Iikka Jaakkola

Virtuaalikone ja -verkkoympäristön hyödyntäminen tietoverkkotekniikan tutkimus- ja opetusympäristöjen rakentamisessa

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 10.5.2010

Työn valvoja:

Prof. Jukka Manner

Työn ohjaaja:

TkL Markus Peuhkuri

Aalto-yliopisto
Teknillinen korkeakoulu

AALTO-YLIOPISTO DIPLOMITYÖN
TEKNILLINEN KORKEAKOULU TIIVISTELMÄ

Tekijä: Iikka Jaakkola

Työn nimi: Virtuaalikone ja -verkkoympäristön hyödyntäminen tietoverkkotekniikan tutkimus- ja opetusympäristöjen rakentamisessa

Päivämäärä: 10.5.2010 Kieli: suomi Sivumäärä:55+26

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkot Koodi: S-38

Valvoja: Prof. Jukka Manner

Ohjaaja: TkL Markus Peuhkuri

Työn tavoitteena oli selvittää virtuaalisen tutkimusverkkoyhteyden tarvetta, vaatimuksia ja toteutuskelpoista tuomista tutkijoiden ja muiden tahojen, kuten opiskelijoiden, käyttöön. Virtuaalinen ympäristö oli tarkoitus rakentaa maksutta saatavilla olevien virtuaalikone- ja VPN-asiakasyhteysohjelmistojen varaan ja sen tulisi olla mahdollista asentaa tutkijoiden keskitetysti hallittuihin työasemiin. Lisäksi tutkittiin ratkaisun käyttökohteita, joista tärkeimpänä oli testiverkkoihin yhdistäminen. Ratkaisulle asetettavia vaatimuksia selvitettiin tietoturvapolitiikan, loppukäyttäjien, tietojärjestelmien ylläpidon ja laitteistovaatimusten kannalta. Käyttäjien ja ylläpidon näkemyksiä kyseltiin haastatteluin ja kyselyin.

Työn tuloksena saatiin VirtualBox-virtualisointiohjelman ja OpenVPN-ohjelmiston muodostama kokonaisuus, joka mahdollistaa läpinäkyvän VPN-yhteyden ja rajoittamattomat käyttöoikeudet virtuaalikoneen sisällä. Ratkaisu täyttää sille asetetut tavoitteet ja vaatimukset melko hyvin, huonona puolena on sen suorituskyky verrattuna isäntäjärjestelmään.

Avainsanat: virtuaalikone, VPN, testiverkko, VirtualBox, OpenVPN

AALTO UNIVERSITY
SCHOOL OF SCIENCE AND TECHNOLOGY

ABSTRACT OF THE
MASTER'S THESIS

Author: Iikka Jaakkola

Title: Improving Networking Technology Research and Teaching Environment by Utilizing Virtual Machine and Virtual Network Environment

Date: 10.5.2010 Language: Finnish Number of pages: 55+26

Faculty of Electronics, Communications and Automation

Department of Communications and Networking

Professorship: Networking Technology Code: S-38

Supervisor: Prof. Jukka Manner

Instructor: L.Sc. Markus Peuhkuri

The objective of this thesis was to study the need for virtual research network connection and requirements for bringing an implementation to researchers and other parties, such as students. Virtual environment was intended to be built upon virtual machine and VPN client software that are available free of charge. This environment should be possible to install to workstations by centralized management system. In addition, other applications for the solution was studied, the most important application is connecting to testbed networks. The requirements for the solution were studied from the viewpoint of security policy, end users, IT administration and hardware. The views of the end users and administrators were studied by a questionnaire and interviews.

The result of this thesis is the combination of VirtualBox virtualization software and OpenVPN software. It enables a transparent VPN connection to a virtual machine, for which the user has unrestricted administration level user rights. The solution fulfills the requirements fairly well, the weak point is its performance compared to the host system.

Keywords: virtual machine, VPN, network testbed, VirtualBox, OpenVPN

Esipuhe

Haluan kiittää äitiäni Saaraa, työn ohjaajaa Markus Peuhkuria ja työn valvojaa professori Jukka Mannerta tuesta ja kommenteista.

Erityiskiitos kaikille Comnetin IRC-kanavan keskustelijoille.

Otaniemi, 7.5.2010

Iikka Jaakkola

Sisällysluettelo

Lyhenteet

AES	Advanced Encryption Standard, eräs lohkosalausmenetelmä
API	Application Programming Interface, ohjelmointirajapinta
DHCP	Dynamic Host Configuration Protocol, protokolla, jonka tehtävä on jakaa IP-osoitteita lähiverkkoon kytketyille koneille
FPS	Frames Per Second, kuvaa sekunnissa
GNU GPL	GNU General Public License, vapaasti muokattavissa ja levitettävissä oleva ohjelmisto
GPU	Graphics Processing Unit, grafiikkasuoritin
H.264	Videopakkausstandardi, tunnetaan myös nimellä MPEG-4 Advanced Video Coding (AVC)
HD	High Definition, teräväpiirto
HTTP	Hypertext Transport / Transfer Protocol, hypertekstin (web-sivu) sovelluskerroksen siirtokäytäntö
I/O	Input/Output, tietokonelaitteiston signalointi sisäisten tai ulkoisten laitteiden kanssa
ICT	Information and Communication Technology, tieto- ja viestintätekniikka
IDEA	International Data Encryption Algorithm, eräs lohkosalausmenetelmä
IETF	Internet Engineering Task Force, Internet-protokollien standardoinnista vastaava organisaatio
IP	Internet Protocol, Internetin yhteyskäytäntö
IPTV	Internet Protocol television, verkon yli välitettävä televisiosignaali
IT	Information Technology, tietotekniikka
ITU-T	International Telecommunication Union Standardization Sector, YK:n alainen televiestintäverkkoja ja -palveluja kansainvälisesti koordinoiva järjestö
L2	Layer 2, OSI-mallin toinen kerros eli siirtoyhteyskerros
L3	Layer 3, OSI-mallin kolmas kerros eli verkkokerros
MAC-osoite	Media Access Control address, verkkoliitännän yksilöivä L2-osoite
NAT	Network Address Translation, osoitteenmuunnos
OSE	Open Source Edition, VirtualBoxin avoimen lähdekoodin versio
OSI-malli	Open System Interconnection Reference Model, tiedonsiirtoprotokollien seitsenkerroksinen referenssimalli
P2P	Peer to Peer, vertaisverkko / hajautettu verkkoarkkitehtuuri
RAM	Random access memory, tietokoneen keskusmuisti
RFC	Request for Comments, IETF:n Internetin protokollia koskeva dokumentti, joka voi

	olla esimerkiksi standardi, ehdotus standardiksi tai tutkimus
RSA	Rivest, Shamir ja Adleman kehittämä epäsymmetrinen julkisen avaimen salausalgoritmi
SHA	Secure Hash Algorithm, eräs kryptografinen tiivistefunktio
SHOK	Strategisen huippuosaamisen keskittymä
SSH	Secure Shell, julkisen avaimen salauksella suojattu sovelluskerroksen yhteyskäytäntö
SSL	Secure Socket Layer, salausprotokolla, nykyisin TLS
TAP	Network tap, virtuaalinen L2-verkkosovitin
TCP	Transmission Control Protocol, yhteydellinen IP-verkon yhteyskäytäntö Internetissä
TLS	Transport Layer Security, salausprotokolla, ennen SSL
TUN	Network TUNnel, virtuaalinen L3-verkkosovitin
TXT	Trusted Execution Technology, Intelin prosessoreihin toteuttama rautapohjainen turvallisuuslaajennus, jonka on tarkoitus estää haitallisten ohjelmien suoritus
UDP	User Datagram Protocol, yhteydetön IP-verkon yhteyskäytäntö Internetissä
USB	Universal Serial Bus, tietokoneen sarjaväylästandardi
VAHTI	Valtiovarainministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä
VM	virtual machine, virtuaalikone
VoIP	Voice over IP, IP-puhe, yleistermi puheenvälitykselle IP-verkossa
VPN	Virtual private network, virtuaalinen erillisverkko
X.509	ITU-T standardi, joka on osa julkisen avaimen järjestelmää, ja määrittelee varmenteet ja niiden hallinnoimisen
x264	x264 on H.264/MPEG-4 AVC-profiilin videokoodekki
x86	Intelin käskykanta/mikroprosessoriarkkitehtuuri
Xvid	Xvid on MPEG-4 Advanced Simple Profile (ASP) -profiilin videokoodekki

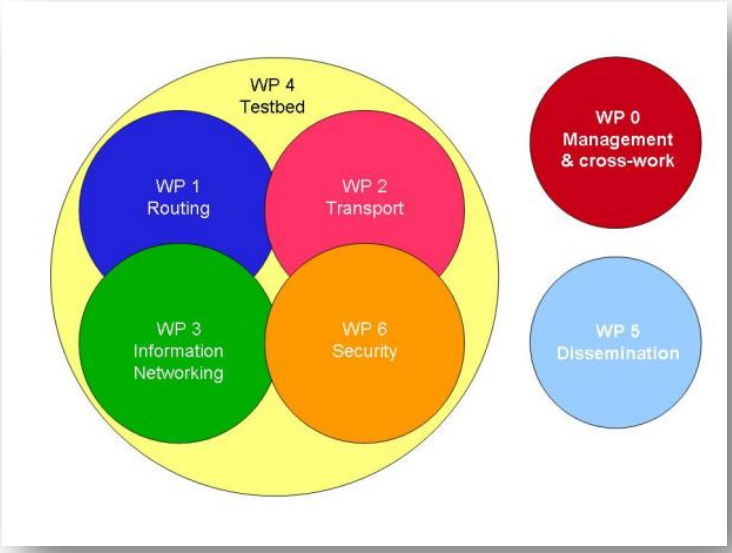
Sanasto

Eheys	Tietoturvan yhteydessä tiedon oikeellisuus siinä mielessä, että viestittyä tai talletettua tietoa ei ole muutettu sen jälkeen, kun tiedon todennettu luoja on sitä viimeksi käsitellyt
Luottamuksellisuus	Viestit eivät ole muiden kuin todennettujen osapuolien luettavissa
Salaus	Viestin salaaminen siten, että sen haltuunsa saava ulkopuolinen ei kykene sitä avaamaan
Todennus	Käyttäjän (tai palvelun) identiteetti varmennetaan

1 Johdanto

Tietoverkot ja Internet ovat tulleet erottamattomaksi osaksi yhteiskuntaa viimeistään 2000-luvun alussa. Internet ei ole kuitenkaan valmis vaan uusia verkkopalveluja ja -protokollia kehitetään jatkuvasti. Niitä ei useinkaan voida suoraan testata tai ottaa käyttöön julkisissa verkoissa, vaan ne on syytä testata suljetussa ja hallittavissa olevassa järjestelmässä. Tällaisia verkkoja kutsutaan testiverkoiksi (testbed). Eräs tällainen testiverkko on PlanetLab, joka on yksi suurimmista maailmanlaajuisista Internetin päällä toimivista tutkimusverkoista. (PlanetLab Consortium, 2010)

Tämä työ on tehty osana Suomen strategisen huippuosaamisen tietotekniikan alueen keskittymä ICT SHOK:in Tulevaisuuden Internet -hankkeen neljättä työpakettia, testiverkkoprojektia (Future Internet WP4 testbed). Kuvassa 1 esitetään yhteys hankkeen muihin työpaketteihin. Projektin tehtävä on rakentaa kansallinen testiverkko ja tuoda siihen palveluja, joita tutkijat ja yhteistyökumppanit voivat hyödyntää omassa toiminnassaan. Testiverkon arkkitehtuuri on jo päätetty, mikä täytyy ottaa huomioon tässä työssä. Projektiin osallistuu Tieteen tietotekniikan keskus (CSC), Aalto-yliopiston teknillinen korkeakoulu, Tampereen teknillinen yliopisto (TTY) ja Tietotekniikan tutkimuslaitos (HIIT). (Huhtanen & Savola, 2009)

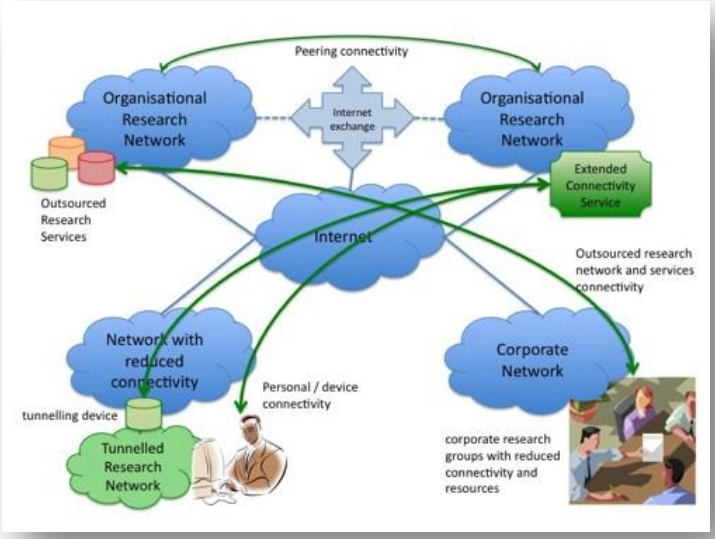


Kuva 1: Tulevaisuuden Internet -hankkeen työpaketit

1.1 Ongelmakuvaus

Harvemman tutkijan työpisteeseen tulee suoraa verkkojohtoa tutkimusverkkoon[1], joten siihen pitää muodostaa yhteys käyttäen saatavilla olevaa toimistoverkkoa. Usein testiverkkoyhteydeksi saattaa riittää pelkkä tekstipohjainen komentotulkkietäyhteys (SSH) tai webpohjainen ympäristö, mutta esimerkiksi multimediapalvelut vaativat suorempaa yhteyttä.

Organisaation tietohallinto haluaa pääsääntöisesti suojata verkkonsa ulkopuolisia ja sisäisiä uhkia vastaan palomuurein tai vastaavin toimin. Tällöin useimmat sovellukset ovat estetty ja esimerkiksi ryhmälähetys (*multicast*), IPv6, vertaisverkko (P2P) ja vastaavat harvinaisemmat palvelut eivät toimi. Tutkijalle näiden palveluiden toimivuus on kuitenkin tärkeää. Myös testiverkot ovat vastaavalla tavalla suojattuja ulkopuolisilta, joten ongelmaksi muodostuu yhteyden muodostaminen näiden kahden verkon, toimistoverkon ja testiverkon, välille siten, että kaikki verkkoprotokollat toimisivat. Ratkaisun tähän tarjoaa virtuaalinen[2] yksityisverkko (*Virtual Private Network, VPN*), joka on de facto -tapa muodostaa suojattu yksityinen verkko yli epäluotetun verkon, kuten Internet. Kuvassa 2 esitetään Tulevaisuuden Internet -testiverkon IP-liitettävyysarkkitehtuuri. VPN tarjoaa niin sanotusti laajennetun liitettävyyden palvelun (*Extended Connectivity Service*) rajoitetun liitettävyyden verkossa.



Kuva 2: Tulevaisuuden Internet testiverkon yleinen IP-liitettävyysarkkitehtuuri, rajoitetun liitettävyden verkoista yhdistetään käyttäen tunneloituja ratkaisuja

[1] Tietoverkkotutkijoille voi tullakin, mutta verkkopalvelujen monipuolistuessa myös monet muut tutkijat saattavat haluta yhteyden testiverkkoihin.
[2] Virtuaalinen, koska verkon koneiden välillä ei ole (välttämättä) suoraa fyysistä yhteyttä

Toinen läheisesti asiaan liittyvä ongelma on, että käyttäjät eivät yleensä saa asentaa työasemiin vapaasti ohjelmia, muuttaa asetuksia tai jopa vaihtaa käyttöjärjestelmää, koska muuten työasemien keskitetysti hallittu ylläpito ja tietoturvasta varmistuminen tulee mahdottomaksi. Kenties tavallisin tapa ratkaista tämä on tuoda työaseman rinnalle toinen kone, jolla käyttäjä saa vapaasti tehdä mitä haluaa. Tämän toisen koneen liittäminen toimistoverkkoon tai Internetiin saattaa kuitenkin olla kiellettyä, johtuen tietoturvapolitiikasta ja haittaohjelmien leviämisen pelosta.

Eräs ratkaisu tähän ongelmaan on virtuaalikoneiden käyttö työasemassa, jolloin hallittu ylläpito on mahdollista, mutta käyttäjällä on kuitenkin mahdollisuus omiin kokeiluihin. Toinen ratkaisu olisi etätyöpöytäyhteys koneeseen, joka on suorassa yhteydessä testiverkkoon. Jälkimmäisen ratkaisun ongelmana lienee video ja muun mediamateriaalin käsittely etäyhteyden yli, mutta toisaalta verkkoyhteyden vaatimukset ovat pienemmät jos kyseessä on erittäin paljon verkkoliikennettä tuottava sovellus. Tässä työssä keskitytään enemmän ensinnä mainittuun ratkaisuun, mutta myös jälkimmäinen ratkaisu otetaan huomioon.

Tämän työn tavoitteena on selvittää virtuaalisen tutkimus-/testiverkkoyhteyden tarvetta, vaatimuksia ja toteutuskelpoista tuomista tutkijoiden ja muiden tahojen, kuten opiskelijoiden, käyttöön heidän työ- ja henkilökohtaisille koneille. Lisäksi työn tuloksena syntyy kokonaisuus, joka voidaan hallitusti asentaa työasemiin tarpeen vaatiessa.

1.2 Työn rajaus

Työssä keskitytään virtuaalikoneen ja VPN-asiakasyhteyden yhteensovittamiseen ja tuotteistamiseen hallittavissa olevaksi paketiksi. VPN-palvelimen asennukseen tai sertifikaattien hallinnointiin ei puututa, muuten kuin yleisellä tasolla. Työssä ei ole tarkoitus kehittää mitään omaa ohjelmakomponenttia, vaan pyrkimys on käyttää parhaiten soveltuvia maksutta saatavilla olevia virtuaalikone- ja VPN-ohjelmistoa.

Loppukäyttäjien tarpeita tarkastellaan yleisellä tasolla, ratkaisun yleistä toteutettavuutta ja tarpeellisuutta ajatellen. Tarpeita selvitetään web-kyselyin ja haastatteluin tarkasti valitulta kohdeyleisöltä. Ylläpidon näkökulmaa ja tietoturvaa selvitetään haastattelemalla Aalto-yliopiston teknillisen korkeakoulun IT-infrastruktuurin ylläpitäjiä ja tietohallintoa.

1.3 Tulokset

Työn tuloksena saatiin VirtualBox-virtualisointiohjelman ja OpenVPN-ohjelmiston muodostama kokonaisuus, joka mahdollistaa yhdistämisen esimerkiksi Tulevaisuuden Internet -testiverkkoon Internetin yli ja käyttäjälleen rajoittamattomat oikeudet virtuaalikoneen sisäl-

lä. Ratkaisu täyttää sille asetetut tavoitteet ja vaatimukset melko hyvin. Ratkaisu on Aalto-yliopiston ohjelmistopolitiikan mukainen eikä sen pitäisi luoda merkittäviä turvallisuusongelmia, lisäksi ratkaisu on mahdollista asentaa ja hallita keskitetysti. Ratkaisun huonona puolena on sen suorituskyky verrattuna isäntäjärjestelmään, mutta toisaalta sitä voi käyttää muuhunkin kuin pelkkään testiverkkoon yhdistämiseen. Ratkaisun voi nähdä täydentävänä vaihtoehtona erilliselle fyysiselle koneelle ja etätyöpöytäyhteyksille.

Tutkijoille tehdyssä kyselyssä suuri osa vastaajista ilmoitti ratkaisun vaikuttavan hyödylliseltä omassa käytössään ja joillakin jo oli vastaavaa käytössä. Toisaalta, kaikki eivät nähneet tarpeelliseksi graafista työpöytää, heille riittää nykyisin käytössä oleva tekstipohjainen yhteys. Ylläpito voi hyödyntää ratkaisua vähentämään fyysisten koneiden määrää organisaatiossa ja siten helpottamaan omaa työtä.

1.4 Työn rakenne

Työ on jaettu kuuteen lukuun, ensimmäisessä eli tässä luvussa on kerrottu taustat, määritelty ratkaistava ongelma ja rajattu työ. Toisessa luvussa esitellään perustiedot virtuaalikoneista, virtuaalisista erillisverkoista, testiverkoista ja toisesta projektista liittyen VPN-palvelimen sertifikaattien hallintaan.

Työn oma osuus jakautuu kahteen osaan, kolmas luku kartoittaa ratkaisulle annettuja vaatimuksia ja hyödyllisyyttä niin loppukäyttäjän kuin ylläpitäjän näkökulmasta. Lisäksi paneudutaan mahdollisiin rajoituksiin, ongelmakohtiin ja vaihtoehtoihin liittyen käyttöön ja ylläpitoon. Neljännessä luvussa paketoidaan kyseinen palvelu siten, että se sopii käytettäväksi ja hallinnoitavaksi tavallisessa toimistoverkossa.

Viidennessä luvussa arvioidaan saavutetun ratkaisun onnistumista asetettuihin tavoitteisiin nähden ja lisäksi listataan ratkaisun edut ja rajoitukset ja verrataan sitä vaihtoehtoisiin ratkaisuihin. Viimeisessä, kuudennessa luvussa summataan työn tulokset ja pohditaan jatkotutkimuskohteita.

2 Taustat

Tässä luvussa käsitellään virtualisointia ja virtuaalisia yksityisverkkoja ja niihin liittyviä seikkoja. Ensiksi luvussa 2.1 esitellään virtualisointi, mitä sillä tarkoitetaan ja mitä hyötyä siitä on. Tämän jälkeen käsitellään järjestelmän virtualisointia, joka tarjoaa oleellisen pohjan virtuaalikoneiden toimintaperiaatteen ymmärtämiselle ja tässä työssä valittujen ratkaisuiden rakentumiseen. Lisäksi esitellään työpöydän virtualisointi, jonka voi nähdä vaihtoehtoisena ratkaisuna tässä työssä esitettyyn ratkaisuun nähden. Luvussa 2.2 esitellään virtuaalinen yksityisverkko ja muutamia yleisimpiä protokollia. Lisäksi käsitellään turvallisuusuhkia. Luvussa 2.3 kerrotaan lisäksi testiverkoista.

2.1 Virtualisointi

Virtualisointi tarkoittaa tietojenkäsittelyssä tietokoneresurssien abstrahointia eli tavallisesti joidenkin teknisten piirteiden piilottamista resurssin käyttäjältä. Käytännössä tämä tarkoittaa esimerkiksi, että fyysisessä tietokoneessa ajettava ohjelma esittää käyttäjälleen toisen, näennäisen, koneen, jota kutsutaan virtuaalikoneeksi. Toisaalta virtualisointi voi tarkoittaa tilannetta, jossa useampi fyysinen resurssi yhdistetään yhdeksi loogiseksi resurssiksi tai resurssipooliksi. Näin toimivat esimerkiksi tallennusjärjestelmät, joissa monta yksittäistä kiintolevyä näkyy yhtenä isona tallennustilana ulospäin. Toisaalta käyttöjärjestelmät käyttävät jo itsessään virtualisointia esimerkiksi muistinkäsittelyssä, sillä ne peittävät koneen fyysisen muistin määrän ja voivat tarjota sovelluksille enemmän muistia kuin koneessa itsessään on. Virtualisoinnissa on tärkeää, että virtualisoitu resurssi ei ole enää suoraan käytettävissä, vaan resurssia käytetään vain virtualisointikerroksen välityksellä. Näin lisätään järjestelmän turvallisuutta ja selkeyttä, kun käyttäjä on eristetty käyttämään vain virtualisointikerroksen palveluja. Virtualisointi voi tarkoittaa siis montaa asiaa, mutta tässä työssä sillä viitataan pääasiassa virtuaalikoneen virtualisointiin.

Virtualisoinnin mahdollistavat tekniikat, kuten laitteiston ja ohjelmiston ositus tai yhdistäminen, osittainen tai täydellinen koneen simulointi, emulointi ja aikaosituskäyttö (*time-sharing*). Virtualisointi ei ole uusi idea, sitä on käytetty jo 1960-luvulla esitellyssä IBM:n keskustietokoneessa. Palvelinkoneissa virtualisointia käytettiin, jotta kalliista laitteesta saatiin täysi hyöty jakamalla resursseja pienempiin paloihin. Siten käyttäjät pystyivät ajamaan ja kehittämään ohjelmia virtuaalikoneessa, jonka kaatuminen ei vaikuttanut koko palvelimen toimintaan. (Nanda & Chiueh, 2005)

Henkilökohtaisten tietokoneiden tultua markkinoille ja moniajomahdollisuuden myötä virtuaalikoneiden tarve oli vähäistä 1980- ja 1990-luvuilla. 1990-luvulla tapahtunut tietokoneiden ja Internetin yleistyminen ja käyttöjärjestelmien monimuotoisuus teki virtualisoin-

nin ideat taas tarpeellisiksi. VMware julkisti ensimmäisen x86-virtualisointituotteen työasemiin vuonna 1999. Nyt virtualisointi mahdollistaa usean erityyppisen koneen tai käyttöjärjestelmän yhtäaikaisen käytön, mikä on hyödyllistä esimerkiksi ohjelmistokehityksessä. (Kleidermacher, 2009)

Virtualisoinnin suurin hyöty saavutetaan kuitenkin palvelinympäristössä, jolloin koneen koko kapasiteetti hyödynnetään paremmin, mikä tuo säästöjä niin laitehankinnoissa, hallittavuudessa kuin tilantarpeessa. Yhdessä tehokkaassa fyysisessä laitteessa voidaan nyt ajaa useita sovelluksia, jotka vaativat oman eristetyn ympäristön. Lisäksi sovelluksia voidaan hallita, siirtää ja hajauttaa joustavasti fyysisillä palvelimilla kun ne toimivat virtuaaliympäristössä. Virtualisointisovellusten tarjonta on viime vuosina kehittynyt selvästi x86-suorittimien virtualisointilaajennusten ohella, ja maksuttomien sovellusten myötä myös kaupallisten tuotteiden hinnat ovat laskeneet. (van Dijk, 2008) (Gartner, Inc., 2008)

Virtualisoinnin kysyntä tulee jatkamaan vahvaa kasvua palvelin puolella pilvilaskennan (*cloud computing*) ja vanhojen palvelimien yhdistämisen (*consolidation*) yleistymisen vuoksi (Gartner, Inc., 2008). VMwaren vision mukaan virtualisoinnin kehityspolku siirtyy kulujen vähentämisestä palvelun laadun parantamiseen eli liiketoimintakriittisten palvelujen hajauttamiseen ja saatavuuden turvaamiseen (*high availability*). Seuraava askel on IT-palveluiden ketteryyden lisääminen. Kun suurin osa palveluista ja infrastruktuurista on virtualisoitu, niihin pystytään soveltamaan kehittyneitä hallintatyökaluja, jotka tuovat joustavuutta ja automatisointia rutiinitehtäviin. (Nielsen, 2010)

Työasemissa virtualisointi ei ole yhtä pitkällä kuin palvelimissa, mutta ylläpidon työmäärä ja järjestelmien monimutkaisuus ja -muotoisuus kasvaa. Tällöin virtualisointi tuo lisää turvallisuutta, joustavuutta ja hallittavuutta. (Lambert, 2008) Yrityksissä on myös paljon vanhoja sovelluksia, jotka eivät toimi uusimmissa käyttöjärjestelmissä. Tämän vuoksi tietyissä Windows 7 versioissa on mahdollisuus niin sanottuun XP-tilaan, jossa Windows XP:tä ajetaan virtuaalikoneessa. (Microsoft Corporation, 2009) Virtualisointia voi käyttää jopa pelikäytössä, sillä van Dijk oli saanut vuoden 2004 ammuskelupeli Half-Life 2:n toimimaan 3D-kiihdytetynä Windows XP virtuaalikoneessa Mac OS X:llä (van Dijk, 2008).

2.1.1 Järjestelmän virtualisointi

Järjestelmän virtualisointi (*hardware virtualization, platform virtualization*) esittää käyttäjälleen kokonaisen laitteiston, joka voi olla isäntäkoneesta riippumaton tai riippuvainen. Isäntäkoneesta riippumatonta kutsutaan täydeksi virtualisoinniksi (*full virtualization*) ja se on nykyään tavallisin tekniikka ja siihen viitataan usein, osin virheellisesti, pelkästään virtualisointina. (VMware, Inc., 2007) Tässä vaiheessa on syytä esitellä asiaankuuluvat termit (taulukko 1).

Taulukko 1: Virtualisointitermejä

Termi	Termi englanniksi	Selitys
isäntäkone	host	fyysinen kone, jossa virtualisointialustaa ajetaan
isäntäkäyttöjärjestelmä	host operating system	isäntäkoneessa ajettava käyttöjärjestelmä, jonka päällä virtualisointialustaa ajetaan
vieraskäyttöjärjestelmä	guest operating system	virtuaalikoneessa ajettava käyttöjärjestelmä
virtuaalikone, näennäiskone	virtual machine (VM)	simuloitu kone, jossa vieraskäyttöjärjestelmää ajetaan
virtuaalikonevalvoja*	virtual machine monitor (VMM)	tarjoaa vieraskäyttöjärjestelmälle virtuaalikoneen ja hallinnoi sitä
hypervisor* **(tyypin 1 VM)**	hypervisor	virtualisointikerros, jota ajetaan suoraan laitteiston päällä
isännöity **(tyypin 2 VM)**	hosted	virtualisointikerros, jota ajetaan isäntäkäyttöjärjestelmän päällä
* Määritelmät ristiriitaisia lähteestä riippuen, voivat tarkoittaa myös samaa asiaa eli virtualisointikerrosta yleisesti. Taulukossa esitetty määritelmä on VMwaren käyttämä (VMware, Inc., 2007)		

Täysi virtualisointi mahdollistaa muokkaamattomien vieraskäyttöjärjestelmien, kuten Microsoft Windows, ajamisen. Virtualisointiratkaisut ovat joko hypervisor tai isännöinti -pohjaisia. Isännöity ratkaisu tuo virtualisointikerroksen tavallisen ohjelman tapaan isäntäkäyttöjärjestelmän päälle. Etuna on isäntäkäyttöjärjestelmän laaja laitteistotuki ja helppo käyttöönotto olemassa olevassa järjestelmässä. Huonona puolena on suuri tehohäviö monissa tapauksissa. Täyden virtualisoinnin isännöityjä alustoja on saatavilla lukuisilta eri valmistajilta kaupallisina ja myös ilmaisina versioina, kuten VMware Player (VMware, Inc., 2010a), Windows Virtual PC (Microsoft Corporation, 2010a) ja VirtualBox (Sun Microsystems, Inc., 2010a).

Hypervisor-ratkaisu puolestaan asennetaan tyhjään koneeseen ikään kuin käyttöjärjestelmäksi ja tarjoaa paremman skaalautuvuuden, sitkeyden (*robustness*) ja suorituskyvyn. Siksi hypervisor ratkaisut ovat käytössä lähinnä palvelinympäristössä ja isännöidyt ratkaisut ovat enemmän työasemakäyttöön. Tämä asetelma saattaa muuttua Citrixin esiteltyä vuonna 2009 XenClient-ohjelman, josta lisää luvussa *2.1.3 Virtuaalikone-pohjainen työpöytä*.

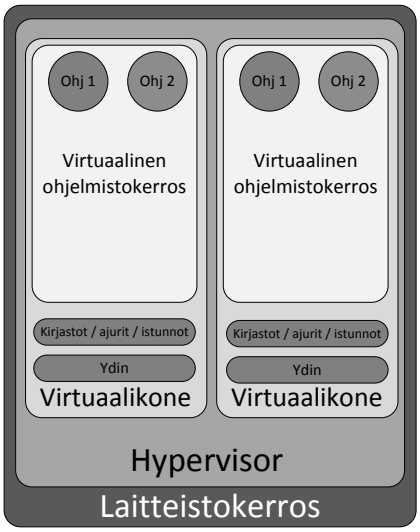
Huomionarvoista on, että täysi virtualisointi ei ollut täydellisesti mahdollista x86-arkkitehtuurilla ennen vuosia 2005 ja 2006 kun Intel että AMD toivat omat virtualisointilaajennukset prosessoreihinsa (VT-x ja AMD-V). VMwaren ratkaisu vuonna 1999 perustui konekäskyjen ajonaikaiseen binäärikäännökseen (*dynamic binary translation*) (VMware, Inc., 2007).

Isäntäkoneesta riippuvaisia virtualisointitekniikoita ovat osittainen, para- ja käyttöjärjestelmätason virtualisointi. Osittainen virtualisointi tarkoittaa nimensä mukaisesti vain koneen joidenkin osien simulointia, mikä tarkoittaa että sen päällä ei voi ajaa muokkaamatonta käyttöjärjestelmää. Paravirtualisoinnissa vieraskäyttöjärjestelmää muokataan niin, että se osaa lähettää käskyt, joita ei voi virtualisoida, suoraan virtualisointikerrokselle. Etuna on parempi suorituskyky, mutta vaatii muokatun käyttöjärjestelmäytimen (*kernel*), jolloin tavallista Windowsia ei voida käyttää. (VMware, Inc., 2007) Käyttöjärjestelmätason virtualisointi tarkoittaa, että itse käyttöjärjestelmän ydin tukee useita eristettyjä käyttäjätiloja, joita kutsutaan säiliöiksi (*container*) tai virtuaaliympäristöiksi (*Virtual Environment, VE*). Tämä tarkoittaa, että kaikissa säiliöissä on sama käyttöjärjestelmä ja laitteisto. (van Dijk, 2008)

Kuvissa 3 – 6 on esitetty yksinkertaistettu kaavio järjestelmän ohjelmistokerroksista neljässä tapauksessa: ilman virtualisointia, isännöity, hypervisor-pohjainen ja säiliöpohjainen virtualisointi. Kerrosten määrä korreloi ratkaisun raskauden kanssa, mitä enemmän kerroksia laitteiston ja suoritettavan ohjelman välissä, sitä hitaampi suoritus. Tämä johtuu suorittimen ympäristön vaihtojen (*context switching*) lisääntymisestä.

Kuva 3: Järjestelmän osat ilman virtualisointia

Kuva 4: Isännöity virtualisointi



Kuva 5: Hypervisor-pohjainen virtualisointi

Kuva 6: Säiliöpohjainen virtualisointi

Tämän työn kannalta vain isännöidyt täyden virtualisoinnin ratkaisut ovat kiinnostavia, koska ratkaisun täytyy olla asennettavissa olemassa olevaan työasemaympäristöön ja käyttäjien omiin koneisiin.

2.1.2 Etätyöpöytä ja työpöydän virtualisointi

Etätyöpöytäohjelma (*remote desktop*) tarkoittaa ohjelmaa, joka mahdollistaa tietokoneen käyttämisen etäältä, esimerkiksi Internetin yli, samaan tapaan kuin käyttäisi paikallista konetta. Ohjelma näyttää etäkoneella näkyvän graafisen käyttöliittymän paikallisella näytöllä ja välittää paikalliset hiiri- ja näppäimistökomennot etäkoneelle. Etätyöpöytäohjelmia ja -protokollia on useita ja niissä on vaihtelevia ominaisuuksia, osa tukee esimerkiksi äänen siirtoa ja USB-laitteiden jakamista. Ohjelma voi yhdistää joko etäkoneen olemassa olevaan istuntoon, jolloin se mahdollistaa etätuen antamisen käyttäjälle tai etäkäyttäjä voi ottaa koneen haltuun ja kirjautua suorittaakseen ylläpidollisia toimia. Etätyöpöytäohjelma voi myös mahdollistaa tietokoneen käyttämisen täysin erilaiselta laitteelta, esimerkiksi kosketusnäyttöpuhelimelta. Tunnetuimpia protokollia ovat Microsoftin *Remote Desktop Protocol* (RDP), Citrixin *Independent Computing Architecture* (ICA) ja avoimen lähdekoodin *X Window System* (X11) ja *Virtual Network Computing* (VNC).

Etätyöpöytäprotokollien ja virtualisoinnin kehitys on mahdollistanut niin sanotun työpöydän virtualisoinnin. Työpöydän virtualisoinnilla (*desktop virtualization, Virtual Desktop Infrastructure, VDI*) tarkoitetaan infrastruktuuria, joka mahdollistaa käyttäjän työpöytäympäristön erottamisen fyysisestä koneesta siirtämällä käyttäjän ohjelmat, tiedostot ja laitteis-

toresurssit palvelimelle. Infrastruktuuriin kuuluvat virtuaalikoneet palvelimilla tai korttitietokoneet (*blade PC*) ja käyttäjien paikalliset suppeat työasemat (*thin client*). Kuvan, äänen ja komentojen siirtoon käytetään etätyöpöytäprotokollaa.

Tällä konseptilla on lukuisia hyviä ja huonoja puolia, eikä ajatus ole uusi, suppeita työasemia yritettiin tuoda markkinoille jo 1990-luvulla ja siinä osin onnistuttiinkin. Suppeita työasemia käytetään eniten kenties julkisissa tiloissa, esimerkiksi kirjastoissa, tarjoamaan web-selaus mahdollisuuden. Nyt ajatus on taas pinnalla pilvilaskennan myötä ja koska palvelinten tehot ovat kasvaneet ja verkkoyhteydet nopeutuneet. Yksi osoitus tästä on Finnetin Supermatrix-hanke, joka pyrkii tuomaan tietokoneen palveluna kotiin nopean verkkoyhteyden myötä (Finnet-liitto ry, 2009).

Työpöydän virtualisointi vaatii nopeahkon ja viiveettömän verkkoyhteyden palvelimelle, sillä käyttäjälle näkyvä kuva joudutaan siirtämään yhteyden yli. Viive käyttäjän komennon, kuten näppäimen painallus, ja näytöllä näkyvän muutoksen välillä ei saa olla liian suuri (suuruusluokka alle 150 ms) tai muuten järjestelmän käyttäjäkokemus on huono (Shneiderman, 2010). Lisäksi liikkuvan kuvan siirto vaatii paljon kaistaa ja prosessointikapasiteettia palvelimelta. Usealla työpaikalla myös hankitaan kannettava ainoaksi työkoneeksi, jolloin ei voida olettaa että kone on aina nopean verkkoyhteyden päässä.

Virtuaalisen työpöydän edut ovat yrityskäytössä ylläpidon ja käytön vaivattomuus ja matalammat ylläpito- ja hankintakustannukset, mikä onkin pääasiallinen syy tekniikan käyttöönottoon (Bowker, 2010). Supermatrix-hankkeessa eduiksi on ajateltu kotikäytössä käytön helppoutta ja automaattista tietojen varmennusta vähemmän tietokoneista tietäville (Finnet-liitto ry, 2009).

Multimediasovellukset

Suurin ongelma etätyöpöydässä ja virtualisoidussa työpöydässä on niiden huono soveltuvuus videotoistoon eli paljon muutoksia sisältävän kuvan esittäminen. Otetaan esimerkkinä videotallenteen katselu web-palvelussa. Normaalitilanteessa videopalvelin lähettää tehokkaasti pakatun kuva- ja äänivirran käyttäjän koneelle, joka purkaa sen ja esittää näytöllä ja toistaa äänilaitteessa. Pakattu videovirta on valmiiksi sovitettu sellaiselle resoluutiolle ja bittinopeudelle, joka ei tuota useimmille Internet-yhteyksille ongelmia, eikä käyttäjän koneelta vaadita juurikaan suorituskykyä sen purkamiseksi. Tilanne muuttuu kuitenkin oleellisesti etätyöpöydän tapauksessa. Nyt videopalvelin lähettää kuvan työpöytäpalvelimelle, joka ei voi lähettää pakattua videovirtaa suoraan käyttäjälle, vaan joutuu itse purkamaan sen ja yhdistämään sen muuhun näytöllä näkyvään sisältöön. Tämä kokonäytön kokoinen kuva pitää nyt siirtää käyttäjän näytölle, mikä tarkoittaa välttämättä kuvan pakkaamista, yleensä siten että vain muutokset kuvassa lähetetään. Käytännössä työpöytäpalvelin joutuu purkamaan ja uudelleenpakkaamaan kuva- ja äänivirrat reaaliajassa. Riippuen kuvan ja ää-

nen tiivistysalgoritmista, jotka voivat olla häviöttömiä tai häviöllisiä, tämä aiheuttaa huomattavan paljon enemmän verkkoliikennettä kuin alkuperäinen video tai sen kuvan- ja äänenlaatu kärsii. Lisäksi työpöytäpalvelimen olisi pystyttävä tahdistamaan kuva ja ääni oikein uudelleenpakatussa muodossa.

Edellistä esimerkkiä jatkaen, pohditaanpa mitä tapahtuu kun käyttäjä päättää suurentaa videon kokonäytön kokoiseksi. Normaalisti ja optimitilanteessa käyttäjän koneen näytönohjain skaalaa kuvan täyteen kokoon, eikä koneen resurssien käyttöaste muutu. Virtuaalisen työpöydän tapauksessa taas työpöytäpalvelin joutuu nyt pakkaamaan näytön täyden resoluution kuvan riippumatta mikä oli videon alkuperäinen tarkkuus. Tyypillisen toimistonäytön resoluutio lienee noin kaksi megapikseliä (esimerkiksi 1600*1200), joka vastaa 1080p-teräväpiirtoresoluutiota, tällä perusteella hyvälaatuinen, mutta silti häviöllinen, kuva vaatisi vähintään 10 Mb/s kaistanleveyden[3].

Tähän ongelmaan on erilaisia ratkaisuja. Hewlett-Packard on parantanut etäyhteysprotokollaa ja kuvan pakkausta *Remote Graphics Software* -ohjelmistolla. Toinen vaihtoehto on siirtää videon purku paikalliselle koneelle (*multimedia redirect*). Videon purku paikallisella koneella on mahdollista esimerkiksi Microsoftin RDP 7.0 versiolla, jonka tuki rajoittuu vain Windows Media Playerin kautta toistettuun materiaaliin tai Citrixin HDX-tekniikalla. Kirjoittajan mielestä tämä tosin hieman rikkoo virtualisoidun etätyöpöydän ideaa vastaan, koska suppea työasema ei voi enää ollakaan niin suppea. Kolmas vaihtoehto hyödyntää virtuaalikonetta, sillä se voi kaapata grafiikkakomennot suoraan virtuaalikoneesta, jolloin näkyvää kuvaa ei tarvitse lähettää kuvana. Eräs tällainen tekniikka on Red Hatin SPICE, joka on julkaistu avoimen lähdekoodin projektina (Red Hat, Inc., 2010).

2.1.3 Virtuaalikone-pohjainen työpöytä

Uusin malli virtualisoinnissa on tuoda hypervisor-pohjainen virtuaalikone suoritettavaksi paikallisesti (*local virtual machine-based desktop, client hypervisor*), mutta jonka käyttöjärjestelmälevykuvat ovat keskitetysti hallittuja. Isännöityyn virtualisointiratkaisuun perustuvia ratkaisuja on olemassa, mutta niiden huono puoli on, että isäntäkäyttöjärjestelmää täytyisi myös ylläpitää ja vieraskäyttöjärjestelmän suorituskyky on heikohko. Hypervisor-pohjainen virtuaalikone on tuttu palvelinympäristöstä, mutta työasemapuolella on paljon enemmän erilaisia komponentteja, joita täytyy tukea, kuten näytönohjaimet, langattomat verkkokortit ja virranhallintaominaisuudet. Lisäksi, palvelinympäristössä vieraiden ei tarvitse käyttää näytönohjaimen, äänikortin ja USB-laitteiden resursseja suoraan. Haasteena

[3] Blu-Ray elokuvissa käytetään yleisesti 15 – 30 Mb/s bittivirtanopeuksia kuvalle, kuvataajuuden ollessa 24 tai 25 kuvaa sekunnissa (nimimerkki"benes", 2009). OnLive-onlinepelipalvelu tarvitsee yhden megapikselin kuvaan (1280*720, 60 FPS) 4 Mb/s.

on ajureiden lisäksi hallintakerroksen toteutus ja toimivuus. Toistaiseksi yhtään kaupallista ratkaisua ei ole saatavilla merkittävältä toimijalta, mutta ainakin Citrix on tuomassa, oletettavasti, markkinoille vuonna 2010 heidän aiemmin esittelemänsä XenClient-ohjelman.

Paikallisesti suoritettavan virtuaalikoneen etuina ovat nopeus, paikallisen työaseman resurssien hyväksikäyttö, multimedian toimivuus ja jatkuvasti auki olevan verkkoyhteyden tarpeettomuus. Toisaalta virtuaalikoneen käyttö mahdollistaa yhden levykuvan käyttämisen kaikissa koneissa, joten sitä voidaan hallita keskitetysti, kuten virtualisoidun työpöydän tapauksessa. Käyttäjän järjestelmä on aina ajan tasalla ja toimii ilman ristiriitoja, eikä järjestelmän päivitysten asentaminen häiritse työntekoa. Hypervisor-pohjainen virtuaalikone myös mahdollistaa usean käyttöjärjestelmän ajamisen samanaikaisesti ja näiden erottamisen toisistaan. Siten käyttäjällä voi olla mahdollisuus käyttää toista käyttöjärjestelmää yksityiskäyttöön ja asentaa sinne haluamiaan ohjelmia, jotka eivät toisaalta häiritse työhön tarkoitettua järjestelmää. Näin ylläpidon työ helpottuu kun monet eri ohjelmisto- ja rautayhdistelmät eivät enää aiheuta ongelmia.

2.1.4 Virtuaalikoneiden turvallisuusuhat

Virtuaalikoneisiin kohdistuvat tietoturvauhat ovat samoja kuin oikeisiin koneisiinkin, samat virukset ja vastaavat toimivat myös virtuaalikoneissa, toisaalta niiden toimintaa on helpompi tutkia, koska ne eivät voi piiloutua samalla tavalla kuin oikeassa koneessa. Virtuaalikoneisiin kohdistuu lisäksi omanlaisiaan uhkia. Virtuaalikonevalvoja on suunniteltu niin, että eri virtuaalikoneet eivät näe toisiaan, eivätkä voi käyttää kaikkia vapaita laiteresursseja, joten ne eivät voi häiritä toisiaan. Ohjelman ei myöskään pitäisi pystyä poistumaan virtuaalikoneesta (*VM escape*), mikä on eristyksen pettämisen pahin tapaus. Virtuaalikoneita pidetään melko turvallisina, mutta kaikissa järjestelmissä on puutteita. Turvallisuusuhat voidaan jakaa kolmeen tapaukseen: virtuaalikoneesta isäntään, isännästä virtuaalikoneeseen ja virtualisointikerrokseen suuntautuvat uhat. Virtuaalikoneesta toiseen ei pitäisi pystyä hyökkäämään, muuten kuin murtautumalla toiseen koneeseen verkon kautta, jos virtuaalikoneet ovat samassa verkossa. (Kirch, 2007) Se ei ole erityisesti virtuaalikoneita koskeva uhka, mutta Gartnerin tutkimuksen mukaan väärin konfiguroitu virtualisointiympäristö on yleinen virhe, sillä jopa 60 prosenttia virtuaalipalvelimista on turvattomampia kuin fyysiset palvelimet (Gartner, Inc., 2010).

Isäntä voi valvoa virtuaalikoneita kuten haluaa, se voi lukea muistia, levyä, verkkoa ja näppäimistöä, siksi isännän turvallisuustaso ei voi olla pienempi kuin vieraan. Vieraassa ei siis voi käsitellä mitään sellaista tietoa, mitä isäntä ei saa saada selville, ja jos isäntäkoneeseen onnistutaan murtautumaan, ovat myös virtuaalikoneiden tiedot vaarassa. Siispä luotettua ympäristöä ei voida suorittaa epäluotettavalla alustalla, jonka vuoksi isäntäkoneen yllä-

pito on erityisen tärkeää. Tämä ei varsinaisesti ole uhka, vaan ominaisuus, joka täytyy ottaa huomioon. (Kirch, 2007)

Virtualisointikerroksen eli itse virtuaalikoneen tai -valvojan muokkaaminen tai viallinen toteutus voi vaarantaa luottamuksen virtuaalikoneessa ajettaviin, muuten luotettuihin sovelluksiin. Tähän auttaa kattava testaus ja ohjelman eheyden varmistaminen. Virtualisoinnin heikko toteutus voi myös mahdollistaa palvelunestohyökkäyksen. Mikäli yksi virtuaalikone saa kaikki fyysisen koneen laitteistoresurssit käyttöön tai suorittaa jotain sellaista koodia, joka aiheuttaa virtualisointiohjelmiston varaamaan kaikki resurssit, ja näin estää isännän ja muiden virtuaalikoneiden toiminnan. (Kirch, 2007)

Virtuaalikoneesta isäntään kohdistuva hyökkäys on vakavin uhkakuva. Tietoturvayritys Immunity paljasti vakavan hyväksikäyttömahdollisuuden kesäkuussa 2009 VMwaren Workstation ja Player ohjelmissa. Haavoittuvuus mahdollisti koodin suorittamisen isäntäjärjestelmässä. (Higgins, 2009) Puolalainen tietoturva-asiantuntija Joanna Rutkowska yhdessä kollegoidensa kanssa on tuonut esille useita haavoittuvuuksia niin Xen-virtualisointiympäristöstä (Wojtczuk, 2008), Intelin prosessoreista (Wojtczuk & Rutkowska, 2009a) (Wojtczuk;Rutkowska;& Tereshkin, 2009) (Wojtczuk & Rutkowska, 2009b) kuin piirisarjasta (Wojtczuk & Tereshkin, 2009). Näitä kaikkia voidaan käyttää muun muassa hyökkäyksessä virtuaalikonetta vastaan ja ne saattavat mahdollistaa ohjelmalle pääsyn pois virtuaalikoneesta. Hän on myös kehittänyt *Blue Pill* -ohjelman jolla voidaan siirtää ajossa oleva käyttöjärjestelmä virtuaalikoneeseen (Invisible Things Lab, 2010).

Rutkowska kollegoineen uskoo kuitenkin, että Intelin *Trusted Execution Technology*n (TXT) kaltaiset tekniikat tulevat olemaan välttämättömiä kehitettäessä turvattuja ympäristöjä. Vaikka TXT:n toteutuksesta on löytynytkin puutteita, jotka mahdollistavat juuri niiden asioiden tekemisen mitä tekniikan piti estää, Rutkowska katsoo, että monimutkaisista järjestelmistä löytyy väistämättä aluksi puutteita.

Seuraavassa aliluvussa käsitellään virtuaalista yksityisverkkoa ja niissä käytettyjä tekniikoita, mikä on oleellinen osa tutkimusverkkoja, sillä siten niihin voidaan yhdistää suojatusti.

2.2 Virtuaalinen yksityisverkko

Virtuaalinen yksityisverkko (*virtual private network, VPN*) on yleisnimitys yksityiselle verkolle, joka on rakennettu tunneloiduista yhteyksistä julkisen verkon päälle. Tunneleiden hyötykuormat ovat usein salattuja ja todennettuja. (Snader, 2005) Virtuaalinen tarkoittaa tässä yhteydessä, että virtuaaliverkon koneiden välissä ei ole suoraa fyysistä yhteyttä vaan

yhteydet muodostuvat yleisen verkon yli VPN-päätelaitteen tai -ohjelman toteuttamina, niin sanottuina tunneleina. Virtuaaliverkon liikenne tavallisesti salataan ja verkkoon liittyminen vaatii tunnistautumisen, mistä termi yksityinen. Virtuaalisen yksityisverkon tavallisin käyttökohde ja tekniikan kehittämisen lähtökohta on yrityksen toimipisteiden verkkojen yhdistäminen Internetin yli. VPN-tekniikalla yritykset korvasivat kiinteät ja kalliit vuokratut kiinteät yhteydet halvemmalla Internet-yhteydellä. Toinen käyttötapa VPN-tekniikalle on tarjota turvalliset etätyöyhteydet työntekijöille yrityksen verkkoon ja sen palveluihin Internetin yli.

Standardoimisjärjestö Internet Engineering Task Force (IETF) on julkistanut useita tunnelointiprotokollia, jotka soveltuvat VPN-käyttöön. Nämä voidaan jakaa kahteen ryhmään: *site-to-site* ja etäyhteys (*remote access*) -protokollat. Site-to-site -protokollat mahdollistavat turvallisten yhteyksien muodostamisen yrityksen toimipisteiden välillä. Etäyhteysprotokollat tarjoavat saumattoman yhteyden yrityksen lähiverkkoon etä- ja matkatyöntekijöille. (Frahim & Huang, 2008) Moni protokolla voi toimia kummassakin roolissa, mutta site-to-site protokollat eivät ole kiinnostavia tämän työn kannalta, joten niitä käsitellään tässä vain etäyhteyden kannalta. Etäyhteysprotokollia ovat esimerkiksi OSI-mallin

- siirtoyhteyskerroksen (2.) Point-to-Point Tunneling Protocol (PPTP) (Hamzeh;Pall;Verthein;Taarud;Little;& Zorn, 1999)
- verkkokerroksen (3.) Internet Protocol Security (IPsec), (Kent & Seo, 2005)
- istuntokerroksen (5.) Layer 2 Tunneling Protocol (L2TP) over IPsec, (Patel;Aboba;Dixon;Zorn;& Booth, 2001), toimii kuten siirtoyhteyskerroksen (2.) protokolla (Cisco Systems, Inc., 2009, ss. 9-1)
- kuljetus- – sovelluskerroksen (4-7.) Secure Socket Layer / Transport Layer Security VPN (SSL/TLS VPN)

2.2.1 Tunnelointi

VPN-protokollat perustuvat tunnelointiin, jonka perusidea on yksinkertainen ja yleinen toimintamalli on esitetty vuonna 1994 RFC-dokumentissa 1701 Generic Routing Encapsulation (GRE) (Hanks;Li;Farinacci;& Traina, 1994). Tunnelointi tarkoittaa, että niin sanottu toimitusprotokolla (*delivery protocol*) kapseloi toisen protokollan mukaisen paketin hyötykuormakseen. Toista protokollaa kutsutaan hyötykuormaprotokollaksi (*payload protocol*). Näin hyötykuorma voidaan tunneloida eli kuljettaa esimerkiksi epäyhteensopivan kuljetusverkon yli. Hyötykuorma voi olla vaikka yksityisverkon IP-paketti, jota ei voida reitittää julkisessa Internetissä. Tämä paketti voidaan kapseloida toiseen IP-pakettiin, jossa on julkiset IP-osoitteet. Pakettien reitittämiseksi vaaditaan vielä yhdyskäytävät verkon reunoilla, jotka hoitavat kapseloimisen ja sen purkamisen yksityisen ja julkisen verkon välillä.

2.2.2 PPTP

Point-to-Point Tunneling Protocol on vanhentunut protokolla, joka on ollut Microsoft Windows-käyttöjärjestelmissä vakio-ominaisuutena versiosta 95 ja siten laajasti levinnyt. Protokollan heikkous on kyky tunneloida ainoastaan Point-to-Point Protocol (PPP) kehyksiä ja turvallisuuspuutteet eikä sitä siksi pitäisi käyttää. (Graham & Cook, 2009)

2.2.3 IPsec

IPsec on viitekehys Internet protokollan (IP) turvallisuuden parantamiseen ja se tarjoaa osapuolten todennuksen, tiedon eheyden ja luottamuksellisuuden päästä päähän yhteyksille (*end-to-end*) tai yhdyskäytävien välille. IPsec ei määrittele käytettäviä salausalgoritmeja, joten se on luonteeltaan hyvin yleinen. Koska IPsec toimii verkkokerroksella, sillä voi suojata kaiken Internet-liikenteen eikä sovelluksilta vaadita erillistä tukea, tämä tosin edellyttää käyttöjärjestelmätason tukea. IPsec on tuettuna kaikissa varteenotettavissa käyttöjärjestelmissä mukaan lukien Windows, Linux ja mobiilikäyttöjärjestelmät, kuten Symbian. IPsec koostuu kolmesta protokollasta: Authentication Header (AH), Encapsulating Security Payload (ESP) ja Internet Key Exchange (IKE). AH ja ESP tarjoavat paketin aidonnuspalvelun, sisältäen lähettäjän todennuksen, tiedon eheyden ja toistohyökkäyksen eston. ESP tarjoaa lisäksi tiedon salauksen. IKE on monimutkainen avaintenvaihtoprotokolla, jota AH:n tai ESP:n käyttö edellyttää. IPsec ja siihen liittyvät protokollat on määritelty alun perin vuonna 1995 (RFC 1825, 1829) ja sittemmin useissa IETF:n dokumenteissa sisältäen RFC 4301 – 4309, 2401 – 2412 ja useat muut.

IPsecin huonoja puolia ovat sen kompleksisuus, ryhmälähetyksen (*multicast*) toimimattomuus sekä AH:n ja ESP:n toimimattomuus osoitteenmuunnoksen kanssa (*Network Address Translation, NAT*), sillä osoitteenmuunnos muuttaa lähettäjän osoitetta eikä tällöin läpäise eheystarkistusta vastaanottajalla. Puutteistaan huolimatta IPsec on erittäin suosittu yritysten yksityisverkkototeutuksissa sillä sitä tukevia laitteita ja ohjelmistoja on runsaasti saatavilla. (Frahim & Huang, 2008) (Feilner, 2009) Tämän työn kannalta varsinkin ryhmälähetyksen toimimattomuus on kriittistä, sillä se estää sitä käyttävien multimediapalvelujen toiminnan. Lisäksi IP-protokollasta riippumattomien protokollien testaus on mahdotonta.

2.2.4 L2TP/IPsec

L2TP yhdistää PPTP ja Ciscon Layer 2 Forwarding (L2F) protokollien hyvät puolet, protokolla on dokumentoitu RFC 3931:ssä (Lau;Townsley;& Goyret, 2005). L2TP ei tarjoa kuitenkaan luottamuksellisuutta, joten sitä suositellaan käytettäväksi IPsec kanssa (L2TP over IPsec), aihe on dokumentoitu RFC 3193:ssa (Patel;Aboba;Dixon;Zorn;& Booth, 2001).

L2TP yhdessä IPsecin kanssa antaa sen edun pelkkään IPseciin nähden, että silloin saadaan myös muita protokollia tunneloitua kuin IP ja myös ryhmälähetys toimii. Yhdistelmän haittapuolina, IPsecin huonojen puolien lisäksi, on protokollapinon suuruus (*overhead*) ja edelleen lisääntynyt monimutkaisuus. (Lewis, 2006)

2.2.5 SSL VPN

SSL VPN on tuorein VPN-tekniikka, ja se toimii aiemmin mainittuja tekniikoita ylemmillä protokollakerroksilla. Secure Sockets Layer (SSL) on alun perin Netscape Communicationsin vuonna 1994 kehittämä turvallisuusprotokolla web-selaimella toimivien palveluiden käyttöön yhteyden salaamista ja käyttäjän todennusta varten. Sen kolmas ja viimeinen versio on julkaistu vuonna 1996 (Freier;Karlton;& Kocher, 1996). IETF:n otettua SSL:n kehitys vastuulleen protokollan nimi muutettiin Transport Layer Securityksi (TLS), mutta nimiä käytetään kirjallisuudessa rinnasteisina. TLS versio 1.2 on dokumentoitu RFC 5246:ssa (Dierks & Rescorla, 2008), joka on vuodelta 2008. SSL VPN ratkaisusta ei sen sijaan ole standardia, niinpä eri toteutukset eivät ole toistensa kanssa yhteensopivia. SSL VPN toimii sovelluskerroksella ja sillä voidaan tunneloida mitä tahansa protokollia siirtoyhteyskerrokselta (L2) lähtien. SSL VPN voi myös tarkoittaa web-selaimessa toimivaa suojattua yhteyttä, esimerkiksi yrityksen sähköisiin palveluihin, mutta on hieman harhaanjohtavaa puhua VPN:stä, sillä kone ei ole tällöin osana yrityksen verkkoa.

SSL:n vahvuus on sen kypsyys, levinneisyys ja yksinkertaisuus ja toteutukset ovat hyvin koeteltuja. Toinen vahvuus on toimivuus NAT:in yli, ja että SSL:n vaatima TCP portti 443 on useimmiten avoin julkisissakin verkoissa, koska muuten suojatut HTTPS-sivut (HTTP over SSL/TLS) eivät toimisi. IPsec ja muut tunnelointiprotokollien portit ovat usein suljettu julkisissa verkoissa. Lisäksi SSL VPN toimii käyttöjärjestelmän käyttäjätilassa (*user space*) eikä ole tekemisissä ydinkerroksen kanssa, kuten IPsec, mikä tekee ylläpidosta helpompaa. (Graham & Cook, 2009)

SSL VPN ja reaaliaikaiset protokollat

SSL-protokollaa ei ole suunniteltu VPN-käyttöön, joten sen suosio on tuonut esiin myös puutteita sovellettaessa. SSL vaatii luotettavan TCP-protokollan toimiakseen, eikä sitä ole suunniteltu käytettäväksi UDP:n päällä. Jos UDP tai muun reaaliaikaprotokollan liikennettä välitetään SSL VPN:n yli, se joudutaan kapseloimaan TCP:n sisälle. Tämä aiheuttaa turhaa ylimäärää, viivettä ja viiveen vaihtelua, koska vastaanottaja joutuu odottamaan uudelleenlähetykset, jotta se voi lukea tietovirtaa. Suorituskyky laskee myös välitettäessä TCP-liikennettä (Honda;Ohsaki;Imase;Ishizuka;& Murayama, 2004), mutta TCP:llä ei tavallisesti välitetä samalla tapaa viiveille herkkää tietoa, kuten videovirtaa. Nämä ongelmat heiken-

tävät käyttäjäkokemusta ja voivat estää esimerkiksi hyvälaatuisen VoIP-puhelun. Tämän vuoksi IETF on ehdottanut Datagram Transport Layer Security (DTLS) standardia, RFC 4347 (Rescorla & Modadugu, 2006), joka mahdollistaa TLS:n käyttämisen UDP:n päällä. DTLS on toteutettuna ainakin avoimen lähdekoodin OpenSSL-työkaluohjelmassa (*toolkit*). (Frahim & Huang, 2008, s. 48)

SSL tunnistautuminen

SSL tunnistautuminen tehdään tavallisesti X.509-varmenteella (*certificate*), joka voi olla yleisesti luotetuksi tiedetyn varmentajatahon (*certificate authority*) myöntämä tai se voi olla itsemyönnetty (*self-signed*). Web-ympäristössä yleensä vain palvelin todentaa itsensä esittämällä varmenteen, jonka perusteella käyttäjä voi päättää onko palvelin luotettava. VPN-sovelluksessa myös käyttäjän on tunnistauduttava palvelimelle. Käyttäjän tunnistautumisen voi hoitaa usealla tavalla, mutta tässä työssä keskitytään varmenteella tehtävään tunnistautumiseen, mikä on suositeltu tapa tunnistaa käyttäjä (katso luku *3.2.3 Etäkäyttö*) ja myös helposti ylläpidettävä. Jotta yhteys voidaan hyväksyä, käyttäjän on esitettävä palvelimen ylläpitäjän hyväksymä varmenne, joka ei ole estolistalla. SSL:ssä on tätä varten määritelty toimintatapa, joka on esitetty liitteessä F. Tässä kohtaa ei ole syytä avata SSL toimintaa tarkemmin, viestien yksityiskohtaisen kuvauksen voi lukea tarkemmin protokollan kuvauksesta (Dierks & Rescorla, 2008) tai kirjallisuudesta (Snader, 2005).

2.2.6 Hajautetut protokollat

Tavallisten palvelin-asiakas -protokollien lisäksi on olemassa lukuisia hajautettuja, P2P-periaatteella toimivia, VPN-tyyppisiä ohjelmia tutkimus- ja kotikäyttöön. Näitä ovat esimerkiksi IP over P2P (IPOP) (Ganguly;Agrawal;Boykin;& Figueiredo, 2006), Social VPN (Figueiredo;Boykin;Juste;& Wolinsky, 2008), N2N: A Layer Two Peer-to-Peer VPN (Deri & Andrews, 2008), Hamachi (LogMeIn, 2010) ja Wippien (Wippien, 2010).

Näissä ei tyypillisesti ole keskuspalvelinta jota kautta kaikki liikenne kulkee, vaan jokaisella solmulla on suoria yhteyksiä moneen muuhun solmuun. Tunneloinnin lisäksi ohjelmien täytyy siis huolehtia myös pakettien reitityksestä kyseisessä verkossa. Varsinkin kotikäyttöön suunnatuissa ohjelmissa on jokin keskuspalvelin, joka helpottaa verkkoon liittymistä ylläpitämällä listaa yksityisistä verkoista, jolloin tavallisesti verkkoon pääsee kun tietää verkon nimen ja salasanan. Tämän työn ratkaisuksi hajautetut yksityisverkot ovat kuitenkin huono ratkaisu, sillä tarvittava yhteystyyppi on nimenomaan *point-to-point* palvelin-asiakas -mallinen; usea asiakas yhdistää yhdelle palvelimelle eikä asiakkaiden ole syytä tietää toisistaan.

2.2.7 Yksityisverkkojen turvallisuusuhat

Yksityisverkko tarjoaa viestien luottamuksellisuuden, eheyden ja lähettäjän todennuksen. Nämä ominaisuudet mahdollistavat salausalgoritmien käyttö, mutta itse salausalgoritmia ei välttämättä tarvitse murtaa, jotta yksityisverkon turvallisuus olisi uhattuna. Protokollat ovat tavallisesti turvallisia oikein käytettyinä, mutta toteutuksissa voi olla vikoja. Siksi ohjelmat ja salausalgoritmit ovat syytä olla ajan tasalla. Suuremman uhan muodostavat kuitenkin puutteelliset yksityisverkon asetukset, valittu tietoturvapolitiikka ja sen toteutus, salasanojen tai sertifikaattien joutuminen vääriin käsiin ja verkon fyysinen turvallisuus. Varsinkin IPsecin turvapolitiikoiden konfigurointi on tunnetusti vaikeaa (Hamed;Al-Shaer;& Marrero, 2005).

SSL ja X.509 haavoittuvuudet

SSL v3 ja TLS protokollia on pidetty turvallisina (Gajek;Manulis;Pereira;Sadeghi;& Schwenk, 2008) (Paulson, 1999), vaikka toteutuksista onkin löydetty haavoittuvuuksia. Vuonna 2009 paljastettiin kuitenkin kolme erilaista haavoittuvuutta liittyen SSL-protokollaan ja X.509-varmenteeseen.

Tutkija Moxie Marlinspike esitteli Black Hat DC 2009 konferenssissa keinoja muuttaa suojattu HTTPS yhteys suojaamattomaksi HTTP yhteydeksi väliintulohyökkäyksellä (*man-in-the-middle attack*). (Marlinspike, 2009a) Tämä ei ole niin vakava haavoittuvuus sillä se vaatii, että hyökkääjällä on mahdollisuus kaapata käyttäjän web-liikenne.

Marlinspike ja tutkija Dan Kaminsky esittelivät toisistaan riippumatta vakavamman ”*null prefix*” hyökkäyksen X.509 varmenteita vastaan Black Hat USA 2009 konferenssissa. Se mahdollistaa varmentajan myöntävän varmenteen esimerkiksi seuraavalle osoitteelle *www.paypal.com\0.somedomain.com*, varmentaja katsoo vain juuriverkkoalueen *somedomain.com* kelpoisuuden. SSL toteutukset toisaalta käsittelevät merkkijonoa omilla metodeillaan ja ”\0” -merkki sattuu olemaan lopetusmerkki C-kielessä, jolloin yllä oleva varmenne menisi läpi kuin se olisi *www.paypal.com*. (Marlinspike, 2009b)

Ohjelmistokehittäjä Marsh Ray löysi itse SSL-protokollasta haavoittuvuuden sen tavasta hoitaa todennuksen uudelleenneuvottelu. Haavoittuvuus mahdollistaa hyökkääjän toimimisen palvelimen ja asiakkaan välissä kummankaan havaitsematta. Koska haavoittuvuus on itse protokollassa, se on vakava ja koskee kaikkia toteutuksia. (Ray & Dispensa, 2009) IETF alkoi heti toimiin TLS-protokollan korjaamiseksi ja korjaus on ilmeisesti valmis, mutta oli vielä kirjoitushetkellä vedos-versiossa (Rescorla;Ray;Dispensa;& Oskov, 2010). Myös SSL-ohjelmien valmistajat ovat korjaamassa ohjelmiaan, mutta korjaamista hidastavat vaadittavat yhteensopivuustestaukset. Toisaalta kaikkia laitteita tai ohjelmistoja, kuten tulostimia, ei ikinä päivitetä, jolloin niihin haavoittuvuus jää pysyvästi. (Higgins, 2010)

2.3 Liittyvä työ

Tässä luvussa esitellään lyhyesti erityyppiset testiverkot sekä Suomessa käynnissä oleva testiverkkoprojekti. Tähän työhön läheisesti liittyvä projekti on PurpleNet, joka on käyttöliittymä OpenVPN-varmenteiden hallintaan.

2.3.1 Testiverkot

Testiverkot (*testbed*) ovat tiettyä tutkimus- tai kokeilutarkoitusta varten pystytettyjä tietoverkkoja ja toimivat kokeen kehitysympäristönä. Testiverkot mahdollistavat toistettavissa olevat olosuhteet teorioiden, työkalujen tai tekniikoiden testaamiseen. Toisaalta ne voivat myös emuloida Internetin arvaamattomuutta, joko satunnaistamalla verkon tapahtumia tarkoituksella tai verkko voi toimia Internetin yli ja olla siten Internetin satunnaisprosessien vaikutusten alainen. Testiverkko voi olla kooltaan muutamasta noodista maailmanlaajuiseen satojen noodien verkkoon, lisäksi sen tyyppiin vaikuttaa onko testiverkko liitetty Internetiin vai onko se täysin suljettu.

Eräs suurimmista testiverkoista on *overlay*-tyyppinen PlanetLab, joka on globaali tutkimusverkko, jonka tehokkaat solmut sijaitsevat yliopistoilla ja ne ovat yhdistetty nopeilla yhteyksillä Internetin yli. Verkko tarjoaa alustan kaikenlaisille kokeille, joita ajetaan virtuaalikoneissa, mahdollistaen resurssien varaamisen monen kokoisiin kokeisiin. PlanetLab on edesauttanut tutkimustyötä ja toimii pohjana esimerkiksi Coral-sisällöntoimitusverkolle (Peterson, 2010). PlanetLabin etu on aidot verkko-olosuhteet, mikä on myös huono puoli, sillä verkko voi olla ylikuormittunut, kokeiden toistettavuus on huono eikä verkossa ole etuoikeuksia (Duerig;Ricci;Zhang;Gebhardt;Kasera;& Lepreau, 2006).

Toinen vastaavantyyppinen suosittu verkko on Emulab, erona PlanetLabiin on emuloitu verkkoympäristö ja siten hyvä toistettavuus, mutta toisaalta verkko on keinotekoinen (Duerig;Ricci;Zhang;Gebhardt;Kasera;& Lepreau, 2006).

Suomessa on käynnissä projekti, ICT SHOK Tulevaisuuden Internet -testiverkko, jonka tavoite on rakentaa maanlaajuinen testiverkko (kuva 7). Verkon tarkoitus on toimia muun muassa Tulevaisuuden Internet -hankkeen tutkimuksen apuvälineenä ja tarjota erilaisia palveluita ja avoimen verkkoympäristön. Tämä työ tehdään osana kyseistä projektia. Erona tällä testiverkolla esimerkiksi PlanetLabin virtualisoituun verkkoon on, että se toteutetaan dedikoiduilla yhteyksillä ja laitteilla ja vastaa näin enemmän tosimaailmaa, mutta suorat L1- ja L2-valopolkuyhteydet antavat mahdollisuuden tutkia monenlaisia laitteita tai protokollia, jotka eivät olisi mahdollisia (L3) IP-verkossa. Testiverkkoon on mahdollista liittyä omalla valopolulla, tavallisella Ethernet-liitynnällä tai Internetin kautta. (Nikander & Mäntylä, 2007) (Savola, 2009)

Kuva 7: Tulevaisuuden Internet -testiverkon maantieteellinen kattavuus, yhteydet muodostuvat käytännössä Funetin kuituverkon pohjalle

2.3.2 PurpleNet

PurpleNet on web-käyttöliittymä OpenVPN-tunnelointipalvelimelle, tarkoituksena helpottaa palvelimen hallintaa ja palveluiden julkaisua loppukäyttäjille ja päätelaitteille. PurpleNet on kehitetty Tampereen teknillisessä yliopistossa ja on kirjoitushetkellä vasta alpha-kehitysvaiheessa. (Pajukanta, 2009) Käytännössä OpenVPN-palvelimen ylläpitäjä voi käyttää PurpleNettiä jakamaan web-sivulta käyttäjille X.509-varmenteet, joilla voi tunnistautua OpenVPN-palvelimelle. Kyseiselle sivulle tunnistaudutaan esimerkiksi käyttäen Haka-tunnistautumista[4]. Näin saadaan jaettua sertifikaatit turvallisesti ja vain asianmukaisille henkilöille. Tunnistautumisen ja varmenteiden jakelunhallinnan käsittely ei kuitenkaan ole tämän työn rajauksen puitteissa.

[4] Haka on identiteettiliitto (*identity federation*) Suomen yliopistoissa, korkeakouluissa ja tutkimuslaitoksissa. Käyttäjät (opiskelijat, opettajat, tutkijat ja ylläpitäjät) pääsevät näin palveluihin yhdellä käyttäjätunnuksella ja salasanalla.

2.4 Yhteenveto

Toisessa luvussa käsiteltiin virtualisointia, virtuaalisia yksityisverkkoja ja lisäksi hieman testiverkkoja. Virtualisointi on nopeasti kasvava liiketoiminta-alue ja tulee visioiden mukaan muuttamaan organisaatioiden koko IT-ympäristön. Kokonaisen järjestelmän virtualisoiminen on tärkeä osa, sillä se tuo joustavuutta, niin palvelimissa kuin työpöydällä. Työn kannalta tärkein virtualisointitapa on isännöity virtuaalikone, joka mahdollistaa virtuaalikoneiden suorittamisen jo olemassa olevassa järjestelmässä. Toinen tapa on hypervisor-pohjainen virtualisointi, joka asennetaan tyhjään koneeseen. On olemassa myös muun tyyppisiä virtualisointiratkaisuja, jotka ovat riippuvaisia isäntäjärjestelmästä tai etäkäytettäviä, jolloin puhutaan etätyöpöydästä tai työpöydän virtualisoinnista. Näiden heikkoutena ovat etenkin multimediasisällön välittäminen verkkoyhteyden yli, mikä kuluttaa paljon verkkokapasiteettia.

Virtuaalisilla yksityisverkoilla muodostetaan suojattuja verkkoja käyttäen tunneloituja yhteyksiä julkisessa verkossa. VPN-protokollia ovat muun muassa PPTP, IPsec ja L2TP, ja lisäksi standardisoimaton SSL VPN ja P2P-tyyppiset protokollat.

Testiverkoissa suoritetaan esimerkiksi verkkoprotokollien tutkimusta. Suomessa rakennetaan parhaillaan tutkimuskäyttöön Tulevaisuuden Internet -testiverkkoa ja palveluita. Tämän työn tuloksia on tarkoitus hyödyntää kyseisen testiverkon käytössä.

3 Vaatimukset virtuaaliympäristölle

Tässä luvussa käsitellään ratkaisulta odotettavia ominaisuuksia, niin käyttäjien, tietoturvapolitiikan, tietojärjestelmien ylläpidon kuin laitteistovaatimusten kannalta. Ratkaisun käyttäjinä toimivat tietoverkkotutkijat ja yhteistyökumppanit. Tietoturvapolitiikkaa käsitellään Aalto-yliopiston politiikoiden ja osittain valtion tietoturvaohjeiden mukaisesti. Laitteistovaatimusten osalta pohditaan vähimmäisvaatimuksia ja suositeltuja laitteisto-ominaisuuksia.

3.1 Käyttötavat

Tulevaisuuden Internet -testiverkon pääkäyttötapauksiksi on ajateltu useita eri tapauksia kun siihen yhdistetään Internetin kautta. Tärkeimpänä tapauksena on verkkoprotokollien testaus ja kokeilu. Testiverkko tarjoaa myös paremmat puitteet verrattuna omaan pieneen laboratorioympäristöön. Kolmas tapaus on tarjota Internetin rajoittamaton käyttö, mikäli yliopiston tai organisaation palomuuri estää verkon täysipainoisen hyödyntämisen.

Tässä työssä esitetty ratkaisu siis mahdollistaa edellä mainitut tapaukset, mutta toisaalta niihin saattaa riittää myös pelkkä tekstipohjainen yhteys. Tämä ratkaisu on toisaalta monipuolisin, se mahdollistaa graafisten ohjelmien käytön, mikä helpottaa niiden henkilöiden toimimista, jotka eivät ole tottuneet pelkän komentorivin käyttöön. Ratkaisu mahdollistaa myös ryhmälähetysten ja muun multimedian seuraamisen, mutta toisaalta kaikki komentoriviohjelmat toimivat myös.

Tutkijalle ratkaisusta on se hyöty, että virtuaaliympäristössä on helppo kokeilla kaikenlaista helposti ja nopeasti, sillä käyttöoikeudet eivät rajoita tekemistä eikä pöydällä ole ylimääräistä laitteistoa. Opetuksessa ratkaisua voisi käyttää esimerkiksi joissakin laboratoriotöissä mahdollistamaan opiskelijoille etätyö tai harjoittelu omassa tahdissa. Yliopistojen kumppaniyrityksille ratkaisu toisi erityisen helpon tavan päästä käsiksi tutkimusverkkoon.

Kotona ratkaisu mahdollistaisi opiskelun lisäksi, esimerkiksi virtuaalikoneen yhdistämisen anonymisointipalveluun, kuten ruotsalainen Relakks. Tämä mahdollistaa esimerkiksi melko anonyymin web-selauksen tai web-sivujen maarajoitusten kiertämisen (mikä voi olla kiellettyä), mutta kaikkea verkkoliikennettä ei tarvitse tällöin kierrättää epäluotetun palvelun kautta. Eräs käyttäjä kertoi kyselyssä (katso alta) käyttäneensä virtuaalikonetta vanhojen Linux-pelien pelaamiseen ja VPN-yhteyttä töissä saatavilla olevien sähköisten palveluiden käyttöön, mutta varsinaisesti näiden yhdistelmälle ei löytynyt käyttöä.

Käyttäjien näkökulma

Käyttäjien, lähinnä tutkijoiden, mielipiteitä selvitettiin web-pohjaisella kyselyllä, joka lähetettiin Aalto-yliopiston tietoliikenne- ja tietoverkkotekniikan laitoksen sähköpostilistalle sekä eräälle toiselle tietoverkkotekniikan tutkimusaiheiselle sähköpostilistalle. Kyselyssä selvitettiin käyttäjien virtuaalikone ja VPN tuntemusta, nykyisin käytössä olleita tapoja yhdistää testiverkkoihin sekä kiinnostuneisuutta tämän työn kaltaiseen ratkaisuun. Lisäksi pyydettiin asettamaan ensisijaisuusjärjestykseen erityyppisillä ohjelmilla fyysinen kone, virtuaalikone ja etätyöpöytäratkaisu. Vastauksia saatiin 15 kappaletta, liitteessä E on esitetty yhteenvetona kyselyn tulokset.

Vastaajat jakautuivat karkeasti ottaen kahteen yhtä suureen ryhmään, niihin joille virtuaalikoneet, -verkot ja testiverkot olivat tuttuja ja niihin, joilla ei ollut niistä niin paljon kokemusta. Vastaajista 53 % oli käyttänyt jotakin testiverkkoa, useimmat heistä pelkästään organisaation sisäistä verkkoa. Myös 53 % vastaajista piti esiasennettua virtuaaliympäristöä hyödyllisenä työkoneellaan, 21 % ei kokenut tällaista ympäristöä tarpeellisena. Kotikäytössä tai etätyössä vastaavaa ympäristöä piti hyödyllisenä suurin osa eli 80 %. Vastaajista 73 % toivoi saavansa valmiiksi asennetun käyttöjärjestelmän, koska se säästäisi aikaa, myös osa lopuista, jotka haluavat säätää itse asetukset kohdilleen, toivoi yksinkertaista käyttöliittymää tähän.

Puolet vastaajista piti tekstipohjaista yhteyttä, kuten SSH, riittävänä ja parhaana vaihtoehtona testiverkkoyhteydeksi. Graafinen työpöytä ei siis vaikuttaisi tällä hetkellä olevan mitenkään vaatimuksena tutkijoiden keskuudessa, 80 % vastaajista piti tekstipohjaisuutta parhaana tai toiseksi parhaana yhteystyyppinä. Sen suosiota selittää tuttuus käyttäjille ja se, että käytettävät ohjelmat ovat lähes aina tekstipohjaisia. Toiseksi suosituin yhteystyyppi kyselyssä oli tässä työssä tutkittava virtuaalikoneen ja VPN-yhteyden yhdistelmä. Seuraavina tulivat pelkkä VPN-yhteys, etätyöpöytäyhteys pääkäyttäjänoikeuksilla, web-käyttöliittymä ja etätyöpöytäyhteys rajoitetuilla oikeuksilla. Hieman yllättäen erillinen fyysinen kone oli vähiten suosittu, ilmeisesti vastaajien tarpeet eivät ole kovinkaan vaativia laitteiston suhteen.

Kyselyn viimeisessä osiossa pyydettiin valitsemaan eri tapauksissa mieluisin vaihtoehto fyysinen koneen, virtuaalikoneen ja etätyöpöytäratkaisun väliltä. Kysymyksessä oletettiin, että tekstipohjainen yhteys ei riittäisi. Tapaukset olivat ohjelmia, jotka rasittavat paljon koneen laitteiston tiettyä komponenttia tai ominaisuutta. Tapaukset olivat suoritinta, muistia, kiintolevyä, verkkoa ja multimediaa rasittavat ohjelmat. Kysymyksenasettelu oli ehkä virtuaalikonetta syrjivä, sillä jokaisessa kohdassa oli ilmoitettuna prosenttiarvo, joka ilmoitti karkeasti suorituskyvyn suhteessa fyysiseen koneeseen. Etäyhteydelle ei asetettu vastaavia lukuja, sillä sen suorituskyky riippuu palvelimesta, ja käyttökokemukseen ei otettu tässä

kohdin kantaa. Kysymyksenasettelu sai myös moitteita vastaajilta epäselvyydestä ja siitä, ettei kysytty oikeita asioita, kuten käyttäjäkokemusta.

Vastauksissa suosittiin selkeästi etätyöpöytää ja fyysistä konetta, kolmeen kuudesta tapauksesta valittaisiin etätyöpöytä, kahteen fyysinen kone, ja yksi meni tasan näiden välillä. Virtuaalikone jäi lähes jokaisessa kohdassa viimeiseksi, mikä onkin ymmärrettävää. Vastauksissa asiaa perusteltiin monesti sillä, että ei haluta virtuaalikonetta viemään kaikkea tehoa kun työskennellään toimisto-ohjelmien parissa. Etätyöpöydän eduksi laskettiin myös sen käytettävyys mistä tahansa. Moni vastaaja myös ilmoitti, ettei tarvitse graafista ympäristöä, vaan pelkkä SSH riittää. Eräs vastaaja toisaalta painotti käyttäjäkokemusta tärkeämpänä, jolloin ei niin haittaa, vaikka virtuaalikone olisikin jonkin verran hitaampi. Graafista käyttöliittymää on mukavampi vain klikkailla kuin muistaa komentorivikäskyt, toisaalta, jos käyttöliittymä on vuorovaikutteinen, niin sen täytyy olla myös vastata syötteeseen nopeasti, kuten luvussa *2.1.2 Etätyöpöytä ja työpöydän virtualisointi* mainittiin.

3.2 Tietoturvapolitiikan asettamat vaatimukset

Tietoturvapolitiikan osalta keskitytään Aalto-yliopiston politiikkaan ja tietoturvaohjeisiin. Jos Aalto-yliopistolla ei ole omia ohjeita, käytetään valtion suosituksia, näin on esimerkiksi salauskäytäntöjen ja etätyöohjeiden kanssa. Muissa organisaatioissa politiikka poikkeaa tässä kuvatusta tai kotikäytössä sitä ei ole. Aalto-yliopiston työasema- (Aalto-yliopisto, 2009) ja ohjelmistopolitiikka (Aalto-yliopisto, 2010) määräävät Aalto-yliopiston työasemien ja ohjelmistojen hankintaa, käyttöä ja hallinnointia ja rajaavat käyttöoikeudet. Ohjelmistopolitiikka astuu voimaan heinäkuussa 2010.

3.2.1 Työasemapolitiikka

Työasemat on luokiteltu neljään eri pääkategoriaan: akateeminen, tutkimus, hallinto ja yleisökäyttöinen. Lisäksi työasema voi olla kiinteä, kannettava, etätyöasema, virtuaalinen tai thin client -tyyppinen.

Akateeminen työasema on työasema, jolla suoritetaan tutkimus- ja opetustoimintaan liittyviä tehtäviä, sen käyttöoikeudet ovat yleensä rajoitetut. Hallintotyöasema on työasema, jolla suoritetaan opetusta ja tutkimusta tukevia hallinnollisia työtehtäviä, sen käyttöoikeudet ovat aina rajoitetut. Yleisökäyttöinen työasema on yleisissä tiloissa sijaitseva ja sekä henkilökunnan että opiskelijoiden käytössä. Kaikki edellä mainitut ovat keskitetysti ylläpidettyjä.

Tutkimustyöasemat eivät ole keskitetysti ylläpidettyjä, sillä niiden käyttötarkoitus vaatii ylläpitotason käyttöoikeuksia tai niiden tietoturvataso ei muuten täytä tietohallinnon vaati-

muksia. Näitä työasemia ei saa liittää työasemaympäristöön, vaan erilliseen tutkimusverkkoon.

Työasemien määrä on pääsääntöisesti rajattu yhteen työasemaan käyttäjää kohden. Lisätyöasemasta määrätään seuraavasti:

”*Lisätyöasemien tarvetta määritettäessä tulee tutkia virtuaalityöasemien soveltuvuus kyseiseen tehtävään. Virtuaalityöasema voi sijaita työasemalla tai palvelimella. Virtuaalityöasemalla voidaan saavuttaa merkittäviä säästöjä niin laitteiden kuin ylläpidonkin osalta. Tässä yhteydessä on kuitenkin varmistuttava emokoneen ja keskitetysti ylläpidetyn työasemaympäristön tietoturvallisuuden säilymisestä. Virtuaalityöasemia ei sallita hallintotyöasemissa, ellei kyseessä ole erillisellä palvelimella toteutettu ratkaisu.*”

Työasemien liittämisestä verkkoympäristöön määrätään seuraavasti:

”*Aalto-yliopiston keskitetysti ylläpidettyyn työasemaympäristöön saa liittää ainoastaan tämän politiikan mukaisia työasemia. Keskitetysti ylläpidettyyn työasemaympäristöön ei saa liittää muita työasemia.*”

Näistä määräyksistä voidaan päätellä, että virtuaalikoneen asentaminen on sallittua ja suositeltua akateemiseen tai yleisökäyttöiseen työasemaan, mutta virtuaalikonetta ei saa liittää työasemaympäristöön ellei se ole keskitetysti ylläpidetty ja politiikan mukainen. Asennus onnistuu myös tutkimustyöasemaan, koska käyttäjällä on yleensä ylläpitotason oikeudet ja hän voi asentaa haluamiaan ohjelmia vapaasti.

Tämän työn ratkaisuun liittyen oleellista on estää pääsy virtuaalikoneesta työasemaverkkoon ja myös estää isäntäkäyttöjärjestelmän pääsy tutkimusverkkoon. Erityisen tärkeää on estää liikenteen reitittyminen työasemaverkon ja tutkimusverkon välillä, jottei kummankaan verkon tietoturvaa vaaranneta.

3.2.2 Ohjelmistopolitiikka

Työasemiin asennettavat ohjelmat voivat olla neljää erilaista tyyppiä: ydin-, perus-, lisä- tai erikoisohjelmisto. Ydinohjelmistoihin kuuluvat valmiiksi asennettavat välttämättömät ohjelmistot, kuten käyttöjärjestelmä. Perusohjelmistoja ovat yleisimpien tehtävien vaatimat ohjelmistot, kuten toimisto-ohjelmat ja Internet-selaimet. Lisäohjelmistoja ovat yleisesti käytettävät ohjelmistot, joita ei tarvita jokaisessa koneessa vaan, jotka asennetaan keskitetysti ylläpidettyihin työasemiin vain tarpeen vaatiessa, esimerkiksi lisenssimäärien vuoksi. Erikoisohjelmistoihin kuuluvat kaikki muut, jotka eivät kuulu edellä mainittuihin kolmeen ryhmään tai jos ohjelmistoa ei voi asentaa keskitetysti. Erikoisohjelmistojen käyttö hoide-

taan virtualisoinnilla tai etäkäytöllä, mikäli se ei ole mahdollista työasema on tutkimustyöasema. Virtualisointi- ja yksityisverkko-ohjelmat kuuluvat lisäohjelmistoihin.

Ohjelmien ylläpidosta vastaa työasemapalveluiden tarjoaja, paitsi yksikön erityistarpeisiin tarkoitetuista lisä- ja erikoisohjelmistoista vastaa yksikkö itse. Tutkimustyöasemien ohjelmistoista vastaavat yksiköt itse, mutta niissä suositellaan käytettävän samoja ohjelmistoja kuin keskitetysti ylläpidetyissä työasemissa. Keskitettyyn ylläpitoon tulevien ohjelmistojen hankinnat tulisi tarkistuttaa työasemapalveluiden tarjoajalla yhteensopivuuden ja tietoturvallisuuden varmistamiseksi.

Tämän työn ratkaisulta vaaditaan siis, että sen käyttö ei vaadi pääkäyttäjän oikeuksia ja että se voidaan asentaa keskitetysti. Lisäksi Aalto-yliopistolla on keskitetty lisenssien hallinta ja tietokanta, mutta koska tässä työssä käytetään vain vapaasti käytettäviä sovelluksia, sen ei pitäisi aiheuttaa ongelmia.

3.2.3 Etäkäyttö

Mikäli testiverkkoon on mahdollista avata yhteys mistä tahansa, on myös pohdittava mitä uhkia siihen liittyy. Valtion etätyön tietoturvallisuusohje (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2002) määrää, että etätyön riskejä täytyy arvioida ja valitsemaan riskeille vastakeinot. Mikäli riskejä ei saada riittävän pieniksi, ei kyseistä työtä voi tehdä etätyönä. Normaaleja tiukempia tietoturvallisuustoimia vaativat esimerkiksi järjestelmien etähallinta ja henkilötietojen käsittely. Kokonaan kiellettyä on salaisten ja erittäin salaisten tietojen käsittely. Etätyön tietoturvan kannalta tärkeimmät asiat ovat käyttäjän tunnistaminen ja verkkoliikenteen salaus ja luottamuksellisuus. Myös etätyöaseman fyysisestä turvallisuudesta täytyy huolehtia, etteivät varmenteet, salausavaimet tai salasanat joudu vääriin käsiin.

Kaikki suositukset on listattu VAHTI-julkaisussa turvallinen etäkäyttö turvattomista verkoista 2/2003 (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2003). Joitakin suosituksia voidaan tosin pitää vanhentuneina, kuten että VPN-ratkaisun täytyisi olla IPsec-pohjainen. Tämän työn kannalta tärkeimpiä suosituksia ovat suositukset käyttää käyttäjän tunnistamiseen julkisen avaimen varmenteita, päätteiden tulisi olla organisaation hallinnoimia laitteita ja että päätelaitteelle ei koskaan tulisi sallia kahta tai useampaa yhtäaikaisesti aktiivista verkkoliitäntää. Verkkoliitäntä pitäisi myös suojata ajan tasalla olevalla virustentorjuntaohjelmistolla ja henkilökohtaisella ohjelmistopalomuurilla. Näin saadaan torjuttua useimmat haittaohjelmat ja hyökkäysyritykset.

Vaikka testiverkkoon olisi mahdollista yhdistää vain organisaation hallinnassa olevista tiloista tai IP-osoiteavaruudesta, ei käyttäjän tunnistautumisesta ole syytä luopua. Näin

varmistetaan, että vain asianmukaisilla henkilöillä on pääsy palveluun. Salauksen tarpeellisuus riippuu lähiverkon luotettavuudesta ja käsiteltävien tietojen laadusta.

3.2.4 Salauskäytännöt

Salauskäytännöt perustuvat valtionhallinnon salauskäytäntöjen tietoturvaohjeeseen (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2008). Salausratkaisujen algoritmeista ja avainpituuksista annetaan yleiset suositukset: salausalgoritmin tulee olla avoin ja avainpituuden tulee olla valittuun algoritmiin nähden riittävän pitkä käyttöhetken käsityksen mukaisesti.

Symmetrisistä algoritmeista suositaan AES-algoritmia, koska se luotettava ja laajasti tuettu, ja vähintään 128-bitin avainpituutta. Muita hyväksyttyjä algoritmeja ovat Twofish, Blowfish ja IDEA. Epäsymmetristen algoritmien ja varmenteiden käyttöä suositellaan, mutta varmenteita myöntävän tahon on syytä olla luotettavaksi tunnettu. RSA-algoritmin avainpituuden ehdottomaksi minimiksi ehdotetaan 1776 bittiä ja riittäväksi minimiksi 2432 bittiä. Tiivistefunktioista suositeltavat algoritmit ovat SHA-256, SHA-384 ja SHA-512 ja avainpituuden tulisi olla kaksinkertainen verrattuna tiedon salaamiseen käytetyn algoritmin avainpituuteen. Suositus perustuu matemaattiseen teoriaan, niin sanottuun syntymäpäiväongelmaan, jossa kahdella 23:sta satunnaisesti valitusta henkilöstä on sama syntymäpäivä yli 50 % todennäköisyydellä. Lisäksi todetaan, että epäsymmetriset algoritmit ovat parhaimmillaan todennuksessa ja symmetriset tehokkaita tietoaineiston salauksessa. Kyseisenlaiseen vahvuuksien hyödyntämiseen tulee pyrkiä kaikissa tilanteissa. (Valtionhallinnon tietoturvallisuuden johtoryhmä, 2008)

Lisäksi käyttötapaukselle, missä päätelaitteelta yhdistetään IP-yhdyskäytävään, eli etäkäyttöyhteys, suositellaan vahvan todennuksen integroinnin mahdollistavaa, avoimia standardeja tukevaa ja markkinoiden kypsäksi osoittamaa ratkaisua. Esimerkkinä ovat kaupalliset ja avoimen lähdekoodin IPsec ja SSL VPN -ratkaisut.

3.3 Ylläpidon vaatimukset

Jotta ratkaisun voisi ottaa laajempaan käyttöön, täytyy sen olla keskitetysti asennettavissa ja hallittavissa. Lisäksi asennettavien ohjelmien lisenssien täytyy sallia keskitetty jakaminen ja asennettavien vieraskäyttöjärjestelmien täytyy olla vapaasti käytettäviä tai niihin tulee hankkia käyttöoikeus.

Ylläpidon näkökulmaa varten haastateltiin järjestelmätukihenkilö Kimmo Pitkäniemeä tietoliikenne- ja tietoverkkotekniikan laitokselta (Comnet). Aalto-yliopiston myötä yliopiston tietohallinnon suositukset ovat muuttuneet määräyksiksi, mutta laitoksilla on silti paljon

vapauksia hoitaa omaa IT-ympäristöään haluamallaan tavalla. Tämän vuoksi ylläpidon työkalut, valmiudet ja oletukset voivat erota eri organisaatioissa huomattavasti. Valtaosa Comnetin keskitetysti ylläpidettävistä tietokoneista on Windows XP ja 7 -koneita. Linux- ja Mac-koneet menevät kokeneille käyttäjille, joten yleensä he saavat pääkäyttäjänoikeudet koneisiinsa. Hallinnon koneita ylläpitää toisaalta Aallon IT-palvelukeskus, eikä hallintotyöasemiin saanut asentaakaan virtuaalikoneohjelmistoa (luku *3.2.2 Ohjelmistopolitiikka*).

Comnetissa ohjelmien asennukset hoidetaan Windowsin ryhmäkäytännöillä (*group policy*), ja jotta ohjelman voisi asentaa, sen täytyy olla saatavilla Windows Installer (MSI) -tiedostona tai tavallisena suoritettavana ohjelmana, jonka asennusta voi ohjata komentoriviparametreilla. Jos ohjelmaa ei voi asentaa edellä mainituin keinoin, sen voi asentaa koneen käyttöönottovaiheessa osana levykuvaa, johon se on valmiiksi asennettu. Jos ohjelman asetuksia täytyy muuttaa asennuksen jälkeen, se onnistuu esimerkiksi komentojonokäskyillä.

Ylläpidon yhtenä tavoitteena voi olla helpottaa omaa työtään yhtenäistämällä ylläpidettävää laitteisto- ja ohjelmistokantaa ja siinä virtualisointi on hyödyllisimmillään. Kun konekantaa uudistetaan, saattaa tutkijan huoneeseen jäädä vanha kone ja sen käyttö voi olla satunnaista, mutta kuitenkin, jos kone on keskitetyn ylläpidon piirissä, se jää jälkeen ohjelmistopäivityksissä ja aiheuttaa harmia ylläpidolle. Kuten Aallon työasemapolitiikassa mainitaan, pitäisi lisätyöasemien osalta aina harkita virtuaalikoneiden käyttöä. Uudet koneet ovat poikkeuksetta riittävän tehokkaita hoitamaan yhtä tai kahta käynnissä olevaa virtuaalikonetta. Siispä ylläpidon kannalta työn ratkaisun helppo asennettavuus voisi tuoda etuja. Toisaalta palvelimella oleva etätyöpöytä voi olla käyttäjälleen ja myös ylläpidolle yhtä hyvä tai parempi, riippuen tilanteesta.

3.4 Lisenssirajoitukset

Ohjelmistolisenssien kanssa täytyy olla tarkkana, mikäli lisenssien ehtoja aikoo noudattaa kirjaimellisesti. Joidenkin ilmaisten ohjelmien ehdoissa sallitaan vain henkilökohtainen asennus ja käyttö, keskitettyyn levitykseen saattaa joutua pyytämään erikseen luvan ohjelmiston jakelijalta. Maksullisten ohjelmien hankkimiseen liittyy aina byrokratiaa ja budjettirajoitteita, joten niitä ei voida pitää vaihtoehtona ilmaisille ratkaisuille tässä tapauksessa, kun kyseessä ei ole kaikille oleellinen, mutta mahdollisesti laajasti levitettävä ratkaisu. Ilmaisten sovellusten käyttäminen oli myös työn rajauksessa mainittu rajoite. Toinen lisensseihin liittyvä asia, joka ei suoraan vaikuta työn ratkaisuun on vieraskäyttöjärjestelmän käyttöoikeus. Vapaassa levityksessä olevat Linux-jakelut, OpenSolaris ja muut vapaat käyttöjärjestelmät voidaan huoletta asentaa vieraskäyttöjärjestelmäksi. Windowsin asentamiseksi vaaditaan kuitenkin lisenssin hankkiminen. Yliopiston volyymilisenssi (*volume licen-*

se) vaatii, että koneessa on jokin Windows-lisenssi jo olemassa, joten periaatteessa volyymilisenssillä ei saa asentaa Windowsia virtuaalikoneeseen. Uusimpia Windows-versioita (Vista, 7, Server 2008) voi tosin käyttää jopa 120 päivää ilman avainta tai aktivointia ja muun organisaation lisenssi saattaa mahdollistaa Windowsin asentamisen volyymikäyttöoikeusavaimella. Applen Mac OS X -käyttöjärjestelmää ei ole mahdollista virtualisoida, sillä lisenssi sallii sen asentamisen vain Applen omaan koneeseen (Apple Inc., 2009, s. 2.A.).

3.5 Laitteistovaatimukset

Tunnetuimpien virtualisointiohjelmien laitteistosuositukset vaihtelevat prosessorin osalta yhden ja kahden gigahertsin välillä ja työmuistin osalta yhden ja kahden gigatavun väliltä. Kirjoittajan kokemuksen mukaan muistia on syytä olla reilusti, etenkin Windowsin uusimmissa versioissa. Kirjoittajan vähimmäissuositus yhdelle virtuaalikoneelle ja Windows XP isäntäkoneelle on kaksi gigatavua ja Vista/7 isäntäkoneelle neljä gigatavua. Ubuntun graafisen työpöydän käyttämiseen vaaditaan 384 megatavua muistia, mitä voidaan pitää minimimääränä, joka täytyy varata virtuaalikoneelle. Windows XP:n virallinen minimisuositus on 128 megatavua, mikä on kirjoittajan mielestä erittäin alakanttiin, jos tarkoitus on myös ajaa ohjelmia.

Microsoft suosittelee Windows vieraalle 15 gigatavua vapaata levytilaa; kokeilussa Windows 7 x64 perusasennus vaati kahdeksan gigatavua levytilaa. Ubuntun perusasennus vie kokeilun perusteella noin kolme gigatavua, joten virtuaalikovalevyn vähimmäiskoon on syytä olla luokkaa kahdeksan gigatavua, joka on Ubuntun pienin suositeltu levytilan määrä. Käyttäjä voi tosin asentaa haluamansa käyttöjärjestelmän, jolloin vaadittu kovalevytila riippuu järjestelmästä ja asennettavista lisäohjelmista.

Virtualisointisovellukset eivät välttämättä vaadi toimiakseen x86-virtualisointilaajennuksia eivätkä peruslaajennukset edes nopeuta virtuaalikoneen toimintaa, vaan saattavat päinvastoin hidastaa virtualisointia (Adams & Agesen, 2006) (VMware, Inc., 2007, s. 6). Virtualisointilaajennusten tuoma hyöty on siinä, että ne tekevät virtualisointialustasta helpommin toteutettavan, mikä tarkoittaa vähemmän kehitettävää koodia ja vähemmän ohjelmointivirheitä. On huomioitava kuitenkin, että 64-bittinen vieraskäyttöjärjestelmä vaatii prosessorilta 64-bittisyyden ja virtualisointilaajennuksen, mutta isäntäkäyttöjärjestelmä voi olla 32-bittinen.

Uusimmissa Intelin Core i7 ja AMD:n Barcelona K10 prosessoreissa on kuitenkin ”*nested paging*” -laajennus (AMD RVI ja Intel EPT), joka nopeuttaa muistinkäsittelyä huomattavasti. VMwaren testien perusteella muistinhallintayksikköä (MMU) kuormittavassa testissä saadaan jopa 48 % nopeusetu (Bhatia, 2009a) (Bhatia, 2009b). Riippumattomassa webpalvelin stressitestissä saavutettiin parhaimmillaan 31 % nopeusetu (De Gelas, 2008). Inte-

lillä on lisäksi Virtual Processor Identifiers (VPID) -laajennus, joka nopeuttaa ympäristön vaihtoja vähentämällä kalliita virtuaalimuistin (*Translation Lookaside Buffer, TLB*) tyhjennyksiä (Sun Microsystems, Inc., 2010b). Intelin mukaan sillä saavutetaan enimmillään 15 % lisähyöty (Gerzon, 2007).

Isäntäkoneen prosessorin on syytä olla kirjoittajan käyttökokemuksen perusteella vähintään kaksiytiminen ja varustettu virtualisointilaajennuksella, sillä työssä valittu VirtualBox-ohjelma ei tue muuten vieraan moniydinprosessointia. Moniydinprosessoinnista (vieraskäyttöjärjestelmässä) on paljon hyötyä, sillä virtualisoinnin tehohäviöt aiheuttavat sen, että muuten isäntäkoneen yksi ydin on usein ylityöllistetty kun muut ovat käyttämättöminä. Näin saadaan tehtyä kuormantasausta isäntäkoneelle ja suorituskyvyn lisäys vieraskoneelle. Varsinkin multimediasovellukset vaativat suorituskykyä prosessorilta, siksi kirjoittaja suosittelee vähintään kahden gigahertsin kellotaajuutta ja *nested paging* -tukea. Tuki ei ole yleinen nykyisin, mutta tulevia laitteistohankintoja ajatellen hyödyllinen ominaisuus virtualisointiympäristössä. Katso alla olevasta taulukosta yhteenveto laitteistosuosituksista.

Taulukko 2: Laitteistosuositukset yleisimpiin käyttöjärjestelmiin

Käyttöjärjestelmä		Virallinen minimisuositus	Kirjoittajan suositus virtuaalikoneelle[5]
Windows XP 32-bit	Muisti	128 Mt	1 Gt
	Prosessori	300 MHz	2-ydin 1,5 GHz
	Levytila	1,5 Gt	8 Gt
Windows 7 32-bit	Muisti	1 Gt	2 Gt
	Prosessori	1 GHz	2-ydin 2 GHz
	Levytila	16 Gt	20 Gt
Ubuntu 9.10 32-bit	Muisti	384 Mt	1 Gt
	Prosessori	700 MHz	2-ydin 2 GHz
	Levytila	8 Gt	8 Gt

3.6 Yhteenveto

Kolmannessa luvussa käsiteltiin ratkaisun käyttötapoja ja odotettavia ominaisuuksia, niin käyttäjien, tietoturvapolitiikan, tietojärjestelmien ylläpidon kuin laitteistovaatimusten kannalta.

Tärkeimpänä ratkaisun käyttötapana on yhdistäminen testiverkkoon ja virtuaalikoneen käyttö käyttäjien testialustana. Käyttäjäkyselyn perusteella, tosin, graafista työpöytää ei

[5] Muistin, levytilan ja ytimien määrä viittaa virtuaalikoneelle määriteltyihin arvoihin, prosessori isäntäkoneen kellotaajuuteen ja ytimien määrään

voida pitää vielä kovin olennaisena testiverkkoyhteyksissä, sillä siihen riittää nykyisin usein pelkkä tekstipohjaisuus. Kuitenkin pelkkä virtuaalikoneen mahdollisuus on jo hyödyllinen olla olemassa käyttäjien koneilla, ja käyttäjät toivoivatkin mahdollisimman helppoa käytettävyyttä ja pääkäyttäjän oikeuksia. Toisaalta mitään raskaita sovelluksia ei haluta missään tapauksessa omaa toimistokonetta rasittamaan.

Aalto-yliopiston ohjelmisto- ja työasemapolitiikka rajaavat yliopiston työasemien käyttöä. Politiikka sallii ja suosittaa virtuaalikoneiden käyttöä, mutta mihin tahansa koneeseen sitä ei voi asentaa. Lisäksi virtuaalikoneita ei saa liittää ylläpidettyyn työasemaympäristöön, siitä huolimatta niiden tietoturvasta tulisi huolehtia. Ratkaisulta vaaditaan toimivuutta peruskäyttäjän oikeuksilla ja sen tulisi olla asennettavissa keskitetysti. Salausalgoritmeista suositellaan käytettäväksi AES:ää vähintään 128-bitin avainpituudella. Etäkäyttöyhteyden tulisi tukea vahvaa tunnistautumista.

Ylläpidon kannalta on tärkeää, että ratkaisun voi asentaa keskitetysti, myös lisenssirajoitukset saattavat tuottaa päänvaivaa. Laitteistovaatimukset eivät ole ehdottomat sinänsä, mutta jotta käyttäjäkokemus olisi edes kohtuullinen, tulisi isäntäkoneessa olla vähintään kaksiytiminen suoritin ja mielellään paljon työmuistia. Lisäksi olisi hyvä, jos suoritin tukisi uusimpia virtualisointilaajennuksia, sillä ne nopeuttavat toimintaa parhaassa tapauksessa huomattavasti.

4 Virtuaaliympäristön toteutus

Tässä luvussa esitellään ratkaisussa käytettävät komponentit, joita on kaksi, VPN-sovellus ja virtualisointisovellus. Lisäksi käydään läpi ja perustellaan käytettävät olennaisimmat asetukset.

4.1 Valitut komponentit

Tässä luvussa esitellään ratkaisussa käytetyt ohjelmat. VPN-ohjelmaksi valittiin avoin OpenVPN ja virtualisointiohjelmaksi Oraclen VirtualBox.

4.1.1 OpenVPN

OpenVPN on avoimen lähdekoodin, GNU GPL -lisensoitu, monipuolinen SSL VPN -ratkaisu, joka sisältää sekä asiakas- että palvelinkomponentit. OpenVPN suunnitteluperiaatteena on ollut modulaarinen rakenne ja monimutkaisuuden välttäminen, siksi siitä on tullut suosittu ratkaisu ja sillä on aktiivinen yhteisö. Koska SSL VPN ei ole standardoitu protokolla, OpenVPN ei ole yhteensopiva IPsecin tai muiden SSL VPN ratkaisuiden kanssa, kuten Microsoftin Secure Socket Tunneling Protocol (SSTP).

OpenVPN tukee sekä verkko- että siirtoyhteyskerroksen tunnelointia eli tunnelin läpi voi siirtää Ethernet-kehyksiä. Tunnelointi tapahtuu oletuksena UDP:n päällä, mutta myös TCP:tä voidaan käyttää. UDP-toteutus ei perustu luvussa 2.2.5 mainittuun DTLS:ään, mutta on kehittäjänsä mukaan samankaltainen (Feilner, 2009, s. 48). OpenVPN toteuttaa SSL:n vaatiman luotettavan kuljetuskerroksen omalla luotettavuuskerroksella. SSL toteutus perustuu avoimen lähdekoodin OpenSSL-työkaluun.

OpenVPN:n ominaisuuksiin kuuluu palvelimen pito vain yhdellä avoimella portilla ja osoitteenmuunnosta (NAT) voi käyttää sekä palvelimen että asiakkaan päässä. OpenVPN mahdollistaa ryhmäkohtaisen pääsynhallinnan joustavilla palomuurisäännöillä ja eri tunnistautumisvaihtoehdot: varmenne, salasana ja älykortti. OpenVPN on saatavilla kaikille yleisimmille työpöytäkäyttöjärjestelmille, kuten Windows, Linux ja Mac OS X ja lisäksi muille alustoille, kuten OpenWRT, Nokian Maemo ja Windows Mobile.

OpenVPN käyttämä protokollapino on dokumentoitu ohjelman kotisivulla epäselvästi, mutta tiedoista päädytään seuraavanlaiseen L2-datapakettiin. Protokollasta huomataan, että se tuottaa 41 tavua ylimääräistä per paketti ja lisäksi IP ja UDP otsikot 28 tavua, yhteensä siis 69 tavua. Tämä ei tosin aivan täsmää kaapattuihin paketteihin joissa oli 2 – 13 lisätavua tähän verrattuna. Dokumentaatiosta ei käy ilmi mitä nämä lisätavut voisivat olla. Taulukos-

sa 3 on avattuna paketin rakenne. OpenVPN-datapaketit lähetetään ilman minkäänlaista luotettavuuskerrosta, signalointipaketit sen sijaan toimitetaan luotettavasti.

Taulukko 3: OpenVPN L2 TLS datapaketti

	Koko tavuissa
pakettityyppi 6-bit + key_id 2-bit	1
aitouskoodi (HMAC)	20
selväkielinen alustusvektori (IV)	16*
järjestysnumero	4
alkuperäinen Ethernet-kehys	14
muut alkuperäiset otsikot ja data	n

salattu

HMAC-suojattu

* riippuu salausavaimesta, pituus on 128 bittiä 128-bittiselle AES avaimelle

L3-datapaketti on IP-otsikolla Ethernet-kehyksen sijaan, lisäksi signalointipaketti on erilainen (esitetty liitteessä D). (OpenVPN Technologies, Inc., 2010) (Snader, 2005)

Vaihtoehdot

OpenVPN oli valittu tähän työhön jo valmiiksi ICT SHOK testbed -projektin puitteissa, toisaalta se on eräs harvoista vapaasti saatavilla olevista VPN-ohjelmistoista, jossa on palvelin- ja asiakaskomponentit. Muita tällaisia ovat avoimen lähdekoodin OpenSwan ja strongSwan IPsec-toteutukset, joista molemmat ovat vain Linuxille. Hajautettua VPN-toteutusta edustavat muun muassa tinc-protokolla ja n2n.

4.1.2 VirtualBox

VirtualBox on Oraclen (ennen Sun Microsystems) ylläpitämä x86-virtualisointisovellus, joka asennetaan olemassa olevaan käyttöjärjestelmään. Tuettuja isäntäkäyttöjärjestelmiä ovat Windows XP ja uudemmat, Linux, Mac OS X ja Solaris. Tuettuja vieraskäyttöjärjestelmiä ovat muun muassa Windows, Linux, Solaris ja jotkin BSD-variantit, mutta ei kuitenkaan Mac OS X. Ohjelma tukee 64-bittisiä isäntä- ja vieraskäyttöjärjestelmiä, suorittimien virtualisointilaajennuksia ja moniydinprosessointia. Tuetuille vieraille on lisäksi oma lisäpalikka (*guest additions*), joka lisää hiiren integroinnin, leikepöydän jakamisen ja muita ominaisuuksia. USB-laitteet voidaan liittää suoraan vieraskäyttöjärjestelmään ilman ajureita isäntäkäyttöjärjestelmässä.

VirtualBoxista on kaksi versiota: avoimen lähdekoodin GNU GPL -lisensoitu versio ja suljetun lähdekoodin versio. Suljettu versio on maksuton henkilökohtaiseen ja akateemiseen käyttöön, ohjelman keskitettyä jakelua ei kielletä, mutta ei erikseen mainita sallituksi-

kaan (Sun Microsystems, Inc., 2008). Versioiden erot ovat etätyöpöytäpalvelimen ja USB-tuen puute avoimesta versiosta.

VirtualBox valittiin koska se on kattavin avoin ja maksuton virtualisointiohjelma, muut varteenotettavat vaihtoehdot olisivat olleet Microsoftin Windows Virtual PC ja VMwaren Player. Toisaalta virtualisointialusta on helppo vaihtaa toiseen, kunhan se tukee verkkoyhteyden siltaamista. Liitteessä A on melko tarkka, muttei täydellinen vertailutaulukko virtualisointiohjelmien eroista.

VMware Player

VMware Player on ominaisuuksiltaan VirtualBoxia vastaava, teknisesti hieman parempi, sillä 3D-tuki on parempi ja moniydinprosessorituki ei vaadi virtualisointilaajennusta. Playeristä puuttuu VirtualBoxiin nähden mahdollisuus ottaa tilannekuvia (*snapshot*), jotka mahdollistavat esimerkiksi muutosten helpon peruuttamisen. Lisäksi VirtualBox tukee useampia isäntäkäyttöjärjestelmiä, mutta toisaalta Player tukee virallisesti useampaa vierasta. Player onkin karsittu versio maksullisesta Workstation versiosta, joka on varauksin ominaisuuksiltaan kattavin ja kehittynein ohjelma kirjoitushetkellä. Tuettuja isäntäkäyttöjärjestelmiä ovat Windows XP ja uudemmat ja Linux. Tuettuja vieraskäyttöjärjestelmiä ovat Windows, Linux ja FreeBSD, Novell NetWare ja Solaris. Playerin lisenssi on VMwaren oma, joka esimerkiksi kieltää ohjelmalla saatujen testitulosten julkistamisen ja ohjelman keskitetyn levityksen ilman VMwaren kirjallista lupaa (VMware, Inc., 2010b).

Virtual PC

Microsoftin Virtual PC toimii vain Windows ympäristössä ja tukee virallisesti vain Windows vieraita. Ohjelmasta on kaksi versiota: vanhempi Virtual PC 2007 ja uudempi Windows Virtual PC. Vanhempi versio on ominaisuuksiltaan suppea ja on suorituskyvyltään heikompi kuin VirtualBox. Uudempi versio vaatii Windows 7 isäntäkäyttöjärjestelmäksi, mutta jää ominaisuuksiltaan selvästi jälkeen VMware Playeristä ja VirtualBoxista (katso liite A taulukko). (Microsoft Corporation, 2010b)

Muut vaihtoehdot

Tunnetuimmista virtualisointisovellusten valmistajista Parallelsilla ei ole tarjota ilmaista ohjelmaa. Parallelsilla olisi Desktop ja Workstation ohjelmat, mutta niitä ei voida edes harkita, koska työn tavoitteena oli ratkaista ongelma ilmaisilla työkaluilla.

Yksi avoimen lähdekoodin vaihtoehto on QEMU, jota voi käyttää virtualisoijana tai emulaattorina. Sen Windows-versiota ei kuitenkaan enää ylläpidetä joten sitä ei oikein voi pitää varteenotettavana vaihtoehtona. (Bellard, 2010) Linuxeissa KVM (*Kernel Based Virtual*

Machine) käyttää QEMU:a (KVM Project, 2010). VirtualBoxin jotkin komponentit perustuvat myös QEMU:n (Sun Microsystems, Inc., 2010c). Lisäksi on tarjolla pelkästään emulaattori-tyyppinen Bochs, joka erittäin raskas virtualisointiratkaisuihin nähden. (The Bochs Project, 2010)

4.2 Asennus ja asetukset

Tässä luvussa käydään läpi valittujen komponenttien asennukseen liittyvät asiat ja millaisia asetuksia ohjelmiin täytyy tai on hyödyllistä tehdä.

4.2.1 Virtuaalisen verkkosovittimen sijoitus

VPN-asiakas voidaan asentaa kahteen paikkaan, joko isäntä- tai vieraskäyttöjärjestelmään. Sijaintipaikoilla on muutamia oleellisia eroavuuksia. Ensinnäkin, järjestelmään, johon VPN-ohjelma asennetaan, tulee yksi ylimääräinen verkkoliitäntä. Useampi aktiivinen verkkoliitäntä voi aiheuttaa liikenteen reitittymisen ei-toivotun liitännän kautta, mikä on ongelmallista varsinkin, jos käytettävää ohjelmaa ei ole mahdollista sitoa (*bind*) tiettyyn paikalliseen osoitteeseen (tai liitäntään). Toiseksi, mikäli VPN-asiakas olisi vieraassa, pitäisi käyttäjän osata ja muistaa asentaa se jokaiseen virtuaalikoneeseen tai käyttäjille pitäisi olla saatavilla valmiita levykuvia. Jos VPN-asiakas on asennettu ylläpidon toimesta isäntäjärjestelmään, niin käyttäjän ei tarvitse huolehtia muusta kuin varmenne- ja asetustiedostojen kopioimisesta oikeaan hakemistoon.

VPN-asiakkaan sijoittaminen isäntäjärjestelmään on edullista sekä tietoturvan ja käytettävyyden kannalta. Virtuaaliselta verkkosovittimelta voi poistaa IP-protokollat käytöstä, jolloin sovitin ei varaa resursseja VPN-palvelimen päästä, eikä isäntäjärjestelmästä ole, edes vahingossa, mahdollista liikennöidä testiverkkoon suoraan. Virtuaalikone asetetaan siltaamaan vieraan verkkosovitin isännän virtuaaliseen sovittimeen. Tällöin vieras näkee vain yhden verkkoliitännän, joka saa osoitteensa automaattisesti VPN-palvelimelta tai testiverkon DHCP-palvelimelta.

Ongelmaksi voi muodostua, jos tarvitaan yhteys useampaan testiverkkoon samanaikaisesti, koska tällöin tarvitaan yksi virtuaalinen verkkosovitin jokaista testiverkkoa kohden. Käyttäjä ei voi itse lisätä verkkosovittimia ilman pääkäyttäjän oikeuksia, joten ylläpidon pitäisi lisätä ne käsin.

4.2.2 OpenVPN

OpenVPN:ää voi käyttää joko suoraan komentoriviltä tai sen voi asettaa Windowsin palveluksi. Ohjelman voi käynnistää komentoriviltä antamalla kaikki yhteysparametrit, mutta helpoiten asetukset voidaan määritellä tallentamalla ne tekstitiedostoon. Palveluna OpenVPN hakee asetukset ennalta määrätystä hakemistosta ja käynnistää VPN-tunnelin tai tunnelit automaattisesti, mikäli palvelu on asetettu käynnistymään automaattisesti. Asetustiedoston tiedostopääte on Windows-versiossa ”*ovpn*” ja Linux-versiossa ”*conf*”. Käytettävät yhteysparametrit määrittelee palvelin ja niiden täytyy olla samat asiakkaan päässä, palvelin voi myös pakottaa asiakkaalle joitakin asetuksia vaikka asiakas olisi toisin määritellyt. Asetustiedosto on Tulevaisuuden Internet -testiverkossa tarkoitus saada samasta paikasta kuin avaintiedostot. Liitteessä B on esitetty malliasetukset palvelimelle ja asiakkaalle.

Palvelin

Palvelimen asetusten läpikäynti ei sikäli ole tämän työn kannalta oleellista, mutta palvelimen asetusten täytyy olla tietyllä tavalla, jotta Ethernet-tunnelointi toimii, ja asiakkaan asetukset ovat riippuvaisia palvelimen asetuksista.

Tunnelointikerroksen määrittää TAP/TUN -rajapinta-asetus; TUN-rajapinta tunneloi L3 IP-paketteja ja TAP-rajapinta L2 Ethernet-kehyksiä. Tutkimuskäytössä on hyödyllistä, että verkko on mahdollisimman avoin, joten Ethernet-kehysten tunnelointi on parempi ratkaisu, sillä se mahdollistaa verkkokerroksen (L3) protokollien tutkimisen. OpenVPN:lle täytyy kertoa, että halutaan muodostaa sillattu yhteys ”*server-bridge*”-muuttujalla ja lisäksi virtuaalinen verkkoliitäntä pitää sillata halutun Ethernet-liitännän kanssa.

Tunnelointiin käytettävä kuljetuskerroksen protokolla voi olla joko UDP, joka on oletusasetus, tai TCP. UDP on kaikin puolin parempi valinta; syyt on kerrottu luvussa *2.2.5 SSL VPN*. Lisäksi palvelin tarvitsee varmentajan varmenteen (*certificate authority*), oman varmenteen, joka on kyseisen varmentajan allekirjoittama ja Diffie-Hellman avaimenvaihtoparametrit. Kyseisten tiedostojen luonti onnistuu OpenVPN:n ohessa tulevilla työkaluilla.

Asiakas

OpenVPN ei ole saatavilla Windows Installer -pakettina, eikä asennuspaketille ilmeisesti voi antaa parametreja, joten keskitetty asennus saattaa vaatia ylimääräistä vaivaa. Tämän työn puitteissa ei ehditty tutkia asiaa tarkemmin, joten asian kokeileminen käytännössä jää myöhemmäksi selvitykseksi. OpenVPN asentamisessa asiakkaalle voidaan tietyt komponentit jättää asentamatta, näitä ovat: RSA-varmenteiden hallintakomentojonot, tiedostopäätteen hallinta ja OpenSSL-työkalut.

OpenVPN:n asennus luo uuden virtuaalisen verkkokortin, joka on ”*TAP-Win32 Adapter V9*” -niminen OpenVPN 2.1.1 Windows-versiossa. Se on kuin mikä tahansa fyysinen verkkokortti Windowsin kannalta. Kuten edellisessä luvussa mainittiin, tältä kortilta voi poistaa IP-protokollat ja muut ylimääräiset palvelut asennuksen jälkeen, mikä onnistuu ylläpitäjältä komentorivikäskyillä.

Vaadittavia asetuksia on yksinkertaisimmillaan hyvin vähän. Asiakkaan päässä tarvitsee määritellä, että ollaan asiakas-tilassa, käytetäänkö TAP- vai TUN-rajapintaa, käytetäänkö UDP- vai TCP-protokollaa tunnelointiin, palvelimen yhteysosoite, varmenne- ja avaintiedostot ja käytetty salausstandardi. Tunnelointiasetus täytyy olla kuten palvelimessa eli TAP ja protokollan UDP.

Varmenne- ja avaintiedostot saadaan OpenVPN-palvelimen ylläpitäjältä jollakin tavalla, miten tarkalleen ottaen ei kuulu tähän työhön rajauksen puitteissa. Luvussa *2.3.2 PurpleNet* on kuitenkin esitelty eräs mahdollinen tapa. Salauskäytäntöjen suositusten mukaisesti (katso luku *3.2.4 Salauskäytännöt*) salausstandardiksi on valittu AES 128-bittisellä avaimella.

Ohjelmaa on helpointa käyttää graafisen käyttöliittymän kautta (OpenVPN GUI), käyttöliittymä asentuu ohjelman mukana ja pikakuvake lisätään Käynnistä-valikkoon. OpenVPN:ää voidaan käyttää joko suoraan ohjelmatiedoston kautta tai Windows-palvelun kautta. Seuraavassa on ohjeet kummankin tavan käyttöön.

Suorittaminen palveluna

Ylläpitäjän pitää antaa käyttäjille oikeudet käynnistää ja pysäyttää OpenVPN-palvelu ryhmäkäytäntöjen kautta. Palvelulle pitää kertoa, että asetustiedostot löytyvät käyttäjän kotihakemistosta (tai muusta sopivaksi katsotusta hakemistosta). Tämä onnistuu muuttamalla rekisteristä avainta

HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN\config_dir

(esimerkiksi ympäristömuuttujalla *%userprofile%* voidaan viitata käyttäjän kotihakemistoon). OpenVPN GUI:lle täytyy kertoa, että se ohjaa palvelua eikä itse ohjelmaa, se onnistuu asettamalla rekisteristä avain

HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN-GUI\service_only

arvoon *1*.

Suorittaminen ohjelmatiedostosta

Koska OpenVPN GUI etsii asetustiedostoja oletuksena OpenVPN-ohjelmakansiosta, jonne peruskäyttäjällä ei ole käyttöoikeuksia, niin Käynnistä-valikon pikakuvakkeeseen kannattaa

lisätä komento ”*--config_dir %userprofile%\openvpn*”. Tämä ohjaa etsimään asetustiedostoja käyttäjän kotihakemiston alta *openvpn*-hakemistosta, joka täytyy luoda erikseen.

4.2.3 VirtualBox

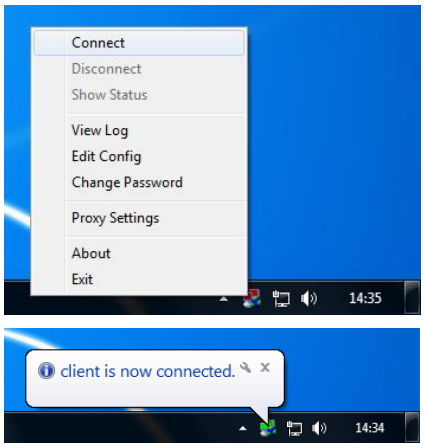
VirtualBoxin saa Windows Installer -pakettina, joka siis mahdollistaa ohjelman keskitetyn jakelun ryhmäkäytäntöjen kautta. VirtualBox asentuu keskitetysti oletuksena siten, että siltaavan verkkoliitännän käyttö ei ole mahdollista. Ohjelmalla on VBoxManage-hallintakäyttöliittymä, josta asian voi oletettavasti muuttaa ”*--nic1 bridged*” -komennolla tai Windowsin rekisteristä. Siltaus on käytössä, jos ohjelma asennetaan paikallisesti pääkäyttäjänoikeuksilla, eikä hallintakäyttöliittymää ehditty tutkia enempää, joten keskitetyn asennuksen siltauksen päälle kytkeminen jää myöhemmäksi selvitykseksi.

Asennus luo useita virtuaalisia laitteita, joiden ajureiden asennus pitää hyväksyä, jos ohjelma asennetaan paikallisesti. Laitteistohallinnassa näkyy vain verkkolaite ”*VirtualBox Host-Only Ethernet Adapter*”.

Liitteessä C on listattuna suorituskyvyn ja toimivuuden kannalta edullisimmat asetukset. Tärkein asetus lienee liittää verkkokortti OpenVPN:n virtuaalisen verkkokortin kanssa ja laittaa se sillattuun tilaan.

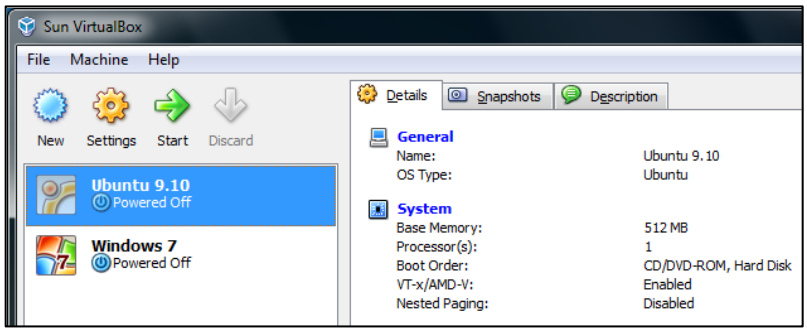
4.3 Käyttö

Ratkaisun käyttäminen on tarkoitus olla melko yksinkertaista. Kunhan käyttäjä on ensin kopioinut VPN-yhteyden asetukset ja avaimet oikeaan hakemistoon, hän voi käynnistää tilailmaisinalueella olevasta OpenVPN GUI -kuvakkeesta yhteyden yksinkertaisesti valitsemalla *Connect*, kuten kuvassa 8.



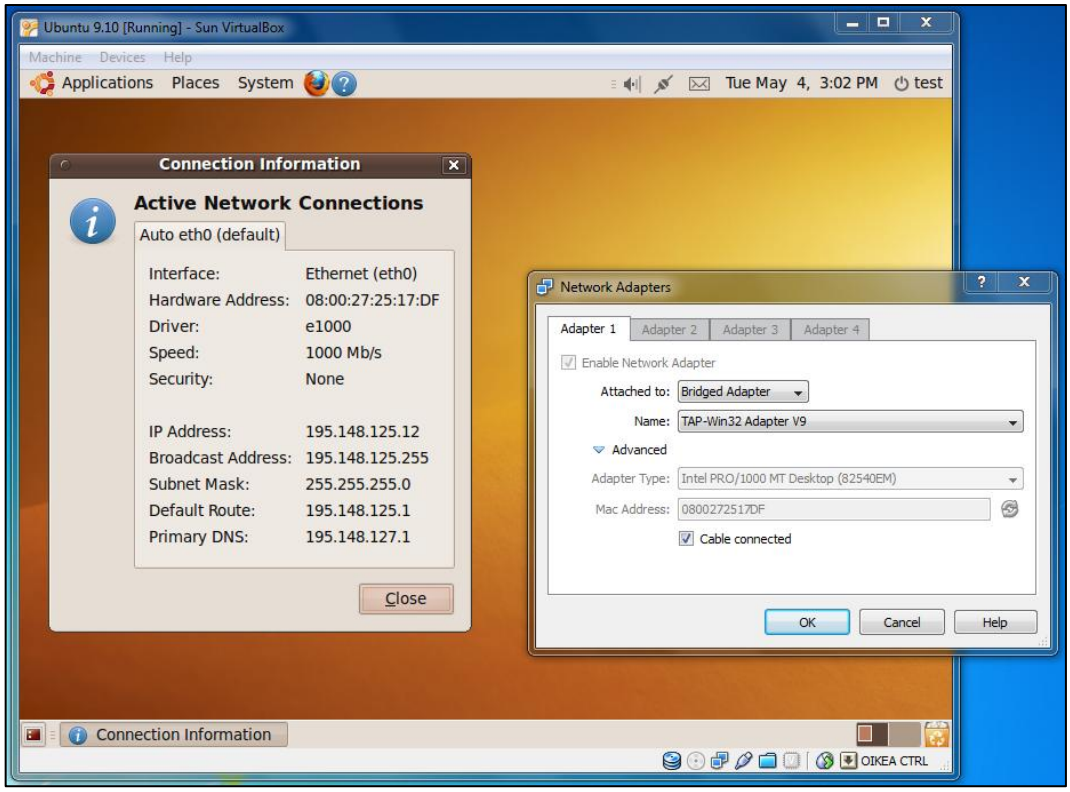
Kuva 8: Yhteyden avaus käyttäen OpenVPN GUI:ta

Yhteyden ollessa avoin, voidaan VirtualBoxin käyttöliittymästä käynnistää haluttu virtuaalikone (kuva 9). Kyseinen virtuaalikone on pitänyt ensin tietysti luoda.



Kuva 9: Osa VirtualBoxin käyttöliittymää

Virtuaalikoneen käynnistyttyä Ubuntu-vieras on käynnissä ja valmis käytettäväksi Windows-isännässä. Vieras näkee vain VPN-yhteyden mukaisen verkkokortin ja -yhteyden (kuva 10).



Kuva 10: Käynnissä oleva Ubuntu-virtuaalikone; verkkoyhteys on VPN:n kautta, mutta sitä ei huomaa virtuaalikoneesta käsin

4.4 Yhteenveto

Neljännessä luvussa käytiin läpi ratkaisun komponentit ja niiden asetukset. Ratkaisun perustan muodostavat avoimen lähdekoodin SSL-pohjainen VPN-ohjelma OpenVPN ja virtualisointiohjelma VirtualBox, josta on saatavilla avoimen ja suljetun lähdekoodin versiot. OpenVPN:lle ei ollut varsinaisesti muita päteviä vaihtoehtoja, joten se oli itsestään selvä valinta. VirtualBoxin valinta ei ollut itsestään selvää, mutta VMware Playerin huonommat lisenssiehdot ja huonompi säätövara vaikuttivat sen valitsemista vastaan. Ohjelmien keskitettyä asennusta ei ehditty kokeilla, mutta pääpiirteissään asian pitäisi olla melko yksinkertaista. Molempien ohjelmien asetuksissa on pientä säädettävää, jotta ratkaisun osat saadaan toimimaan yhteen halutusti.

5 Arviointi

Tässä luvussa arvioidaan ratkaisun onnistuneisuutta mittauksin, pohtimalla tietoturvariskejä, sen etuja sekä huonoja puolia, tavoitteiden täyttymistä ja vertailulla vaihtoehtoisiin ratkaisuihin.

5.1 Mittaukset

Virtualisointi heikentää suorituskykyä väistämättä verrattuna paljaaseen ympäristöön. Seuraavissa luvuissa esitellään muutamia mittaustuloksia, jotka keskittyvät vertaamaan loppukäyttäjän näkemää suorituskykyä. Suorittimen ja muistin mittauksessa on tosin tyydytty synteettisiin testeihin. Kirjallisuudesta löytyy enemmän ja tarkemman tason testejä (Barham, ym., 2003) (Domingues;Araujo;& Silva, 2009), mutta tulokset ovat yhteneväisiä; suoritinrajoitteisissa tehtävissä tehohäviö ei ole niin suuri kuin I/O-rajoitteisissa. Tämä johtuu siitä, että kaikki I/O-komennot täytyy kierrättää suorittimen kautta. Parhaimmillaan näissä testeissä saavutettiin yli 90 % hyötysuhde prosessoritesteissä, ja heikoimmillaan noin 10 % hyötysuhde verkon läpäisykyvyssä. Peruskäytössä, kuten nettiselauksessa, virtuaalikoneen suorituskyky useimmiten riittää täysin sujuvaan käyttäjäkokemukseen, mutta tahmeuden huomaa toisinpaikoin, esimerkiksi vierityksen hitautena.

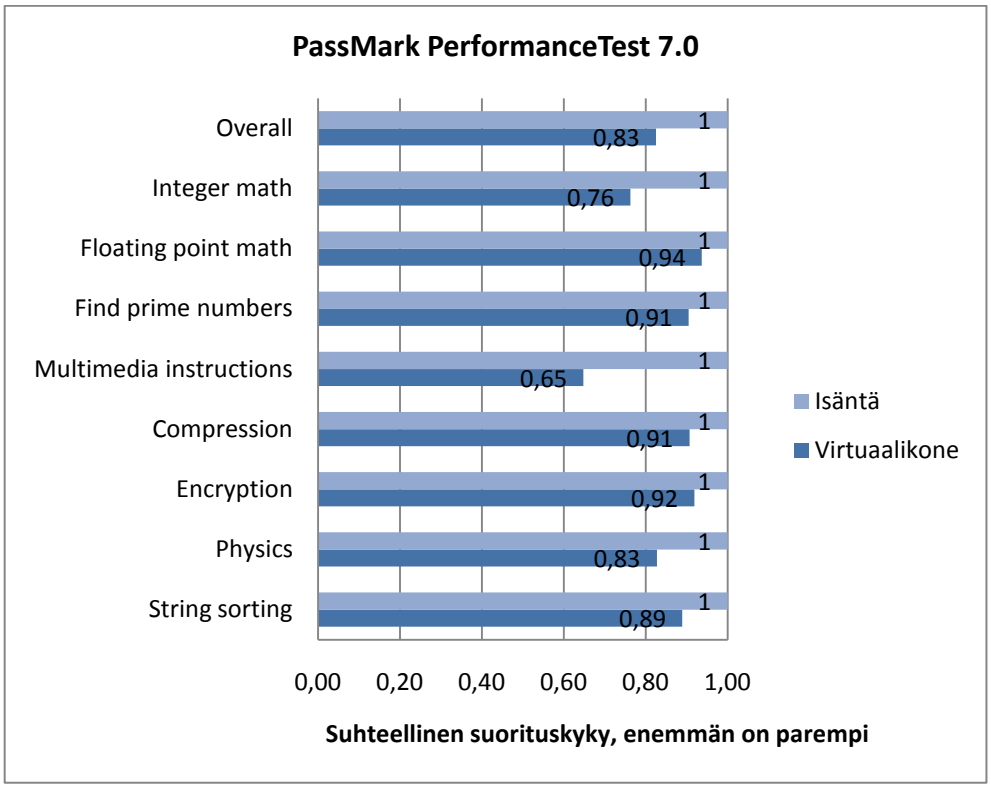
Kokeiden aikana havaittiin, että VirtualBoxin virtuaalikoneen kello jää jälkeen, jos virtuaalikoneen pysäyttää, virtuaalikoneen suorituksen jatkaminen taas aiheuttaa kellon edistämisen (virtuaalikoneen kellon sekunti on 2/3 oikeasta sekunnista) kunnes oikea kellonaika saavutetaan. Tämä aiheuttaa vääristymiä esimerkiksi videontoistossa. Internetin keskustelupalstoilla on vastaavanlaisia kokemuksia eri virtualisointialustoista ja vierasjärjestelmistä, joten kellon edistäminen tai jätättäminen ei ole poikkeuksellista. Tämän vuoksi virtualisointia ei välttämättä voi käyttää aikakriittisten sovellusten suorittamiseen ja kellon epätarkkuus saattoi aiheuttaa myös erikoisia tuloksia synteettisiin testeihin.

Laitteisto
Intel Q8200 4-ytiminen 2,33 GHz (ei VT-x tukea)
4 Gt DDR2 667 MHz RAM
Intel GM4500 integroitu näytönohjain
Western Digital RE3 250 GB (WDC WD2502ABYS)

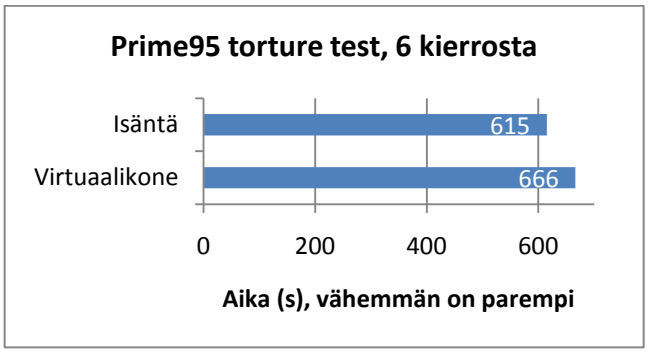
Ohjelmisto
Isäntä: Windows 7 Enterprise 64-bit
Vieraat: Windows 7 Enterprise 32-bit ja Ubuntu Desktop 9.10 32-bit
OpenVPN 2.1.1 ja VirtualBox 3.1.4

5.1.1 Suoritin

Suoritintesteinä käytettiin alkulukuja laskevaa Prime95 ohjelmaa ja sen *torture test* -rasitustestiä ilman muistin rasitusta ja PassMarkin PerformanceTest 7.0:aa, joka erottelee nopeudet eri osa-alueisiin. Prime95 testissä virtuaalikone saavuttaa noin 92 % isäntäkoneen suorituskyvystä (kuva 12), ajat mitattiin käsiajanotolla, jotta mahdollinen kellovirhe ei vaikuttaisi. PerformanceTest antaa kokonaistulokseksi 83 % isäntäkoneen tehosta, alkulukujen laskemisesta PerformanceTest antaa saman tuloksen kuin Prime95, joten testiä voidaan pitää melko luotettavana. Ainut poikkeava tulos saadaan multimediakäskyjen kohdalla, joissa saadaan vain 65 % hyötysuhde. Ohjelman asetuksista asetettiin testi käyttämään vain yhtä ydintä isäntäkoneessa, jolloin tuloksista saatiin vertailukelpoiset (kuva 11).



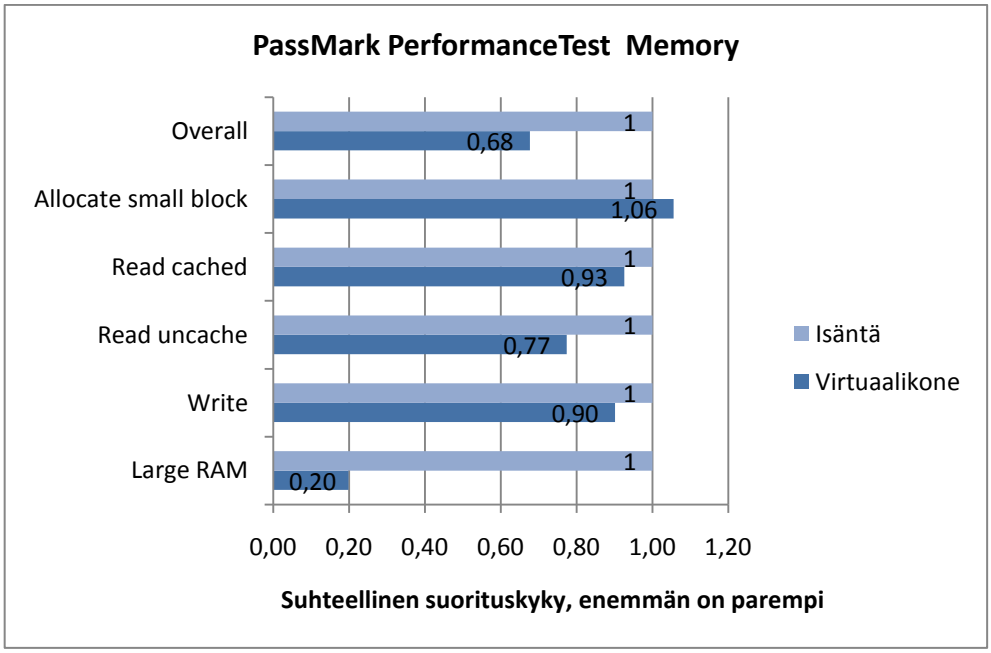
Kuva 11: Suorittimen suhteellinen nopeus virtuaalikoneessa



Kuva 12: Alkulukujen laskemiseen kulunut aika

5.1.2 Muisti

Muistin nopeuden mittaaminen käytännön testissä on vaikeaa, joten päädyttiin ajamaan synteettinen muistitesti PassMark PerformanceTest 7.0 ohjelmassa. Kokonaistehokkuus virtuaalikoneessa on 68 % isäntäkoneen tehosta, mutta yksityiskohtaiset tulokset vaihtelevat paljon. Pienen muistilohkon varaamisessa virtuaalikone oli jopa nopeampi, mahdollisesti virtuaalikoneen optimointien vuoksi. Large RAM -testissä suorituskyky oli toisaalta erittäin heikkoa, vain 20 % normaalista, testi mittaa suuren muistimäärän varaamista ja sen lukemista, joka vastaa paljon muistia käyttävää ohjelmaa. Kuvassa 13 on esitelty tarkemmat tulokset.



Kuva 13: Muistin suhteellinen nopeus virtuaalikoneessa

5.1.3 Verkko

Verkkomittauksissa mitattiin virtuaalikoneen ja VPN-tunnelin vaikutukset erikseen, jotta saataisiin paremmin selville komponenttien häviöt. Todellisuudessa virtuaalikoneen verkkoyhteys on tarkoitus kulkea vain VPN-tunnelin läpi. Koska verkkomittausten absoluuttinen suorituskyky riippuu laitteiston, verkkoyhteyksien ja ohjelmien nopeuksista, näiden mittausten tarkoitus on selvittää suuntaa antavasti VPN-yhteyden ja sen asetusten ja virtuaalikoneen vaikutus suorituskykyyn.

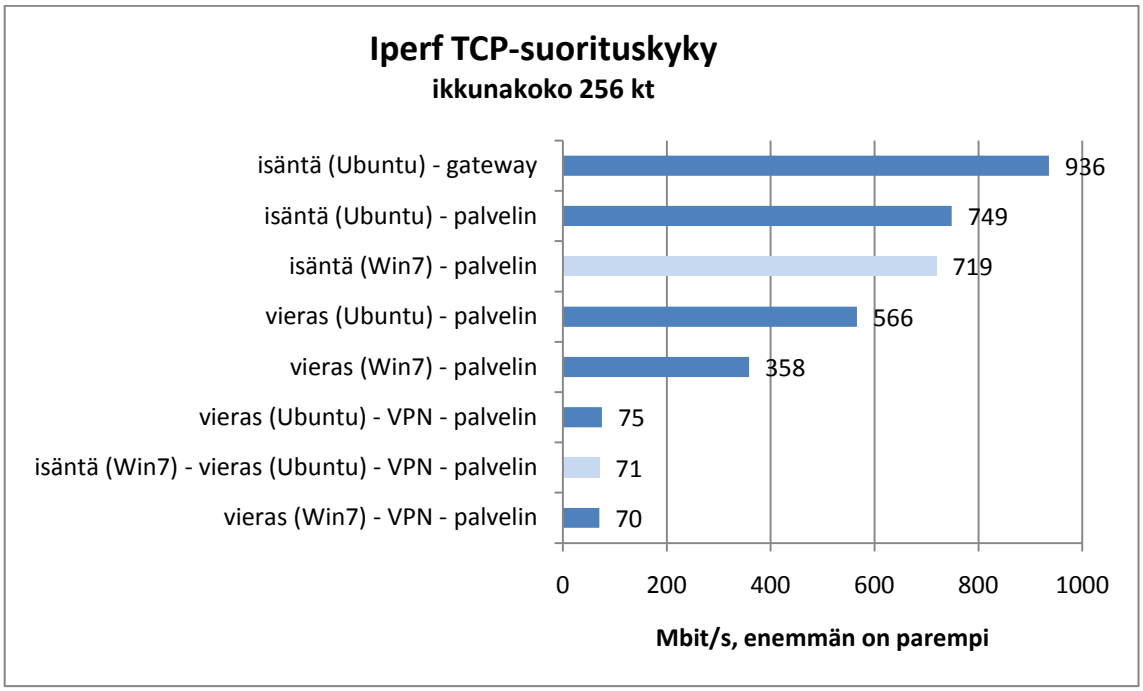
Mittauksissa käytettiin laitoksen (Comnet) virtualisoitua OpenVPN-palvelinta (Debian) vastaanottajana, jolloin VPN-liikennettä ei tarvinnut välittää eteenpäin ja tulokseen siltä osin ei vaikuttanut muita muuttujia. Testikone oli samassa verkossa palvelimen kanssa, ja yhteysnopeus oli yksi gigabitti sekunnissa. Poikkeuksellisesti testit suoritettiin Ubuntu 9.10 -ympäristössä, sillä Windowsissa oli suorituskykyongelmia. Ongelmien syyksi osoittautui pääosin vanha Iperf-versio, joka toimi hitaasti uudemman version kanssa. Lopulta Windows-testit päädyttiin ajamaan Cygwin[6]-ympäristössä, jossa oli sama Iperf-versio kuin Linux-koneissa. Cygwin-ympäristön vaikutus testituloksiin on tuntematon. Iperf versio oli 2.0.4 ja VirtualBoxin versio oli 3.0.8 OSE.

OpenVPN-yhteyden liikenteen pakkaus vaikuttaa saavutettuun nopeuteen, mikäli liikenne on pakkautuvaa. Testeissä pakkausta ei käytetty, sillä sen ei haluttu vääristävän tuloksia. Yhteyden salauksen poistolla ei ollut mainittavaa vaikutusta saavutettuihin nopeuksiin, kaikissa mittauksissa on siis käytetty AES-128 salausta.

TCP

Mittaukset suoritettiin Iperf-mittausohjelmalla ajamalla kymmenen sekunnin TCP-lähetystesti useita kertoja ja ottamalla tuloksista keskiarvo. TCP-mittausten vertailuarvoksi suoraan testikoneesta yhdyskäytäväkoneelle tehdyssä mittauksessa saatiin 936 Mb/s. Virtuaaliselle OpenVPN-palvelimelle saadaan vielä 749 Mb/s. Palvelinvirtuaalikoneen vaikutus suorituskykyyn on siis noin 20 %, myös asiakasvirtuaalikoneen osuus on suunnilleen sama, ja näiden yhteisvaikutus on 40 % (Ubuntu virtuaalikoneesta OpenVPN palvelimelle, 566 Mb/s). VPN-tunnelin kanssa suorituskyky suorastaan romahtaa, alle kymmenesosaan alkuperäisestä, ollen vain 75 Mb/s Ubuntu-vieraassa. Vertailun vuoksi mittauksia suoritettiin myös Windows-isännällä ja vieraalla, tulokset olivat pääosin heikompia kuin Ubuntulla. Kuvassa 14 esitetään mittaustulokset.

[6] Cygwin on Linux-ympäristöä emuloiva komentotulkki ja työkalukokoelma Windowsille



Kuva 14: Mittaustulokset, TCP-suorituskyky, isäntänä toimi Ubuntu, jos ei muuta mainittu

Paluusuuntaa ei erikseen mitattu, mutta kokeilujen perusteella tulokset ovat hyvin samankaltaisia. Suorituskykyä yritettiin parantaa muuttamalla virtuaalikoneessa verkkokortin asetuksia, lähinnä poistamalla tarkistussummien laskenta verkkokortilta, mutta tällä ei ollut vaikutusta. OpenVPN huolehtii pakettien osittamisesta, eikä käsisäätöön ollut tarvetta. Vaikka suorituskyky laskee dramaattisesti, täytyy huomioida, että reilu 70 Mb/s nopeus riittää kuitenkin moneen tehtävään. Mikäli liikennöintinopeutta tarvitaan enemmän, niin ohjelmistopohjainen VPN-ratkaisu täytyy korvata jollakin muulla ratkaisulla. OpenVPN:llä on huonompi suorituskyky kuin IPsec-ratkaisulla, tämä johtuu siitä, että IPsec toimii käyttöjärjestelmäydintasolla ja OpenVPN käyttäjätasolla, siten sillä on enemmän suorittimen ympäristön vaihtoja, mikä vie aikaa jokaisen paketin kohdalla (Škoberne, 2008).

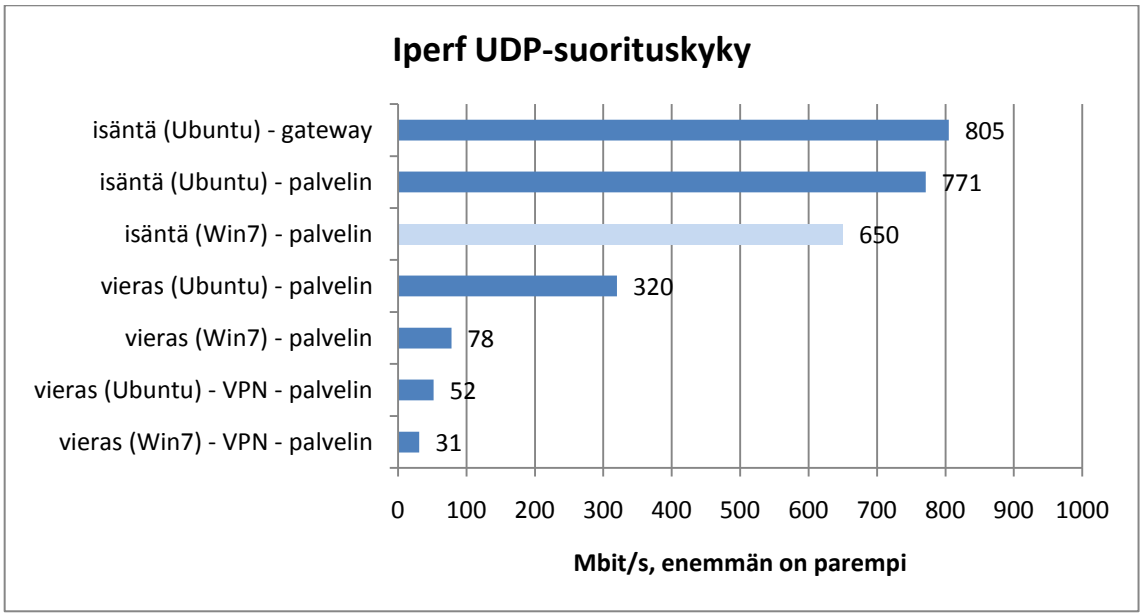
UDP

UDP-mittaukset suoritettiin samalla ohjelmalla haarukoimalla suurinta mahdollista liikenteen läpäisykykyä tarjoamalla UDP-liikennettä eri nopeuksilla ja tarkastelemalla saavutettua nopeutta vastaanottajan päässä ja hävinneiden pakettien osuutta.

Mittaukset osoittautuivat haastaviksi, koska liikenne ei toiminut täysin odotetulla tavalla. UDP on yhteydetön protokolla, joten lähettäjä ei saa protokollan puolesta mitään tietoa menevätkö lähetetyt paketit perille vai eivät. Niin ikään lähettäjä voi lähettää millä tahansa no-

peudella minkä paikallinen verkkokortti mahdollistaa, koska UDP ei tue ruuhkanhallintaa. Mittauksissa ilmeni kuitenkin, että jokin rajoittaa UDP-lähetysnopeutta erikoisesti siten, että paketteja ei juuri häviä eli liikenne käyttäytyy kuin protokollassa olisi ruuhkanhallinta. Ominaisuus ei ollut riippuvainen VPN-tunnelista. Alla olevaan kaavioon on koottu mittaustulosten pääkohdat, tulokset ovat käsin haarukoituja, siten että hävikki on enintään 2 % luokkaa.

Vertailuarvoksi saatiin tällä kertaa 805 Mb/s testikoneesta yhdyskäytäväkoneelle, virtuaalikone palvelimen päässä pudottaa suorituskykyä vain 4 %. Virtuaalikone asiakkaan päässä toisaalta tiputtaa suorituskykyä 58 %. VPN-tunnelin kanssa suorituskyky on enää 6 % alkuperäisestä läpäisykyvystä. Windows on jälleen Ubuntua hitaampi. Kuvassa 15 esitetään mittaustulokset.

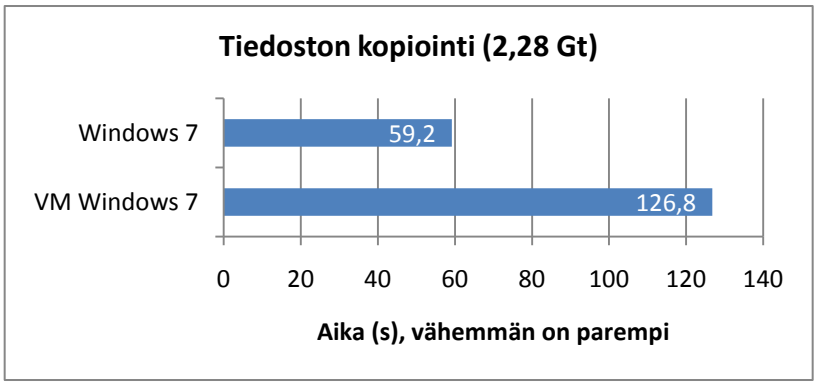


Kuva 15: Mittaustulokset, UDP-suorituskyky, isäntänä toimi Ubuntu, jos ei muuta mainittu

5.1.4 Kiintolevy

Levyoperaatioiden nopeutta mitattiin tekemällä 2,28 gigatavun kokoisesta tiedostosta kopio samalle levylle. Testi mittaa samalla kertaa luku- ja kirjoitusnopeuden. Tällaiseen testiin päädyttiin, koska synteettiset testit antoivat erikoisia tuloksia, mahdollisesti liittyen kellon epätarkkuuteen. Kopiointi tehtiin viidesti ja tuloksista otettiin keskiarvo, ajat mitattiin käsiajanotolla. Kuten alla olevasta kuvasta (kuva 16) nähdään, on virtuaalikoneen keskimääräinen aika yli kaksinkertainen normaaliin nähden. Normaalissa järjestelmässä ajallinen vaihtelu oli huomattavasti pienempää, noin kaksi sekuntia keskiarvosta molempiin suuntiin. Virtuaalikoneen tulokset vaihtelivat 68 – 168 sekuntiin. Kyseisenkaltaiseen mittaukseen

liittyy niin paljon muuttujia, että tulosta voidaan pitää lähinnä suuntaa antavana, virtuaalikoneessa esimerkiksi suoritinkäyttö oli kopioinnin aikana 100 %. Toisaalta asiaan vaikuttavat käyttöjärjestelmien välimuistin toiminta, muut levyä käyttävät prosessit, kuten virustorjunta, ja virtuaalikoneen asetukset, kuten levyohjaimen ja levyn tyyppi. Vastaavanlaista tiedoston kopiointia kokeiltiin myös virtualisointia tukevassa koneessa ja kolmella prosessoriytimellä, tulokset olivat vastaavia. Vaikka suoritintehoa oli teoriassa kolminkertaisesti, vei kopiointi edelleen lähes kaiken suoritinajan.



Kuva 16: Tiedoston kopiointiin kulunut aika

5.1.5 Multimedia

Multimedian toimivuutta testattiin lähinnä subjektiivisesti toistamalla eri resoluutioilla ja algoritmeilla pakattuja videotiedostoja ja nettivideoita. Samalla testattiin ryhmälähetyspohjaisen IPTV:n toiminta, Windows Aero -tuki ja 3D-tuki.

Matalahkon resoluution Xvid-pakattu video toistuu sulavasti testikokoonpanolla ilman ongelmia. Teräväpiirtoresoluution, 720p (numero viittaa videon pystyresoluutioon, kirjain lomittamattomaan kuvaan) x264-pakattu video tuottaa enemmän vaikeuksia ja purkavan koodekin valinnalla on jo merkitystä. Videon saa kuitenkin toistumaan sulavasti oikeilla ohjelmavalinnoilla.

Nettivideoista kokeiltiin Applen web-sivulta elokuvien ennakkomainoksia ja YouTuben videoita eri laaduilla. Apple käyttää teräväpiirtovideoissaan omaa H.264-yhteensopivaa koodekkia, joka on tunnetusti melko laskentaintensiivinen, ja videotoistimena oli Applen oma QuickTime. Vaativuuden vuoksi edes 480p-merkityt videot eivät toistuneet kuvan osalta sujuvasti. YouTube käyttää videoissaan myös H.264-koodekkia ja resoluutioista löytyy monesti useampi vaihtoehto riippuen millä laadulla video on palveluun lähetetty. Videotoistimena toimii Adoben Flash Player -selainlisäosa. 360p versio toistui ongelmitta, kuten myös 480p. 720p versio oli jo häiritsevästi pätkivä, eikä 1080p versiota ollut syytä

edes kokeilla. Täydenruudun tilassa 480p-resoluutio ei toiminut lainkaan, suoritinteho ei vain riittänyt.

Kaikissa testeissä tuli ilmi, että virtualisointi ja videontoisto, varsinkin ilman virtualisointitukea prosessorilta, vaatii todella paljon laskentatehoa. Lisäksi videoiden suoratoisto oli tuskaista, sillä videon purku vei kaiken tehon, jopa verkkoliikenne hidastui niin, että videon lataus ei ollut riittävän nopeaa toiston yhteydessä. Testikoneen prosessori ei riittänyt kunnolla toistamaan teräväpiirtoresoluution videoita virtuaalikoneessa, vaikka normaalissa järjestelmässä se ei ole ongelma. VMwaren Player oli tässä suhteessa ylivoimaisesti parempi kuin VirtualBox, sillä toistui jopa YouTuben 1080p video sulavasti ja ilman ongelmia.

Ryhmälähetyspohjainen IPTV toimi pääosin hyvin, mutta se oli melko herkkä sekä lähetys- että vastaanottopään viiveille. Jos lähetyspäässä oli paljon muuta verkkoliikennettä tai virtuaalikoneen prosessorilla oli muita tehtäviä, niin kuva pikselöityi ja ääni katkoi jatkuvasti. Videotoistimena toimi VLC media playerin versio 1.0.3.

VirtualBoxin näytönohjainajuri ei tue Windowsin visuaalista Aero-teemaa, jonka toimimista voidaan pitää modernin näytönohjaimen minimivaatimuksena. VirtualBoxissa on myös kokeellinen 2D-video ja 3D-kiihdytystuki, mutta molemmat toimivat vain Windows XP:ssä, testeissä käytettiin Windows versiota 7. VMwaren Player tukee sekä Aeroa ja 3D-kiihdytystä, joten on hyvin mahdollista, että tuki tulee joskus myös VirtualBoxiin. Äänikorttina VirtualBoxissa on Intelin AC97-määrityksen mukainen stereoäänikortti, joten monikanavaääniä voi toistaa vain stereona.

5.2 Ratkaisun tietoturva

Ratkaisun tietoturvaa voidaan arvioida arvioimalla komponentteja erikseen sekä niiden yhteisvaikutusta. VirtualBoxin tai OpenVPN:n tietoturvaa on vaikea arvioida itsenäisesti, joten siinä ollaan julkisen tiedon varassa ja turvallisuuspuutteet eivät ole useinkaan julkisia. Vanhojen versioiden vikoja julkaistaan jossakin määrin eli niistä voi päätellä minkä tyyppisiä puutteita ohjelmissa saattaa olla. Itse ohjelmissa oleville vioille ei voi tehdä mitään, mutta päivittämällä ohjelmat säännöllisesti uusimpiin versioihin välttynee ongelmilta. Hyökkäystä virtuaalikonetta vastaan voidaan pitää tällä hetkellä melko epätodennäköisenä, todennäköisempää ovat aivan tavalliset hyökkäykset järjestelmää vastaan. Tärkeämpää on siis suojata virtuaalikone, kuten mikä tahansa muukin verkkoon liitetty kone, palomuurilla ja virustorjunnalla. Virtuaalikoneen saastumisen ei pitäisi vaarantaa toimistoverkon konetta, ellei käyttäjä siirrä ohjelmatiedostoja koneiden välillä tai pidä tiedostonjakoa järjestelmien välillä. Tämän vuoksi Aallon tietohallinnossa oltiin sitä mieltä, että virtuaalikoneesta ei tulisi olla pääsyä isännän levyosioihin, tosin asiasta oli selvitys vielä kesken (Salin, 2010).

Se mikä pitää varmistaa, on että ohjelmien asentaminen ja niiden asetukset eivät tee aukkoja tietoturvaan. OpenVPN:n virtuaalinen verkkosovitin mahdollistaa (teoriassa) liikennöinnin testiverkon ja toimistoverkon välillä ja toimistokoneen saastumisen tai hyökkäykset testiverkon kautta. Tämän voi estää poistamalla sovittimelta IP-rajapinnan, eikä normaali käyttäjä voi muuttaa sovittimen asetuksia. OpenVPN sisältää sekä asiakas- että palvelinkomponentit, joten käyttäjä voi halutessaan käynnistää avoimen VPN-palvelimen toimistokoneelleen. Tämän estäminen onnistuu helpoiten estämällä saapuvat yhteydet paikallisesta ohjelmistopalomuurista, johon käyttäjällä ei ole muutosoikeuksia.

VirtualBoxissa ainoa merkittävä asetus on verkkoliitännän konfiguroiminen. Käyttäjä voi valita käytetyn verkkosovittimen ja asettaa virtuaalikoneen verkkoliitännän joko sillatuksi, osoitteenmuutostilaan (NAT) tai paikalliseen käyttöön (ei liikennettä fyysisen koneen ulkopuolelle). Näistä sillatussa tilassa oleva sovitin voi saada toimistoverkosta osoitteen, mikäli verkon DHCP-palvelin antaa osoitteen tuntemattomille tai jos käyttäjä on kloonannut fyysisen verkkosovittimen MAC-osoitteen virtuaalikoneelle. Virtuaalikoneen asetuksia ei voi muuttaa virtuaalikoneesta itsestään, joten käyttäjän olisi tehtävä tämä tahallaan. IP-osoitteen kaappaamisesta ei tosin pitäisi olla erityistä hyötyä, sillä pääsynvalvonta palveluihin hoidetaan muilla keinoilla.

5.3 Ratkaisun edut ja rajoitukset

Ratkaisun tärkeimpänä etuna on nähtävä käyttäjän saama vapaus tehdä virtuaalikoneessa haluamiaan asioita ilman ylläpitotyön vaikeutumista. Käyttäjä voi valita käyttöjärjestelmän lisenssirajoitusten puitteissa ja voi täysin päättää mitä ohjelmia asentaa. Käyttäjä voi myös asentaa useita käyttöjärjestelmiä ja perustaa pienen verkon ilman yhtään ylimääräistä fyysistä laitetta. VPN-yhteys mahdollistaa liittymisen avoimeen verkkoon vaikka organisaation verkko olisi muuten toiminnallisuudeltaan erittäin rajoitettu. Virtualisointi säästää uuden laitteiston ja verkkoliitännän ylläpitokulun kaikissa muissa paitsi vaativimmissa tehtävissä.

Ratkaisun heikkona puolena ovat melko suuret tehohäviöt riippuen tehtävätyypistä ja lisenssiongelmat. Tavallisten toimisto-ohjelmien ajo onnistuu ongelmitta, mutta varsinkin useaa komponenttia (kuten suoritin, levy ja verkko) samanaikaisesti rasittavat ohjelmat hidastuvat merkittävästi, jopa käyttökelvottomaksi. Hidastuminen johtuu aiemmin mainitusta I/O-toimintojen suoritinriippuvuudesta. Toinen heikkous on käyttöjärjestelmälisensointi eli virtuaalikone tarvitsee oman lisenssin, mikä mahdollisesti rajoittaa Windowsin käyttöä. Mac OS X:ää ei toisaalta voi asentaa edes rahalla virtuaalikoneeseen. Lisenssiasiat käsiteltiin luvussa *3.4 Lisenssirajoitukset*.

Puutteista huolimatta virtualisoinnin suorituskyky kasvaa ja se soveltuu vaihtoehdoksi tulevaisuudessa mihin tahansa tehtävään virtualisoinnin laitteistotuen laajentuessa ja ohjelmistojen kehittyessä.

5.4 Asetettujen tavoitteiden täyttyminen

Työn tavoitteena oli tuoda tutkijoille yhteys testiverkkoon ja samalla virtuaalikoneympäristö laajoilla käyttöoikeuksilla heidän toimistokoneilleen. Toteutuksessa oli tavoitteena käyttää maksutta saatavilla olevia ohjelmistoja. Jo alusta saakka oli selvillä, että edellä mainittujen tavoitteiden mukainen ratkaisu on mahdollinen, mutta sen lisäksi oli tarkoituksena selvittää ratkaisun käyttökelpoisuutta loppukäyttäjille ja ylläpidolle sekä ratkaisun mahdollisia ongelmakohtia esimerkiksi tietoturvan kohdalla.

Ratkaisun tekninen puoli toimii ongelmitta, suorituskyky tosin on väistämättä heikompaa kuin fyysisessä koneessa, varsinkin verkkoliikenteessä suorituskyvyn pudotus on huomattava, nopeuden pitäisi silti riittää useimpiin tehtäviin. Ratkaisu koostuu vain kahdesta komponentista; virtualisointiohjelmasta ja VPN-yhteydestä. Näiden komponenttien asennus käsin ei tuota ongelmaa, mutta yhtenä tavoitteena ollut keskitetty asennus tuo pieniä eroavaisuuksia prosessiin. Mahdollisia ongelmakohtia on käsitelty työssä, mutta se miten asia käytännössä hoidetaan, riippuu muun muassa ylläpitäjän käytössä olevasta hallintajärjestelmästä.

Ratkaisu on yhteensopiva Aallon työasema- ja ohjelmistopolitiikan kanssa, eikä sen pitäisi aiheuttaa tietoturvaongelmia, kunhan muutamia asioita huomioidaan komponenttien asennuksessa ja käyttäjille tiedotetaan mahdollisista uhkakuvista. Asiaan perehtymättömän saattaa virheellisesti olettaa, että virtuaalikoneen toiminta on eristetty molempiin suuntiin, vaikka todellisuudessa isäntäkoneessa oleva haittaohjelma voi seurata virtuaalikoneen toimintaa.

Vastaavaa ratkaisua ei ole ollut ylläpidetyissä työasemissa ennen, mutta tutkijoilla on voinut olla henkilökohtaisia ratkaisuja heidän tutkimustyöasemissaan. Tämäkään ratkaisu ei ole kaiken kattava ja kaikille sopiva, mutta se on siinä mielessä yleiskäyttöinen, että sitä voi käyttää monessa asiassa hyväksi. Raskaissa tehtävissä virtuaalikoneen ja varsinkin VPN-yhteyden hitaus on merkittävä haitta, siksi erillisiä valopolkuyhteyksiä ja laitteita ei voi korvata tällä ratkaisulla. Toisissa tehtävissä etätyöpöytäratkaisu voi olla paljon käytännöllisempi, koska silloin sen käyttö ei ole rajattu vain yhteen koneeseen. Tämän työn ratkaisu on edullinen silloin, kun halutaan helposti ja nopeasti kevyt testiympäristö, kaikki tarvittavat säädöt ovat käyttäjän valittavissa, käyttöjärjestelmää myöden.

Kokonaisuutena ratkaisu täyttää kaikki sille asetetut vaatimukset, ratkaisun on myös melko helppokäyttöinen, kunhan kaikki asetukset säädetään ylläpidon toimesta toimiviksi. Helppokäyttöisyyttä korostaisi, jos ratkaisun mukana toimitettaisi tai erikseen ladattavissa olisi levykuva toimivasta järjestelmästä, jonka voisi vain käynnistää napin painalluksella. Täysin ilman ohjeita ei tosin esimerkiksi VPN-yhteyttä saa muodostettua, sillä se vaatii asetus- ja avaintiedostot oikeaan paikkaan.

Vaikka ratkaisu olisikin kuinka onnistunut ja toimiva tahansa, ei siitä ole mitään hyötyä jos sitä ei kukaan käytä, joten ensin IT-järjestelmien ylläpidon on todettava ratkaisu hyväksi ja toimivaksi, jonka jälkeen he voivat tarjota sitä loppukäyttäjille.

5.5 Vertailu vaihtoehtoisiin ratkaisuihin

Tälle ratkaisulle vaihtoehtoina voidaan pitää luvussa *2.1 Virtualisointi* esiteltyjä etä-, virtuaalista ja virtuaalikone-pohjaista työpöytää sekä erillistä fyysistä konetta. Periaatteellisena vaihtoehtona voidaan pitää myös niin sanotusti kaksoiskäynnistystä (*dual boot*), jossa koneeseen asennetaan kaksi tai useampi käyttöjärjestelmä rinnakkain. Kaikille vaihtoehtoisille ratkaisuille yhteistä on mahdollisuus antaa käyttäjälle järjestelmänvalvojan oikeudet, mutta käyttöjärjestelmän valinnanvapaus on jo enemmän ylläpidon käsissä.

Fyysinen kone

Erillinen fyysinen kone suoriutuu tehtävistä nopeammin ja paremmin kuin virtualisoitu järjestelmä, mutta lienee itsestään selvää mitkä sen huonot puolet ovat. Fyysinen kone vaatii pöytätilaa, ylläpitotyötä, verkkoliitännän, sähköä ja sitoo pääomaa. Lisäksi VPN-yhteys ei toimi aivan yhtä läpinäkyvästi kuin tämän työn ratkaisussa, sillä koneeseen tulee vähintään kaksi aktiivista verkkoliitäntää, fyysinen ja VPN-ohjelman virtuaalinen verkkoliitäntä.

Etätyöpöytä

Oletetaan, että etätyöpöytä yhteys olisi fyysiseen koneeseen eikä virtuaalikoneeseen, muuten se on käytännössä sama asia kuin virtuaalinen työpöytä. Ohjelmien ajo fyysisessä koneessa tuo selvää tehoetua virtuaalikoneeseen nähden. Lisäksi jotkin ominaisuudet toimivat toistaiseksi ainoastaan aidossa ympäristössä, kuten näytönohjaimen hyödyntäminen erilaisissa tilanteissa, mukaan lukien 3D-grafiikka, videopurku ja GPU-laskenta. NVIDIA ja Parallels ovat kuitenkin esitelleet tekniikan, jolla vieraalle voidaan varata yksi grafiikkaohjain kokonaan, mikä siis vaatii useamman näytönohjaimen käyttämistä (NVIDIA Corporation, 2009).

Fyysinen kone on ihanteellisesti suoraan testiverkkoon yhteydessä, jolloin VPN-ratkaisu ei rajoittaisi verkon suorituskykyä, mutta käytännössä tämä ei liene aina mahdollista. Pullonkaulaksi muodostuu käytetty etätyöpöytäprotokolla, vapaasti saatavilla oleva tarjonta on niukkaa ja tehotonta verrattuna markkinoiden parhaisiin ratkaisuihin. Perustason käyttö onnistuu, mutta protokollia ei ole suunniteltu multimedian siirtoon ja se vaatii kymmenien megabittien kaistanleveyden. Selkeästi suurin ongelma on oletettavasti erillisen fyysisen laitteiston tarve ja sen ylläpitokustannukset, joten etätyöpöytäratkaisu ei tuo käyttäjän suorassa käytössä olevaan koneeseen verrattuna mitään etuja, ellei yksi fyysinen kone palvele useaa etätyöpöytäkäyttäjää. Lisäksi ongelmaksi voivat muodostua käyttöpolitiikkakysymykset, kuten saako käyttäjä järjestelmänvalvojan oikeudet etähallittavaan koneeseen.

Virtuaalinen työpöytä

Virtuaalisella työpöydällä tarkoitetaan tässä palvelimessa ajettavaa virtuaalikonetta, johon käyttäjä yhdistää etätyöpöytäprotokollaa käyttäen. Tämä vaihtoehto oikeastaan yhdistää etätyöpöydän ja virtualisoinnin huonot puolet loppukäyttäjän kannalta. Virtualisointi tosin tuo mahdollisuuden parempaan etätyöpöytäprotokollaan, josta esimerkkinä voidaan pitää Red Hatin SPICEa. Ratkaisun edut tulevat esille vasta useamman käyttäjän ympäristössä ja tarkasteltaessa etuja ylläpidon kannalta. Etuina käyttäjälle ovat järjestelmäresurssien (suoritin, muisti) parempi saatavuus, riippuen tosin palvelimesta ja käyttäjämäärästä. Toinen etu on, että työpöytä on saatavilla mistä tahansa verkkoyhteyden yli. Huonoina puolina ovat virtuaalikoneen ominaisuuspuutteet, kuten 3D-grafiikka, ja etätyöpöytäyhteyden tuoma viive ja kaistankäyttö. Lisäksi palvelinta ei kannattane perustaa yhden käyttäjän tarpeisiin eli ratkaisu ei ole kovin joustava.

Virtuaalikone-pohjainen työpöytä

Virtuaalikone-pohjaisella työpöydällä tarkoitetaan nyt paikallisesti ajettavaa hypervisor-virtuaalikonetta, joka toimii siis suoraan laitteiston päällä, toisin kuin tässä työssä käytetty isännöity virtuaalikone. Ratkaisu tarjoaa periaatteessa paljon tehokkaamman tavan käsitellä laitteistoa, mukaan lukien grafiikkakortit, ja olisi siten teknisesti ylivertainen tässä työssä esitettyyn ratkaisuun. Ratkaisu on toisaalta vielä niin tuore, että alan suurilla toimijoilla ei ole yhtään tuotetta markkinoilla, eivätkä ne melko varmasti ole ilmaisia ilmestyessään. Lisäksi hypervisorin asentaminen vaatii koko koneen tyhjentämisen ja suuria muutoksia oikeastaan koko ylläpitoinfrastruktuuriin, sillä järjestelmä on suunniteltu ennemminkin ylläpidon työkaluksi eikä käyttäjän koealustaksi.

Kaksoiskäynnistys tai liveCD

Kaksoiskäynnistys tarkoittaa, että käyttäjä voi valita koneen käynnistyksen yhteydessä käynnistettävän käyttöjärjestelmän. Toinen käyttöjärjestelmä voi olla ainakin teoriassa hypervisor-pohjainen virtuaalikonealusta, joka toisi lisää joustavuutta. LiveCD tarkoittaa optiselta levyltä tai muistitikulta käynnistettävää käyttöjärjestelmää, jota ei tarvitse erikseen asentaa. Toisella käyttöjärjestelmällä saadaan koneen koko kapasiteetti käyttöön samoin kuin toisella fyysisellä koneella. Kyseisen ratkaisun heikkouksia ovat vakavat tietoturvaongelmat, joita toinen, valvomaton, järjestelmä voi aiheuttaa ja se, että käyttäjä ei voi laittaa jotakin aikaa vievää tehtävää suorittumaan samalla kun tekee muita töitä toimistopuolen järjestelmällä.

5.6 Yhteenveto

Viidennessä luvussa arvioitiin ratkaisun toimivuutta mittauksin, pohtimalla tietoturvariskejä, ratkaisun etuja sekä huonoja puolia, tavoitteiden täyttymistä ja vertailemalla vaihtoehtoisia ratkaisuja.

Mittauksissa kävi ilmi, että vaikka virtuaalikoneen suorituskyky putoaa paperilla, välillä huomattavastikin, niin silti käyttökokemus on yleensä riittävä peruskäyttöön. Verkkoliikenteessä suorituskyky putoaa radikaaleimmin, yli 90 %. Lisäksi videotoisto ja videon suoratoisto web-sivuilta osoittautui melko vaativaksi.

Ratkaisun tietoturvassa ei ole vakavia ongelmia, mutta kuitenkin joitakin mahdollisia ongelmakohtia, joita kannattanee selvittää tarkemmin. Ratkaisun etuja ovat käyttäjän saama vapaus vierasjärjestelmässä ja fyysisten koneiden tarpeen väheneminen, mikä ilahduttaa ylläpitäjää. Ratkaisulle asetetut tavoitteet täyttyivät hyvin. Ratkaisuun valittujen ohjelmien lisenssit ovat riittävän avoimet vapaaseen käyttöön ja jakeluun, ja molemmista on jopa saatavilla avoimen lähdekoodin versiot. Ratkaisu sopii myös muilta osin Aallon ohjelmistopolitiikkaan. Ratkaisun voi nähdä täydentävänä vaihtoehtona erilliselle fyysiselle koneelle ja etätyöpöytäyhteyksille, täysin edellä mainittuja korvaavaksi siitä ei ole.

6 Yhteenveto

Työn tavoitteena oli selvittää virtuaalisen tutkimusverkkoyhteyden tarvetta, vaatimuksia ja toteutuskelpoista tuomista tutkijoiden ja muiden tahojen, kuten opiskelijoiden, käyttöön. Virtuaalinen ympäristö oli tarkoitus rakentaa maksutta saatavilla olevien virtuaalikone- ja VPN-asiakasyhteysohjelmistojen varaan ja sen tulisi olla mahdollista asentaa keskitetysti hallittuihin työasemiin ja käytettävissä peruskäyttäjän oikeuksilla.

Ratkaisulle asetettavia vaatimuksia selvitettiin tietoturvapolitiikan, loppukäyttäjien, tietojärjestelmien ylläpidon ja laitteistovaatimusten kannalta. Käyttäjien ja ylläpidon näkemyksiä kyseltiin haastatteluin ja kyselyin. Tärkeimpänä ratkaisun käyttötapana on yhdistäminen testiverkkoon ja virtuaalikoneen käyttö käyttäjien testialustana. Käyttäjäkyselyn perusteella, tosin, graafista työpöytää ei voida pitää vielä kovin olennaisena testiverkkoyhteyksissä, sillä siihen riittää usein pelkkä tekstipohjaisuus.

Ratkaisu on yhteensopiva Aallon työasema- ja ohjelmistopolitiikan kanssa, eikä sen pitäisi aiheuttaa tietoturvaongelmia, kunhan muutamia asioita huomioidaan komponenttien asennuksessa ja käyttäjille kerrotaan mahdollisista uhkakuvista. Virtuaalikoneita ei saa liittää ylläpidettyyn työasemaympäristöön, mutta siitä huolimatta niiden tietoturvasta tulisi huolehtia. Ylläpidon kannalta on tärkeää, että ratkaisun voi asentaa keskitetysti, myös lisenssirajoitukset täytyy huomioida. Isäntäkoneessa tulisi olla vähintään kaksiytiminen suoritin, paljon työmuistia ja uusimmat virtualisointilaajennukset, sillä ne nopeuttavat toimintaa parhaassa tapauksessa huomattavasti.

Ratkaisun perustan muodostavat avoimen lähdekoodin SSL-pohjainen VPN-ohjelma OpenVPN ja virtualisointiohjelma VirtualBox, josta on saatavilla avoimen ja suljetun lähdekoodin versiot. OpenVPN oli käytännössä valittu jo tulevaisuuden Internet -testiverkkoprojektin yhteydessä. Virtualisointiohjelman valintaa puolsi muita vaihtoehtoja avoimempi käyttöehtolisenssi. Keskitetyn asennuksen tuomia haasteita on tarkoitus tutkia myöhemmin. Mittauksissa kävi ilmi, että vaikka virtuaalikoneen suorituskyky putoaa paperilla, välillä huomattavastikin, niin silti käyttökokemus on yleensä riittävä peruskäyttöön. Verkkoliikenteessä suorituskyky putoaa radikaaleimmin, lisäksi videotoisto ja videon suoratoisto web-sivuilta osoittautui melko vaativaksi.

Vastaavaa ratkaisua ei ole ollut ylläpidetyissä työasemissa ennen, mutta tutkijoilla on voinut olla henkilökohtaisia ratkaisuja heidän tutkimustyöasemissaan. Ratkaisu ei sovi raskaisiin tai korkeaa luottamuksellisuutta vaativiin tehtäviin, mutta sitä voi silti käyttää monessa asiassa hyväksi. Toisissa tehtävissä etätyöpöytäratkaisu voi olla paljon käytännöllisempi, koska silloin sen käyttö ei ole rajattu vain yhteen koneeseen. Tämän työn ratkaisu on edullinen silloin, kun halutaan helposti ja nopeasti kevyt testiympäristö, kaikki tarvittavat säädöt ovat käyttäjän valittavissa, käyttöjärjestelmää myöden.

Kokonaisuutena ratkaisu täyttää kaikki sille asetetut vaatimukset, ratkaisun on myös melko helppokäyttöinen, kunhan kaikki asetukset säädetään ylläpidon toimesta toimiviksi. Helppokäyttöisyyttä lisäisi ratkaisun mukana toimitettava levykuva toimivasta järjestelmästä, jonka voisi käynnistää napin painalluksella.

6.1 Jatkotutkimus

Jatkotutkimuksen kohteita voisivat olla: Ensinnäkin, komponenttien keskitetyn asennuksen ja asetusten yksityiskohtien selvittäminen käytännössä, mikä on kuitenkin melko käyttöympäristökohtaista. Toiseksi, loppukäyttäjän työmäärän vähentämiseksi voisi asentaa jonkin vapaasti saatavilla olevan käyttöjärjestelmän, kuten Ubuntun, valmiiksi levykuvaksi, jotta käyttäjät saisivat nopeasti toimivan järjestelmän käyttöönsä. Tässä tulisi huomioida mitä ohjelmia olisi hyvä löytyä perusasennuksen lisäksi, mutta siten että levykuvan tiedostoko säilyy kohtuullisena. Kolmanneksi, tulisi selvittää, mikäli käyttäjä haluaa yhdistää kahteen virtuaaliverkkoon yhtä aikaa, tarvitseeko ylläpidon lisätä käsin toinen virtuaalinen verkkokortti kyseiselle käyttäjälle vai voiko asian hoitaa jotenkin muuten.

Neljänneksi, tässä työssä esitetty ratkaisu on tarkoitettu ylläpidon asennettavaksi, sillä komponenttien asennus vaatii järjestelmänvalvojan oikeuksia. Jatkotutkimuskohde voisi olla miten ratkaisusta saisi niin sanotusti siirrettävän (*portable*) version, jota voisi käyttää esimerkiksi muistitikulta suoraan erillisen ohjelman tavoin peruskäyttäjän oikeuksilla. Ubuntu liveCD -pohjainen versio on jo olemassa, mutta tietokone täytyy käynnistää uudelleen, jotta sitä voisi käyttää, ja käyttömukavuus on muutenkin melko alhainen.

Sekä OpenVPN:stä että VirtualBoxista on olemassa epäviralliset portable-versiot, jotka teoriassa mahdollistaisivat siirrettävyyden. Niissä on kuitenkin omat ongelmat, koska molemmat vaativat tiettyjen virtuaalilaitekomponenttien olemassaoloa. Siispä molemmat asentavat laitteita ohjelman käynnistyessä, mikä taas vaatii järjestelmänvalvojan oikeuksia. Lisäksi Portable VirtualBoxin käynnistäminen rikkoi olemassa olevan VirtualBoxin asennuksen. Haaste saada kummastakaan ohjelmasta siirrettävä versio ja lisäksi niiden yhteensovittaminen on siis melko vaativa tai mahdoton projekti.

Viitteet

Aalto-yliopisto. (2009). *Aalto-yliopiston työasemapolitiikka versio 1.0.*

Aalto-yliopisto. (2010). Aalto-*yliopiston työasemien ohjelmistopolitiikka versio 1.0.*

Adams, K.;& Agesen, O. (2006). A Comparison of Software and Hardware Techniques for x86 Virtualization. *Proceedings of the 12th international conference on Architectural support for programming languages and operating systems* (ss. 2-13). San Jose: Association for Computing Machinery.

Apple Inc. (2009). *Software license agreement for Mac OS X Snow Leopard.* Haettu 16.4.2010 osoitteesta http://images.apple.com/legal/sla/docs/macosx106.pdf.

Barham, P.;Dragovic, B.;Fraser, K.;Hand, S.;Harris, T.;Ho, A.;ym. (2003). Xen and the Art of Virtualization. *Proceedings of the 19th ACM symposium on Operating systems principles* (ss. 164-177). New York: Association for Computing Machinery.

Bellard, F. (2010). *QEMU.* Web-sivusto. Haettu 16.4.2010 osoitteesta QEMU: http://wiki.qemu.org/Main_Page

Bhatia, N. (2009a). *Performance Evaluation of AMD RVI Hardware Assist, VMware ESX 3.5.* Technical Paper. Haettu 19.4.2010 osoitteesta www.vmware.com/pdf/RVI_performance.pdf. VMware, Inc.

Bhatia, N. (2009b). *Performance Evaluation of Intel EPT Hardware Assist, VMware ESX.* Technical Paper. Haettu 19.4.2010 osoitteesta www.vmware.com/pdf/Perf_ESX_Intel-EPT-eval.pdf. VMware, Inc.

Bowker, M. (1.2.2010). *2010 Desktop Virtualization Trends*. Brief. Haettu 16.4.2010 osoitteesta Enterprise Strategy Group: http://www.enterprisestrategygroup.com/2010/02/2010-desktop-virtualization-trends/

Cisco Systems, Inc. (2009). *Cisco Active Network Abstraction Technology Support and Information Model Reference Manual Version 3.6.4.* San José: Cisco Systems, Inc.

De Gelas, J. (10.7.2008). *The very first independent Nested Paging Virtualization tests*. Web-artikkeli. Haettu 16.4.2010 osoitteesta AnandTech: http://www.anandtech.com/show/3413

Deri, L.;& Andrews, R. (2008). N2N: A Layer Two Peer-to-Peer VPN. *Second International Conference on Autonomous Infrastructure, Management and Security, AIMS 2008 Bremen, Germany, July 1-3, 2008 Proceedings / Lecture Notes in Computer Science 5127.* 5127/2008, ss. 53-64. Bremen: Springer Berlin / Heidelberg.

Dierks, T.;& Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol Version 1.2, Request for Comments: 5246, Standards Track.* Internet Engineering Task Force (IETF).

Domingues, P.;Araujo, F.;& Silva, L. (2009). Evaluating the performance and intrusiveness of virtual machines for desktop grid computing. *2009 IEEE International Symposium on Parallel&Distributed Processing* (ss. 1-8). Rome: IEEE Computer Society.

Duerig, J.;Ricci, R.;Zhang, J.;Gebhardt, D.;Kasera, S.;& Lepreau, J. (2006). Flexlab: A Realistic, Controlled, and Friendly Environment for Evaluating Networked Systems. *In Record of the 5th Workshop on Hot Topics in Networks: HotNets V*, (ss. 103-108). Irvine, CA.

Feilner, M. (2009). *Beginning OpenVPN 2.0.9.* Birmingham: Packt Publishing.

Figueiredo, R.;Boykin, P. O.;Juste, P. S.;& Wolinsky, D. (2008). Social VPNs: Integrating Overlay and Social Networks for Seamless P2P Networking. *Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises* (ss. 93-98). Washington DC: IEEE Computer Society.

Finnet-liitto ry. (25.10.2009). *Mikä on Supermatrix?.* Web-sivu. Haettu 31.3.2010 osoitteesta Supermatrix: http://www.supermatrix.fi/sx2/index.php?option=com_content&view=article&id=34&Itemid=8

Frahim, J.;& Huang, Q. (2008). *SSL Remote Access VPNs* (1. painos). Indianapolis: Cisco Press.

Freier, A. O.;Karlton, P.;& Kocher, P. C. (1996). *The SSL Protocol Version 3.0, Internet draft.* Haettu 16.4.2010 osoitteesta http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt. Internet Engineering Task Force (IETF).

Gajek, S.;Manulis, M.;Pereira, O.;Sadeghi, A.-R.;& Schwenk, J. (2008). Universally Composable Security Analysis of TLS - Secure Sessions with Handshake and Record Layer Protocols. *Proceedings of Second International Conference, ProvSec 2008, Shanghai, China, October 30 - November 1, 2008* (ss. 313-327). Springer Berlin / Heidelberg.

Ganguly, A.;Agrawal, A.;Boykin, P. O.;& Figueiredo, R. (2006). IP over P2P: Enabling Self-configuring Virtual IP Networks for Grid Computing. *In Proceedings of the 20th IEEE International Parallel and Distributed Processing Symposium (IPDPS)* (ss. 1-10). IEEE Computer Society.

Gartner, Inc. (15.3.2010). *Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than the Physical Servers They Replace Through 2012.* Press Release. Haettu 1.4.2010 osoitteesta Gartner Newsroom: http://www.gartner.com/it/page.jsp?id=1322414

Gartner, Inc. (2.3.2008). *Gartner Says Virtualization Will Be the Highest-Impact Trend in Infrastructure and Operations Market Through 2012.* Press Release. Haettu 16.4.2010 osoitteesta Gartner Newsroom: http://www.gartner.com/it/page.jsp?id=638207

Gerzon, G. (2007). *Intel Virtualization Technology Processor Virtualization Extensions and Intel Trusted execution Technology*. Esityskalvot. Haettu 19.4.2010 osoitteesta Intel: http://software.intel.com/file/1024

Graham, J. S.;& Cook, M. (2009). *Secure Virtual Private Networks, Technical Guide.* Haettu 19.4.2010 osoitteesta http://www.ja.net/documents/publications/technical-guides/tg-vpn.pdf. Didcot, UK: JANET (UK).

Hamed, H.;Al-Shaer, E.;& Marrero, W. (2005). Modeling and Verification of IPSec and VPN Security Policies. *Proceedings of 13th IEEE International Conference on Network Protocols (ICNP),* 2005, (ss. 268-277). Chicago.

Hamzeh, K.;Pall, G.;Verthein, W.;Taarud, J.;Little, W.;& Zorn, G. (1999). *Point-to-Point Tunneling Protocol (PPTP), Request for Comments: 2637, Informational.* Internet Engineering Task Force (IETF).

Hanks, S.;Li, T.;Farinacci, D.;& Traina, P. (1994). *Generic Routing Encapsulation (GRE), Request for Comments: 1701, Informational.* Internet Engineering Task Force (IETF).

Higgins, K. J. (4.6.2009). *Hacking Tool Lets A VM Break Out And Attack Its Host.* Uutinen. Haettu 22.3.2010 osoitteesta DarkReading: http://www.darkreading.com/securityservices/security/app-security/showArticle.jhtml?articleID=217701908

Higgins, K. J. (12.1.2010). *IETF Fix For SSL Protocol Complete*. Uutinen. Haettu 19.4.2010 osoitteesta DarkReading: http://www.darkreading.com/vulnerability_management/security/vulnerabilities/showArticle.jhtml?articleID=222300635

Honda, O.;Ohsaki, H.;Imase, M.;Ishizuka, M.;& Murayama, J. (2004). *Understanding TCP over TCP: Effects of TCP Tunneling on End-to-End Throughput and Latency*. IEIC Technical Report (Institute of Electronics, Information and Communication Engineers), 104 (438), 79-84.

Huhtanen, K.;& Savola, P. (16.6.2009). *WP4 Testbed Phase 2 Objectives*. Esityskalvot. Haettu 19.4.2010 osoitteesta http://wiki.hiit.fi/download/attachments/9962871/WP4_Huhtanen_phase2-objectives.pdf?version=1

Invisible Things Lab. (2010). *bluepillproject.org*. Web-sivusto. Haettu 16.4.2010 osoitteesta bluepillproject.org: http://bluepillproject.org/

Kent, S.;& Seo, K. (2005). *Security Architecture for the Internet Protocol, Request for Comments: 4301, Standards Track.* Internet Engineering Task Force (IETF).

Kirch, J. (2007). *Virtual Machine Security Guidelines Version 1.0*. Technical paper. Haettu 19.4.2010 osoitteesta http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf. The Center for Internet Security.

Kleidermacher, D. (2009). Methods and Applications of System Virtualization using Intel® Virtualization Technology (Intel® VT). *Intel Technology Journal*, 13 (1), Haettu 19.4.2010 osoitteesta http://download.intel.com/technology/itj/2009/v13i1/pdf/ITJ-06-Virtualization.pdf.

KVM Project. (2010). *KVM Project Main Page*. Web-sivu. Haettu 26.1.2010 osoitteesta KVM: http://www.linux-kvm.org/

Lambert, N. (2008). *Demystifying Client Virtualization.* Market research paper. Haettu 19.4.2010 osoitteesta http://www.vmware.com/files/pdf/analysts/Forrester_Demystifying-Client-Virtualization.pdf. Forrester Research, Inc.

Lau, J.;Townsley, M.;& Goyret, I. (2005). *Layer Two Tunneling Protocol - Version 3 (L2TPv3), Request for Comments: 3931, Standards Track.* Internet Engineering Task Force (IETF).

Lewis, M. (2006). *Comparing, Designing, and Deploying VPNs.* Saatavilla osoitteesta http://www.fengnet.com/book/CDDV/toc.html: Cisco Press.

LogMeIn. (2010). *Virtual Networking with LogMeIn Hamachi²*. Web-sivusto. Haettu 19.4.2010 osoitteesta LogMeIn: https://secure.logmein.com/products/hamachi2/

Marlinspike, M. (2009a). *New Tricks For Defeating SSL In Practice.* Esityskalvot. Haettu 19.4.2010 osoitteesta http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf. Washington, DC: Black Hat DC 2009.

Marlinspike, M. (2009b). *Null Prefix Attacks Against SSL/TLS Certificates.* Technical paper. Haettu 19.4.2010 osoitteesta http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf. Las Vegas: Black Hat USA 2009.

Microsoft Corporation. (2010a). *Windows Virtual PC*. Web-sivusto. Haettu 19.4.2010 osoitteesta Microsoft Windows: http://www.microsoft.com/windows/virtual-pc/default.aspx

Microsoft Corporation. (2010b). *Windows Virtual PC: Requirements*. Web-sivu. Haettu 19.4.2010 osoitteesta Windows Virtual PC: http://www.microsoft.com/windows/virtual-pc/support/requirements.aspx

Microsoft Corporation. (2007). *Windows Vista Enterprise Hardware Planning Guidance*. Web-opastietokanta. Haettu 19.4.2010 osoitteesta Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc507845.aspx

Microsoft Corporation. (2009). *Windows XP Mode for Windows 7.* Esite. Haettu 16.12.2009 osoitteesta Microsoft Windows Virtual PC: http://www.microsoft.com/windows/virtual-pc/default.aspx

Nanda, S.;& Chiueh, T.-c. (2005). *A Survey on Virtualization Technologies*. Technical paper. Stony Brook University, Department of Computer Science, New York.

Nielsen, T. (23.2.2010). *Time to remove IT from the boardroom agenda*. Web-artikkeli. Haettu 19.4.2010 osoitteesta FT.com / Technology / Digital Business: http://www.ft.com/cms/s/0/89536372-1fc5-11df-8975-00144feab49a.html

Nikander, P.;& Mäntylä, M. (2007). *ICT SHOK Future Internet — Research Agenda.* Haettu 19.4.2010 osoitteesta http://www.futureinternet.fi/publications/ICT_SHOK_FI_SRA_Research_Agenda.pdf. TIVIT Oy.

nimimerkki "benes". (12.6.2009). *Blu-ray Movie Bitrates Here.* Forum-viesti. Haettu 19.4.2010 osoitteesta Blu-ray Forum: http://forum.blu-ray.com/blu-ray-movies-north-america/3338-blu-ray-movie-bitrates-here.html

NVIDIA Corporation. (30.3.2009). *NVIDIA SLI Multi-OS Empowers World's First Virtualized Graphics Workstation*. Press release. Haettu 17.3.2010 osoitteesta NVIDIA: http://www.nvidia.com/object/io_1238408514209.html

OpenVPN Technologies, Inc. (2010). *Security Overview*. Web-sivu. Haettu 15.4.2010 osoitteesta OpenVPN: http://openvpn.net/index.php/open-source/documentation/security-overview.html

Pajukanta, S. (2009). *PurpleNet OpenVPN User Interface*. Web-sivusto. Haettu 19.4.2010 osoitteesta SourceForge.net: http://purplenet.sourceforge.net/

Patel, B.;Aboba, B.;Dixon, W.;Zorn, G.;& Booth, S. (2001). *Securing L2TP using IPsec, Request for Comments: 3193, Standards Track.* Internet Engineering Task Force (IETF).

Paulson, L. C. (1999). Inductive Analysis of the Internet Protocol TLS. *ACM Transactions on Information and System Security (TISSEC).* Volume 2, Issue 3, ss. 332-351. New York: Association for Computing Machinery.

Peterson, L. L. (2010). *PlanetLab Impact*. Web-sivu. Haettu 1.4.2010 osoitteesta Planet-Lab: http://www.planet-lab.org/impact

PlanetLab Consortium. (2010). *PlanetLab*. Web-sivusto. Haettu 16.4.2010 osoitteesta PlanetLab: http://www.planet-lab.org/

Ray, M.;& Dispensa, S. (2009). *Renegotiating TLS.* Technical paper. Haettu 19.4.2010 osoitteesta www.phonefactor.com/sslgapdocs/Renegotiating_TLS.pdf. PhoneFactor, Inc.

Red Hat, Inc. (2010). *SPICE*. Web-sivu. Haettu 16.4.2010 osoitteesta redhat.com: http://www.redhat.com/virtualization/rhev/desktop/spice/

Rescorla, E.;& Modadugu, N. (2006). *Datagram Transport Layer Security, Request for Comments: 4347, Standards Track.* Internet Engineering Task Force (IETF).

Rescorla, E.;Ray, M.;Dispensa, S.;& Oskov, N. (2010). *Transport Layer Security (TLS) Renegotiation Indication Extension, Request for Comments: 5746, Standards Track.* Internet Engineering Task Force (IETF).

Salin, T. J. (4.5.2010). *Kommentti ratkaisun tietoturvasta sähköpostitse.* (I. Jaakkola, Haastattelija)

Savola, P. (29.5.2009). *The testbed architecture*. Wiki-artikkeli. Haettu 9.4.2010 osoitteesta ICT SHOK Future Internet - HIIT Wiki: http://wiki.hiit.fi/display/FISHOK/The+testbed+architecture

Shneiderman, B. (2010). *Designing the user interface : strategies for effective human-computer interaction.* Boston: Pearson/Addison Wesley.

Škoberne, N. (2008). *IPSec and OpenVPN Performance.* Technical paper. University of Ljubljana, Faculty of Computer and Information Science, Ljubljana.

Snader, J. C. (2005). *VPNs Illustrated: Tunnels, VPNs, and IPsec* (1. painos). Addison-Wesley Professional.

Sun Microsystems, Inc. (2010c). *Frequently Asked Questions (FAQ) for developers (Developer FAQ).* Web-sivu. Haettu 16.4.2010 osoitteesta VirtualBox: http://www.virtualbox.org/wiki/Developer_FAQ

Sun Microsystems, Inc. (2010b). *Sun VirtualBox User Manual Version 3.1.4.* Haettu 19.4.2010 osoitteesta http://download.virtualbox.org/virtualbox/3.1.4/UserManual.pdf. Sun Microsystems, Inc.

Sun Microsystems, Inc. (10.9.2008). *VirtualBox Personal Use and Evaluation License (PUEL).* Haettu 3.5.2010 osoitteesta VirtualBox: http://www.virtualbox.org/wiki/VirtualBox_PUEL

Sun Microsystems, Inc. (2010a). *VirtualBox*. Web-sivusto. Haettu 16.4.2010 osoitteesta VirtualBox: http://www.virtualbox.org/

The Bochs Project. (2010). *bochs: The Open Source IA-32 Emulation Project (Home Page).* Web-sivusto. Haettu 16.4.2010 osoitteesta bochs: http://bochs.sourceforge.net/

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2003). *Turvallinen etäkäyttö turvattomista verkoista, Julkaisu 2/2003*. Haettu 16.4.2010 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/44981/44978_fi.pdf. Valtiovarainministeriö.

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2002). *Valtionhallinnon etätyön tietoturvallisuusohje. Julkaisu 3/2002.* Haettu 19.4.2010 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060411Valtio/etatyon_ohje.pdf. Valtiovarainministeriö.

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2008). *Valtionhallinnon salauskäytäntöjen tietoturvaohje. Julkaisu 3/2008.* Haettu 19.4.2010 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080307Valtio/Vahti_3-2008_netti.pdf. Valtiovarainministeriö.

van Dijk, L. (28.10.2008). *An Introduction to Virtualization.* Web-artikkeli. Haettu 16.4.2010 osoitteesta AnandTech: http://it.anandtech.com/show/2653

Wippien. (2010). *Free P2P VPN software.* Web-sivusto. Haettu 5.1.2010 osoitteesta Wippien: http://www.wippien.com/

VMware, Inc. (2007). *Understanding Full Virtualization, Paravirtualization, and Hardware Assist.* White paper. Haettu 16.4.2010 osoitteesta http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf.

VMware, Inc. (2010b). *VMware Player 3 EULA*. Haettu 4.5.2010 osoitteesta VMware End User License Agreements: http://www.vmware.com/download/eula/player3.html

VMware, Inc. (2010a). *VMware Player*. Web-sivusto. Haettu 19.4.2010 osoitteesta VMware Desktop Products: http://www.vmware.com/products/player/

Wojtczuk, R. (2008). *Adventures with a certain Xen vulnerability (in the PVFB backend).* Technical paper. Haettu 19.4.2010 osoitteesta http://invisiblethingslab.com/resources/misc08/xenfb-adventures-10.pdf. Invisible Things Lab.

Wojtczuk, R.;& Rutkowska, J. (2009a). *Attacking Intel Trusted Execution Technology.* Technical paper. Haettu 19.4.2010 osoitteesta http://invisiblethingslab.com/resources/bh09dc/Attacking%20Intel%20TXT%20-%20paper.pdf. Black Hat DC 2009. Washington, DC: Invisible Things Lab.

Wojtczuk, R.;& Rutkowska, J. (2009b). *Attacking SMM Memory via Intel CPU Cache Poisoning.* Technical paper. Haettu 19.4.2010 osoitteesta

http://invisiblethingslab.com/resources/misc09/smm_cache_fun.pdf. Warsaw: Invisible Things Lab.

Wojtczuk, R.;& Tereshkin, A. (2009). *Introducing "Ring -3" Rootkits.* Esityskalvot. Haettu 19.4.2010 osoitteesta http://invisiblethingslab.com/resources/bh09usa/Ring%20-3%20Rootkits.pdf. Black Hat USA 2009. Las Vegas: Invisible Things Lab.

Wojtczuk, R.;Rutkowska, J.;& Tereshkin, A. (2009). *Another Way to Circumvent Intel Trusted Execution Technology.* Technical paper. Haettu 19.4.2010 osoitteesta http://invisiblethingslab.com/resources/misc09/Another%20TXT%20Attack.pdf. Invisible Things Lab.

A Virtualisointiohjelmien vertailu

Allaolevissa taulukoissa on vertailtu VirtualBoxin, VMware Playerin ja Windows Virtual PC:n oleellisimpia ominaisuuksia. VirtualBoxin avoimen lähdekoodin version puuttuvat ominaisuudet on merkitty OSE-merkinnällä.

Taulukko A1: Taulukossa on verrattu ilmaisten, isännöityjen virtualisointiohjelmien ominaisuuksia

	VirtualBox	VMware Player	Windows Virtual PC
Tuetut isäntäkäyttö-järjestelmät	Windows XP ja uudemmat, Linux, Solaris, Mac OS X	Windows XP ja uudemmat, Linux	Windows 7
Tuetut vieraskäyttö-järjestelmät	Windows NT ja uudemmat, Linux, Solaris, OS/2	Windows 95 ja uudemmat, Linux, Solaris, Mac OS X Server, FreeBSD, NetWare	Windows XP/Vista/7
64-bittinen vierastuki	Kyllä	Kyllä	Ei
Virtualisointi-laajennustuki	Kyllä	Kyllä	Kyllä
Nested paging tuki	Kyllä	Kyllä	?
Jaetut kansiot	Kyllä	Kyllä	Kyllä
Seamless-tila	Kyllä	Kyllä	Vain Windows XP
Snapshot	Kyllä	Ei	Ei
Live migration	Kyllä	Ei	Ei
Komentorivi	Kyllä	Ei	Ei
Julkinen API	Kyllä	Ei	Ei
Etätyöpöytätuki	Kyllä (ei OSE)	Ei	Ei

Taulukko A2: Taulukossa on verrattu virtualisointiohjelmien tarjoamien virtuaalikoneiden ominaisuuksia

	VirtualBox	VMware Player	Windows Virtual PC
Moniydintuki	Kyllä, vaatii virt.laajennustuen	Kyllä	Ei
Hiiren integrointituki	Kyllä	Kyllä	Kyllä
Leikepöydän jako	Kyllä	Kyllä	Kyllä
3D-tuki	OpenGL, DirectX (vain Windows XP)	OpenGL, DirectX	Ei
Windows Aero -tuki	Ei	Kyllä	Ei
Useamman näytön tuki	Kyllä, vain Windows XP, monimutkainen	Kyllä	Kyllä?
USB-tuki	Kyllä (ei OSE)	Kyllä	Kyllä
Sillattu/NAT/host only -verkko	Kyllä	Kyllä	Kyllä
Tuetut verkkokortit	5	1	1
Verkkoliitäntöjen enimmäismäärä	4	10	4
PXE-verkkokäynnistys	Kyllä	Ei?	Ei?
Tuetut äänikortit	2	1	1
Monikanavaäänet	Ei	Ei	Ei
DVD-asematuki	Kyllä	Kyllä	Kyllä
Sarjaporttituki	Kyllä	Kyllä	Kyllä
Rinnakkaisporttituki	Ei	Kyllä	Ei
SCSI-tuki	Kyllä	Kyllä	Ei
Älykorttituki	Ei	Ei	Kyllä

B OpenVPN esimerkkiasetukset

Alla on asiakkaan OpenVPN-malliasetukset

```
# client mode
client

# TAP or TUN device
dev tap

# UDP or TCP
proto udp

# remote address
remote openvpn.research.netlab.hut.fi 1194

# resolve address indefinitely
resolv-retry infinite

# no binding to local address/port
nobind

# Try to preserve some state across restarts.
persist-key
persist-tun

# SSL/TLS certificates/keys
ca certificate_authority.crt
cert client_certificate.crt
key client_secretkey.key

# verify server certificate type
ns-cert-type server

# cryptographic cipher
cipher AES-128-CBC   # AES

# enable compression
comp-lzo

# Set log file verbosity.
verb 3
```

Alla on palvelimen OpenVPN-malliasetukset

```
# bind to local address/port (optional)
;local a.b.c.d
# Which TCP/UDP port should OpenVPN listen on?
port 1194
# TCP or UDP server?
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging and have precreated a tap0 virtual
interface and bridged it with your ethernet interface.
dev tap

# Windows needs the TAP-Win32 adapter name from
# the Network Connections panel if you have more than one.
;dev-node MyTap

# certificate files
ca certificate_authority.crt
cert server_certificate.crt
key server_secretkey.key

# Diffie hellman parameters.
dh dh2048.pem

# Maintain a record of client <-> virtual IP address associations in this file.
;ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging, DHCP in proxy mode
server-bridge
# Ping every 10 seconds, assume after 120 seconds
keepalive 10 120
# Select a cryptographic cipher.
cipher AES-128-CBC   # AES
# Enable compression
comp-lzo
# It's a good idea to reduce the OpenVPN daemon's privileges
# after initialization on non-Windows systems
user nobody
group nobody
# The persist options will try to avoid accessing certain resources on restart
# that may no longer be accessible because of the privilege downgrade.
persist-key
persist-tun
# Output a short status file
status openvpn-status.log
# log verbosity.
verb 3
```

C Suositellut asetukset VirtualBoxiin

Alla olevassa taulukossa on eritelty tärkeimmät asetukset VirtualBoxiin ja niiden suositeltu asetus. (Sun Microsystems, Inc., 2010)

Taulukko C1: Suositellut asetukset VirtualBoxiin

Asetukset	Välilehti	Asetus	Selitys/arvo
General	Basic	OS, Version	Asennetun käyttöjärjestelmän tyyppi ja versio
System	Motherboard	Base memory	Virtuaalikoneelle varatun muistin määrä, tavalliset arvot 512 MB – 2 GB
System	Motherboard	Enable IO APIC	Täytyy valita 64-bittiselle vieraalle tai jos käytetään useampaa ydintä virtuaalikoneessa. Hidastaa hieman vieraan toimintaa.
System	Processor	Processor(s)	Virtuaalikoneelle näkyvien ytimien määrä, valitaan enintään fyysisten ytimien määrä
System	Processor	Enable PAE/NX	Jos valittu, fyysisen prosessorin PAE ja NX ominaisuudet näkyvät virtuaalikoneelle. Ei vaikuta nopeuteen, joten kannattaa pitää päällä.
System	Acceleration	Enable VT-x/AMD-V	Mikäli prosessori tukee virtualisointiominaisuuksia, ne on hyödyllistä kytkeä päälle. Tuki vaaditaan moniydinprosessoritukeen ja 64-bittisten järjestelmien ajamiseen. Virtuaalikoneiden ajaminen, joissa tämä asetus on eri tilassa, johtaa suorituskyvyn heikkenemiseen Intelin VT-x järjestelmässä.
System	Acceleration	Enable nested paging	Nopeuttaa muistinkäsittelyä, joten kannattaa pitää päällä, jos prosessori tukee
Display	Video	Video memory	Vähintään 26 MB vaaditaan HD videon ajamiseen. Windows Aero vaatii vähintään 64 MB, rajoitetuilla resoluutioilla (Microsoft Corporation, 2007) (huomioi, että nykyinen VirtualBoxin näytönohjainajuri ei ole WDDM-yhteensopiva eikä siten tue Windows Aeroa)
Display	Video	3D acceleration	Direct3D 8/9 3D-kiihdytys on kokeellinen ja toimii ainoastaan Windows XP 32-bittisessä versiossa (VirtualBox 3.1.4) OpenGL vaatii Linux ytimen 2.6.27 ja X.org server 1.5 tai uudemmat
Display	Video	2D video accele-	Kokeellinen DirectDraw-videorajapintatuki. Toi-

		ration	mii ainoastaan Windows XP tai uudemmille vieraille.
Storage		Hard disk controller	SATA-ohjain toimii nopeammin ja vie vähemmän prosessoriresursseja kuin IDE-ohjain, joten sitä kannattaa suosia mikäli vieraskäyttöjärjestelmä tukee AHCI-tilaa. Windows XP ei tue.
Audio		Audio controller	Intel AC97 on ominaisuuksiltaan parempi kuin Soundblaster 16. Uudemmissa Linuxeissa tulisi käyttää PulseAudio alijärjestelmää (Ubuntu 8.04 ja Fedora 8 ja uudemmat).
Network	Adapter 1	Adapter type	Intel PRO/1000 sarjan kortit ovat paremmin tuettuina uudemmissa käyttöjärjestelmissä (Windows Vista) kuin AMD PCNet kortit. MT Desktop lienee varmin valinta.
Network	Adapter 1	Attached to	Bridged Adapter
Network	Adapter 1	Name	”TAP-Win32 Adapter V9” (OpenVPN virtuaalinen verkkokortti)

D OpenVPN signalointipaketti

Alla olevassa taulukossa on esitetty OpenVPN:n signalointipaketti.

Taulukko D1: OpenVPN TLS signalointipaketti P_ACK ja P_CONTROL

	Koko tavuissa	
local session_id	8	
HMAC signature	20	
packet-id	4	
P_ACK packet_id array length	1	
P_ACK packet-id array	length*4	
P_ACK remote session_id	0/8	
message packet-id	4	
literal 0	4	vain P_CONTROL
key_method type	1	TLS key_method 2
key_source	?	
options_string_length	2	
Options string	n	
username_string_length	2	valinnainen
Username string	n	
password_string_length	2	
Password string	n	

E Käyttäjäkyselyn tulokset

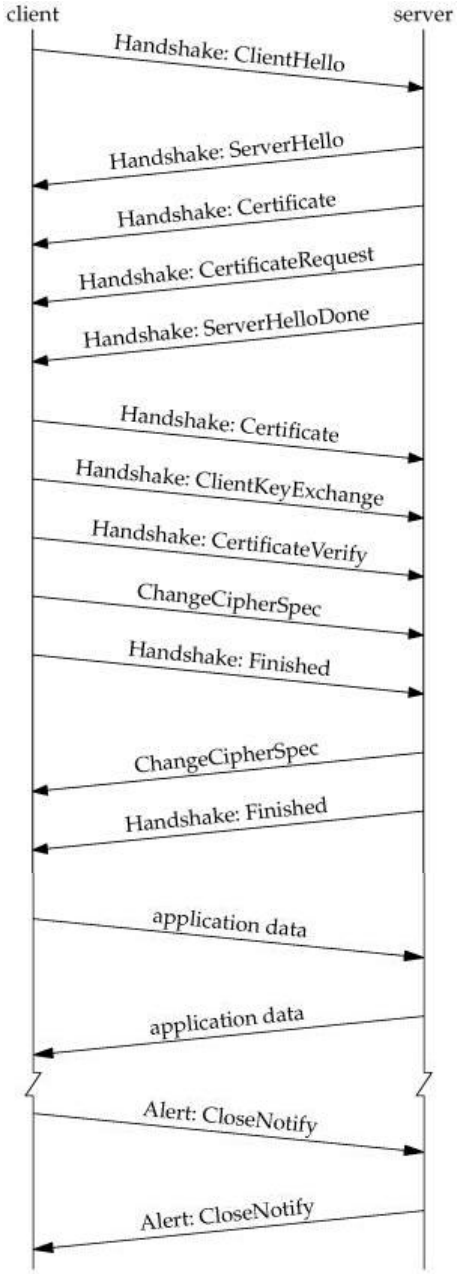
Alla olevassa taulukossa on yhteenveto web-kyselynä toteutetusta käyttäjien käyttötarpeita kartoittavan kyselyn tuloksista.

Taulukko E1: Käyttäjäkyselyn tulokset

n=15	Kyllä	Ei	EOS
On käyttänyt testiverkkoa	8	7	-
Katsoo virtuaalikoneen VPN-yhteydellä hyödylliseksi työkoneellaan	8	3	4
Katsoo työkoneensa olevan riittävän tehokas virtuaalikoneelle	12	2	1
Katsoo virtuaalikoneen VPN-yhteydellä hyödylliseksi kotikoneellaan tai kannettavalla	12	3	0
Katsoo kotikoneensa olevan riittävän tehokas virtuaalikoneelle	11	3	1
Haluaa valmiiksi konfiguroidun virtuaalikoneen	11	3	1
Tarvitsee työssään tulevaisuudessa testiverkkoa	3	1	10
Mieluisin yhteystapa testiverkkoon **Asteikko 1-5, 1 on mieluisin**	**Vastausten keskiarvo**		
Tekstipohjainen (SSH)	1,73		
Virtuaalikone ja VPN	2,33		
Pelkkä VPN toimistokoneelta	2,47		
Etätyöpöytä, järjestelmänvalvojan oikeuksilla	2,80		
Web-käyttöliittymä	2,93		
Etätyöpöytä, rajoitetuilla oikeuksilla	3,27		
Erillinen fyysinen kone	3,40		
Mieluisin käyttöympäristö raskailla sovelluksilla **Asteikko 1-4**	**Fyysinen**	**Etätyöpöytä**	**Virtuaali-kone**
Suoritinintensiivinen sovellus	2,09	2,00	2,73
Muisti-intensiivinen sovellus	1,83	1,83	3,00
Multimediaintensiivinen sovellus	1,64	2,45	3,00
Verkkointensiivinen sovellus	2,18	1,82	3,00
Levyintensiivinen sovellus	1,82	1,64	3,27
Yleiskäyttö	1,91	2,45	2,27

F SSL-kättely

Alla olevassa kuvassa on esitetty SSL-protokollan mukainen kättely, kun käytetään varmenteita sekä palvelimen, että asiakkaan puolella.



Kuva F1: SSL-kättely varmenteilla