti, tekstiviesti/hakulaite, syslog ja SNMP Trap, HTTP pyyntö, tapahtumakirjaus, äänihälytykset, Amazon SNS ja sisäiset teknologiat, joita voidaan suorittaa EXE tai batch tiedostoilla. Erilaisia hälytysvaihtoehtoja on useita erilaisia, kuten esimerkiksi tilahälytykset (ylhäällä, alhaalla, varoitus), rajahälytykset (arvo yli/alle jonkin), raja-arvohälytykset (arvo yli/alle jonkin tietyn aikaa) ja usean kohteen tilahälytykset. PRTG pystyy myös tarkasta-

maan hälytyksien riippuvuuksia, jolloin vältytään turhilta hälytyksiltä ja niiden tulvalta. Hälytyksiä pystytään myös aikatauluttamaan, esimerkiksi yöaikaan voidaan matalan prioriteetin hälytykset jättää kokonaan pois. (Paessler 2014b.)

PRTG Network Monitorilla on mahdollista luoda klusteri jopa viiden eri asennuksen kesken. Mahdollisen vikatilanteen tai sovelluksen päivityksen yhteydessä toinen yksikkö korvaa vikautuneen yksikön. Klusteriin määritetään ennalta pääyksikkö, jonka vikautuessa varayksikkö ottaa automaattisesti sen paikan ja huolehtii järjestelmien valvonnasta. Perus PRTG lisenssi mahdollistaa yksinkertaisen klusterin luomisen yhdellä lisenssiavaimella, jos halutaan luoda useamman kuin kahden yksikön klusteri tarvitaan useampi lisenssiavain. (Paessler 2014b.)

Verkosta kerätty valvontatieto voidaan julkaista suorana kojelaudoilla, joista voi olla joko yksityisiä tai julkisia versioita eri käyttäjäryhmille. Verkoista ja kerätystä tiedosta voidaan julkaista karttoja, jotka voivat sisältää yli 300 erilaista objektia. PRTG:stä voidaan tuottaa raportteja niin HTML kuin PDF muodossa. Raportit voi luoda lennosta tai suunnitellusti päivittäin, viikoittain tai kuukausittain. Valvontahistorian pystyy kopioimaan ulos sovelluksesta joko HTML, XML tai CSV muotoisena. (Paessler 2014b.)

PRTG ei käytä tiedon tallentamiseen SQL servereitä vaan sovelluksen kehittäjä on kehittänyt oman tietokantatyypin, johon se tallentaa sovelluksen keräämän datan. Kehittäjän mukaan tietokanta on sata kertaa nopeampi kuin tavallinen SQL tietokanta. Tämä antaa merkittävän edun muihin sovelluksiin nähden. Sovelluksen tietokanta on integroitu juuri serverin kanssa samaan, jolloin ei tarvita siirtoja verkon yli tietokantapalvelimelle ja näin ollen verkko kuormittaa vähemmän ja verkon toiminta on sulavampaa. Erityisen tärkeä ominaisuus kun ajatellaan toimeksiantajan isoa ja laajaa verkkorakennetta, sekä tärkeitä prosessiverkkoja ja niiden toimintavarmuutta. (Paessler 2014c.)

4.6.2 Toiminta

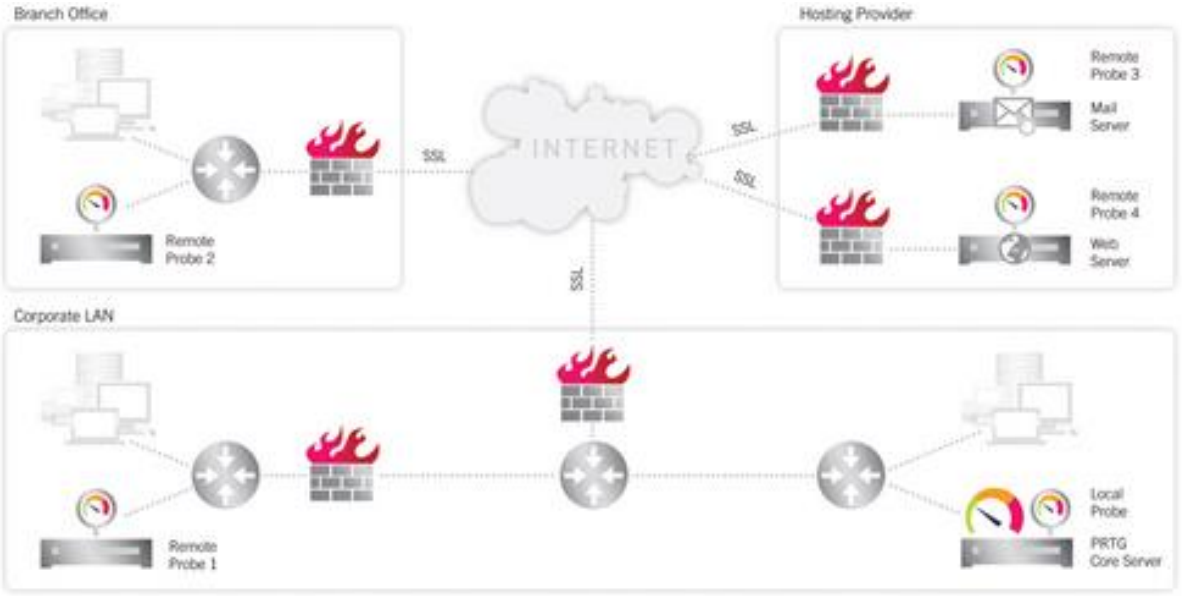
PRTG käyttää tiedon keruuseen ja valvontaan erilaisia sensoreita. Sensoreita on yli 200 erilaista jotka kattavat kaikki verkonvalvonnan osa-alueet. Sovelluksessa luodaan laite tai se havaitsee laitteet automaattisesti ja näillä laitteille luodaan sensoreita, joita käytetään valvontatoimintoihin. Yksi Sensori käsittää yhden mitattavan arvon esimerkiksi kytkimen portin, verkon palvelun, web-osoitteen, prosessorin kuorman tai vapaan levytilan kiintolevyllä. Keskiarvoisesti yhden serverin tietojen mittaamiseen menee 20 sensoria tai kahdeksan porttisen kytkimen tarkkailuun tarkalleen kahdeksan sensoria. (Paessler 2014d; Paessler 2014b.)

Eri tietojen valvontaan ja tietojen keräämiseen laitteista käytetään eri sensoreita, eri sensorit vaativat eri tekniikoita esimerkiksi laitteen prosessorikuorman mittaamiseen käytetään SNMP protokollaa. (Paessler 2014e.)

Kuva 6. Sensorin toiminta PRTG ohjelmassa (Paessler 2014e.)

Kuvassa keskellä oleva PRTG ydinserveri kyselee laitteilta, kuten reitittimiltä, kytkimiltä ja servereiltä, liikenteen määrän jokaisesta portista käyttäen pieniä datapaketteja. Nämä kyselyt laukaisevat laitteessa vastauspaketin, jonka ne lähettävät sovellukselle analysoitavaksi. SNMP protokolla verrattuna esimerkiksi Flow tekniikoihin luo se vähemmän prosessorikuormaa ja rasitetta verkolle. Tämä on tärkeää, kun tarkkailtavia verkkoja on useita ja niissä liikkuu liiketoiminnalle tärkeää tietoa. (Paessler 2014e.)

Erillisverkkojen ja etäverkkojen hallintaan PRTG Network Monitor käyttää etäluotaimia. Näiden etäluotaimien käyttö edellyttää ainoastaan yhden ydin serveri asennuksen. (Paessler 2014b.)



Kuva 7. Etäluotaimien sijointtuminen infrastruktuurissa ja toiminta. (Paessler 2014f.)

Ydinserveri pystyy valvomaan yrityksen verkkoa paikallisella luotaimella. Palveluita ja verkkoja palomuurien takana se valvoo etäluotaimen avulla, kuten myös suojattuja palveluita sivutoimiston ja palveluntarjoajan verkoissa. Se pystyy myös valvomaan julkisia palveluja internetverkossa. Etäluotaimien käyttömahdollisuus luo selvän eron muihin verrattaviin sovelluksiin sillä erillisiä lisenssejä ei tarvita muille valvotuille verkoille. Kuvasta voidaan myös havaita, että etäluotaimien välittämä data internetin kautta PRTG sovellukseen on salattu SSL tekniikalla, joka oli yksi toimeksiantajan kriteereistä. (Paessler 2014f.)

4.6.3 Versiointi

PRTG:n lisensointi on yksinkertainen. Kaikkiin lisensseihin kuuluu kaikki ominaisuudet mitä ohjelmassa on. Ainoastaan sensorien ja ydin asennuksien (core server) määrä on rajallinen. Versioita on kymmenen erilaista alkaen ilmaisesta 30 sensoria käsittävästä aina 5000 sensoria käsittävään versioon. Näiden lisäksi on kolme versioita rajoittamattomalla sensori määrällä. Versiot erottaa toisistaan ydinserverien asennuksien määrä. Lisänä on myös 30 päivän kokeiluversio rajoittamattomalla sensorimäärällä. (Paessler 2014g.)

PRTG suosittelee käytettäväksi fyysisiä tietokoneita PRTG Core serverille ja PRTG etäluotaimille virtuaalikone asennuksien sijaan. Virtuaalikonetta käytettäessä ei ole suositeltavaa käyttää yli 2000 sensoria, suorituskyky syistä. Sovelluksen valmistaja Paessler ei pysty antamaan teknistä tukea virtuaaliratkaisuille, jotka käyttävät yli 5000 sensoria. (Paessler 2014h.)

4.6.4 Kyselyjen ja web-sovelluksen tietoturva

PRTG keskittää tietoturvaansa erityisesti internetliikenteen suojattuihin yhteyksiin. Vakiona se käyttää 2048 bitin RSA-sertifikaattia. SSL-salaus on käytössä internetselain pohjaisessa käyttöliittymässä ja mobiilikäyttöliittymissä. PRTG käyttää kaikissa luotain ja klusteri yhteyksissä SSL salausta. Luotainten on mahdollista suodattaa yhteyksiä ja ne vaativat erityisen pääsyavaimen luodakseen yhteyden. (Paessler 2014i.)

Sovelluksen pääkäyttäjä voi jakaa käyttäjille ja käyttäjäryhmille yksittäisiä tai ryhmä oikeuksia sovellukseen. Jokainen käyttäjätili vaatii salasanan ja kirjautuessa sovellukseen salasanaa ei koskaan lähetetä takaisin internetselaimelle. PRTG tallentaa sisäiset salasanat aina salattuina, eikä kirjaa niitä lokitiedostoihin. Sovellukseen kirjautuneet käyttäjät, jotka ovat tietyn ajan käyttämättä sovellusta, kirjataan ulos automaattisesti. Automaattinen uloskirjaus ja uudelleen kirjautuminen tietyn väliajoin estävät molemmat tehokkaasti mahdollisia luvattomia käyttöjä ja turvaavat internetkäyttöliittymää mahdollisilta kalasteluhyökkäyksiltä (phishing attack). (Paessler 2014i.)

Kaikki käyttöliittymät sallivat SSL turvatun paikallisen kirjautumisen ja etäkirjautumisen, niitä voidaan käyttää myös samanaikaisesti. (Paessler 2014b; Paessler 2014c.)

4.7 Yhteenveto

Nagios XI vastasi liitteenä olevan taulukon mukaisesti kaikkiin vaadittuihin kriteereihin, mutta siltä puuttui valmiit kielivalinnat ja valmius erillisverkkojen hallintaan ilman erillisiä asennuksia (liite 1). Lisensoinnin osalta sovellus osoittautui myös hankalaksi ja kolmansien osapuolien laatimat lisäominaisuudet eivät tuo lisäarvoa sovellukselle, kun ajatellaan sitä osaksi tärkeitä prosessiverkkoja.

Liitteen ja tutkitun aineiston perusteella voidaan sanoa, että WhatsUp Gold täyttää pääpiirteittäin toimeksiantajan asettamat kriteerit kuten käyttäjähallinnan ja valvonta protokollien käytön (liite 1). Etä- ja erillisverkkojen valvonta on toteutettu niin, että se vaatii kahden uuden eri ominaisuuden asentamisen fyysisesti verkon osaksi. Sovelluksen lisensointi on ongelmallinen, kuten aikaisemmin olevassa selvityksessä käy ilmi.

Kolmesta vertailun sovelluksesta PRTG Network Monitor täyttää parhaiten toimeksiantajan kriteerit liitteenä olevan taulukon mukaan (liite 1) ja tutkittujen aineistojen perusteella. Vaikkakin ARP protokollan käyttö ei sovelluksella ole mahdollista, on sen tarjoama hyöty saavutettavissa toisella menetelmällä. Liitettä tarkasteltaessa voidaan huomata, että WhatsUp Gold ja PRTG ovat ominaisuuksiltaan hyvin tasavertaisia, mutta eroa muodos-

tuu tietoturvan ja etä- ja erillisverkkojen valvonnan saralla (liite 1). Myös läpikäytyjen aineistojen perusteella voidaan sanoa, että PRTG vaikuttaa helpoiten käyttöönotettavalta sovellukselta. Erityisesti, jos ajatellaan lisäominaisuuksia, joita kahteen muuhun sovellukseen joudutaan asentamaan erikseen.

Liitteestä kaksi voidaan havainnoida sovelluksien hinnoittelujen eroja (liite 2). Nagios XI on sovelluksista selvästi halvin, mutta aineiston perusteella yksi lisenssi mahdollistaa vain yhden verkon valvonnan. Tällöin jokaiselle erillisverkolle jouduttaisiin hankkimaan oma lisenssi. Tämä tulisi toimeksiantajan tapauksessa todella kalliiksi. WhatsUp Gold ei tarjonnut suoraan vastausta mitä toimeksiantajan vaatima 1000 laitteen käsittävä sovellus maksaisi. Toimeksiantajan kaikki vaatimat valvontaa ja hallintaa koskevat kriteerit sisältyy kalleimpaan versioon. PRTG Network Monitor on hintaluokaltaan samoissa lukemissa WhatsUp Gold ratkaisun kanssa. Selvä ero syntyy, kun tarkastellaan mahdollisuutta jalkauttaa PRTG ulkomaille, jolloin siis tarvitaan erillinen asennus. PRTG:n kallein lisenssi, joka tarjoaa viisi ydin asennusta minne tahansa, maksaa 35 000 euroa (liite 2). Vastaavaa tietoa WhatsUp Goldista ei ollut saatavilla, joten sovelluksia ei voida tässä suhteessa vertailla.

5 Pohdinta

5.1 Tulosten tarkastelu

Nagios XI voidaan jättää laskuista pois. Se pohjautuu niin vahvasti vapaaseen lähdekoodiin ja sen ympärillä olevaan sitä kehittävään yhteisöön, että se ei sovi tarkkuutta vaativiin prosessiverkkoihin. Lisäksi, jotta siitä saadaan monipuolinen ratkaisu, vaatii se erillisten asennusten tekemistä, joka hankaloittaa sovelluksen käyttöönottoa. Vaikka valmistaja takaa sovellukselle täyden tuen ja ylläpidon, vaatisi se kuitenkin perusteellisen perehtymisen sen alkuperäiseen isäntäsovellukseen Nagios Coreen, jotta siitä saadaan kaikki hyöty irti. Sovellus ei myöskään tarjoa yksinkertaista ratkaisua erillis- ja etäverkkojen hallinnalle vaan vaatii useamman lisenssin.

WhatsUp Goldin uusin versio on tutustumisen arvoinen sovellus vaikkakin sen suurin kompastuskivi on todella massiivinen lisäominaisuuksien määrä. Ne kaikki ovat tuotteistettu erikseen. Tämä vaatii perusteellisen tutustumisen ominaisuuksiin, jotta voidaan sanoa mitä tarvitaan ja mitä ei. Ominaisuuksien irrallisuus vaikuttaa heikentävästi sovelluksen käyttöönoton helppouteen ja toimintavarmuuteen. Mitä enemmän erikseen asennettavia ominaisuuksia, sen helpommin jotain jää asentamatta ja mahdollisia ristiriitoja esiintyy. Tämä samainen seikka tulee ottaa huomioon myös Nagios XI sovelluksen kanssa, jolla on myös paljon erikseen asennettavia ominaisuuksia. Lisensoinnin puolesta sovellus saattaa osoittautua edullisimmaksi vaihtoehdoksi, koska toimeksiantajalla on jo valmiiksi sovelluksen aikaisempi versio. Vaikkakaan ei ole tiedossa tarkkaa hintaa lisenssille, joka kattaisi toimeksiantajan vaatiman laitemäärän, eikä hintatietoja mahdollisille erillisasennuksille ja muille toimipisteille.

PRTG:n kiistatta ylivoimaisin etu on sen lisensointi, joka perustuu siihen, että kaikilla sovelluksen eri versioilla on kaikki ominaisuudet käytössä. Tämä näkyy sovelluksen hinnassa, mutta se tuo myös helppoutta ja mahdollistaa nopean käyttöönoton. Hinta ei poikkea mitenkään dramaattisesti WhatsUp Goldin hinnasta (liite 2). Voidaan myös ajatella, että 35 000 euroa ei ole kovinkaan paljoa viidestä erillisestä asennuksesta, joissa voidaan kaikissa valvoa ja hallita useita erillisiä verkkoja ja palveluita etäluotaimien avulla.

5.2 Luotettavuus

Verkonhallinnan tekniikoita käsittelevät osuudet laadittiin pääosin käyttäen alan kirjallisuutta. Nämä tiedot eivät vanhene, sillä ne ovat verkon perusta ja perusominaisuuksia verkkojen toiminnassa ja siltä osin luotettavia lähteitä. Sovelluksia käsittelevät tiedot kerättiin erinäisistä internetlähteistä, kuten artikkeleista ja arvosteluista, sekä sovelluksien val-

mistajien verkkosivuilta. Näitä lähteitä jouduttiin tulkitsemaan ja pohtimaan mahdollisimman puolueettomasti ja ajatellen toimeksiantajan etua sekä tarvitsemia ominaisuuksia. Tästä syystä sovelluksista kerrottaviin tietoihin pitää suhtautua tietyllä varauksella sillä kukaan ei halua omaa tuotettaan haukkua.

5.3 Johtopäätökset ja jatkaminen

Kolmesta valitusta verkonvalvonta ja -hallintasovelluksesta PRTG oli paras ja kannattavin vaihtoehto annettujen kriteerien ja tarjolla olleiden tietojen perusteella. Opinnäytetyöstä selviää myös, että nykyaikaiset verkonvalvonta ja -hallintasovellukset ovat monipuolisia ja monikäyttöisiä niin pienessä kuin suuressakin ympäristössä. Sovellukset tarjoavat pääkäyttäjille ja verkkojen ylläpitäjille uusia työkaluja vikojen ennaltaehkäisyyn, korjaamiseen ja verkkojen suorituskyvyn parantamiseen sekä optimointiin.

Yllättävää oli myös huomata, kuinka monipuolisesti nykyaikaiset sovellukset käyttävät erilaisia verkko-protokollia ja verkon ominaisuuksia hyödykseen, kuten WMI, Flow-tekniikat ja pakettien haistelu. Ne eivät enää pelkästään painotu SNMP-protokollaan tai yksinkertaisiin kysely menetelmiin. Hienoa oli myös havaita, että kun kytkimet ja reitittimet ovat kehittyneet ajan myötä ja saaneet uusia ominaisuuksia, niin myös sovellukset ovat kehittyneet ja pystyvät näin hyödyntämään uusia ominaisuuksia.

Yritysten kasvavissa tietoverkoissa ja kehittymisessä sekä verkkolaitteiden jatkuvassa kehityksessä on haastetta uusien ja olemassa olevien verkonvalvonta ja -hallintasovelluksien kehittäjille. Siirtyminen IPv6-protokollaan tulee tuomaan haasteita jo pelkästään yritysten laitteiden kommunikoinnissa vanhoihin protokolliin. Uusien verkonvalvontamenetelmien ja uusien protokollien huomioiminen tulevissa järjestelmissä ja sovelluksissa tuo omat haasteensa. Samalla kun tekniikka kehittyy ja yritysten verkon kasvavat entisestään, tulee entistä tärkeämmäksi, että verkonvalvonta ja -hallintajärjestelmä on ajanmukainen ja pysyy kehityksen mukana. Jatkuva verkkojen käytön lisääntyminen ja uudenlaisten laitteiden liittäminen osaksi verkkoa lisää yksityiskohtaisemman ja tarkemman valvonnan tarvetta. Toimiva, ajantasainen ja helposti ylläpidettävä verkko on tärkeä osa nykyaikaista tietoturvallisuutta.

Seuraava askel työstä olisi ottaa perusteelliseen testaukseen sekä WhatsUp Gold ja PRTG Network Monitor. Testattavia ominaisuuksia olisi ainakin sovelluksien käyttöönotto, käyttöliittymät, kyky havainnoida uusia laitteita ja verkossa tapahtuvia muutoksia, vasteajat sekä erillisverkkojen valvontaominaisuudet. Erityisesti WhatsUp Gold vaatisi katta-

van kartoituksen ominaisuuksista, joita sillä on tarjolla ja tarkat hintatiedot. Luontevinta olisi järjestää sovelluksille identtiset testiympäristöt ja vertailla kerättyä dataa keskenään.

5.4 Kokonaisprosessi ja oppiminen

Työaikataulu oli aavistuksen tiukka, koska työ päästiin kunnolla aloittamaan vasta syyskuun loppupuolella. Työ ei kuitenkaan osoittautunut erityisen hankalaksi sillä oli selvää mitä tullaan tekemään ja mihin työ rajataan. Aikataulu ei olisi mitenkään riittänyt sovelluksien syvällisempään tutkimiseen. Tätä työtä pystytään hyödyntämään, kun halutaan ottaa syvällisempään tarkasteluun sopivia vaihtoehtoja uudelle sovellukselle. Työstä saadaan kattava pohjatieto, kuinka nykyaikaiset sovellukset toimivat ja mitä tekniikoita ne käyttävät. Itsessäni tämä työ herätti mielenkiinnon ja halun tutkia sovelluksia paremmin. Olisi mielenkiintoista päästä jatkamaan tätä työtä ja viemään sitä pidemmälle. Erityisesti sovelluksien käyttöönotto, konfigurointi ja testaus oli mielekästä suunnitella sekä toteuttaa. Tällä tavalla saisi myös kokonaisvaltaisemman kuvan sovelluksien toiminnasta ja toimintaperiaatteista. Työ jää kuitenkin vielä pintaraapaisun asteelle ja sitä voidaan jatkojalostaa useampaan suuntaan.

Lähteet

Baxter, M. 2008. ICMP Header. Luettavissa: http://www.fatpipe.org/~mjb/drawings/. Luettu: 13.11.2014.

Cisco 2002. SNMP Management Information Base. Luettavissa: http://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/ses/software/ses_pnni_r3-0/configuration/guide/scg/oricgape.pdf. Luettu: 21.10.2014.

Crenshaw, A. A Quick Intro to Sniffers: Wireshark/Ethereal, ARPSpoof, Ettercap, ARP poisoning and other niceties. Luettavissa: http://www.irongeek.com/i.php?page=security/AQuickIntrotoSniffers luettu: 20.10.2014. Luettu: 9.11.2014.

DenHartog, M. 2010. SNMP Tutorial Part 1: An Introduction to SNMP. Luettavissa: http://www.dpstele.com/layers/l2/snmp_tutorial_what_is_snmp.php. Luettu: 21.10.2014.

Feldman, J. 1999. Verkonhallinta Trainer. Jyväskylä: Gummerus.

Hale, B. Netflow V9 Datagram Knowledge Series: Part 1 – Netflow Overview. Luettavissa: https://thwack.solarwinds.com/community/solarwinds-community/geek-speak_tht/blog/2012/09/06/netflow-v9-datagram-knowledge-series-part-1--netflow-overview. Luettu: 19.10.2014.

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Diblomityö. Helsingin teknillinen korkeakoulu. Luettavissa: http://www.tct.hut.fi/julkaisut/tyot/diplomityot/611/thesis.html. Luettu: 9.10.2014.

Ipswitch 2014a. WhatsUp Gold - Monitor performance and availability from a single dashboard. Luettavissa: http://www.whatsupgold.com/products/whatsup-gold.aspx. Luettu: 10.10.2014.

Ipswitch 2014b. WhatsUp Gold Suite. Luettavissa: http://www.whatsupgold.com/resources/datasheets/WhatsUp_Gold_Core_Product_DS.pdf. Luettu: 10.10.2014.

Ipswitch 2014c. WhatsUp Gold v16.2 - Getting Started Guide. Luettavissa: http://docs.ipswitch.com/NM/69_WhatsUpGoldv16.2/02_Guides/WhatsUpGoldv16_2GettingStartedGuide.pdf. Luettu: 10.11.2014.

Ipswitch 2014d. Buy WhatsUp Gold. Luettavissa: http://www.whatsupgold.com/buy/index.aspx. Luettu: 13.11.2014.

Ipswitch 2014e. Deployment Guide - Installing WhatsUp Gold Distributed Edition to Central and Remote Sites. Luettavissa: http://docs.ipswitch.com/NM/79_WhatsUp%20Gold%20v15/05_Additional%20Resources/Distributed/WhatsUp%20Gold%2015%20Distributed%20Deployment%20Guide.pdf. Luettu: 20.11.2014.

Ipswitch 2014f. WhatsUp Gold v16.2 Distributed Edition. Luettavissa: http://docs.ipswitch.com/NM/69_WhatsUpGoldv16.2/05_AdditionalResources/Distributed/WhatsUpGold16_2DistributedDeploymentGuide.pdf. Luettu: 20.11.2014.

Jaakohuhta, H. 2002. Lähiverkot – Ethernet. Helsinki: Edita.

Keys, B. 2014. A Secure Nagios Server. Luettavissa: http://www.linuxsecurity.com/content/view/144088. Luettu: 1.11.2014

Kozierok, C. M. 2005. TCP/IP Structure of Management Information (SMI) and Management Information Bases (MIBs) Overview. Luettavissa: http://www.tcpipguide.com/free/t_TCPIPStructureofManagementInformationSMIandManagem-3.htm. Luettu: 23.10.2014.

Nagios 2014a. Nagios XI Overview. Luettavissa: http://www.nagios.com/products/nagiosxi Luettu: 22.10.2014.

Nagios 2014b. Nagios XI Features. Luettavissa: http://www.nagios.com/products/nagiosxi/features. Luettu: 22.10.2014.

Nagios 2014c. Nagios XI 2014 – How It Works. Luettavissa: http://assets.nagios.com/handouts/nagiosxi/Nagios-XI-2014-How-It-Works.pdf. Luettu: 22.10.2014.

Nagios 2014d. Configuring Monitoring. Luettavissa: http://assets.nagios.com/downloads/nagiosxi/guides/user/configmonitoring.php#availablewizards. Luettu: 8.11.2014.

Nagios 2014e. Nagios XI For Nagios Admins. Luettavissa: http://www.nagios.com/products/nagiosxi/fornagiosadmins. Luettu: 22.10.2014.

Nagios 2014f. Nagios XI Pricing. Luettavissa: http://www.nagios.com/products/nagiosxi/pricing. Luettu: 22.10.2014.

Nagios 2014g. Nagios XI – Understanding User Rights. Luettavissa: http://assets.nagios.com/downloads/nagiosxi/docs/Understanding-Nagios-XI-User-Rights.pdf. Luettu: 19.11.2014.

Nagios 2014h. Enhanced CGI Security and Authentication. Luettavissa: http://nagios.sourceforge.net/docs/3_0/cgisecurity.html . Luettu: 19.11.2014.

Nash, K. S. & Behr, A. 2008. Network Monitoring Definition and Solutions. Luettavissa: http://www.cio.com/article/2438133/networking/network-monitoring-definition-and-solutions.html. Luettu: 15.10.2014.

Neste Oil 2014a. Porvoon jalostamo. Luettavissa: http://www.nesteoil.fi/default.asp?path=35,52,62,12271,12280. Luettu: 7.10.2014.

Neste Oil 2014b. Lyhyesti. Luettavissa: http://nesteoil.fi/default.asp?path=35,52,107,2999. Luettu: 7.10.2014.

Paessler 2014a. PRTG Network Monitor. Luettavissa: http://www.paessler.com/prtg. Luettu: 15.10.2014.

Paessler 2014b. PRTG Network Monitor Feature Overview. Luettavissa: http://www.paessler.com/prtg/features. Luettu: 15.10.2014.

Paessler 2014c. Frequently Asked Questions (FAQs). Luettavissa: http://www.paessler.com/support/faqs. Luettu: 16.10.2014.

Paessler 2014d. What is a "Sensor" in PRTG?. Luettavissa: http://kb.paessler.com/en/topic/33023-what-is-a-sensor-in-prtg. Luettu: 16.10.2014.

Paessler 2014e. SNMP Sensors. Luettavissa: http://www.paessler.com/manuals/prtg7/snmp_sensors. Luettu: 12.11.2014.

Paessler 2014f. PRTG Manual: Remote Probes and Multiple Probes. Luettavissa: http://www.paessler.com/manuals/prtg/remote_probes_and_multiple_probes.htm. Luettu: 12.11.2014.

Paessler 2014g. Price List of PRTG Network Monitor. Luettavissa: http://www.paessler.com/prtg/price_list. Luettu: 12.11.2014.

Paessler 2014h. System Requirements for PRTG Network Monitor. Luettavissa: http://www.paessler.com/prtg/requirements. Luettu: 12.11.2014.

Paessler 2014i. What security features does PRTG include?. Luettavissa: http://kb.paessler.com/en/topic/61108-what-security-features-does-prtg-include. Luettu: 12.11.2014.

Postel, J. 1981. Internet Control Message Protocol. Luettavissa: http://tools.ietf.org/html/rfc792. Luettu: 13.10.2014.

Puska, M. 2000. Lähiverkkojen tekniikka –Pro Training. Jyväskylä: Gummerus.

Scott, N. 2014. Installation. Luettavissa: http://assets.nagios.com/downloads/ncpa/docs/html/installation.html. Luettu: 8.11.2014.

Liitteet

Liite 1. Sovelluksien vertailu taulukko

Sovelluksien vertailu	**Sovellukset (edistynein lisenssi)**		
Vaaditut kriteerit sovelluksille	**Nagios XI**	**WhatsUp Gold**	**PRTG**
Käyttöliittymä ja käyttäjä hallinta			
Web-pohjainen käyttöliittymä	●	●	●
Selkeä ja konsolimainen näkymä	●	●	●
Muunneltavuus ja personoidut näkymät	●	●	●
Käyttäjien sekä käyttäjäryhmien hallinta	●	●	●
Käyttäjille ja käyttäjäryhmille personoitujen näkymien luonti	●	●	●
Kieliavaihtoehdot			
Englanti	●	●	●
Saksa	-	●	●
Venäjä	-	●	●
Espanja	-	●	●
Kiina	-	●	●
	Mahdollisuus kääntää itse mille tahansa kielelle .po tiedostoa muokkaamalla.	Mahdollista kääntää mille tahansa kiellelle käyttäen omaa kääntötyökalua.	Mahdollista kääntää mille tahansa kiellelle käyttäen omaa kääntötyökalua.
MONITOROINTI JA TOIMINNOT			
Laitteiden suorituskyky monitorointi (CPU kuorma, levytila ja käyttö, muistit, ping viive)	●	●	●
Oheislaitteiden monitorointimahdollisuus (tulostimet, tuulettimet, virtalähteet ja lämpötilat)	●	●	●
Laitteiden monitorointi käyttäen SNMP protokollaa	●	●	●
Laitteiden monitorointi käyttäen ARP protokollaa	●	●	-
Laitteiden monitorointi käyttäen ICMP protokollaa	●	●	●
Laitteiden monitorointi käyttäen SSH protokollaa	●	●	●
Laitteiden monitorointi käyttäen WMI protokollaa	●	●	●
Laitteiden monitorointi käyttäen Flow protkollia	●	●	●
Automaattinen ja manuaalinen kytkintasojen 2/3 tunnistus ja verkkotopologia kartoitus	●	●	●

Manuaalinen ja ajastettu uusien laitteiden havainnointi	●	●	●
Ajastustyökalu huoltotoimenpiteiden automatisointiin	●	●	●
Useampien sovelluksen ja laitteiden konfiguraatioiden tallennus	●	●	●
Etä- ja erillisverkkojen valvonta ja hallinta	Yhdellä lisenssillä voidaan valvoa yhtä verkkoa, tarvitaan useampi.	Kuuluu lisenssiin mutta erikseen asennettava lisäominaisuus.	●
LAAJENNETTAVUUS			
Valmiit lisäosat ja laajennukset	●	●	●
Laajennettavat arkkitehtuuri (ohjelmointirajapinta, API)	●	Ei APIa. Skriptaus mahdollista, lisenssin omistajalla oikeudet muokata sovellusta.	●
Skriptien luonti	●	●	●
HÄLYTYKSET			
Sähköpostin välityksellä	●	●	●
Käyttäjille ja käyttäjätyhmille personoidut hälytysilmoitukset	●	●	●
RAPORTOINTI			
Valmiita raporttipohjia	●	●	●
Omien raporttien luonti	●	●	●
TIETOTURVA			
RSA salaus SSH yhteyksissä	Ladattava lisäominaisuus (esim. tietylle kytkin tyypille).	Ostettava lisäominaisuus.	●
SSL yhteyksien käyttömahdollisuus web-sovelluksessa ja verkon laitteiden valvonnassa	●	●	●
Käyttäjien oikeuksien hallinta ja ryhmäoikeuksien luonti mahdollisuus	●	●	●

Liite 2. Sovelluksien hinta vertailu

Suuntaa-antava sovelluksien hintavertailu		
Nagios XI	**Hinta**	**Lisätieto**
Enterprise versio Rajoittamaton valvottavien isäntien määrä	5 180 €	Ainoa järkevä vaihtoehto versioista. Hinta kertautuu mitä enemmän valvottavia verkkoja. Paljousalennus. Erilaiset lisäominaisuudet nostavat hintaa
WhatsUp Gold Distributed versio (paikallinen) Maksimissaan 500 laitetta	8 148,40 €	Ainoa saatavilla oleva hinta, yli 500 laitteen järjestelmille löytyy räätälöity hinnasto. Erilaiset lisäominaisuudet nostavat hintaa
PRTG Network Monitor Unlimited versio Rajoittamaton määrä sensoreita	10 000 € / 35 000 €	Halvempi versio mahdollistaa yhden ydin serverin asennuksen ja yhden varajärjestelmäksi. Kalliimpi versio mahdollistaa viisi erillistä asennusta ympäri maailman.