KARELIA-AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Eerik Kynsijärvi
Ville Toppila

VARMUUSKOPIOINTIPALVELIMEN SUUNNITTELU JA TOTEUTUS BITTIGURU OY:LLE

Opinnäytetyö
Huhtikuu 2016

OPINNÄYTETYÖ
Huhtikuu 2016
Tietotekniikan koulutusohjelma

Karjalankatu 3
80200 JOENSUU
(013) 260 600

Tekijä(t)
Ville Toppila ja Eerik Kynsijärvi

Nimeke
Varmuuskopiointipalvelimen suunnittelu ja toteutus Bittiguru Oy:lle

Toimeksiantaja
Bittiguru Oy

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli suunnitella ja asentaa backup- eli varmuuskopiointipalvelin Bittiguru Oy:lle. Tarkoituksena oli, että palvelin käy hakemassa asiakkaiden aktiivilaitteista, kuten palomuureista, kytkimistä ja reitittimistä, konfiguraatiot ajastetusti talteen. Työhön ei kuulunut työasemien tai palvelinten varmuuskopiointi.

Tavoitteena oli myös tutkia, miten tiedot saadaan haettua laitteista tietoturvallisesti, etteivät ulkopuoliset pysty lukemaan konfiguraatioita ja niissä mahdollisesti esiintyviä salasanoja. Backup-palvelin rakennettiin Windowsille ja käyttöjärjestelmäksi valittiin Windows Server 2012 R2. Tehtävänä oli saada palvelin toimimaan demoverkossa olevien laitteiden kanssa. Opinnäytetyön jälkeen yritys päättää itse, ottaako se palvelimen tuotantokäyttöön.

Kieli
suomi

Sivuja 82
Liitteet 0

Asiasanat
Varmuuskopiointi, tietoturva, verkkolaite

THESIS
April 2016
Degree Programme in Information Technology
Karjalankatu 3
80200 JOENSUU
FINLAND
(013) 260 600

Author (s)
Ville Toppila ja Eerik Kynsijärvi

Title
Planning and building a backup server for Bittiguru Oy

Commissioned by
Bittiguru Oy

Abstract

The purpose of this thesis was to plan and implement a backup server for Bittiguru Oy. The objective was to design a server that automatically retrieves and secures configurations from Bittiguru's customers' devices including firewalls, switches and routers. The backup server was not supposed to acquire data from workstations or other servers.

One objective was to research how to transport these configurations securely, so that the data is unavailable to outsiders. The backup system was built on a Windows Server 2012 R2, which ran on a virtual platform in Bittiguru's server farm. The primary goal was to have a working server in Bittiguru's demo network where the backup server retrieves data from other devices in that network. After building a working system, the company will then decide if they want to implement the backup system to their server infrastructure.

Language	Pages 82
Finnish	Appendices 0

Keywords

Backuping, information security, network device

Sisältö

Lyhenteet ja käsitteet

BATCH	Skriptitiedosto, joka käyttää Windowsin komentorivitulkkia suorittamaan komentoja.
FTP	File Transfer Protocol, protokolla tiedostojen siirtoon kahden laitteen välillä.
KOMENTORIVITULKKI	Tekstipohjainen työkalu, jolla suoritetaan käyttöjärjestelmä- ja ohjelmakohtaisia käskyjä kyseisessä ohjelmassa.
KONFIGURAATIO	Lista komennoista ja protokollista, jotka on otettu käyttöön laitteessa.
PING	TCP/IP-protokollaan perustuva toiminto, jolla lähetetään ICMP ’echo request’ viestejä toiselle laitteelle. Toinen laite vastaa lähettämällä ’echo reply’ -paketin. Käytetään yleensä testaamaan kahden laitteen välistä yhteyttä.
POWERSHELL	Windowsin komentorivitulkki, jolla suoritetaan erilaisia skriptejä automatisoidusti. Perustuu .Net Framework –rajapintaan, jolla hallitaan Windowsin eri objekteja.
RANCID	Really Awesome New Cisco confIg Differ, avoimen lähdekoodin ohjelma, jolla voidaan valvoa ja varmuuskopioida verkkolaitteita.
RDC	Remote Desktop Connection eli etätyöpöytäyhteys on Windowsin työkalu, jolla voidaan kirjautua koneelta toiselle etänä. Se on graafinen ohjelmisto, joka tarjoaa suojatun yhteyden ja sisältää tiedostonsiirtomahdollisuuden koneelta toiselle.

SKRIPTI	Lista komentoja, jotka on tarkoitus suorittaa jossakin komentorivissä. Skriptejä voi kirjoittaa monilla eri ohjelmointikielillä. Näitä kieliä ovat esimerkiksi Bash, Batch, Perl.
SNMP	Simple Network Management Protocol, protokolla, jolla voidaan kerätä ja muuttaa IP-verkossa olevien laitteiden informaatiota.
SSH	Secure Shell, protokolla, jonka avulla voidaan turvallisesti ottaa yhteys etälaitteelle.
TCP	Transmission Control Protocol, tietoliikenneprotokolla, jota käytetään yhteyksien luotiin ja ylläpitoon tietokoneiden välillä.
TFTP	Trivial File Transfer Protocol, protokolla tiedostojen siirtoon kahden laitteen välillä.
UDP	User Datagram Protocol, protokolla, joka mahdollistaa yhteydettömän tietojen siirron laitteiden välillä.
VPN	Virtuaalinen yksityinen verkko (Virtual Private Network) suojaa kokonaan tietoliikenneyhteyden paikasta toiseen. VPN luo fyysisen yhteyden päälle toisen yhteyden, joka voidaan suojata eri salausalgoritmeilla. Se on turvallisempi ja vakaampi protokolla kuin SSH.

1 Johdanto

Tämän opinnäytetyön tarkoituksena oli etsiä ja pystyttää varmuuskopiointijärjestelmä Bittiguru Oy:n testiverkkoon. Varmuuskopioinnin kohteena ovat Bittigurun ja sen asiakasyritysten verkkolaitteet. Järjestelmää etsittiin Windows-pohjaiselle palvelinkäyttöjärjestelmälle, jonka pohjana toimii virtuaalipalvelin. Vaihtoehtona on joko rakentaa järjestelmä itse tai hyödyntää valmiina olevia varmuuskopiointiohjelmistoja.

Ohjelman piti täyttää Bittigurun asettamat vaatimukset, joita ovat mm. tiedonsiirto- ja etäyhteysprotokollat. Näitä protokollia piti myös vertailla ja tutkia, jotta saadaan tietoturvallinen ja vakaa kokonaisuus. Järjestelmän valinnassa oli otettava huomioon myös se, että sen pitää tukea useita eri laitevalmistajan laitteita. Bittigurulla on valmiina ohjelma, jolla tarkkaillaan verkkolaitteiden tilaa, joten rakennettavan järjestelmän tarvitsi keskittyä vain varmuuskopiointiin.

Tässä raportissa kerrotaan tarkemmin varmuuskopioinnista yleensä sekä varmuuskopiointiohjelmistojen käytössä olevista protokollista ja ominaisuuksista. Raportin tavoitteena oli selvittää useiden varmuuskopiointiohjelmistojen toiminta, ja kykyä toimia automaattisena varmuuskopiointipalvelimena. Näistä ohjelmistoista ja järjestelmistä valittiin käyttökelpoisin testaamalla niitä Bittigurun ja Wärtsilän laboratorion testiverkoissa.

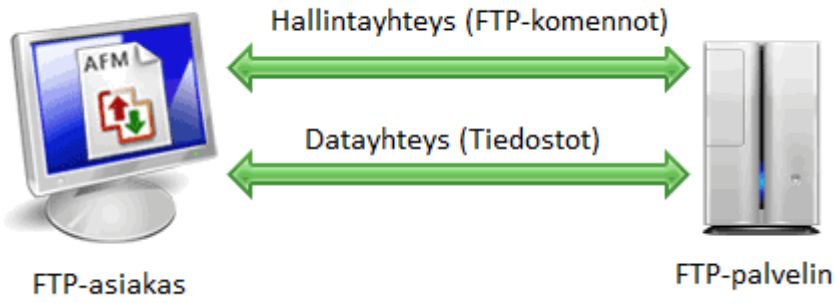
2 Varmuuskopiointijärjestelmän protokollat

2.1 FTP

FTP eli File Transfer Protocol on protokolla, jota käytetään tiedostojen siirtoon tietokoneiden välillä. FTP kehitettiin 1970-luvulla. FTP-yhteys muodostetaan palvelimen (server) ja asiakkaan (client) välille. Asiakas voi ladata (download)

tiedostoja palvelimelta tai lähettää (upload) tiedostoja palvelimelle. FTP-palvelinyhteyden muodostamiseen voidaan käyttää verkkoselainta tai erillistä FTP-asiakasohjelmistoa. Selaimella yhteyttä otettaessa laitetaan http://:n paikalle ftp://. Tässä opinnäytetyössä käytetään WinSCP:tä, joka on FTP-asiakasohjelmisto [1.]

FTP muodostaa kaksi yhteyttä laitteiden välille (Kuva 1). Toista porttia käytetään datan lähetetykseen ja toista yhteyden hallintaan. Datayhteys käyttää porttia 20, ja yhteyden hallinta tapahtuu portin 21 kautta. Hallintayhteyden välityksellä lähetetään komennot. Palvelimelle voidaan antaa mm. tiedoston latauskomento tai tiedustelu palvelimella olevista tiedostoista. Tiedostojen lähetys tapahtuu datayhteyden välityksellä hallintayhteydellä annettujen käskyjen mukaan. Hallintayhteys on auki koko FTP-istunnon ajan, mutta datayhteys avataan vain tiedostoa lähetettäessä ja suljetaan heti, kun lähetys on valmis [2, 631.]



Kuva 1. FTP-yhteys

FTP-palvelin voi olla aktiivinen tai passiivinen. Aktiivisessa yhteydessä asiakas avaa portin ja odottaa, että palvelin yhdistää siihen. Passiivisessa yhteydessä palvelin avaa portin ja odottaa, että asiakas yhdistää siihen. Yleensä on parempi käyttää passiivista tilaa, sillä asiakkaan palomuuri on usein määritetty estämään ulkopuolelta alkunsa saaneet yhteydet. Passiivista yhteyttä käytettäessä asiakas ottaa ensin yhteyden, jolloin palomuuri sallii yhteyteen liittyvät vastaukset palvelimelta [3.]

SSH-palvelimelle kirjaudutaan yleensä käyttäjänimellä ja salasanalla. Jotkin tiedostot voivat olla kuitenkin kaikkien käytettävissä, jolloin niihin ei vaadita kirjautumista. Käyttäjät voivat ladata näitä tiedostoja anonyymisti. FTP ei käytä minkäänlaista tietojen salausta, koska sen kehityksen aikana salaukselle ei ollut tarvetta. FTP lähettää kaiken, salasanat mukaan lukien, selkokielellä verkon yli, jolloin hyökkääjä voi varastaa ja käyttää tunnuksia ja muuta dataa. Tämän takia FTP:tä ei tule käyttää ilman kryptausta, vaan se pitää suojata käyttämällä esimerkiksi Transport Layer Security (TLS) -salausprotokollaa tai SSH-tunnelia. Myöhemmin tässä opinnäytetyössä käytetään FTP:tä tiedostojen siirtoon SSH-yhteyden kautta [2, 642–643.]

2.2 TFTP

TFTP eli Trivial File Transfer Protocol on yksinkertainen protokolla tiedostojen siirtämiseen. Se standardisoitiin ensimmäisen kerran vuonna 1981. TFTP on toteutettu UDP:n avulla (User Datagram Protocol) ja se käyttää porttia numero 69. TFTP on pieni protokolla ja helppo ottaa käyttöön. Siitä puuttuu kuitenkin paljon FTP:ssä olevia ominaisuuksia. TFTP pystyy vain lukemaan ja kirjoittamaan tiedostoja etäpalvelimelta. Alussa TFTP:tä käytettiin lataamaan boot- eli käynnistyskoodeja työasemille, jossa ei ollut kovalevyä. Nykyään sitä käytetään lähinnä siirtämään tiedostoja reitittimiltä, kytkimiltä ja muilta verkon aktiivilaitteilta lähiverkossa [4;5.]

TFTP-yhteyden ottaminen alkaa luku- tai kirjoituspyynnöllä, joka toimii myös samalla yhteyspyyntönä. Kun palvelin sallii yhteyden, data lähetetään 512 tavun paketteina. Vaikka TFTP käyttää UDP:tä, sillä on kuitenkin oma menetelmänsä pakettien perillemenon varmistamiseksi. Jos toinen osapuoli ei vastaa, toinen lähettää uudestaan viimeksi lähetetyn paketin. Kun paketti on alle 512 tavua, se merkitsee lähetyksen päättymistä. Myöhemmin tullut TFTP Blocksize Option -standardi lisäsi lähetettävien pakettien maksimikokoa [4.]

TFTP ja FTP ovat molemmat tiedostonsiirtoprotokollia, mutta niissä on paljon eroavaisuuksia. TFTP ei käytä minkäänlaista autentikointia kirjautumiseen eli

siinä on vielä FTP:täkin huonompi turvallisuus. TFTP on FTP:tä hitaampi, sillä TFTP:n käyttämä datapakettien perillemenon varmistusmenetelmä rajoittaa tiedonsiirtonopeutta. FTP käyttää TCP:tä, joka mahdollistaa suuremman tiedonsiirtonopeuden, sillä siihen sisältyy tiedonkulun hallinta (flow control) ja ruuhkan hallinta (congestion control). Lisäksi FTP käyttää kahta porttia, mutta TFTP vain yhtä. FTP on siis usein TFTP:tä parempi valinta. TFTP on kuitenkin hyödyllinen, kun käynnistetään tietokoneita, joissa ei ole paljon levytilaa [5.]

2.3 SSH

SSH eli Secure Shell on protokolla, jonka avulla voidaan kirjautua turvallisesti etälaitteisiin ja lähettää salattua tietoliikennettä verkon kautta [6]. Sen kehitti SSH Communications Security yrityksen perustaja Tatu Ylönen vuonna 1995 [7]. SSH suunniteltiin korvaamaan telnet ja muut vanhat epäturvalliset etäyhteysprotokollat. SSH toimii turvallisena kanavana kahden laitteen välillä epäluotettavassa verkossa. Toinen laitteista on SSH-asiakas ja toinen SSH-palvelin. SSH:ta käytetään yleensä ottamaan komentorivipohjainen yhteys toiselle laitteelle, jota voidaan sitten hallita komentoriville syötettävien komentojen kautta. SSH:lla pystytään myös suojaamaan muuta liikennettä kuten FTP-liikennettä. SSH käyttää porttia TCP 22 [8.]

SSH:ssa on otettu huomioon monia turvallisuuteen liittyviä asioita. SSH-yhteys on salattu eli kryptattu, jolloin muut eivät pysty lukemaan lähetettävää dataa. Datan eheys on otettu huomioon tekemällä tarkistus, onko dataa muokattu. Sekä asiakaan että palvelimen täytyy tunnistaa toinen osapuoli, jolloin syntyy kunnollinen autentikointi [9]. SSH-protokolla koostuu kolmesta pääkomponentista. Transport Layer Protocol huolehtii palvelimen autentikoinnista, luottamuksellisuudesta ja eheydestä. User Authentication Protocol autentikoi asiakkaan palvelimelle. Connection Protocol jakaa kryptatun tunnelin useaksi loogiseksi kanavaksi [6.]

SSH voi käyttää useita eri autentikointitapoja, mutta yleisimmät tavat ovat julkinen avain (public key) ja salasana. Julkinen avain -menetelmässä asiakas luo

avainparin. Julkinen avain lähetetään palvelimelle, mutta yksityinen avain pysyy vain asiakkaalla. Ideana on, että kaikki data, joka salataan julkisella avaimella, voidaan lukea vain yksityisellä avaimella. Salasana-autentikoinnissa käyttäjä kirjautuu palvelimelle yksinkertaisesti käyttämällä käyttäjänimeä ja salasanaa [9.]

SSH käyttää symmetrisiä avaimia yhteyden salaamiseen. Symmetrisessä salauksessa käytetään vain yhtä avainta datan salaamiseen ja salauksen purkamiseen. Asymmetrisiä avaimia käytetään vain yhteyden muodostamisessa symmetrisessä salauksessa käytetyn avaimen neuvotteluun ja käyttäjän autentikointiin [10.]

Datan eheys varmistetaan hash-funktioilla. Hashin ideana on, että sama viesti ja hash-funktio tuottaa aina samanlaisen lopputuloksen. Tällöin voidaan selvittää, onko data muuttunut matkalla [10.]

SSH:sta on olemassa kaksi eri versiota, SSHv1 ja SSHv2. SSHv1 on jo vanhentunut eikä sitä suositella enää käytettäväksi. SSHv2:ssa on korjattu SSHv1:n heikkoudet. SSHv2 käyttää mm. parempia salaamisstandardeja ja autentikointikoodeja. Se tukee lisäksi julkisten avainten sertifikaatteja sekä istuntoavainten jaksottaisia vaihtoja [9.]

2.4 Batch

Batch-tiedosto on vanha tekniikka, jonka avulla voidaan suorittaa mm. Windows-komentoja automatisoidusti. Niiden helppokäyttöisyyden takia lähes kuka tahansa voi hyödyntää batch-tiedostoja muutamien ohjeiden avulla. Olennainen osa batchia ovat erikoismuuttujat, joiden avulla batch-komentoihin asetetaan parametreja. Oletuksena batch-tiedostot käyttävät Windowsin komentorivitulkkia ’CMD.EXE’ suorittamaan tiedostoon kirjoitetut komennot. Batch-tiedostojen tarkoituksena on suorittaa tiedostoon kirjoitettu sarja komentoja, joita halutaan käyttää useamman kerran. Tällöin ei tarvitse joka kerta tehdä samoja asioita

uudelleen ja uudelleen, vaan säästetään aikaa ja suoritetaan vain yksi batch-tiedosto [11, 372–401.]

Useimmiten batch-tiedoston luomiseen ei tarvita ohjelmointikokemusta. Käyttäjän pitää ainoastaan luoda tavallinen tekstitiedosto, johon kirjoitetaan käsin suoritettavat komennot. Tekstitiedostot pitää tallentaa puhtaana tekstiformaattina, jotta tiedosto toimisi oikein (esim. käyttäen Notepad-ohjelmaa). Tämän jälkeen tiedosto tallennetaan batch- tai cmd-tiedostona, jota Windows tukee oletuksena [11, 372–401.]

Yleisimpiä batch-komentoja:

Call kutsuu toista batch tiedostoa toisesta batch tiedostosta. Batch tiedosto jatkaa toimintaansa kutsun jälkeen normaalisti.

Echo käynnistää tai sulkee echo-ominaisuuden, tai näyttää viestin. Echo komennon avulla voidaan nähdä komennon suoritus ja tulokset reaaliaikaisesti.

Endlocal palauttaa erikoismuuttujat oletusarvoiksi

For suorittaa tietyn komennon useille tiedostoille

Pause keskeyttää batch tiedoston toiminnan ja kysyy komentorivillä toiminnan jatkamista

[11, 372–401]

Batch-tiedostoja voidaan käyttää myös muiden ohjelmien tai komentorivitulkkien aukaisemiseen. Tällöin tiedostoon voidaan syöttää ohjelma ja komentorivikohtaisia käskyjä. Yhteensopivuus riippuu siitä, onko toisella ohjelmalla komentorivitulkkia, joka tunnistaisi komentoja. Useimmat ohjelmat, joilla on tulkki, pystyvät tekemään automatisoituja toimintoja ja skriptejä ilman batch-tiedostojen apua. Kuitenkin käyttämällä batch-tiedostoja helpottuu useiden ohjelmistojen toimintojen integrointi keskenään, lisäksi näiden toimintojen ajastus on vaivattomampaa. Usein muiden ohjelmien sivuilla on ohjeita miten kyseistä ohjelmaa voi-

daan käyttää yhteistyössä batch-tiedostojen kanssa. Yleispätevä sääntö batchin kanssa on, että tiedostoja ja ohjelmia voidaan avata kirjoittamalla batch-tiedostoon tiedostopolku, esimerkiksi ’C:\Users\Käyttäjänimi\Documents\ohjelma.exe’. Tämän jälkeen batch-tiedosto tallennetaan ja suoritetaan, jolloin halutun ohjelman pitäisi aueta.

Seuraavassa vaiheessa lisätään ohjelman komentotulkkiin perustuvia komentoja. Em. komennot kirjoitetaan usein selkeyden vuoksi erilliselle tekstitiedostolle, joka sitten määritetään avattavaksi batch-tiedostossa. Näin toimitaan, koska eri ohjelmien komentorivitulkkien komennot ja syntaksit eroavat jonkin verran Windowsin komentorivitulkista.

2.5 SNMP

SNMP eli ’Simple Network Management Protocol’ on protokolla, jolla kerätään tietoa verkossa olevista laitteista. Protokollasta on kehitetty kolme versiota, jokainen edellistä tietoturvallisempi. Protokolla on kehitetty hallitsija/agentti –kaavalla. Tämä tarkoittaa sitä, että SNMP-hallintaohjelma lähettää kyselyitä (Get, GetNext, Set, jne.) laitteelle tietyin väliajoin, mikä tukee SNMP:tä. Tämä laite vastaa ’Trap-viestillä’ hallintaohjelmalle, mitä laitteen tila on. Sekä ohjelmiston (manager), että laitteen (agent) SNMP-protokollien pitää olla samat, jotta Trap-viestit kulkevat onnistuneesti [12, 634-640.]

Lista SNMP-protokollan viestintätavoista:

Get managerin lähettämä kysely, jossa pyydetään yhden muuttujan arvoa. Kyselyyn vastataan ’Response-viestillä’.

GetNext tässä viestissä manager haluaa tietää seuraavan kohteen MIB-hierarkiassa.

Set set-viesti on managerin pyyntö muuttaa tietyn agentin muuttujan arvoa. Kyseinen pyyntö on ainoa tapa hallita etänä laitetta SNMP:n avulla.

GetBulk manager pyytää useita ’GetNext-tiedusteluja’. Vastauksessa on maksimimäärä dataa. Maksimimäärän määrittelee ’GetBulk-pyynnön’ raja-arvot.

Response agenttilaitteen lähettämä viesti hallintalaitteelle (managerille), joka sisältää kaiken pyydetyn tiedon. Jos agentilta on pyydetty tietoja jota ei ole, viesti sisältää virheilmoitukset kyseisistä puutteista.

Trap viesti on agenttilaitteen lähettämä huomautus, jossa yleensä ilmoitetaan laitteen tapahtumista.

Inform hallintalaitteen lähettämä kuittaus Trap-viestistä.

[13]

SNMP:n viestit kulkevat ’yhteydetöntä’ UDP/IP palvelua käyttäen. Yhteydetön tarkoittaa tässä tapauksessa sitä, ettei mitään ennalta määritettyä reittiä ole rakennettu viestien kulkemiseksi, joten viestit ovat alttiita häiriöille, eivätkä välttämättä aina saavu perille. Jos vastauksia ei kuulu kohdelaitteelta/ohjelmalta tietyn ajan kuluessa, lähetetään viestit uudelleen. SNMP vaatii ’Data Link-kerroksen’ protokollan muodostaakseen yhteyden hallintalaitteesta kohdelaitteeseen. Näitä ovat esimerkiksi ’Ethernet LAN’ ja ’frame relay WAN’. Vaikka yhteys hallintalaitteesta hallittavaan laitteeseen katkeaisi, hallintalaitteen toiminta säilyy vakaana eikä katkennut tai heikko yhteys sekoita sen toimintaa [12, 634-640.]

SNMP:n kolmesta versiosta käytetyin tällä hetkellä on SNMPv1, koska siitä on karsittu kaikki ylimääräiset autentikointi ja kryptausprotokollat, jotka pitäisi manuaalisesti konfiguroida agentteina toimiviin laitteisiin. Kuitenkin yhä useammat laitteet ja ohjelmat alkavat tukea SNMPv3:sta sen turvallisuuden takia. SNMPv3:ssa jokaisella SNMP-objektilla on tunniste (EngineID). Tällöin SNMP-viestintä toimii vain ja ainoastaan niiden laitteiden välillä, jotka tietävät toistensa tunnisteet. Tämän lisäksi SNMPv3:een on lisätty USM-malli (User-based Security Model), jolloin SNMP:n käyttämiseen voidaan vaatia erilliset käyttäjätunnukset ja yksityisyyden suojaukset. Käyttäjätunnuksissa käytetään MD5:sta ja SHA

-salausta, sekä yksityisyyden suojauksessa CBC_DES- ja CFB_AES_128-protokollia [12, 634-640.]

SNMP hakee tietoja laitteiden kohteista eli muuttujista, jotka täyttävät tietyt perusvaatimukset. Vaatimuksia ovat nimi, syntaksi ja koodaus. Haettavan kohteen nimellä (Object ID) ei saa olla päällekkäisyyksiä muiden nimien kanssa eli sen pitää olla uniikki. Syntaksi puolestaan määrittelee tiedon tyypin eli onko kyseessä numerosarja vai jokin toinen tietotyyppi. Koodaus kertoo miten kyseinen data jaksotetaan lähetystä varten [12, 634-640.]

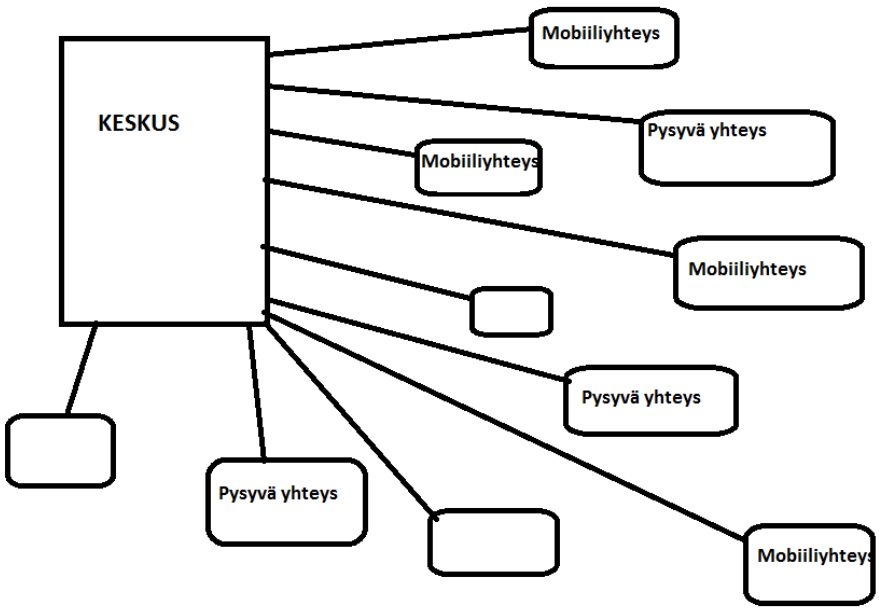
Jokaisella agenttilaitteella on hierarkkinen tietokanta laitteen eri muuttujista. SNMP-hallintaohjelmisto käyttää kyseistä muuttujatietokantaa hakeakseen tietoja, ja kääntää tiedon luettavaan muotoon. Tietokantaa kutsutaan yleisesti nimellä MIB (Management Information Base). Tietokanta sisältää ennalta määritetyt arvot, jotka on mahdollista lähettää hallintalaitteelle. Kyseiset arvot kerätään MIB-tietokantaan väliajoin. MIB:stä on muodostunut standardi, jolloin kaikki laitteet suurin piirtein sisältävät samankaltaiset perustiedot laitteistoistaan [14.]

2.6 VPN

VPN eli ’virtual private network’ tarkoittaa väliaikaista fyysistä reittiä julkisen verkon yli. VPN-ominaisuus löytyy tyypillisesti reitittimistä. VPN:n avulla on tarkoitus lähettää dataa paikasta toiseen, minkä takia yhteyden pitää olla hyvin suojattu. Useimmiten VPN toimii OSI-mallin data link- tai network-kerroksessa. VPN:stä on olemassa siis kaksi perusversiota, OSI-mallin kakkoskerroksen versio sekä kolmoskerroksen versio. Kakkoskerroksen VPN muodostuu ’permanent virtual circuiteista’ (PVC), joka on looginen yhteys kahden pisteen välillä verkossa. Kerroksen 2 PVC on pysyvä yhteys ’frame relay’ ja ’asynchronous transfer mode’ verkoissa. Käytännössä se tarkoittaa sitä, että fyysisen verkkoyhteyden päälle rakennetaan toinen, looginen yhteys [15;16.]

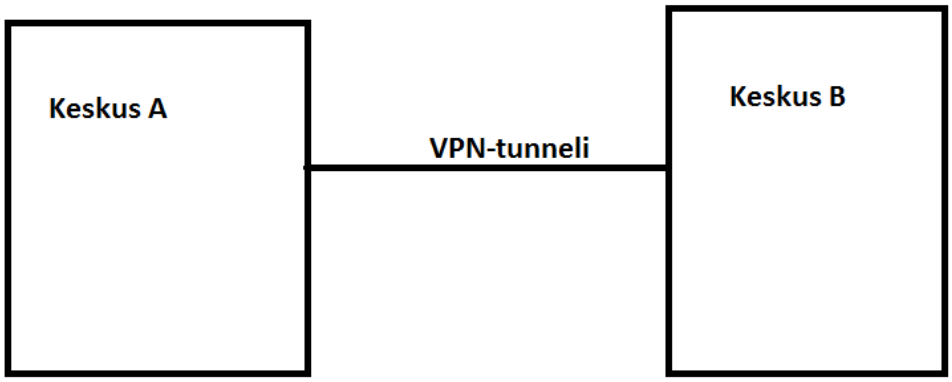
Kakkoskerroksen VPN:stä tekee turvallisen se, että PVC:tä pitkin kulkeva data on ’end-to-end’ –tyyppiä. Tämä tarkoittaa sitä, että data voi ainoastaan tulla tietyistä paikoista ja päätyä tiettyyn paikkaan. Kolmoskerroksen VPN kulkee esimerkiksi Internetin yli, joten tässä tapauksessa pitää käyttää autentikointia yhteyden lähteen tunnistamiseen. Koska käytössä ei ole ennalta määritettyä reittiä, kuten kakkoskerroksen PVC:t, pitää luoda väliaikainen reitti mm. reitityksen takia. Tällöin VPN:n kohde on väliaikainen, koska kohteena on verkossa olevan reitittimen julkinen osoite, joka ohjaa sitten yhteyden eteenpäin eri osoitteelle ja reitittimelle. VPN:n reitit vaihtelevat myös reitittimien aktiviteetin mukaan [15.]

VPN:stä on olemassa kaksi perusluokkaa. Toinen on etäyhteys (remote access) ja toinen paikasta paikkaan (site-to-site) yhteys. Etäyhteys VPN:ssä otetaan sekä ennalta määritetyistä paikoista, että vaihtelevista sijainneista tiettyyn keskukseen. Etäyhteydessä otetaan yhteys yhteen tai useampaan laitteeseen keskuksessa, riippuen keskuksessa olevan VPN-laitteen ominaisuuksista (Kuva 2). Yksi etäyhteyden mahdollisuus on soittaa puheluita puhelinverkon kautta keskukseen [15.]



Kuva 2. Remote-access VPN

Paikasta paikkaan (Site-to-Site) VPN:ssä yhdistetään kaksi ennalta määritettyä sijaintia keskenään julkisen verkon yli (Kuva 3). Tällöin kyseisistä paikoista voidaan ottaa suojattuja yhteyksiä molempien sijaintien tietokoneisiin ja laitteisiin. Tässä VPN:ssä voidaan käyttää reititintä, palomuuria tai jotain muuta alustaa, joka toimii VPN-yhdyskäytävänä. Paikasta paikkaan VPN vähentää myös manuaalisen konfiguroinnin määrää, koska yhteydessä ei tarvita luoda yksittäisiä VPN-asiakkaita tai autentikoida jokaista käyttäjää erikseen [15.]



Kuva 3. Site-to-Site VPN

VPN:iä voi olla samanaikaisesti useampi käytössä. Esimerkiksi kuvan 3 keskuksilla A ja B voi myös olla käytössä muita paikasta paikkaan- sekä etäyhteys-VPN:iä. VPN-yhteyksiä suojataan usealla tavalla, jotta yhteys olisi mahdollisimman turvallinen. Yleisin tapa on ’IP security’ (IPSec), jota voidaan käyttää kuljetus- tai tunnelitilassa VPN-datan salaamiseksi. Kuljetustila salaa vain viestin data-paketissa (payload), kun taas tunnelointi salaa koko paketin. Toinen tapa salata VPN-yhteys on SSL (Secure Sockets Layer) ja TLS (Transport Layer Security). Metodit perustuvat ‘kättelyautentikointiin’ (handshake), jossa protokollat sopivat asiakas- ja isäntälaitteiden verkkoasetuksista. Yhteyden muodostamiseksi kättelyautentikoinnissa käytetään suojausavaimia varmentamaan yhteys [15.]

Kolmas yhteyden salaustapa on pisteestä pisteeseen -tunnelointi (Point-To-Point Tunneling Protocol, PPTP). Tässä tapauksessa yhdistetään etäkäyttäjä tiettyyn palvelimeen verkon yli. Protokolla on suosittu, koska se on asennettu Windows-järjestelmiin oletuksena ja se on helppo ottaa käyttöön. Neljäntenä ja viimeisenä suosittuna salaustekniikkana on kakkoskerroksen tunnelointi (Layer 2 Tunneling Protocol, L2TP). Se käyttää 'pre-shared key –metodia' tai suojausavaimia varmentamaan yhteyden. [15]

3 Varmuuskopiointi

Varmuuskopioiminen on olennainen osa palvelinympäristöä ja verkkoinfrastruktuuria. Kun järjestelmät pettävät, on oltava jonkinlainen varasuunnitelma toimintakyvyn ylläpitämiseksi. Tätä varten on kehitetty varmuuskopiointiohjelmistoja sekä -metodeja, joilla voidaan automaattisesti tallentaa ja palauttaa dataa tehokkaasti. Koska jokaisella yrityksellä on yksilölliset tarpeensa, on tärkeää tutkia, minkälainen järjestelmä tukee tarpeita sekä kustannustehokkaasti että luotettavasti. Varmuuskopiointijärjestelmää suunniteltaessa pitää ottaa huomioon useita tekijöitä, joihin käyttötarpeet perustuvat.

Ensiksi halutaan tietää mitä varmuuskopioidaan. Ovatko kyseessä kriittiset palvelimet, joiden saatavuuden pitäisi olla korkea vaiko vain yrityksen käyttäjien henkilökohtaiset tiedostot, jotka on otettava talteen kerran kuukaudessa? Toisena tekijänä ovat kustannukset. Kuten palvelinlisenssit, saattavat varmuuskopiointiohjelmat ja –lisenssit maksaa useita kymmeniä tuhansia euroja vuodessa. Toisaalta kalliimpiin lisensointiohjelmistoihin kuuluu yleensä aina ympärivuotinen tuki, mikä ehkä kompensoi hintaa. Kustannuksia tulee ohjelmiston lisäksi myös tietokoneesta, jossa palvelinohjelmisto on. On edullisempaa, jos virtualisoidaan varmuuskopiointipalvelin. Mutta koska yleensä varmuuskopiointipalvelin halutaan pitää erillään muista palvelimista, on investoitava ainakin toiseen virtualisointialustaan, jolloin yksittäinen fyysinen palvelin tulisi mahdollisesti kustannustehokkaammaksi. Varmuuskopiointipalvelimet pidetään erillään muista palvelimista, jotta esimerkiksi tulipalon sattuessa eivät kaikki palvelimet hajoaisi.

Kolmantena kysymyksenä on palvelimen ylläpito. Yleensä palvelimien pitää olla joka viikko 24 tuntia vuorokaudessa toiminnassa, jolloin fyysisille palvelimille pitää ehkä vaihtaa jotain kuluvia osia, huolehtia tietoturvasta ja huolehtia palvelimen päivityksistä ja mahdollisista tulipalovaaroista. Tällöin kannattaa harkita kolmannen osapuolen pilvipalveluratkaisuja. Näissä on kuitenkin vaarana se, että muut saattavat päästä käsiksi yrityksen tärkeisiin tietoihin. Toisaalta, jos yrityksellä on jo valmiina palvelinympäristö, joita huoltavat It-asiantuntijat, ei pilvipalveluratkaisuihin tarvitse välttämättä turvautua. Yleensä varmuuskopiointiohjelmistot eivät vaadi kohtuutonta määrää perehtymistä ja osaamista.

Neljäntenä huomioitavana tekijänä on varmuuskopioitavan datan määrä ja kasvu. Jokaisessa palvelinympäristössä ja verkkoinfrastruktuurissa datan määrä lisääntyy jatkuvasti. Tämän takia pitäisi pystyä ennustamaan esimerkiksi noin viiden vuoden kasvu, jolloin varmuuskopiointipalvelinta ei tarvitsisi modifioida jatkuvasti. Tässä vaiheessa erityisesti virtualisointi on kätevää, koska virtuaalipalvelimien tallennustilan määrää on helppo lisätä, jos fyysisellä palvelinalustalla riittää kapasiteettiä.

3.1 Varmuuskopiointityypit

Useimmat varmuuskopiointiohjelmistot tarjoavat pääasiassa kolmea erilaista varmuuskopiointitapaa. Eri tapojen avulla pyritään maksimoimaan tiedostojen turvallisuus sekä minimoimaan tarvittava tallennustila. Nämä kolme tunnetuimpaa tapaa ovat full backup, incremental backup sekä differential backup. Muut tavat ovat erilaisia variaatioita kolmesta pääasiallisesta varmuuskopiointimetodeista [17.]

Monissa tietokoneissa tulee mukana laitevalmistajan henkilökohtainen varmuuskopiointiohjelma, joka on asennettu valmiiksi ja toimii heti, kun tietokone otetaan käyttöön. Tällöin, jos laite ei esimerkiksi käyttöjärjestelmävirheen takia pysty käynnistymään oikein, pystytään ohjelman avulla palauttaamaan toimiva kopio järjestelmästä. Tällöin ohjelma ei käynnisty käyttöjärjestelmän rajapinnalla, vaan avautuu automaattisesti tietokoneen vielä käynnistyessä. Nämä ohjel-

mat varmuuskopioivat tietokoneen yleensä huomaamattomasti aika ajoin, eikä käyttäjän tarvitse välittää ylimääräisistä prosesseista. Käyttäjä itse voi muuttaa aikataulutusta ja sen voi halutessaan ottaa pois käytöstä tai poistaa koko ohjelmiston tietokoneelta.

3.2 Full backup

Ensimmäinen ja yksinkertaisin varmuuskopiointitapa on full backup eli täysi varmuuskopio. Täysi varmuuskopio ottaa kopion kaikista tietokoneen tiedostoista, käyttöjärjestelmä mukaan lukien. Ohjelmistot pakkaavat usein oletuksena kaikki tiedostot samaan pakettiin (set), josta varmuuskopiointiohjelman on helppo palauttaa ne tarvittaessa. Huonona puolena täydessä varmuuskopioinnissa on se, että se joudutaan suorittamaan silloin, kun laite on vähäisessä käytössä tai toimettomana. Täysi varmuuskopioiminen on raskas prosessi ja vie paljon suorituskykyjä koneelta. Tämän lisäksi tiedostojen muokkaaminen ja käyttäminen varmuuskopioinnin aikana saattaa aiheuttaa virheitä varmuuskopioissa [17.]

Yleensä täydet varmuuskopiot ajetaan vain kerran viikossa, koska niiden suoritukseen kuluu paljon aikaa, riippuen kopioitavan laitteen tyypistä ja tiedostomäärästä. Jos kyseessä ovat tärkeät palvelimet tai laitteet, joiden pitää olla päällä jatkuvasti, otetaan niistä ehkä täydet varmuuskopiot kerran päivässä. Yksi suuri vaikuttava tekijä varmuuskopioinnin kestossa on varmuuskopioivan laitteen tehokkuus ja yhteyden kaistanleveys. Tällöin suuretkin määrät dataa voidaan kopioida lyhyessä ajassa, jos laitteet ovat tarpeeksi tehokkaita ja yhteys varmuuskopioitavan laitteen ja varmuuskopiointiohjelman välillä on erinomainen.

3.3 Incremental backup

Incremental eli lisäävä varmuuskopiointi on täyttä varmuuskopiointia kevyempi prosessi. Se hakee vain tiedostot, jotka ovat muuttuneet viimeisen varmuusko-

pioinnin jälkeen, varmuuskopiointitavasta riippumatta. Tiedostoja vertaillaan niiden Viimeksi muokattu- tai Luotu-päivämäärien avulla. Tällöin uusien tiedostojen tallennustila on kohtalaisen pieni ja vältytään samojen tiedostojen kopioinnilta uudelleen. Koska varmuuskopio ei kuormita laitetta suunnattomasti, se voidaan suorittaa paljon useammin kuin täysi varmuuskopio. Tämä mahdollistaa sen, että varmuuskopiointi voidaan suorittaa halutessa useita kertoja päivässä [17.]

Riippuen varmuuskopiointiohjelman ominaisuuksista ei lisäävä varmuuskopiointiohjelma tee uutta kansiota tiedostoille, vaan sijoittaa ne aiemmilla kerroilla kopioitujen kanssa samaan kansioon korvaten ne. Kuitenkin näissä ohjelmistoissa on mahdollista luoda uusille kopioiduille tiedostoille omat kansiot, jotta vanhemmat versiot säilyisivät. Tällöin ohjelman kannattaa luoda samojen tiedostojen eri versioiden säilömiseen omat kansiot aikaleimoilla, johon kaikki tiedostot kopioidaan. Toisaalta se taas saattaa sekoittaa ohjelmiston toimintaa, mikäli halutaan palauttaa koko järjestelmä kerralla.

3.4 Differential backup

Differential backup kopioi vain sen datan, joka on muuttunut viimeisestä täydestä varmuuskopiosta. Se toimii ensimmäisellä toimintakerrallaan käytännössä samoin kuin lisäävä varmuuskopiointi. Tämä ’erotteleva’ tapa vie enemmän tallennustilaa kuin lisäävä varmuuskopiointi, koska se kopioi usein muuttumattomiakin tiedostoja uudelleen. Erottelevaa kopiointia pitää aikatauluttaa siten, että se ei häiritse laitteen käyttäjiä, koska se vie enemmän prosessointitehoa ja suoritusaika on pidempi [17.]

Tämän version varmuuskopioista on hankalampaa löytää tietyt versiot tiedostoista, sillä ohjelma ei erittele muuttuneita tiedostoja muuttumattomista, kun järjestelmästä tehdään taas täysi varmuuskopio. Kuitenkin erotteleva varmuuskopiointi varmistaa sen, että kaikki muuttuneet tiedostot täyden varmuuskopion jälkeen ovat tallessa, koska ne on kopioitu useampaan kertaan. Eli vaikka yhdessä tai useammassa erottelevassa varmuuskopioinnissa ilmenisi tiedostojen

korruptoimista tai yhteysvirheitä, jolloin tiedostoja puuttuu, ne haetaan silti uudelleen seuraavassa varmuuskopiossa. Useat ohjelmistot ilmoittavat virheistä mm. sähköpostitse, jolloin varmuuskopioinnin hallitsijan on helppo käynnistää varmuuskopiointi tarvittaessa uudelleen.

3.5 Varmuuskopiontityyppien vertailu

Kolmesta pääasiallisesta versiosta ainoastaan täysi varmuuskopiointi toimii itsenäisesti. Sekä erotteleva että lisäävä varmuuskopionti toimivat täyden varmuuskopioinnin rinnalla. Kuitenkin niissä molemmissa pitää vähintään käyttää täyttä varmuuskopiointia yhden kerran. Tämän jälkeen varmuuskopiointitavat toimivat itsenäisesti. Kaikki kolme tapaa vaativat kuitenkin hyvän yhteyden kopioitavaan kohteeseen, jotta varmuuskopiointi onnistuu. Niillä kaikilla on myös hyvät ja huonot puolensa (Kuva 4), ja niiden käyttö riippuu siitä, minkälainen varmuuskopiointisuunnitelma on.

Kopiointityyppi	Tallennustila	Ajoitus	Luotettavuus
Täysi	Suuri	Harvoin. Kerran viikkoon tai kuukauteen. Kriittiset laitteet kerran päivässä.	Tiedostojen kopiointiaika suuri. Tiedostojen häviämisriski täten kohtalainen.
Lisäävä	Pieni	Usein. Käytännöllinen jopa pari kertaa päivässä ajettuna.	Tiedostojen kopiointiaika pieni, tiedostojen häviämisriski pieni.
Erotteleva	Keskiverto	Usein. Järkevintä ajaa kerran 1-2 päivässä.	Tiedostojen kopiointiaika kasvaa ajan kuluessa. Tiedostojen häviämisriski alussa pieni, mutta kasvaa koko ajan.

Kuva 4. Varmuuskopiointityypit

Useat yritykset hyödyntävät usein varmuuskopiontimetodien yhdistelmää, jolloin täysi versio ajoitetaan suoritettavaksi kerran viikossa tai kuukaudessa ja lisäävä tai erotteleva varmuuskopiointi suoritetaan kerran päivässä tai kahdessa. Täysi varmuuskopiointi vaatii lähes aina sen, että laite on kevyessä rasituksessa.

Usein myös erotteleva kopiointi on hyvä suorittaa työpäivän jälkeen, jos täyden varmuuskopioinnin suoritusväli on useita viikkoja.

Selkeästi kevyin ja tilaa säästävin ratkaisu on lisäävä varmuuskopiointi. Se voidaan ajaa niin usein kuin halutaan eikä se siten vie yhtään enempää muistia. Ohjelmasta riippuen voi varmuuskopioinnin laittaa hakemaan tiedostot heti, kun niitä on muokattu. Riippuen tiedostojen tärkeydestä, kannattaa harkita, haluaako varmuuskopiointilaitetta rasittaa jatkuvilla prosesseilla.

4 Varmuuskopiointiohjelmistot

4.1 Palvelinohjelmiston valinta

Opinnäytetyössä on tarkoitus varmuuskopioida sekä Bittigurun omia että sen asiakasyritysten verkkolaitteiden konfiguraatioita. Verkkolaitteisiin kuuluu palomuureja, kytkimiä ja reitittimiä. Varmuuskopiointia varten opinnäytetyön tilaaja on pystyttänyt Bittigurun Hyper-V -virtuaalipalvelinalustaan yhden Windows Server 2012 R2 –virtuaalipalvelimen. Alustavasti palvelimelle laitettiin minimaaliset määrät suorituskykyä ja muistia, joita tarpeen mukaan kasvatetaan tulevaisuudessa. Ohjelmistoja tutkiessa piti huomioida seuraavat seikat: ohjelmiston piti olla ilmainen, sen piti tukea joko FTP- tai TFTP-protokollaa, sen piti olla Windowsille ja sen piti tukea noin 1000:ta verkkolaitetta. Verkkolaitteissa ongelmana oli se, etteivät laitteet ole saman valmistajan tekemiä. Tällöin on vaikeaa löytää ohjelmistoa, joka tukee kaikkia mahdollisia laitteita, sillä jokaisella laitevalmistajan laitteella on yksilölliset komennot protokollille. Tilaaja halusi myös varmuuskopion automaattisen palauttamisen tarpeen vaatiessa, mikäli se on mahdollista.

Tilaaja määritteli varmuuskopioinnin aikataulutuksen sekä versioinnin. Varmuuskopiot tulisi ottaa jokaisesta asiakkaan ja heidän omista verkkolaitteista kerran päivässä. Käytännössä tämä tarkoittaa sitä, että palvelin on jatkuvasti

päällä. Todennäköisesti varmuuskopiointiohjelmisto ei tule viemään paljon tehoja palvelimelta, joten palvelimen jatkuva toiminta ei häiritse muiden virtuaalipalvelimien toimintoja. Tilaajan määrityksiin kuului myös, että varmuuskopioita tulisi kerrallaan olla 7 kappaletta laitetta kohtaan. Tällöin 7 päivää vanhemmat kopiot pitäisi poistaa automaattisesti.

Varmuuskopiointiohjelmaa valitessa piti miettiä myös sitä, kuinka kauan verkkolaitteet voivat maksimissaan olla pois päältä sekä mitkä tiedostot laitteista kopioidaan. Tämän lisäksi piti etsiä ominaisuutta, jonka avulla voitaisiin palauttaa konfiguraatio takaisin laitteeseen. Varmuuskopioitavaksi tiedostoksi valittiin alustavasti startup-konfiguraatio, koska se on konfiguraatio, jonka laite ottaa oletuksena käyttöön sen käynnistyessä uudelleen. Tämän takia laitteiden konfiguroijien pitää aina muistaa tallentaa tehdyt muutokset lopetettuaan konfiguroinnin.

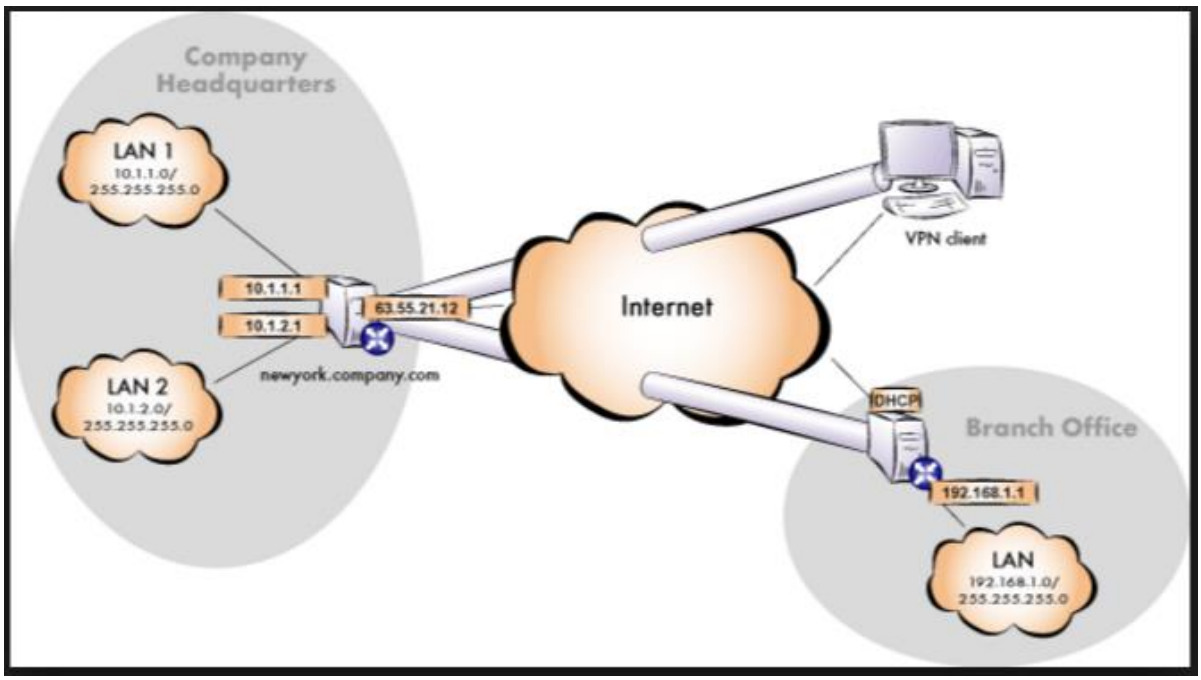
Varmuuskopiointeja suunniteltaessa kannattaa määritellä kaksi asiaa, palautumisaika sekä versio varmuuskopiosta, joka otetaan käyttöön. Suurempia varmuuskopiointeja otettaessa esimerkiksi palvelimista saattaa version valinta olla hankalampaa. Versiointi verkkolaitteiden konfiguraatiosta on helppoa, koska konfiguraatiot ovat niin pienikokoisia, eikä uusien konfiguraatioiden asettaminen pitäisi viedä aikaa. Verkkolaitteissa on kuitenkin se ongelma, että jos niiden konfiguraatiot jostain syystä menevät solmuun, tai itse laitteen rauta menee vikatilaan, on ongelmaa vaikeaa ratkaista etäyhteyden päässä olevalla varmuuskopiointipalvelimella. Tämä johtuu siitä, että etäyhteyden mahdollistavat konfiguraatiot saattavat hävitä tai laitevika estää etäyhteyden [18.]

4.2 Varmuuskopioinnin protokollat

Opinnäytetyön varmuuskopiointiohjelma haluttiin mahdollisimman tietoturvalliseksi ja vakaaksi, jotta ulkopuoliset henkilöt eivät pääsisi käsiksi varmuuskopioitaviin konfiguraatioihin. Varmuuskopioinnissa oli valittavana kaksi tiedostonsiirtoprotokollaa, jotka piti suojata jollakin kryptausprotokollalla. Työssä ei kuitenkaan voitu valita jompaakumpaa protokollaa tiedostonsiirtoa varten, sillä

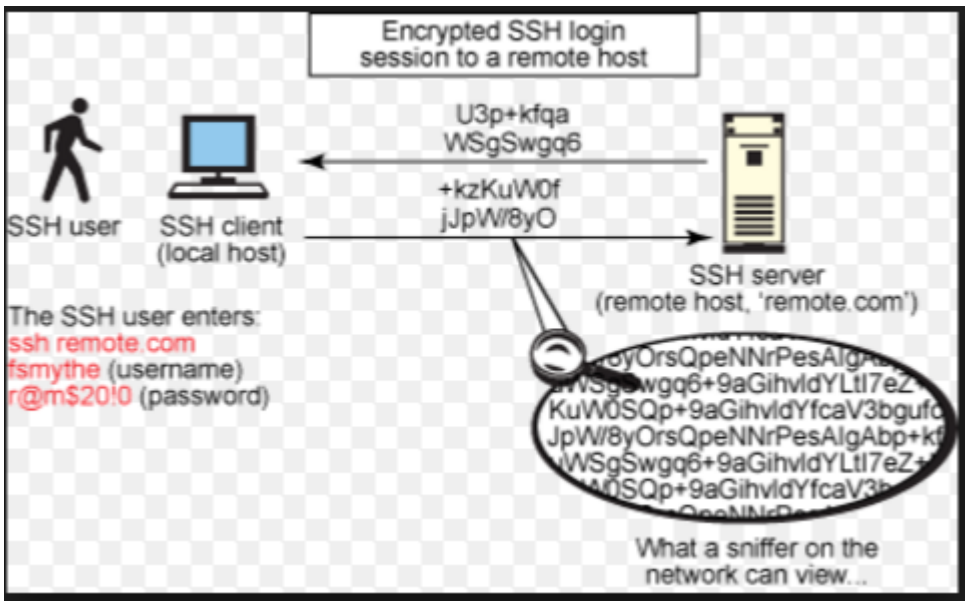
esimerkiksi testattavina olleet laitteet eivät tukeneet samoja menetelmiä. Zyxel-palomuuria varmuuskopioidessa pystyttiin käyttämään ainoastaan FTP-protokollaa, kun taas Cisco-kytkintä käsitellessä haluttiin käyttää yksinkertaisempaa TFTP:tä. Kuitenkin Ciscossa oli mahdollista käyttää FTP:tä, mutta opinnäytetyön tilaaja halusi ottaa TFTP:n käyttöön. Tilaajan mukaan TFTP on niin yleinen protokolla, että yritys haluaa käyttää jatkossa pääasiassa sitä varmuuskopiointien siirtämistä varten. Yleisesti FTP on turvallisempi ja vakaampi tiedostonsiirtomenetelmä, joka tarjoaa käyttäjien tunnistautumiset ja tietoliikenteen ohjaukset. TFTP kuitenkin vaatii vähemmän tehoja isäntälaitteelta ja sisältää vähemmän prosesseja tiedoston siirron aikana.

Opinnäytetyöryhmän piti pohtia, mitä tiedostojen kryptausprotokollaa haluttiin käyttää. Työn tilaajalle protokollalla ei sinänsä ollut väliä, sillä heillä oli valmiit työkalut niiden käyttöön ottamiseksi. Valittavana oli kaksi vaihtoehtoa – SSH ja VPN. Yrityksellä on käytössä VPN-yhteydet kaikkiin hallittaviin verkkoihin, joten sen käyttäminen olisi helpompaa. Toisaalta SSH-yhteys ei vaadi paljoa konfiguroimista, jotta se voidaan ottaa käyttöön. Jos kryptausprotokollana halutaan käyttää SSH:ta, on järkevintä ottaa käyttöön SFTP Zyxel-laitteita varten ja TFTP+SSH-yhdistelmää kaikkia muita laitteita varten. Tällöin halutaan ehdottomasti käyttää SSH:n turvallisempaa versiota, SSHv2:sta. Ja koska tarkoituksena on käyttää WinSCP:tä (FTP-yhteyksiin) ja esim. TFTPD32 (TFTP-yhteyksiin), pitäisi ainoastaan TFTPD32:en kanssa käyttää puttyn SSH:ta, koska WinSCP tukee valmiiksi SFTP:tä. Toisaalta, koska VPN-yhteydet ovat jo valmiiksi pystyssä, vältytään muun muassa laitteiden ylimääräisiltä konfiguroinneilta (SSHv2), ja nykyisiä batch-skriptejä ei tarvitsisi enää muokata. Täten suositeltavaa olisi, että varmuuskopioidessa käytetään VPN-yhteyttä, jotta varmuuskopiointi tapahtuisi mahdollisimman vakaasti ja turvallisesti (Kuva 5).



Kuva 5. VPN-yhteydet [20]

Vaikka VPN ja SSH ovat molemmat turvallisia ja vakaita kryptausprotokollia, niillä on kuitenkin huomattavia eroavaisuuksia. SSH-tunnelin voi tavan IT-osaaja asentaa kohtuullisen helposti, mutta sillä on useita puutteita ja rajoituksia, mikä tekee siitä heikommin hallittavan. VPN-yhteys varmistaa sen, että yksikään ulkopuolinen ei näe, mistä VPN-tunnelin yhteys oikeasti tulee ja minne se menee ja mitä paketteja se sisältää. VPN-versiosta riippuen lähes kaikki verkkoliikenne kulkee VPN:n kautta. VPN vaatii kuitenkin paljon määritysasetuksia ennen kuin se saadaan toimintaan ja sen käyttöönotto vaatii kohtuullisen paljon IT-osaamista ja ymmärrystä. SSH-tunneloinnissa pitää konfiguroida erikseen tunnelointi jokaista ohjelmistoa ja yhteyttä varten. Tunnelointi SSH:ssa on käytännössä yhtä turvallinen kuin VPN:ssä. Jos SSH-yhteyttä ei haluta tunneloida (esim. SOCKS-proxyllä), vaan otetaan suora kryptattu SSH-yhteys, ulkopuoliset henkilöt näkevät kryptatut paketit ja sen mihin paketit ovat menossa (Kuva 6). Toisaalta kryptaus on sen verran vahvaa, että paketteja ei todennäköisesti vaivauduta kaappaamaan ja avaamaan [19].



Kuva 6. SSH-paketit [21]

Jos varmuuskopiointijärjestelmässä halutaan hyödyntää SSH:ta, joudutaan tekemään useita portti/ip-avauksia yritysten palomuureihin. SSH käyttää oletuksena porttia 22 kohteenaan. Tällöin jokaiseen yrityksen palomuuriin laitettaisiin sääntö, jossa sallitaan portin 22 TCP liikenne sisäänpäin varmuuskopiointipalvelimen julkisesta IP-osoitteesta. Jos otetaan käyttöön VPN, pitäisi VPN-asetuksista ohjata/reitittää varmuuskopiointipalvelimen liikenne. Tämän on yksinkertainen prosessi, jossa palvelin lisätään vain käyttämään VPN-yhteyttä. Riippuen siitä, onko varmuuskopioitavien verkkolaitteiden ja varmuuskopiointipalvelimen välillä palomuuria, pitää varmuuskopiointiskripteihin lisätä oikeat IP-osoitteet. Tällöin pitää ottaa huomioon, että jos eri yrityksillä on samoja sisäverkon ip-osoitteita, tulee varmuuskopiointipalvelimelle laiteristiriitoja, jos liikennettä ei ole reititietty oikein.

4.3 CrashPlan

Ohjelmalla on seuraavanlaiset käyttöjärjestelmävaatimukset (Kuva 7):

OS	Hardware	Software
Windows[1]	• 1 GHz CPU • 1 GB Memory • 450 MB free drive space	• Windows operating systems: ◦ Windows XP [2] ◦ Windows Vista Service Pack 2 ◦ Windows 7 ◦ Windows 8, 8.1 (in desktop mode) ◦ Windows 10 ◦ Server 2008/2012 (excludes Windows Server Essentials, Windows Small Business Server, and Windows Home Server) • Java JRE 1.7.0_45 (packaged with the CrashPlan app)

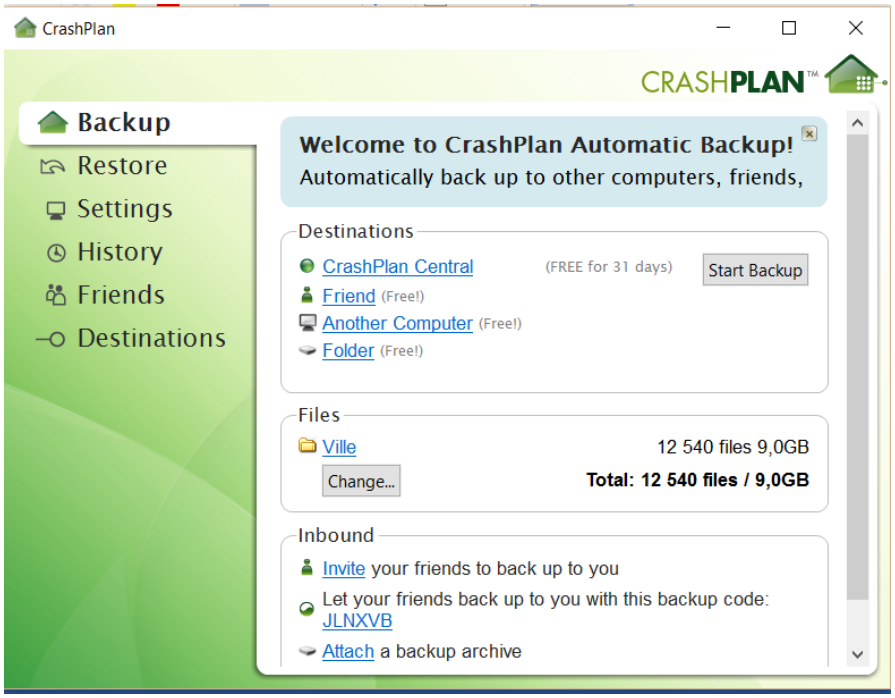
Kuva 7. CrashPlan järjestelmävaatimukset

CrashPlan for Home on ilmainen varmuuskopiointiohjelmisto. Ohjelmistosta on kaksi muutakin versiota, jotka eroavat ilmaisversiosta tallennusmahdollisuuksiIlaan. Niissä voidaan hyödyntää pilvitallennusmahdollisuutta, mutta käytännössä käyttäjä voi tallentaa varmuuskopionsa ilmaiseksi mihin tahansa. Maksullisissa versioissa maksetaan siis vain pilvitallennustilasta. Maksullisista versioista on saatavilla 30 päivän ilmaiset kokeilujaksot, jonka aikana voidaan testata ohjelmaa sen täysillä ominaisuuksilla. Tällä kertaa testattiin kuitenkin Home-versiota, joka täyttää opinnäytetyön tilaajan vaatimuksen kustannuksiltaan.

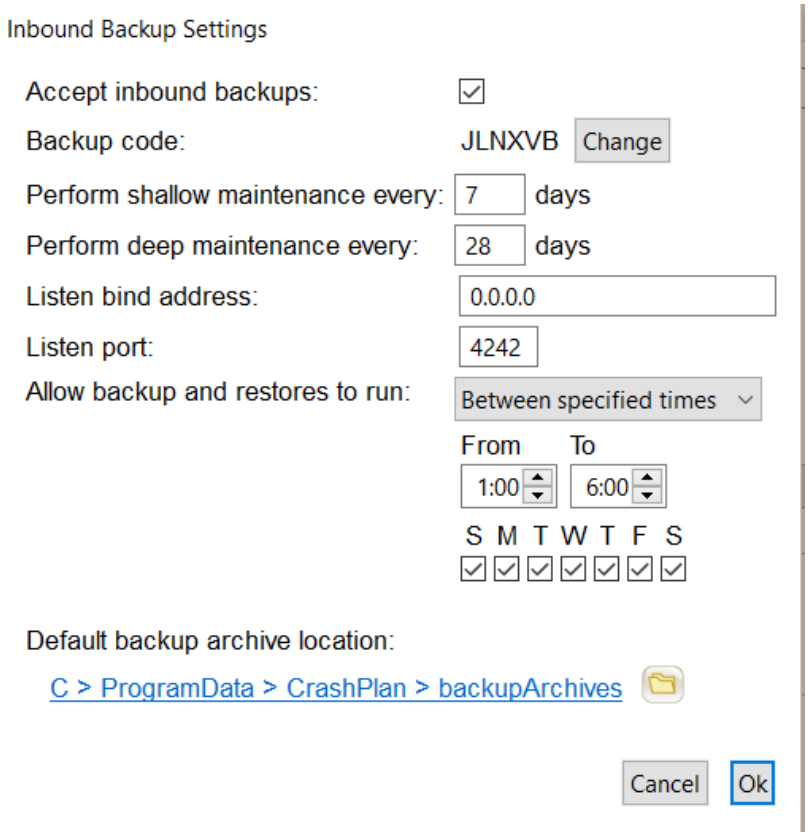
Asennus on yksinkertainen: käyttäjän pitää vain ladata ohjelmisto, hyväksyä käyttöehdot ja valita asennussijainti. Sen jälkeen ohjelma pakottaa käyttäjän luomaan käyttäjätilin, jotta ohjelmaa voi käyttää. Käyttäjätiliä luodessa pitää antaa oma nimi, sähköpostiosoite ja salasana käyttäjätilille. Kuitenkaan sähköpostiosoitteeseen ei tullut vahvistusviestejä, joissa pitäisi vahvistaa käyttäjätili. Ohjelmiston saa todella nopeasti käyttöönsä. Valitaan varmuuskopioitavat kohteet ja tallennussijainnit sekä varmuuskopionnin alkamisajankohdat, ja jätetään ohjelmisto käyntiin käyttöjärjestelmän taustalle.

Käyttäjätilin luomisen jälkeen avautuu ohjelman päävalikko (Kuva 8). Ohjelmassa ei loppuen lopuksi ole muutettavaa, mutta ensimmäisenä kannattaa kui-

tenkin mennä ohjelman asetuksiin. Asetuksista pystyy määrittämään muun muassa varmuuskopiointiaikavälin muista laitteista (kuin paikallisesta koneesta) ja niiden varmuuskopioiden tallennussijainnin (Kuva 9).

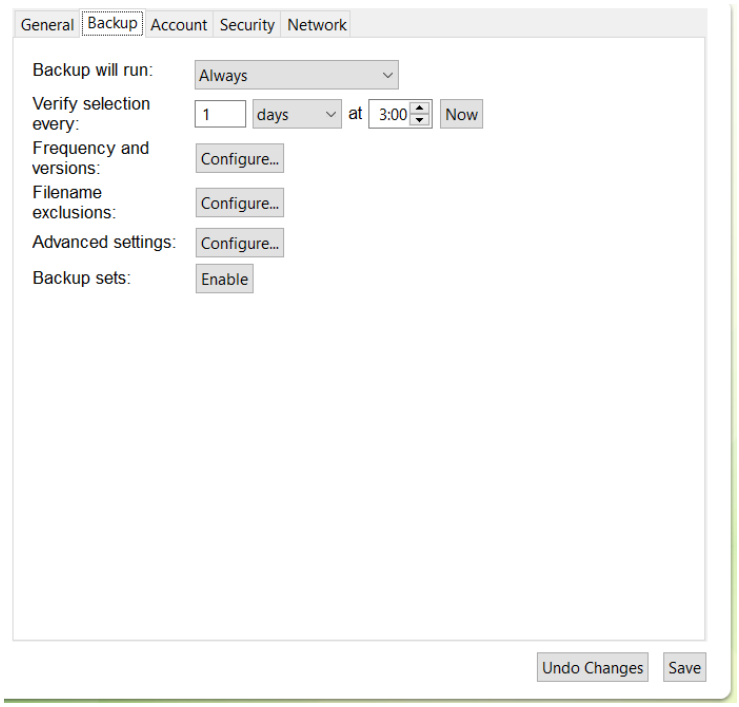


Kuva 8. CrashPlan päävalikko

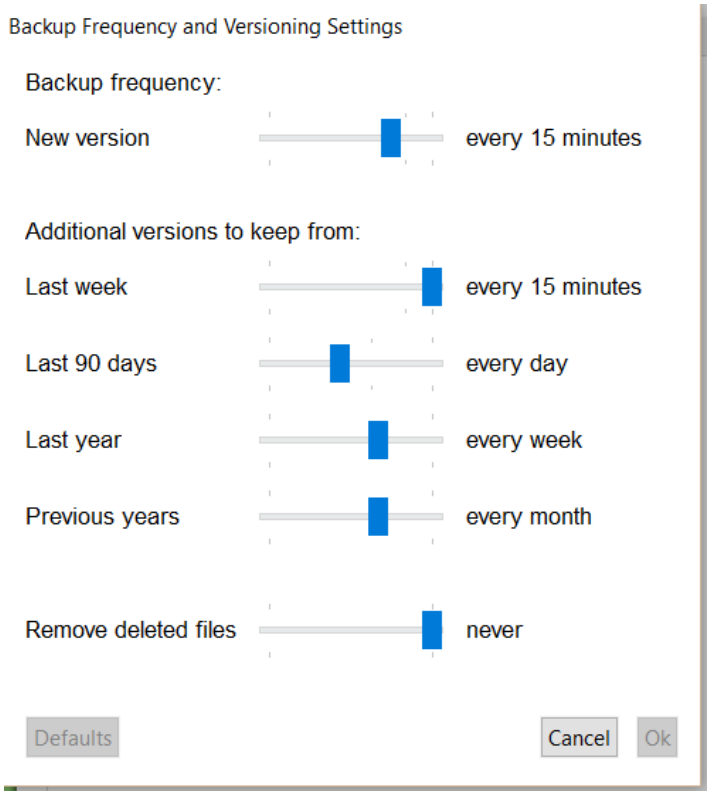


Kuva 9. CrashPlanin asetukset

Ohjelma keskeyttää varmuuskopioinnin turvallisesti, jos tietokone yritetään sammuttaa ja jatkaa varmuuskopiointia automaattisesti koneen käynnistämisen jälkeen. Ohjelmisto osaa myös varoittaa, jos yhteys varmuuskopioitavaan kohteeseen ei toimi tai siinä on ongelmia. CrashPlan antaa valita varmuuskopioinnille tarkempia asetuksia omassa välilehdessä, jossa voi määrittää, kuinka monta eri versiota ohjelma säilyttää kerrallaan (versions) ja kuinka usein uusi versio tiedostosta haetaan (frequency) (Kuva 10, Kuva 11).

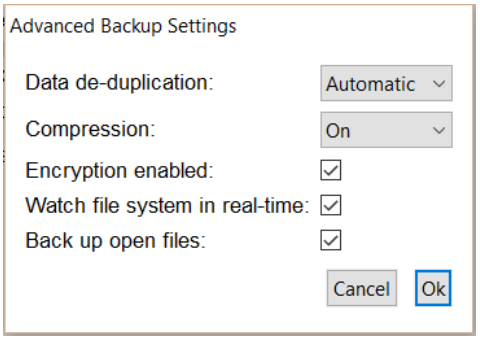


Kuva 10. CrashPlanin varmuuskopioinnin asetukset



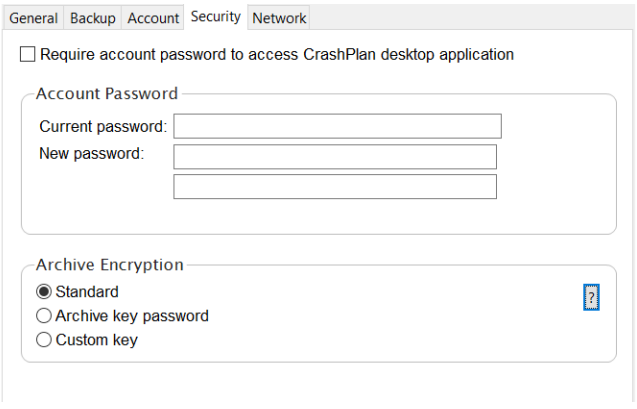
Kuva 11. CrashPlanin varmuuskopioinnin ajastus

Asetuksissa määritetään myös duplikointi-asetukset eli halutaanko varmuuskopioida tiedostoja, jotka eivät ole muuttuneet viime varmuuskopioinnista (Kuva 12). Asetuksissa määritetään lisäksi datan pakkaamisasetukset. Vaihtoehtoina ovat On, Off sekä Automatic. Koska työssämme on tarkoitus kopioida pelkkiä tekstiä sisältäviä tiedostoja, ei niitä pysty pakkaamaan pienempään tilaan. Tällöin pakkaaminen on käytännössä hyödytöntä.



Kuva 12. Deduplikointi ja kryptaus

Asetuksissa käyttäjä voi valita, millä tavalla CrashPlan salaa tiedostot ennen varmuuskopiointia valittuun sijaintiin (Kuva 13). Koska tietoturva oli tärkeää varmuuskopioidessa asiakkaiden laitteistoja, kiinnitettiin tähän ominaisuuteen enemmän huomiota.



Kuva 13. CrashPlanin tiedostonsalaus

Valittavana oli kolme vaihtoehtoa. Ensimmäisenä on ’Standard’, joka käyttää ns. ”Salted and Hashed” –metodia, jossa suojataan käyttäjätilin salasana kertakäyttöisellä salausavaimella. Metodi tarkoittaa käytännössä sitä, että salasana on

kryptattu kahteen kertaan – ensin salausavaimella, johon sen jälkeen lisätään satunnainen lukujono [22.]

Toisena vaihtoehtona on ’Archive key password’ -metodi, jossa annetaan uusi salasana, jolla salataan tieto. Tämä salausavain kryptataan ”Salted and Hashed” -metodilla. Viimeinen vaihtoehto on ’Custom key’, jossa data salataan käyttäjän määrittämällä salasanalla, jota ei välitetä ohjelman hallintapalvelimelle. Tämä avain on siis vain käyttäjällä eikä CrashPlan-ohjelmisto tallenna sitä omiin varastoihinsa [23.]

Huomioitavaa kuitenkin on, että ainoastaan kolmas vaihtoehto on turvattu niin, ettei Code42, joka on ohjelmiston kehittäjä, pääse käsiksi dataan. Ohjelmiston tukisivustoilla mainitaan, että sekä ’Standard’- että ’Archive key’-salasanat tallentuvat Code 42:sen autentikointipalvelimelle. Jos CrashPlan-ohjelmisto otetetaan opinnäytetyössä käyttöön, tulee ohjelmassa käyttää Custom Key -vaihtoehtoa, jotta vältytään tietoturvariskeiltä [23.]

Testattavissa oleva ilmaisversio käyttää Blowfish-kryptausta, joka on avoimen lähdekoodin metodi. Versio käyttää symmetristä 128-bittistä salausavainta. Blowfish-kryptaus korvaa ohjelmassa DES sekä IDEA metodit. Salausmetodi on metodin kehittäjän mukaan paljon nopeampi vaihtoehto kuin DES sekä IDEA. Kuitenkaan Blowfish-metodi ei ole kovinkaan tunnettu eikä sen toiminnasta ole opinnäytetyön tekijöillä aiempaa tietoa [24.]

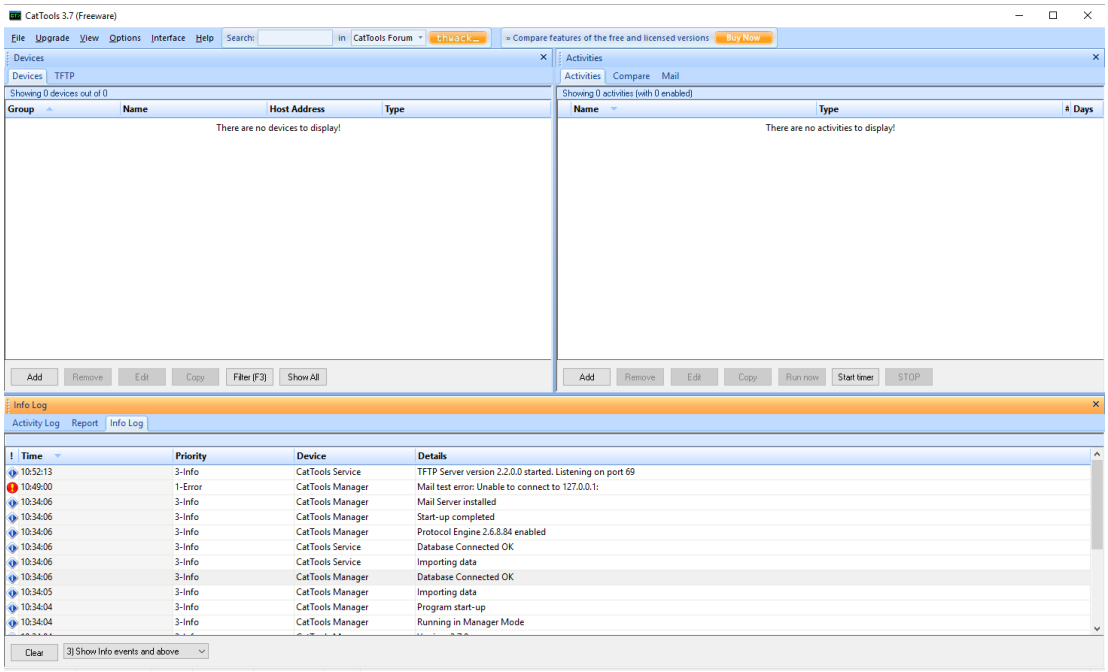
Pikaisen tarkastelun jälkeen huomattiin, että ohjelma soveltuu ainoastaan etätietokoneiden varmuuskopiointiin eikä verkkolaitteisiin. Huolimatta siitä, että ohjelma tukee useita käyttöjärjestelmiä ja laitteita, järjestelmä vaatii sen, että CrashPlan-ohjelmisto asennetaan varmuuskopioitavaan laitteeseen, joka ei ole verkkolaitteiden kohdalla mahdollista. Ohjelmisto sopii kuitenkin jonkin yrityksen lähiverkossa olevien koneiden ja tiedostojen varmuuskopiointiin ja se pystyy tallentamaan varmuuskopiot useaan eri kohteeseen.

4.4 CatTools

CatTools-ohjelmisto on SolarWindsin kehittämä verkkolaitteiden ylläpitoon ja tarkasteluun tarkoitettu työkalu. Ohjelmasta ladattiin ilmaisversio (3.7.0), jota SolarWinds ei enää tue. Nykyisellään versio maksaa noin 640 $. Tuen loppuminen ei kuitenkaan tarkoita sitä, että ohjelmisto ei sovellu opinnäytetyön tilaajan määrittämiin raameihin. Ohjelmasta löytyy pdf-muotoinen ohjekirja, jota voi soveltaa ohjelman eri versioihin aivan mainiosti. CatToolsia ei ole kuitenkaan mahdollista ladata sen valmistajan omilta sivuilta, vaan pitää turvautua toiseen verkkosivustoon.

CatToolsia asennettaessa ohjelmistosta voidaan valita ns. palveluversio tai ohjelmistoversio. Palveluversiossa tietyn käyttäjän ei tarvitse olla kirjautuneena Windowsiin, vaan ohjelma pyörii koko ajan taustalla. Versio asentaa graafisen CatTools hallintaohjelmiston, jolla hallitaan palvelun laitteistoja, toimintoja ja aikataulutusta. Palveluversio on suunnattu yritystoimintaan ja toimimaan yhtäjaksoisesti kellon ympäri. Ohjelmistoversio on optimaalinen koneelle tai palvelimelle, joka keskittyy CatToolsin käyttöön. Application- eli ohjelmistoversiota on suositeltu käyttäjille, jotka käyttävät ohjelmistoa epäsäännöllisesti tai niille, joilla ohjelmisto on asennettu omalle koneelle.

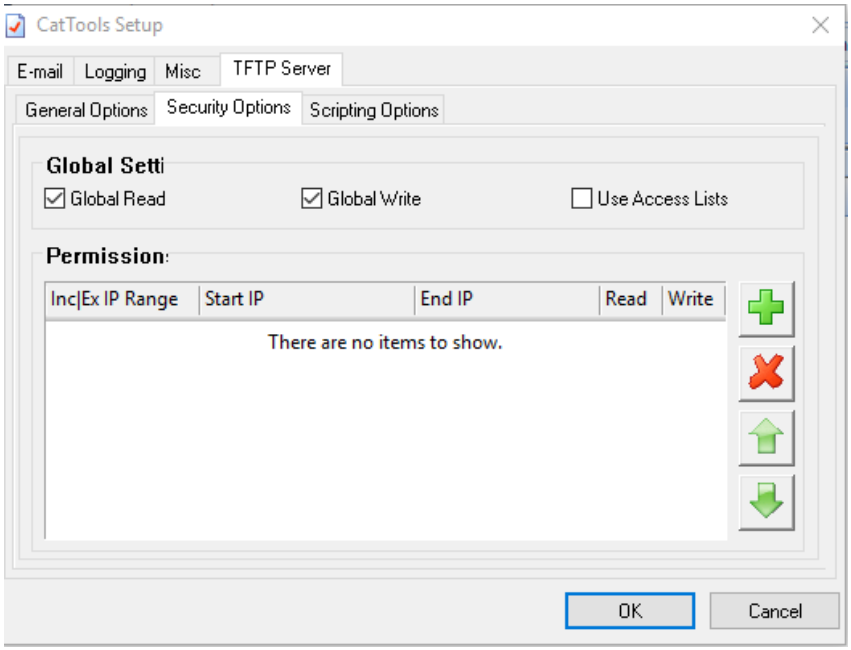
Ohjelman asennuksessa määritetään myös halutut pikakuvakkeet, quick-launch painikkeet sekä käynnistysvalikon kuvakkeet. Kun ohjelma käynnistetään ensimmäistä kertaa asennuksen jälkeen, avautuu ’CatTools Setup Wizard’, jossa voidaan lisätä laitteita, ajastettuja aktiviteettejä sekä varoituksia ja huomautuksia. Laitteita lisätessä käyttäjä voi valita yli 60 laitevalmistajan laitteistoista, mukaanlukien HP, Cisco, Zyxel ja Dlink. Ohjelmistossa on myös mahdollista lisätä laitteita ja valmistajia, joita ei ole valmiiksi määritettyinä ohjelmistossa. Ensimmäisten konfigurointi wizardien suorittamisen jälkeen aukeaa ohjelman graafinen käyttöliittymä. Käyttöliittymä on yksinkertainen, ja oletuksena siinä näkyy laitteet, aktiviteetit ja tapahtumaloki (Kuva 14). Käyttäjä voi halutessaan muokata näkymää omiin tarkoituksiinsa sopivaksi. Ilmaisversiossa käyttöliittymän muokkaaminen on rajallista.



Kuva 14. CatToolsin käyttöliittymä

Ohjelman laitteiden lisäysvalikko on monipuolinen. Laitteelle voidaan määrittää valmistaja, laitetyyppi, ryhmä, nimi, ip-osoite, malli ja yhteydenottotapa (Telnet tai SSH1,2). Laitetta voidaan myös pingata sen lisäämisen yhteydessä, jotta saataisiin varmuus siitä, onko laite tavoitettavissa. Ohjelmistossa ei voi valita SNMP-protokollaa laitteiden etsimiseen, mikä olisi yksi kätevämmistä vaihtoehdoista SSH:n rinnalle.

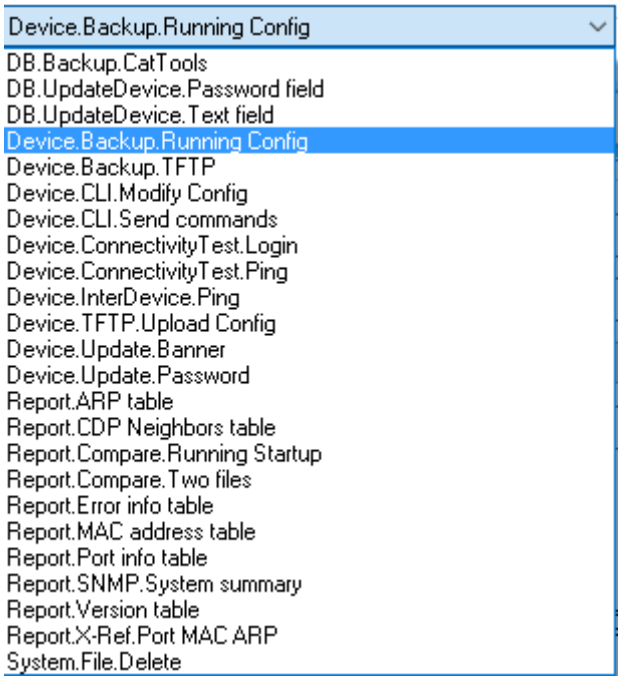
CatToolsissa on mahdollista lisätä huomautuksia sähköpostiin. Käyttäjän pitää vain määrittää sähköpostipalvelimen osoite, jota kautta se voi lähettää viestejä. Ohjelmaan voi määrittää ensisijaisen sekä toissijaisen palvelimen, jotta viestit varmasti lähtevät eteenpäin. Myös lokitiedostoja voidaan lähettää Syslog palvelimelle, jos sellainen on käytettävissä. Ohjelma asentaa myös TFTP-palvelimen, jonka yhteyteen voidaan sallia ja estää laitteita ip-osoitteiden avulla (Kuva 15).



Kuva 15. CatToolsin TFTP-asetukset

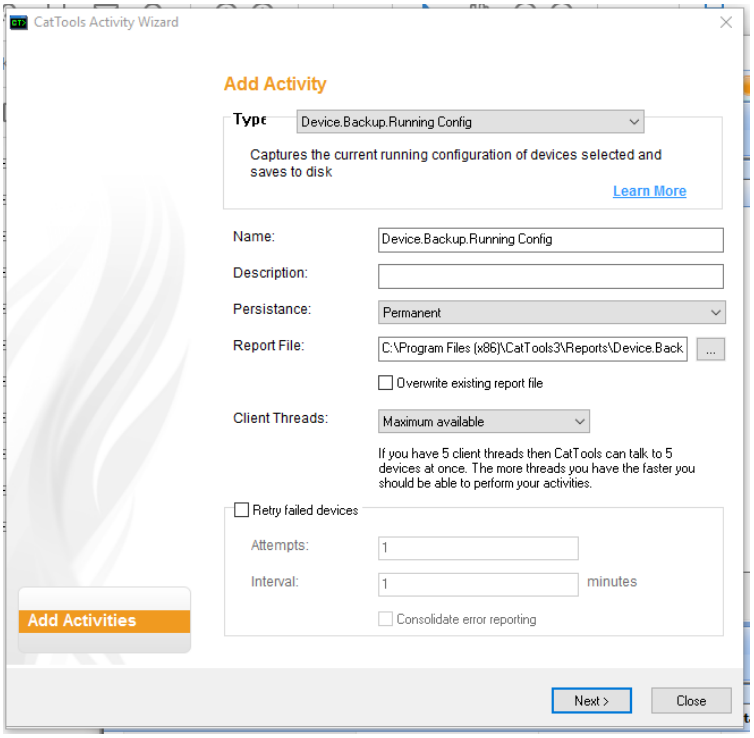
Jos ohjelmaan halutaan lisätä ajastettuja toimintoja, käytetään CatTools Activity Wizardia. Sekä Activity- että Device-Wizardit löytyvät kätevästi CatTools GUI:n Options-valikosta. Ohjelmassa voidaan käyttää myös aktiviteetit ja laitteet-paneeleiden Add-painikkeita laitteiden lisäämiseksi. Aluksi määritetään aktiviteetin tyyppi, joita on useita (Kuva 16).

Tärkeimpänä opinnäytetyössä on mahdollisuus varmuuskopioida senhetkinen konfiguraatio eli ’Running Config’, joka löytyy aktiviteettien listasta. Muita olennaisia toimintoja listassa on laitteen asetusten muokkaaminen lähettämällä automaattisesti tiettyjä komentoja (CLI Send Commands), konfiguraatiotiedoston lähettäminen takaisin verkkolaitteelle ja laitteen salasanojen vaihtaminen tietyin väliajoin (Update Password).



Kuva 16. CatToolsin aktiviteetit

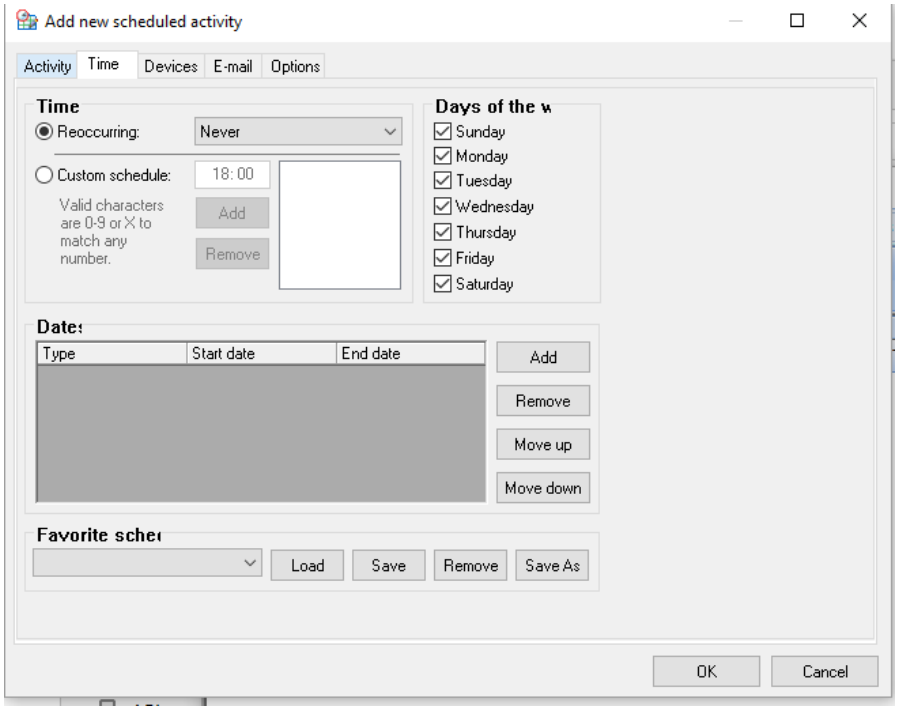
Aktiviteetille annetaan myös nimi, kuvaus, persistance eli aktiviteetin toistuvuus, aktiviteetin raportin tallennussijainti, aktiivisuussäikeet sekä uudelleenyritykset, jos aktiviteetti epäonnistui (Kuva 17). Aktiivisuussäikeet tarkoittavat sitä, kuinka moneen laitteeseen ollaan samanaikaisesti yhteydessä. Eli mitä parempi tietokone, sitä useampaan laitteeseen voidaan olla yhteydessä kerrallaan. Aktiviteetin toistuvuuden muokkaaminen on kätevää siinä tapauksessa, jos halutaan hakea esimerkiksi testailuja varten laitteiden konfiguraatioita.



Kuva 17. CatToolsin activity wizard

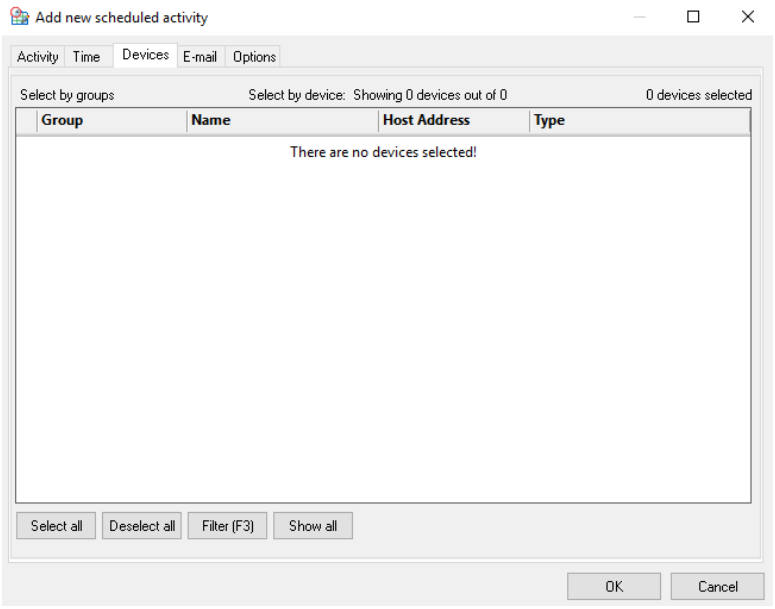
CatToolsissa konfiguraation varmuuskopiointi tapahtuu seuraavanlaisesti: ohjelma lataa ensin laitteen konfiguraation ja vertaa sitä sen jälkeen CatToolsissa aiemmin olevaan tiedostoon. Jos ohjelmassa ei ole aiempaa versiota varmuuskopiosta, vertailuja ei tapahdu. Lisäksi, jos tiedostoista löytyy eroja, ohjelma merkkaa uuden ladatun tiedoston ”Running Configiksi”. Tämän jälkeen ohjelma luo raportin aktiviteetista, oli tiedostoissa eroja tai ei. Jos tiedosto oli eroavainen, lähetetään raportista sähköpostihuomautus [25.]

Seuraavaksi määritetään aktiviteetin ajankohta. Aktiviteetti voidaan asettaa alkavaksi mihin kellonaikaan tahansa ja tiettyinä viikonpäivinä. Ajankohdassa määritetään myös, kuinka usein aktiviteetti tapahtuu. Ikkunassa voidaan määrittää ajankohta, jos halutaan tarkempi kellonaika tapahtumalle (Kuva 18).



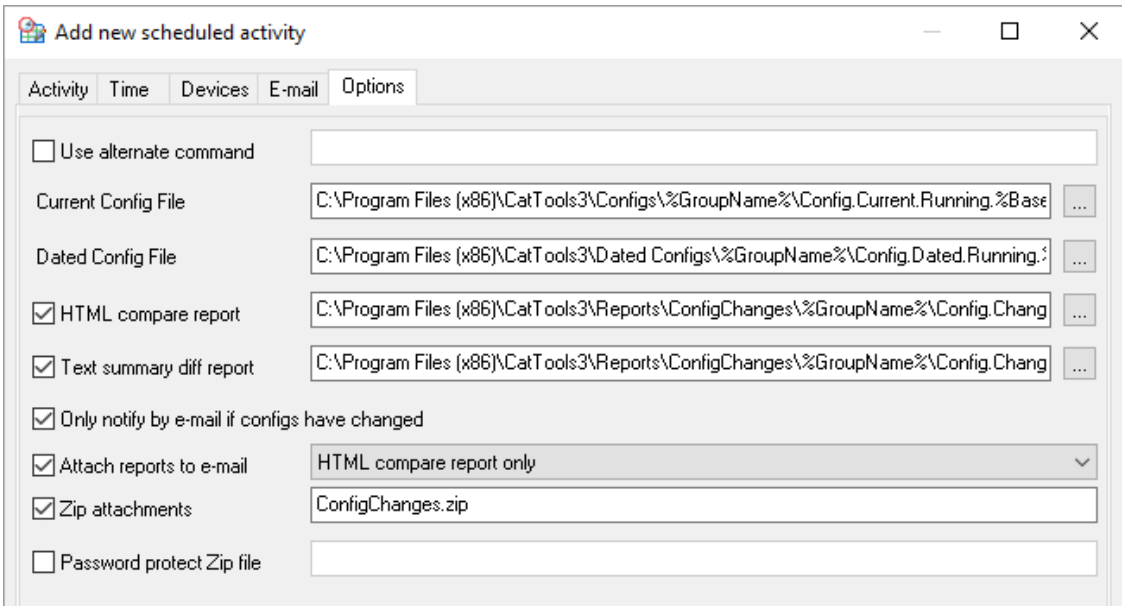
Kuva 18. CatToolsin aikataulutus

Aktiviteetissä valitaan myös kaikki laitteet, joita aktiviteetti koskee (Kuva 19). Valinnassa voidaan hyödyntää laitteiden ryhmittämistä, jota opinnäytetyön tilaaja tulee tarvitsemaan, sillä asiakkaita ja laitteita on kohtuullisen paljon. Laitteita valittaessa voidaan hyödyntää filter-ominaisuutta, joka suodattaa laitteet niiden nimen, ryhmän, ip-osoitteen, sijainnin tai mallin mukaan.



Kuva 19. CatToolsin aktiviteettien aikataulutus

Aktiviteetistä voidaan lähettää sekä häiriö- että statistiikkatietoja sähköpostiin. Oletussähköpostiosoitetta voidaan aktiviteetin kohdalla muuttaa, mutta kutakin sähköpostityyppiä (häiriö, statistiikka) ei voida lähettää useampaan kuin yhteen osoitteeseen. Viimeisenä asetuksena aktiviteettien tallennussijaintia voidaan muuttaa ja valita, mitä liitetiedostoja sähköposteihin laitetaan (Kuva 20) [25.]



Kuva 20. CatToolsin aktiviteettien tallennussijainnit

4.5 WinAgents Hyperconf

Ohjelman järjestelmävaatimukset ovat seuraavanlaiset:

CPU: Intel P4 (or greater) • Memory: 512MB RAM or more • Disk space: not less than 30 MB to install the program, recommended 100 MB • Platform: Windows 2000/XP/2003/Vista/2008/7 [26]

Ohjelman asennuspaketti asentaa seuraavat komponentit:

WinAgents HyperConf Server , GUI manager, TFTP Server, SYSLOG service [26]

Järjestelmä ei ole ilmainen ja sitä testattiin 30-päivän kokeiluversion avulla. Lisensointi on seuraavanlainen (Kuva 21) [26].

Ohjelma	+	10	laitetta	–	225€
Ohjelma	+	25	laitetta	–	395€
Ohjelma	+	50	laitetta	–	625€
Ohjelma	+	100	laitetta	–	1035€
Ohjelma	+	200	laitetta	–	1725€
Ohjelma	+	300	laitetta	–	2195€
Ohjelma	+	500	laitetta	–	2595€
Ohjelma + rajaton laitemäärä – 3175€					

Kuva 21. Winagentsin lisensointi

Lisensointiin sisältyy yhden vuoden täysi tuki ja laitteidenpäivitysmahdollisuudet. Vuoden jälkeen käyttäjän ei tarvitse hankkia uutta ohjelmisto- ja laitelisenssiä, mutta päivitys ja ylläpito pitää ostaa uudelleen, jos niin halutaan. Päivitys ja ylläpitolisenssit ovat laitemääräkohtaisia ja ne ovat hinnoiteltu seuraavasti (Kuva 22) [26.]

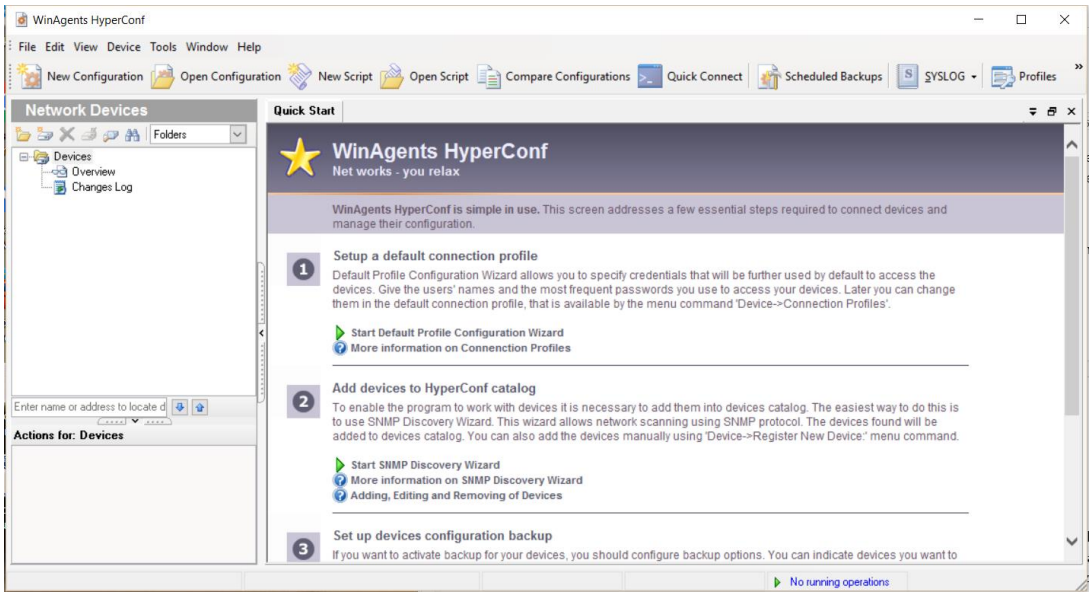
päivityslisenssi	10	(lisä)laitteelle	–	115€/vuosi
päivityslisenssi	25	laitteelle	–	195€/vuosi
päivityslisenssi	50	laitteelle	–	310€/vuosi
päivityslisenssi	100	laitteelle	–	515€/vuosi
päivityslisenssi	200	laitteelle	–	865€/vuosi
päivityslisenssi	300	laitteelle	–	1095€/vuosi
päivityslisenssi	500	laitteelle	–	1295€/vuosi
päivityslisenssi rajattomalle laitemäärälle – 1575€/vuosi				
Ylläpitolisenssi	10	laitteelle	–	65€/vuosi
Ylläpitolisenssi	25	laitteelle	–	115€/vuosi
Ylläpitolisenssi	50	laitteelle	–	185€/vuosi
Ylläpitolisenssi	100	laitteelle	–	310€/vuosi
Ylläpitolisenssi	200	laitteelle	–	515€/vuosi
Ylläpitolisenssi	300	laitteelle	–	665€/vuosi
Ylläpitolisenssi	500	laitteelle	–	785€/vuosi
Ylläpitolisenssi	rajattomalle	laitemäärälle	–	955€/vuosi

Kuva 22. Winagentsin päivitys- ja ylläpitolisenssit

Päivityslisenssit tarkoittavat, että nykyisen lisenssin rinnalle lisätään toinen lisenssi, joka kasvattaa laitemäärää HyperConf-ohjelmistossa. Ylläpitolisenssi antaa mahdollisuuden ladata ja päivittää ohjelmiston versioita HyperConfin verkkosivuilta. Lisenssit ovat (palvelin)laitekohtaisia, ja laitelisenssin oston jälkeen käyttäjä voi ostaa halvempaan hintaan uusia lisenssejä päivittääkseen oman versionsa tukemaan suurempia määriä laitteita [26.]

Ohjelmisto tukee tällä hetkellä kohtalaisen pientä määrää laitevalmistajia (9 eri valmistajan tuotetta). Yritys lupaa laittavansa tuen muille laitteille ilmaiseksi, kunhan heille ilmoitetaan, mitkä valmistajat ja mallit ovat kyseessä. Nykyiset tuetut valmistajat verkkosivuston (Winagentsin sivusto) mukaan ovat: 3Com, Cisco, Nortel, Netgear, Juniper, HP, Foundry, Fortigate, Dell ja D-Link. Kuitenkin laitteita lisätessä itse ohjelmassa, on valittavana useita muitakin valmistajia, joten verkkosivujen tieto saattaa olla vanhentunutta.

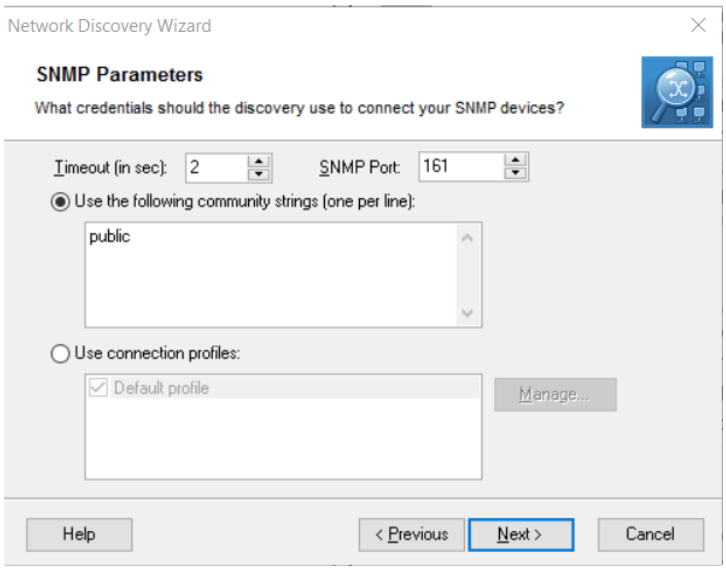
HyperConf Managerin avulla hallitaan verkkolaitteita ja niiden konfiguraatioita (Kuva 23). Sen kautta voidaan hallita kaikkia Hyperconfin toimintoja, kuten varmuuskopioita ja niiden palauttamista. Konfiguraatioita voidaan myös muokata ohjelmiston avulla sekä versioida niitä. Laitteita ohjelmaan lisätään joko Discovery Wizardin avulla tai manuaalisesti syöttämällä ip-osoite.



Kuva 23. Winagentsin käyttöliittymä

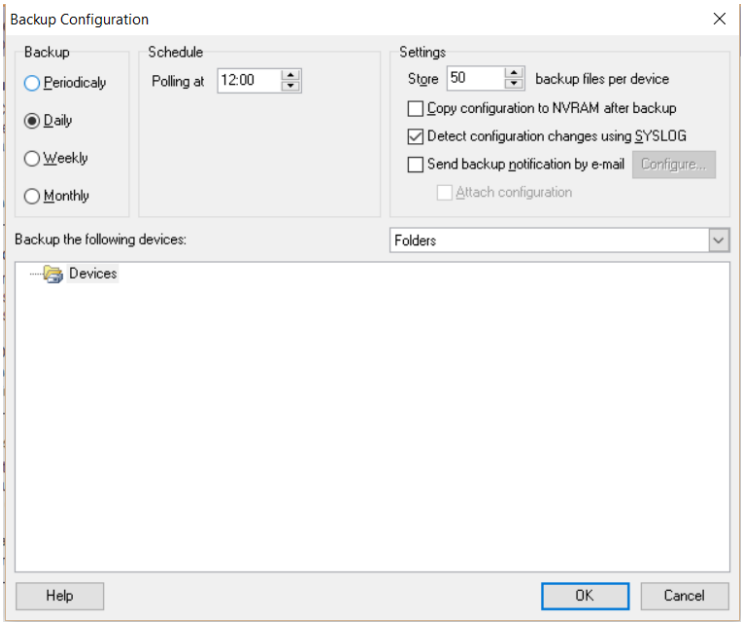
Kun ohjelma käynnistetään ensimmäistä kertaa, voidaan käynnistää suoraan konfiguraatio wizardit, jotka helpottavat ohjelman käyttöönottoa. Ensimmäisenä ohjelma suosittelee käynnistämään ”Default Profile Configuration Wizardin”. Wizardissa kysytään ensimmäisen laitteen lisäämisestä. Laitteesta valitaan valmistaja ja malli. Seuraavaksi pitää syöttää Telnet/SSH-yhteyden käyttäjätunnukset, sekä privileged password. Tämän jälkeen valitaan SNMP-asetukset laitteeseen yhdistämiselle, kuten versio, read community -salasana sekä write community -salasana. Jos käyttäjä haluaa, voidaan lisätä myös HTTP-yhteyden tunnukset. Sen jälkeen ohjelma varmistaa palomuuri- ja NAT-asetukset. Tällöin valittavana on dataliikenteen kulku TFTP-portista 69 sekä ohjelman ulkoinen osoite. Tämän jälkeen alkukonfiguraatio on valmis ja ohjelman käyttö voi alkaa. Jälkeenpäin asetuksia voidaan muuttaa erillisessä asetusvalikossa, jossa voidaan lisätä useampia käyttäjäprofiileita.

Laitteita voi lisäillä HyperConfiin ’SNMP discovery wizardin’ avulla tai manuaalisesti oman valikon kautta. Wizardin alussa valitaan, mitä verkosta halutaan etsiä. Valittavana on kaikki verkkolaitteet sekä reitittimet ja kytkimet. Sitten kerrotaan, mistä verkoista laitteita etsitään tai sen perusteella kuinka monen verkkoyhteyden (hops) päästä etsitään. Tämän jälkeen valitaan SNMP-asetukset haulle. Käyttäjä valitsee joko connection profilet tunnistautumiseen tai kirjoittaa itse community stringit (Kuva 24). Erittäin hyödyllinen perusominaisuus ohjelmassa on, että laitteet voidaan ryhmitellä, mikä helpottaa niiden hallittavuutta.



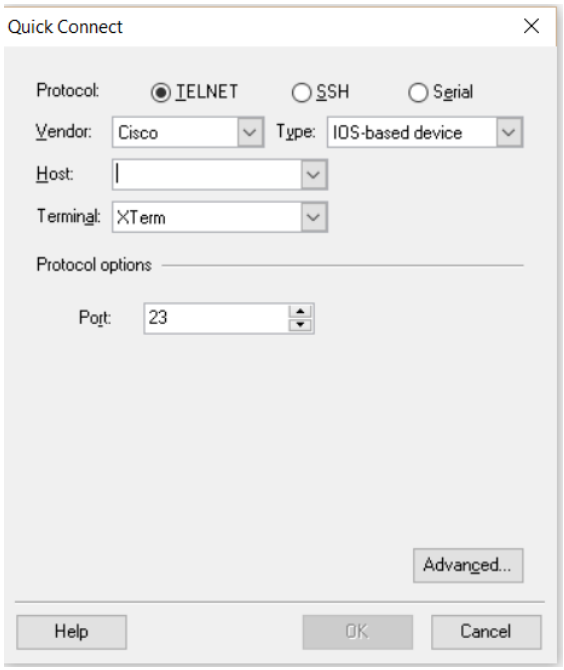
Kuva 24. Winagentsin SNMP-asetukset

Toinen erittäin olennainen asia ohjelmassa on aikataulutettu varmuuskopiointi (Kuva 25). Varmuuskopiointivälin voi asettaa suoritettavaksi minimissään 15 minuuttiin ja maksimissaan 1440 minuuttiin. Käyttäjä voi myös valita minä viikonpäivinä tai minä kuukauden päivinä kopiointi suoritetaan. Varmuuskopioinnista määritellään samalla kuinka monta varmuuskopiota yhdestä laitteesta säilytetään, ja lähetetäänkö varmuuskopioista sähköpostihuomautuksia. Ohjelman voi asettaa myös tunnistamaan muutoksia varmuuskopioissa.



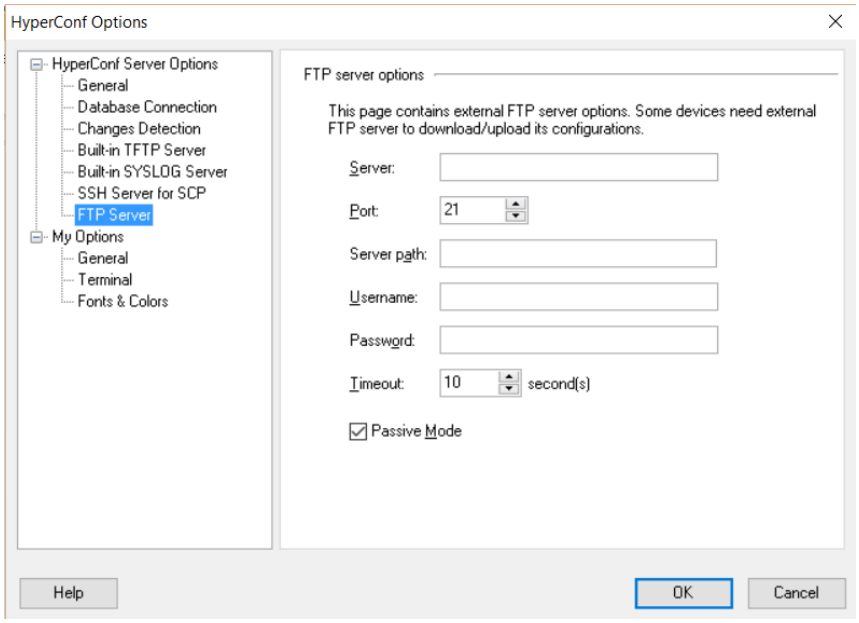
Kuva 25. Winagentsin aikataulutettu varmuuskopiointi

Ohjelman avulla voidaan myös kirjoittaa omia konfiguraatioita ja lähettää niitä laitteille. Verkkolaitteet pitää konfiguroida kuitenkin oikein ennenkuin ohjelmisto toimii kunnolla. Käyttäjä voi halutessaan lisätä verkkolaitteelle syslog-ominaisuuden ja asettaa viestit lähetettäväksi HyperConf-ohjelmalle, joka osaa toimia syslog-palvelimena. Tällöin varmuuskopiointiohjelma säilyttää laitteen sisäiset ilmoitukset muutoksista ja tapahtumista, joita voidaan sitten tarkastella. Ohjelmassa on lisäksi integroitu terminaaliohjelma, jolla voidaan ottaa verkkolaitteisiin sarjaporttiyhteys tai etäyhteys (telnet, ssh) (Kuva 26).



Kuva 26. Winagentsin terminaaliohjelma

Varmuuskopioita voidaan hakea laitteilta kahdella tavalla, mutta molemmat tavat käyttävät TFTP:tä. Ohjelman kehittäjien mukaan siihen ei ole integroitu FTP:tä, koska suurin osa verkkolaitteista tukee TFTP:tä. TFTP:ssä on huonoa se, että konfiguraatiot siirtyvät selvänä tekstinä paikasta toiseen. Kuitenkin ohjelmaan on mahdollista linkittää ulkoinen FTP-palvelin (Kuva 27). Ensimmäinen varmuuskopiointitapa hyödyntää telnetiä ja toinen tapa SSH:ta (versio 1 tai 2). Jos laite on pelkästään web-hallinnan avulla toimiva, voidaan asettaa myös http-yhteys. Jotta HyperConf tunnistaisi verkkolaitteet, se käyttää SNMP:n versioita 1 2c ja 3.



Kuva 27. Hyperconfin FTP-asetukset

Kaiken kaikkiaan ohjelma olisi optimaalinen ratkaisu opinnäytetyön ohjelmistoksi, sillä se kattaa lähestulkoon kaikki tilaajan vaatimukset. Ohjelmassa on mahdollisuus lisätä rajaton määrä laitteita sekä kopioida ja tallentaa varmuuskopioita päivittäin. Ohjelma tukee konfiguraatioiden palauttamista takaisin laitteisiin sekä käyttää SSH-yhteyttä laitteisiin yhdistämiseksi. HyperConf antaa myös verrata konfiguraatioita keskenään kätevästi ja käyttäjän niin halutessa kertoo, mitkä osat konfiguraatiosta eroavat toisistaan.

Ainoa huono puoli ohjelmistossa on, että se on maksullinen. Käyttäjän ei tarvitse maksaa ohjelmasta kuin kerran ja kyseinen versio pysyy hänellä, vaikka ohjelman tuki loppuisikin. Toisaalta käyttäjä ei voi ladata uusia versioita ohjelmasta, ellei hänellä ole maksullista päivitystukea. Koska opinnäytetyössä haluttiin ohjelma, jolla voisi hallita noin tuhatta verkkolaitetta, tarvittaisiin ohjelmasta kallein lisenssivaihtoehto (rajaton määrä laitteita).

4.6 WinSCP (32-bit)

Ohjelman käyttöjärjestelmävaatimukset ovat seuraavat:

Käyttöjärjestelmä: Microsoft Windows XP SP2/Windows Server 2003 SP1 and Newer
WinSCP toimii sekä Windows Server Core ja GUI versioissa
Levytila: 35-70 MB [27]

WinSCP on FTP-client ohjelmisto, jolla kokeiltiin konfiguraatiotiedostojen lataamista Zyxel USG 50 -palomuurilaitteesta. Ohjelmistossa on vaihtoehtoina käyttää FTP-, SFTP-, SCP- tai WebDAV-protokollia tiedostojen hakemiseen. Tiedostoja voi hakea joko graafisen käyttöliittymän tai komentorivipohjaisen shellin kautta.

Ohjelman kehittäjän sivustoilla on kattava tuki ohjelman käyttöön sekä ohjeet sen komentorivitulkin hyödyntämiseen. Myös batch-tiedostojen käyttö ohjelman komentorivitulkin kanssa oli opastettu sivuilla kohtuullisen hyvin. Ohjelmasta ei tässä työssä kerrota paljon, sillä työssä käytettiin yksinomaan WinSCP:n komentorivitulkkia.

4.7 RANCID

Vaikka alun perin aioimme etsiä ohjelmia vain Windowsille, niiden vähäisen määrän takia halusimme tutkia myös hiukan Linux-pohjaisia vaihtoehtoja. Yksi ohjelma erottui edukseen. RANCID eli Really Awesome New Cisco confIg Differ on avoimen lähdekoodin ohjelma, jonka avulla voidaan valvoa verkkolaitteen konfiguraatiota ja ylläpitää sen muutoshistoriaa. Se käyttää SSH:ta tai telnetiä laitteisiin yhdistämiseen. RANCID tukee mm. AW+ ajavia Allied Telesis kytkimiä, Cisco reitittimiä, Juniper reitittimiä, Catalyst kytkimiä, Foundry/Brocade kytkimiä, Redback NASs, ADC EZT3 kanavointilaitteita, MRTd, Alteon kytkimiä ja HP Procurve kytkimiä [28.]

RANCIDin toimintaperiaate on melko yksinkertainen. Se kirjautuu kaikille laitteille, jotka on määritelty reititystauluun ja ajaa erilaisia komentoja saadakseen tallennettavat tiedot. Tämän jälkeen RANCID muokkaa datan selkeämmäksi ja lähettää sähköpostilla muutokset edellisestä konfiguraatiosta. Lopuksi se tallettaa tiedot versionhallintajärjestelmään. RANCID ajastetaan toimimaan Linuxissa cron:n avulla [29] [28.]

Asensimme RANCIDin testimielessä virtuaalikoneelle, jossa oli Ubuntu 12.04 LTS -käyttöjärjestelmä. Meillä ei kuitenkaan ollut tarvittavasti kokemusta Linuxista, joten ongelmia tuli vastaan. Löysimme verkosta asennusohjeen, jota seurasimme. Pääsimme ohi parista ongelmakohdasta, mutta lopulta totesimme asennusohjeiden olevan puutteellisia. RANCID vaikutti hyvältä ohjelmalta ja monilla keskustelufoorumeilla suositeltiin sitä. Sen asennus ja konfigurointi on kuitenkin hankalaa sellaiselle, joka ei käytä paljon Linuxia.

4.8 Spiceworks

Spiceworks on laaja yrityksille sopiva IT:n hallintaohjelma. Spiceworks on täysin ilmainen ja se on saatavilla vain Windowsille. Kuten monet ilmaisohjelmat myös Spiceworks näyttää käyttäjälle mainoksia. Spiceworks sisältää paljon erilaisia ominaisuuksia, jotka helpottavat hallitsemaan tietotekniikkaympäristöä. Sen avulla voi mm. ylläpitää help deskiä, valvoa tietoliikenneverkkoa ja hallita verkossa olevia laitteita. Myös mobiililaitteiden hallinta on mahdollista. Spiceworksia käytetään verkkoselaimen kautta. Spiceworksia käyttää suuri yhteisö, jonka jäsenet voivat kysyä ja jakaa tietoa toistensa kanssa. Spiceworksin minimijärjestelmävaatimukset näkyvät taulukossa 1. Vaatimukset kasvavat sen mukaan, montako laitetta verkossa on [30].

Taulukko 1. Spiceworks järjestelmävaatimukset

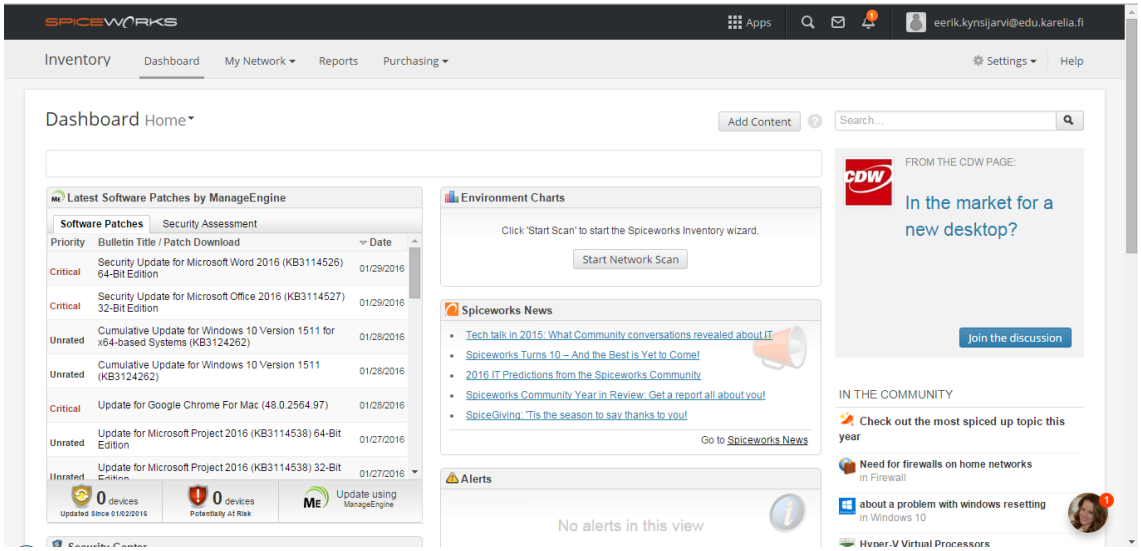
Minimijärjestelmävaatimukset: **1-30 laitetta**	
Prosessori:	1.5 GHz Pentium 4 Class
Muisti (RAM):	4 GB
Käyttöjärjestelmä:	Windows 8.1 Windows 7 Windows 2012 Server R2 Windows 2012 Server Windows 2008 Server R2 Windows 2008 Server
Verkkoselain:	Firefox uusin versio Chrome uusin versio Internet Explorer 10+

Tässä opinnäytetyössä tutkimme vain Spiceworksin laitteiden valvonta- ja hallintaosiota. Spiceworksin avulla voidaan hallita mm. Windows, Linux ja Mac OS tietokoneita, VOIP puhelimia, verkkotulostimia, reitittimiä, palomuureja ja muita SNMP:tä tukevia laitteita, aktiivihakemiston ryhmiä, Windowsin päivityksiä, palveluita ja tapahtumalokeja sekä virtuaalikoneita. Spiceworks voi automaattisesti etsiä latteita verkosta tai laitteet voidaan lisätä manuaalisesti. Spiceworks tarvitsee asentaa vain yhdelle koneelle. Verkon muihin laitteisiin ei tarvitse asentaa mitään, sillä Spiceworks ei tarvitse agentteja laitteiden löytämiseen. Muut käyttäjät voivat ottaa verkon kautta yhteyden Spiceworksiin [31.]

Opinnäytetyön kannalta tärkein ominaisuus on, että Spiceworksin avulla pystyy hallitsemaan verkkolaitteiden konfiguraatioita sisään rakennetun TFTP-palvelimen avulla. Laitteista voi varmuuskopioida käynnistys- ja ajonaikaisia konfiguraatioita. Vanhoja ja uusia konfiguraatioita pystyy helposti vertailemaan vierekkäin ja vanhan konfiguraation voi tarvittaessa palauttaa. Spiceworks käyttää SNMP-protokollaa skannatakseen ja yhdistääkseen verkkolaitteeseen ja sitten SSH:ta tai telnetiä suorittaakseen siinä komentoja. Spiceworks varmuusko-

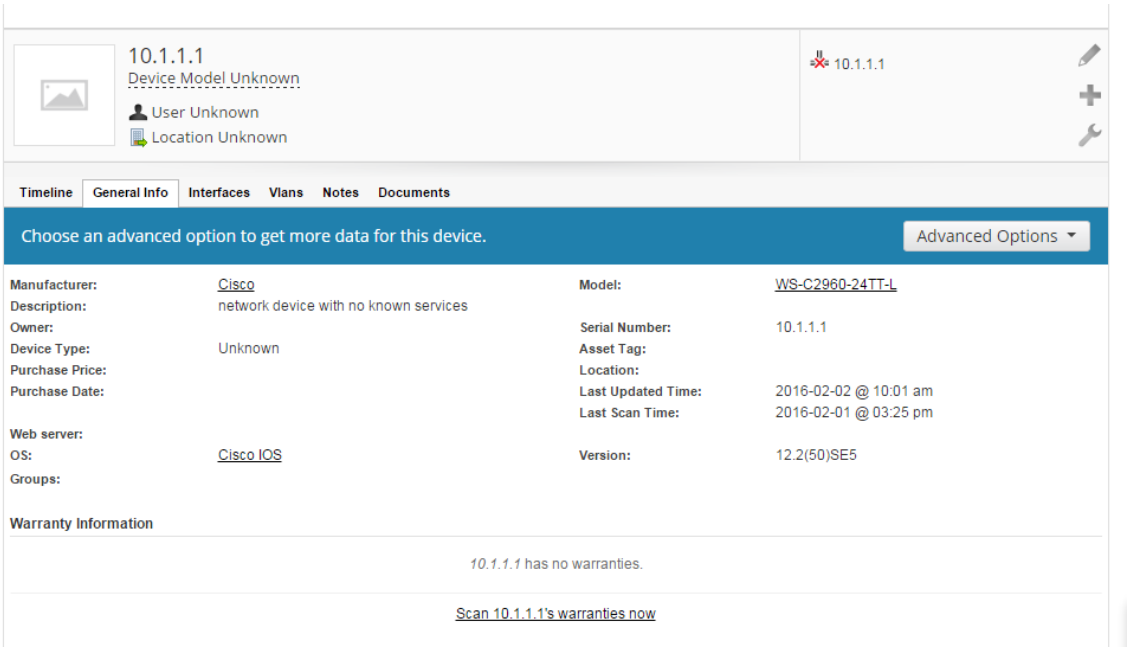
pioi konfiguraatiot ja siirtää ne käyttämällä TFTP:tä. Varmuuskopiot tallennetaan TFTP-hakemistoon Spiceworksin isäntäkoneelle [32.]

Kun Spiceworks käynnistetään, se avautuu selaimeen. Dasboardilla (Kuva 28) näkyy oletuksena mm. uutisia, yhteisön tapahtumia ja viimeisimpiä päivityksiä ohjelmiin. Dashboardin voi kuitenkin muokata itselleen sopivaksi lisäämällä ja poistamalla siitä tavaraa. Tärkein valikko on kuitenkin yläpalkista löytyvä My Network. Sen avulla voidaan skannata verkosta uusia laitteita ja tutkia niitä.



Kuva 28. Spiceworksin käyttöliittymä

Testasimme, että Spiceworks löysi Ciscon kytkimen SNMP:n avulla ja saimme siitä tiedot näkyviin (Kuva 29). Samalla ohjelma varmuuskopioi automaattisesti käynnistys- ja ajonaikaisen konfiguraation. Spiceworks tekee uudet varmuuskopiot, kun se havaitsee muutoksia laitteen konfiguraatioissa.



Kuva 29. Spiceworksin laitenäkymä

Spcieworks vaikutti aluksi lähes täydelliseltä ratkaisulta opinnäytetyöhön. Se oli erittäin helppo asentaa ja siinä oli selkeä käyttöliittymä. Laitteiden hakeminen ja varmuuskopiointi oli myös helppoa. Harkitsimme vakavasti sen käyttämistä lopullisena ratkaisuna tässä opinnäytetyössä. Pitkän tutkimisen jälkeen huomasimme, että siinä on kuitenkin puutteita. Spiceworksin ongelma on se, että se tukee vain TFTP-protokollaa verkkolaitteiden konfiguraatioiden varmuuskopioinnissa. Kaikki laitteet eivät kuitenkaan tue TFTP:tä. Saimme Ciscon kytkimestä helposti konfiguraatiot TFTP:n avulla, mutta Zyxelin palomuurista se ei onnistunut, sillä se ei tukenut TFTP-komentoja.

5 Testausympäristöt

5.1 Wärtsilä-kampuksen laboratorio

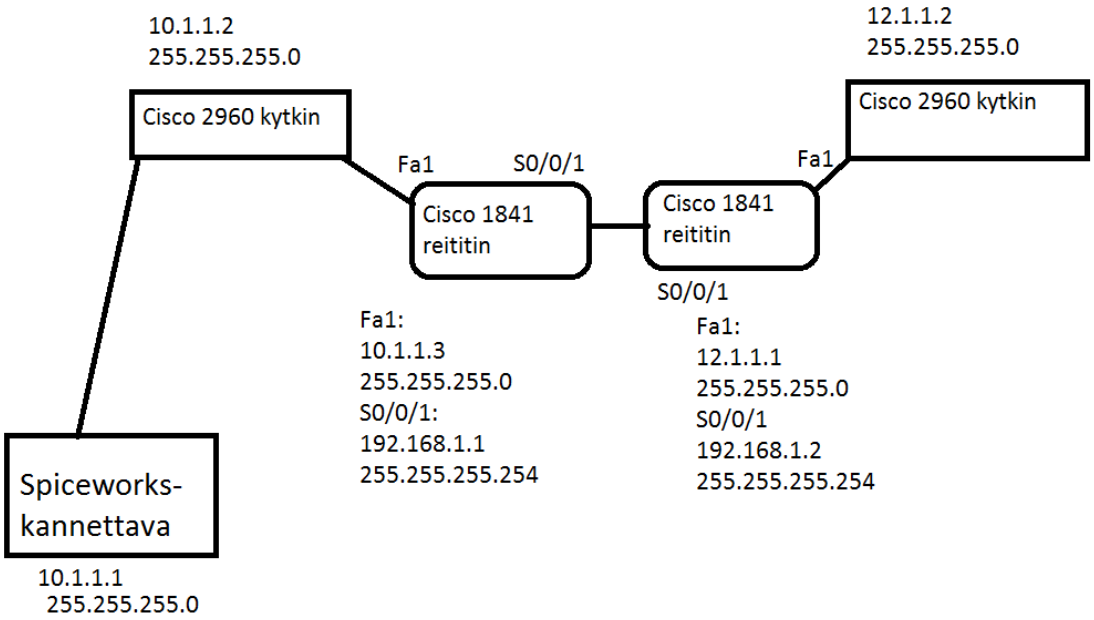
Wärtsilä-kampuksella testattiin sekä Spiceworksin että Xlight-FTP serverin toimintaa. Molempien järjestelmien testauksissa käytettiin koulun verkkolaitteistoa

(Cisco), joiden avulla rakennettiin pienimuotoinen verkkoympäristö. Verkkoympäristöllä mallinnettiin Bittigurun omaa verkkoa ja yhteyksiä muiden yritysten verkkoihin.

5.1.1 Spiceworks koulun testiverkossa

Opinnäytetyön tilaajan kanssa sovittiin, että palvelinta hallitaan Windowsin Remote Desktop Connectionin (RDP) avulla. Palvelinta hallittiin paikallisena järjestelmänvalvojana. Jotta varmuuskopiointia voitaisiin testata, liitettiin palomuurilaite samaan verkkoon palvelimemme kanssa. Palomuurilaitteesta oli tarkoitus kopioida talteen sekä running- että startup-konfiguraatiot.

Olimme luoneet koululla oman testiympäristön sekä tunnukset varmuuskopioinnin testausta varten. Emme kuitenkaan halunneet sekoittaa palvelinta koulun laitteilla, joten loimme kokonaan uudet tunnukset palvelinta varten. Palvelimelle pitää luoda kertaalleen vielä lopulliset Spiceworksin käyttäjätunnukset, koska käyttäjätunnukselle määritettiin mm. opiskelijan sähköposti ja nimitiedot. Koulun testiympäristö koostui kannettavasta tietokoneesta, Ciscon kahdesta 2960 kytkimestä sekä kahdesta Ciscon 1841 reitittimestä. Halusimme kokeilla, hakisiko Spiceworks erillisistä verkoista konfiguraatiot, joten eristimme kytkimillä kaksi eri verkkoa (10.1.1.0 /24 ja 12.1.1.0 /24) (Kuva 30).



Kuva 30. Wärtsilä-kampuksen testiverkko

Jotta saimme yhteydet reitittimien välillä kulkemaan, konfiguroimme molemmat laitteet RIPv2 –protokollalla ja mainostimme 10.1.1.0 ja 12.1.1.0 verkkoja. Tämän lisäksi konfiguroimme kaikki laitteet SSHv2:lla, jotta Spiceworks pääsisi ottamaan niihin yhteyttä. SSHv2:sen käyttöönottamiseksi piti laitteelle laittaa domain-nimi ja luoda rsa-salausavain [33.]

username admin privilege 15 password cisco
line vty 0 4
transport input ssh
login local
ip domain-name karelia.network
crypto-keys generate rsa general-keys modulus 1024
ip ssh version 2
no ip ssh version 1

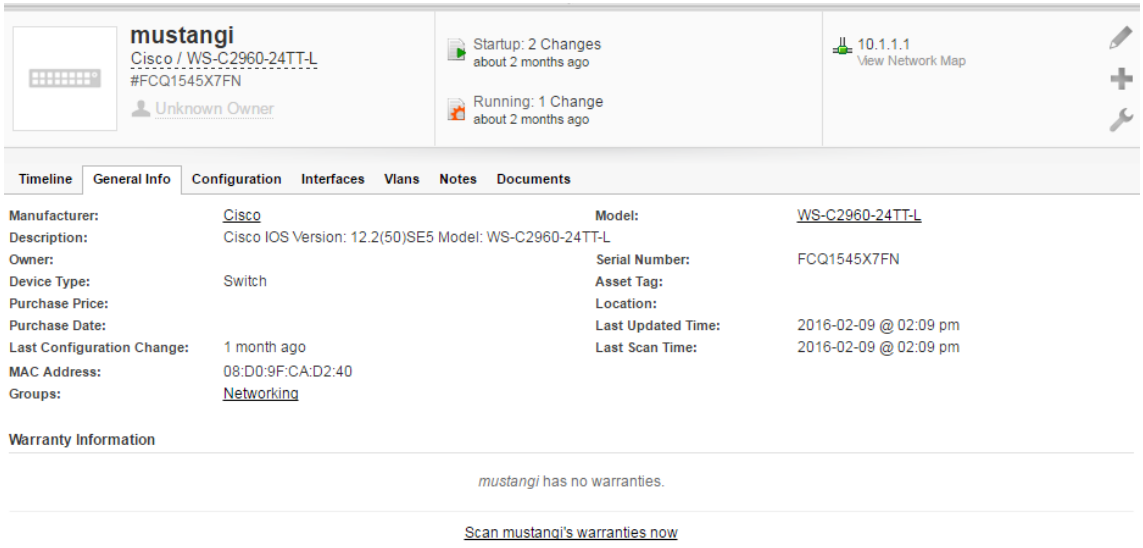
Tämän lisäksi laitteet piti konfiguroida SNMPv1-, v2- tai v3-protokollalla. Käytimme testeissämme v2:sta ilman autentikointia. Sen lisäksi konfiguroimme SNMP community stringit RW (read write) ja RO (read only) -oikeuksin. Spice-

worksissa piti määritellä, minkäniminen community string on laitteessa. Kyseinen nimi on käytännössä salasana snmp:lle. Viimeiseksi SNMP:llä piti ottaa ’Trap’ viestit käyttöön, ja määrittää mihin osoitteeseen viestejä lähetetään [34.]

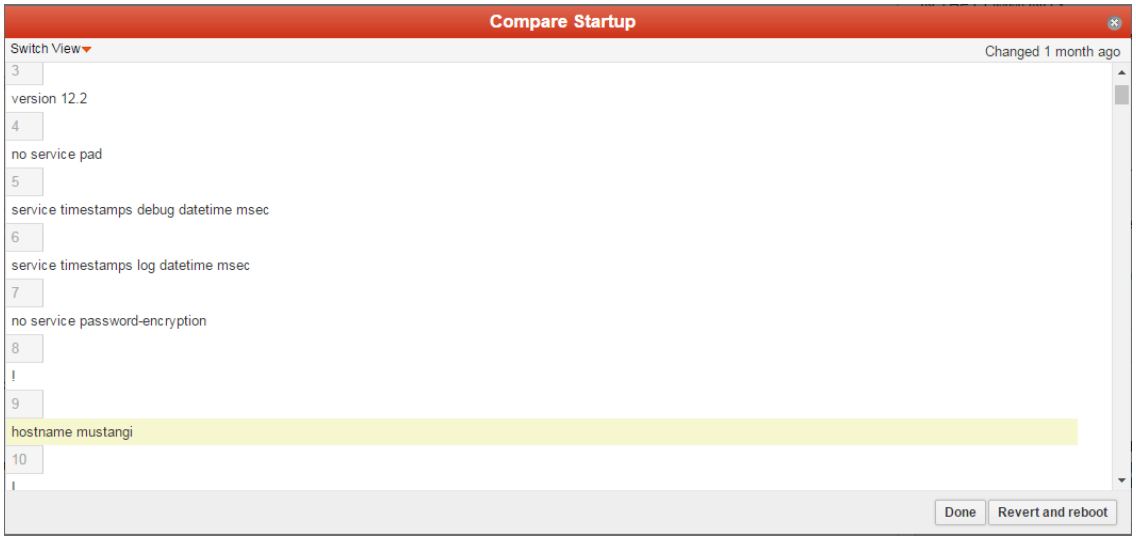
snmp-server community public RO
snmp-server community private RW

snmp-server enable traps
snmp-server host host-id [traps | informs][version {1 |2c | 3 [auth | noauth | priv]}] community-string [udp-port port-number] [notification-type]

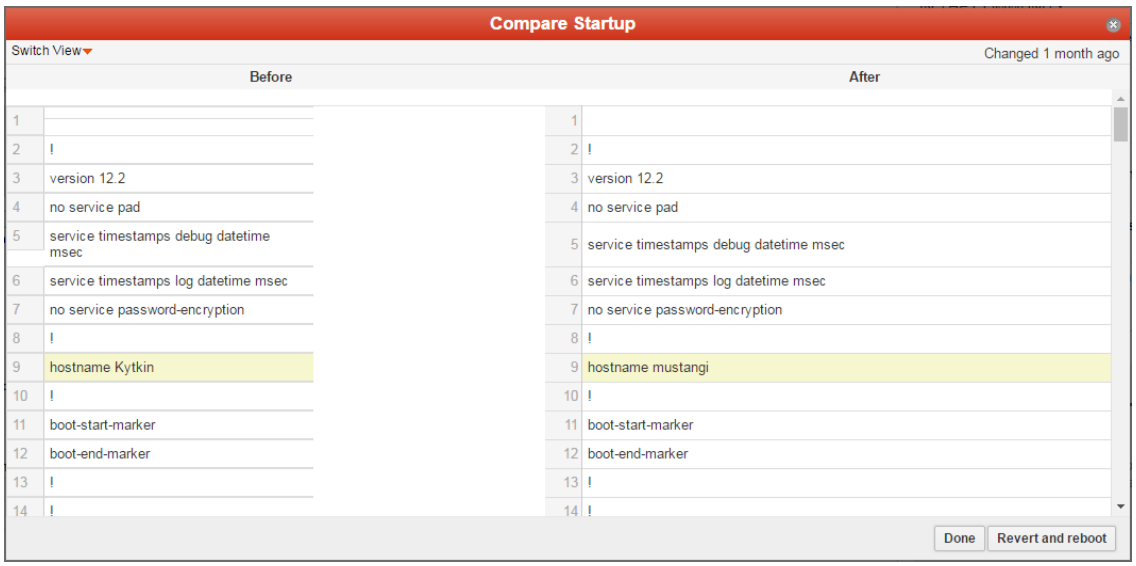
Seuraavaksi kokeilimme skannata kaikkia Spiceworksin kanssa yhteydessä olevia laitteita. Saimme laitteista laitetiedot (Kuva 31) ja konfiguraatiotiedostot (Kuva 32) jokaisen skannauksen jälkeen. Vanhaa ja uutta konfiguraatiota pystyy vertailemaan vierekkäin valitsemalla ’Switch View -valikosta’ ’Side by Side View’ (Kuva 33). Halutessa näkyviin saa pelkät muutokset valitsemalla ’Changes Only’. Testasimme vielä konfiguraatioiden hakua automaattisien skannauksien kohdalla ja totesimme Spiceworksin toimivan moitteetta. Ohjelma haki konfiguraatiot kaikista testiympäristön laitteista.



Kuva 31. Laitetiedot



Kuva 32. Laitekonfiguraatio

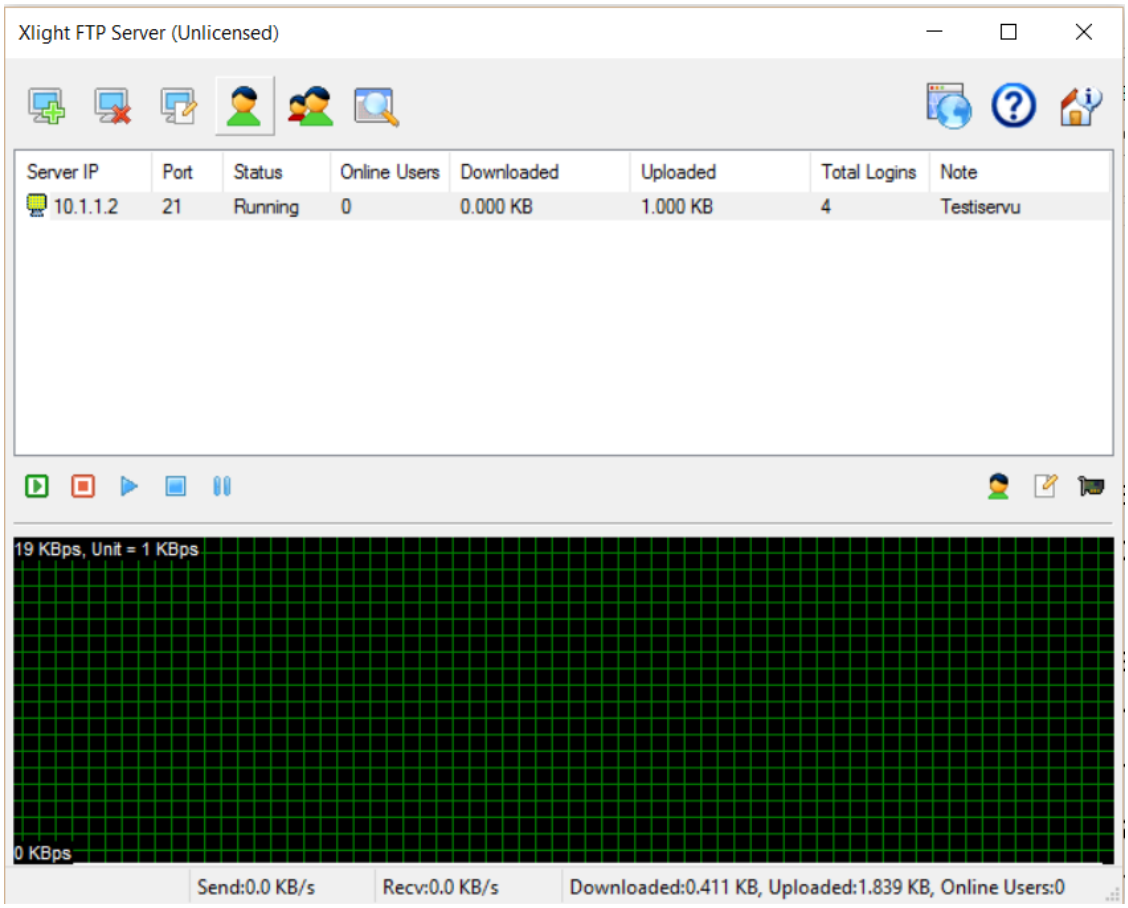


Kuva 33. Konfiguraatioiden vertailu

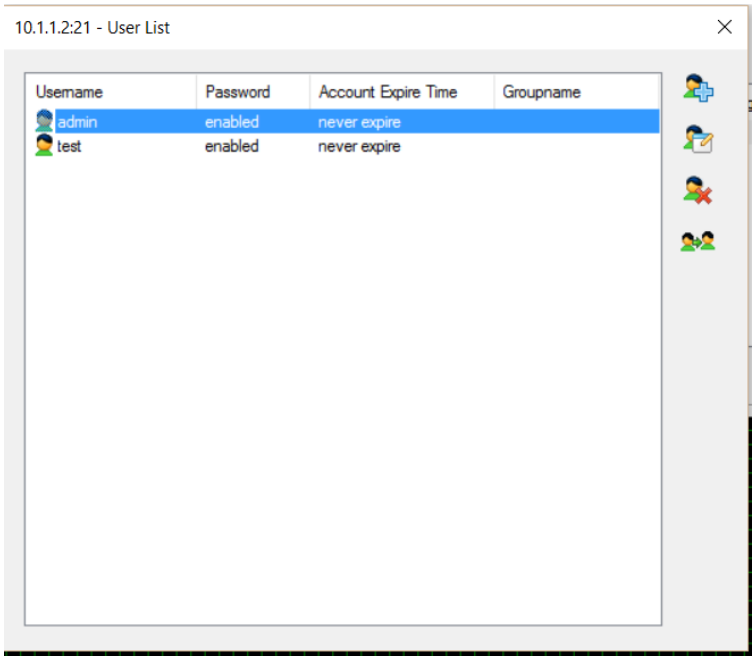
5.1.2 Xlight FTP server

Ciscon kytkimien IOS-käyttöjärjestelmät eivät tue enää FTP-Server ominaisuutta tietoturvariskien vuoksi. Tämän takia kytkimestä ei voida hakea konfiguraatiotiedostoja FTP-Clientin avulla, toisin kuin esimerkiksi Zyxelin USG-50 -palomuurista. Tällöin joudutaan asentamaan FTP- tai TFTP-Server, johon tiedot työnnetään. Testauksia varten asennettiin Xlight FTP Server, joka on koh-

tuullisen luotettava ja kätevä ohjelmisto. Ohjelmistoon luodaan virtuaalisia FTP-palvelinrajapintoja, jotka toimivat palvelimina joihin voidaan ottaa yhteyttä (Kuva 34). Ohjelmistoon pitää tehdä käyttäjätunnus ja liittää se johonkin kansioon, joiden avulla ohjelmistoon tunnistaudutaan ja voidaan tallentaa tiedostoja (Kuva 35). Kansiossa pitää olla tarvittavat oikeudet, jotta ohjelmisto pystyy tallentamaan siihen.



Kuva 34. Xlight FTP-server ohjelmisto



Kuva 35. Xlightin käyttäjät

Ohjelmiston ja käyttäjien luonnin jälkeen varmuuskopioitavaan laitteeseen (Cisco 2960) piti luoda vastaavat käyttäjätunnukset. Tämä tapahtui ’configure terminal -tilassa’ komennoilla:

ip ftp username käyttäjätunnus
ip ftp password salasana

Tämän jälkeen kytkimelle annettiin ’enable-tilassa’ komento:

copy nvram: startup-config ftp://ftp-palvelimen ip-osoite

Tiedosto tallentui ‘Tiedosto-formaatissa’, jolloin se piti avata Notepad++- ohjelmistolla. Tiedoston avaaminen Notepad++-ohjelmalla mahdollisti sen, että konfiguraatiossa oleva teksti on selväkielistä. Seuraavaksi tiedostosta piti tehdä batch-skripti sekä tekstitiedosto, jossa ovat varmuuskopiointikomennot. Skriptissä käsketään avata ’putty.exe -työkalu’, jolla otetaan SSH-yhteys IP-osoitteeseen tietyillä käyttäjätunnuksilla. Tämän jälkeen komento avaa tekstitie-

doston, jossa ovat laitteen komennot. Komennot menevät puttyn etäyhteysikkunan kautta verkkolaitteelle [35.]

Batch-tiedosto:

C:\"Program Files"\Putty\putty.exe -ssh 10.1.1.1 -l admin -pw cisco -m C:\FTPutty.txt

Tekstitiedosto:

copy nvram:startup-config ftp://10.1.1.2

Koska haluttiin automatisoida koko prosessi, piti kytkin asettaa ’quiet-tilaan’. Tällöin laite ei pyydä käyttäjää varmistamaan komentoja painamalla ’enter-painiketta’. Tämä johtuu siitä, että kytkin on niin sanotussa interaktiivisessa tilassa. ’File prompt quiet -komennolla’ saadaan kytkin pois interaktiivisesta varmistustilasta.

Jos halutaan viedä skriptin automaattisuutta hieman pidemmälle, voidaan kaikki kytkimelle tarkoitetut asetukset ja käyttäjätunnukset kirjoittaa skriptiin. Tässä tapauksessa kannattaisi tehdä erillinen skripti, joka asettaa kyseiset asetukset vain yhden kerran eikä varmuuskopioinnin yhteydessä, muuten jouduttaisiin konfiguroimaan jokainen laite erikseen etäyhteyksien kautta. On otettava huomioon se, että aiemmin mainitut komennot ovat laitekohtaisia. Kuitenkin kaikille Ciscon kytkimille voidaan asettaa kyseiset komennot skriptin avulla.

5.2 Bittigurun demoverkko

Bittigurun vastaava tietoteknikko loi valmiiksi testiympäristön, johon liitettiin palomuurilaite konfiguraatiotestauksia varten. Testiympäristössä oli myös Windows Server 2012 R2 palvelin, jota käytimme varmuuskopiointipalvelimena. Palvelimeen sallittiin etäyhteys, jotta voisimme hallita sitä.

5.2.1 Spiceworks Bittigurun demoverkossa

Vältimme palvelimen selainyhteyksien käyttöä tietoturvariskien takia. Sen sijaan siirsimme kaikki tarpeelliset asennuspaketit RDP:n kautta sekä asensimme Spiceworksin palvelimelle. Aluksi ohjelmistosta poistettiin kaikki automaattiset skannausprosessit, koska järjestelmä on suunniteltu skannaamaan automaattisesti erilaisia verkkoympäristöjä 5-180 minuutin välein. Järjestelmästä ei oteta käyttöön kaikkia skannausoperaatioita ainakaan aluksi, sillä ne vain hidastavat ja vaikeuttavat alkukonfiguraatioita ja testauksia. Koulun testausympäristössä todettiin, että jos palvelin skannaa verkkolaitteita, niin laitteista ei voi silloin ottaa varmuuskopioita ja ohjelma saattoi hidastella paljonkin. Toisin kuin koulun testausympäristössä, Spiceworks tunnisti automaattisesti siihen liitetyn palomuurin ilman manuaalista skannausta.

Huomasimme, että varmuuskopiointi ei toimi luotettavasti, ellei ohjelmalle kerro sen isäntälaitteen ip-osoitetta. Tämä tapahtui palvelimen komentorivin (cmd.exe) avulla, josta avattiin Spiceworksin konsoli sen asennuskansiosta. Konsolia avatessa kesti hieman, kun ohjelma latasi asetuksia. Konsoliin kirjoitettiin komento, jossa kerrottiin nykyinen ’local_ip_address’, minkä jälkeen konsolista poistuttiin ja Spiceworks käynnistettiin uudelleen (Kuva 36).

Kuva 36. Spiceworks ip-komento

Komentoriviltä:

cd C:\Program Files\Spiceworks\bin
spiceworks.exe console
Configuration[:local_ip_address] = “ip-osoite”
quit

Tämän jälkeen testasimme, toimiiko varmuuskopiointi. Meidän piti manuaalisesti syöttää ohjelmalle kaikki kirjautumistiedot, joilla halusimme ohjelman kirjautu-

van muille laitteille. Palomuuria varten syötimme SSH-tunnukset, jotka oli annettu erillisessä dokumentaatiossa. Skannauksessa valitsimme myös skannattavaksi pelkän palomuurin osoitteen, sillä koko verkon skannaamisessa saattaisi kestää hetken. Tämä johtuu siitä, että ohjelmalla kestää hetki prosessoida käyttämätön ip-osoite. Tyhjät osoitteet skannataan nopeammin kuin käytetyt, sillä ohjelma kokeilee eri käyttäjätunnuksia kaikkiin laitteisiin. Skannauksen nopeuttamiseksi voidaan jokaiselle kohdelaitteelle määrittää, miten laitteelle kirjaudutaan tai miten se skannataan.

Ensimmäinen skannaus haki onnistuneesti kaikki laitteen tiedot, mukaanlukien tarkat porttitiedot ja ip-osoitteet. Skannaus ei kuitenkaan hakenut konfiguraatioita, kuten sen olisi pitänyt. Tämän takia kokeilimme ottaa palvelimelle käyttöön TFTP-client -toiminnon. Toiminto lisättiin Server Managerin avulla ’Add Roles and Features -valikosta’. Oletuksena Spiceworksissa on TFTP-palvelin, mutta Spiceworksin ohjeistus kehottaa sallimaan Windows-pohjaisista koneista TFTP-client palvelun. Tämän lisäksi palvelimen omasta palomuurisoftasta sallittiin UDP-portti 69 liikenne sisään ja ulos TFTP-liikenteen sallimiseksi.

Huolimatta tekemistämme lisäasetuksista ei skannauksella saatu haettua Zyxelin palomuurilaitteesta konfiguraatioita. Yritimme seuraavaksi tehdä manuaalisesti Spiceworksin toiminnot. Otimme SSH-yhteyden laitteeseen, jonka jälkeen aloimme etsiä TFTP-komentoja. Emme löytäneet minkäänlaisia TFTP-komentoja laitteesta. Huomasimme Zyxelin verkkosivuja tutkiessamme, että yksikään Zyxel-laite ei tue TFTP-protokollaa.

Opinnäytetyön tilaaja oli kuitenkin testannut Spiceworksia ja totesi että ohjelmisto toimii ja näyttää vakuuttavalta. Hän ehdotti, että selvitämme, voiko Spiceworksiin lisätä esimerkiksi FTP-skriptejä, koska Zyxel-laitteet tukevat FTP-protokollaa. Tällöin Spiceworksin rinnalle lisättäisiin erillinen FTP-Ohjelmisto, joka lataisi konfiguraatiot.

Otimme seuraavaksi yhteyttä Spiceworksin tukeen Zyxelin varmuuskopioinnista. Tukihenkilö pyysi lähettämään Spiceworksin konfiguraatiot ja TFTP-komennot Zyxeliä varten. Saimme selville, että Zyxel ei tue TFTP-komentoja,

joten ehdotimme erillisten FTP-skriptien käyttöä Spiceworksiin. Tukihenkilö totesi, että valitettavasti FTP-skriptejä ei voi tällä hetkellä liittää Spiceworksiin, joten Zyxelin varmuuskopiointi ei tulisi onnistumaan Spiceworksilla.

5.2.2 WinSCP ja Batch

Testasimme aluksi graafista käyttöliittymää FTP-yhteydellä, eikä konfiguraation hakemisessa ollut ongelmia. Kun testasimme samaa toimintoa komentorivillä, ohjelma ilmoitti, että käytettävä shell ei ole yhteensopiva kohdelaitteen kanssa. Ongelma yritettiin ratkaista siten, että vaihdettiin ohjelman lisäasetuksista shelliksi ’Bash’. Myös tämän jälkeen ongelma ilmaantui uudelleen, koska komentorivipohjainen shell yritti ottaa yhteyttä palomuurilaitteeseen oletettavasti SCP-yhteydellä. Laitoimme seuraavan komennon WinSCP:n shelliin, jotta saimme FTP-yhteyden laitteeseen [36]:

open ftp://x.x.x.x

Tämän jälkeen ohjelma kysyi käyttäjätunnuksia. Seuraavaksi kirjoitimme komennon, jossa oli hakukomento, haettava tiedosto sekä tallennuskohde ja tiedostonimi [36]:

get /conf/startup-config.conf C:\users\administrator\documents\konffit\testi

Komennon syöttämisen jälkeen ohjelma ilmoitti, kuinka suuri tiedosto on ja missä vaiheessa tiedoston kopioiminen on. Seuraavaksi kävimme tarkastamassa tiedoston. Jouduimme käyttämään tiedoston avaamisessa Notepad++- ohjelmistoa, koska tiedostolla ei ollut formaattia. Jälkeenpäin huomattiin, että jos tiedoston tallennussijainnin perään laittaa esimerkiksi txt-formaatin, se on luettavissa tavallisella tekstinkäsittelyohjelmistolla.

Seuraavaksi piti miettiä, miten manuaalinen toiminto saadaan automaattiseksi. Käytimme tähän batch-tiedostoa, jossa määritettiin WinSCP-tiedoston avaaminen ja FTP-komentojen syöttäminen. Ohjelmiston kehittäjän sivulla oli kohtuullisen hyvät tiedot siitä, miten skriptien luominen onnistuu. Aiemmista ohjelmista

(putty) ei löytynyt niin hyviä tietoja siitä, miten komentorivipohjainen skripti onnistuu ja mitä komentoja ja syntakseja tarvitaan. Suurin ongelma aiemmin oli siinä, miten skripti kirjoittaa komennot haluamaamme komentorivi-ikkunaan. Tällä kertaa kyseinen toiminto ei tuottanut ongelmia. Skripti on yksinkertainen:

"C:\Program Files (x86)\WinSCP\WinSCP.com" /command ^
"open ftp://admin:12345@172.18.1.100:21" ^
"get /conf/startup-config.conf C:\users\administrator\documents\konffit\" ^
"exit"

Ensimmäinen rivi avaa WinSCP-komentorivin. Rivillä oleva ’/command’ mahdollistaa sen, että .bat tiedostoon voidaan suoraan kirjoittaa komennot, jotka halutaan kohdeikkunaan. Tällöin ei tarvitse luoda erillistä skriptitiedostoa syötettäville komennoille ja järjestelmästä tulee yksinkertaisempi ja helpompi ymmärtää. ’^’ -merkki rivien lopussa mahdollistaa rivien vaihtamisen. Muuten skriptistä tulisi yksi pitkä rivi, joka olisi vaikeampi ymmärtää.

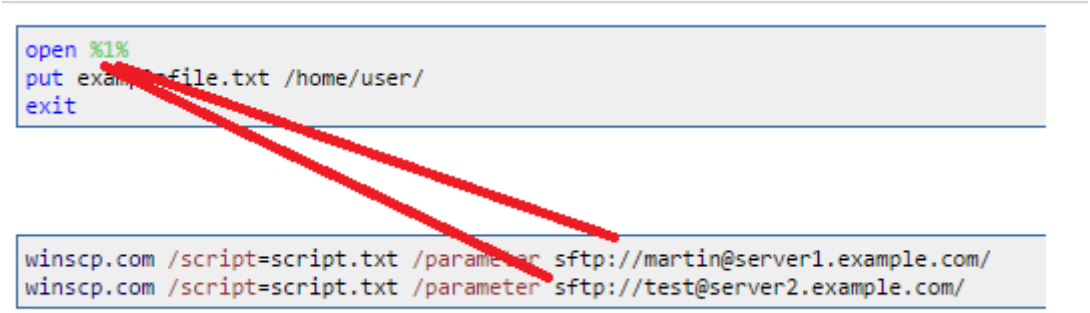
Toinen rivi skriptissä ottaa ftp-yhteyden palvelimelle tietyillä käyttäjätunnuksilla. Toiseksi viimeinen rivi hakee konfiguraatiotiedoston ja tallentaa sen tiettyyn kohteeseen. Viimeinen rivi sulkee yhteyden ja sammuttaa WinSCP-komentorivin. Tällä kertaa haetut konfiguraatiotiedostot tallentuivat ’.conf-formaatissa’. Tällöin tiedostot voitiin avata tavallisella tekstinkäsittelyohjelmalla, ja teksti oli luettavaa.

Jotta tiedostoista tulee tunnistettavia, niihin on hyvä lisätä jonkinlainen aikaleima ja ehkä lisäksi laitteen nimi. Aikaleiman saa tiedostonimeen lisäämällä siihen ’Timestamp-funktion’. Funktio tulee siis skriptin kolmannelle riville ’get-komennon’ rinnalle. Tämän lisäksi funktion perään pitää kirjoittaa ’.conf’, jotta ohjelma osaa tallentaa tiedoston oikeassa formaatissa [36.]

"get /conf/startup-config.conf C:\users\administrator\documents\konffit\startup-config.%%TIMESTAMP#dd.mm.yyyy%%.conf"" ^

Ohjelmiston pitäisi ottaa yhteys useampaan laitteeseen, tunnistautua eri käyttäjätunnuksilla ja ladata konfiguraatio. Tämä onnistuu parametrien avulla.

WinSCP voi muuttaa skriptissä olevia muuttujia, jotka ovat formaatissa ’%1%’, ’%2%’, ’%3%’, jne. Batch tiedostossa määritetään ohjelma ja skripti. Batch-tiedostoon kirjoitetaan /parameter, jonka perään kirjoitetaan komento tai teksti. Em. teksti korvaa skriptissä olevan ’%1%-merkin’ (Kuva 37).



Kuva 37. Parametrin toiminta

Kuvassa toisella rivillä oleva komento avaa saman skriptin, mutta asettaa muuttujille eri parametrit. Tämä mahdollistaa useampiin osoitteisiin yhdistämisen samalla .bat-tiedostolla. Myös käyttäjätunnukset voidaan täten asettaa laitekohtaisesti. Jos halutaan lisää muuttujia, kirjoitetaan ensimmäisen parametrikomennon jälkeen toinen komento, jolla ohjelma viittaa merkkiin ’%2%’ [36]:

/parameter ftp://user.password@10.1.1.1(1 parametri) network configuration (2 parametri)

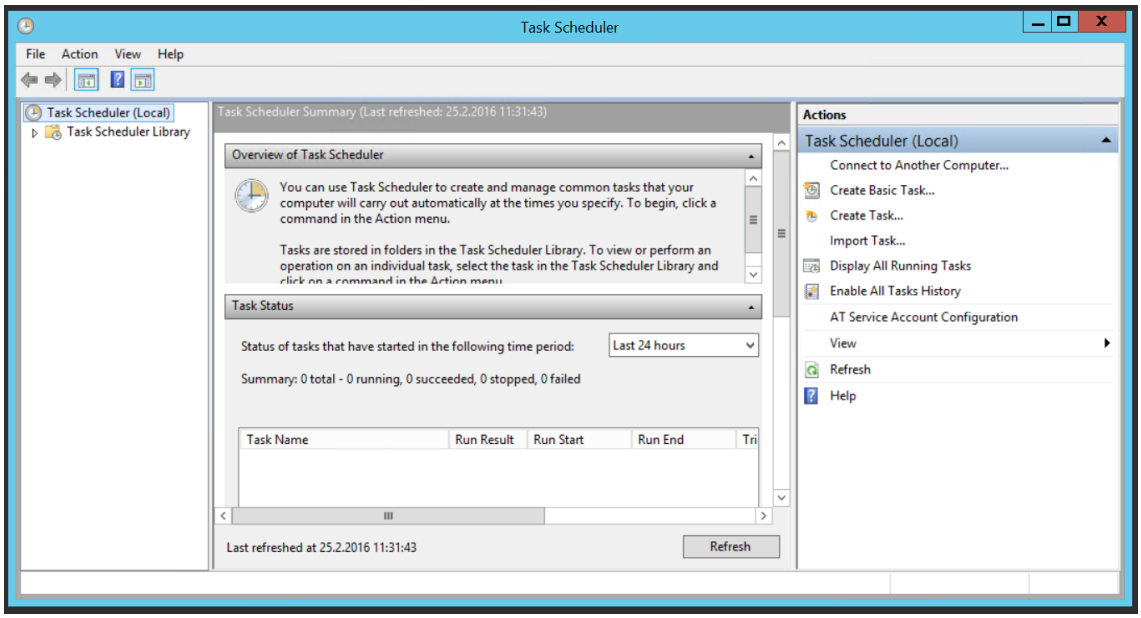
Seuraavaksi testasimme batch scriptin vikasietoisuutta. Lisäsimme saman parametrikomennon kahteen kertaan skriptiin, mutta vaihdoimme toisen komennon tallennussijaintia. Sen jälkeen muutimme ensimmäisen komennon ip-osoitteen sellaiseksi, johon ei voitu saada yhteyttä. Skripti yritti ottaa yhteyttä vääräksi muutettuun osoitteeseen noin viiden sekunnin ajan, minkä jälkeen se lakkasi yrittämästä. Tämän jälkeen komentorivi-ikkuna sulkeutui ja näytöllä vilahti toinen komentorivi-ikkuna. Varmistimme sitten toisen komennon toiminnan tarkastamalla, oliko konfiguraatiotiedosto tallentunut. Seuraavaksi kokeilimme samaa, mutta toisen rivin komennon ip-osoitetta muuttamalla ja korjasimme ensimmäisen ip-osoitteen oikeaksi. Testit menivät moitteettomasti läpi. Oletuksena

siis WinSCP yrittää muodostaa yhteyttä noin viiden sekunnin ajan, minkä jälkeen lopettaa yrittämisen.

Toisena testinä kokeilimme, riskeeraavatko väärät käyttäjätunnukset skriptin toiminnan. Kirjoitimme tahallaan skriptiin väärät käyttäjätunnukset sekä ensimmäiselle että toiselle komennolle. Kummassakaan kohdassa skripti ei takkuillut, vaan katkaisi automaattisesti yhteyden, jos käyttäjätunnukset eivät kelvanneet laitteelle. Halusimme testata kyseiset seikat, sillä skriptin käyttöönotossa pitää tehdä paljon manuaalista työtä eli kopioida komentoja riveiltä toiselle.

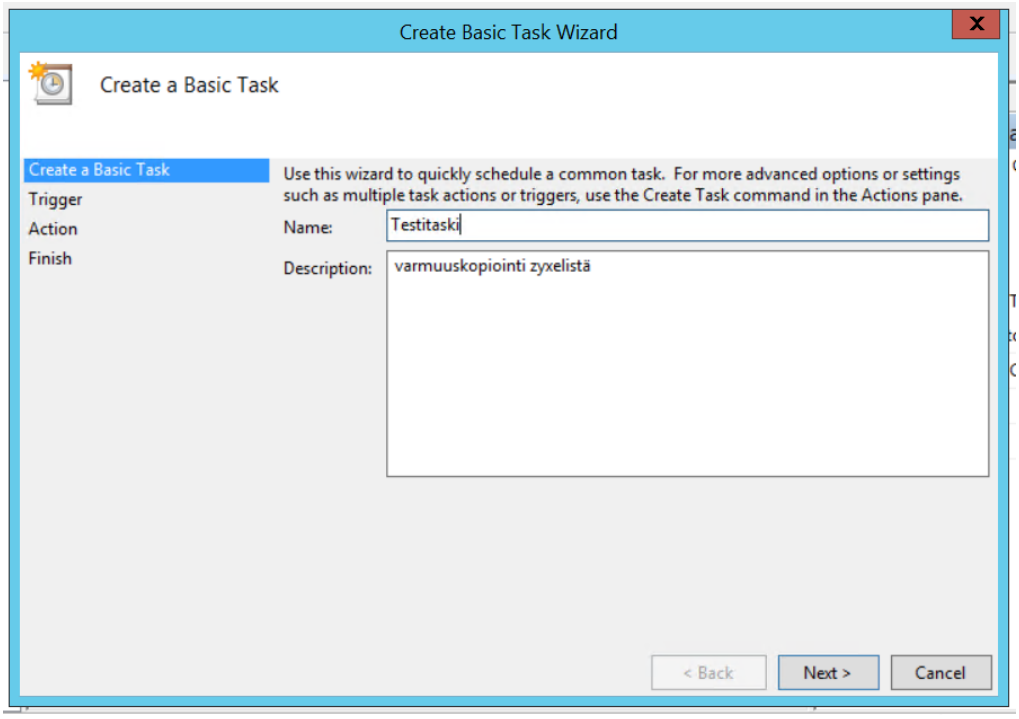
5.2.3 Batch-skriptin lisäominaisuudet

Jotta varmuuskopiointia ei tarvitse suorittaa manuaalisesti joka kerta, varmuuskopiontiskriptin suorittaminen pitää automatisoida. Windows-käyttöjärjestelmässä on tehtävien ajastusta varten oma komponenttinsa nimeltä Windows Task Scheduler (Kuva 38). Task Scheduler löytyy mm. Windows 7:ssa ja Windows Server 2012:ssa ohjauspaneelin valvontatyökaluista.

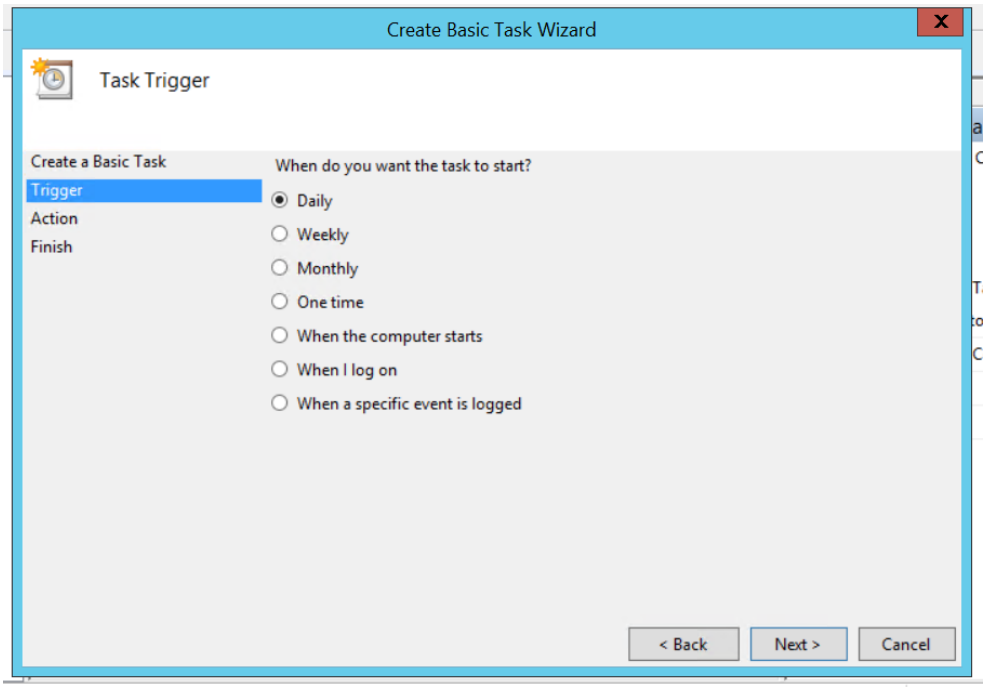


Kuva 38. Task Schedulerin käyttöliittymä

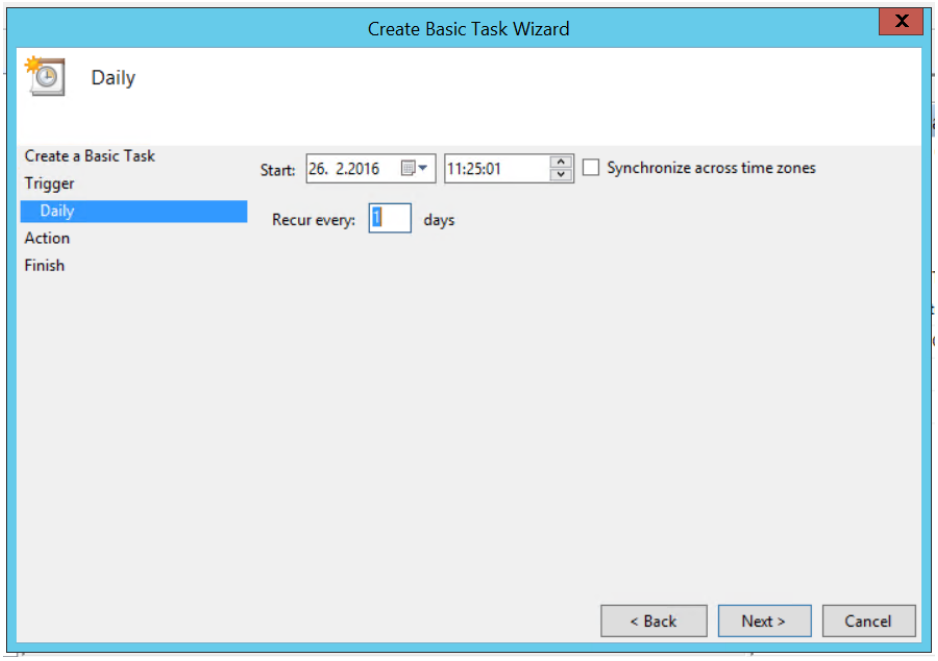
Uusi tehtävä saadaan valitsemalla oikealla olevasta tehtäväpalkista Create Basic Task. Tämän jälkeen kysytään tehtävän nimeä ja sen kuvausta (Kuva 39). Seuraavaksi tehtävälle määritellään laukaisin (trigger) eli ehto, jonka täyttyessä tehtävä suoritetaan. Valitsimme tässä testissä, että varmuuskopiointi suoritetaan päivittäin kello 11.27 (Kuva 40 ja Kuva 41). Viimeisenä valitaan toiminta, joka tapahtuu, kun määritelty ehto täyttyy (Kuva 42). Valittavissa on mm. ohjelman käynnistys, sähköpostin lähetys ja viestin näyttö. Valittaessa ohjelman aloitus, pitää seuraavassa vaiheessa määritellä ohjelman tai skriptin tiedostosijainti. Määritimme tähän varmuuskopiontiskriptimme sijainnin (Kuva 43). Lopuksi näkyy vielä yhteenveto syötetyistä tiedoista (Kuva 44).



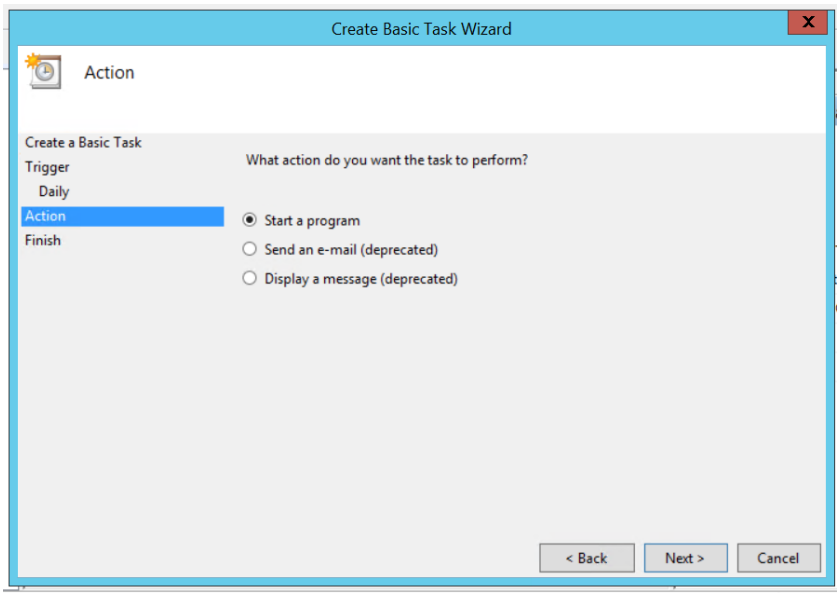
Kuva 39. Tehtävän nimeäminen



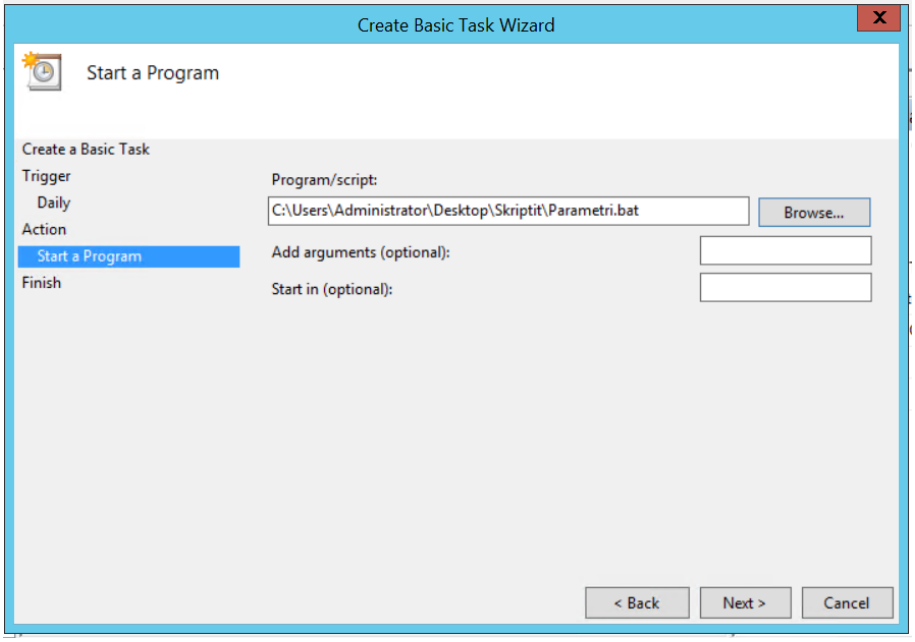
Kuva 40. Tehtävän ajastusajankohta



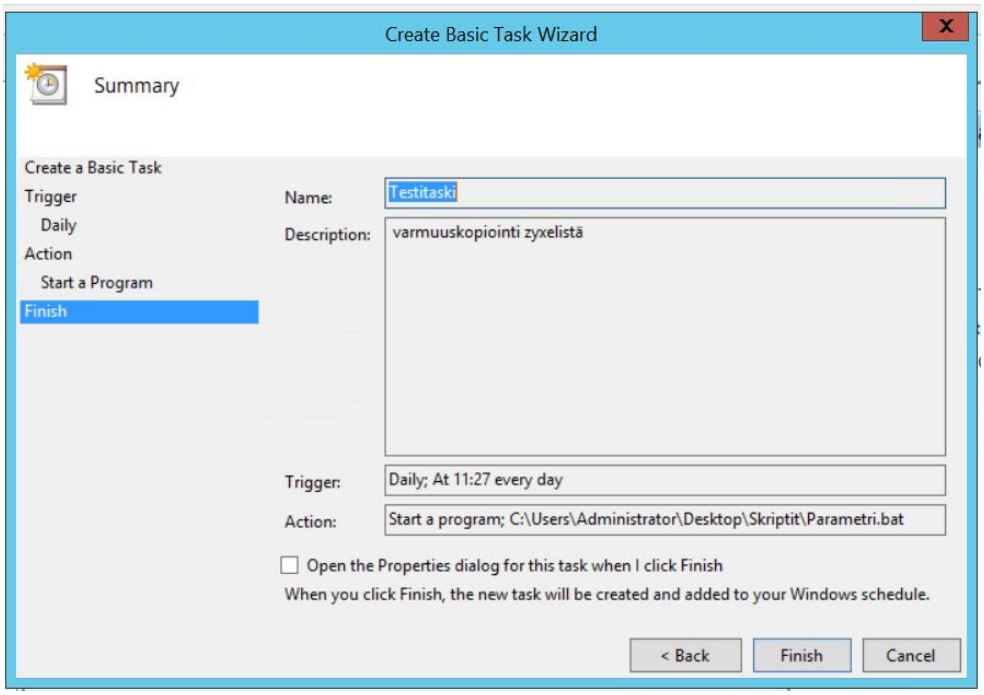
Kuva 41. Ajastustehtävän tarkempi ajankohta



Kuva 42. Valittava aktiviteetti



Kuva 43. Skriptin valinta



Kuva 44. Tiivistelmä tapahtumasta

Seuraavaksi tarkastelimme varmuuskopiointitapahtumaa, jota varten käytetään lokeja. Loki tarkoittaa tallennetta, johon kirjataan aikajärjestyksessä tapahtumia. Ohjelmien ja tietojärjestelmien toiminta ja niissä tapahtuvat muutokset voidaan kirjata lokiin eli ne lokitetaan. Lokitietojen avulla voidaan tarkistaa, että käsitelty tieto on oikeaa ja ettei virheitä ole syntynyt. Hyvästä lokitiedostosta löytyy Viestintäviraston mukaan aikaleima, tapahtuma ja sen lähde, kohde, toimija, käyttöoikeus sekä tapahtuman tila [37]. Lokien avulla voidaan tutkia järjestelmän toimintaa, käyttäjien toimintaa, järjestelmässä tapahtuvia muutoksia ja siihen lisättyä ja siitä poistettua tietoa ja virheilmoituksia. Yksi lokien tärkeimmistä hyödystä on virhetilanteiden selvittäminen. Lokitietoja tulee säilyttää tarpeeksi pitkään, koska niitä voidaan tarvita pitkänkin ajan kuluttua [38.]

Tässä opinnäytetyössä meitä kiinnosti erityisesti ohjelman suorittamiseen liittyvät lokitiedot. Halusimme, että kaikki varmuuskopiointiskriptin suorittamisen aikana komentoriville tuleva teksti menee lokitiedostoon. Lokin avulla voimme tarkistaa, onko varmuuskopiointi sujunut onnistuneesti.

Seuraavan komennon avulla voidaan tallentaa lokitiedostoon haluttujen komentojen tuloste [39]:

```
@echo off
>output.txt (
  command1
  command2
  ...
  command
)
```

Komento tallentaa output.txt-nimiseen tiedostoon sulkujen sisällä olevien komentojen komentorivitulosteen. Jotta oikean lokitiedoston löytäminen olisi helpompaa, päätimme määritellä lokitiedoston nimeen päivämäärän, jolloin varmuuskopionti on suoritettu. Päivämäärän saa tiedostonimeen määrittämällä siihen seuraavan formaatin [40]:

```
%DATE:~-10,-8%-%DATE:~-7,-5%-%DATE:~-4%
```

Tämä formaatti on riippuvainen tietokoneen lokaalista ja yllä mainittu formaatti on Yhdysvaltojen lokaalille. ’%DATE:~-10,-8%’ hakee päivämäärän, ’%-%DATE:~-7,-5%’ hakee kuukauden ja ’%DATE:~-4%’ hakee vuoden.

Varmuuskopiointia varten käytimme työssä mm. seuraavaa skriptiä:

```
@echo off
>C:\Users\Administrator\Documents\Konffit\Lokit\%DATE:~-10,-8%-%DATE:~-7,-5%-%DATE:~-4%.log (
"C:\Program Files (x86)\WinSCP\WinSCP.com" /script=C:\"FTPscript.txt" /parameter ftp://admin:12345@172.18.1.100:21 liperi konfiguraatio
"C:\Program Files (x86)\WinSCP\WinSCP.com" /script=C:\"FTPscript.txt" /parameter ftp://admin:12345@172.18.1.100:21 eno konfiggi
Powershell.exe -Command "& {Start-Process PowerShell.exe -ArgumentList '-ExecutionPolicy Bypass -File
""C:\Users\Administrator\Desktop\Skriptit\Tiedostonpoisto Po-
```

wershell\poisto.ps1"" -Verb RunAs}"
)

Skriptissä oleva FTPscript.txt on:

open %1%
get /conf/startup-config.conf
C:\users\administrator\documents\konffit\%2%\%3%.%TIMESTAMP#dd.mm.yyyy%.conf"
exit

Kun skripti ajetaan esimerkiksi 2.3.2016, saadaan lokitiedosto, jonka nimi on 02-03-2016.log. Tiedoston sisältö on seuraavanlainen:

Connecting to 172.18.1.100 ...
Connected
Starting the session...
Session started.
Active session: [1] admin@172.18.1.100
startup-config.conf | 13 KB | 231,5 KB/s | binary | 100%
Connecting to 172.18.1.100 ...
Connected
Starting the session...
Session started.
Active session: [1] admin@172.18.1.100
startup-config.conf | 13 KB | 843,9 KB/s | binary | 100%

Lokitiedostosta nähdään, että kumpikin varmuuskopionti on suoritettu onnistuneesti, sillä kopiointi on 100 %.

Opinnäytetyön suunnitelmassa määritettiin, että konfiguraatioita pitää olla kerrallaan vain 7 kappaletta. Tämä tarkoittaa sitä, että vanhat konfiguraatiot pitää poistaa automaattisesti muistin tuhlaamisen välttämiseksi. Kyseinen toiminto oli valmiina Spiceworksissa sekä muissa testatuissa ohjelmistoissa. Poistamisen

lisäominaisuudet sai määritettyä kohtalaisen tarkasti. Kyseinen ominaisuus piti ottaa käyttöön täten myös skripteissä.

Onneksi kyseinen batch-skriptin toiminto oli valmiina, paitsi että sitä piti hieman mukauttaa. Kyseessä oleva ’forfiles-komento’ on usein käytetty batch-tiedostoissa ja sitä käytetään tiedostojen tarkastelemiseen. Useilta verkkosivuilta löytyi kohtalaisen identtisiä ratkaisuja komennon käyttöön, joita piti vain testata. Skripti ei ole yhtä riviä pitempi, mutta siihen voi tarvittaessa lisäillä erikoistoimintoja. Tällaisia toimintoja voisivat olla esimerkiksi tiedostojen päivämäärien tai konfiguraatioiden muutosten vertailut.

Komento tullaan mahdollisesti liittämään osaksi varmuuskopiointiskriptiä, jolloin palvelimen tarvitsee ajaa vain yksi skripti kerran päivässä ’Windows Task Schedulerin’ avulla. Automaattisen poistokomennon sijainnilla ei skriptissä ole väliä, koska skripti tunnistaa, milloin tiedosto on 7 päivää vanha eikä milloin varmuuskopioita on 7 kappaletta/laite [41.]

*forfiles /p "C:\tiedostosijainti" /s /m *.* /d -7 /c "cmd /c Del @path"*

Forfiles-komento käy läpi annetun tiedostosijainnin tiedostot ja myös kaikkien sen alikansioiden tiedostot parametrillä ’/p’. Parametri ’/s’ ohjeistaa etsimään kaikista alikansioista, kun taas ’/m’ etsii tiedostoja, joiden formaatti vastaa annettua esimerkkiä (*-merkki etsii kaikkia tiedostoja). ’/d’ parametrin jälkeen annetaan tiedoston suurin sallittu ikä, minkä jälkeen tiedosto poistetaan. Komennossa oleva ’/c’ ilmaisee, että seuraava komento tehdään jokaisen määritellyn tiedoston kohdalla. ’/c:n’ jälkeen määritetään, että Windows aukaisee komentorivin sekä poistaa kyseisessä polussa olevan tiedoston.

Kun komentoa kokeiltiin varmuuskopiointipalvelimella Zyxel-palomuurilaitteen konfiguraatioiden poistoon, ilmeni ongelmia. Selvisi, että forfiles-komento tarkistaa tiedostojen iän niiden viimeksi muokattu -päivämäärän perusteella. Kun WinSCP:llä haettiin konfiguraatiot, ainoastaan tiedostojen luotu-päivämäärä muuttui varmuuskopiointipäivämääräksi. Vastaavasti viimeksi muokattu -päivä pysyi sinä samana, jolloin laitteen konfiguraatiota on muokattu. Koska tiedostot,

jotka haettiin laitteesta, olivat aina saman ikäisiä niiden viimeksi muokattu -päivämäärän perusteella, tuhosi forfiles automaattisesti kaikki konfiguraatiot kansioista.

Ratkaisuna tähän oli kaksi vaihtoehtoa: piti joko etsiä toinen komento, jolla saisi tiedostot poistettua tai muokata skriptillä tiedostojen päivämäärämuuttujia. Selvittelytyön jälkeen huomattiin, ettei vastaavia yksinkertaisia komentoja ole tiedostojen poistamiselle niiden luotu-päivämäärän perusteella batch-tiedostoissa. Useat vaihtoehdot esittivät kohtuullisen pitkiä VBScript-skriptejä, joiden avulla luotiin ympäristömuuttujia ja suoritettiin laskutoimintoja niiden ja päivämäärien kanssa.

Löysimme korvaavan vaihtoehdon poistamiselle. Vastaus löytyi kuitenkin Windowsin Powershellistä. Powershell on Windowsiin rakennettu koodikieli, joka on kohtuullisen hyvä alusta yksinkertaiselle ja monimutkaisellekin skriptaukselle. Poweshell käyttää hyödyksi '.Net Frameworkia', jonka avulla hallitaan Windowsin toimintoja ja objekteja. Se toimii tekstipohjaisena komentorivi-ikkunana, jonka avulla suoritetaan cmdlet-toimintoja. Näiden toimintojen/komentojen avulla kirjoitetaan esimerkiksi skriptejä ja pieniä ohjelmia.

Löydetty koodinpätkä ei sisällä mitään tiettyä komentoa, vaan koostuu yhdistelmästä eri komentoja. Poisto tapahtuu siten, että Remove-Item-komento tuhoaa tiedoston, mikäli tietyt koodissa määritetyt ehdot täyttyvät. Tässä tapauksessa 'tuhoaminen' tarkoittaa, että tiedosto ei mene roskakoriin, vaan deletoidaan kokonaan järjestelmästä. Testien aikana haluttiin kokeilla, onko tiedostot silti palautettavissa. Selvisi, että suurin osa (85%) tiedostoista oli korruptoituneita, eikä niitä voitu palauttaa enää kovalevyltä luettavaan muotoon ainakaan ilmaisohjelmalla (Piriform Recuva, Easeus Data Recovery System). Powershelliin tehdyssä poistokoodissa verrataan tämänhetkistä päivää ja tiedostojen luotupäivää, vertauksen perusteella päätetään, poistetaanko kyseinen tiedosto [41]:

*Get-ChildItem –Path "C:\Backups" –include *.log, *.conf –Recurse | Where-Object{$_.CreationTime –lt (Get-Date).AddDays(-X)} | Remove-Item*

Koodissa ‘Get-ChildItem’ hakee määritellyssä polussa (-Path) olevat tiedostot. ’-include’ komennolla määritetään mitkä tiedostotyypit halutaan poistaa. ’Recurse-komento’ määrittää, että objektit haetaan kyseisestä polusta ja sen kaikista alikansioista. Seuraavaksi verrataan ’-lt-syntaksilla’ (less than) ’CreationTime-ominaisuutta’ (luotu-päivämäärä) ’Get-Date-ominaisuuden’ (nykyinen päivä) kanssa. Tässä siis lasketaan kuinka monta päivää on niiden välissä. Tuloksesta vähennetään seuraavaksi x päivää. Tiedostot, joiden päivämäärien vähennyksen tulokseksi jää 1 tai enemmän, poistetaan.

Seuraava vaihe tiedostonpoistossa on tehdä sille batch komento Powershell-skriptin käynnistämiseksi, koska halutaan ajastaa ainoastaan yksi tiedosto käynnistyväksi varmuuskopiointipalvelimella. Tällöin batch-komento tulee varmuuskopiointiskriptin perään, kuten aiemmin mainittu forfiles-komentokin [42]:

PowerShell.exe -Command "& {Start-Process PowerShell.exe -ArgumentList '-ExecutionPolicy Bypass -File ""%~dpn0.ps1""" -Verb RunAs}"

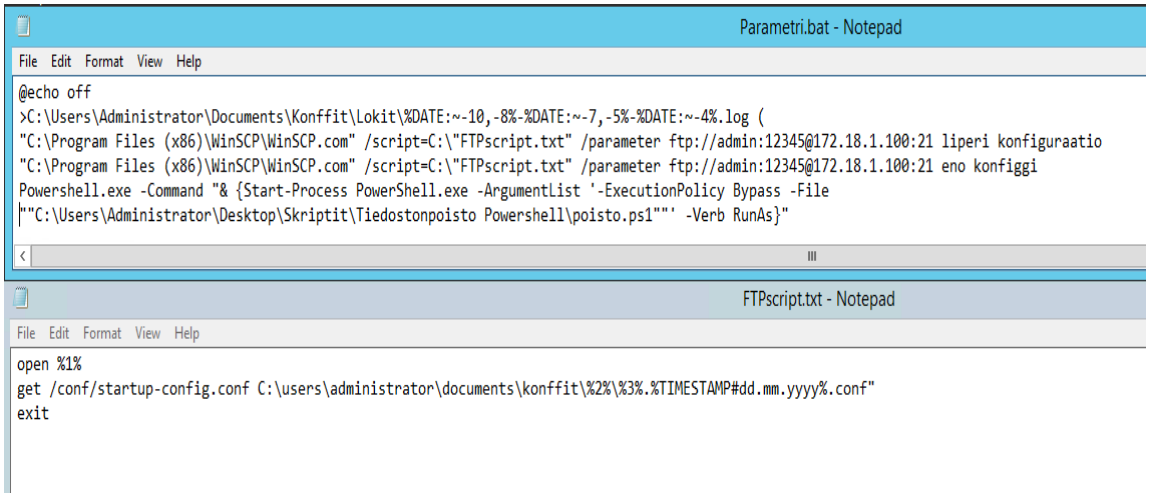
Tässä komennossa ‘PowerShell.exe -toiminto’ käynnistää Powershell-ohjelman tietyillä parametreillä. Command-komento kertoo, että Powershellin pitää suorittaa seuraava tiedosto. Toinen ’Start-Process Powershell.exe’ ohjeistaa Powershellin käynnistämään Start-Prosessi, joka käynnistää skriptin. Start-Prosessia tarvitaan avaamaan skripti admin-oikeuksin. ’Argumentlist’ ohjeistaa, millä ominaisuuksilla Start-Prosessi käynnistetään (useampi kuin yksi ominaisuus). ’ExecutionPolicy Bypass’ ohittaa kiellon suorittaa Powershell skriptejä mm. automaattisesti. Viimeisenä ’Verb RunAs -määritelmä’ laittaa Start-Prosessin käynnistämään valitun ohjelman tai skriptin järjestelmänhallinnoitsijan oikeuksilla.

6 Tulokset

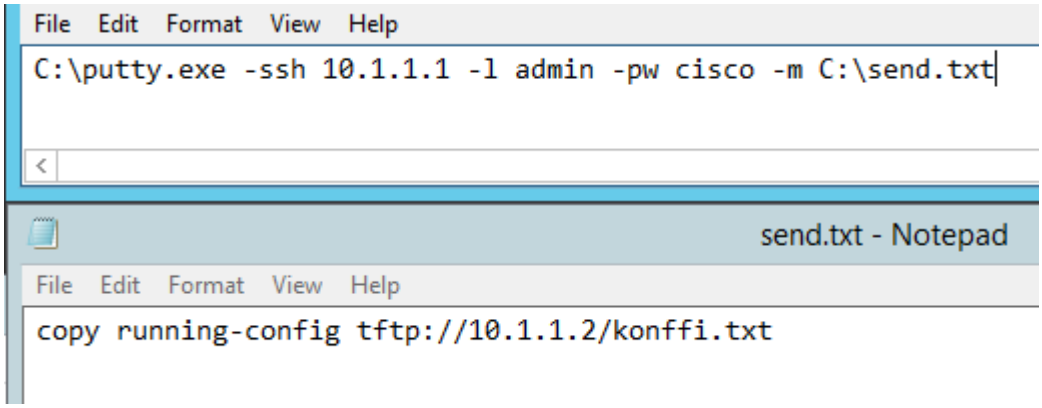
Tulokseksi saatiin kaksi toimivaa ratkaisua varmuuskopioida Bittigurun ja sen asiakkaiden verkkolaitteet. Opinnäytetyön tilaaja oli tyytyväinen tarjoamaamme ratkaisuun. Tilaaja ehdotti myös vastaavan ratkaisun tutkimista Linuxilla, mutta

päätimme rajata sen pois, koska meillä oli jo valmis ratkaisumalli Windowsille. Ratkaisuja oli kaksi, koska eri laiteet tukevat erilaisia protokollia.

Ensimmäinen ratkaisumalli käyttää hyväksi verkkolaitteen FTP-server ominaisuutta, jolloin laitteesta varmuuskopioidaan konfiguraatio FTP-client ohjelmiston avulla (Kuva 45). Toinen ratkaisu toimii siten, että laitteeseen muodostetaan SSH-yhteys ja syötetään TFTP-komennot, jolloin laite ottaa yhteyttä varmuuskopiointipalvelimen TFTP-serverille (Kuva 46). Nämä ratkaisut voidaan helposti yhdistää, koska molemmat toimivat batch-tiedoston avulla.



Kuva 45. Valmis FTP-skripti



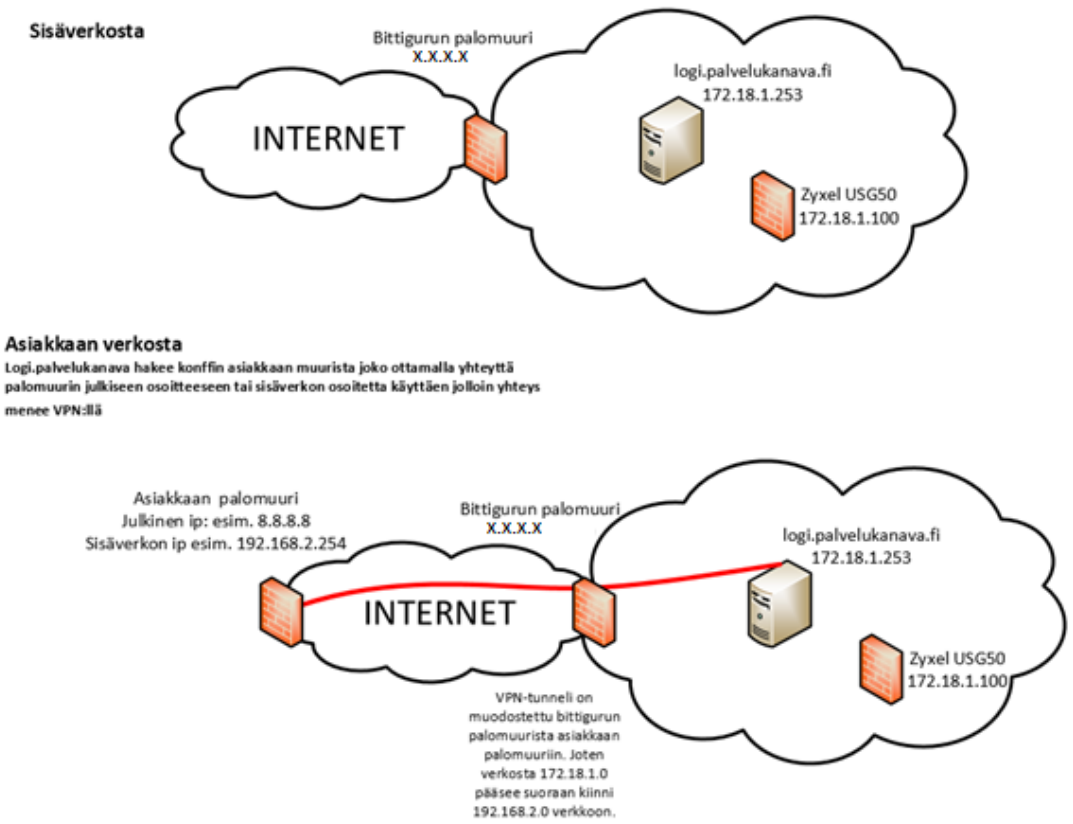
Kuva 46. Valmis TFTP-skripti

Ratkaisun yhteyteen lisättiin tiedostonpoisto- ja lokiominaisuus. Tiedostonpoisto-ominaisuudella pyrittiin säilyttämään kerrallaan seitsemän konfiguraatio- ja

lokitiedostoa. Tällöin vältytään tiedostonpaljoudelta ja varmuuskopiointiarkisto pysyy kohtuullisen siistinä. Tiedostonpoistossa käytetään Powershell-skriptiä, jossa poistetaan jokainen määritetty tiedostotyyppi tietyssä polussa, joka on vanhempi kuin seitsemän päivää. Lokien avulla voidaan tarkistaa, onko varmuuskopiointi suoritettu onnistuneesti. Lokitiedostoon menee kaikki varmuuskopiointiskriptin ajon aikana komentoriville (cmd.exe) tuleva tuloste.

Ratkaisun lopullinen toteuttaminen ja käyttöönotto jäävät Bittigurun vastuulle, kuten opinnäytetyösuunnitelmassa määriteltiin. Toteuttamisen osana on mm. yhteys varmuuskopioitaviin laitteisiin. Suositeltavaa olisi, että yhteysprotokollana käytetään jo olemassa olevaa VPN-infrastruktuuria SSH-tunneloinnin sijaan. Sen lisäksi, että VPN on jo valmiina, se on vakaampi ja helpompi ottaa käyttöön.

Ainoastaan FTP-server/client ratkaisua testattiin Bittigurun omalla virtuaalipalvelimella. FTP-client ohjelmana käytettiin WinSCP:tä, joka tarjosi kattavan tuen batch-tiedostojen käyttöön. Bittigurun testiverkossa (172.18.1.0 /24) oli kaksi laitetta – varmuuskopiointipalvelin (172.18.1.253) sekä Zyxel-palomuurilaite (Kuva 47). Tulevaisuudessa varmuuskopiointiskripteihin lisätään laitteiden sisäverkkojen IP-osoitteet, sillä VPN ymmärtää ne automaattisesti.



Kuva 47. Bittigurun testiverkko

7 Pohdinta

Opinnäytetyöprojektin alussa haluttiin ensisijaisesti turvautua Windows-pohjaisiin ratkaisuihin. Ajattelimme, että Windowsille löytyisi enemmän käyttäjäystävällisempiä varmuuskopiointijärjestelmiä kuin Linuxille. Suunnitelmassa esitettiin, että etsittäisiin reilusti erilaisia varmuuskopiointiohjelmistoja, mutta niitä etsiessä opinnäytetyön tilaajan täyttämiä kriteerejä ei löytynyt useimmista ohjelmistoista. Lähestulkoon 85 % ohjelmistoista oli maksullisia ja niiden kapasiteetti ei riittänyt täyttämään haluttua laitemäärää. Useat henkilöt olivat keskustelupalstojen mukaan turvautuneet automatisoituihin Linux varmuuskopiointiskripteihin.

Aloimme varhaisessa vaiheessa työn suunnittelua miettiä, että olisi järkevämpi turvautua Linux-pohjaisiin ratkaisuihin. Näiden ratkaisujen tutkimisessa olisi mennyt paljon enemmän aikaa kuin suunniteltiin, sillä emme ole tutustuneet Linux-skriptaukseen ja halusimme tutustua mahdollisimman moneen ratkaisuun. Yksi Linux-pohjainen ratkaisu oli ohjelma nimeltä Rancid, jolla pystyttiin saamaan statustietoa verkkolaitteilta ja varmuuskopioimaan niitä. Suurin haitta Rancidissa oli se, että sen asennus oli todella monimutkainen ja vaikea. Vaikka meillä on kohtuulisesti kokemusta erilaisten ohjelmien asennuksesta Linuxille, emme onnistuneet asentamaan Rancidia.

Jos yrityksellä olisi hallittavanaan vain esimerkiksi Ciscon ja HP:n verkkolaitteita, järkevintä olisi ottaa käyttöön Spiceworks. Spiceworksillä pystytään automatisoimaan samat asiat kuin Rancidillä, mutta käyttöönotto on paljon helpompaa. Suurin työ Spiceworksissä on konfiguroida verkkolaiteet sekä SSHv2:lla ja sallia SNMP-ominaisuudet. Spiceworks voidaan asettaa lähettämään varmuuskopiot ja järjestelmävirhetiedot sähköpostitse, mikäli niin halutaan. Suurin syy, miksi Spiceworksiä ei otettu käyttöön on, että se tukee vain TFTP-protokollaa verkkolaitteiden konfiguraatioiden varmuuskopioinnissa. Spiceworksin sivuilla luvataan mahdollistaa varmuuskopioinnin tuki myös muille verkkolaitteille, kunhan ne tukevat TFTP:tä.

Suurin ongelma kehittämässämme varmuuskopiointijärjestelmässä on, että yhteen skriptiin joudutaan yhdistämään useita eri protokollia. Tällöin pitää luoda monia eri laitekohtaisia skriptitiedostoja, jota batch-tiedostolla suoritetaan. Lisäksi tiedostonpoistoa ei voitu lisätä samaan lokitiedostoon konfiguraatioiden kanssa, koska poisto tapahtui Powershellissä. Myöskin TFTP-ratkaisussa pitää ottaa huomioon, että tiedostoja ei voida nimetä eri parametrien avulla, vaan yksittäisten tiedostojen nimeämisestä vastaa TFTP-server-ohjelmisto. Tämän lisäksi batch-tiedostoon pitää luoda erillinen tiedostonpoistokomento, jolla viitataan TFTP-serverin tallennussijaintiin. Toisena vaihtoehtona on vaihtaa sijainti samaan polkuun, jonne FTP:n avulla siirretyt tiedostot menevät.

Opinnäytetyön tilaaja pyysi tarkastelemaan SSH:n ja VPN:n eroja ja sitä kumpi kannattaa ottaa järjestelmässä käyttöön. Jos VPN-infrastruktuuria ei olisi val-

miina, voisi yritys harkita helpommin konfiguroitavaa SSH:ta. Koska Bittiguru on pilvipalveluja tarjoava yritys, jolla on paljon asiakkaita, on VPN selkein ja oikeastaan ainoa varteenotettava vaihtoehto. SSH:ta käytettäessä jouduttaisiin tunneloimaan jokainen etäyhteys yritysten sisäverkkoon, jolloin käyttöönotto vie suhteessa enemmän aikaa.

Lähteet

1. Reynolds, J. & Postel, J. File Transfer Protocol (FTP). IETF. 1985. https://tools.ietf.org/html/rfc959. 2.3.2016.
2. Forouzan. B.A. TCP/IP: Protocol Suite (4th ed.). Tata McGraw-Hill Pub lishing Company Limited. Yhdysvallat, New York. 2010.
3. Deskshare Inc. Understanding How FTP Works. 2016. http://www.deskshare.com/resources/articles/ftp-how-to.aspx. 2.3.2016.
4. Sollins, K. The TFTP Protocol (Revision 2). IETF. 1992. https://tools.ietf.org/html/rfc1350. 7.3.2016.
5. Egli, P.R. Trivial File Transfer Protocol. Indigoo.com. 2015. http://www.indigoo.com/dox/itdp/07_FTP-TFTP/TFTP.pdf. 7.3.2016.
6. Ylonen, T. The Secure Shell (SSH) Protocol Architecture. IETF. 2006. https://tools.ietf.org/html/rfc4251. 25.2.2016.
7. SSH Communications Security. About SSH Communications. 2016. http://www.ssh.com/about. 25.2.2016.
8. Ylonen, T. The Secure Shell (SSH) Authentication Protocol. 2006. https://tools.ietf.org/html/rfc4252 25.2.2016.
9. Pillai, S. Secure Shell: How Does SSH Work. Slashroot.in. 2013. http://www.slashroot.in/secure-shell-how-does-ssh-work. 26.2.2016.
10. Ellingwood, J. Understanding the SSH Encryption and Connection Process. DigitalOcean Inc. 2014. https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process. 26.2.2016.
11. Mueller, J.P. Windows Command Line Administration Instant Reference. Sybex. 2010.
12. Miller, M.A. Internet technology handbook – optimizing the Ip network. John Wiley & Sons Inc. Yhdysvallat, New Jersey. 2004.
13. Ellingwood, J. An Introduction to SNMP (Simple Network Management Protocol). DigitalOcean Inc. 2014. https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol. 6.3.2016.
14. ManageEngine. SNMP tutorial. 2016. https://www.manageengine.com/network-monitoring/what-is-snmp.html. 10.3.2016.
15. Held, G. Virtual Private Networking: A Construction, Operation and Utilization Guide. John Wiley & Sons Inc. Yhdysvallat, New Jersey. 2005.
16. Techopedia. Permanent Virtual Circuit (PVC). 2016. https://www.techopedia.com/definition/8841/permanent-virtual-circuit-pvc. 5.3.2016.

17. TechTarget. Full, incremental or differential: How to choose the correct backup type. 2008. http://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type. 6.3.2016.
18. Preece, J. Server Backup Software Reviews. TopTenReviews.com. 2016. http://server-backup-software-review.toptenreviews.com/. 23.1.2016.
19. Hoffman, C. VPN vs. SSH Tunnel: Which Is More Secure?. How-To Geek.com. 2012 .http://www.howtogeek.com/118145/vpn-vs.-ssh-tunnel-which-is-more-secure/. 7.3.2016.
20. Cbshieldheritage. How Vpn Works. 2012. http://cbshieldheritage.com/category/vpn/ 7.3.2016.
21. Hill. R. Getting started with SSH security and configuration. 2014. http://www.ibm.com/developerworks/aix/library/au-sshsecurity/. 7.3.2016
22. BlackWaspTM. Salted Password Hashing. 2011. http://www.blackwasp.co.uk/SaltedPasswordHashing.aspx. 23.2.2016.
23. CODE42 Inc. Archive Encryption Key Security. 2016. http://support.code42.com/CrashPlan/4/Configuring/Archive_Encryption_Key_Security. 23.2.2016.
24. Schneier, B. The Blowfish Encryption Algorithm. 2016. https://www.schneier.com/cryptography/blowfish/. 4.3.2016.
25. Solarwinds Inc. Kiwi CatTools. 2016. www.kiwicattools.com/downloads/cattools/CatTools.pdf. 16.2.2016.
26. WinAgents Software Group. WinAgents HyperConf. 2016. http://www.winagents.com/en/products/hyperconf. 18.2.2016.
27. Prikyl, M. Free FTP Client for Windows. 2016. https://winscp.net/eng/docs/free_ftp_client_for_windows#what_is_ftp_client. 26.2.2016.
28. Shrubbery networks Inc. RANCID – Really Awesome New Cisco config Differ. 2014. http://www.shrubbery.net/rancid/. 8.2.2016.
29. Ogenstad, P. Getting started with RANCID. 2014. https://networklore.com/rancid-getting-started/. 8.2.2016.
30. Spiceworks. Spiceworks Requirements. 2016. https://community.spiceworks.com/help/Spiceworks_Requirements. 2.2.2016.
31. Spiceworks. Spiceworks Inventory. 2016. https://community.spiceworks.com/help/Spiceworks_Inventory. 2.2.2016.
32. Spiceworks. Spiceworks Configuration Management. 2016. https://community.spiceworks.com/help/Network_Configuration_Management. 4.2.2016.
33. Cisco Systems Inc. Configuring Secure Shell on Routers and Switches Running Cisco IOS. 2007. http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html. 3.2.2016.

34. Cisco Systems Inc. Working with the Cisco IOS File System, Configuration Files, and Software Images. 2016. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_58_se/configuration/guide/2960scg/swiosfs.html#wp1257792. 3.2.2016.
35. Mortensen, P. How to run a command file in PUTTY using automatic login in a command prompt? 2013. http://superuser.com/questions/515601/how-to-run-a-command-file-in-putty-using-automatic-login-in-a-command-prompt. 27.2.2016.
36. Prikyl, M. Automate file transfers (or synchronization) to FTP server or SFTP server. 2016. https://winscp.net/eng/docs/guide_automation. 25.2.2016.
37. Viestintävirasto. [Teema] Loki on ylläpidon tärkein turvallisuustyökalu. 2015. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603091742.html. 14.3.2016.
38. Viestintävirasto. [Teema] Lokitiedot tietoturvallisuuden tukena. 2016. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603040919.html. 14.3.2016.
39. Dbenham. Redirecting Output from within Batch file. 2013. http://stackoverflow.com/questions/20484151/redirecting-output-from-within-batch-file. 3.3.2016.
40. Opello. Creating a file name as a timestamp in a batch job. 2009. http://stackoverflow.com/questions/1064557/creating-a-file-name-as-a-timestamp-in-a-batch-job. 3.3.2016.
41. Gibb, T. How to Delete Files Older than X Days on Windows. 2012. http://www.howtogeek.com/131881/how-to-delete-files-older-than-x-days-on-windows/. 26.2.2016.
42. Zinicola, J. How to Use a Batch File to Make PowerShell Scripts Easier to Run. 2014. http://www.howtogeek.com/204088/how-to-use-a-batch-file-to-make-powershell-scripts-easier-to-run/. 26.2.2016.