Insinöörityö

Varmistetun tietoverkkoratkaisun suunnittelu ja konfigurointi

Johanna Kotisaari

Tietotekniikan koulutusohjelma

SAVONIA-AMMATTIKORKEAKOULU TEKNIIKKA KUOPIO

Koulutusohjelma

Tietotekniikan koulutusohjelma

Tekijä

Johanna Kotisaari

Työn nimi

Varmistetun yritysverkon suunnittelu ja konfigurointi

Työn laji	Päiväys	Sivumäärä
Opinnäytetyö	16.9.2010	41 + 14

Työn valvoja	Yrityksen yhdyshenkilö
Projekti-insinööri Seppo Voutilainen	TJ Eric Valta

Yritys

Savon Tietokeskus Oy

Tiivistelmä

Savon Tietokeskus Oy, toiselta nimitykseltään Data Group Kuopio, on kuopiolainen yritys, joka myy, korjaa, huoltaa ja ylläpitää tietoliikennelaitteita. Lisäksi yritys tarjoaa asiakkailleen mm. sähköposti- ja kotisivupalveluita. Tämän opinnäytetyön aiheena oli suunnitella Savon Tietokeskus Oy:lle varmistettu yritysverkko.

Tietoverkkoratkaisun suunnittelussa ei otettu huomioon yrityksen käytössä olevaa aiempaa verkkoratkaisua vaan suunniteltiin täysin uusi tietoverkkoratkaisu. Työssä haluttuihin tarkoituksiin valittiin sopivat laitteistot ja suunniteltiin näistä toimiva verkkoratkaisu. Tämän lisäksi kirjattiin verkkoratkaisussa tarvittavat kytkinkonfiguraatiot ja ratkaisun kustannusarvio. Ratkaisu varmistettiin mm. UPS–laitteistolla sekä kahdennetuilla verkkolaitteilla.

Tähän opinnäytetyöhön kootun tiedon pohjalta Savon Tietokeskus Oy voi tulevaisuudessa rakentaa uuden tietoverkkoratkaisun. Valmiiksi tehdyt konfiguroinnit helpottavat verkon rakentamisen toteutusta. Yrityksen pohdittavaksi jää, onko yritys halukas toteuttamaan verkkoratkaisun.

Avainsanat

verkko, varmistettu

Luottamuksellisuus

julkinen

SAVONIA UNIVERSITY OF APPLIED SCIENCES

Degree Programme

Information Technology

Author

Johanna Kotisaari

Title of Project

Designing and Configuring an Enterprise Network Solution with Backup

Type of Project	Date	Pages
Final Project	16 September 2010	41 + 14

Academic Supervisor	Company Supervisor
Mr Seppo Voutilainen, Project engineer	Mr Eric Valta, CEO

Company

Savon Tietokeskus Oy

Abstract

Savon Tietokeskus Oy, also known as Data Group Kuopio, is a company in Kuopio. The company sells data network equipment and also repairs them. The company also offers for example e-mail and homepage services to its customers. The aim of this thesis was to design an enterprise network solution with backup.

This new network solution is not based on Savon Tietokeskus Oy's old network solution. This solution consists of the equipment which is required to accomplish the wanted result. The final project was carried out by designing the network solution, writing down the required configurations and estimating the costs of this solution. The backup is executed by UPS and device duplications in the network solution.

Based on the information, which was collected in this final year project, Savon Tietokeskus Oy will be able to implement the new network solution. The configurations which were completed will make the solution implemention easier. The company will decide whether to implement the solution or not.

Keywords

network, backup

Confidentiality

public

ALKUSANAT

Aloitin tämän opinnäytetyön teon keväällä 2010 ja sain sen valmiiksi vuoden 2011 tammikuussa.

Osoitan kiitokset työn ohjaajalle projekti-insinööri Seppo Voutilaiselle sekä toimitusjohtaja Eric Vallalle ja muille Savon Tietokeskus Oy:n henkilökunnalle. Haluan kiittää myös aviomiestäni Tommi Kotisaarta tuesta opinnäytetyön teon aikana.

Siilinjärvellä 20.1.2011

Johanna Kotisaari

SISÄLTÖ

LYHENTEET JA SANASTO

AIP SSM ja AIP SSC	Ciscon kehittämiä turvallisuus -ratkaisuja
ASA	Adaptive Security Appliance, Ciscon kehittämä palomuuri-ratkaisu.
ASDM	Adaptive Security Device Manager, sovellus, jonka avulla voi konfiguroida, tarkkailla ja selvittää ongelmia Ciscon palomuuri-ratkaisussa.
CLI	Command Line Interface eli komento-ikkuna
DMZ	Demilitarized Zone, looginen tai fyysinen aliverkko, joka yhdistää yrityksen oman verkon turvattomampaan alueeseen
UPS	Uninterruptible Power Supply, varavirran syöttäjä virtakatkoksien sattuessa.
GSM	Global System for Mobile Communicatios, maailmanlaajuinen matkapuhelinjärjestelmä
IP	Internet Protocol, TCP/IP-mallin Internet-kerroksen prokolla, huolehtii IP-tietoliikennepaketin perille toimittamisesta pakettipohjaisessa Internet-verkossa.
IPS	Intrusion Prevention System, turvallisuus-sovellus, joka tarkkailee sitä, ettei verkossa ole vaarallista liikennettä.
IPSec	IP Security Architecture, joukko tietoliikenne-protokollia Internet-yhteyksien turvaamiseen. Kuuluvat IP/TCP-perheeseen.
LAN	Local Area Network eli lähiverkko
MD5	Message Digest, algoritmi, jota käytetään kryptografiassa, muuttaa viestin muodon lukemattomaksi ja näin suojaa viestin.
MIB	Management Information Base, virtuaalinen tietokanta, jossa säilytetään verkon kokonaisuuksia ja joka on SNMP:n käyttämä.
PoE	Power over Internet, tekniikka, jonka avulla syötetään käyttöjännite laitteelta toiselle kierretyn parikaapelin avulla.

PRTG	Paessler Router Traffic Grapher, sovellus, joka tarkkailee ja suojaa verkon liikennettä.
SHA	Secure Hash Algorithm, algoritmi, jota käytetään kryptografiassa, muuttaa viestin muodon lukemattomaksi ja näin suojaa viestin. Pidetään MD5:n seuraajana.
SIM	Subscriber Identity Module, kortti, jota käytetään tunnistamaan käyttäjä matkapuhelimissa tai tietokoneissa.
SNMP	Simple Network Management Protocol, protokolla, jota käytetään IP/TCP-verkkojen hallintaan.
SSL	Secure Sockets Layer, salausprotokolla, jota käytetään suojaamaan Internet-sovellusten liikenne IP-verkkojen ylitse.
STP	Spanning Tree Protocol, protokolla, jota käytetään varmistamaan sujuva liikenne lähiverkossa.
TCP	Transmission Control Protocol, tietoliikenneprotokolla, jonka avulla voi luoda yhteyden sellaisten tietokoneiden välille, joilla on yhteys Internettiin.
UDP	User Datagram Protocol, yhteyskäytäntö, jonka avulla kone voi lähettää viestin toiselle koneelle.
UPS	Uninterruptiple Power Supply, laite, jolla turvataan verkon laitteiden virransaanti virtakatkoksen aikana.
URL	Uniform Resource Locator, merkkijono, jolla kerrotaan tietyn tiedon paikka.
VLAN	Virtual LAN, tekniikka, jolla jaetaan fyysinen tietoliikenneverkko loogisiin osiin.
VPN	Virtual Private Network, tapa, jonka avulla kaksi tai useampaa turvallista verkkoa voidaan yhdistää julkisen verkon yli siten, että muodostuu näennäisesti yksityinen verkko.

1 JOHDANTO

Tietoverkon toimivuus on nykyään tärkeää yrityksien toiminnassa. Katkokset tietoverkon toimivuudessa aiheuttavat usein vakaviakin ongelmia yritystoiminnalle, kuten taloudellisia menetyksiä. Monella yrityksellä tuottavuus on kytköksissä tietoverkon toimivuuteen. Näistä syistä yrityksien on tärkeää kiinnittää huomiota tietoverkkonsa rakenteeseen ja sen myötä myös sen toimintaan. Tietoverkon toimintaa tulisi varmistaa mahdollisuuksien mukaan.

Itä-Suomen keskuksena ja alati kehittyvänä kaupunkina Kuopio tarjoaa oivan paikan yritystoimintaan. Savon Tietokeskus Oy on kuopiolainen yritys, joka myy ja huoltaa tietokoneita ja oheislaitteita sekä tarjoaa asiakkailleen muita palveluita, esim. sähköpostipalvelun. Tämän opinnäytetyön tarkoituksena on suunnitella Savon Tietokeskus Oy:lle varmistettu verkkoratkaisu ja lisäksi kirjata ratkaisussa tarvittavat kytkinkonfiguraatiot. Näiden lisäksi työssä laaditaan suunnittelutyön pohjalta kustannusarvio.

Työssä tutustutaan tietoverkkoratkaisussa käytettäviin laitteisiin ja muihin ratkaisussa tarvittaviin asioihin, esim. laitteiden kahdennukseen. Työssä on esitelty vaihtoehtoja toteuttaa laitteiden valinta.

Tässä opinnäytetyössä verkkosuunnitelmaa ei ole toteutettu käytännössä, vaan Savon Tietokeskus Oy:lle on tehty suunnitelma uudesta tietoverkkoratkaisusta ja siihen liittyvistä kustannuksista. Yrityksen ratkaistavaksi jää, toteutetaanko tämä verkkoratkaisu käytännössä.

2 UPS-LAITTEISTOT

Monet yhtiöt ja erityisesti kotikäyttäjät eivät ole varautuneet lyhyisiin sähkökatkoksiin. Tällaiset tapahtumat voivat kuitenkin hävittää tallentamattomia tietoja ja johtaa jopa verkon laitteen rikkoontumiseen. UPS-laitteella tai -järjestelmällä taataan tasainen virransyöttö lyhyissä sähkökatkoksissa ja silloin, kun syöttöjännite vaihtelee ja sisältää erilaisia häiriöitä. Se sijoitetaan virtalähteen ja virtaa käyttävän laitteen väliin. (*UPS* Wikipedia.)

UPS-laitteen akusta on mahdollista syöttää virtaa muutamista minuuteista puoleen tuntiin, mutta pitkäaikaisempaan virransyöttöön akkua ei ole tarkoitettu. Tähän tarkoitukseen tulee käyttökohteessa olla omat generaattorinsa. Ennen kuin UPS-laitteen akku on kokonaan tyhjentynyt, laitteeseen liitetty ohjelmisto sammuttaa tietokonelaitteistot hallitusti tai erillinen varavoimalaitteisto tulee käyttöön ja sähkönsyöttöä jatketaan käyttäen varavoimalaitteistoa. (*UPS* Wikipedia.)

UPS-laitteilla voidaan suojata tietokonelaitteistojen lisäksi myös viestintälaitteita, kuten esimerkiksi lennonohjausjärjestelmän. Nykyään myös tietokoneen kotikäyttäjille myydään UPSeja. (*UPS* Wikipedia.)

2.1 Toiminta

UPS on tavallisesti tasasuuntaja, jolla verkkovirran vaihtojännite ensin tasasuunnataan. Tämän tasasuunnatun tasajännitteen rinnalle on kytketty vähintään yksi akku, josta jännite syötetään katkoksen sattuessa. Lopulta tasajännite muunnetaan vaihtojännitteeksi vaihtosuuntajalla. Useimmat käyttölaitteet käyttävät vaihtojännitettä, mutta mikäli käyttölaite käyttää tasajännitettä, voidaan tasajännitteen vaihtojännitteeksi muuntava vaihtosuuntaja jättää pois. (*UPS* Wikipedia.)

UPS voi olla toteutettu myös vauhtipyörällä. Tällöin moottori ja generaattori on yhdistetty toisiinsa ja akselilla on raskas vauhtipyörä. Sähkökatkos aikana vauhtipyörään varastoitunut energia pyörittää generaattoria, joka tuottaa sähköä. (*UPS* Wikipedia.)

2.2 UPSin hankinnassa huomioitavaa

Ennen UPSin hankintaa tulisi selvittää seuraavat asiat:

- suojattavan laitteiston vaatima teho sekä häiriötyypit, joilta halutaan suojautua
- verkkokatkoksen sattuessa haluttu toiminta-aika (yleensä muutamia minuutteja)
- mahdollinen laajennusvara (ilmaistaan usein prosentteina varsinaisesta tehotarpeesta).

(Voutilainen S. 2007.)

2.3 UPSin käyttö

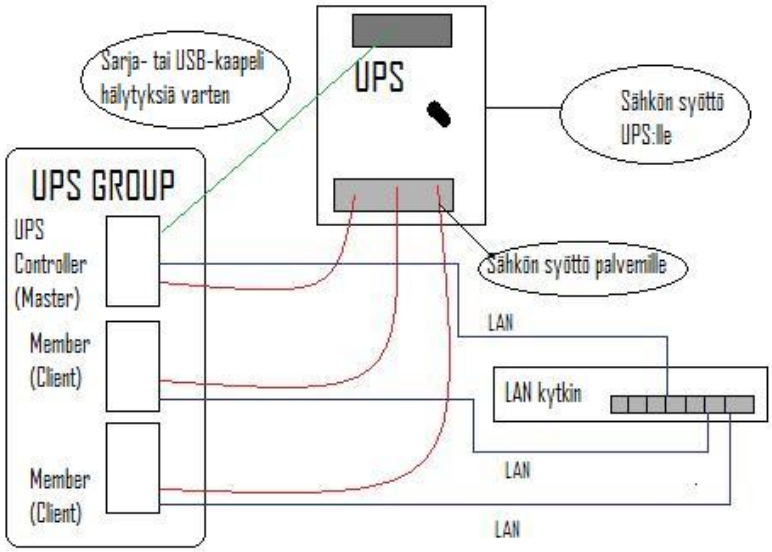
UPSia voidaan valvoa ja etähallita verkkomoduulin avulla. Suhteellisen edullisetkin UPSit voivat sisältää tämän moduulin ja pienemmissä malleissa se voi olla lisävaruste. (Voutilainen S. 2007.)

Sähkökatkoksen sattuessa on tärkeää sammuttaa laitteet hallitusti, erityisen tärkeää tämä on erikoissovelluksissa, esimerkiksi tietokannoissa. Tämän mahdollistamiseksi UPSiin tarvitaan alasajo-ohjelmisto. Alasajo- ja hallintaohjelmistot voivat ohjata useamman koneen alasajoa. Tällaista ratkaisua sanotaan UPS-ryhmäksi (UPS group). (Voutilainen S. 2007.)

2.4 UPS-ryhmä

UPS-ryhmässä yksi koneista on valvontakone (UPS Controller tai Master). Muut koneet ovat ryhmän jäseniä (member tai client). Ryhmän jäsenet ajetaan ensin alas ja viimeiseksi valvontakone. (Voutilainen S. 2007.)

Oikealla oleva kuva on periaatekuva järjestelystä, jossa yksi UPS syöttää kolmea palvelinta. Ylin koneista on ryhmän isäntä tai valvontakone, joka saa hälytyksen sähkökatkosta tässä tapauksessa sarjakaapelilla. Hälytyksen tapahtuessa sen vastaanottaa



Kuva 1 UPS-ryhmä

isäntäkoneessa sijaitseva UPS-ohjelmisto. Tämä ohjelmisto odottaa ennalta määritellyn ajan ennen kuin tekee mitään. Määräajan kuluttua UPS-ohjelmisto lähettää lähiverkon (LAN) kautta ryhmän jäsenille käskyn sammuttaa itsensä. Sammumiskäskyn ottaa jäsenkoneessa vastaan UPS-ohjelmiston client-osa, joka sammuttaa jäsenkoneen hallitusti. Viimeiseksi isäntäkone sammuttaa itsensä hallitusti. (Voutilainen S. 2007.)

Sähkökatkoksen jälkeen kukin ryhmän kone toimii itsenäisesti. Joissain palvelimissa on kuitenkin tarpeen määritellä erikseen verkkokatkon jälkeinen käyttäytyminen. Tällöin on mahdollista valita kone käynnistymään normaalisti tai jäädä odottamaan tarkistustoimenpiteitä. (Voutilainen S. 2007.)

Monissa tapauksissa UPS-ohjelmiston versio voi olla sama isäntä- ja jäsenkoneessa, mutta ohjelmiston konfigurointi on tällöin erilainen. On kuitenkin mahdollistaa asentaa isäntakoneelle ohjelman eri versio kuin jäsenkoneelle. (Voutilainen S. 2007.)

Tärkeää muistaa:

- On tärkeää muistaa merkitä akkujen käyttöönottopäivä UPSiin ja muistaa myös vaihtaa akut ajoissa.
- Kun kytketään jokin laite UPSin perään, täytyy muistaa asentaa alasajo-ohjelmisto (sen ollessa mahdollista).
- Koko järjestelmä tulee testata heti UPSin ja alasajo-ohjelmiston asennuksen jälkeen.

(Voutilainen S. 2007.)

2.5 Tavallisimpia sähkönsyötön ongelmia

UPSeja käytetään korjaamaan ja torjumaan yhdeksää erilaista häiriötyyppiä, mutta kaikki UPSit eivät korjaa kaikkia yhdeksää. UPSin ominaisuusluettelosta käy ilmi, miltä häiriötyypeiltä kyseinen UPS suojaa. (Voutilainen S. 2007.)

Häiriötyyppejä on yhteensä yhdeksän kappaletta ja ne on lueteltu seuraavassa listassa.

- sähkökatkos (blackout) – sähkönsyöttö katkeaa
- jännitteen notkahdus (sag) – lyhytaikeinen alijännite
- jännitepiikki (Power surge, spike) – lyhytkestoinen ylijännite
- alijännite (Undervoltage, brownout) – pitkäkestoinen alijännite
- ylijännite (Overvoltage) – pitkäkestoinen ylijännite
- suurtaajuiset häiriöt (Line noise) – suurtaajuuksia summautuu jännitteeseen
- taajuuden vaihtelut (Frequency) – verkkojännitteen taajuuden vaihtelu
- kytkentätransientit (Switching Distortion) – hyvin lyhytaikaiset yli-tai alijännitteet
- harmoninen särö (Harmonic Distortion) – verkkotaajuuden kerrannaiset summautuvat verkkojännitteeseen.

UPSit voidaan ryhmitellä eri tyyppeihin toimintatavan mukaan, joita käsitellään luvussa 2.6. (Voutilainen S. 2007.)

2.6 UPS-tyypit

On-line ja *off-line* -UPSit ovat kaksi päätyyppiä. Kun UPS syöttää kuormaa jatkuvasti omasta sisäisesti virtalähteestään, on kyseessä *on-line* -UPS. Alatyyppejä ovat *Line-interactive* ja *Dual Conversion*. *Off-line* –UPS eli *standby* -UPS syöttää kuormaan verkkojännitettä ja siirtyy käyttämään omaa virtalähdettä syöttöön vasta verkkojännitteen katketessa. (Voutilainen S. 2007.)

2.6.1 Off-line (standby) UPS

Off-line -UPS syöttää verkkosähköä kuormaan niin kauan, kunnes havaitsee verkkokatkoksen tai jonkin muun häiriötyypin olemassaolon. Tällöin UPS alkaa verkkosähkön sijaan syöttää kuormaa omasta virtalähteestään akun (tai akkujen) kautta. (Voutilainen S. 2007.)

Virtalähteeseen kuuluu akku tai akusto sekä invertteri, joka muuntaa tasajännitteen vaihtojännitteeksi. *Off-line* -UPS pystyy yleensä eliminoimaan tyyppien 1 - 3 häiriöt ja tyypin akkujen käyttöaika on pitkä, koska ne ovat käytössä vain vikatapauksissa. (Voutilainen S. 2007.)

2.6.2 Interactive UPS

Interactive UPS syöttää kuormaa jatkuvasti invertterin kautta. Invertteri puolestaan saa tehonsa verkkosähköstä. Kun virtakatkos tapahtuu, invertteri alkaa ottaa tehonsa sisäisestä akusta. Tämä toiminta tarjoaa kuormalle paremman suojan kuin *off-line (standby)* –toiminta, koska invertteri syöttää kuormaa koko ajan. (Voutilainen S. 2007.)

Tämä tyyppi sisältää yleensä lähtöjännitteen vakavoinnin ja suojaa näin myös pitkäaikaisilta ali- ja ylijännitteiltä sen lisäksi, että eliminoi tyyppien 1 - 5 häiriöt. Akun (tai akkujen) käyttöaika on tässä tyypissä pitkä, sillä se (ne) ovat käytössä vain vikatapauksissa. (Voutilainen S. 2007.)

2.6.3 Dual Conversion online

Duan Conversation online -UPS toimii muuntamalla verkkosähkön vaihtojännitteen tasajännitteeksi ja sitten muuntamalla tasajännitteen takaisin vaihtojännitteeksi, joka sitten syötetään kuormaan. Tämän tyypin UPSia kutsutaan myös *double conversion* tai *dual conversion* -nimityksillä. (Voutilainen S. 2007.)

Tämä tyyppi tarjoaa erinomaisen suodatuksen suurtaajuisille häiriöille, koska akusto on kytketty tasajännitteeseen. Se myös eristää kuorman sähköverkosta ja generoi aaltomuodon uudelleen. Tämä toiminta tuo monia etuja:

- Tarjoaa suojan kaikkia yhdeksää häiriötyyppiä vastaan ja sallii käyttää tulojännitteenä miltei millaista sähköä tahansa (myös generaattorit).
- Lähtöjännitettä ja -taajuutta voidaan muuttaa helposti.
- Sähkökatkon sattuessa ei ole mitään kytkeytymisaikaa vaihtaa verkkosähkön syöttöä akuston ja invertterin käyttöön, koska kuormaa syötetään jatkuvasti invertterin läpi.

(Voutilainen S. 2007.)

Kuormaan syötettävän jännitteen taajuus ja vaihe on synkronoitu verkkosähkön jännitteeseen ja taajuuteen. *Duan Conversation online* -UPSin akkujen käyttöaika on lyhyempi kuin edellisten tyyppien, koska akut ovat käytössä jatkuvasti. (Voutilainen S. 2007.)

2.7 Akustojen vaihto

Jotta UPS voisi tarjota lisävirtaa sähkökatkon sattuessa, tulee akustoja ylläpitää oikein. Suljettujen lyijy-happo-akkujen käyttöaika on 3 - 5 vuotta. On kuitenkin tarpeen muistaa, että akut voivat olla käyttökelvottomia jo kolmen vuoden kuluttua käyttöönotosta. Akun ikä vaikuttaa myös käytettävyysaikaan, esim. uuden akun käyttöaika voi olla yksi tunti, mutta yhden vuoden käytön jälkeen aika on 45 minuuttia ja vähenee vuosi vuodelta. (Voutilainen S. 2007.)

UPSin akkujen vaihto riippuu UPSin mallista. Joissakin tapauksissa käyttäjän on itse tehtävä vaihto ja valmistajan tarjoavat tarkat ohjeet tähän. Joissakin malleissa vaihto on mahdollista suorittaa ns. lennossa eli katkaisematta jännitteen syöttöä kuormaan. (Voutilainen S. 2007.)

2.8 Verkkoratkaisussa käytetty UPS

Aloituspalaverissa tuli ilmi, että Savon Tietokeskus Oy halusi käyttää verkkoratkaisussaan Powerwaren 9300 -räkkisarjan mallia. Sopivan UPS-laitteiston etsiminen oli kuitenkin ensin selvitettävä. Ensimmäinen askel oli selvittää laitteet, joiden virransaanti oli turvattava. Aloituspalaverissa päädyttiin siihen tulokseen, että olisi turvattava kytkimet, palomuurit ja valvontakoneet. Palvelimille oli olemassa omat UPSinsa.

Seuraavaksi oli selvitettävä, minkä verran kytkimet, palomuurit ja valvontakoneet vaativat yhteensä tehoa. Tämä saatiin selville vasta, kun tiedossa oli tarkat tiedot laitteista. Ciscon hierarkkisen mallin mukainen Access-kerroksella sijaitsevaan kahteen Cisco Catalyst 2960S-48FPS-L -kytkimeen tahdottiin PoE-ominaisuus, joka nosti huomattavasti kytkimien tehontarvetta. Kaikkien neljän kytkimien tehontarpeeksi asetettiin 890 W. Palomuurikokonaisuuden maksimi tehontarve oli 380 W (2 * 190 W). Hallinta-kytkimen tehontarpeeksi asetettiin 800 W. PRTG-hallintakoneen tehontarpeeksi asetettiin 300 W.

Kun tiedossa oli tarvittu tehontarve, voitiin siirtyä käyttämään halutun valmistajan (Powerware) sivuilta löytyvää laskinta. Tähän laskimeen tiedot syöttämällä saadaan tietää sopiva UPS. Tehontarvetta lisättiin vielä siten, että yhteensä tarpeeksi tuli 5100 W. Kun Savon Tietokeskus Oy:ltä kysyttiin haluttua laajennusvaraa, oli vastaus, että laajennetaan tarvittaessa lisäakuilla. Tämän vuoksi laajennusvaraa ei tässä ratkaisussa tarvinnut huomioida. Haluttu toiminta-aika oli 12 min. Laskimen mukaan sopivin tuote olisi Eaton 9140 10 000 HW with 1 EBM (EMEA). Tämä UPS on Dual Conversion online -tyyppinen UPS, joten sillä saadaan suoja kaikkia häiriötyyppejä vastaan.

3 LÄHIVERKON LAITTEET JA NIIDEN TOIMINNAN VARMISTAMINEN

Verkkorakenteissa, joissa on tärkeää, että toimivuus säilyy aina, on huomioitava myös mahdollinen laitteen vikaantuminen. Tällöin verkon toimivuus on varmistettava kahdentamalla laitteita. Tämä tapahtuu siten, että verkossa on kaksi samanlaista laitetta, jotka ovat kytkettynä toisiinsa. Kytkentä on toteutettu siten, että toinen laitteista on aina varalla, sitä ei siis käytetä aktiivisesti, mikäli ensisijainen laite on käytettävissä. Mikäli ensisijainen laite kuitenkin vikaantuu, verkon liikenne ja toiminta kulkee varalla olevan laitteen kautta. Yleensä kahdennettujen laitteiden toimivuus on täysin samanlainen, koska varalla olevalla laitteella halutaan nimenomaan korvata ensisijainen laite. Laitteiden ja kytkentöjen kahdennus tuottaa lisäkustannuksia, mutta verkon toiminnan varmistaminen koetaan lisäkustannuksia merkittävämmäksi asiaksi.

Toinen verkon toiminnan varmistamiseksi tehtävä asia on virransaannin varmistaminen. On hyvin merkittävää, etenkin yritys-ympäristössä, varmistaa se, ettei yrityksen toiminnalle merkitsevien laitteiden käytössä tapahdu yllättäviä katkoksia. Tätä on käsitelty tarkemmin luvussa kaksi (s.10).

Savon Tietokeskus Oy halusi verkon, joka rakentuisi seuraavasti: kaksi kytkintä Acces-kerroksena, joista olisi kytkennät palomuuriin. Palomuuriin olisi kytkettynä myös erillinen päätelaite, tietokone, jota käytettäisiin valvomaan verkon ja laitteiden toimintaa. Ensiksi valvonta-ohjelmia tuli esille kaksi: Nagios ja PRTG. Ohjelmiin perehtymisen jälkeen huomattiin kuitenkin, että PRTGllä olisi mahdollista valvoa kaikkia valvottaviksi haluttavia asioita, joten valvonta-ohjelmana päädyttiin käyttämään vain PRTGtä. Valvonta asemalla olisi myös PageGate-ohjelmisto, johon olisi kytkettynä GSM-modeemi, joka siirtäisi PRTG-valvonta-asemalta tulevat hälytykset tekstiviestinä haluttuihin puhelimiin. PageGate-ohjelmistosta enemmän luvussa neljä (s. 19).

Savon Tietokeskus Oy halusi kahdentaa Access-kerroksella olevat kytkimet, mutta koska kahdentamista ei voi tehdä Access-kerroksella vaan Distribution-kerroksella, päädyttiin kahdentamaan kytkimet Distribution-kerroksella. Savon Tietokeskus Oy halusi kahdentaa myös palomuurin, joka haluttiin toteuttaa rautapalomuurina sovelluspalomuuri-ratkaisun sijasta. Palomuuriratkaisuun haluttiin käyttää Cisco ASA 5510-nimistä laitetta, tästä kerron enemmän luvussa viisi (s. 21). Palomuurien väliin haluttiin hallintakytkin, joka hallitsisi sitä, kumpi palomuuri on toiminnassa, jotta palo-

muuriratkaisun toiminnan varmistaminen onnistuisi. Verkkorakenteeseen tuli siis yhteensä viisi kytkintä. Verkkoon kytkeytyneet päätelaitteet kytkeytyisivät Access-kerroksen kytkimiin. Myöhemmin kävi ilmi, että Savon Tietokeskus Oy halusi Access-kerroksen kytkimiin myös PoE-ominaisuuden. Tällä tarkoitetaan ominaisuutta, joiden avulla kytkin antaa virran päätelaitteille omasta virtalähteestään.

Ratkaisussa päädyttiin käyttämään Cisco Catalyst 2960S-48FPS-L -kytkimiä. Näiden kytkinten toimivuus, niin kuin yleensäkin tietoverkkolaitteiden, riippuu laitteeseen tehtävistä konfiguroinneista. Ratkaisuun tekemäni konfiguroinnit löytyvät liitteestä 1. Konfiguroinnit ovat merkittävä osa tietoverkkoratkaisua, sillä siten halutut toiminnot saadaan toimimaan käytännössä.

4 ILMOITUSTEN SIIRTO

Savon Tietokeskus Oy halusi hälytykset verkossa ja sen laitteissa tapahtuvissa häiriöistä sähköpostitse ja tekstiviestitse haluamilleen henkilöille. PRTG-ohjelmistolla saatiin haluttu hälytys sähköpostiin, mutta tekstiviestitse tuleva hälytys piti hoitaa toisella ohjelmistolla tai laitteella. PRTG-ohjelmistoa on käsitelty luvussa seitsemän (s. 30). Aloituspalaverissa Savon Tietokeskus Oy:n toimitusjohtaja Eric Valta mainitsi, että tämän ongelman voisi ratkaista Metis-nimisellä GSM-ilmoitussiirtolaitteella. Myöhemmin kävi kuitenkin ilmi, ettei kyseisellä laitteella saada haluttua ominaisuutta toimimaan. Toimiva ratkaisu olisi käyttää PRTG-ohjelmiston sivuilla suositeltua PageGate-ohjelmistoa.

PageGate on NotePage Oy:n kehittämä maksullinen ohjelmisto. Ohjelmiston avulla voi lähettää viestejä useilla tavoilla, kuten viestinä hakulaitteeseen, tekstiviestin matkapuhelimeen tai viestinä sähköpostiin. PageGate voidaan asettaa tarkkailemaan tiettyä tekstitiedostoa ja kun tähän syötetään jotain tekstiä, voi ohjelmisto lähettää tämän tekstin eteenpäin esimerkiksi sähköpostiin. (*PageGate.*)

PageGate ottaa tietoa vastaan monipuolisesti. Ohjelmisto voi vastaanottaa tietoa mm. ASCII-rajapinnan kautta, nettisivujen kautta ja sarjaportin kautta. Ohjelmisto voi myös lähettää tiedon eteenpäin monessa eri muodossa, kuten esimerkiksi SNMP-muodossa eli sähköpostitse tai GSM-AT-muodossa eli langattoman verkon kautta modeemille tai matkapuhelimeen. (*PageGate.*)

PRTG-ohjelmiston ja PageGate-ohjelmiston toiminnan yhdistämistä ratkaisuun sopivaksi on käsitelty liitteessä 2. Tässä liitteessä on käsitelty myös GSM-modeemin liittämistä PageGate-ohjelmistoon.

5. PALOMUURI

Tämän pääluku perustuu Ciscon *Cisco ASA 5500 Series Adaptive Security Appliances* -dokumenttiin.

Cisco ASA 5500 -tuoteperheen laitteet ovat alustoja, jotka yhdistävät palomuurin, VPN:n, IPS:n sekä sisällön turvaavia palveluita samaan laitteeseen. Cisco ASA on laite, jonka sisälle voi luoda useita virtuaalisia palomuureja. Näitä loogisia palomuureja on mahdollista pitää erillään samassa laitteessa niiden kuitenkin vaikuttamatta toistensa toimintaan. Tämä mahdollistaa palomuuripalveluiden tarjoamisen usealle eri taholle yhdellä laitteella. Näin laite vähentää käyttöönotto- ja käyttökustannuksia sekä tarjoaa monipuolisesti turvallisuutta verkkorakenteeseen.

Cisco ASA kykenee pysäyttämään tietoturvahyökkäykset jo ennen kuin hyökkääjä pääsee tunkeutumaan verkon sisälle. Tämän lisäksi se kontrolloi verkkoa ja siinä toimivien sovellusten aktiivisuutta. ASA takaa myös turvallisen etäkäytön.

Cisco ASA:ssa on laajat hallintarajapinnat, kuten graafinen Cisco Adaptive Security Device Manager (ASDM), laaja CLI ja runsassanainen loki-järjestelmä. ASDM:n avulla voi hallita 5 - 5000 laitetta. ASA:ssa on ohjelmisto (Cisco Security Monitoring) turvallisuuden tarkkailua varten. ASA:ssa oleva Response System (Cisco Security MARS) tarkkailee ja tekee huomioita oikeista verkon hyökkäyksistä ja määrittelee keinot pysäyttää hyökkäykset. Näin ohjelmisto pysyy ajan tasalla hyökkäyksistä ja parantaa sekä yksinkertaistaa vaadittuja tarkastuksia.

ASA on tarkoitettu pienten ja keskisuurten yrityksien sekä yritysten kaukotoimipisteiden käyttöön. Se tarjoaa kehittynyttä turvallisuutta ja verkkopalveluita sekä on helppokäyttöinen. Verkkopalveluita voidaan hoitaa jo aiemmin mainitulla ASDM-sovelluksella.

Data Group Kuopion haluama Cisco ASA 5510 Adaptive Security Appliance tarjoaa palomuuri- ja VPN -palveluita sekä viisi sisäänrakennettua 10/100 Fast Ethernet -porttia. Laite on laajennettavissa ja DMZ-yhteensopiva. Cisco ASA 5510:een voidaan luoda enintään viisi virtuaalista palomuuria.

Cisco ASA:lla on mahdollista laajentaa SSL ja IPSec VPN -valmiuksia, jotta saataisiin tuettua useampia liikkuvia työntekijöitä, kaukosivustoja sekä liikekumppaneita. Ilman lisäosia tuettuna on jopa 250 kpl IPSec VPN-naapuria. Cisco ASA 5510 tukee jopa kymmenen laitteen laitekokoonpanoja ja enintään 2500 SSL VPN -naapuria tai IPSec VPN -naapuria yhdessä laitekokoonpanossa.

5.1 Päivityslisenssejä

Tarpeiden kasvaessa voi Cisco ASA:aa käyttävä yritys asentaa Security Plus -lisenssin. Näin saadaan käyttöön kaksi uutta Cisco ASA 5510 -liittymää, Gigabittinen Ethernet-yhteys sekä mahdollisuus yhdistyä ympärillä oleviin verkkoympäristöihin VLAN-tuen ansiosta. Tämä lisenssi mahdollistaa myös aktiivinen /aktiivinen ja aktiivinen-valmiustilan palvelut. Tällä lisenssillä saadaan käyttöön myös VPN-klusterointi ja kuormituksen tasapainottaminen. Nämä ominaisuudet parantavat VPN-kapasiteettia ja vikasietoisuutta.

Mikäli käyttäjät haluavat laajentaa SSL VPN -skaalautumista, on heidän hyvä hankkia SSL VPN -linsessi. Asentamalla SSL VPN -päivityslisenssin Cisco ASA:n käyttäjät voivat skaalautua jopa 250 SSL VPN:n naapurin kanssa. Jokaisella näistä naapureista on oltava käytössä Cisco ASA 5510.

Cisco VPN FLEX -lisenssin avulla järjestelmänvalvojat voivat reagoida tai suunnitella toimintaansa lyhyen aikavälin liikennepurskeisiin. Tässä lisenssissä on lisäksi SSL VPN -kaukoyhteys käyttäjille kahden kuukauden ajaksi. Näin yhdellä lisenssillä saadaan monia etuja käytettäväksi.

5.2 AIP SSM ja AIP SSC

AIP SSM ja AIP SSC ovat verkkopohjaisia ratkaisuja, jotka turvaavat verkkoa. Sovellukset tunnistavat, luokittelevat ja pysäyttävät vaarallisen liikenteen ennen kuin se vaikuttaa yrityksen verkko-liikenteeseen katkoksia. Sovellukset yhdistävät avoimia estopalveluita uudenlaisiin tekniikoihin. Sovellukset tekevät yhteistyötä muiden verkossa sijaitsevien turvallisuusratkaisujen kanssa ja suojaavat verkkoa OSI-kerroksen kerroksien 2 - 7 välillä.

5.3 Internetin rajalla

ASA:n CSC SSM tarjoaa Internetin rajalla mm. viruksentorjunnan, roskaposti-suodattimen, phishing-suojan ja URL-suojan ja suodattimen. Yritys voi aina laajentaa turvaustaan käyttämällä lisenssejä. Näin yritys voi muokata Cisco ASA -sovelluksesta mieleisensä ja omiin tarpeisiinsa sopivimman.

6 VERKON DOKUMENTOINTI

Tämä pääluku perustuu Kari Pasasen insinöörityöhön
Turun ammattikorkeakoulun tietoverkon aktiivilaitteiden dokumentointi.
Verkon dokumentointi tarkoittaa kaiken verkkoa koskevan tiedon kokoamista.
Se auttaa yritystä turvaamaan jatkuvuutta ja kehitystä, huolehtimaan turvallisuudesta ja ratkaisemaan ongelmia.

Jatkuvuuden turvaamisessa turvataan yrityksen avainhenkilön tietotaito. Verkon dokumentointi on toteutettava siten, että jopa henkilö, jolle verkon rakenne ei ole tuttu, voi helposti ymmärtää sen tehdyistä dokumenteista. Näin turvataan tietotaidon säilyttäminen yrityksen sisällä.

Verkon dokumentoinnilla turvataan myös kehitystä. Kun verkosta on olemassa hyvät dokumentit, on uusien laitteiden kytkeminen verkkoon paljon yksinkertaisempaa, kun voidaan olla varmoja siitä, mihin laitteet kannattaa kytkeä. Tämä auttaa myös yrityksen uusia henkilöitä ymmärtämään verkon rakennetta.

Turvallisuuden huolehtiminenkin paranee dokumentoinnin myötä. Hyvän dokumentoinnin jälkeen on tiedossa mm. laitteiden fyysiset sijaintipaikat, joten esim. tulipalon sattuessa, tiedetään varmasti mitä laitteita sijaitsee missäkin. Tämä auttaa niin hätätilanteissa kuin antaa varmuutta toiminnalle arkitilanteissakin.

Hyvin tehty dokumentointi auttaa myös ongelmien ratkaisemisessa. Dokumenttien avulla säästetään ongelman ratkaisussa aikaa ja vaivaa, kun tiedetään esim. mihin alueelle ongelma voidaan rajata. Tämä on myös kustannustehokasta yrityksen toiminnalle.

6.1 Dokumentoinnin eteneminen

Ensimmäinen tehtävä dokumentoinnissa on esitutkimus, jossa selvitetään miten ja miksi nykyinen verkko toimii. Tulisi selvittää verkon käytetyt, käyttämättömät ja käytettävissä olevat IP-verkot, VLAN:it, laitteet ja niiden versiot sekä niiden tehtäväratkaisut ja syyt niihin sekä tietoturva -asetukset: pääsylistat, palomuurit, verkonhallinta-asetukset, kriittiset palvelut ja henkilöt.

Seuraavaksi tulisi suunnitella, mitä halutaan dokumentoitavan, millä ohjelmalla ja millä tavalla. Yleensä voidaan ajatella siten, että jos tiedon menettäminen aiheuttaa taloudellisia menetyksiä, tulee tämä tieto dokumentoida. Tämä ajattelutapa auttaa hahmottamaan dokumentointiin otettavaa tietoa paremmin.

Dokumenttien lukumäärään on myös hyvä kiinnittää huomiota. Dokumentteja tulisi olla tehtyinä kaksi kappaletta, jotka ovat sijoitettu eri paikkoihin. Näin toimimalla yritetään varmistaa dokumentoinnin saatavuus tarvittaessa.

6.2 Laitedokumentit

Tekniset laitteet ja koneet tulisi dokumentoida. Näistä dokumenteista tulisi selvitä ainakin seuraavat tiedot verkon laitteista:

- laitteiden käyttöohjeet
- tekniset tiedot
- laitepäiväkirja sisältäen: hankinta-ajankohdan, muutoshistorian, takuut, määräaikaishuoltojen ajankohdat ja ylläpitävän yrityksen yhteystiedot
- vastuuhenkilöiden yhteystiedot
- ongelmatilanteiden ratkaisuohjeet.

6.3 Dokumenttien jako turvaluokkiin

Yrityksen dokumentit tulisi jakaa neljään eri turvaluokkaan, joita ovat: julkiset tiedot (public), sisäiset eli ei julkiset tiedot (internal), luottamukselliset tiedot (confidental) ja salaiset tiedot (secret). Verkon dokumentit voivat olla sähköisessä tai paperisessa muodossa. Dokumentointiin on olemassa monia hyödyllisiä ohjelmia, esim. Microsoft Office Exel tai Visio.

6.4 Verkkokartat

Verkkojen dokumentoinnissa luodaan kaksi erilaista verkkokarttaa, fyysinen ja loogi-nen. Verkkokarttojen avulla ylläpitäjä saa käsityksen yrityksen verkkorakenteesta. Karttojen avulla yrityksen ulkopuolinenkin henkilö ymmärtää helposti verkon raken-teen.

Loogisella verkkokartalla ilmennetään laitteiden keskinäisiä yhteyksiä. Nimensä mu-kaisesti loogisella verkkokartalla kuvataan verkon loogista rakennetta. Loogisessa verkkokartassa kuvataan laitteiden loogisia yhteyksiä ja sijaintia.

Fyysisellä verkkokartalla kuvataan verkon fyysistä rakennetta. Tämä verkkokartta rakennetaan yleensä rakennusten pohjapiirustuksien pohjalta, jotta laitteiden todelli-nen fyysinen sijainti on nähtävissä. Näistä pohjapiirustuksista on tätä ennen karsittu kaikki fyysiselle verkkokartalle epälooginen tieto, jotta kartta olisi mahdollisimman selkeä.

6.5 Ylläpito

Dokumenttien on tärkeää pysyä ajan tasalla. Tästä syystä, aina muutoksien tapahtu-essa, tulisi verkkodokumentteja ylläpitää. Näin verkon ylläpitäjät pysyvät ajan tasalla verkon tapahtumista ja henkilöstön vaihtuessa, tieto on nähtävissä dokumenteista.

7 VERKON VALVONTA

Verkkoa voi valvoa usealla eri tavalla. Tässä ratkaisussa on käytetty SNMP-protokollaa ja PRTG-ohjelmistoa. Näitä on käsitelty seuraavissa luvuissa.

7.1 SNMP

Yksi tapa toteuttaa verkon valvonta on käyttää SNMP:tä. SNMP on tietoliikenneprotokolla, jota käytetään TCP/IP-verkkojen hallintaan. Sen avulla voidaan tehdä kyseitä verkon laitteille ja näiden kyselyiden perusteella voidaan laukaista hälytyksiä. Se on suunniteltu yksinkertaiseksi ja helposti käytettäväksi. (*SNMP* Wikipedia.)

TCP/IP-verkonhallintamallissa on neljä osaa:

- Hallinta-asema (Management station)
- Hallinta-agentti (Management agent)
- Hallintatietokanta (Management Information Base, MIB)
- Verkonhallinan yhteyskäytäntö (Network-management protocol). (Tietoverkkolaboratorio *diplomityö.*)

Hallinta-asemalla valvotaan ja analysoidaan verkon laitteita. Hallinta-asema on laite, joka lähettää kyselyitä verkon laitteille ja ottaa niiden lähettämät tiedot vastaan. Yleensä hallinta-asemalla on myös jonkinlainen tietokanta verkon laitteista saatujen tietojen säilyttämistä ja käsittelemistä varten. (Tietoverkkolaboratorio *diplomityö.*)

Hallinta-agentti on verkon laite, jota valvotaan. Agenttia myös hallitaan hallinta-asemasta käsin. Hallinta-agentti vastaa hallinta-asemasta tulleisiin SNMP-kyselyihin ja voi lähettää myös itsenäisesti tietoja verkon tapahtumista. (Tietoverkkolaboratorio *diplomityö.*)

Hallintatietokanta koostuu asioista, joista valvonnassa ollaan kiinnostuneita ja joiden tilaa valvonnassa halutaan tutkia. SNMP:ssä näitä tietoja säilytetään MIB:ssä. (Tietoverkkolaboratorio *diplomityö.*)

Hallinta-asema, hallinta-agentti ja hallintietokanta kytketään yhteen yhteyskäytännön avulla. SNMP:ssä on olemassa neljänlaisia viestejä: GET, GETNEXT, SET ja TRAP. GET-viestillä palautetaan nimetty tieto. GETNEXT-viestillä palautetaan seuraava tieto ja voidaan käydä läpi kaikki tiedot järjestyksessä. SET-viestillä voidaan muuttaa tietoa. TRAP-viestillä raportoidaan jonkin asian muuttuneesta tilanteesta, esim. kytkimen virran katkeamisesta. Jokaisen hallinta-agetin on toteutettava SNMP, UDP ja IP. Tämän lisäksi jokaisessa agentissa on oltava mekanismi, jonka avulla SNMP-viestien

tulkinta onnistuu ja joka hallitsee agentin paikallista tietokantaa (MIB). (Tietoverkkolaboratorio *diplomityö.*)

SNMP toimii IPn UDP-protokollan (User Datagram Protocol) päällä. Se käyttää UDP-portteja 161 ja 162. Porttia 161 käytetään kyselyihin ja porttia 162 hälytyksiin. Koska SNMP käyttää UDP-protokollaa, on SNMP UDP-protokollan mukaan yhteydetön. Tämä tarkoittaa sitä, että verkon laitteiden välillä ei ole jatkuvaa yhteyttä vaan jokainen SNMP-viesti on erillinen. Tällöin viesteihin vastaamisesta on SNMP:n huolehdittava itse. (Tietoverkkolaboratorio *diplomityö.*)

Jotta SNMP-protokolla toimisi verkkoratkaisussa, on SNMP käynnistettävä. Tämä tapahtuu konfiguroimalla se laitteisiin. Ratkaisussa käytettävät kytkinkonfiguraatiot ovat liitteessä 1.

7.1.1 SNMP-valtuusagentti

Koska verkkoratkaisuissa on usein laitteita, jotka eivät tue SNMP:n käytössä tarvittavia UDP- ja IP-protokollia, on mahdollista käyttää SNMP-valtuusagenttia. Tässä SNMP:tä käyttävä laite voi edustaa joukkoa laitteita, jotka eivät tue UDP- ja IP-protokollaa. Kun hallinta-asema lähettää hallinta-agentille kyselyitä ko. agentin edustamista laitteista, agentti kääntää kyselyn edustamiensa laitteiden ymmärtämälle protokollalle ja vastaavasti laitteiden lähettämät vastaukset takaisin SNMP-protokollalle. Myös laitteiden lähettämät TRAP-viestit voidaan kääntää SNMP-protokollalle ja lähettää sitten hallinta-asemalle. (Tietoverkkolaboratorio *diplomityö.*)

7.1.2 Versiot

SNMP:n suurin rajoite on autentikoinnin puuttuminen. Tällä tarkoitetaan sitä, että SNMP ei voi varmistaa tietoa siitä, että tietoja lähettävät laitteet ovat todella niitä laitteita, joilta tietoa halutaan saada. Tämä rajoite on korjattu SNMPv2:ssa. (Tietoverkkolaboratorio *diplomityö.*)

SNMPv2 eroaa SNMP:stä mm. siinä, että se sisältää kaksi uutta viestityyppiä, GetBulkRequest ja InformRequest. Ensimmäisen avulla voivat hallinta-asemat pyytää agenteilta entistä helpommin suuria määriä tietoja. Jälkimmäisen viestityypin avulla agentin on mahdollista lähettää TRAP-tyyppisiä viestejä toiselle hallinta-asemalle. (Tietoverkkolaboratorio *diplomityö.*)

Autentikoinnin lisäksi SNMPv2:n turvallisuutta parantaa tiedon eheyden tarkistukset. Lisäksi viestit voidaan salata. Autentikointi ja eheyden tarkistukset toteutetaan MD5-

algoritmin avulla. Viestin salaamiseen käytetään DES-algoritmia. (Tietoverkkolaboratorio *diplomityö.*)

SNMPv3:ssa turvallisuutta on parannettu vielä lisää. Siinä on mm. sisään rakennettu salaukseen perustuva tietoturva. Autentikoinnin ja eheyden tarkistuksiin voi käyttää joko MD5- tai SHA-algoritmia. (Tietoverkkolaboratorio *diplomityö.*)

7.2 PRTG

PRTG Network Monitor on ohjelmisto, jonka avulla yritys voi valvoa verkkoaan ja sen laitteita. PRTG:n avulla järjestelmävalvojan on mahdollista mitata verkossa sijaitsevien laitteiden käyttämää kaistanleveyttä ja näin mitoittaa laitehankinnat mahdollisimman todenmukaisiksi sekä ennaltaehkäistä ongelmia. PRTG käyttää mm. SNMP- ja NetFlow-protokollaa. (PRTG *Network Monitor.)*

PRTG pyörii jatkuvasti Windows-alustaisessa koneessa. Ohjelmisto seuraa verkon toimintaa ja sen laitteita ennalta määriteltyjen parametrien perusteella. Nämä kerätyt tiedot tallennetaan tietokantaan, josta niitä voi myöhemmin hakea tarkasteltaviksi. (PRTG *Network Monitor.)*

PRTG:ssa on helposti käytettävä web-pohjainen käyttöliittymä. Tämän käyttöliittymän avulla on mahdollista konfiguroida laitteita ja sensoreita, joita haluaa tarkasteltavan. Käyttöliittymän avulla on myös mahdollista luoda erilaisia raportteja. (PRTG *Network Monitor.)*

PRTG sisältää yli 50 sensorityyppiä. Näiden avulla on mahdollista seurata kaikkia tyypillisiä verkon palveluita, esim. PING, http ja SMTP. Sensorin ilmoittaessa jonkin ennalta mainitun raja-arvon ylittyneen tai alittuneen, PRTG laukaisee hälytyksen ja lähettää tapahtumasta tiedon halutulla tavalla, esim. SMS:llä, sähköpostilla tai viestillä hakulaitteeseen. (PRTG *Network Monitor.)*

PRTG:n avulla on mahdollista valvoa verkossa sijaisevien laitteiden käynnistymis- ja sammusaikoja sekä liikennettä ja tehon käyttöä. PRTG käyttää hyväksi myös SNMP:tä ja NetFlow-nimistä apuvälinettä. PRTG:llä on mahdollista tutkia myös verkossa kulkevien pakettien sisältöä ja varmistaa kaapeleiden ja laitteiden, esim. sähköpostipalvelimen, toimivuus verkossa. Myös lähempi laitteiden tutkiminen on mahdollista tutkimalla esim. laitteen suorittimen käyttöastetta. (PRTG *Network Monitor.)*

7.2.1 Hinta

PRTG:stä on saatavilla täydellinen versio ilmaiseksi 30-päivän koekäyttöön. Yksityis- ja yrityskäyttöön on saatavissa täysin ilmainen versio, jossa voidaan käyttää enintään kymmentä sensoria. Mikäli halutaan käyttöön versio, jossa on enemmän kuin kymmenen sensoria, täytyy ostaa PRTG-lisenssi, jonka hinta on 250 €. Koska yhdellä sensorilla tarkoitetaan yhtä valvottavaa asiaa yhdessä laitteessa, ei kymmenen sensoria riitä Savon Tietokeskuksen tarpeisiin. (PRTG *Network Monitor.)*

7.2.2 Raportit

PRTG luo keräämästään tiedoista raportteja. Raportit sisältävät tekstin lisäksi helposti luettavia taulukoita ja muita graafisia kuvauksia verkon tilasta. Raportteja voi seurata nettiselaimen avulla mistä tahansa, esim. matkapuhelimella. (PRTG *Network Monitor.)*

7.2.3 NetFlow

NetFlow on Cisco Systems:n kehittämä verkkoprotokolla, joka kerää IOS-pohjaisista laitteista tietoa niiden kautta kulkevasta IP-liikenteestä. Ciscon reitittimet, joissa NetFlow on käynnissä, keräävät tietoa IP-liikenteestä ja sen jälkeen lähettävät raportit joko UDP- tai SCTP-paketteina verkon valvonta -koneelle. (*Netflow* Wikipedia.)

NetFlow voi kerätä versioittain monenlaista tietoa liikenteestä. Esimerkiksi NetFlow:n versio 5:n paketeissa on seuraavat tiedot:

- versio
- sekvenssi-numero
- SNMP:n käyttämät sisään- ja ulostuloportit
- verkkoliikenteen alkamis- ja loppumisajankohdat millisekunteina laitteen edellisestä käynnistymisestä
- liikenteen määrä bitteinä ja paketteina
- OSI-mallin kolmannen eli verkko-kerroksen otsikot, kuten lähettäjän ja vastaanottajan IP-osoitteet ja portit sekä IP-protokolla sekä ToS-arvo
- verkkokerroksen reititysinformaatiota kuten reitissä seuraavana olevan laitteen IP-osoite.

Näiden tietojen avulla NetFlow rakentaa kattavan kuvan verkossa tapahtuvasta liikenteestä ja sen määrästä. (*Netflow* Wikipedia.)

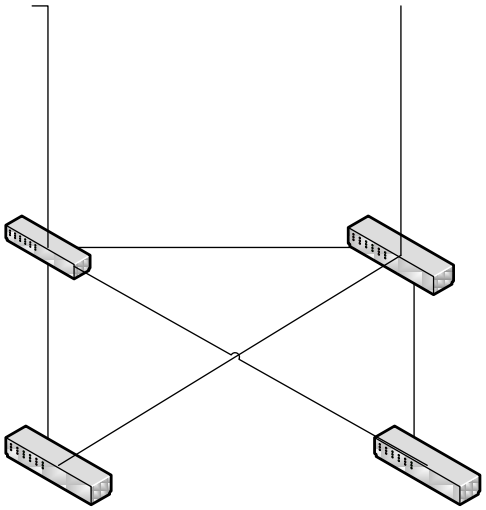
8 KAHDENTAMINEN

Tässä luvussa käsitellään laitteiden kahdentamista. Ensin tarkastellaan laitteiden kahdentamista yleisesti ja sitten Cisco ASA -laitteen kahdennusta. Jälkimmäistä asiaa tarkastellessa on nähtävissä myös vaadittavat konfiguraatiot.

8.1 Kahdentaminen yleisesti ja verkkoratkaisussa

Laitteiden kahdentamisella tarkoitetaan käytäntöä, jossa verkkoratkaisuun sovitetaan kaksi samanlaista laitetta samoilla asetuksilla. Tällä halutaan varmistaa, että mikäli toinen laite rikkoontuu tai muuten sen käyttö estyy, voidaan käyttöön ottaa toinen laite. Jotta laitteen vaihtuminen ei aiheuta suurta katkosta käyttäjille, on laitteiden asetuksien oltava mahdollisimman samanlaiset. Varalla oleva laite voidaan asettaa tarkkailemaan ensisijaisesti käytettävää laitetta esimerkiksi STP-rakenteen avulla, jossa käytettävä laite määräytyy laitteille määriteltyjen arvojen perusteella. Tällöin ensisijaisen laitteen käytön estyessä toissijainen laite huomaa ensisijaisen laitteen käytön estyneen ja alkaa itse hallita verkon toimintaa.

Savon Tietokeskus Oy:lle tehdyssä verkkosuunnitelmassa kahdennettiin kytkimet sekä Cisco ASA -laitteet. Kytkinten kahdentaminen Access-kerroksella on monimutkaisempaa kuin Distribution-kerroksella tapahtuva kahdennus, koska Access-kerroksella tapahtuva kahdennus vaatii mm. työasemiin kahdennetut verkkokortit. Tämän monimutkaisuuden välttämiseksi päätettiin kahdennus toteuttaa Distribution-kerroksella. Koska Data Group Kuopio halusi ratkaisuun kaksi kytkintä, tuli kummallekin käyttökerrokselle kaksi kytkintä ja näiden välille yhteydet menivät ristiin kuvan 2 mukaan.



Kuva 2 Kytkinten kahdentaminen verkkoratkaisussa.

8.2 Cisco ASA:n kahdennus

Ciscon ASA -laite voidaan kahdentaa sijoittamalla verkkoratkaisuun kaksi laitetta yhden sijaan. Kahdennus voidaan toteuttaa kahdella eri tavalla. Active/active Failover -vaihtoehdossa kumpikin laite välittää liikennettä. Tämä vaihtoehto mahdollistaa liikenteen tasaamisen verkossa. Active/active Failover -vaihtoehtoa voi käyttää vain multiple context -tilassa. Multiple context -tilalla tarkoitetaan tilannetta, jossa laitteeseen on tehty useita loogisia palomuureja. Active/standby Failover -vaihtoehdossa vain toinen laitteista välittää liikennettä. Tätä vaihtoehtoa voi käyttää huolimatta siitä, montako loogista palomuuria Cisco ASA:ssa on. Käsittelen tässä työssä tarkemmin vain Active/standby Failover-vaihtoehtoa, sillä se sopi Savon Tietokeskus Oy:n suunnitelmiin paremmin. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Kahdennettaessa laitteita tulee niiden olla samanlaisia malliltaan ja keskusmuistin määrältään sekä liitäntöjen tyyppien ja määrien tulee olla samankaltaiset. Laitteiden täytyy olla myös tilaltaan samanlaiset ja niiden ohjelmistoversioiden tulee täsmätä. Ainakin toisen laitteista tulee sisältää UR unrestricted-lisenssi. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Active/standby Failover-tyyppisessä kahdennuksessa päälaitteen kaatuessa toissijaisena oleva laite ottaa ensisijaisen laitteen IP- ja MAC-osoitteen käyttöönsä ja aloittaa liikenteen välittämisen. Muut verkon laitteet eivät huomaa mitään muutosta liikenteessä, koska käytössä on edelleen sama IP- ja MAC-osoite. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Laitteet pitävät itsenäisesti huolta konfiguraatioidensa samankaltaisuudesta. Kun kumpikin tai jompikumpi laitteista käynnistyy, ensisijainen laite lähettää konfiguraationsa toissijaiselle laitteelle. Ensisijaiselle laitteelle konfiguraatioita kirjoittaessa laite lähettää konfiguraatiot heti toissijaiselle laitteelle. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Laite kaatuu, kun jokin seuraavista asioista tapahtuu:

- laitteen vikaantuminen
- virran syötön vikaantuminen
- ohjelmiston vikaantuminen
- liian moni valvottavan rajapinnan sammuminen
- *no failover active* -käskyn syöttäminen ensisijaiselle laitteelle tai *failover active* -käskyn syöttäminen toissijaiselle laitteelle.

(Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Active/Standby failover-tyyppinen kahdennus tukee sekä tavallista laitteen kaatumista että stateful-kaatumista. Tavallisessa kaatumisessa muut verkon laitteet huomaavat Cisco ASA -laitteen kaatumisen ja niiden yhteydet tulee uusia, kun toissijainen laite aloittaa toimintansa. Stateful-kaatumisessa ensisijainen laite lähettää yhteys-tietonsa toissijaiselle laitteelle. Tämän toiminnan ansiosta verkon muiden laitteiden ei tarvitse uusia yhteyksiään eivätkä laitteet edes huomaa ensisijaisen Cisco ASA -laitteen kaatumista. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Active/Standby Failover-tyyppisen kahdennuksen voi toteuttaa sijoittamalla laitteiden väliin sarjakaapelin tai käyttämällä LAN-pohjaista ratkaisua. Käsittelen sarjakaapelilla toteutettavan ratkaisun ensin. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Kytketään ensisijaiseen laitteeseen kaapelin ensisijainen pää. Seuraavaksi syötetään seuraava komento käynnistettyyn ensisijaiseen laitteeseen:
(1)**hostname(config-if)#ip address <*ensisijainen_ip_osoite*> <*verkko-peite*> standby <*toissijainen_ip_osoite*>**.
Edellä mainitussa käskyssä kohtaan <*ensisijainen_ip_osoite*> tulee ensisijaisen laitteen IP-osoite ja *verkko-peite*-kohtaan ko. osoitteen verkko-peite. Kohtaan <*toissijainen_ip_osoite*> tulee toissijaisen laitteen IP-osoite. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Mikäli laitteessa on useampi looginen palomuuri, tulee jokaiselle loogiselle palomuurille konfiguroida osoitteet erikseen. Vaihtaminen loogisesta palomuurista toiseen onnistuu syöttämällä seuraava käsky:
(2)**hostname(config)#changeto context *loogisen_palomuurin_nimi***.
Edellä mainitussa käskyssä kohtaan *loogisen_palomuurin_nimi* tulee kirjoittaa sen loogisen palomuurin nimi, jota halutaan siirtyä konfiguroimaan. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Mikäli käytetään Stateful-kaatumista, tulee seuraavaksi konfiguroida siihen käytettävä rajapinta seuraavalla käskyllä:

(3)**hostname(config)#failover link *rajapinnan_nimi rajapinta***.

Edellä mainitussa käskyssä kohtaan *rajapinnan_nimi* tulee määritellä rajapinnan looginen nimi ja *rajapinta*-kohtaan tulee määritellä haluttu rajapinta, esim. Ethernet2. Tätä rajapintaa ei tule käyttää muuhun tarkoitukseen. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Seuraavaksi Stateful-kaatumista konfiguroitaessa tulee rajapinnalle määritellä ensisijainen ja toissijainen IP-osoite seuraavalla käskyllä:

(4)**hostname(config)#failover interface ip *<rajapinnan_nimi> <ip-osoite> <verkko-peite>* standby *<ip-osoite>***.

Käskyn <*rajapinnan_nimi*>-kohtaan tulee määritellä rajapinnan nimi, <*ip-osoite*>-kohtaan ensisijainen IP-osoite, kohtaan <*verkko-peite*> ensisijaisen IP-osoitteen verkko-peite ja jälkimmäiseen <*ip-osoite*>-kohtaan toissijainen IP-osoite. Toissijaisen IP-osoitteen tulee olla samalla verkkoalueella ensisijaisen IP-osoitteen kanssa. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Seuraava askel Stateful-kaatumisen konfiguroinnissa on käynnistää rajapinta seuraavilla käskyillä:

(5)**hostname(config)#interface *<rajapinta>***

(6)**hostname(config-if)#no shutdown**.

Käskyjen ensimmäisessä olevaan <*rajapinta*>-kohtaan tulee määritellä käytettävä rajapinta, esim. Ethernet2. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Käynnistetään seuraavaksi kaatumisen tarkkailu seuraavalla käskyllä:

(7)**hostname(config)#failover**.

Käynnistetään toissijainen laite ja konfiguroidaan siinäkin kaatumisen tarkkailu käynnistymään samalla käskyllä kuin ensisijaisessa laitteessakin (7). Kun käsky on annettu, toissijainen laite hakee konfiguraatiot ensisijaiselta laitteelta ja asettaa itsensä toissijaiseksi laitteeksi. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Lopuksi tallennetaan tehdyt konfiguraatiot ensisijailla laitteella seuraavalla käskyllä:
(8)**hostname(config)#copy running-config startup-config**.
Ensisijainen laite välittää nyt konfiguraatiot automaattisesti toissijaiselle laitteelle.
(Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Käsitellään nyt aiemmin mainittua LAN-pohjaista ratkaisua. Tämä ratkaisu käyttää Ethernet kaatumis-yhteyttä. Laitteet voi kytkeä toisiinsa suoraan crossover-kaapelilla, mutta Cisco suosittelee käyttämään laitteiden välissä kytkintä. Tässä ratkaisussa on määriteltävä toissijainen laite huomaamaan kaatumis-yhteyden, jotta konfiguraatioiden noutaminen ensisijaiselta laitteelta on mahdollista. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Ensiksi konfiguroidaan ensisijainen laite. Mikäli käytössä on useita loogisia palomuureja, tulee seuraavat konfiguraatiot suorittaa toteutus-tilassa. Konfiguroidaan ensimmäiseksi aiemmin mainittujen ohjeiden (1) mukaan ensisijainen ja toissijainen IP-osoite. Mikäli käytössä on useita loogisia palomuureja, tulee osoitteet konfiguroida niille erikseen aiemmin mainitun ohjeen (2) mukaan. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Käynnistetään LAN-pohjainen kaatuminen seuraavalla käskyllä:
(9)**hostname(config)#failover lan enable**.
Määritellään laite seuraavaksi ensisijaiseksi laitteeksi seuraavalla käskyllä:
(10)**hostname(config)#failover lan unit primary**.
Määritellään kaatumiseen käytettävä rajapinta seuraavalla käskyllä:
(11)**hostname(config)#failover lan interface *rajapinnan_nimi rajapinta***.
Edellä mainitussa käskyssä kohtaan *rajapinnan_nimi* tulee määritellä käytettävän rajapinnan nimi, esim. failover, ja *rajapinta*-kohtaan tulee määritellä käytetty rajapinta, esim. Ethernet3. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Määritellään seuraavaksi rajapinnan ensi- ja toissijainen IP-osoite aiemmin mainitun ohjeen (4) mukaan. Käynnistetään seuraavaksi rajapinta päälle aiemmin mainittujen ohjeiden (5 ja 6) mukaan. Jos käytössä on Stateful-kaatuminen toimitaan aiemmin mainittujen ohjeiden (3, 4, 5 ja 6) mukaan. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Lopuksi käynnistetään kaatumisen tarkkailu aiemmin mainitun ohjeen (7) mukaan.
Seuraavaksi konfiguroidaan toissijainen laite. Mikäli käytössä on useita loogisia palomuureja, tulee seuraavat konfiguraatiot suorittaa toteutus-tilassa. Käynnistetään LAN-pohjainen kaatuminen aiemmin mainitun ohjeen (9) mukaan ja määritellään seuraavaksi kaatumiseen käytettävä rajapinta aiemmin mainittujen ohjeiden (11) mukaan. Tämän jälkeen määritellään rajapinnan ensi- ja toissijainen IP-osoite aiemmin mainittujen ohjeen (4) mukaan ja käynnistetään rajapinta aiemmin mainittujen ohjeiden (5 ja 6) mukaan. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Määritellään laite toissijaiseksi laitteeksi seuraavalla käskyllä:
(12)**hostname(config)#failover lan unit secondary**.
Käynnistetään kaatumisen tarkkailu aiemmin mainitun ohjeen (7) mukaan. Tallennetaan konfiguraatiot aiemmin mainitun ohjeen (8) mukaan. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Tehtyjä konfiguraatioita voi tarkastella seuraavalla käskyllä:
(13)**hostname#show failover**.
Kaatumisen tarkkailu-toiminnan tilaa voi tarkastella seuraavalla käskyllä:
(14)**hostname#show failover state**.
Kaatumisen tarkkailuun käytettäviä rajapintoja voi tarkastella seuraavalla käskyllä:
(15)**hostname#show failover interface**.
Ko. rajapintojen tilaa voi tarkastella seuraavalla käskyllä, mikäli käytössä ei ole useita loogisia palomuureja:
(16)**hostname#show monitor-interface**.
(Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Mikäli käytössä on useita loogisia palomuureja, rajapintojen tilaa voi tarkastella samalla käskyllä tiettyä loogista palomuuria konfiguroitaessa.
Mikäli halutaan tarkastella jonkin tietyn rajapinnan tilaa, käytetään seuraavaa käskyä:
(17)**hostname#show monitor-interface *rajapinnan_nimi***,
jossa *rajapinnan_nimi*-kohtaan määritellään halutun rajapinnan nimi. (Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Jos halutaan tarkkailla kaatumis-toiminnan konfiguraatioita sillä hetkellä käytettävästä konfiguraatiosta (running konfiguration), voidaan käyttää seuraavaa käskyä:
(18)**hostname#show running-config failover**.
Mikäli haluaa samalla tarkastella konfiguraatioita, joita ei ole muuttanut perustilastaan, voidaan käyttää seuraavaa käskyä:
(19)**hostname#show running-config all failover**.
(Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Testattaessa konfiguraatioiden toimivuutta on ensin testattava, että laitteet päästävät liikennettä lävitseen. Seuraavaksi voi pakottaa ensisijaisen laitteen kaatumaan seuraavalla käskyllä:
(20)**hostname(config)#no failover active**.
Tämän jälkeen tulisi jälleen yrittää lähettää liikennettä laitteiden läpi. Mikäli tämä ei onnistu, tulisi tilannetta tutkia seuraavalla käskyllä:
(21)**hostname#show failover command**.
Kun edellä mainittu testi onnistuu, tulee ensisijainen laite asettaa jälleen ensisijaiseksi seuraavalla käskyllä:
(22)**hostname(config)#failover active**.
On myös mahdollista pakottaa toissijainen laite ensisijaiseksi laitteeksi syöttämällä toissijaiseen laitteeseen seuraava käsky:
(23)**hostname#failover active**.
Tällöin on muistettava kaataa ensisijainen laite aiemmin mainitulla käskyllä (20).
(Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

Jos halutaan kytkeä kaatumisen tarkkailu pois päältä, se voidaan toteuttaa seuraavalla käskyllä:
(24)**hostname#no failover**.
Mikäli halutaan palauttaa epäonnistunut yksikkö, voidaan käyttää seuraavaa käskyä:
(25)**hostname(config)#failover reset**.
(Cisco *PIX/ASA: Active/Standby Failover Configuration Example.)*

8.2 Kahdennus ja STP-protokolla

STP on protokolla, jonka tarkoitus on estää silmukoiden muodostuminen verkossa. Silmukalla tarkoitetaan tilannetta, jossa tietoverkossa kulkeva liikenne kiertää ikään kuin silmukkana samoja laitteita eikä pääse kohteeseensa. STP-protokolla estää silmukoiden muodostumista tarkkailemalla laitteiden välisiä yhteyksiä ja sulkemalla tarpeettomia yhteyksiä. (*Spanning tree protocol* Wikipedia.*)*

STP-protokollassa on aina myöskin jokin laite, joka saa päällikön roolin tiedon välityksessä. Tämä päällikön rooli määräytyy kaikissa kytkimissä olevan arvon (bridge ID) mukaan. Se kytkin, jonka arvo on pienin, saa päällikön roolin. Mikäli päällikkönä toimiva laite jossain vaiheessa kaatuu eikä näin ollen voi välittää liikennettä, toiseksi pienimmän arvon omaava kytkin ottaa päällikön roolin. Näin verkon toiminta jatkuu mahdollisimman moitteettomasti jonkin yksittäisen laitteen kaatumisesta huolimatta. (*Spanning tree protocol* Wikipedia.*)*

STP-protokolla ei toimi laitteissa automaattisesti. Jotta protokolla tulisi toimivaksi, tulee se konfiguroida laitteisiin. Tämä STP-konfigurointi on näkyvissä verkkoratkaisuun tekemissäni konfiguroinnissa, jotka ovat liitteessä 1.

9 POHDINTA

Nykyään on yleistä, että yrityksillä on liiketoimintaa Internetissä tai liiketoiminta tarvitsee tuekseen tietoverkkoja. Tarvittavat tiedot tallennetaan yritystoiminnassa tietokantoihin tietoverkon avulla. Näiden asioiden vuoksi tietoverkon toimivuus on yritystoiminnassa merkittävää.

Tässä opinnäytetyössä suunniteltiin Savon Tietokeskukselle uusi tietoverkkoratkaisu. Kun tiedossa oli tietoverkkoa koskevat tarpeet, valittiin ratkaisuun sopivat laitteet. Työssä tutustuttiin tietoverkkoratkaisussa käytettäviin laitteisiin, kuten UPS-laitteistoihin.

Työssä käsiteltiin verkkoratkaisun turvallisuutta käsittelemällä palomuurilaite Cisco ASA:aa ja verkon valvontaan tarkoitettua PRTG Network Monitor -ohjelmistoa. Koska Savon Tietokeskus halusi valvontaohjelmiston lähettämiä hälytyksiä sekä sähköpostitse että tekstiviestitse, käsiteltiin työssä myös PageGate-ohjelmistoa. Tätä ohjelmistoa käsiteltiin nimenomaan sen ominaisuuden vuoksi, että sen kautta PRTG-ohjelmisto saadaan ilmoittamaan hälytyksistä tekstiviestitse matkapuhelimeen.

Tietoverkkoratkaisun jatkuvan toimivuuden kannalta työssä käsiteltiin laitteiden kahdennusta ja verkon dokumentointia. Työssä selvitettiin Cisco ASA:n kahdennus. Työssä oli myös ohjeistus kahdennuksen toteuttamisesta.

Insinöörityöhön ei kuulunut tietoverkkoratkaisun toteuttaminen. Tämän tietoverkkoratkaisun suunnittelun perusteella Savon Tietokeskus voi päättää, haluaako yritys toteuttaa suunnitelman. Valmiiksi tehdyt konfiguroinnit kytkimiin ja ohjeistukset toimintojen saamiseksi käyttöön helpottavat suunnitelman toteuttamista merkittävästi.

LÄHDELUETTELO

Cisco. *Cisco ASA 5500 Series Adaptive Security Appliances.* [viitattu 20.08.2010] Saatavissa: http://nextclickmedia.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.pdf.

Cisco. *PIX/ASA: Active/Standby Failover Configuration Example* [viitattu 16.09.2010]. Saatavissa: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00807dac5f.shtml.

Eaton*. UPS –selector.* [viitattu 24.08.2010]. Saatavissa: http://powerquality.eaton.com/UPS/selector/byLoad_01.asp?SelectorCountryID=79&ByLoad=Configure+by+Load

NetFlow. Wikipedia. [viitattu 15.8.2010]. Saatavissa: http://en.wikipedia.org/wiki/Netflow.

Notepager. *PageGate*. [viitattu 29.11.2010]. Saatavissa: www.notepager.com/pagegate.htm

Pasanen. K. 2002. *Turun ammattikorkeakoulun tietoverkon aktiivilaitteiden dokumentointi*. Turun ammattikorkeakoulu, Tietoliikennetekniikan koulutusohjelma [viitattu 13.07.2010]. Saatavissa: http://www.dc.turkuamk.fi/graduation/Verkkodokumentointi-kpasanen.pdf. Opinnäytetyö.

PRTG. *PRTG Network Monitor*. [viitattu 2.9.2010]. Saatavissa: http://www.paessler.com/prtg.

SNMP. Wikipedia. [viitattu 15.8.2010]. Saatavissa: http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Spanning Tree Protocol. Wikipedia. [viitattu 22.09.2010]. Saatavissa: http://en.wikipedia.org/wiki/Spanning_tree_protocol

Tietoverkkolaboratorio. *Diplomityö* [viitattu 2.9.2010]. Saatavissa: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html. Diplomityö.

UPS. Wikipedia. [viitattu 2.6.2010]. Saatavissa: http://fi.wikipedia.org/wiki/UPS.

Voutilainen. S. 2007. *Uninterruptible Power Supply (UPS)*. opetusaineisto Savonia-ammattikorkeakoulu Tekniikka/ Kuopio.

KYTKINTEN KONFIGUROINNIT

1) Suljetaan kaikki portit kaikissa kytkimissä

Switch(config)#**interface range *fa0/1-24***

Switch (config-if-range)#**shutdown**

Switch (config-if-range)#**interface range *gi0/1-2***

Switch (config-if-range)#**shutdown**

2)Configuroidaan kytkimien nimet, estetään DNS lookup, asetetaan EXEC-tilan salasanaksi oi34jfdl ja konsoli- sekä vty-yhteyksien salasanaksi ewr345ref.

Switch >**enable**

Switch #**configure terminal**

Switch(config)#**hostname *A1***

A1(config)#**enable secret *oi34jfdl***

A1(config)#**no ip domain-lookup**

A1(config)#**line console 0**

A1(config-line)#**password *ewr345ref***

A1(config-line)#**login**

A1(config-line)#**line vty 0 15**

A1(config-line)#**password *ewr345ref***

A1(config-line)#**login**

A1(config-line)#**end**

3) Avataan A1:n ja A2:n ne portit, joissa on kiinni pääte-laite (esim. fa0/6).

A1(config)#**interface *fa0/6***
A1(config-if)#**switchport mode access**
A1(config-if)#**no shutdown**

4) Avataan kaikissa kytkimissä trunk-porteiksi halutut portit (esim. fa0/1 ja fa0/2).

A1(config)#**interface *fa0/1***
A1(config-if)#**no shutdown**
A1(config)#**interface *fa0/2***
A1(config-if)#**no shutdown**

5)Konfiguroidaan PC.

Vaihdetaan PC:n IP-osoitteeksi yksi osoite valitusta aliverkko-osoitenipusta. Vaihdetaan PC:n default gateway-osoite palomuurin IP-osoitteeksi.

6)Konfiguroidaan VTP kytkimiin.

Tarkistetaan ensin kytkimien tämän hetkiset VTP-konfiguraatiot.
A1#**show vtp status**

Asetetaan D1 VTP serveriksi ja muut kytkimet client:ksi. Asetetaan VTP-alueeksi DG ja salasanaksi Sjlk3irj3i.
D1(config)#**vtp mode server**
D1(config)#**vtp domain *DG***
D1(config)#**vtp password *Sjlk3irj3i***
D1(config)#**end**

D2(config)#**vtp mode client**
D2(config)#**vtp domain *DG***
D2(config)#**vtp password *Sjlk3irj3i***
D2(config)#**end**

A1(config)#**vtp mode client**
A1 (config)#**vtp domain *DG***
A1 (config)#**vtp password *Sjlk3irj3i***
A1 (config)#**end**

A2(config)#**vtp mode client**
A2 (config)#**vtp domain *DG***
A2 (config)#**vtp password *Sjlk3irj3i***
A2 (config)#**end**

7)Konfiguroidaan trunking ja hallinnointi-VLAN kaikkiin kytkimiin

D1(config)#**interface range *fa0/1-5***
D1(config-if-range)#**switchport mode trunk**
D1(config-if-range)#**switchport trunk native vlan *99***
D1(config-if-range)#**no shutdown**
D1(config-if-range)#**end**

8)Konfiguroidaan halutut VLAN:t D1:llä, esim. VLAN 99, jonka nimeksi määritellään management.

D1(config)#**vlan *99***
D1(config-vlan)#**name *management***
D1(config-vlan)#**exit**

9)Konfiguroidaan hallinnointi VLAN:n IP-osoite kaikkiin kytkimiin.

D1 (config)#**interface vlan *99***
D1(config-if)#**ip address *172.17.99.11 255.255.255.0***
D1(config-if)#**no shutdown**

10)Liitetään halutut portit haluttuihin VLAN:hin, esim. portit fa0/6-10 VLAN:iin 30.

D1(config)#**interface range *fa0/6-10***
D1(config-if-range)#**switchport access vlan *30***
Muistetaan tallentaa tehdyt muutokset.

D1#**copy running-config startup-config**

11)Konfiguroidaan VTP Pruning
D1(config)# **vtp pruning**

12)Konfiguroidaan STP

Katsotaan jokaisen kytkimen ohjelmisto-versiot.

D1#**show version**

Katsotaan jokaisen kytkimen nykyiset STP-konfiguraatiot. Varmista, että jokaisen kytkimen STP-arvo on 32768.

D1#**show spanning-tree**

Konfiguroidaan D1 olemaan STP root. Perus STP -arvo kytkimillä on 32768. Seuraavalla käskyllä konfiguroidaan D1:n STP –arvoksi 8192, mikä on pienempi kuin perus –arvo ja näin D1:stä tulee STP root. Numero yksi edustaa käskyssä Vlan1:stä, jossa D1 on STP root.

D1(config)#**set spantree priority *8192 1***

Mikäli A1:een tai A2:een on kiinnitettynä päätelaitteita, esim. PC,
huomioidaan seuraava konfiguraatio. Seuraavassa esimerkissä A1:n portissa fa0/1 sallitaan portfast-ominaisuus, sillä siihen kiinnitetään päätelaite.
A1(config)#**set spantree portfast *fa0/1* enable**

Varmistetaan, että D1 on STP root.

D1#**show spantree *1***

Varmistetaan, että designated root ja bridge ID MAC address-kohdan MAC-osoitteet vastaavat ja että kyseinen osoite on D1:n MAC-osoite.

13)Konfiguroidaan SNMP

Asetetaan ensimmäiseksi SNMP-salasana seuraavalla käskyllä. ro tarkoittaa luku-oikeutta ja rw luku- ja kirjoitus-oikeutta. Kohtaan number voidaan asettaa haluttu pääsylistan numero.

D1(config)# **snmp-server community *string* [view view-name] [ro | rw] [*number*]**

esim. D1(config)#**snmp-server community *comaccess ro 4***

Pääsylistan konfigurointi onnistuu seuraavasti

D1(config)#**access-list *access-list-number*** {**deny** | **permit**} ***source*** [***source-wildcard***]

Tallennetaan tässä vaiheessa tehdyt muutokset.

D1#**copy running-config startup-config**

Konfiguroidaan seuraavaksi niin sanotut trap:t. Niiden avulla voidaan määrittää, mistä tilanteista hälytyksiä syntyy.

Seuraavassa listassa on näkyvissä erilaisia trap-vaihtoehtoja.

c2900 – Luo hälytyksen 2950-kytkimiin liittyvistä ilmoituksista.

cluster – Luo hälytyksen, kun ns.cluster:n konfiguraatiot muuttuvat.

config – Luo hälytyksen, kun SNMP:n konfiguraatiot muuttuvat.

entity – Luo hälytyksen, kun SNMP:n kokonaisuus muuttuu.

HSRP – Luo hälytyksen, kun Hot Standby Router Protocol (HSRP) muuttuu.

MAC notification –Luo hälytyksen MAC-osoitteisiin liittyvistä ilmoituksista.

RTR – Luo hälytyksen SNMP Response Time Reporter (RTR):n perusteella.

SNMP – Luo hälytyksen SNMP:n ilmoituksista.

syslog – Luo hälytyksen SNMP syslog-ilmoituksista.

TTY – Lähettää Cisco enterprise-erikoistuneita ilmoituksia, kun Transmission Control Protocol (TCP)-yhteys sulkeutuu.

UDP-port - Lähettää ilmoituksen isännän User Datagram Protocol (UDP) portti-numerosta.

vlan-membership – Luo hälytyksen, kun SNMP VLAN -jäsenyys muuttuu.

VTP – Luo hälytyksen, kun VLAN Trunking Protocol (VTP) muuttuu.

Tietyt trap -tyypit ovat aina sallittuja, esim. tty ja udp-port. Muut voidaan aktivoida **snmp-server enable** -käskyllä, joka annetaan global configuration -tilassa. **snmp-server host** -käskyä voidaan käyttää global configuration -tilassa, jotta tietty isäntä saadaan vastaanottamaan haluttuja trap -tyyppejä.
Konfiguroidaan kytkimet lähettämään tietoja valvonta-asemalle.
Seuraavalla käskyllä kerrotaan kytkimelle, kenelle lähettää trap-viestejä ja millaisia viestejä lähettää. *informs* | *traps* -kohdassa voidaan valita halutaanko lähettää pelkästään jommankumman tyyppisiä viestejä ja version-kohdassa voidaan määritellä käytettävä SNMP-versio. *community-string-kohdassa* voi määritellä käytettävän salasanan. On kuitenkin suositeltavampaa käyttää yllä mainittua
D1(config)# **snmp-server community string [view view-name] [ro | rw] [number]** -käskyä.
Notification-type -kohtaan voidaan määritellä jokin aiemmin määritelmistäni trap-tyypeistä.
A1(config)# **snmp-server host** host-addr {**informs** | **traps** } {**version** {**1** | **2c**}} *community-string notification-type*

Seuraavaksi määritellään, millaisia ilmoituksia kytkin lähettää. *notification-type* – kohtaan voidaan määritellä jokin aiemmin määritelmistäni trap-tyypeistä.
A1(config)#**snmp-server enable traps** *notification-types*

Varmistetaan tehdyt muutokset seuraavalla käskyllä.

A1#**show running-config**

Tallennetaan tehdyt muutokset.

A1#**copy running-config startup-config**

Asetetaan SNMP Agent:n yhdys- ja sijanti-tiedot sekä sarjanumero.
D1(config)# **snmp-server contact *text***
D1(config)# **snmp-server location *text***
D1(config)# **snmp-server chassis-id *number***
Muistetaan lopuksi varmistaa ja tallentaa tehdyt muutokset.
A1#**show running-config**

A1#**copy running-config startup-config**

Seuraavaksi voidaan rajoittaa SNMP:n kautta käytettäviä TFTP-palvelimia. Näitä palvelimia käytetään tallentamaan ja lataamaan konfigurointi-tiedostoja SNMP:n kautta

palvelimille, jotka ovat määritelty pääsy-listassa. *access-list-number* -kohdassa määrittele perinteinen pääsy –lista eli numeroltaan 1-99 tai 1300-1999.

A1(config)#**snmp-server tftp-server-list *access-list-number***

Seuraavaksi voidaan määritellä halutun kaltaisen pääsy-lista, jonka avulla voidaan sallia tai estää halutun TFTP-palvelimen käytön.

A1(config)#**access-list *access-list-number*** {**deny** | **permit**} ***source*** [***source-wildcard***]

Muistetaan taas lopuksi tarkastaa ja tallentaa tehdyt muutokset.

A1#**show running-config**

A1#**copy running-config startup-config**

SNMP asetuksia voidaan tarkastella seuraavalla käskyllä.

D1# **show snmp**

Lähteet:

Cisco. *Understanding and Configuring Spanning Tree Protocol (STP) on Catalys Switches* [viitattu 10.08.2010]. Saatavissa: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_configuration_example09186a008009467c.shtml

Cisco. *Introduction* [viitattu 10.08.2010]. Saatavissa: http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.html

PRTG:N JA PAGEGATEN TOIMINNAN YHDISTÄMINEN

Kone, johon PageGate voidaan asentaa, täytyy täyttää tietyt ehdot. Prosessorin täytyy olla vähintään Pentium 500 mhz. Vapaata muistia vaaditaan 123 Mb. Kovalevyllä täytyy olla vähintään 50Mb tilaa. Verkkoyhteyden täytyy olla vähintään 300 baudia dialup –yhteyttä varten, täytyy olla olemassa sarja –kaapeli suoria yhteyksiä varten tai omistettu Internet –yhteys. Käyttöjärjestelmäksi soveltuu Windows 2000, XP, 2003 tai Vista (32 bit). Asentaminen onnistuu myös Windows 7 –käyttöjärjestelmään, tästä on nähtävissä ohje osoitteessa http://www.notepage.net/pagegate-windows-7.htm.

PageGate:n asentaminen XP –koneeseen

Ensimmäiseksi tulee ladata PageGate. Tämä onnistuu vierailemalla sivustolla www.notepage.net. Keskellä sivua pitäisi olla PageGate –osio. Tässä osiossa on Download –painike. Paina painiketta hiiren vasemmalla painikkeella. Tämän jälkeen avautuu pieni ikkuna. Paina tässä ikkunassa olevaa Save –painiketta ja valitse mine haluat ohjelman asennus –tiedoston tallentaa.

Seuraavaksi etsi paikka, mihin tallensit tiedoston ja avaa se. Koneesi voi varoittaa tiedoston sisällöstä, mutta käynnistä ohjelma siitä huolimatta. Paina painiketta, jossa lukee ” Install PageGate Server”.

Seuraavaksi ohjelma tarjoaa sinulle luettavaksi ohjeita, joten lue ne ja paina sen jälkeen Next –painiketta. Lue seuraavaksi nähtävä käyttäjän linsenssi -sopimus huolellisesti ja paina Next –painiketta. Valitse, mihin haluat tallentaa ohjelman. Ohjelma on automaattisesti tallentumassa C –levyn Program Files –kansioon, mutta kohteen voi muuttaa toiseksi painamalla Browse –nappia ja valitsemalla haluttu kohde. Paina sitten Next –painiketta. Paina seuraavan kahden sivun kohdalla vain suoraan Next –painiketta.

Nyt asennus on alkanut. Kun asennus on valmis, paina Finish –painiketta. Nyt olet asentanut PageGate –ohjelman onnistuneesti.

Video asennuksesta on nähtävissä osoitteessa: http://www.notepage.net/videos/pagegate-xp-installation.htm. Tämä ohje perustuu ko. videoon.

Tämä kappale perustuu sivuston NotePage:n kotisivun tietoihin.PageGate ottaa parametreja vastaan monista eri kohteista, esim. e-mail ja ASCII –tiedostosta. Tässä tapauksessa käytetään ASCII tiedostoa lukemiseen ja lähetetään parametrit GSM-AT muodossa PageGate:ssa kytkettynä olevaan GSM -modeemiin. Modeemi taas lähettää viestin eteenpäin SMS:nä haluttuihin matkapuhelimiin.

PageGate:n ja PRTG:n toiminnan yhdistäminen

Jotta PRTG –ohjelma saataisiin toiminaan yhdessä PageGate:n kanssa, tulee tehdä asennuksia. Tämä ohje perustuu PAESSLER Knowledge Base:stä löytyneisiin neuvoihin. Ensimmäinen tehtävä on luoda PageGate:en carrier.
Tämä tehdään PageGate Admin:lla valitsemalla valikosta Carriers –osio ja sen jälkeen Settings –kohta. Tähän täsmennetään käytettävät protokolla –asetukset.
Tämän jälkeen tulee luoda recipient eli vastaanottaja. Tämä tehdään PageGate Admin:ssa Recipients –osassa valitsemalla sieltä Settings –kohta. Tänne kirjoitetaan haluttu nimi ja vastaanottaja.
Enabled Services = GetAscii.
Tyyppi = Normal
Carrier = edellisessä kohdassa tehty carrier
Failover = (none)
Email To = haluttu osoite
Max Chars = haluttu määrä
Notify Code = 999
Loput asetukset halutun mukaisiksi.

Nyt asennetaan PageGate käyttämään GetAscii –muotoa tietojen saamiseen. Tämä kappale perustuu NotePagen kotisvuilla olevaan ohje –videoon. Käynnistetään PageGate Admin ja valitaan valikosta Interfaces –osiosta GetAscii –kohdasta Settings. Mikäli on olemassa jo tiedosto, josta tiedot halutaan hakea PageGateen, tämä valitaan kohtaan Polling Directory. Mikäli tiedostoa ei kuitenkaan vielä ole, se täytyy luoda. Tämä onnistuu tekemällä normaaliin tapaan uusi kansio esim. suoraan C –levyn alle. Tämä kansio valitaan Polling Directory –kohtaan kirjoittamalla polku kenttään tai etsimällä se ”…” painikkeen kautta. Polling Interval –asetus kertoo PageGate:lle, kuinka monen sekunnin välein tiedostoa tulee tarkkailla. Perusasetuksena tämä tieto on viisi sekuntia. Tämä tieto muutetaan tarpeelliseksi. Tämän jälkeen valitaan vielä täppä Enabled –kohtaan ja painetaan Apply. Seuraavaksi ohjelma kysyy, halutaanko ko. rajapinta sallia kaikille ryhmille ja vastaanottajille. Valitaan tässä kohdassa Yes. Tämän jälkeen varmistetaan, että PageGate on toiminnassa ja luodaan .BAT –tyyppinen tiedosto PRTG:n \Notifications\exe –kansioon. Kirjoitetaan ko. tiedostoon C:\PageGate\sendpage32.exe prtg_admin %1 %2. Varmista, että ko. polku on sama

kuin polku, joka on täsmennetty PageGate:n Interfaces/GetAscii/Settings –kohdassa eli on edellisen asetuksen tiedoston polku.

Luodaan seuraavaksi ilmoitus PRTG:ssä. Valitaan Home –valikosta Setup ja sitten @notification. Asetaan nimeksi haluttu nimi ja Status –kohtaan started. Mikäli hälytyksiä ei haluta tietyin väliajoin, valitaan Schedule -kohtaan None ja Postpone –kohtaan Yes. Asetetaan täppä "Execute Program" –kohtaan ja valitaan listasta Pagegate. Parametriksi asetetaan esim. "[%sitename]" "%device %name %status %down (%message)". Muista tallentaa asetukset painamalla Save –painiketta.

GSM –modeemin asennus PageGate:en

Ensimmäiseksi tulee varmistaa, että GSM –modeemi tukee GSM AT –komentoja. Tämän jälkeen voidaan jatkaa modeemin asennukseen. Nämä ohjeet perustuvat PageGate:n Teknisen tuen sivuston neuvoihin.
Avataan PageGate Admin PageGate:n palvelimella. Valitaan Connectors –osio ja sieltä Connector 1. Painetaan hiiren vasemmalla napilla Connector 1 –alla olevaa Settings –kohtaa. Vaihdetaan ”Serial Port” –kohtaan portti, jossa modeemin sijaitsee. Sitten painetaan Apply –painiketta.
Painetaan hiiren oikealla napilla Carriers –osassa. Valitaan hiiren vasemmalla napilla Add. Vaihdetaan protokollaksi GSMAT. Asetetaan baudi -määrä, tieto bitit, pariteetti ja pysäytys biti sellaisiksi kuin modeemi vaatii. Nämä tiedot pitäisi löytää valmistajan tiedoista, mutta yleiset tiedot ovat 9600, none, 8 ja 1. Paina Apply –painiketta saattaaksesi muutokset voimaan.
Mikäli käytät PageGate Monitoria, varmista, että Server, Scheduler ja Connectors –kohdat ovat vihreät. Voit myös tarkistaa, että PageGate Admin:in Settings –osiossa on ”Run on this server” –kohdassa vain Scheduler, GetAscii ja Connector 1 valittuina.

PageGate:n automaattinen käynnistäminen

Mikäli PageGate halutaan käynnistyvän automaattisesti Windowsin käynnistyessä, tulee noudattaa seuraavia ohjeita. Näistä ohjeista on nähtävissä video osoitteessa http://www.notepage.net/videos/pagegate-run-styles.htm ja nämä ohjeet perustuvat ko. videoon. Tämä muutos voidaan tehdä vain PageGate:n palvelimella.
Ensin käynnistetään PageGate Admin. Avataan ohjelma –osio painamalla + -näppäintä Program –sanan vieressä. Sitten avataan Settings –osio.
PageGate toimii automaattisesti sovellus –muodossa. Nyt halutaan muuttaa tämä muoto Windowsin palveluna, joten kohdassa ”Run PageGate as:” vaihdetaan näkyvä täppä Application –kohdasta Windows Service –kohtaan ja painetaan Apply –painiketta. Tämän jälkeen ohjelma kysyy käyttäjänimeä ja salasanaa. Tämä tapahtuu sen vuoksi, että PageGate tarvitsee käyttäjä –tiedot Windowsin rekisteriin, joka voi olla salattu. Voidaan käyttää useimmissa järjestelmissä käytettävää tiliä ja jättää käyttäjä –tiedot tyhjiksi ja painaa Apply –painiketta. Mikäli sijaitaan domain:ssa, voi käyttäjä –tietojen antaminen olla välttämätöntä. Käyttäjä –tietojen antamisen jälkeen ja sen jälkeen kun on painettu Apply –painiketta, tulisi nähdä pieni ikkuna, joka kertoo, että käyttäjä –tietoja varmennetaan ”Verifying the account information”, päivitetään palveluja ”Updating Services” ja vaihdetaan käynnistymis –muoto ”Switching Run styles”.
Tämän jälkeen tulisi Windowsissa nähdä kellon vieressä hakulaitteen logo. Klikkaa hiiren vasemmalla napilla logoa ja se antaa vaihtoehtoja, jotka ovat Start, PG Admin, PG Monitor ja Stop. Valitaan Start. Tästä lähtien PageGate käynnistyy automaattisesti Windowsin käynnistyessä.

LÄHTEET

NotePage. *PageGate Basic ASCII Setup Video Tutorial.* [viitattu 5.10.2010] Saatavissa: http://www.notepage.net/videos/pagegate-basic-ascii-setup.htm

NotePage. *PageGate - sms server and paging gateway for networks.* [viitattu 5.10.2010] Saatavissa: http://www.notepage.net/pagegate.htm.

NotePage. *PageGate Switching Run Styles Video Tutorial*. [viitattu 5.10.2010] Saatavissa: http://www.notepage.net/videos/pagegate-run-styles.htm.

NotePage. *PRTG and PAgegate to send TXT messages.* [viitattu 5.10.2010] Saatavissa: http://www.notepage.net/forum/viewtopic.php?t=7568775.

PAESSLER. *Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?* [viitattu 5.10.2010] Saatavissa: http://www.paessler.com/knowledgebase/en/topic/393-how-can-i-send-sms-text-message-notifications-via-a-modem-or-a-mobile-phone-with-prtg.