INTERNET-LIIKENTEEN JA SISÄLLÖN SUODATUS

Ville Pietiläinen

Opinnäytetyö
Maaliskuu 2011

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) PIETILÄINEN, Ville	Julkaisun laji Opinnäytetyö	Päivämäärä 28.3.2011
	Sivumäärä 84	Julkaisun kieli SUOMI
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)
Työn nimi INTERNET-LIIKENTEEN JA SISÄLLÖN SUODATUS		
Koulutusohjelma Tietotekniikka		
Työn ohjaaja(t) NARIKKA, Jorma		
Toimeksiantaja(t) Jyväskylän ammattikorkeakoulu, SILTANEN, Jarmo		

Tiivistelmä

Koska perustieto Internet-liikenteen ja sisällön suodatuksesta on hajautunut eri tuotevalmistajien omiin materiaaleihin, oli työn tavoitteena saada kerättyä tärkein informaatio aiheesta samoihin kansiin ja toimia käsikirjana tukemassa verkkoliikenteen suodatustekniikoiden valintaa ja toteutuksen suunnittelua, niin että pystytään valitsemaan oikeanlainen suodatustekninen ratkaisu.

Työn perimmäisenä tarkoituksena oli selvittää lukijalle olennaiset asiat Internet-liikenteen suodatuksesta, eli mitä suodatus on, miten se toimii ja mitä toimenpiteitä on suositeltavaa suorittaa suodatusjärjestelmää käyttöönotettaessa.

Työssä läpikäytiin tekniikoita, joilla verkon ylläpitäjä voi suodattaa Internet-liikennettä ja näin rajoittaa ei-haluttua liikennettä tietoverkossaan. Suodatettavissa sovellusprotokollissa pääpaino oli World Wide Webin perustana toimivalla HTTP-protokollalla, mutta monet käytetyistä ratkaisuista mahdollistavat myös muunkin verkkoliikenteen suodatuksen.

Työn testausosassa tutustuttiin noin kahteenkymmeneen erilaiseen DNS, välityspalvelin, yhdyskäytäväpalvelin sekä virustorjuntaohjelmistoon, joita verrattiin asetettuihin vaatimuksiin. Näistä ohjelmistoista suurin osa karsiutui hyvin nopeasti pois, yleensä suuresti käsityötä vaativan suodatuksenhallinnan vuoksi. Alustavan tutkimustyön pohjalta lopullisiin testeihin ja esittelyyn valikoitui kuusi ohjelmistoa, jotka edustavat varsin kattavasti yleisimpiä sisällön- ja liikenteensuodatuksen menetelmiä.

Työn tuloksena saatiin kattava ja monipuolinen aineisto jota voidaan käyttää ohjekirjana suodatustekniikoiden suunnitteluun ja toteutukseen.

Avainsanat (asiasanat)
Liikenteen suodatus, sisällön suodatus, Domain Name System, proxy, yhdyskäytävä

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Author(s)	Type of publication	Date
PIETILÄINEN, Ville	Bachelor´s Thesis	28.3.2011
	Pages 84	Language FINNISH
	Confidential ( ) Until	Permission for web publication (X)

Title
INTERNET TRAFFIC AND CONTENT FILTERING

Degree Programme
Information Technology

Tutor(s)
NARIKKA, Jorma

Assigned by
JAMK University of Applied Sciences, SILTANEN, Jarmo

Abstract

Basic information about Internet traffic and content filtering is not readily obtainable, as it is divided between the manuals and help pages of different suppliers. The purpose of this work was to collect this information into a single volume and to make it usable as a support manual for choosing and implementing the right solution for traffic filtering.

The main focus of this thesis was to find the most important issues concerning Internet traffic filtering: what is filtering, how does filtering work and what procedures should be undertaken during the deployment process of a filtering system.

In this thesis techniques were studied that a network administrator can use to filter Internet traffic and limit the amount of un-wanted traffic in the network. When filtering application protocols, the primary target was the Hypertext Transfer Protocol that forms the basis of the World Wide Web. Many of the filtering solutions can also be used to filter other protocols.

In the testing section of this work, twenty different DNS, proxy server, gateway server and antivirus programs were explored and compared against the assigned requirements. Of these programs, most were eliminated fairly quickly, usually because of the manual labor needed to manage the filtering system. Based on the preliminary analysis, six programs were chosen for final testing. These programs adequately represent the most commonly used techniques of content and traffic filtering.

As a result of this thesis, a comprehensive and diverse material was created, that can be used as a manual in designing and implementing Internet traffic and content filtering.

Keywords
Traffic filtering, content filtering, Domain Name System, proxy, gateway

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

DHCP	Dynamic Host Configuration Protocol. TCP/IP-osoitteiden jakojärjestelmä jolla voidaan määrittää IP-osoitteet automaattisesti.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi.
DOMAIN	Hallinta-alue. Tietoverkon osa, jonka laitteet kuuluvat samaan hallinnallisesti yhtenäiseen alueeseen.
FTP	File Transfer Protocol. TCP-protokollaa käyttävä tiedonsiirtoprotokolla.
HTTP	Hypertext Transfer Protocol. Protokolla jota käyttäen WWW-selaimet ja palvelimet käyttävät tiedonsiirtoon.
HTTPS	Hypertext Transfer Protocol Secure. HTTP-protokollan salattu versio. Tiedot salataan SSL tai TLS-protokollan avulla.
IP	Internet Protocol. Reitittävä yhteydetön tiedonsiirtoprotokolla.
ISO	International Organization for Standardization. Kansainvälinen standardointijärjestöjen kattojärjestö.
NAT	Network Access Translation. Verkko-osoitteiden muuttopalvelu sisä- ja ulkoverkon välillä.
OSI	Open Systems Interconnection Reference Model. Tiedonsiirtoprotokollien toimintaa kuvaava malli.
SAAS	Software as a Service. Kolmannen osapuolen tarjoama palvelu.
SSL	Secure Sockets Layer. Kryptograafinen protokolla joka tarjoaa turvallisuutta Internet-tiedonsiirtoon.
TCP	Transmission Control Protocol. Luotettava, yhteydellinen tiedonsiirtoprotokolla.
TCP/IP	Transmission Control Protocol / Internet Protocol. Yleisimmin käytetty tiedonsiirtoprotokolla perhe.
TLS	Transport Layer Security. Kryptograafinen protokolla joka tarjoaa turvallisuutta Internet-tiedonsiirtoon.
UDP	User Datagram Protocol. Yhteydetön tiedonsiirtoprotokolla.

URL	Uniform Resource Locator. Internetissä käytetty osoitemuoto, jolla ilmaistaan sivuston tai tiedoston paikka sekä käytettävä yhteyskäytäntö. Muodoltaan protokolla://kone:portti/hakemisto/tiedosto#kohta.
VPN	Virtual Private Network. Tapa jolla kaksi tai useampia verkkoja voidaan yhdistää julkisen verkon yli näennäisesti yksityiseksi verkoksi.
WWW	World Wide Web. Internet-verkossa toimiva, maailman laajuinen, hypertekstitiedon välityspalvelu.

1 TYÖN LÄHTÖKOHDAT

Koko ajan kehittyvä tietoyhteiskunta tarvitsee koko ajan kehittyvää tekniikkaa. Viime vuosina verkkoturvallisuus on kehittynyt dramaattisesti, ei ainoastaan käytössä olevien työkalujen tai tietoturvaan kohdistuvien uhkien vuoksi, vaan myös niiden menetelmien osalta, jolla tietoyhteyksien ja tietoverkkojen turvallisuutta lähestytään. Osaltaan tähän kehitykseen on myös vaikuttanut voimistunut halu työpaikoilla rajoittaa ja kontrolloida työntekijöiden Internetin käyttöä tuotannollisista syistä.

Koska perustieto Internet-liikenteen ja sisällön suodatuksesta on hajautunut eri tuotevalmistajien omiin materiaaleihin, oli työn tavoitteena saada kerättyä tärkein informaatio aiheesta samoihin kansiin ja toimia käsikirjana tukemassa verkkoliikenteen suodatustekniikoiden valintaa ja toteutuksen suunnittelua, niin että pystytään valitsemaan oikeanlainen suodatustekninen ratkaisu.

Työn perimmäisenä tarkoituksena oli selvittää lukijalle olennaiset asiat Internet-liikenteen suodatuksesta, eli mitä suodatus on, miten se toimii ja mitä toimenpiteitä on suositeltava suorittaa suodatusjärjestelmää käyttöönotettaessa. Työssä läpikäytiin tekniikoita, joilla verkon ylläpitäjä voi suodattaa Internet-liikennettä ja näin rajoittaa ei-haluttua liikennettä tietoverkossaan. Suodatettavissa sovellusprotokollissa pääpaino oli World Wide Webin perustana toimivalla HTTP-protokollalla, mutta monet käytetyistä ratkaisuista mahdollistavat myös muunkin verkkoliikenteen suodatuksen.

Työssä käsiteltiin ensin tietoliikenne- ja palomuuritekniikan perusteita. Koska palomuurit ovat todella laaja-alainen teknologia, ei tässä työssä perehdytty niiden osalta kuin tärkeimpiin määritelmiin. Kuitenkin palomuureista täytyi kerrata olennaisimmat asiat, koska sisällön suodatus on osaltaan perinteisen palomuurin jatkumo sekä sitä täydentävä tekniikka, joten tietyt perustaustatiedot oli hyvä palauttaa mieliin. Tämän lisäksi käytiin läpi verkkotekniikan perusteita, jotta lukijan olisi helpompi hahmottaa toteutusten toiminta sekä niiden vahvuudet ja heikkoudet.

Käytännön osuudessa testattiin eri suodatusmenetelmiä. Suodatusratkaisujen testaus suoritettiin Windows Server–ympäristössä joka mahdollisti helppokäyttöisen käyttäjien hallinnan sekä verkkoliikenteen seurannan toteuttamisen. Asiakaslaitteina toimivat Windows 7 -työasemat.

Työn tilaajana toimi Jyväskylän ammattikorkeakoulu joka on monialainen ja kansainvälinen korkeakoulu jossa opiskelee noin 8000 opiskelijaa kahdeksalla eri koulutusalalla. Koulutusalat ovat jakautuneet neljään koulutusyksikköön: ICT (Information and Communication Technologies), konetekniikka, logistiikka ja luonnonvarat sekä rakennustekniikka, joissa tarjotaan opetusta eri puolilla Jyväskylää. (Jyväskylän ammattikorkeakoulu 2010.)

ICT-yksikkö sijaitsee Jyväskylän Lutakossa ja tarjoaa opetusta neljässä eri koulutusohjelmassa: automaatio-, media-, ohjelmisto- ja tietotekniikka. Tämä opinnäytetyö toteutettiin tietotekniikan koulutusohjelman alaisuudessa ja ICT-yksikkö tarjosi tarvittavat tilat ja laitteet työn toteutukseen. (Jyväskylän ammattikorkeakoulu 2010.)

2 TIETOLIIKENNEPROTOKOLLAT

2.1 Yleistä

Tietoliikenneprotokollia kuvataan käyttämällä pinomallia, jonka avulla monimutkainen kokonaisuus saadaan pilkottua pienemmiksi ja paremmin hallittaviksi kokonaisuuksiksi. Eri järjestelmien sisällä samalla kerroksella olevat toiminnot mahdollistetaan yhteiskäytännön eli protokollan avulla. (Kaario 2002, 18.)

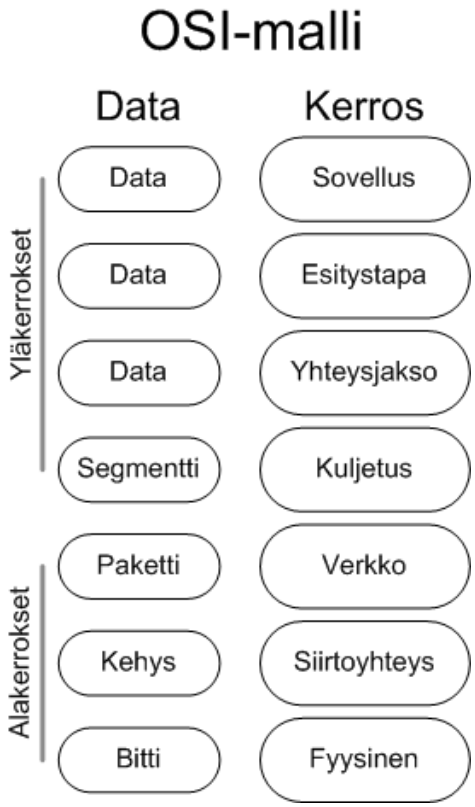
Yleisin tietoliikennejärjestelmien protokollapinon kuvaamiseen käytetty viitemalli on ISO:n (International Standards Organization) 1980-luvun alussa kehittämä OSI-malli (Open Systems Interconnection Reference Model), joka on kansainvälinen standardi. Siinä tietojärjestelmälle on määritelty seitsemän perustehtävää, joita mallissa kuva-

taan kerroksina (layer). Kerrokset tarjoavat palveluja itseään ylemmälle kerrokselle ja käyttävät itseään alemman kerroksen palveluja. (Hakala & Vainio 2005, 138.)

Toinen tärkeä viitemalli on TCP/IP-malli (Transmission Control Protocol / Internet Protocol), joka kuvaa TCP/IP-protokollan toimintaa. Tässä mallissa on neljä kerrosta, joista jokainen huolehtii yhden tai useamman OSI-mallin kerroksen toiminnasta. (Hakala & Vainio 2005, 183.)

2.2 OSI-malli

OSI-malli on seitsemän kerroksinen kerrosmalli jossa kerrokset on numeroitu yhdestä seitsemään. Kerroksia 1-3 kutsutaan alemmiksi kerroksiksi ja ne määrittelevät laitteistojen ja niihin läheisesti liittyvien protokollien toiminnan. Kerroksia 4-7 kutsutaan ylemmiksi kerroksiksi ja ne määrittelevät asiakas-palvelinsovelluksien ohjelmallisen toiminnan. Kuvio 1 kuvaa OSI-mallin kerrosrakenteen. (Hakala & Vainio 2005, 138.)



KUVIO 1. OSI-malli

1. Fyysinen kerros

Mallin alin kerros on fyysinen kerros. Tällä kerroksella määritellään kaapelointiin ja signaalinsiirtoon liittyvät sähköiset ja mekaaniset arvot. Tyypillisiä määrityksiä ovat liitin- ja kaapelityypit, signaalien jännitetasot, vaimennus, ylikuuluminen, heijastukset jne. Verkon aktiivilaitteista keskittimet, toistimet ja mediamuuntimet kuuluvat fyysisen kerroksen laitteisiin. (Hakala & Vainio 2005, 139.)

2. Siirtokerros

Siirtokerros, joskus käytetään myös nimeä siirtoyhteyskerros, määrittelee, miten lähetettävästä datasta muodostetaan kaapelointi-

järjestelmässä siirrettäviä yksiköitä, kuten kehyksiä (frame) tai soluja (cell). Tällä kerroksella määritellään lähettävän ja vastaanottavan laitteen fyysiset osoitteet (MAC-osoitteet). Kerroksen tärkeimmät aktiivilaitteet ovat verkkokortit, sillat ja kytkimet. (Hakala & Vainio 2005, 139.)

3. Verkkokerros

Tämä kerros määrittelee verkkojen välisessä tietoliikenteessä tarvittavan reitityksen sekä eri liikennöintimuotojen välisen priorisoinnin. Tehtävien hoitamiseen käytetään tarkoitukseen suunniteltuja protokollia, joista nykypäivänä yleisimmin on käytössä IP-protokolla. Kerroksen keskeisin aktiivilaite on reititin. (Hakala & Vainio 2005, 139.)

4. Kuljetuskerros

Kuljetuskerros on ensimmäinen ohjelmallisista ns. isäntäkerroksista. Kerroksen tehtävistä huolehtivat kuljetusprotokollat, joista yleisimmät ovat TCP ja UDP. Kuljetusprotokollat pilkkovat sovellusten lähettämän datavirran käsittelykokoisiin yksiköihin, joista yleisimmin käytetään nimitystä segmentti (segment) tai paketti (packet). Datan pilkkominen, lähetettävän pakettikoon määritys ja kuittaus ovat tehtäväkokonaisuus, jota kutsutaan vuonohjaukseksi. (Hakala & Vainio 2005, 140.)

5. Istuntokerros

Istuntokerroksen tehtäviin kuuluvat käyttöoikeuksien tarkistukset ja muut järjestelmän suojauksiin liittyvät tehtävät. Nykyisissä järjestelmissä useimmista tämän kerroksen tehtävistä vastaa käyttöjärjestelmä. Salausohjelmat ja tietokantojen hallintajärjestelmät toimivat osittain tämän kerroksen ohjelmistoina. (Hakala & Vainio 2005, 140.)

6. Esitystapakerros

Esitystapakerros määrittelee asiakkaan ja palvelimen välisen sanomaliikenteen muodon. Kerroksen määrittelyihin kuuluvat erilaiset koodausjärjestelmät. Tiedonsiirto tapahtuu binäärimerkkijonoina, ja koska siirrossa käytetään vain yhtä tietotyyppiä, joudutaan sanomarakenteeseen määrittelemään, miten alkuperäiset tietotyypit koo-

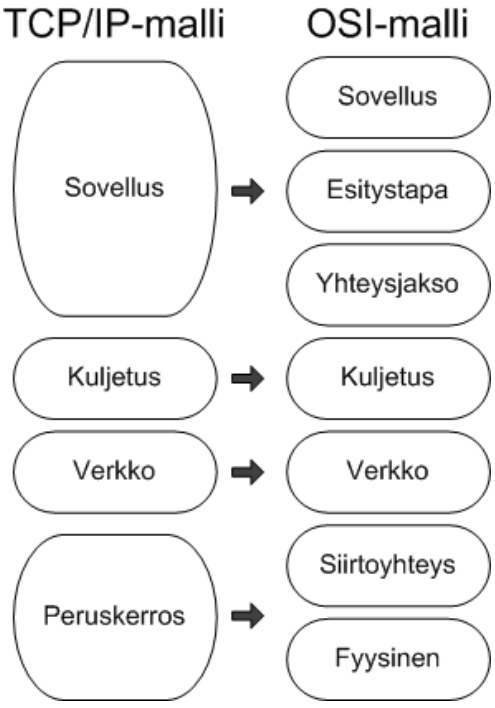
dataan lähetettäessä ja miten ne dekoodataan vastaanottavassa sovelluksessa. (Hakala & Vainio 2005, 140.)

7. Sovelluskerros

Ylintä kerrosta kutsutaan sovelluskerrokseksi ja siinä määritellään tietoliikennesovelluksille yhtenäinen kommunikaatiorajapinta verkkoon (Kaario 2002, 21). Tämä sisältää sovellusten ja käyttöjärjestelmien toiminnasta ne osat, joita alemmissa kerroksissa ei ole määritelty. Nykyisissä verkkosovelluksissa ja käyttöjärjestelmissä sovellus-, esitystapa- ja istuntokerrosten erottaminen toisistaan ei ole mahdollista, vaan niistä muodostuu yksi ohjelmallinen kokonaisuus. (Hakala & Vainio 2005, 140.)

2.3 TCP/IP-malli

TCP/IP-viitemalli koostuu neljästä kerroksesta ja rakentuu samaan tapaan kuin OSI-malli mutta on huomattavasti yksinkertaisempi. Siinä ei ole otettu huomioon kaikkia OSI-mallin tehtäviä ja yksittäinen TCP/IP-kerros huolehtii useammasta OSI-kerroksen tehtävästä. Kuvio 2 esittelee TCP/IP-mallin kerrosrakenteen verrattuna OSI-malliin. (Hakala & Vainio 2005, 184.)



1. Peruskerros: mallin alimmaisena kerroksena oleva peruskerros pitää sisällään OSI-malli fyysisen ja siirtokerroksen toiminnot.
2. Verkkokerros: vastaa OSI-mallin verkkokerrosta.
3. Kuljetuskerros: vastaa OSI-mallin kuljetuskerrosta.
4. Sovelluskerros: Ylimpänä on sovelluskerros, joka pitää sisällään OSI-mallin kolme ylintä kerrosta eli istunto-, esitystapa- sekä sovelluskerroksen. (Hakala & Vainio 2005, 184.)

KUVIO 2. TCP/IP-malli

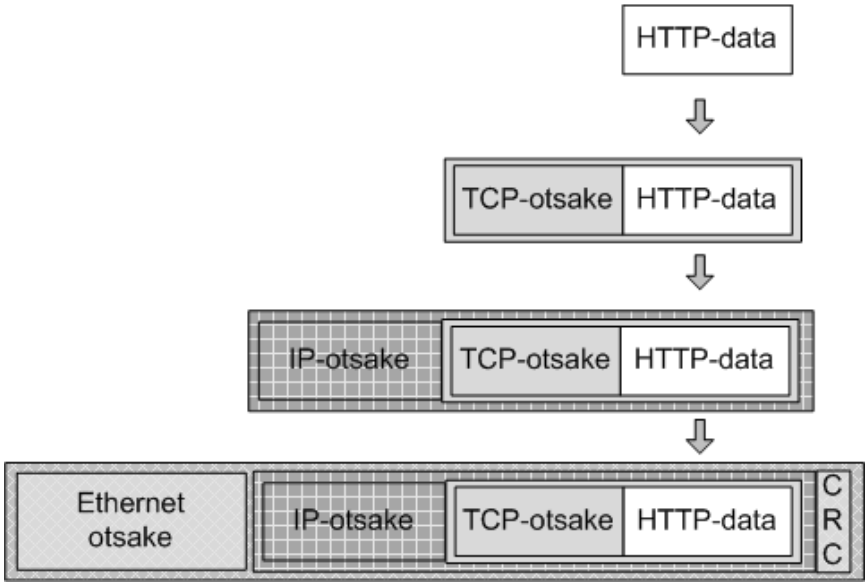
2.4 TCP/IP-protokollaperhe

2.4.1 Yleistä

TCP/IP-verkoissa lähtökohtana on verkkojen välinen tietoliikenne. Nimi- ja osoitejärjestelmät ovat hierarkkisia ja määrittelevät sekä verkon sijainnin Internetissä että koneen sijainnin verkon sisällä. Nimien ja osoitteiden yhdistämiseksi tarvitaan nimipalveluita, jotka muodostavat TCP/IP-verkkojen tärkeimmän ydinpalvelun. Toinen tärkeä ydinpalvelu on reititys, joka mahdollistaa tiedonsiirron eri arkkitehtuureja noudattavien Internetin osaverkkojen välillä. (Hakala & Vainio 2005, 178.)

Arkikielessä puhutaan usein TCP/IP:stä protokollana. Se ei kuitenkaan ole yksittäinen protokolla vaan protokollaperhe, joka koostuu useista erilaisista ja eri tehtäviä hoitavista protokollista. Sen jäsenprotokollat voidaan jakaa käyttötarkoituksensa mukaan sovellus-, kuljetus-, verkko- ja siirtoyhteysprotokolliin, joista tässä työssä esitellään suodatuksen kannalta tärkeimmät. (Hakala & Vainio 2005, 178.)

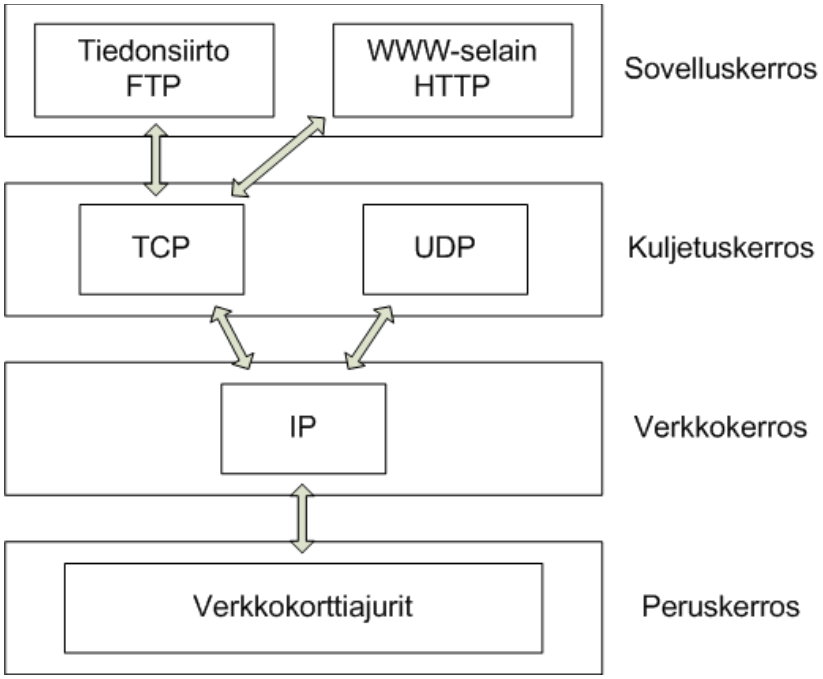
Esimerkkinä näistä protokollista voidaan käyttää WWW-sovellusta joka käyttää HTTP-protokollaa sovellustasolla. Seuraavana kuljetustason protokolla huolehtii tietovirran paloittelusta jotta verkon laitteet pystyvät sitä käsittelemään. HTTP:n tapauksessa tähän käytetään TCP-protokollaa. Jotta lähetettävät paketit löytäisivät oikean kohdeverkon, tarvitaan IP-protokollaa ja kohdeverkossa vielä ARP-protokollaa sekä fyysisellä tasolla jotain lähiverkkoprotokollaa, esim. Ethernet IEEE 802.3, siirtämään kehykset. Kuvio 3 esittelee kapseloinnin toteutuksen protokolla tasolla. (Hakala & Vainio 2005, 296.)



KUVIO 3. Ethernet kapselointi

- Www-palvelin antaa html-sivun HTTP-protokollan lähetettäväksi. HTTP-protokolla lähettää sanoman TCP-protokollalle.
- TCP-protokolla lisää sanomaan omat määrityksensä TCP-otsakkeessa muodostaen näin TCP-segmentin.
- IP-protokolla lisää TCP-segmenttiin omat määrityksensä, jolloin muodostuu IP-paketti.
- Ethernet-protokolla lisää omat määrityksensä jolloin muodostuu Ethernet-kehys.
- Vastaanottavassa päässä kehys puretaan päinvastaisessa järjestyksessä jolloin vastaanottaja saa tietoonsa lähetetyn sanoman.

Helpoiten näiden protokollien tehtäviä ja niiden välistä yhteistyötä hahmottaa sijoittamalla ne nelikerroksiseen TCP/IP-malliin. Kuvio 4 näyttää muutamien eri protokollien sijoittumisen TCP/IP-mallin kerroksille. (Hakala & Vainio 2005, 180.)



KUVIO 4. TCP/IP-protokollat

2.4.2 IP

TCP/IP-protokollaperheen ydin on IP-protokolla. Tästä protokollasta koko Internet on alun perin saanut nimensä (Kaario 2002, 46). IP-protokollan keskeisin tehtävä on loogisten osoitteiden lisääminen datavirtaan. Verkkojen välinen liikenne perustuu sekä verkon että koneen määrittäviin IP-osoitteisiin. IP-osoitteen verkon määrittävä osa mahdollistaa sovellusten lähettämien viestien reitittämisen läpikulkuverkkojen yli vastaanottajalle. (Hakala & Vainio 2005, 310.)

2.4.3 TCP & UDP

TCP on yhteydellinen protokolla. Tätä protokollaa käytettäessä asiakas ja palvelin sopivat yhteyden muodostamisesta laitteiden välille. Kun yhteys on muodostunut, voidaan aloittaa pakettien lähettäminen. Pakettien vastaanottaja lähettää kuittauksen jokaisesta vastaanottamastaan paketista ja jos kuittausta ei saada määräajassa, lähettäjä lähettää paketin uudestaan. TCP:tä käytetään lähes kaikkien sovellusten kuljetusprotokollana. (Hakala & Vainio 2005, 298.)

UDP on huomattavasti TCP:tä kevyempi ja epäluotettavampi, yhteydetön protokolla. Kaikki sovellukset eivät kuitenkaan vaadi tiedonsiirron luotettavuutta. Näitä ovat esimerkiksi sovellukset, jotka lähettävät jatkuvasti mutta epäsäännöllisin väliajoin lyhyitä viestejä verkkoon. Myös Internetin ryhmä- ja yleislähetykset on toteutettu UDP:lla. (Kaario 2002, 156.)

Ainoana osoitekenttänään TCP ja UDP sisältävät lähde- ja kohdeporttinumerot. Näitä käytetään datan lähettäneen sovelluksen tunnistamiseen. (Kaario 2002, 156.)

2.5 HTTP

Hypertext Transfer Protocol on sovellustason protokolla, jota käytetään hypermedia tiedon kuten WWW-sivujen ja niiden sisältämien kuvien, ohjelmien tai äänen välittämiseen. HTTP on tilaton protokolla, joka toimii pyyntö-vastaus periaatteella. Käyttäjän selain lähettää pyynnön Web-palvelimelle, joka käsittelee pyynnön ja lähettää vastauksen. Vaikka HTTP-protokollaa yleisimmin käytetään HTML-sisällön siirtoon, se ei ole sisältöriippuvainen, joten sitä voi käyttää monien muidenkin tietomuotojen siirtoon. (RFC 2616, 1999, 6-7.)

Yleensä HTTP-liikenne käyttää TCP-protokollaa ja porttia 80, mutta myös muita portteja tai protokollia voidaan käyttää. HTTP edellyttää vain, että sitä siirtävä protokolla pystyy takamaan tiedonsiirron luotettavuuden. (RFC 2616, 1999, 12.)

2.6 HTTPS

Verkkoliikenteen yksityisyyden ja turvallisuuden varmuuden takaamiseksi, esimerkiksi sähköisessä kaupankäynnissä, on kehitetty HTTPS-protokolla, joka salaa HTTP-liikenteen joko SSL tai TLS-protokollaa käyttäen. Suojaus toteutetaan turvaamalla kommunikaatiotunneli digitaalisella varmenteella. Salaus tapahtuu lähtöpisteestä määränpäähän, työaseman ja kohdepalvelimen välillä. HTTPS-liikenne käyttää TCP-protokollaa ja porttia 443. (Zwicky, Cooper & Chapman 2001, 514 -515.)

3 PALOMUURI

3.1 Yleistä

Palomuuri suojelee tietoverkon laitteita ulkopuolisilta hyökkäyksiltä, jotka voisivat häiritä verkon toimintaa tai aiheuttaa vahinkoa verkon laitteille. Palomuurina toimii tehtävään suunniteltu laite tai ohjelmisto joka, sijoitetaan rajapintaan tai yhdyskäytävään kahden verkon välille. Tässä kohdassa palomuuri tutkii kaiken liikenteen, joka kulkee sen läpi niin sisään kuin ulospäin etsien tiettyjä tunnusmerkkejä. Jos ne täyttyvät, se päästää paketin eteenpäin, muussa tapauksessa paketin lähetys estetään. (Zwicky, Cooper & Chapman 2001, 49.)

Palomuurien kaksi tärkeintä tyyppiä ovat tilallinen pakettisuodatin (stateful packet inspection) ja sovellustason yhdyskäytävä (application level gateway) (Kaario 2002, 305).

3.2 Tilallinen pakettisuodatin

Tilallinen pakettisuodatus on OSI-mallin tasolla 4 toimivan palomuurin operaatio, jossa suodatetaan liikennettä TCP/IP-osoitetietojen perusteella. Näistä tiedoista tärkeimpiä ovat lähettäjän ja kohteen osoitteet, lähettäjän ja kohteen portit, protokolla sekä paketin koko. Näiden lisäksi se pystyy pitämään kirjaa avatuista, puoliavoimista sekä jo suljetuista yhteyksistä. Näin palomuuriin voidaan luoda sääntöjä, jotka voivat esimerkiksi sallia TCP-yhteyksien avaamisen sisäverkosta Internetiin mutta kieltää Internetistä sisäänpäin tulevat yhteydet, elleivät ne ole osana jo avattua yhteyttä. (Zwicky, Cooper & Chapman 2001, 49.)

3.3 Sovellustason yhdyskäytävä

Sovellustason yhdyskäytävä toimii OSI-mallin tasolla 7 ja pystyy käyttämään suodatuspäätöksissään kaikkien kerrosten tietoja. Tämän tyyppinen palomuuri on erittäin tehokas, mutta kokonaisten pakettien sisällön analysoiminen vaatii paljon resursseja (Kaario 2002, 307). Sovellustasolla toimivan palomuurin täytyy myös kyetä tunnista-

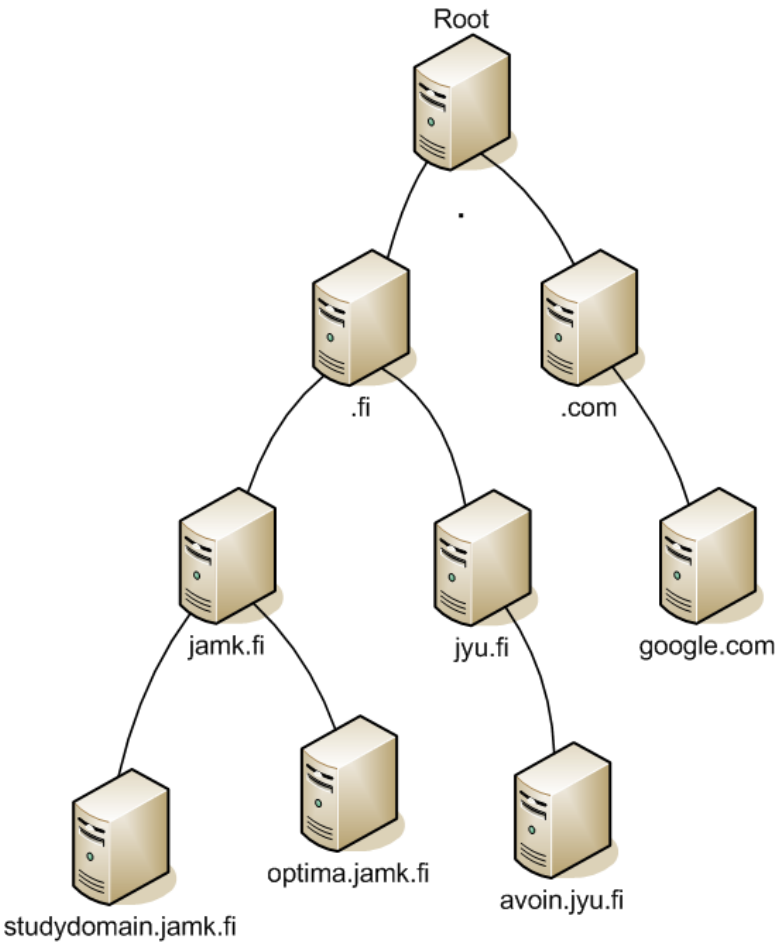
maan mahdollisimman monia sovelluksia niiden käyttämien sovellusprotokollien perusteella. Suurin hyöty sovellustason yhdyskäytävästä, verrattuna alempien tasojen palomuureihin on, että se erottaa sisäverkon ulkoisesta tietoverkosta ja toimii välikätenä kaikessa verkkojen välisessä liikenteessä. (RFC 1636, 1994, 11.)

4 DOMAIN NAME SYSTEM

Internet-verkossa koneeseen viitataan loogisella verkko-osoitteella, IP-osoitteella, joka koostuu neljästä kentästä, oktetista, jotka määrittelevät hierarkkisesti verkon sekä koneen osoitteen. IP-osoitenumerot ovat kuitenkin hankalia muistaa ja siksi niiden rinnalla käytetään kirjaimista koostuvia osoitteita eli domain-nimiä. (Hakala & Vainio 2005, 185.)

Domain Name System eli DNS on Internetin hajautettu puumainen tietokanta, joka hallitsee TCP/IP-verkkojen IP-osoitteiden muuntamisen domain-nimiksi ja päinvastoin. Hajautus on DNS-järjestelmässä välttämätöntä, koska mikään yksittäinen palvelin ei kykenisi vastaamaan kaikkiin maailman nimenselvityspyyntöihin. Hajautus myös parantaa tietoturvaa, koska palvelimet varmuuskopioivat toistensa tietoja. (Kaario 2002, 75.)

Nimipalvelimet hoitavat nimipalvelutehtäviä käsittelemällä useampia alemman tason haaroja. Nimiavaruuden korkeimmasta tasosta ns. juuresta huolehtivat juuritason nimipalvelimet (root nameservers). Juuritason alapuolelle sijoittuvat solmujen nimipalveluista vastaavat alemman tason nimipalvelimet, joille on määrätty oma alueensa eli vyöhyke (zone) alapuolella olevasta puurakenteesta (ks. kuvio 5). (Hakala & Vainio 2005, 187.)



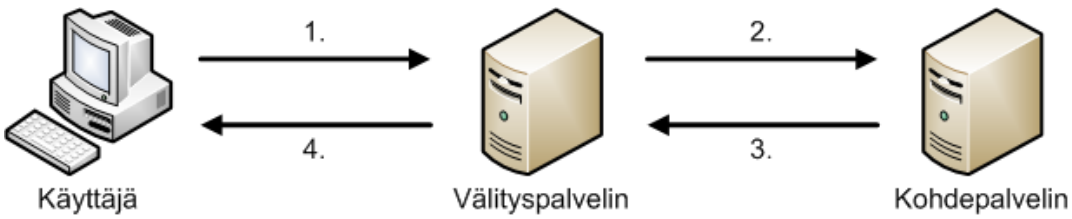
KUVIO 5. DNS-puurakenne

DNS-nimipalvelun perustana ovat rekursiiviset DNS-kyselyt, joita lähetetään DNS-nimipalvelimille, kun halutaan tietää jollekin domain-nimelle kuuluva IP-osoite. Kyselyssä käytetään hyväksi DNS:n hierarkkista rakennetta. Nimipalvelukysely ohjautuu ensimmäisenä paikalliselle nimipalvelimelle. Jos paikallinen nimipalvelin ei löydä vastausta, se ohjautuu askel kerrallaan hierarkiassa ylemmän tason nimipalvelimelle. Näin toimitaan kunnes, viimeistään DNS-puun juurisolmusta löydetään haluttu tieto. (Kaario 2002, 78.)

5 VÄLITYSPALVELIN

5.1 Yleistä

Välityspalvelu (proxy) on ohjelmisto, joka välittää palvelimien ja työasemien välillä tapahtuvaa liikennettä. Välityspalvelua käyttävät työasemat keskustelevat välityspalvelimen kanssa, joka välittää hyväksytyt pyynnöt eteenpäin todellisille palvelimille ja siltä saapuvat vastaukset takaisin työasemille (ks. kuvio 6). Yleisimmin välityspalvelua käytetään HTTP-liikenteen välittämiseen mutta myös muita protokollia kuten FTP tai Telnet voidaan ohjata välityspalvelimen kautta. (Zwicky, Cooper & Chapman 2001, 153.)



KUVIO 6. Välityspalvelimen toiminta

Välityspalvelinten (proxy server) tärkeimpinä ominaisuuksina ovat Internet-liikenteen nopeuttaminen sekä liikenteen sisällön hallinnan tehostaminen. Välityspalvelimet voivat tarkkailla, analysoida sekä tarvittaessa muokata niiden lävitse kulkevaa liikennettä. Usein välityspalvelimet toimivat myös varastoina (caching proxy) jotka säilyttävät kopioita jokaisen välittämänsä pyynnön tiedoista. Varastoinnin etu on että jos useat työasemat pyytävät samoja tietoja, tiedot voidaan tarjota suoraan välimuistipalvelimesta. Tämä parantaa palvelujen saatavuutta sekä vähentää verkon kuormitusta. (Zwicky, Cooper & Chapman 2001, 161.)

5.2 Välityspalvelin tyypit

HTTP-protokollan toiminnan määrittelevä RFC 2616 jakaa välityspalvelimet kahteen luokkaan: läpinäkyviin ja ei-läpinäkyviin palvelimiin.

- Läpinäkyvä palvelin ei muokkaa pyyntöjä tai vastauksia enempää, kuin mitä on tarvetta autentikoinnin ja tunnistuksen toteuttamiseksi.
- Ei-läpinäkyvä palvelin voi tehdä muutoksia paketteihin, jos siihen on tarvetta ylimääräisten palvelujen toteuttamisen kuten tiedostomuotojen vaihtamisen tai anonymiteetin takaamisen vuoksi. (RFC 2616, 1999, 9.)

Tämä virallinen määrittely ei kuitenkaan enää vastaa käytössä olevaa sanastoa, vaan nykyisissä ohjelmistoissa läpinäkyvällä palvelimella tarkoitetaan ns. kaappaavaa palvelinta. Tämän tyyppinen palvelin sieppaa verkkoliikenteestä HTTP-liikenteen ja ohjaa sen määriteltyyn porttiin pakottaen liikenteen menemään välityspalvelimen kautta ilman, että käyttäjä saa tästä tietoa tai kykenee menettelyyn vaikuttamaan. Näin välityspalvelin on käyttäjälle näkymätön. Läpinäkymättömällä välityspalvelimella tarkoitetaan nykyään välityspalvelinta jonka käyttö määritellä joko käsin Internet-selaimessa tai automaattisesti ylläpidon toimesta. (Gourley & Totty 2002, 140.)

Koska tämä merkitys välityspalvelimen näkymättömyydelle on nykypäivän valmistajien materiaaleissa yleinen, käytetään sitä tässä työssäkin puhuttaessa suodatuksen näkymättömyydestä.

Useimmat välityspalvelimet tukevat myös käyttäjän tunnistusta. Tunnistus voi tapahtua joko erillisen kirjautumisikkunan kautta tai käyttäjätietokantaa hyödyntäen. Tunnistus mahdollistaa, että eri käyttäjille ja/tai käyttäjäryhmille voidaan asettaa erilaiset oikeudet verkkoresurssien käyttöön. Yleensä verkon käytön rajoitus tapahtuu erilaisilla sallittujen ja/tai kiellettyjen osoitteiden tai sanojen listauksilla. (Hakala & Vainio 2005, 376.)

Osaltaan välityspalvelimet parantavat myös verkkoturvallisuutta, koska niiden avulla voidaan analysoida liikennettä sovelluskerroksen tasolla ja näin estää esimerkiksi mahdollisia viruksia tai muita haittaohjelmia pääsemästä verkon sisälle. (Hakala & Vainio 2005, 376.)

6 YHDYSKÄYTÄVÄPALVELIN

Perinteisesti yhdyskäytävällä (gateway) on tarkoitettu verkkolaitteita, jotka pystyvät yhdistämään eri protokollia käyttäviä verkkoja toisiinsa, eli purkamaan yhden protokollan mukaisen paketin ja kokoamaan sen uudelleen toista protokollaa käyttäen niin, että sisältö ei muutu (Kaario 2002, 31). Nykypäivänä termi on laajentunut merkitsemään mitä tahansa verkkolaitetta, jonka kautta tarjotaan reittiä toiseen verkkoon. Yleisesti tästä roolista huolehtii reititin, mutta sen voi tehdä myös yhdyskäytäväpalvelin, joka usein yhdistää reitityksen lisäksi muita palvelinominaisuuksia kuten esimerkiksi välityspalvelimen, DNS-palvelimen, VPN-palvelimen, osoitteenmuutospalvelun (NAT) sekä sovellustason palomuurin toiminnot.

7 WINDOWS SERVER

Windows Server on Microsoft Corporationin palvelinkäyttöjärjestelmä, jonka historia alkoi vuonna 1993 julkaistussa Windows NT Advanced Server 3.1 käyttöjärjestelmästä (Windows Products and Technologies History, 2003.).

Microsoft Corporationin viimeisin palvelinkäyttöjärjestelmäsukupolvi on Windows Server 2008, joka on toteutettu samalla koodipohjalla kuin työpöytäkäyttöjärjestelmä Windows Vista. Tämän palvelinkäyttöjärjestelmän viimeisin versio on vuonna 2009 julkaistu R2, joka on saatavilla vain 64-bittisenä versiona, ja se sisältää monia uudistuksia Windows 7 -työpöytäkäyttöjärjestelmästä. Suurin ero näiden palvelinkäyttöjärjestelmien ja käyttäjille tarkoitettujen työpöytäkäyttöjärjestelmien välillä on, että palvelinkäyttöön suunniteltujen järjestelmien suunnittelussa on kiinnitetty enemmän huomiota tehokkuuteen ja luotettavuuteen. (Hassell 2008, 2.)

Windows-palvelin voidaan asentaa suorittamaan monia eri tehtäviä tietoverkossa kuten DNS-palvelua, jonka käyttöä Windows Server 2008 R2 vaatii, jotta tietokoneet

löytävät toisensa tietoverkon sisällä. Ehkä tärkein ominaisuus Internet-liikenteen suodatusta ajatellen on Active Directory, joka pitää sisällään Group Policyn. Näiden avulla voidaan kontrolloida laitteiden, käyttäjien sekä käyttäjäryhmien oikeuksia keskitetysti. (Minasi, Gibson, Finn, Henry & Hynes 2010, 359.)

8 SUODATUS

8.1 Mitä on suodatus?

Termit estäminen (blocking) ja suodatus (filtering) tarkoittavat teknologioita, jotka estävät Internet-sisällön saatavuuden osoitteen, protokollan, tietoformaatin tai sisällön perusteella. Estäminen on tekniikka, jossa (OSI-mallin kerros 4) reititykseen kykenevä verkkolaite estää liikenteen perustuen sen osoitetietoihin, suodatuksessa (OSI-mallin kerros 7) palvelinlaitteisto pysäyttää verkkoresurssin käytön analysoituaan sen sisällön. Suodatusta käytetään myös yleisnimikkeenä tarkoittamaan verkkoliikenteen rajoittamista. (Turvallisten sisältöjen valikointi ja arviointi 2006, 9.)

8.2 Miksi suodattaa?

Suodatusta käytetään monista eri syistä. Yrityksissä suodatusta voidaan käyttää tuottavuuden nostamiseen. Sanomalehti Karjalaisen tekemässä kyselyssä ilmeni että Suomessa kahdestakymmenestä eniten työllistävästä suur-yrityksestä kahdeksantoista rajoittaa Internetin käyttöä tästä syystä (Nevalainen 2010). Internetin käyttöä rajoittamalla pyritään varmistamaan, että henkilökunta keskittyy työn tekemiseen eikä käytä työaikaa esimerkiksi ostossivuilla tai seuraa urheilu-uutisia. Suodatusta voidaan käyttää myös parantamaan yhtiön tietoturvallisuutta niin ulkoisten kuin sisäistenkin uhkien varalta. (Björkman 2008, 9.)

8.3 Suodatuksen suunnittelu

Suodatus- ja estomenetelmien suunnittelun ja asennuksen ei tule perustua pelkästään päätökseen, että Internetin käyttöä pitää rajoittaa. On myös tarkasteltava sitä, missä laajuudessa Internetin käyttöä halutaan rajoittaa, keneltä käyttöä rajoitetaan, millä perusteilla rajoitukset tehdään, mitkä ovat toimenpiteet väärien rajoitusten korjaamiseksi ja miten rajoitusten noudattamista valvotaan. Päätöksiä tarvitaan myös siitä, miten pitkälle rajoitukset tulee ulottaa. (Turvallisten sisältöjen valikointi ja arviointi 2006, 9.)

Järjestelmää suunniteltaessa on tärkeää määrittää täsmällisesti sen käyttötarkoitus ja tavoitteet, erityisesti tulee ottaa huomioon, kuinka kattava suodatuksen halutaan olevan. Näin suodatusjärjestelmä voidaan rakentaa asianmukaisesti täyttämään sille asetetut vaatimukset. Kun tiedetään, mihin tarkoitukseen suodatusjärjestelmä rakennetaan, voidaan päästä kohtuullisiin kustannuksiin suodatusta rakennettaessa sekä ylläpidettäessä. Mikäli vaatimukset ovat puutteelliset, voi tuloksena olla suodatusjärjestelmä, jonka käyttäjät pystyvät kiertämään. Täytyy kuitenkin pitää mielessä, että suodatusjärjestelmä, jota käyttäjät eivät kykene kiertämään, on vaikea rakentaa. (Turvallisten sisältöjen valikointi ja arviointi 2006, 28.)

Suodatuksen hallinnointi ja suodatusperusteet tulisi kuvata selkeästi, ja tämän tiedon tulisi olla julkista. Käyttäjien tulisi aina olla tietoisia tietoverkon käyttöehdoista, joissa suodattaminen tulisi mainita riittävän tarkasti. Myös toteutus olisi suositeltavaa tehdä niin, että suodatinjärjestelmää ei pyrittäisi piilottamaan, vaan että järjestelmä ilmoittaisi selkeästi, miksi materiaaliin ei päästä. Näin käyttäjä voi ilmoittaa virheellisistä tapauksista. (Turvallisten sisältöjen valikointi ja arviointi 2006, 28.)

Jotta järjestelmän toimivuus olisi moitteetonta, tulee myös järjestelmän hallinnointiin kiinnittää huomiota. Politiikkojen, käytäntöjen, prosessikuvausten ja ohjeiden avulla pystytään määrittelemään, mitä järjestelmän ylläpitohenkilöstön tulee tehdä ja missä rajoissa. (Turvallisten sisältöjen valikointi ja arviointi 2006, 9.)

Jos suodatusta toteutetaan organisaation eri osissa, tulisi suodatinohjelmien toteutukset yhtenäistää politiikoin ja ohjein sekä määrittää käytännöt, joilla päätökset suodatinohjelmien käytöstä, kattavuudesta ja valvontatoimista tehdään ylläpitoorganisaatiossa (Turvallisten sisältöjen valikointi ja arviointi 2006, 13).

Suodatuspolitiikassa on suositeltavaa määrittää, mitä suodatetaan sekä kuka vastaa suodatuksen toteuttamisesta, sen hallinnasta ja suodatukseen liittyvistä päätöksistä. Lisäksi näitä politiikkoja, ohjeita, määräyksiä ja käytäntöjä tulisi arvioida säännöllisesti. (Turvallisten sisältöjen valikointi ja arviointi 2006, 13.)

8.4 Suodatuksen sijoittaminen

Suodatus voidaan toteuttaa käyttäjän tietokoneella, verkkolaitteessa, verkossa sijaitsevalla palvelimella, palveluntarjoajan toimesta tai kolmannen osapuolen palveluna (Greenfield, Rickwood & Tran 2001, 12). Tässä työssä pääpaino on verkkolaitteessa tai palvelimessa toteutetussa suodatuksessa, jonka avulla suodatus toteutetaan niin, että se kattaa tarvittaessa tietoverkon kaikkien käyttäjien Internet-liikenteen.

8.4.1 Käyttäjän tietokoneella tapahtuva suodatus

Kotikäytössä yleisesti käytetty suodatus tapahtuu käyttäjän tietokoneella toimivalla ohjelmistolla. Tämän tyyppinen suodatus on epäluotettava, koska se on helppo ohittaa tai poistaa käytöstä. Suurissa verkoissa tällaisen suodatuksen ylläpito ja hallinta on työlästä. (Greenfield, Rickwood & Tran 2001, 12.)

8.4.2 Palvelimella tapahtuva suodatus

Suodatus voidaan toteuttaa palvelimella, jonka läpi Internet-liikenne kulkee. Palvelinpohjaisen suodatuksen suurin etu on, että se on tietoturvallisin tapa toteuttaa suodatus ja käyttäjän on vaikea ohittaa sitä. Käyttäjän tietokoneelle ei tarvita ylimääräisiä ohjelmia ja kaikki Internet-liikenne voidaan ohjata kulkemaan suodatuksen läpi. (Greenfield, Rickwood & Tran 2001, 13.)

8.4.3 Kolmannen osapuolen suodatus

Tässä ratkaisussa käyttäjän lähettämät pyynnöt välitetään kolmannen osapuolen, kuten jonkin tietoturvayhtiön tai Internet-palveluntarjoajan palvelimelle, joka tarkastaa ne suodatuslistausta vasten. Jotta tämä suodatus olisi tehokas, täytyy käyttäjän selain olla asetettu käyttämään kolmannen osapuolen verkkosivuja tai palvelimia kaikkiin pyyntöihin eikä muuta reittiä Internetiin tule olla sallittuna. (Greenfield, Rickwood & Tran 2001, 13.)

Tämän suodatuksen huonona puolena on, että kolmannella osapuolella on täysi kontrolli käyttäjän Internetin käytöstä (Greenfield, Rickwood & Tran 2001, 13).

9 SUODATUKSEN TOIMINTA

9.1 Yleistä

Kolme yleisintä tapaa suodattaa Internet-liikennettä ovat

- valkoinen listaus, ”hyvän” liikenteen salliminen (inclusion filtering)
- musta listaus, ”huonon” liikenteen estäminen (exclusion filtering)
- liikenteen sisällön analysoiminen ja estäminen jos se havaitaan ei-toivotuksi (content filtering).

Monet suodatustuotteet pohjautuvat Web-osoitelistoihin, joita tuotteen tarjoaja ylläpitää ja toimittaa käyttäjälle (Greenfield, Rickwood & Tran 2001, 6). Yleensä listat myös sisältävät suodatusluokittelun tai sisällön kategorioinnin sivuston aiheen perusteella. Näitä tietoja voidaan käyttää kiellettävien kohteiden valintaan ja suodatus pystytään paremmin kohdistamaan tietynlaiseen sisältöön (Turvallisten sisältöjen valikointi ja arviointi 2006, 19). Näiden listojen valmistaminen on kallista, koska niitä kerätessä joudutaan suodatettavat sivustot tarkastamaan. Tästä johtuen listat ovat usein salaisena pidettyä sovelluskohtaista tietoa. Salaisen luonteensa vuoksi näistä

listoista on vaikea tietää, mitä osoitteita on estetty ja mistä syystä. (Greenfield, Rickwood & Tran 2001, 6.)

Suomen kielen erityisluonne voi aiheuttaa myös suodatuksen yhteneväisyyteen eroja eri tuotteiden välillä. Sivustot saattavat eri tuotteissa olla eri kategorioissa tai kokonaan luokittelematta. Myös suoranaiset virheetkin ovat mahdollisia ja useimmat tuotteet sisältävät mahdollisuuden ilmoittaa listan ylläpitäjille vääristä listauksista. (Turvallisten sisältöjen valikointi ja arviointi 2006, 19.)

Suurin osa tunnetuimmista estettävistä kansainvälisistä materiaaleista löytyy kaikkien toimittajien tuotteista, mutta suomenkielinen haitalliseksi katsottu aineisto ei aina päädy kansainvälisten tuotteiden piiriin. Myös kulttuuriset erot eri toimittajien järjestelmien kesken voivat aiheuttaa suodatinjärjestelmissä eroja. (Turvallisten sisältöjen valikointi ja arviointi 2006, 19.)

9.2 Suodatuksen toimintaperiaatteet

9.2.1 Valkoinen listaus (inclusion filtering)

Valkoista listaa (sallittu lista) käytettäessä vain suhteellisen pieni määrä osoitteita on määritetty sallituiksi ja yhteydet muualle Internetiin on estetty. Tämän tyyppinen suodatus voi olla 100 % tehokasta, koska vain hyväksyttyihin osoitteisiin on yhteys mahdollisuus. (Greenfield, Rickwood & Tran 2001, 7.)

9.2.2 Musta listaus (exclusion filtering)

Musta listaus (estolista) perustuu tunnettujen epäsopimattomien osoitteiden keräämiseen ja on suodatusmenetelmänä yleisempi kuin valkoinen listaus. Mustan listan etuna on koko muun Internetin salliminen, koska vain kielletyt osoitteet ovat estettyjä. Huonona puolenaan se saattaa sallia ei-haluttua liikennettä jota ei ole vielä luokiteltu tuotteen tarjoajan tai ylläpidon toimesta. (Greenfield, Rickwood & Tran 2001, 7.)

9.2.3 Sisällön analysointi (content filtering)

Sisällön analysoinnissa Internet-liikenne tarkastetaan, ennen kuin sen sallitaan mennä käyttäjälle. Tämän tyyppisessä suodatuksessa etsitään määriteltyjä avainsanoja verkkosivuilta tai muita tuntomerkkejä, joilla voidaan havaita ei-haluttua liikennettä. Sisällön suodatuksen dynaamisuus tekee siitä houkuttelevan, liikenne luokitellaan sen saapuessa eikä käsin koottuja listauksia tarvita. (Greenfield, Rickwood & Tran 2001, 7.)

9.2.4 Yhdistelmäsuodatus

Kaupalliset tuotteet usein yhdistelevät edellä mainittuja tekniikoita. Esimerkiksi pääasiallisesti voidaan käyttää estolistausta ja sen lisäksi valvoa Web-liikennettä sisällön analysoinnilla ei-toivottujen luokittelemattomien verkkosivustojen estämiseksi. (Greenfield, Rickwood & Tran 2001, 8.)

9.3 Lähteeseen perustuva suodatus

Lähteeseen perustuvassa suodatuksessa estetään kiellettyyn kohteeseen menevät pyynnöt tai sieltä palaavat vastaukset. Estäminen tapahtuu viestissä olevan URL-osoitteen tai paketin IP- osoitteen perusteella. (Greenfield, Rickwood & Tran 2001, 10.)

9.3.1 Pakettisuodatus

Kaikki Internet-liikenne välitetään paketteina, joilla on kohde- ja lähtöosoitteet. Pakettisuodatuksessa tarkastellaan paketin IP- osoitekenttiä ja estetään paketit jos ne tulevat kielletystä osoitteesta. Pakettisuodatus usein toteutetaan reitittimessä pääsylistalla (Access Control List). (Greenfield, Rickwood & Tran 2001, 10.)

9.3.2 URL-suodatus

URL suodatuksessa suodatus tapahtuu viestissä olevan URL-osoitteen perusteella (Greenfield, Rickwood & Tran 2001, 7).

9.4 Sisältöön perustuva suodatus

Sisältöön perustuvissa suodatustekniikoissa tarkastellaan sisään tulevaa liikennettä ja ulosmeneviä pyyntöjä, jotta voidaan määritellä, onko liikenne ei-toivottua. (Greenfield, Rickwood & Tran 2001, 8.)

9.4.1 Avainsanasuodatus

Avainsanasuodatuksessa tutkitaan Internet-liikenteestä sanoja, jotka ovat mustalla listalla. Sivuston lataus pysäytetään, jos se sisältään mitään sanoja estolistalta. Lisäksi useat tuotteet tutkivat myös latauspyynnöt ennen lähettämistä, jotta käyttäjät eivät pysty käyttämään hakukoneita kielletyn sisällön löytämiseen. (Greenfield, Rickwood & Tran 2001, 8.)

9.4.2 Lausekesuodatus

Lausekesuodatus on hienostuneempi versio avainsana suodatuksesta. Lauseke suodatuksessa tutkitaan sanoja lausekkeen osina. Tämä mahdollistaa suodatuksen tarkemman määrittelyn. (Greenfield, Rickwood & Tran 2001, 9.)

9.4.3 Profiilisuodatus

Profiilisuodatuksessa analysoidaan Internet-sisällön ominaisuuksia kuten kuva/teksti suhdetta sekä linkkejä muille tunnetuille kielletyille sivustoille. (Greenfield, Rickwood & Tran 2001, 9.)

9.4.4 Kuva-analyysisuodatus

Kuva-analyysisuodatuksessa tutkitaan käyttäjälle latautuvia kuvia. (Greenfield, Rickwood & Tran 2001, 9.)

10 Suodatus OSI- mallin tasoilla 4 ja 7

Vuosituhannen vaihteessa OSI-mallin kuljetuskerroksella (layer 4) toimiva tilallinen palomuuri oli riittävä rajoittamaan ei-toivottua liikennettä ja puolustamassa yleisimpiä uhkia vastaan. Suunnitelmallisella palomuuri määrityksellä, jossa valittiin tarkkaan sallitut TCP/IP osoitteet, portit ja liikenteen suunnat, oli mahdollista estää suurin osa ulkoapäin tulevista hyökkäyksistä sekä huomattavasti laskea ei-toivottujen verkkoyhteyksien määrää sisältä ulospäin. (From Network Security To Content Filtering 2007, 1.)

Kuljetuskerroksen palomuurit ovat edelleen tärkeimpiä verkkoturvallisuuden takaajia mutta toimiakseen tehokkaasti täytyy niiden pystyä tunnistamaan protokollat TCP/IP porttien perusteella sekä luottamaan kohteen ja lähettäjän IP-osoitteiden oikeellisuuteen. Tästä johtuen, kun uusia ohjelmistoja tai palveluja otetaan verkon sisällä käyttöön, joudutaan palomuuriin tekemään muutoksia, koska muuten nämä uudet sovellukset eivät pysty viestimään palomuurin läpi. Nykypäivänä sovelluskehittäjät ovat alkaneet kiertämään näitä protokollamäärityksiä helpottaakseen uusien ohjelmien toimintaa. (From Network Security To Content Filtering 2007, 1.)

Koska Web-selaus Internetissä on yleensä sallittu kulkemaan palomuurien läpi, tarjoavat monet sovellukset mahdollisuuden tunneloida liikenteensä kuin se olisi web-liikennettä. Osa ainoastaan käyttää Web-liikenteen porttia 80 liikennöintiinsä, toiset tunneloivat datan siirron HTTP-protokollalla niin että liikenne näyttää selaimen liikenteeltä. (From Network Security To Content Filtering 2007, 2.)

Jos suurin osa verkkoliikenteestä käyttää HTTP-porttia ja näyttää HTTP-liikenteeltä niin kuljetuskerroksen tilallinen palomuuri, joka suodattaa liikennettä TCP/IP-osoitteiden ja porttien perusteella, ei yksin pysty valvomaan verkon turvallisuutta. Tämän lisäksi IP-osoitteistukseen perustuvaa autentikointia ei voida pitää luotettavana koska tunnelointi, Network Access Translation (NAT) ja Virtual Private Networks (VPN) tekniikat tekevät lähettäjän tunnistamisen mahdottomaksi. (From Network Security To Content Filtering 2007, 2.)

Edellä mainituista syistä johtuen ei voida enää luottaa sovellusten käyttämiin portteihin datansiirron tyypin tunnistamisessa koska portin 80 liikenne voi olla melkein mitä tahansa. Tämä johtaa siihen että kun halutaan selvittää mitä dataa verkossa liikkuu, joudutaan analysoimaan TCP/IP-pakettien sisältöä sovelluskerroksella (layer 7). Tässä joudutaan kuitenkin ottamaan huomioon muutamia seikkoja:

- Nopeus: porttinumeron tarkastaminen on nopeaa mutta koko paketin datan analysoiminen vie enemmän aikaa. Analysoiminen saattaa vaikuttaa yhteyden nopeuteen tai palomuurin kuormitukseen.
- Protokolla analyysi: analysointia voidaan rajoittaa tarkastelemaan että datan formaatti on käytetyn protokollan mukainen, esimerkiksi portti 80 ja HTTP-protokolla. Tämä rajoittaa portin käyttöä muulta liikenteeltä mutta ei estä sovelluksia jotka käyttävät HTTP-protokollaa liikennöintiinsä.
- Sisällön analysointi: täydellinen sisällön analysointi olisi paras mahdollinen turvallisuusratkaisu mutta sen toteuttaminen on hankalaa. Kun lähes mitä tahansa liikennettä voidaan tunneloida HTTP-muodossa, miten erotamme ”hyvän” liikenteen ”huonosta”?
- Sisällön suodatus: suodatuksella voidaan liikenteestä suodattaa pois paketit jotka tiedetään ”huonoiksi” eli vaikuttavat epäilyttäviltä, eivät noudata standardeja tai eivät ole turvakäytäntöjen mukaisia. Tämäkin vaatii jokaisen paketin sisällön täydellistä analysointia mutta nyt etsitään vain tunnettuja hyökkäyksiä tai kiellettyä liikennettä sen sijaan että yritettäisiin tunnistaa liikenteen data täydellisesti. (From Network Security To Content Filtering 2007, 3.)

Sovelluskerroksella tapahtuva suodatus toteutetaan yleensä välitys- tai yhdyskäytäväpalvelimella. Asiakkaan ja palvelimen välillä oleva välityspalvelin kaappaa paketit ja käyttäytyy asiakasta kohtaan kuin se olisi kohdepalvelin, kohdepalvelimelle välityspalvelin käyttäytyy kuin se olisi asiakas. Näin välityspalvelin katkaisee yhteyden kahteen osaan ja pystyy tarkastamaan kaikkien pakettien sisällön niiden kulkiessa sen läpi. (From Network Security To Content Filtering 2007, 4.)

11 SUODATUSTEKNIIKAT KÄYTÄNNÖSSÄ

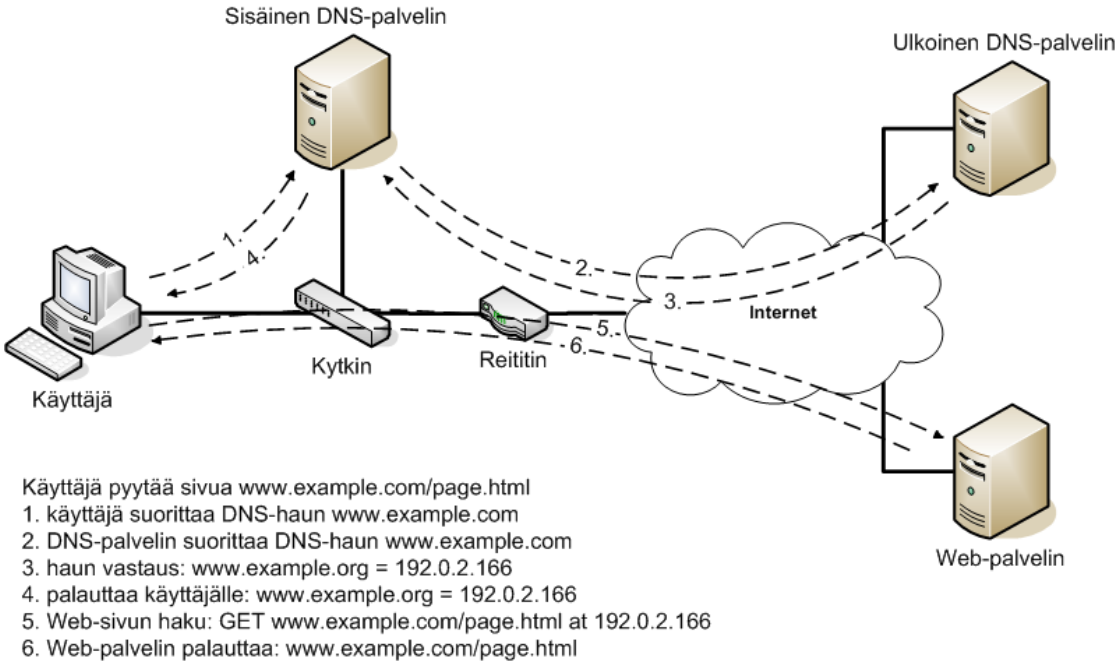
11.1 Yleistä

On monia tekniikoita joita voidaan käyttää Internet-sisällön estämiseen. Tärkeimpiä näistä ovat IP-osoitteen estäminen, DNS-suodatus sekä välityspalvelin pohjainen analysointi. (Access Denied 2008, 12 -13.)

Kaikkia edellä mainittuja tekniikoita voidaan myös käyttää käyttäjän ohjaamiseen toiselle verkkosivulle hänen hakemansa sivuston sijasta. Eri suodatustekniikoilla voidaan myös rakentaa erilaisilla näkyvyysasteilla toimivia suodatuksia. Tällä tavoin voidaan yrittää salata suodatustapahtumaa tai jos käytetään estosivua, on käyttäjälle selvää että haluttu sivusto on tietoisesti estetty. (Access Denied 2008, 15 -16.)

11.2 Tavallinen Web-sivun haku

Normaali Web-sivun hakeminen noudattaa seuraavaa kaavaa. Jos halutun osoitteen IP-osoite ei ole tietokoneen välimuistissa, suoritetaan ensimmäisenä DNS–haku, jossa selain lähettää kyselyn määritetylle DNS-nimipalvelimelle. Jos palvelin ei tiedä haettua osoitetta, se lähettää kyselyn eteenpäin ylemmälle palvelimelle, joka tarvittaessa toimittaa kyselyn eteenpäin, kunnes domainin example.com IP-osoite löytyy. Kun IP-osoite on saatu määritettyä, selain ottaa yhteyden kohdepalvelimeen ja pyytää sivua, jonka palvelin palauttaa käyttäjälle. (Access Denied 2008, 58.) Tämä tapahtumaketju on esitetty kuviossa 7 jossa käyttäjä hakee Web-selaimella verkkosivua www.example.com/page.html.



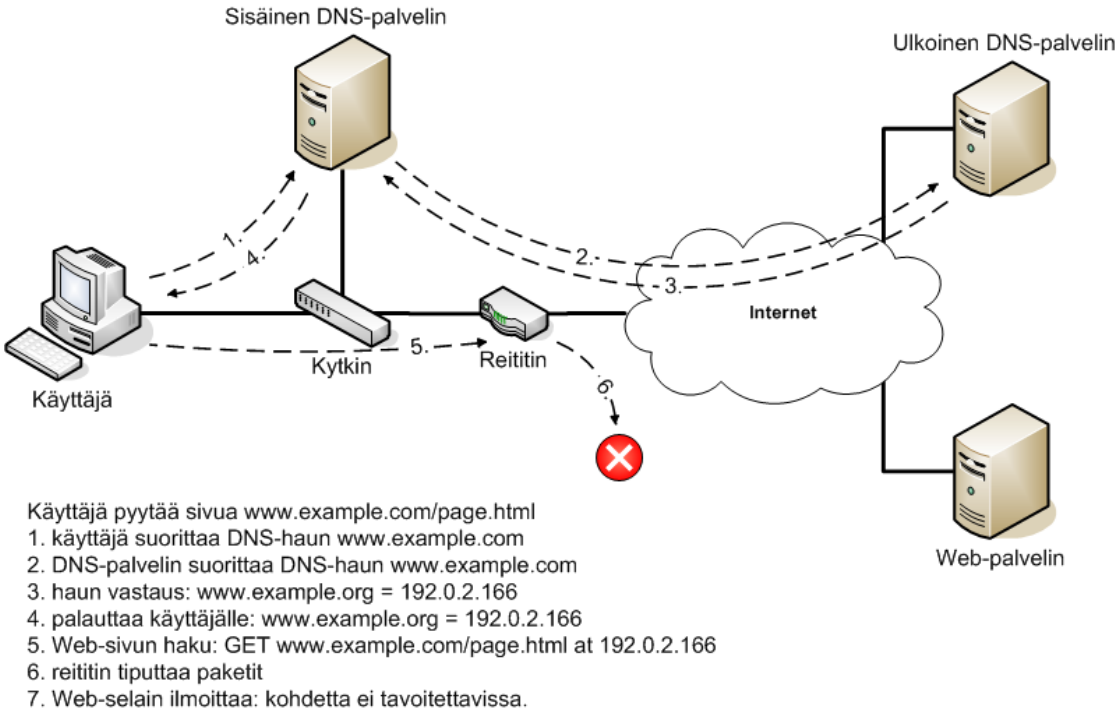
KUVIO 7. Web-sivun haku

11.3 TCP/IP-otsakesuodatus

IP-osoitteen estäminen on tehokas tapa estää liikenne kohteeseen, eikä sen toteuttamiseen yleensä tarvitse hankkia uutta tekniikkaa. IP-osoitteisiin perustuvan estämisen huonona puolena on huomattava yli-estämisen mahdollisuus koska osoitteen takana saattaa olla muitakin, eston syyhyn liittymättömiä, palvelimia ja nettisivuja, joiden käyttö myös estyy. (Access Denied 2008, 13.)

IP-paketti koostuu osoitetiedot sisältävästä otsakkeesta, sekä hyötykuormasta, joka sisältää siirrettävän datan. Reitittimet tutkivat otsakkeen osoitetiedot löytääkseen IP-osoitteen. Kun halutaan estää tiettyjen kohdepalvelinten käytön, voidaan reitittimet konfiguroida pudottamaan paketit, jotka ovat matkalla ei-listalla olevaan kohteeseen. Yksi kohdepalvelin saattaa kuitenkin ylläpitää useampaa palvelua, kuten Web-sivuja ja e-mail palvelinta. Tällöin pelkällä IP-osoitteella suoritettu estäminen kieltää kaikkien näiden palveluiden käytön. On myös hyvä huomioida että saman IP-osoitteen takana voi olla useampiakin verkkopalvelimia, sekä domaineja ja tällöin liikenne myös niihin estyy. (Access Denied 2008, 59.)

Tarkempi estäminen voidaan suorittaa kun käytetään ei-listassa myös porttinumeroita, jotka myös löytyvät TCP/IP-otsakkeesta. Yleensä Internet-sovellukset käyttävät tiettyä porttinumeroa, joiden perusteella reitittimet voivat tehdä arvion siitä, minkä palvelun liikennettä paketti sisältää. Näin ollen jos halutaan estää vain Web-liikenne tiettyyn osoitteeseen, voidaan estää liikenne porttiin 80, jota Web-palvelimet yleensä käyttävät. (Access Denied 2008, 59.) Kuviossa 8 havainnollistetaan IP-osoitteeseen perustuvan suodatuksen toiminta.

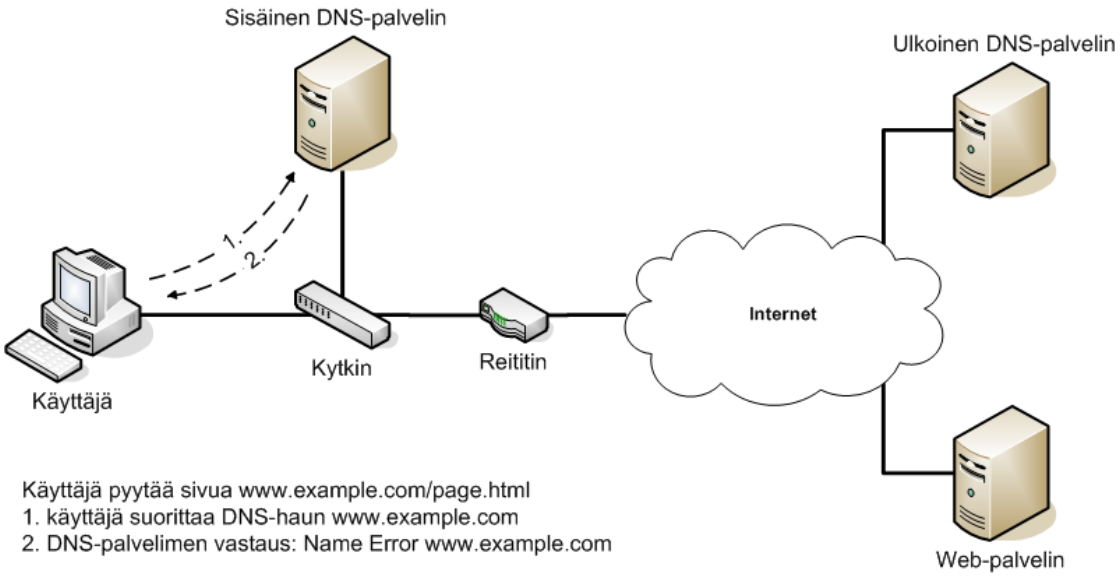


KUVIO 8. IP-osoitteen esto

11.4 DNS-suodatus

Suurimmassa osassa Internet-kommunikaatiota, etenkin Web-selauksessa, käytetään domain-nimiä IP-osoitteiden sijaan. DNS-kyselyjä suodattamalla voidaan kiellettyjä sivustoja tehokkaasti estää. Tässä toiminnassa DNS-palvelimelle määritellään lista kielletyistä domain-nimistä. Kun käyttäjä tekee IP-osoitteen ratkaisupyynnön jollekin näistä sivuista, palauttaa palvelin käyttäjälle virheilmoituksen. Ilman IP-osoitetta ei käyttäjä pysty tavoittamaan kohdepalvelinta. DNS-vaiheessa tapahtuva suodatus tapahtuu ennen kuin käyttäjä lähettää pyyntöä varsinaiselle kohdesivustolle, joten

domainin kaikki alasivustot ovat estettyjä. Kuvio 9 havainnollistaa DNS-suodatuksen toiminnan. (Access Denied 2008, 60 -61.)



KUVIO 9. DNS-suodatus

Toinen tapa rajoittaa ei-toivottua liikennettä DNS-palvelimella on DNS-tietojen muuttaminen. DNS-tietojen muuttamisessa liikenne kohteeseen estetään syöttämällä DNS-palvelimen tietoihin virheellinen IP-osoitekenttä, jolloin DNS-kysely palauttaa väärän IP-osoitteen. Tämä osoite voi olla esimerkiksi joku muu Web-palvelin, epäpätevä osoite kuten 0.0.0.0 tai localhost (127.0.0.1) osoite. (Access Denied 2008, 13 - 14.)

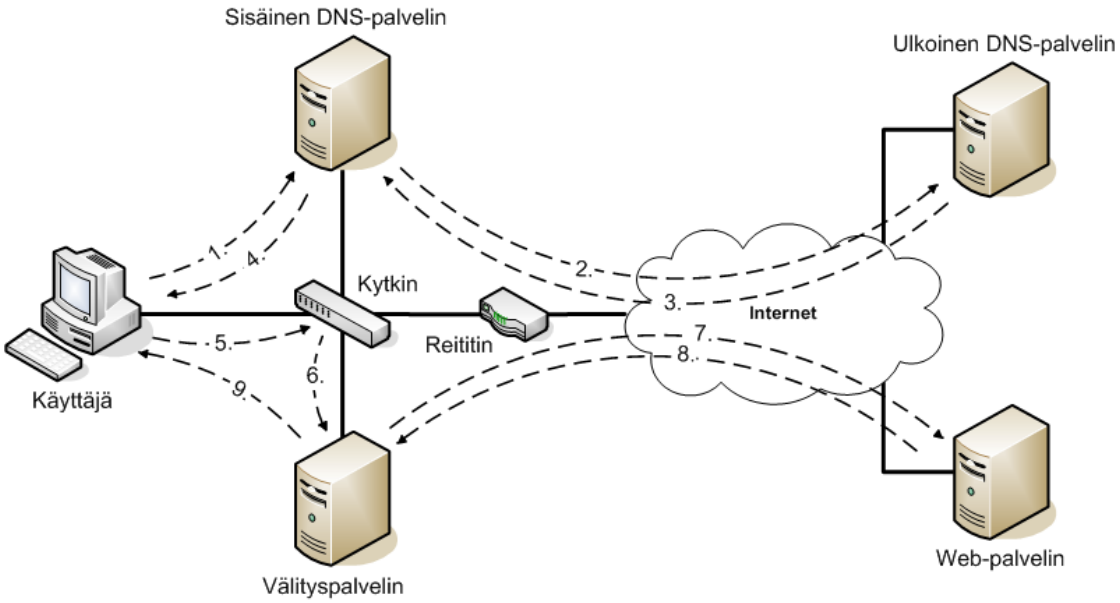
Vaikka DNS-palvelimella toteutettu suodatus tarjoaa helpon tavan estää tietyt verkko-osoitteen, se on myös helppo kiertää. Tämä on mahdollista käyttämällä osoitteena suoraa IP-osoitetta tai asettamalla tietokoneen käyttämään jotain muuta DNS-palvelinta, ellei tätä ole sisäverkossa tai käyttäjän oikeuksissa estetty. (Access Denied 2008, 14.)

11.5 Välityspalvelinsuodatus

Verkko voidaan konfiguroida niin, että käyttäjät eivät suoraan keskustele kohdepalvelimen kanssa, vaan liikenteen välikätenä toimii välityspalvelin. Tässä tilanteessa

Web-sivun haku toimii hieman eri tavoilla riippuen siitä onko välityspalvelin toteutettu määriteltynä vai läpinäkyvänä.

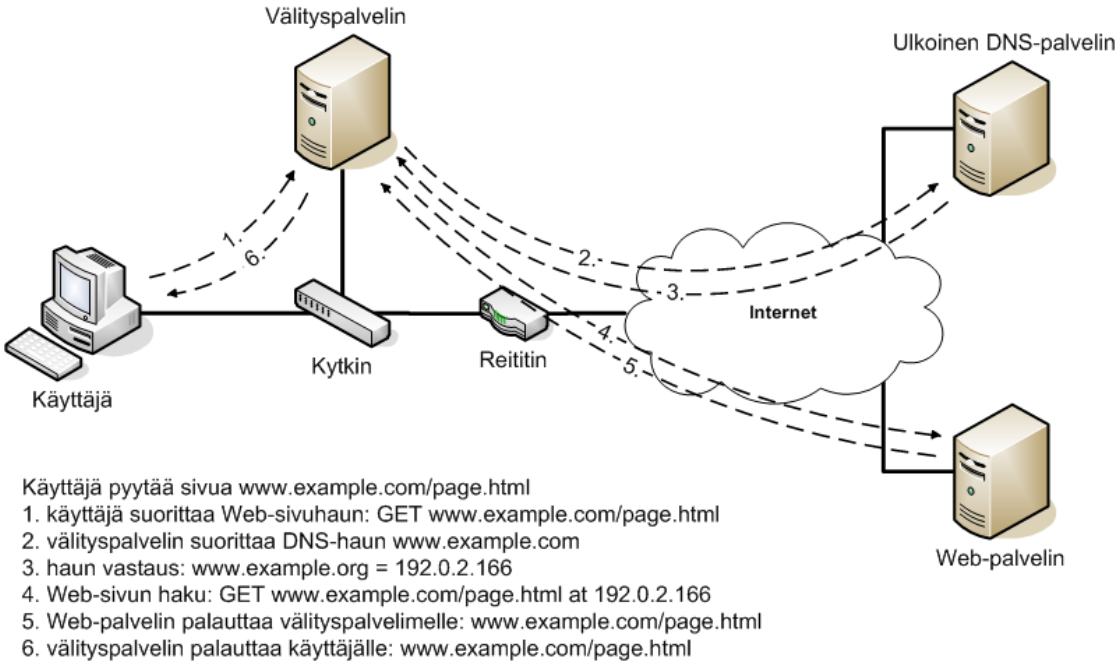
Läpinäkyvän välityspalvelimen käyttö vaatii että verkossa ohjataan HTTP-liikenne, esimerkiksi TCP/IP-otsakesuodatuksella välityspalvelimelle, joka kaappaa liikenteen ja välittää sen eteenpäin (ks. kuvio 12). Toiminta voidaan varmistaa ohjelmoimalla reititin estämään HTTP-liikenne joka ei kulje välityspalvelimen kautta. (Access Denied 2008, 61 -62.)



Käyttäjä pyytää sivua www.example.com/page.html
1. käyttäjä suorittaa DNS-haun www.example.com
2. DNS-palvelin suorittaa DNS-haun www.example.com
3. haun vastaus: www.example.org = 192.0.2.166
4. palauttaa käyttäjälle: www.example.org = 192.0.2.166
5. Web-sivun haku: GET www.example.com/page.html at 192.0.2.166
6. kytkin ohjaa HTTP-viestin välityspalvelimelle
7. Web-sivun haku: GET www.example.com/page.html at 192.0.2.166
8. Web-palvelin palauttaa välityspalvelimelle: www.example.com/page.html
9. välityspalvelin palauttaa käyttäjälle: www.example.com/page.html

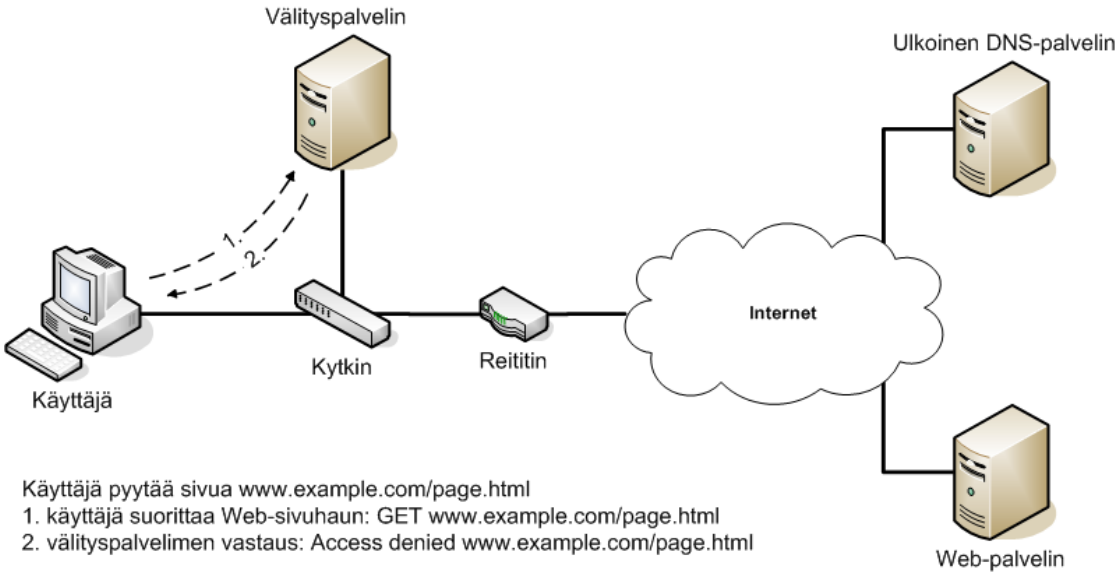
KUVIO 10. Läpinäkyvä välityspalvelin

Läpinäkymätöntä, määriteltyä, välityspalvelinta käytettäessä käyttäjä lähettää Web-sivun hakupyynnön suoraan välityspalvelimelle, luottaen että välityspalvelin suorittaa myös DNS-haun jos siihen on tarvetta (ks. kuvio 11). (Access Denied 2008, 61 -62.)



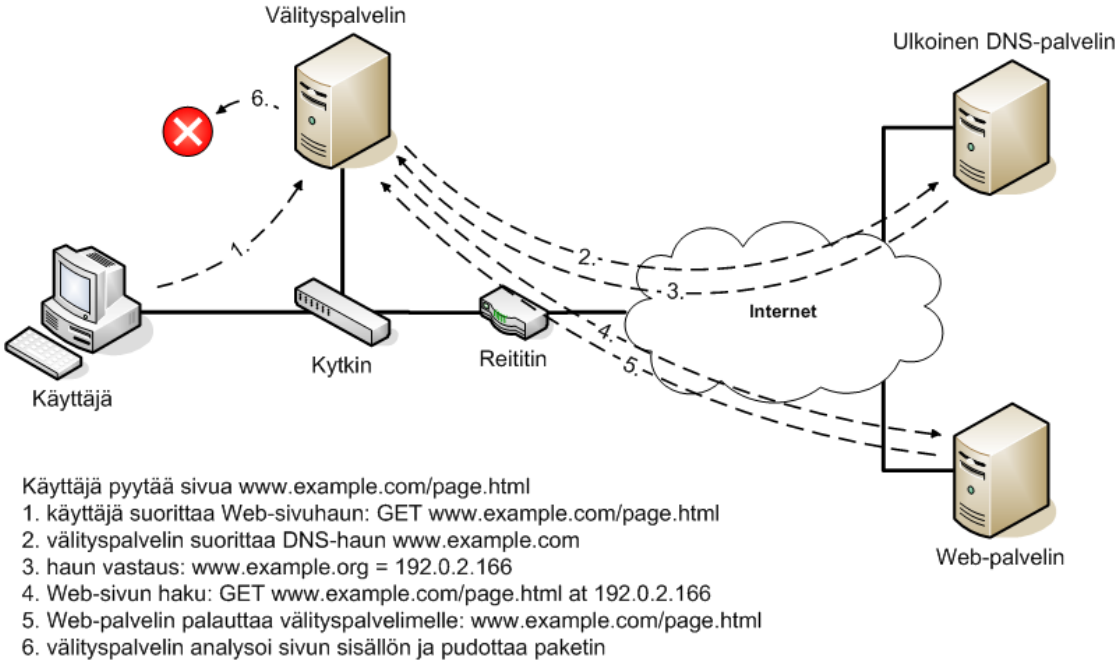
KUVIO 11. Määritetty välityspalvelin

Välityspalvelinpohjaisessa suodatuksessa Internet-liikenne kulkee suodatusjärjestelmän läpi, joka analysoi välitettävän paketin ja tarkastaa sen HTTP-osoitteen estolistan perusteella. Listassa voidaan käyttää yksittäisiä domaineja, ala-domaineja, kokonaisia URL-osoitteita, tai avainsanoja domain ja URL osioissa. Kun kiellettyä liikennettä havaitaan, sen kulku estetään ja käyttäjälle lähetetään virhe- tai estoviesti (ks. kuvio 12). (Access Denied 2008, 15.)



KUVIO 12. Välityspalvelimella tapahtuva URL-suodatus

Välityspalvelin voidaan asettaa myös suorittamaan sisällön analysointi läpikulkevalle HTTP-liikenteelle. Jos kuljetettava paketti sisältää tietoa mikä on määrätty estettäväksi, voi palvelin tehdä erilaisia ratkaisuja. Kielletty data voidaan leikata pois paketin sisältä tai paketin eteneminen voidaan estää. On mahdollista myös lisätä URL-osoite kieltolistaa ja estää tiedonsiirto osoitteesta. Kuviossa 13 esitetään HTTP välityspalvelimen liikenteen sisältösuodatuksen toiminta. (Access Denied 2008, 63.)



KUVIO 13. Välityspalvelimella tapahtuva sisällönsuodatus

11.6 Yhdyskäytäväpalvelinsuodatus

Yhdyskäytäväpalvelin voi käyttää edellä kuvattuja tekniikoita, sekä tarjota erilaisia mahdollisuuksia yhdistellä niitä. Esimerkiksi tietyistä IP-osoitteista, joita pidetään epäilyttävinä, tulevat viestit voidaan ohjata läpinäkyvään HTTP-välityspalvelimeen. Välityspalvelin suorittaa niille sisältöanalyysi ja jos kiellettyä sisältöä löytyy, sen kulku estetään. Muutoin liikenne kulkee normaalisti. Yhdyskäytäväpalvelin yleensä pystyy analysoimaan myös useiden eri protokollien pakettien sisältöä. (Access Denied 2008, 63- 64.)

12 SUODATUSTEKNIIKOIDEN TESTAUS

12.1 Testiympäristö

Edellisissä luvuissa esiteltyjen suodatustekniikoiden testaamista varten pystytettiin testiympäristö. Testiympäristönä toimi kolme pc-tietokonetta sekä reitittävä kytkin. Kahdelle pc-tietokoneelle asennettiin Windows Server R2 64-bittinen palvelinkäyttöjärjestelmä ja asiakaskoneelle Windows 7 64-bittinen käyttöjärjestelmä. Käyttöjärjestelmät saatiin Microsoft MSDN Academic Alliance palvelun kautta. Asennustoimenpiteiden jälkeen käyttöjärjestelmiin ladattiin viimeisimmät päivitykset Windows Updaten avulla. Reitittävän kytkimen toimintaan ei, IP-osoitteen asettamisen lisäksi, tehty muutoksia.

Käytössä olleet koneet olivat muutaman vuoden vanhoja ja nykypäivän laitteisiin verrattuna melko hitaita mutta työn tekemiseen täysin riittäviä.

- Prosessori: Inter Core2 6700 2,67GHz
- Muisti: 2GB

Käyttöjärjestelmien asentamisen jälkeen rakennettiin testaamista varten domain STUDYDOMAIN.JAMK.FI. Domainin rakentaminen aloitettiin asentamalla SERVER-palvelimelle Domain Controller-tehtävän vaatimat palvelut. Seuraavana Active Directoryssä luotiin organisaatioyksikkö Studydomain, jonka sisään luotiin organisaatioyksiköt Admins, Clients, ja People.

- Admins, pääkäyttäjätunnukset.
- People, tavalliset käyttäjätunnukset.
- Clients, verkon tietokoneet.

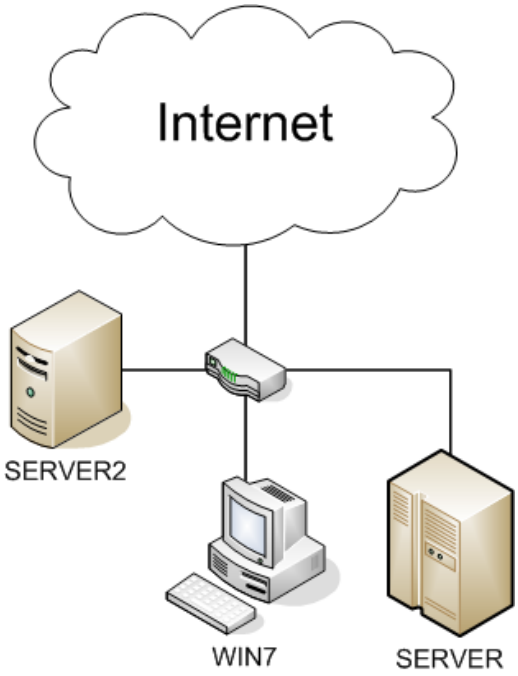
Lisäksi luotiin niille määriteltyihin organisaatioyksikköihin ADMIN käyttäjätunnus pääkäyttäjälle ja muutamia tavallisia käyttäjätunnuksia suodatuksen testausta var-

ten. Näillä toimenpiteillä saatiin hallinnasta selkeämpi kuin jos olisi käytetty Active Directoryn valmiita organisaatioyksiköitä ja käyttäjätunnuksia. Tämän jälkeen SERVER2 ja WIN7 koneet nimettiin ja liitettiin domainiin. Näin saatiin kaikki laitteet yhdistettyä ympäristöön jota voitiin hallita keskitetysti Domain Controller palvelimelta.

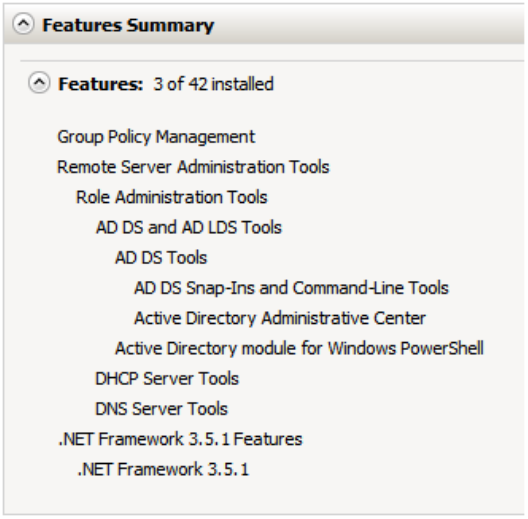
TAULUKKO 1. Verkon laitteiden tiedot

Nimi	Tehtävä	Palvelut / Ohjelmistot	IP-osoitteet
SERVER	Domain Controller	Active Directory, DHCP & DNS	192.168.1.10
SERVER2	Suodatuspalvelin	Suodatusohjelmistot	192.168.1.30
WIN7	Asiakaskone	Internet Explorer 8	DHCP:n myöntämä
Kytkin			192.168.1.1

Kuviossa 14 näkyy työssä käytetyn lähiverkon topologia ja kuviossa 15 SERVER-palvelimelle asennetut palvelut.



KUVIO 14. Lähiverkon topologia



KUVIO 15. Domain Controller-palvelimelle asennetut palvelut

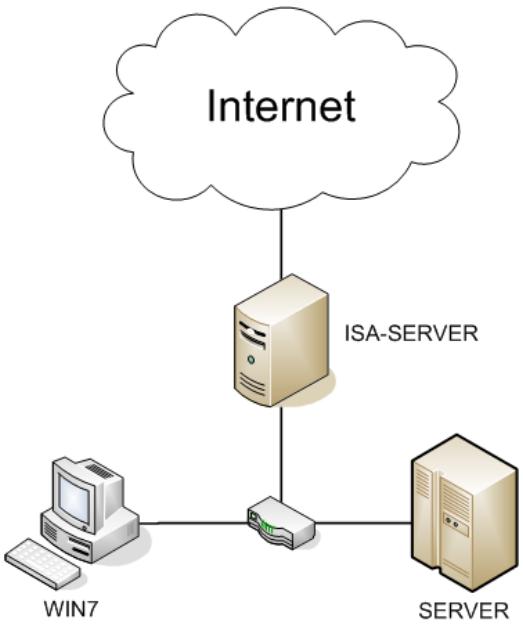
12.2 Ohjelmistojen testaus

Testien suorittaminen toteutettiin asentamalla testattavana oleva ohjelmisto SERVER2 palvelimelle. Tämä jälkeen tehtiin mahdolliset Active Directory tai DHCP-muutokset, jos niihin oli tarvetta. Testien suorittamisen jälkeen testattavana ollut ohjelmisto poistettiin kokonaan mahdollisten konfliktien välttämiseksi. Kaikki ohjelmistot asentuivat oikein ja lisäsivät itsensä käyttöjärjestelmän palvelulistaan (Services). Kaikki ohjelmat toimivat moitteettomasti, lukuun ottamatta WinGate Proxy Server joka asennuksen ja palvelimen uudelleen käynnistysten yhteydessä laittoi kaikki palvelunsa päälle, vaikka niitä oli kielletty ajamasta. Tämä käytös havaittiin joka käynnistyksen jälkeen.

Verkon ja suodatusmenetelmien toiminnan tarkkailemiseksi palvelimille ja asiakaskoneelle asennettiin Microsoft Network Monitor 3.3. Tämä ohjelma on protokolla-analysaattori ja verkkoliikenteen kaappaustyökalu. Tämän ohjelmiston käyttö mahdollisti verkkoliikenteen täydellisen analysoimisen ja tehtyjen suodatusratkaisujen toiminnan varmistamisen. Heinäkuun alussa ohjelma päivitettiin uusimpaan 3.4 versioon joka oli julkaistu muutama päivä aikaisemmin.

12.3 Testiympäristön vaatimat muutokset

Yhdyskäytäväpalvelin ohjelmistojen testejä varten täytyi verkon topologiaan tehdä muutoksia. SERVER2 siirrettiin yhdyskäytäväpalvelimeksi ulko- ja sisäverkkojen väliin jolloin kaikki liikenne saatiin kulkemaan sen läpi. Nimeksi vaihdettiin ISA-SERVER joka kuvasi palvelimen uutta roolia paremmin. Verkon rakenteeseen tehdyt muutokset näkyvät kuviossa 16.



KUVIO 16. Gateway-topologia

12.4 Testiohjelmistojen valinta

Testattavia ohjelmistoja valitessa olivat valintakriteereinä seuraavat asiat.

1. Ohjelmiston täytyi toimia 64-bittisessä Windows-ympäristössä.
2. Ohjelmiston täytyi pystyä suodattamaan koko verkon liikenne sekä tarvittaessa skaalautua isommankin tietoverkon tarpeisiin.
3. Ohjelmiston tuli olla palvelinohjelmisto ja toimia niin ettei asiakaskoneeseen tarvinnut asentaa ylimääräisiä ohjelmia.
4. Ohjelmiston tuli tarjota mahdollisuus suodatuksen automatisoimiseen esimerkiksi Web-sivujen luokituksella.
5. Active Directoryn hyödyntäminen käyttäjien, verkkoliikenteen ja suodatuksen kontrolloinnissa.
6. Helppo käytettävyys ja hallinta.
7. Ohjelmistosta tuli olla saatavilla ilmainen testiversio.

Alkututkimuksissa mukana oli noin kaksikymmentä erilaista DNS, välityspalvelin, yhdyskäytäväpalvelin sekä virustorjuntaohjelmistoa, joita verrattiin asetettuihin vaatimuksiin. Näistä ohjelmistoista suurin osa karsiutui hyvin nopeasti pois, yleensä suuresti käsityötä vaativan suodatuksenhallinnan vuoksi. Monet näistä karsiutuneista ohjelmista tarjosivat tehokkaita mahdollisuuksia suodattaa, joko Web-sivun sisällön tai URL-osoitteiden perusteella, käyttäen Perl-ohjelmointikielellä luotuja lausekkeita. Nämä olisi kuitenkin pitänyt luoda ja ylläpitää manuaalisesti mikä katsottiin liian työlääksi, hankalaksi ja aikaa vieväksi.

Virustorjunta ohjelmia ei testeihin valittu koska kaikki alkuvaiheessa tarkastellut virustorjuntaohjelmistot olivat kotikäyttäjille suunnattuja, vaativat ohjelman asentamista asiakaskoneelle, eivätkä yleensä tukeneet keskitettyä hallintaa. Useimmat virustorjuntaohjelmien valmistajat myyvät myös omia välitys- tai yhdyskäytäväpalvelin ratkaisujaan sisällönsuodatukseen. Nämä tuotteet kuitenkin yleensä toimitetaan omilla erillispalvelimillaan joten niitä ei voitu työhön sisällyttää.

Kolmannen osapuolen suodatuspalveluja löytyi jokaiselta Internet-palveluntarjoajalta. Näistä ei kuitenkaan ollut saatavilla ilmaisia testiversioita ja niitä

markkinoidaan yleensä vain operaattorien oman verkon asiakkaille. Myös monet erilaisia tietopalveluja tarjoavat yritykset myyvät kolmannen osapuolen ratkaisuja. Näitä ei kuitenkaan testeihin otettu koska haluttiin pitäytyä vakiintuneissa tuotteissa.

Alustavan tutkimustyön pohjalta lopullisiin testeihin ja esittelyyn valikoitui kuusi ohjelmistoa, jotka edustavat varsin kattavasti yleisimpiä sisällön- ja liikenteensuodatuksen menetelmiä.

TAULUKKO 2. Testaukseen valitut ohjelmistot

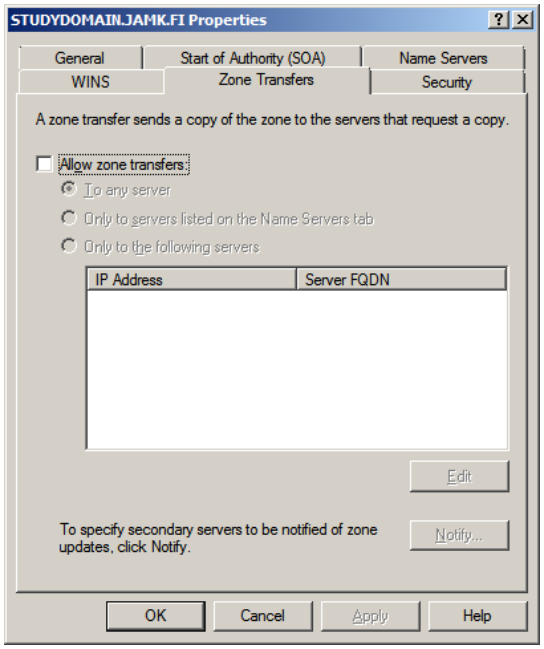
DNS-ratkaisut	Windows DNS
	Simple DNS
	OpenDNS
Välityspalvelin	WinGate Proxy Server
Yhdyskäytäväpalvelimet	Microsoft Forefront TMG
	Kerio Control

13 DNS-SUODATUS

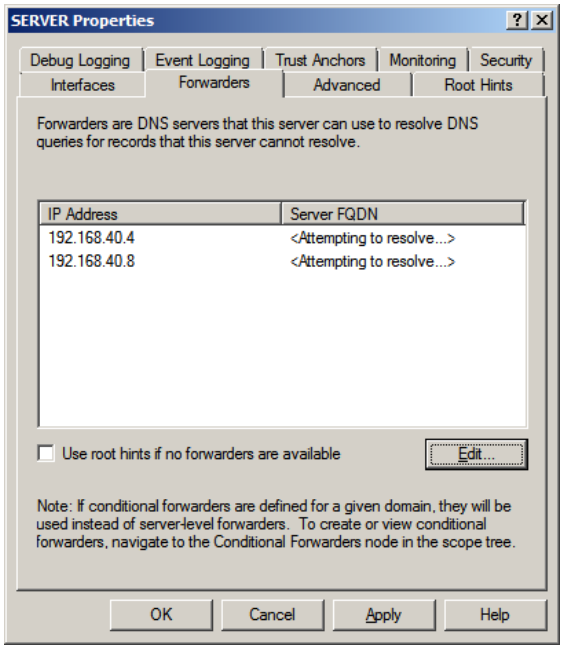
13.1 DNS-palvelimen sijoittaminen lähiverkkoon

Active Directory domainin tietokoneet tarvitsevat DNS-palvelimen löytääkseen Domain Controller palvelimen. Tämä sisäinen DNS-palvelin on suositeltavaa suojata häiriöiltä ja hyökkäyksiltä asentamalla puolueettomalle vyöhykkeelle ulkoinen DNS-palvelin. Sisäisen DNS-palvelimen ei tulisi koskaan olla sallittua kommunikoida suoraan ulkoverkkoihin. Kun asiakaslaitteiden lähettämät DNS-kyselyt tulevat ensin sisäiselle DNS-palvelimelle, tämä ohjaa ulospäin suuntautuvat kyselyt määritetylle ulkoiselle DNS-palvelimelle. Tämä ulkoinen palvelin vastaa kaikesta DNS-liikenteestä sisäverkosta Internetiin. (Davies & Northrup 2008, 174 -175.)

Lisäturvallisuutta sisäiselle DNS-palvelimelle Active Directory domainia käytettäessä saadaan kun kielletään zone transfer toiminnot (ks. kuvio 17) jotka ovat Active Directoryn kanssa tarpeettomia, sekä poistetaan root hints käytöstä koska kaikki ulkoiset DNS-kyselyt halutaan ohjata vain nimetylle ulkoiselle DNS-palvelimelle (ks. kuvio 18) (Davies & Northrup 2008, 178 -179). Nämä muutokset tehtyyn SERVER-palvelimen DNS-palveluun ja ulkoiset DNS-kyselyt ohjattiin Jyväskylän ammattikorkeakoulun DNS-palvelimille.



KUVIO 17. Zone transfer poisto.



KUVIO 18. Root hints poisto.

13.2 Microsoft DNS

13.2.1 Yleistä

Tämän työn testiympäristössä, kuten Windows-verkoissa yleensä, Microsoft DNS palvelin on asennettu toimimaan sisäisenä DNS-palvelimena, jonka tärkeimpänä roolina on ylläpitää tietoja Active Directory-tietokannan jäsenistä, jotta verkossa toimivat laitteet löytävät toisensa. Tällaista sisäistä DNS-palvelinta ei tulisi ikinä käyttää ulkoverkkoon suuntautuvan liikenteen suodatukseen, koska sisäisellä palvelimella ei pitäisi olla mitään tietoja verkoista jotka ovat sen oman hallintoalueen ulkopuolella, eikä Microsoft DNS tuekaan mitään liikenteen suodatusmenetelmiä. Liikennettä ei-

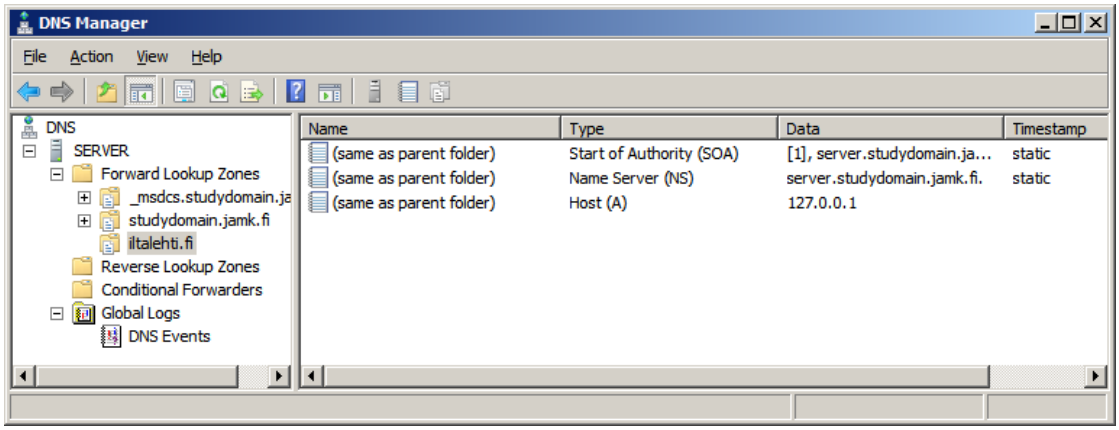
toivottuun domainiin voidaan kuitenkin hätätapauksessa estää DNS-tietoja muuttamalla.

13.2.2 DNS-tietojen muuttaminen

Muuttamisessa lisätään DNS-tietokantaan seuraavat tiedot: domain-nimi, hallitseva palvelin, palvelimen nimi sekä IP-osoite minne kyselyn tehnyt käyttäjä halutaan ohjata, tässä tapauksessa localhost-osoite mutta osoitteena voisi yhtä hyvin olla vaikka verkon sisäinen Web-palvelin. DNS-palvelimelle lisätyt tiedot näkyvät taulukossa 2 sekä kuviossa 19.

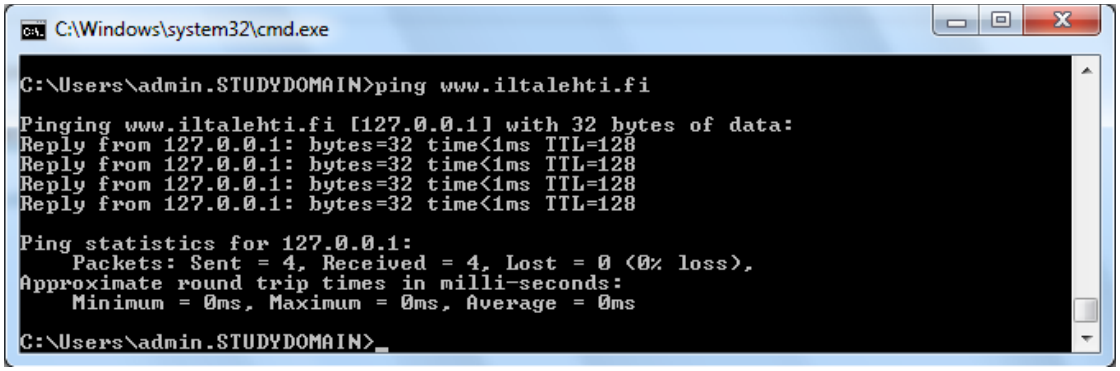
TAULUKKO 3. DNS-tietojen muuttamisessa tietokantaan lisätyt tiedot

Tietotyyppi	**Selitys**	**Data**
Forward Lookup Zone	domain-nimi	iltalehti.fi
Start of Authority (SOA)	hallitseva palvelin	[1], server.studydomain.jamk.fi
Name Server (NS)	palvelimen nimi	server.studydomain.jamk.fi
Host (A)	IP-osoite	127.0.0.1



KUVIO 19. DNS-tietojen muuttaminen

Kuviosta 20 havaitaan ping ohjelmaa käyttäen DNS-tietomuutoksen vaikutukset ja nähdään liikenteen kääntyvän asettamaamme IP-osoitteeseen.



KUVIO 20. DNS-muutoksen testaus ping ohjelmalla

13.3 Simple DNS Plus

13.3.1 Yleistä

Simple DNS Plus on JH Softwaren kehittämä, yksinkertainen ja käyttäjäystävällinen DNS-palvelinohjelmisto. Simple DNS Plus:n hallinta on toteutettu helppokäyttöisen käyttöliittymän avulla, jossa kaikki säätömahdollisuudet ja asetukset ovat helposti saatavilla. Se tarjoaa myös asennusavusteita tavallisimpien toimintojen kuten uusien alueiden ja päivitysten tekemiseen. Mukana on myös monia tietoturvaominaisuuksia, jotka helpottavat suojautumista erilaisia hyökkäyksiä vastaan. Lisäksi Simple DNS Plus mahdollistaa yksityiskohtaisen lokin tekstimuodossa sekä tilannekuvan (snapshot) DNS-palvelimeen tallentuneista osoitetiedoista. (Simple DNS Plus 2010.)

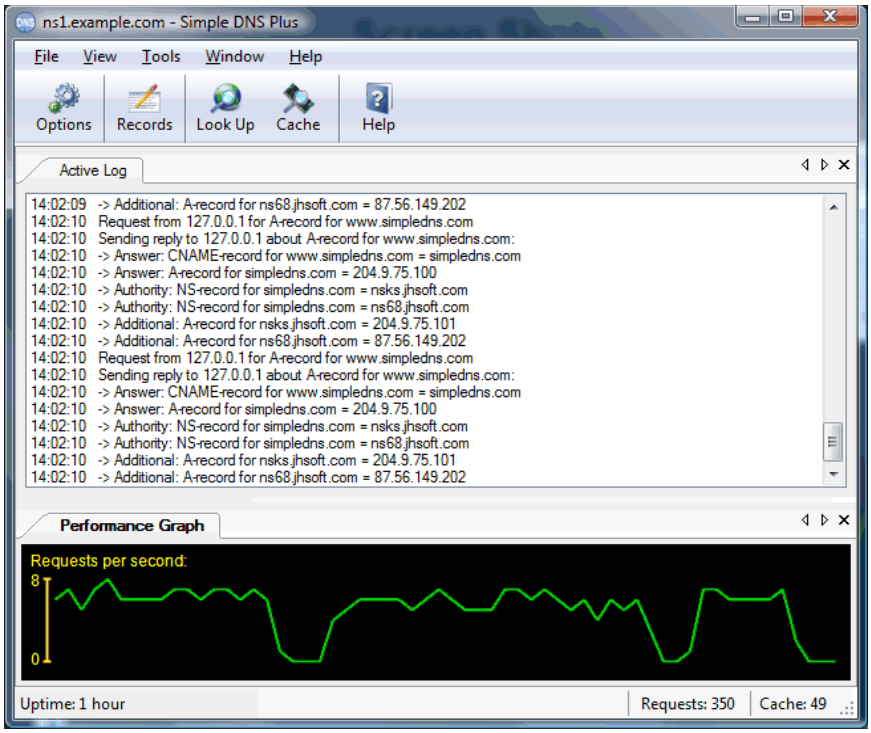
Valmiiden ominaisuuksien lisäksi Simple DNS Plus sisältää liitännäisjärjestelmän (plug-in system) joka mahdollistaa kolmannen osapuolen, sekä ohjelmiston valmistajan vaihtoehtoisten toiminnallisuuksien lisäämisen. Liitännäiset tarjoavat erilaisia lisätoimintoja kuten HTTP-liikenteen uudelleenohjauksen, DHCP-palvelimen, sekä tärkeimpänä verkko-osoitteen ei-listaus (Domain Blacklist) ominaisuuden jolla voidaan luoda kieltolista domaineille joihin ei haluta käyttäjien pääsevän. (Simple DNS Plus 2010.)

13.3.2 Käyttöliittymä

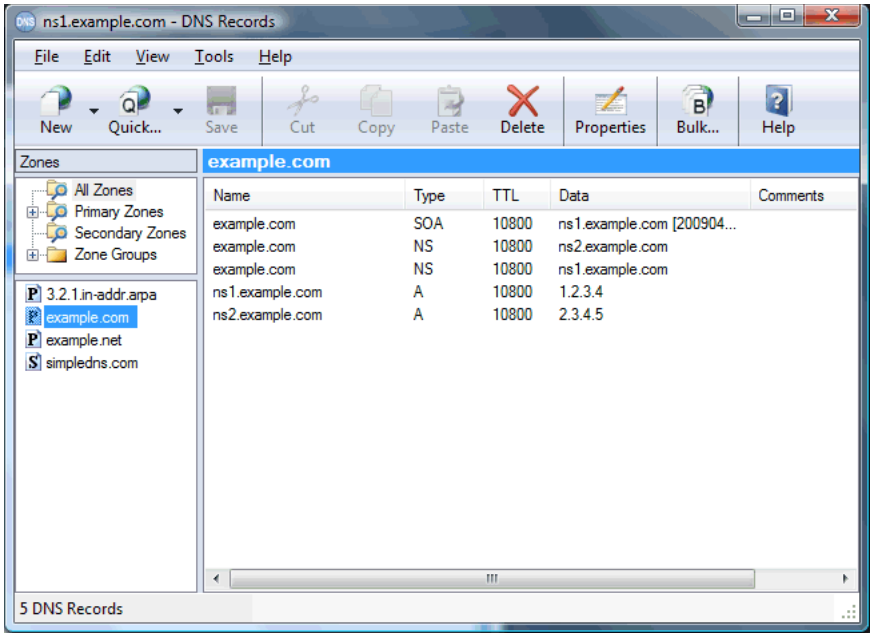
Simple DNS Plus:n käyttäjäliittymä koostuu neljästä päämodulista

- Pääikkuna: jonka kautta tarkkaillaan palvelimen toimintaa sekä tehdä säätötoimenpiteitä ja lisätä tai poistaa palveluita. (Ks. kuvio 21.)
- DNS-tietoikkuna: näyttää hallinnoitavat alueet ja DNS-tiedot, sekä mahdollistaa näiden lisäämisen, poistamisen ja muuttamisen. (Ks. kuvio 22.)
- DNS-kyselyikkuna: työkalu jonka avulla voi suorittaa kyselyjä toisille DNS-palvelimille. (Ks. kuvio 23.)
- DNS-välimuistin tilannekuvaikkuna: näyttää välimuistiin tallennetut osoitetiedot Windows-tyyppisessä tiedostonäkymässä. (Ks. kuvio 24.)

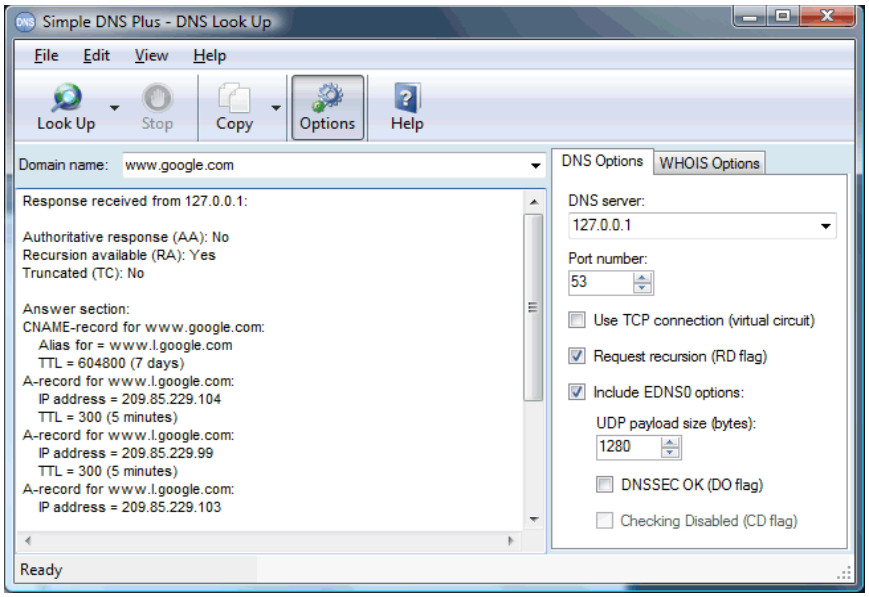
Jokainen näistä moduuleista toimii erillisenä prosessina jotka voivat toimia itsenäisesti, riippumatta muista moduuleista. (Simple DNS Plus 2010.)



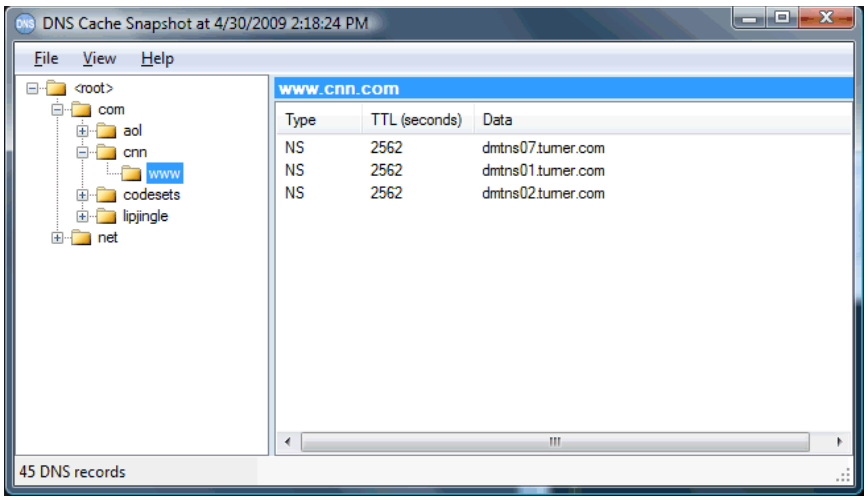
KUVIO 21. Simple DNS Pääikkuna (Simple DNS Plus 2010)



KUVIO 22. DNS-tietoikkuna (Simple DNS Plus 2010)



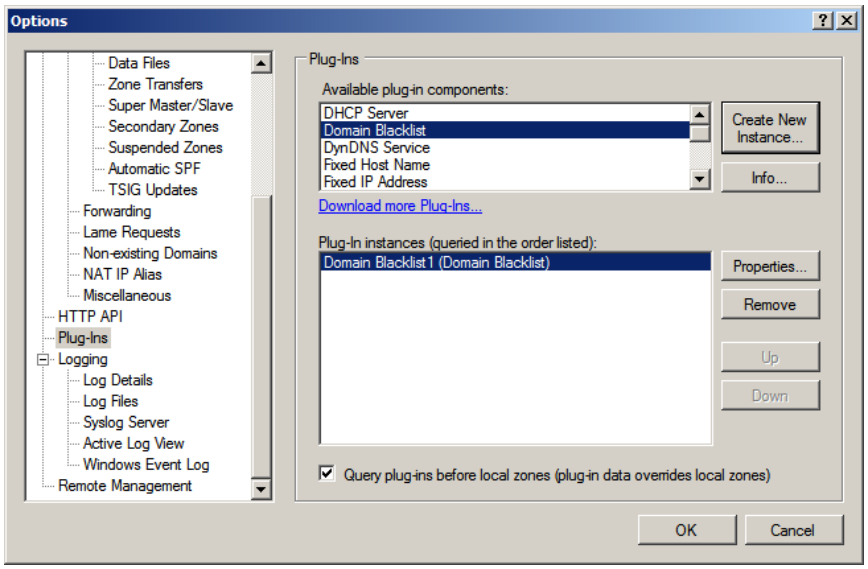
KUVIO 23. DNS-kyselyikkuna (Simple DNS Plus 2010)



KUVIO 24. Välimuistin tilannekuvaikkuna (Simple DNS Plus 2010)

13.3.3 Domain Blacklist-liitännäinen

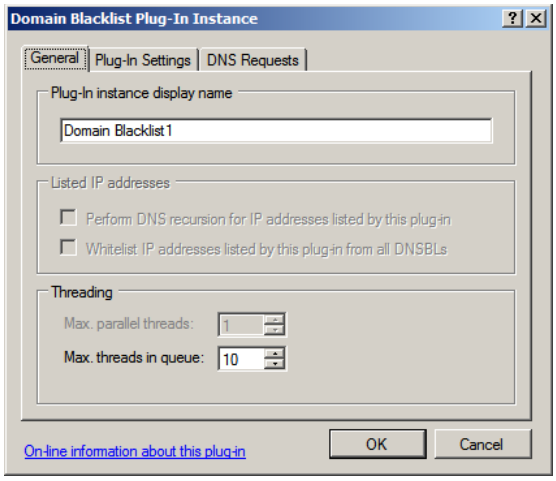
Suodatus toteutetaan Domain Blacklist-liitännäisellä. Liitännäinen asetetaan toimintaan pääikkunan Tools-valikon Options kohdasta, jonka jälkeen Options-ikkunasta valitaan Plug-Ins ja liitännäisvalikosta Domain Blacklist. Create New Instance...-nappi käynnistää uuden ei-listan luomisen. (Ks. kuvio 25.)



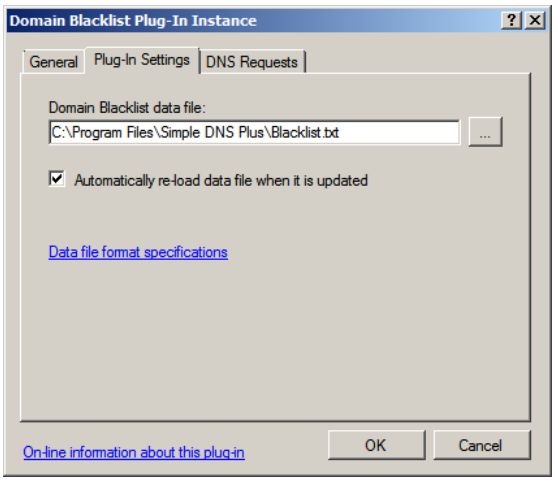
KUVIO 25. Options-ikkunasta valittuna Domain Blacklist-liitännäinen

Domain Blacklist-liitännäisen General-sivulla (ks. kuvio 26) määritellään instanssin nimi ja Plug-In Settings-sivulla (ks. kuvio 27) ei-listan nimi. Nämä nimimääritykset

mahdollistavat useampien eri listausten käytön ja tarjoavat monipuolisuutta suodatusratkaisuihin.



KUVIO 26. General-välilehti



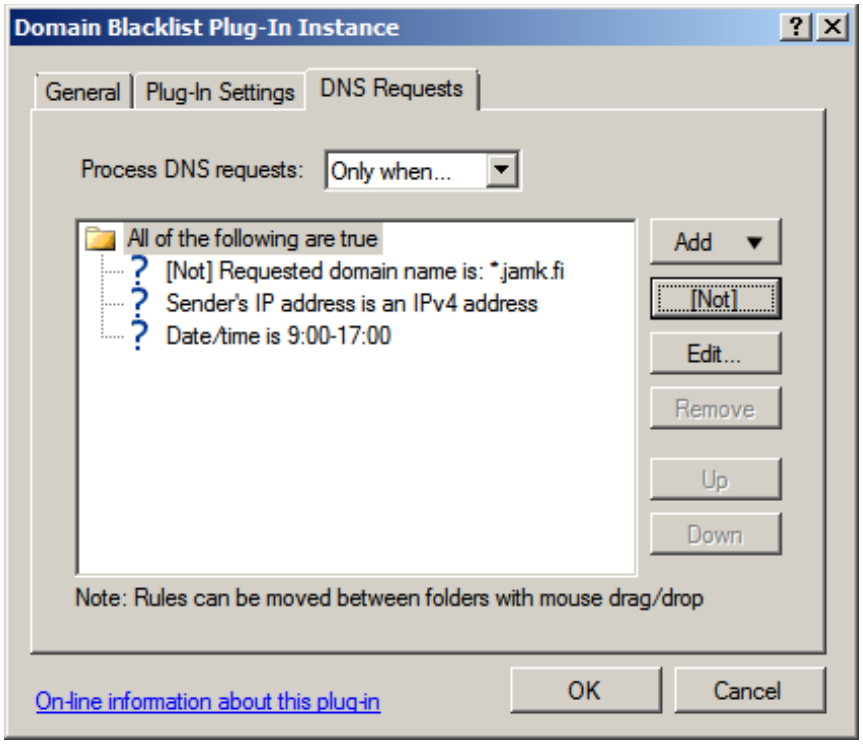
KUVIO 27. Plug-In Settings-välilehti

Kolmanteen ikkunaan, DNS Requests (ks. kuvio 28), määritellään mahdolliset optiot miten, milloin tai keneen suodatuksen halutaan ulottuvan. Asetuksissa voidaan määritellä IP-osoitteita, joihin suodatus vaikuttaa tai jotka ovat siitä vapautettuja, sekä kellonajat milloin suodatuksen halutaan olevan toiminnassa. Myös ei-määritykset, milloin suodatuksen ei haluta toimivan, ovat mahdollisia.
Esimerkiksi kuviossa 28 on asetettu seuraavat säännöt.

Suodatus tapahtuu vain jos DNS-kyselyssä:

- EI pyydetä domainia *.jamk.fi
- kyselyn lähetetään IP versio 4 osoitteesta
- kellonaika on välillä 9:00 -17:00.

Näissä esimerkki asetuksissa taataa aina pääsy kaikkiin jamk.fi päättyviin domaineihin, vaikka Blacklist.txt määrityksessä olisikin sääntö, joka muuten estäisi liikenteen. Lisäksi liikenne IP version 6 osoitteista ja kaikki liikenne kello 17:00 -9:00 välisenä aikana on sallittua.



KUVIO 28. DNS Requests-välilehti

13.3.4 Domain Blacklist estolistauksen dataformaatti

Estolista on puhtaassa tekstimuodossa oleva tekstitiedosto, esimerkiksi .txt-muotoinen, ja sitä voi editoida millä tahansa tekstieditorilla. Jokainen tekstitiedoston rivi alkaa suurella kirjaimella I, T, X, M, E tai R jota seuraa välilyönti ja mahdolliset määrittelyt.

I	IP-osoite joka palautetaan estetyille DNS-kyselyille. Oletuksena 127.0.0.1.
T	TTL (time to live)-arvo. Kuinka pitkään kyselyn tietoja säilytetään muistissa.
X	Päivämäärä milloin estolista poistuu käytöstä.
M	Tarkka vastaavuus. Haku estetään jos domain-nimi on täsmälleen sama kuin määrityksessä.
E	Domain-nimen loppuosan vastaavuus. Haku estetään jos domain-nimen loppuosa vastaa määritystä.
R	Säännöllinen lauseke. Haku estetään jos domain nimen osa täyttää määrityksen. Voi olla yksi merkkijono jossain päin domainia.

Tarkassa vastaavuudessa (M) lauseke voi alkaa villillä kortilla (*.jamk.fi), mikä tarkoittaa kaikkia domainin ala-domaineja. Ero tämän ja nimen loppuosan vastaavuuden (E) kanssa on että loppuosa vastaavuus suodattaa myös pää-domainin.

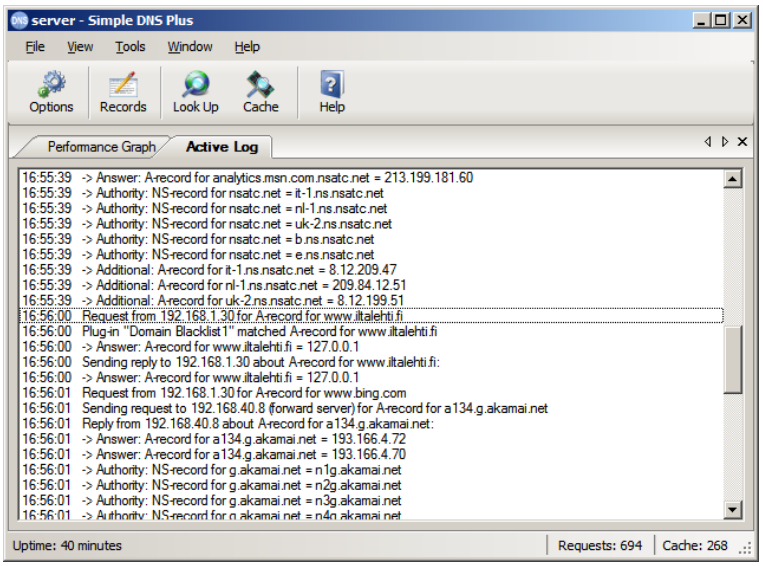
M, E ja R määrityksen kanssa voidaan käyttää etumerkkinä huutomerkkiä (!) merkitsemään poikkeusta, joka tarkoittaa ”älä estä”. Poikkeukset käsitellään aina ennen kaikkia muita rivejä. Lisäksi tyhjät rivit ja riveillä #-merkin jälkeen olevat tekstit jätetään huomioimatta. (Domain Blacklist Plug-In 2009.)

Esimerkki suodatuslistasta

#Start of Domain Blacklist data file “Blacklist.txt”
I 127.0.0.1 #localhost
T 600 #TTL – 10 minuuttia
!E jamk.fi #sallii kaiken liikenteen jamk.fi päättyviin domaineihin
M esimerkki.fi #kieltää esimerkki.fi
R lehti #kieltää kaikki domain-nimet joissa esiintyy ”lehti”

13.3.5 Toiminnallisuuden testaus

Domain Blacklist liitännäisen toiminta voidaan havaita DNS-palvelimen pääikkunan lokista joka näkyy kuviossa 29. Lokista voimme havaita miten iltalehti.fi domainin nimessä oleva ”lehti” vastaa Blacklist.txt estolistan määritettyä R-lauseketta. Tämän seurauksena DNS-palvelin estää käyttäjän DNS-kyselyn etenemisen ja palauttaa asetuksissa määritellyn osoitteen



KUVIO 29. Blacklist Plug-in toiminnassa

127.0.0.1.

13.4 OpenDNS

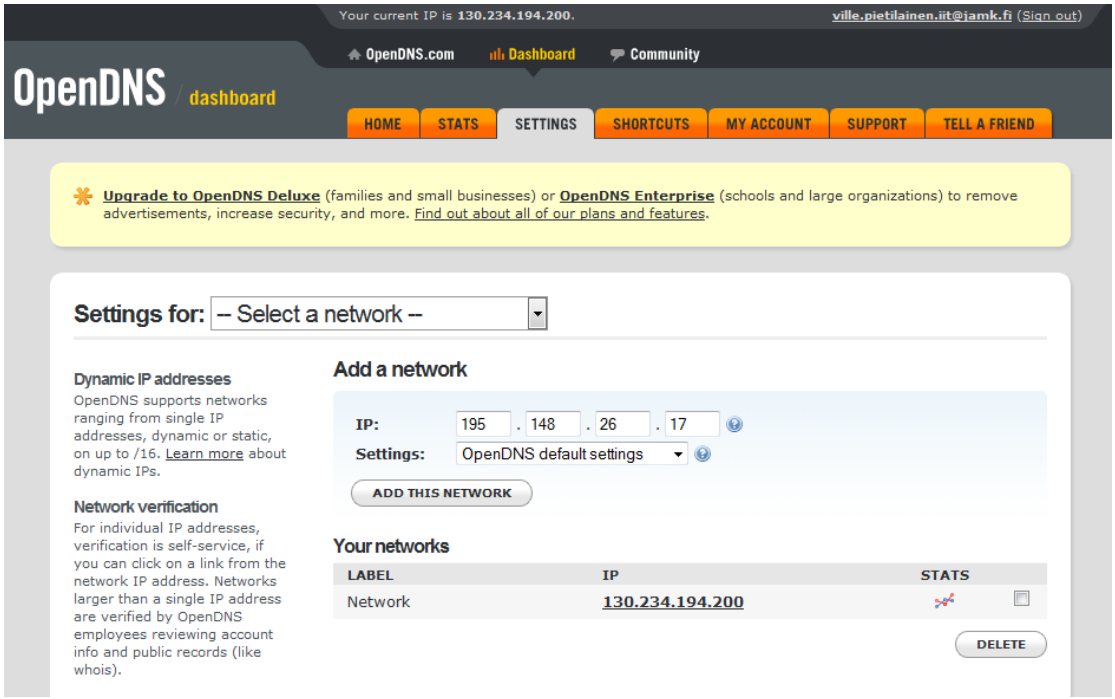
13.4.1 Taustaa

OpenDNS on ilmainen kolmannen osapuolen palveluna toteutettu (SaaS – Software as a Service) suodatusjärjestelmä, jossa suodatus tapahtuu palveluntarjoajan palvelimilla. Näin OpenDNS eroaa muista tässä työssä käsitellyistä tekniikoista, koska se ei vaadi ohjelmisto- tai laitteistoasennuksia testiympäristöön. Tällaisten kolmannen osapuolen, Internetiin hajautettujen, palveluiden suurin hyöty on, että ne ovat saatavilla aina kun yhteys Internetiin on käytettävissä ja niiden käyttö vaatii yleensä hyvin vähän laitteistoasennuksia ja ylläpitoa.

SaaS-palveluiden vahvuudet tulevat parhaiten esille kun yrityksellä on useita konttoreita, toimipaikkoja tai myyntipisteitä, jolloin perinteisen keskitetyn hallinnan toteuttaminen on hankalaa. Näissä tilanteissa on aikaisemmin usein jouduttu rakentamaan monimutkaisia VPN-ratkaisuja, joilla liikenne kierrätetään oman verkon kautta tarkastettavaksi, tai asentamaan ylimääräisiä palvelimia joka toimipisteeseen. Kun suodatuspalvelu on kolmannen osapuolen hallinnoima ja ylläpitämä, liikenne saadaan tarkastettua Internet-pilven sisällä (OpenDNS 2010).

13.4.2 Suodatuksen käyttöönotto

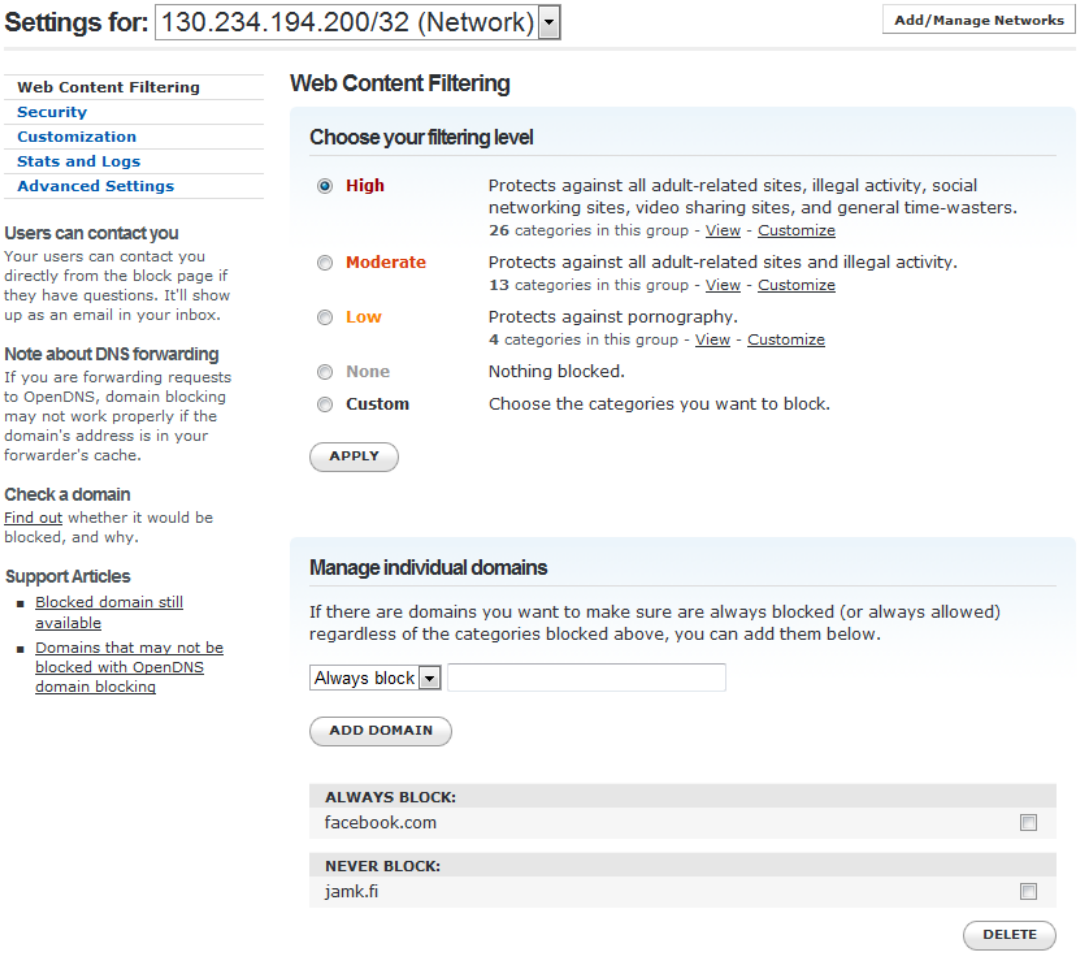
Käyttöönotto aloitetaan luomalla käyttäjätili palveluntarjoajan Web-sivuilla www.opendns.com, ja kirjautumalla sisälle palveluun. Kirjautumisen jälkeen siirrytään Settings-välilehdelle ja lisätään halutun verkon ulkoinen IP-osoite Add a network kohtaan ja painetaan Add This Network-nappia (ks. kuvio 30). Tämän jälkeen OpenDNS pyytää antamaan verkolle nimen, sekä lähettää sähköpostiviestillä verkko-osoitteen rekisteröinnin varmistuspyynnön.



KUVIO 30. OpenDNS Settings

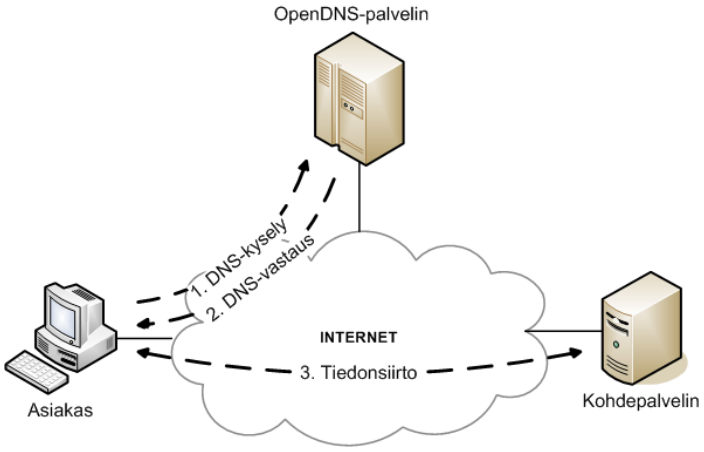
Kun verkko on määritelty, voidaan sen asetuksia muokata Settings-välilehdeltä, valitsemalla verkko osoitelistasta. Tämän jälkeen suodatusasetukset sisältävä, Web Content Filtering-välilehti, aukeaa automaattisesti.

Web Content Filtering-välilehdeltä (ks. kuvio 31) valitaan haluttu suodatuksen taso, tai Custom vaihtoehto, jolloin voi itse päättää mitkä kategoriat halutaan estää. Lisäksi voidaan estää tai sallia yksittäisiä domaineja.



KUVIO 31. Web Content Filtering

Kun estettävät kategoriat ja domainit on asetettu, täytyy verkon sisäiseltä DNS-palvelimelta ohjata ulospäin suuntautuvat DNS-kyselyt Open DNS:n palvelimille (ks. kuvio 32), IP-osoitteisiin 208.67.222.222 ja 208.67.220.220 joilla suodatus tapahtuu. Jos verkon tietokoneet eivät ole keskitetysti hallittuja, tehdään muutokset suoraan tietokoneiden verkkoasetusten DNS-asetuksiin käsin. (OpenDNS 2010)

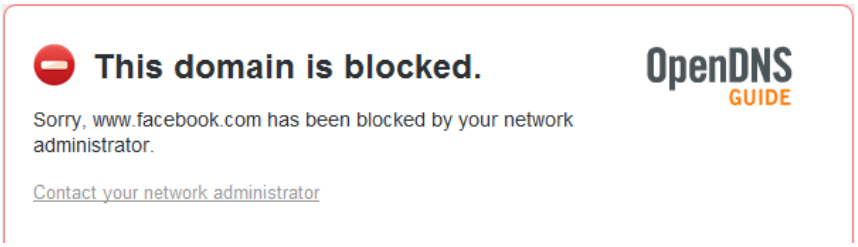


KUVIO 32. OpenDNS-suodatuksen toiminta

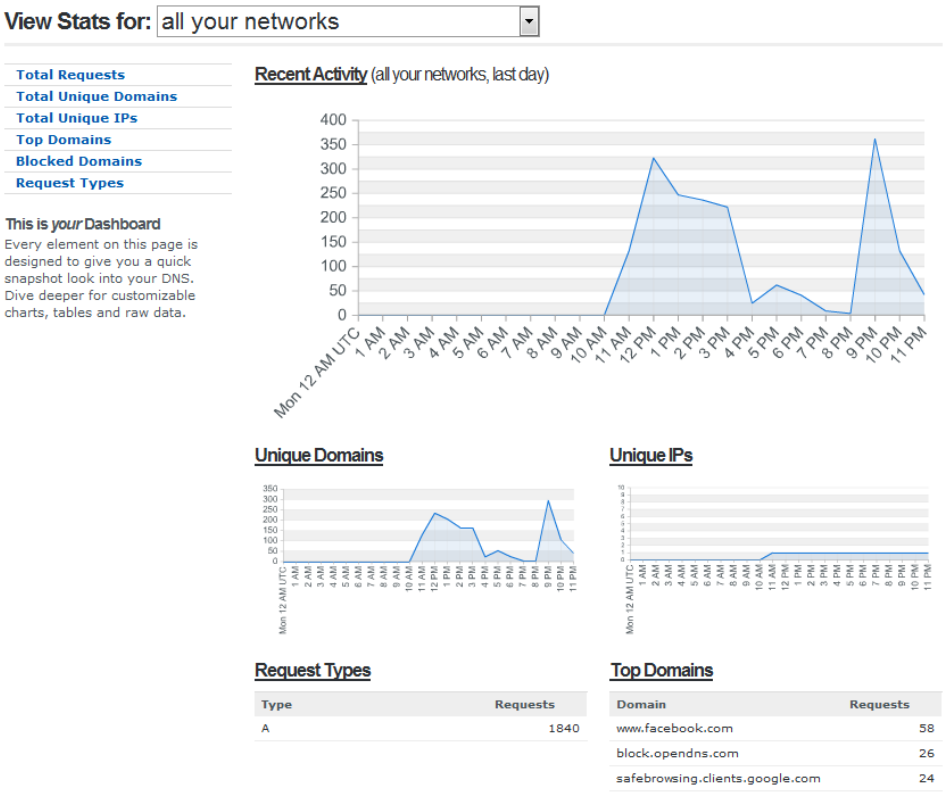
13.4.3 Ominaisuuksia

- OpenDNS tarjoaa turvaominaisuudet joilla voidaan estää liikenne epäilyttäviltä sivuilta, vaikka niitä ei olisi suodatuksessa listattu.
- Estosivun sisältö on muokattavissa ja voi sisältää enintään 150 merkkiä pitkän viestin (ks. kuvio 33).
- Yleisimpiä domain-nimien väärinkirjoitustapauksia voidaan korjata automaattisesti.
- Raportointiominaisuudet jotka tallettavat, ilmaisella käyttäjätilillä, kahden viikon tiedot (ks. kuvio 34).

Tarjolla on myös maksulliset palvelut jotka tarjoavat paremmat hallinta- ja raportointityökalut, suodatuksen suuremman muokattavuuden, suuremmat musta- ja valkoiset listat sekä muita ominaisuuksia. (OpenDNS 2010)



KUVIO 33. OpenDNS block message



KUVIO 34. OpenDNS Statistics

14 VÄLITYSPALVELIMELLA TOTEUTETTU SUODATUS

14.1 Välityspalvelimen käyttöönotto

Koska Web-palvelimet ovat suosittuja kohteita erilaisille verkkohyökkäyksille, on ulkoliikennettä käsittelevä välityspalvelin parasta sijoittaa puolueettomalle vyöhykkeelle sisä-, ja ulkoverkkojen väliin. Lisäksi kaikki HTTP-liikenne voidaan ohjata sisäverkosta aina välistyspalvelimelle sekä sallia HTTP-liikenteen tuleminen sisäverkkoon vain välityspalvelimelta. Näin saadaan varmistettua sisäverkon turvallisuus. Windows Active Directory hallitussa verkossa voidaan välityspalvelimen käyttö asettaa pakolliseksi Group Policyn avulla.

14.2 WinGate Proxy Server

14.2.1 Yleistä

WInGate on Qbik yhtiön kehittämä välityspalvelinohjelmisto jonka ensimmäinen versio julkaistiin vuonna 1995. Ensimmäisten versioiden tarkoitus oli toimia yhdyskäytäväpalvelimena ja mahdollistaa useamman tietokoneen kommunikointi Internetiin. Tämän jälkeen siitä on muodostunut helppokäyttöinen Internet-yhteyden hallintaohjelmisto. (WinGate: The Comprehensive Internet Management Solution for Windows 2010.)

WinGate Proxy Server on hienostunut, integroitu välitys- ja kommunikaatiopalvelin, joka on suunniteltu täyttämään tämän päivän yritysten kontrolli-, turvallisuus- ja kommunikaatiotarpeet. Tärkeimpinä ominaisuuksinaan WinGate Proxy Server tarjoaa mahdollisuuden hallita verkon Web-liikennettä, käyttäen edistyneitä ja joustavia säännöstöjä. Verkon toimintaa voidaan nopeuttaa tallettamalla haetut verkkosivut palvelimen välimuistiin. WinGate Proxy Server tarjoaa myös mahdollisuuden tosiaikaiseen käyttäjien Internetin käytön tarkkailuun ja hallintaan. (WinGate Proxy Server 2010.)

Vaikka WinGate Proxy Server mainostaa itseään myös Internet-yhdyskäytäväksi, siitä kuitenkin testattiin ainoastaan välityspalvelinominaisuuksia koska tämä on sen tärkein toiminta-alue, eivätkä ohjelmiston palomuuriominaisuudet yltäneet muiden, varsinaisten yhdyskäytäväpalvelinten tasolle. Lisäominaisuuksina WinGate sisältää DHCP-, DNS- ja E-mail-palvelinominaisuudet. Näihin lisäominaisuuksiin täytyy lisätä myös pieni varoituksen sana, sillä asennuksen jälkeen ne ovat automaattisesti kaikki päällä, ilman erillisiä kyselyitä.

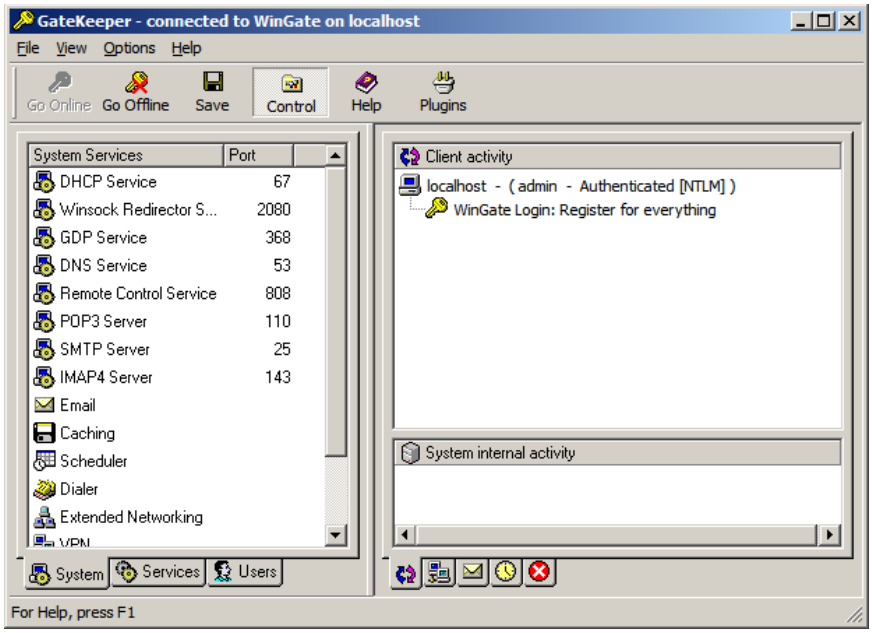
WinGate tarjoaa Active Directory domainin käyttäjätietokannan käyttämisen välityspalvelimen käyttäjien luokittelemiseksi. Tämä mahdollistaa keskitetyn hallinnan PureSight 3.0 for WinGate Web-sisällön luokittelu liitännäisen kanssa, jonka avulla ylläpitäjä voi asettaa pääsyrajoituksia verkkosivuille domainin tai URL-osoitteen perusteella. (PureSight for WinGate 2010.)

14.2.2 Käyttöliittymä

WinGate:n hallinta tapahtuu GateKeeper-modulilla jota käytetään kaikkien asetusten tekoon sekä palvelimen toiminnan tarkkailuun. GateKeeperin ikkunassa (Ks. kuvio 35.) ylimpänä on valikkopalkkia ja sen alla kaksi paneelia joista vasemmalla on kontrollipaneeli ja oikealla toimintapaneeli.

Kontrollipaneelin alalaidasta löytyy kolme välilehteä: System (järjestelmä), Services (palvelut) ja Users (käyttäjät).

- System-välilehteä käytetään kaikkien järjestelmän komponenttien, kuten DHCP, DNS ja E-mail, hallintaan.
- Services-välilehdeltä löytyvät kaikki välityspalvelimen asetukset ja tarkkailutyökalut.
- Users-välilehti pitää sisällään käyttäjä ja käyttäjäryhmien hallintatyökalut.

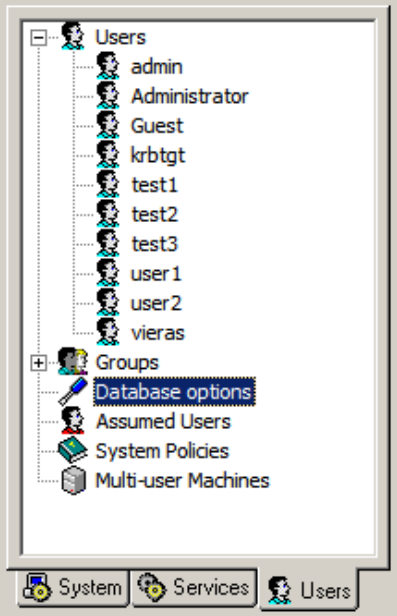


KUVIO 35. GateKeeper-ikkuna ja System-välilehti

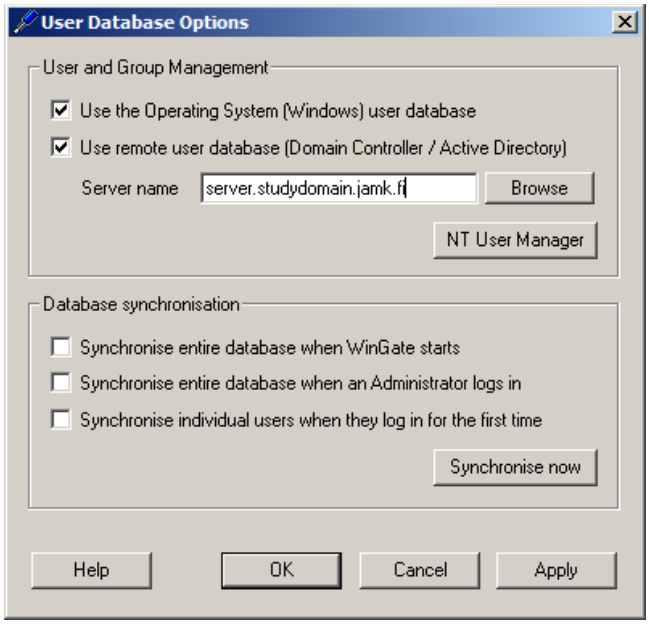
14.2.3 Käyttäjien hallinta

Jotta Active Directory tietokannan käyttäminen käyttäjien hallintaan olisi mahdollista, täytyy WinGate-palvelimen tietää domainia hallitsevan Domain Controller-

palvelimen osoite. Tämä tapahtuu tuplaklikkaamalla User-välilehden kohdasta Database options (ks. kuvio 36), jolloin User Database Options ikkuna (ks. kuvio 37) avautuu. Tässä ikkunassa valitaan kaksi ylintä optiota joilla määritellään käyttöön Windowsin käyttäjätietokanta. Lisäksi valintaikkunaan kirjoitetaan Domain Controller-palvelimen täydellinen DNS-osoite.

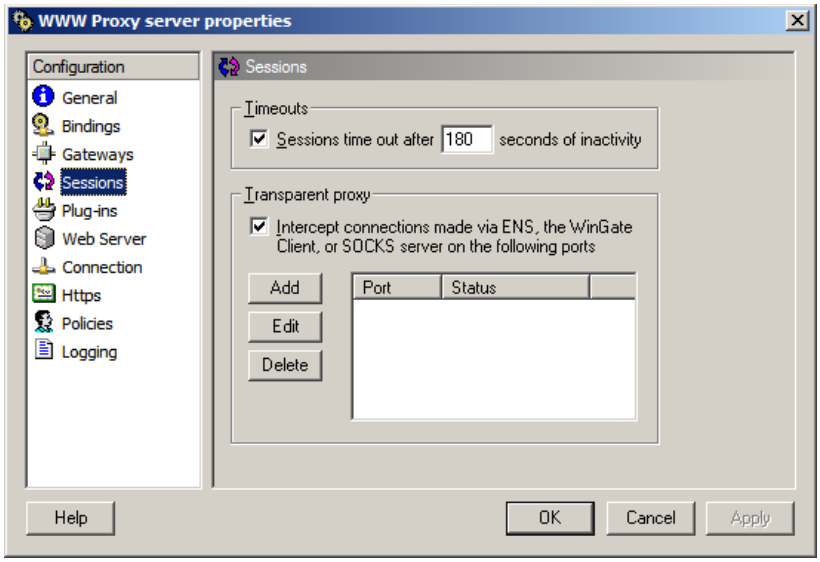


KUVIO 36. Users-välilehti



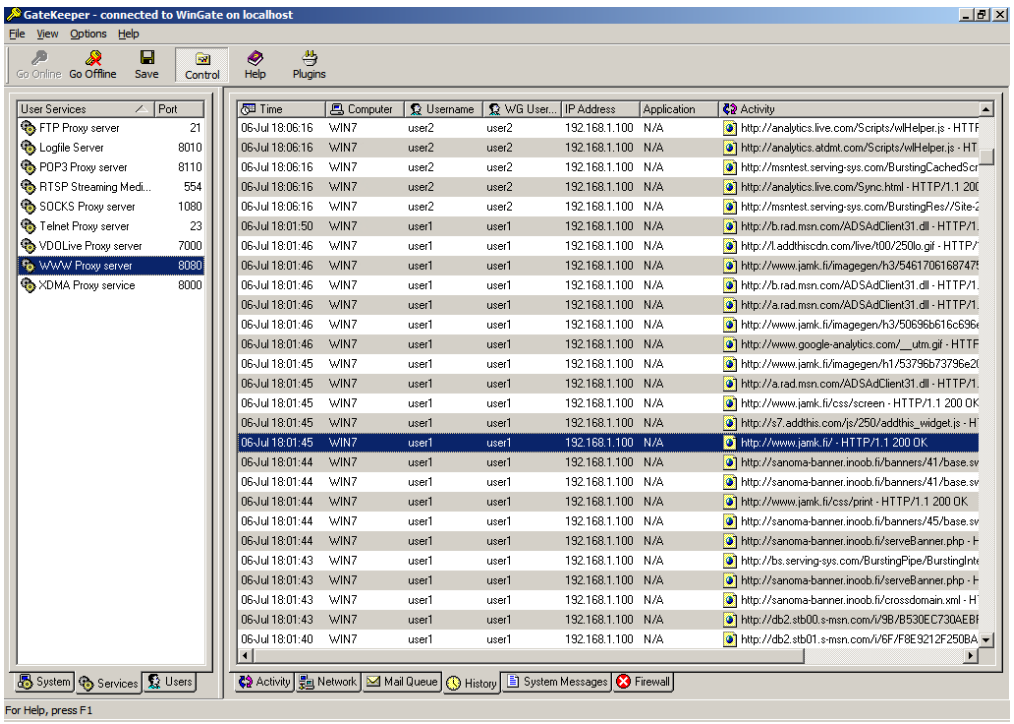
KUVIO 37. User Database Options ikkuna

Kun käyttäjätietokanta on otettu käyttöön, on suositeltavaa varmistaa suodatuksen toiminta asettamalla välityspalvelin näkymättömäksi, eli kaappaamaan kaikki sen havaitsema HTTP-liikenne automaattisesti tarkasteluun. Tämä tapahtuu Services-välilehden WWW Proxy server-kohdasta tuplaklikkaamalla jolloin WWW Proxy server properties-ikkuna aukeaa. Tämän ikkunan Sessions kohdasta valitaan Transparent proxy asetus (ks. kuva 38).



KUVIO 38. WinGate Transparent proxy-asetus

Kun käyttäjätietokanta on määritetty ja liikenne ohjattu välityspalvelimen läpi, voidaan palvelimen toimintaa tarkkailla reaali-ajassa toimintapaneelin alalaidasta löytyvillä työkaluilla (ks. kuvio 39). Nämä työkalut tarjoavat hyvin yksityiskohtaisia tietoja sivustoista, joita käyttäjät ovat hakeneet. Historiatiedot näyttävät jokaisen tiedoston joka välistyspalvelimen läpi on kulkenut ja kertovat tiedoston hakijan käyttäjätunnuksen, tietokoneen nimen ja sisäverkon IP-osoitteen.



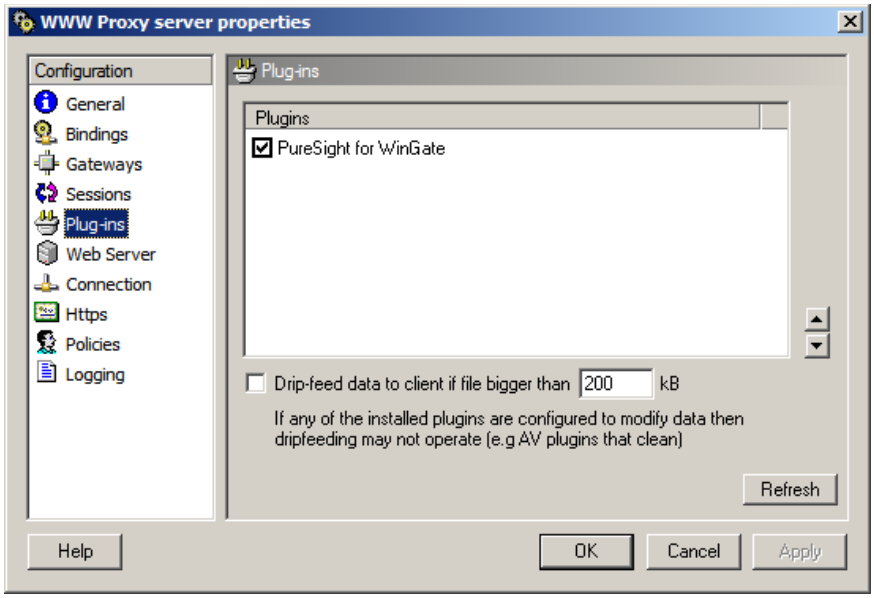
KUVIO 39. WinGate-välityspalvelimen historiatiedot

14.2.4 Suodatus WinGate Proxy Serverillä

PureSight on liitännäisenä asennettava Web-sisällön luokittelujärjestelmä WinGate välityspalvelimelle. Web-sivujen luokittelua hyväksikäyttäen voi ylläpitäjä määritellä minkä tyyppisille Internet-sivuille käyttäjät pääsevät, ilman että sivuja tarvitsisi yksitellen estää. PureSight liittää itsensä välityspalvelimeen ja pystyy näin tarkkailemaan ja suodattamaan palvelimen läpi menevää Web-liikennettä. (PureSight 3.0 for WinGate documentation 2009.)

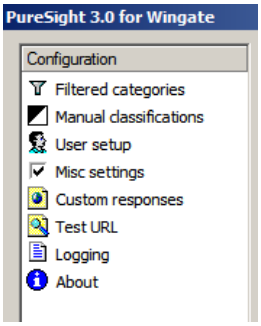
Web-liikenteen suodattamiseen PureSight for Wingate käyttää kaksoisjärjestelmää. Pääasiallinen luokittelujärjestelmä käyttää automaattista sisällöntunnistusmoottoria (Automatic Content Recognition Engine), joka analysoi Web-sivujen sisällön. Toisena järjestelmänä toimii tietokanta joka pitää sisällään poikkeavuudet ja erikseen määritellyt sivujen estot. Dynaaminen päivitysjärjestelmä pitää suodatusluokittelun automaattisesti ajan tasalla. (PureSight 3.0 for WinGate documentation 2009.)

Suodatuksen käyttöönottamiseksi täytyy WinGate-palvelimelle asentaa PureSight-liitännäinen. Asennuksen jälkeen liitännäinen asetetaan toimintaan Services-välilehden WWW Proxy server-valikon kohdasta Plug-ins (ks. kuvio 40).



KUVIO 40. WinGate Plug-ins

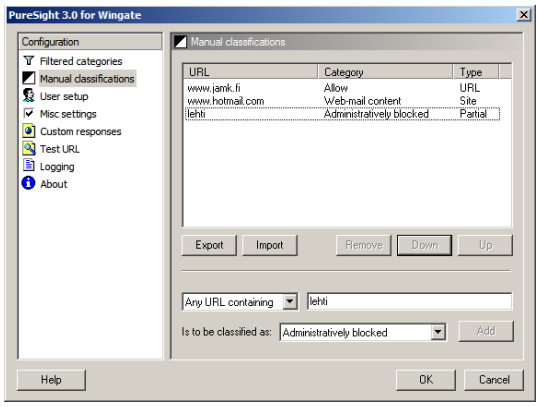
PureSight-liitännäisen hallintaominaisuudet löytyvät GateKeeper-ikkunan valikkopalkin Plug-ins napin takaa, josta aukeavasta listasta tupla klikataan PureSight 3.0 for WinGate kohtaa. Tämän jälkeen PureSight-liitännäisen hallintaikkuna aukeaa (ks. kuvio 41).



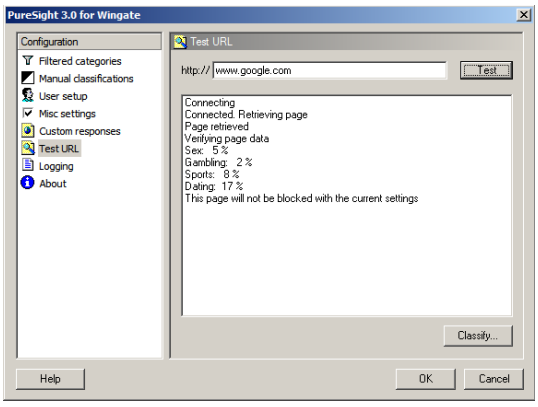
KUVIO 41. PureSight

TAULUKKO 4. PureSight-liitännäisen päävalikon koostumus

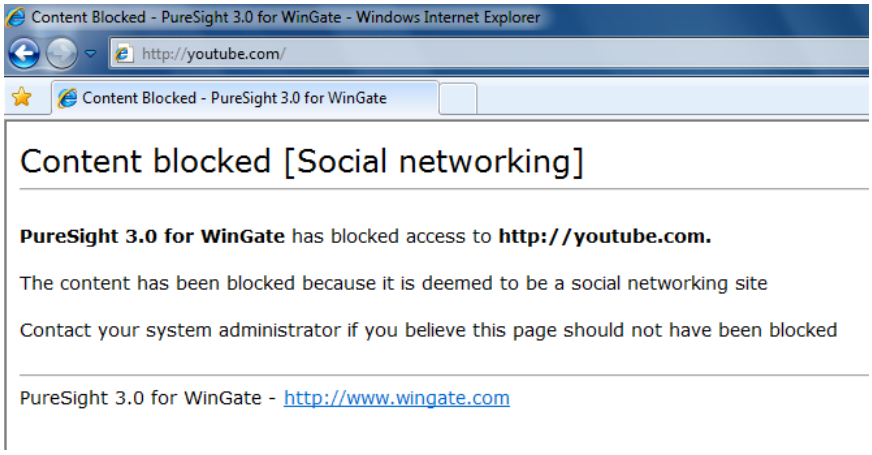
Filtering Categories	Sisältää 28 suodatuskategoriaa, joiden avulla liikennettä voidaan määrittää estettäväksi.
Manual classifications (ks. kuvio 42)	Määritykset joilla voidaan sallia tai estää sivustoja manuaalisesti. Määritykset voidaan tehdä domainin, URL-osoitteen tai URL-avainsanan perusteella.
User setup	Suodatuksen alle otettavien käyttäjien ja käyttäjäryhmien valinta.
Misc settings	Liitännäisen päivitysasetukset.
Custom responses	Estoviestien suunnittelu. Joka estokategorialle voidaan tehdä oma estoviesti (ks. kuvio 44).
Test URL (ks. kuvio 43)	URL-osoitteiden testaus. Tämän työkalun avulla voi nähdä osoitteen kategoriamäärittelyt, sekä selvittää onko URL-osoite estettyjen listalla.
Logging	Lokiin kirjattavien tapahtumien valinta.
About	Liitännäisen versio tiedot.



KUVIO 42. PureSight classifications

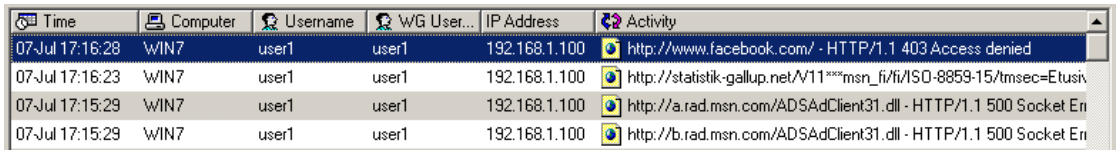


KUVIO 43. PureSight URL test



KUVIO 44. PureSight estoviesti

WinGate-palvelimen historiatiedoista voidaan varmistaa suodatuksen toiminta. Tässä tapauksessa estettynä on www.facebook.com (ks. kuvio 45).



KUVIO 45. Web-sivun esto WinGate:n historiatiedoissa

15 YHDYSKÄYTÄVÄPALVELIMELLA TOTEUTETTU SUODATUS

15.1 Microsoft Forefront TMG (Threat Management Gateway) 2010

15.1.1 Yleistä

Microsoft Forefront on Microsoftin tuoteperhe, joka on suunniteltu yrityksille liiketoiminnan suojaamiseen, turvaamalla tietoverkko ja tietoverkon palvelimet kuten Microsoft Exchange Server ja Microsoft SharePoint Server. (Microsoft Forefront 2009.)

Forefront TMG mahdollistaa yrityksen työntekijöille turvallisen ja tehokkaan Internetin-käytön ilman että heidän tarvitsee huolestua haittaohjelmista tai muista uhkista. Forefront TMG tarjoaa monikerroksisen, yhtäjaksoisesti päivittyvän suojauksen, joka on integroitu yhdistettyyn, helposti hallittavaa yhdyskäytävään, vähentäen näin verkkoturvallisuuden hintaa ja monimutkaisuutta. Microsoft Forefront Threat Management Gateway tunnettiin aikaisemmin nimellä Microsoft Internet Security and Acceleration Server (ISA Server). (Forefront Threat Management Gateway: Overview 2009.)

TAULUKKO 5. Forefront TMG, tärkeimmät suodatus- ja turvallisuusominaisuudet

URL-suodatus	Kohdeosoitteet tutkitaan kiellettyjen sekä haitallisten osoitteiden varalta.
Web-antivirus & haittaohjelmien torjunta	Saapuva ja lähtevä liikenne tarkastetaan virusten ja haittaohjelmien varalta, mukaan lukien pakatut tiedostot.
HTTP-liikenteen kontrollointi	Web-liikennettä voidaan ohjata ja rajoittaa keskitetysti.
HTTPs-tarkastus	HTTPs-salattua liikennettä voidaan tarkkailla haittaohjelmien tai sääntörikkomusten varalta.
Monikerroksinen palomuuri	Palomuuri toimii kolmella tasollaa: pakettisuodatus, tilallinen suodatus ja sovellustason suodatus.
Sovellustason suodatus	Mahdollistaa sisällön suodatuksen sisäänrakennetuilla sovellus-suodattimilla.
Laaja protokollatuki	Tunnistaa useita protokollia. Uusia voi määritellä.
Reaaliaikainen monitorointi ja raportointi	Lokeja voi tarkastella reaaliaikaisesti tai historiallisesti, mukaan lukien aktiiviset tiedonsiirrot.
Kyselyiden rakennus	Historiatietoa voidaan tutkia tehokkailla kyselyillä.

Forefront TMG sisältää kaksi erillistä komponenttia

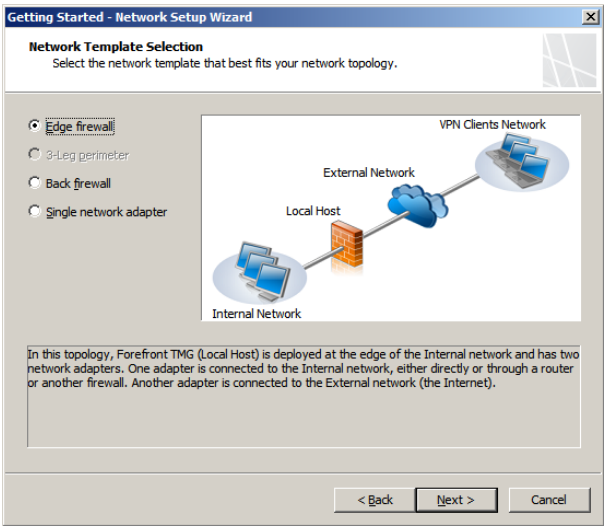
- **Forefront TMG server** – tarjoaa URL-suodatuksen, haittaohjelmien tarkastuksen, tunkeutumisen eston, sovellustason palomuurin sekä HTTP/HTTPS-tarkastuksen.

- **Forefront TMG Web Protection Service** – tarjoaa yhtäjaksoiset päivitykset haittaohjelmien suodatukseen sekä pääsyn pilvi-pohjaisiin URL-suodatusteknologioihin jotka keräävät tietoja useilta verkkoturvallisuustoimijoilta. (Forefront Threat Management Gateway: Overview 2009.)

15.1.2 Käyttöönotto ja käyttöliittymä

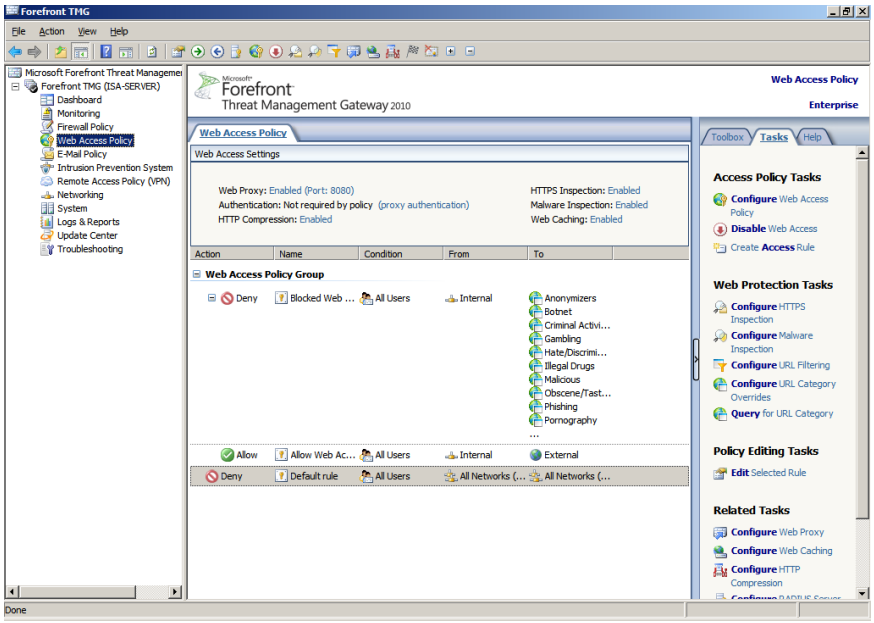
Forefront TMG on helpointa ottaa käyttöön asennustyökalujen kautta. Ohjelmiston asennuksen jälkeen automaattisesti käynnistyvä Getting Started Wizard auttaa tekemään alkuvaiheen käyttöönottoasetukset. Tämä asennusohjelma sisältää kolme ala-ohjelmaa, joita käytetään eri alueiden asennukseen.

- **Network Setup Wizard** – käytetään verkkoasetusten asettamiseen, sisältäen asennustopologia (ks. kuvio 46), käytettävät verkkokortit ja niiden IP-osoitteet, sekä sisä-, ulko- ja mahdollisen reunaverkon määritykset.
- **System Configuration Wizard** – käytetään järjestelmäasetuksien, kuten palvelimen nimen ja domain nimen, määrittelemiseen.
- **Deployment Wizard** – käytetään erilaisten ominaisuuksien, kuten järjestelmä- ja haittaohjelmapäivitysten ja asiakaspalautejärjestelmän määrittelemiseen.



KUVIO 46. Network Setup Wizard

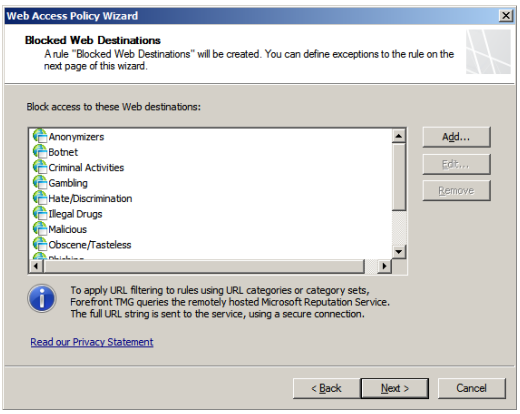
Kun perusasetukset on suoritettu, aukeaa hallintakonsoli josta Forefront TMG:n toimintaa hallitaan. Käyttöliittymä on Microsoft Management Consolen liitännäinen ja sen hallinta toimii samoin kuin esimerkiksi Active Directoryn. Vasemmalla puolella on valikkorakenne. Keskellä näytetään tietoja valitusta kohteesta kuten Web-liikenteen tai palomuurin säännöt. Oikealla ovat yleisimmin suoritettavat tehtävät, kuten uusien sääntöjen luonti tai olemassa olevien muokkaus (ks. kuvio 47).



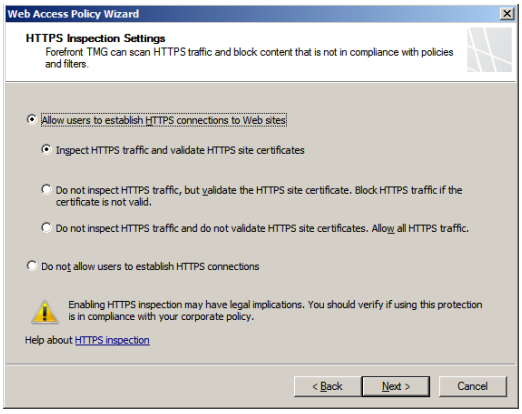
KUVIO 47. Forefront TMG pääikkuna

15.1.3 Suodatuksen määrittely

Suodatus otetaan käyttöön hallintakonsolista valitsemalla Web Access Policy ja Tasks-panelin kohdasta Configure Web Access Policy, jolloin Web-liikennepolitiikan hallintaohjelma (Web Access Policy Wizard) aukeaa. Tämä ohjelman avulla tehdään verkon Web-liikenteen määritykset, kuten URL-suodatuksen (ks. kuvio 48), HTTP- sekä HTTPS-liikenteen analysoinnin (ks. kuvio 49) ja välityspalvelimen välimuistiasetukset.



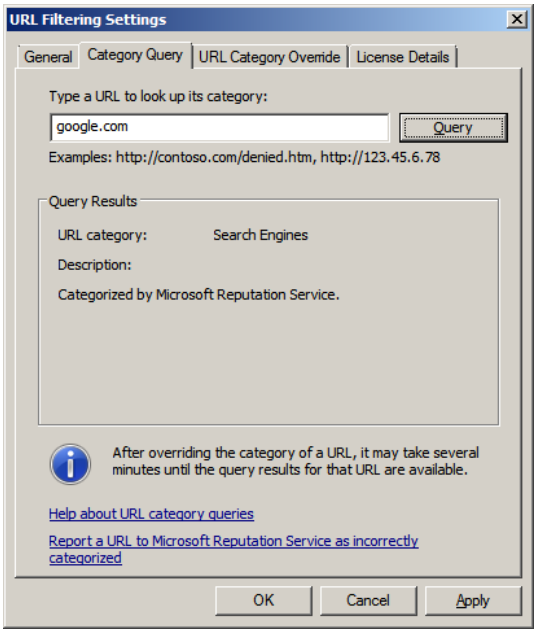
KUVIO 48. URL Blocking



KUVIO 49. HTTPs Inspection

Suodatin määrityksiä tehdessä päätetään mitkä Web-sivujen kategoriat halutaan estää. Kategorioita on seitsemänkymmentäviisi kappaletta ja Web-sivut voivat kuulua useaan kategoriaan. Lisäksi määritellään käyttäjät ja käyttäjäryhmät joiden Web-liikennettä halutaan suodattaa. Sääntöjä voidaan tehdä useampia ja näin estää tietyiltä käyttäjiltä tai käyttäjäryhmiltä enemmän sivustoja kuin toisilta. Jokaiselle säännölle voidaan myös tehdä oma estosivunsa tai vaihtoehtoisesti ohjata käyttäjä toiseen osoitteeseen.

Tasks-paneelin Configure URL Filtering kohdasta aukeaa URL Filtering Settings -ikkuna jossa voidaan testata suodatuksen toimintaa sekä muuttaa osoitteiden kategoriamäärityksiä.



KUVIO 50. URL Filtering Settings

General – Määritellään URL-suodatus päälle tai pois.

Category Query – Voidaan tarkastella mihin kategoriaan sivusto on määritelty (ks kuvio 50).

URL Category Override – Voidaan siirtää URL-osoitteita eri kategoriaan.

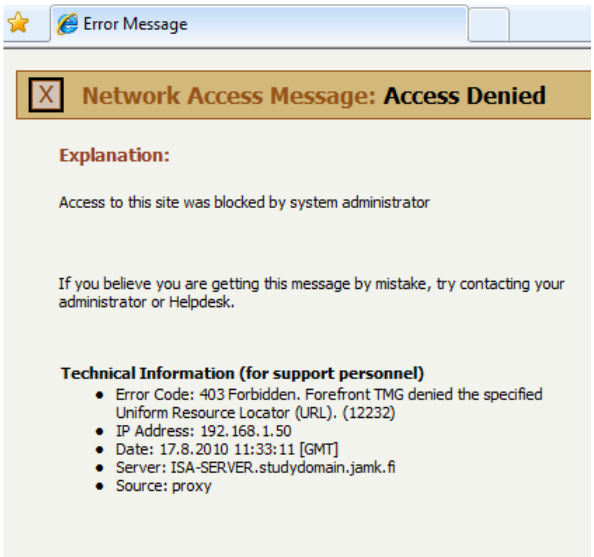
License Details – Käyttölisenssin tiedot.

URL-tietojen kategorioinnista vastaa Microsoft Reputation Service (MRS). Tämä verkkopalvelu tarjoaa suojatun yhteyden suureen pilvipohjaiseen, dynaamiseen tietokantaan joka sisältää tiedot kymmenistä miljoonista URL-osoitteista ja niiden määritellyistä kategorioista.

Tietokanta yhdistää usean eri toimittajan tarjoamia tietoja, niin Microsoft:in sisäisistä kuin myös kolmansien osapuolien lähteistä. Näin tietokanta pysyy tehokkaasti, koko-ajan päivitettynä (Elharrar 2010). Tietokannan URL-määrityksiä voi tarkastella myös osoitteessa HTTP://www.microsoft.com/security/portal/mrs/.

15.1.4 Suodatuksen toiminta ja raportointi

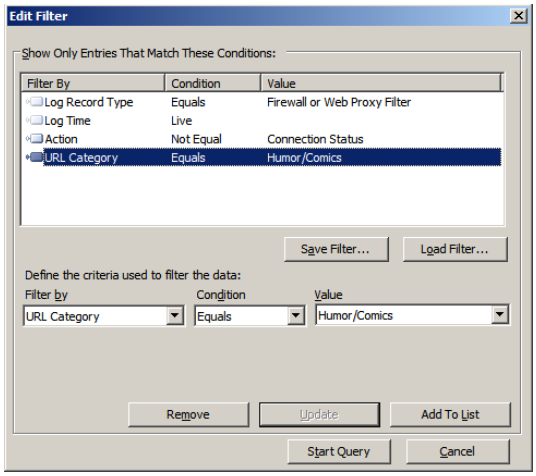
Käyttäjälle sivuston estosta ilmoitetaan estoikkunassa (ks. kuvio 51), jossa kerrotaan sivun olevan estetty sekä mahdollisia lisätietoja. Tämän ikkunan tiedot ovat täysin ylläpitäjän muokattavissa.



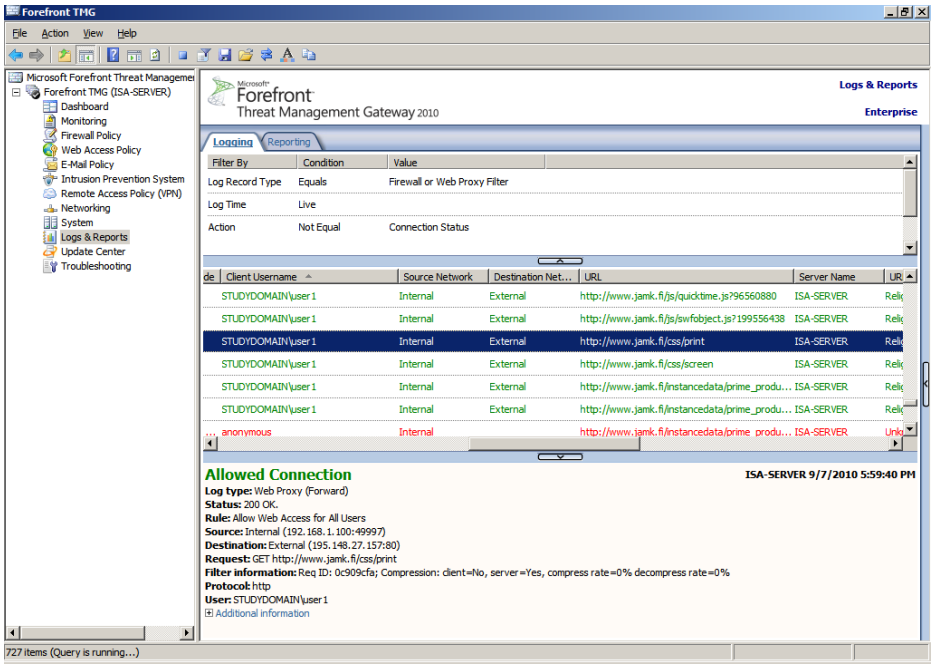
KUVIO 51. Forefront TMG Error Message

Forefront tarjoaa monipuoliset työkalut liikenteen monitorointiin ja raportointiin. Näiden tuottamia tietoja voidaan hallita ja kohdentaa eri protokolliin, käyttäjiin tai yhteyksiin erittäin tehokkaasti (ks. kuvio 52 & 53). Näin ylläpitäjä saa tietoa juuri haluamastaan kohteesta. Raportoinnilla saadaan erittäin tarkkaa tietoa verkkoliikenteestä, sen määrästä ja mahdollisista tietoturvauhkista. Suodatuksen osalta näkyvillä

ovat käytetyimmät protokollat ja Web-sivut, tarvittaessa käyttäjäkohtaisesti eritelty-
nä.



KUVIO 52. Forefront TMG Filter Options



KUVIO 53. Forefront TMG Logs

15.2 Kerio Control

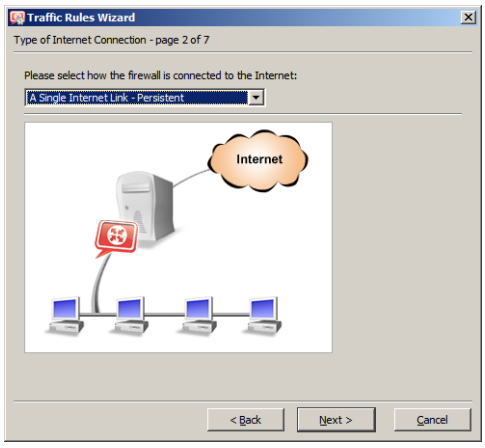
15.2.1 Yleistä

Kerio Control (aikaisemmin Kerio WinRoute Firewall) on yhdistetty tietoturvauhkien hallintaohjelmisto joka tarjoaa sovellustason palomuurin, anti-virustoiminnot, VPN-palvelut, välityspalvelimen, DNS-tietojen välityksen, tietoliikenteen hallinnan ja verk-

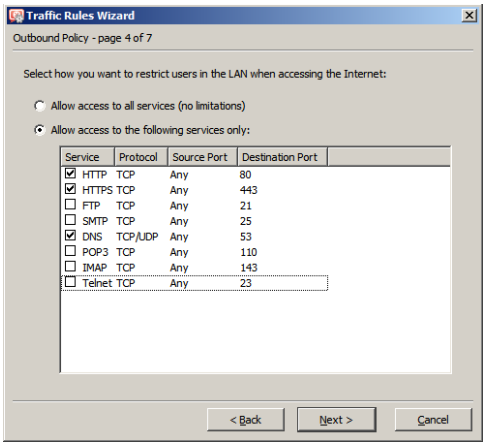
koliikenteen suodatuksen. Active Directory integroitu käyttäjienhallinta, joka mahdollistaa käyttäjien verkonkäytön tarkkailun ja liikenteen rajoittamisen käyttäjätunnuksen perusteella. Kerio Control on ihanteellinen verkkoihin, joissa vaaditaan tiukkaa käyttäjätunnuspohjaista turvallisuuspolitiikkaa sekä yksityiskohtaista liikenteenanalysointia ja raportointia. (Kerio Control 7 Datasheet 2010.)

15.2.2 Käyttöönotto ja käyttöliittymä

Ohjelmiston asennuksen ja palvelimen uudelleen käynnistyksen jälkeen aukeaa ohjattu asennusohjelma, Traffic Rules Wizard, jonka avulla määritellään fyysiset verkkoasetukset (ks. kuvio 54), verkkoliikenteen säännöt ja sallitut liikenneprotokollat (ks. kuvio 55).

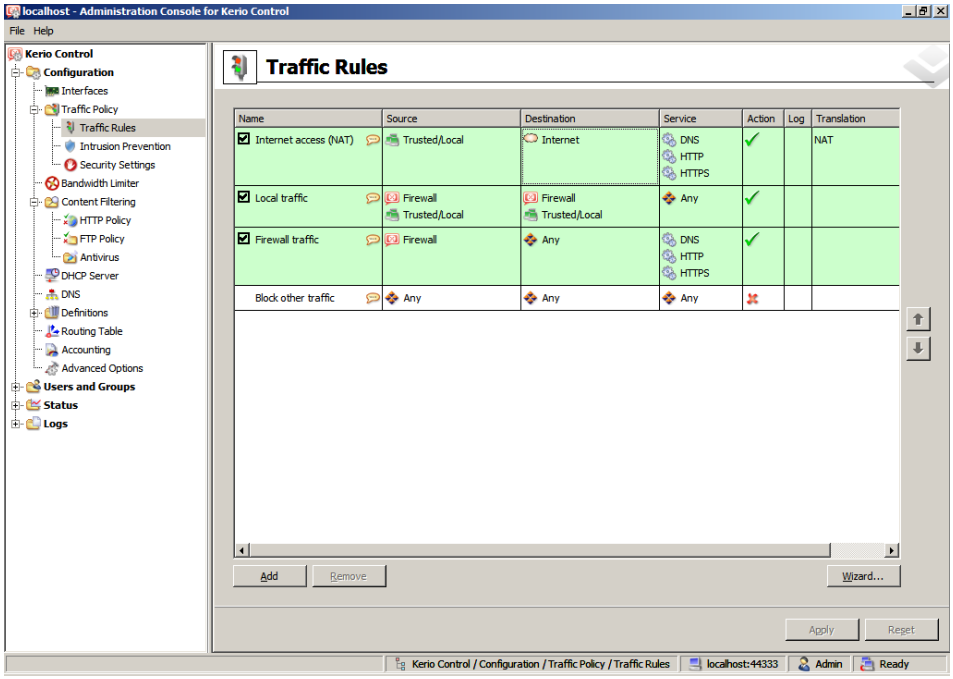


KUVIO 54. Traffic Rules Wizard



KUVIO 55. Sallitut protokollat

Kerio Administration Console on ohjelma jonka avulla Kerio Control:n toimintaa hallitaan. Tämä hallintakonsoli pitää sisällään kaikki ohjelman ominaisuudet ja mahdollistaa määritysten tehokkaan hallinnan sekä toiminnan tarkkailun. Esimerkiksi verkkoliikenteen säännöt näytetään havainnollisena listana, josta sääntöjen järjestyksen ja asetusten muuttaminen on helppoa (ks. kuvio 56). Liikenne tarkastetaan sääntöjen pohjalta ylhäältä alaspäin ja jonkin säännön vastatessa, suoritetaan sen määrittämä toiminto. Eri protokollille ja osoitteille voidaan määrittää eri oikeudet ja kaikki ylimääräinen liikenne estää. (Kerio Control Administrator's Guide 2010.)



KUVIO 56. Administration Console

15.2.3 Suodatuksen toteutus

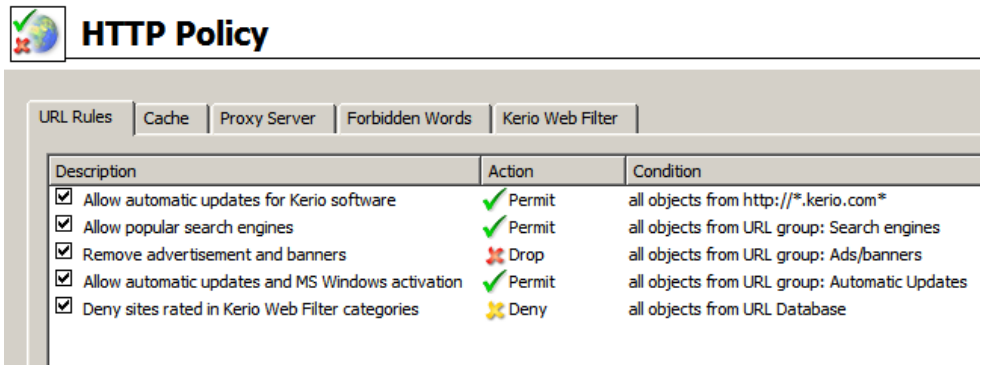
Kerio Control tarjoaa laajat ominaisuudet HTTP-protokollaa käyttävän liikenteen suodatukseen. Suodatuksella voidaan rajoittaa ei-toivottujen Web-sivujen käyttöä, estää tietyn tyyppisten tiedostojen siirto sekä estää viruksien ja haittaohjelmien pääsy verkkoon. (Kerio Control Administrator's Guide 2010.)

Web-sivuja voidaan kattavasti suodattaa seuraavilla tavoilla:

- rajoittaa pääsy URL-osoitteen perusteella
- kieltää tietyt HTML-elementit (skriptit, Active X-objektit, jne.)
- suodattaa Kerio Web Filter-moduulin kategoria määritysten perusteella
- estää sivun lataaminen sen sisältämien sanojen perusteella
- antivirus-moduuli estää sivun latauksen.

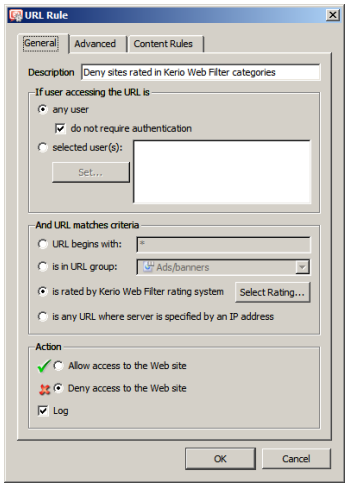
Web-liikenteen rajoitukset määritellään hallintakonsolin sivulta Configuration – Content Filtering – HTTP Policy. URL Rules välilehdellä (ks. kuvio 57) asetetaan säännöt joita vastaan Web-sivuja testataan. Testaus aloitetaan ylhäältä ja siirrytään kohta kerrallaan alaspäin. Säännöissä sallitut osoitteet päästetään läpi ja kielletyt estetään.

Jos pyydetty URL-osoite läpäisee kaikki säännöt, pääsy sivustolle sallitaan. Kaikki URL-osoitteet ovat siis oletuksellisesti sallittuja, ellei niitä erikseen kielletä. Jos halutaan sallia vain tietyt verkkosivut, täytyy ne erillisesti sallia ja tämän jälkeen listauksen loppuun lisätä lauseke, joka kieltää kaikki Web-sivut. (Kerio Control Administrator's Guide 2010.)

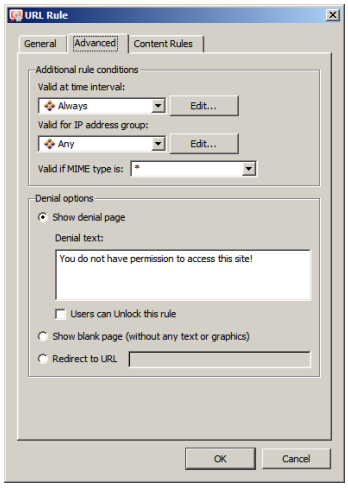


KUVIO 57. URL Rules

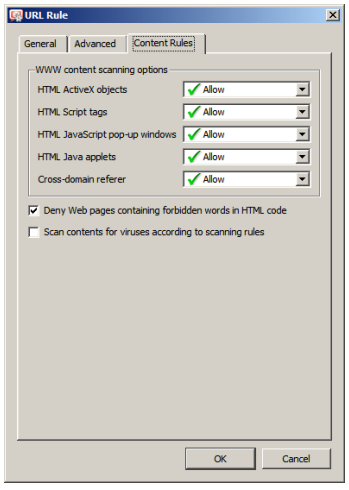
Kuviot 58, 59 ja 60 sisältää URL Rule-ikkunan välilehdet, joiden avulla luodaan uusia suodatusmäärityksiä, sekä muokataan olemassa olevia sääntöjä. General-välilehdeltä määritellään suodatuksen kriteerit, eli millä perusteella liikennettä suodatetaan ja käyttäjät joita sääntö koskee. Advanced-välilehdeltä määritellään kellonajat, jolloin sääntö on voimassa, sekä estoikkunan tai uudelleenohjauksen toteutus. Content Rules-välilehdeltä asetetaan sisältöön perustuvat säännöt, kuten HTML-elementit tai tietyt sanat jotka haluaan estää. (Kerio Control Administrator's Guide 2010.)



KUVIO 58. General-välilehti

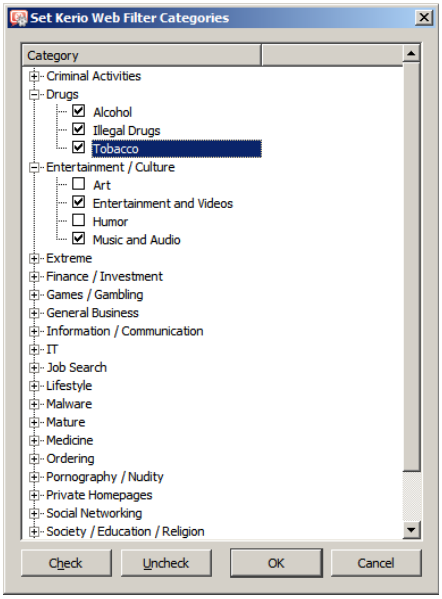


KUVIO 59. Content Filter-välilehti



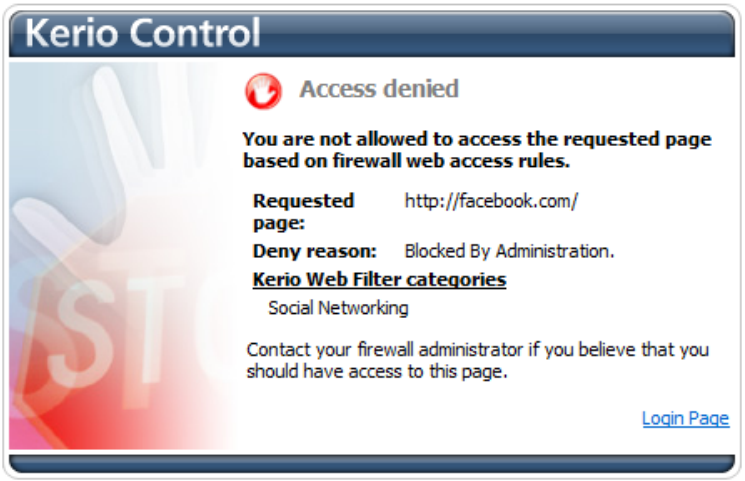
KUVIO 60. Advanced-välilehti

Kategoriasuodatus



KUVIO 61. Web Filter Categories

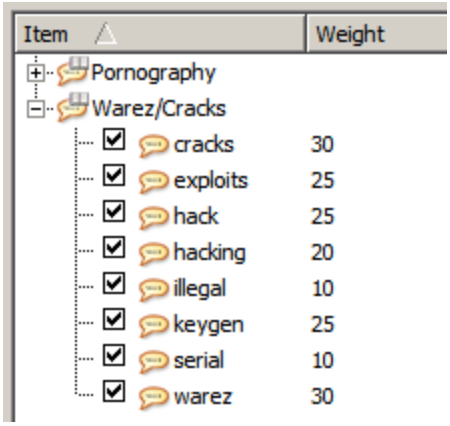
HTTP-sivun, Kerio Web Filter-välilehdeltä asetetaan kategorioihin perustuva suodatus toimintaan. Tämän jälkeen voidaan luotuihin sääntöihin määritellä estettävät kategoriat. General-välilehden Select Rating-nappi avaa Set Kerio Web Filter Categories-ikkunan (ks. kuvio 61) josta valitaan estettäväksi halutut Web-sivukategoriat. Jokainen ladattu verkkosivu tarkistetaan Kerio Web Filter-tietokantaa vastaan. Tämä maailman laajuinen tietokanta sisältää tietoja URL-osoitteista ja niiden luokituksista. Haetut verkkosivut sallitaan tai estetään tämän luokituksen perusteella (ks. kuvio 62). Toimenpidettä on mahdollista nopeuttaa, tallentamalla tarkastettujen sivujen tiedot palvelimen välimuistiin. Tietokanta sisältää kaikkiaan 53 Web-sivukategoriaa. (Kerio Control Administrator's Guide 2010.)



KUVIO 62. Kerio Control estoviesti

Avainsanasuodatus

Forbidden Words-välilehdellä määritetään avainsanoihin perustuva suodatus. Kielletyille sanoille asetetaan painoarvo (ks. kuvio 63) ja sivustolla esiintyvien sanojen arvot lasketaan yhteen. Jos sanojen painoarvojen summa ylittää asetetun raja-arvon (ks. kuvio 64), sivu estetään.



KUVIO 63. Forbidden Words

Uusia sanoja ja sanaluokkia voi vapaasti lisätä, sekä olemassa olevia muuttaa. Myös painoarvot ovat täysin ylläpitäjän määriteltävissä. (Kerio Control Administrator's Guide 2010.)

KUVIO 64. Threshold value

URL-suodatus

URL-suodatuksessa määritellään URL Rule-ikkunan General-välilehdellä URL begins with kohtaan suodatettavan URL-osoitteen alku, ilman protokolla osaa. Osoitteen määrityksessä voidaan käyttää korvausmerkkejä * ja ? korvaamaan merkkijonoja tai yksittäisiä merkkejä. (Kerio Control Administrator's Guide 2010.)

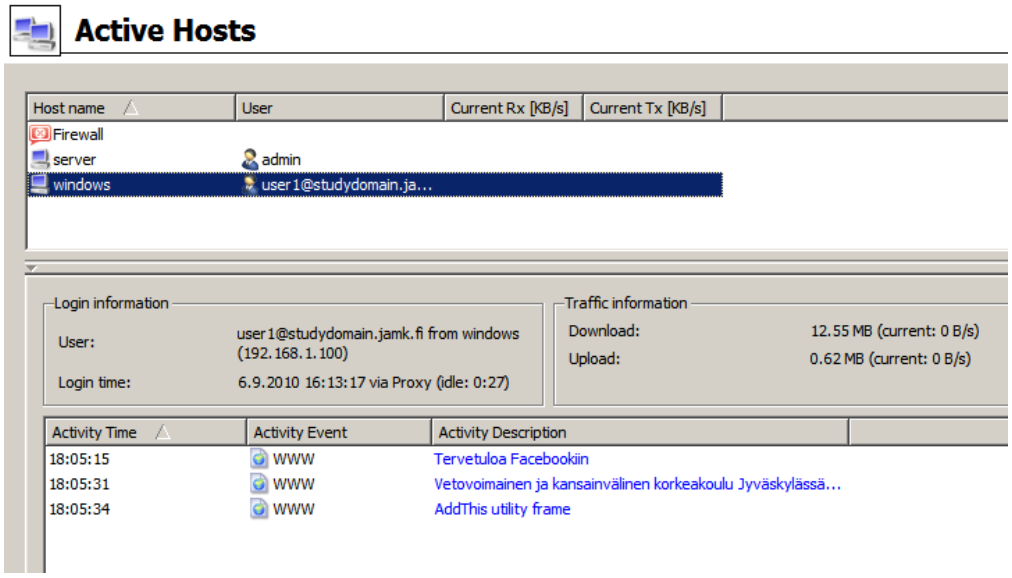
IP-osoitteen käyttö URL-kentässä

"Is any URL where server is given as IP address"-valinnalla voidaan estää URL-pohjaisen suodatuksen kiertäminen IP-osoitteita käyttäen. Kun tämä optio on asetettu, eivät käyttäjät voi ottaa selaimella yhteyttä IP-osoitetta käyttäen, koska palvelin estää yhteyden muodostamisen. (Kerio Control Administrator's Guide 2010.)

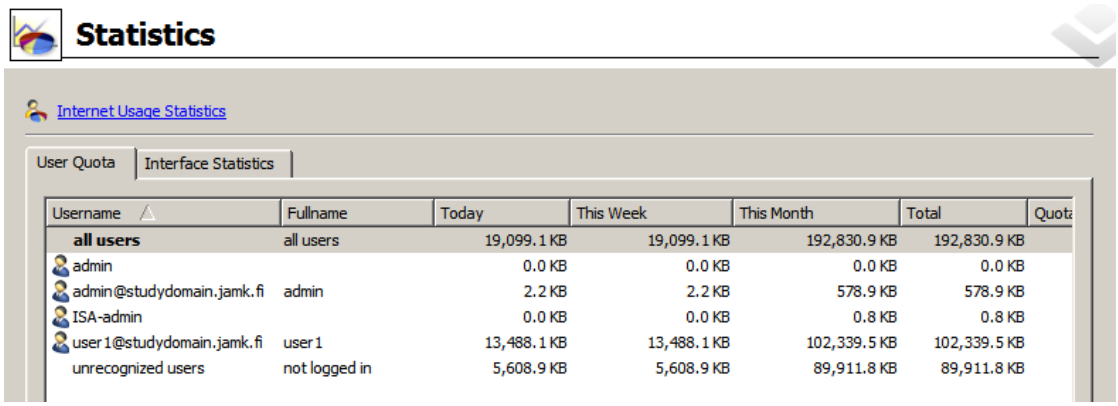
15.2.4 Raportointi ja lokit

Kaikkea palvelimen läpi kulkevaa liikennettä voidaan valvoa. Kerio Control tarjoaa kolmen tyyppistä informaatiota: tilan seuranta, statistiikka ja lokitiedostot.

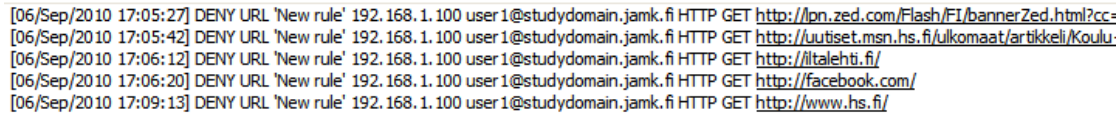
- Tilan seurannassa voidaan kaikkien käyttäjien ja tietokoneiden yhteyksiä palvelimen läpi valvoa (ks. kuvio 65).
- Statistiikka tarjoaa tietoa käyttäjistä ja verkkoliikenteestä tiettynä, määriteltynä ajan jaksona (ks. kuvio 66).
- Lokitiedot kertovat informaatiota tietyistä tapahtumista kuten virheilmoituksista, tiedostojen siirrosta tai päivityksistä (ks. kuvio 67).



KUVIO 65. Verkon aktiiviset käyttäjät



KUVIO 66. User statistics

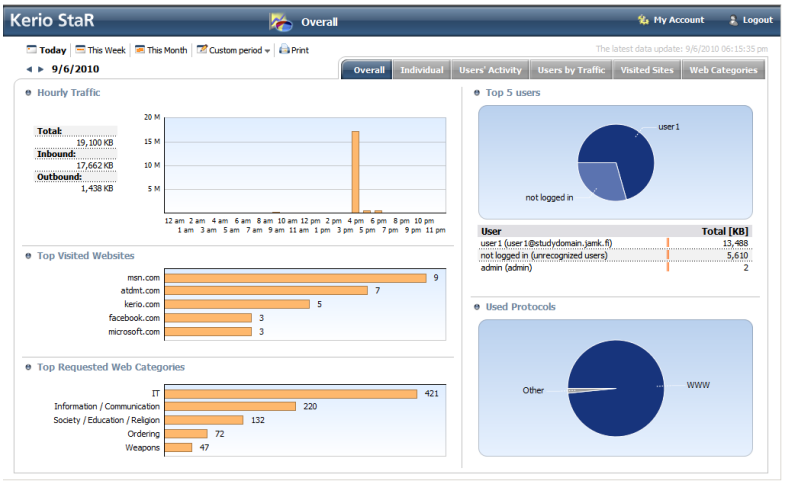


KUVIO 67. URL filter log

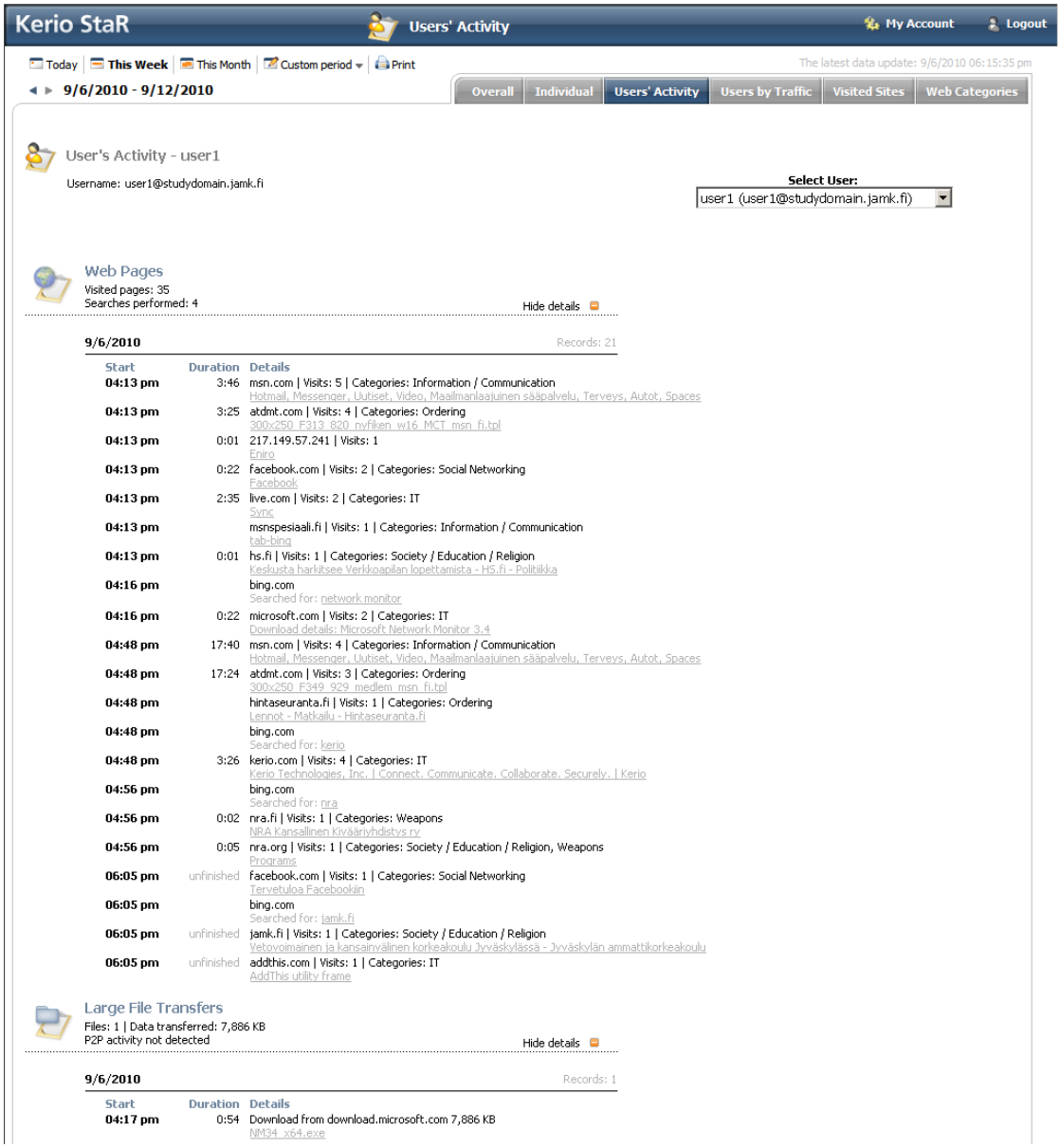
Kerio StaR

Pitempi aikaiseen tiedon keräämiseen ja tilastointiin Kerio Control tarjoaa Kerio StaR – statistic and reporting, raportointityökalun (ks. kuvio 68). Kerio StaR on verkkopohjainen ja mahdollistaa näin tietojen hyvän saatavuuden. Yhteyttä varten ei tarvitse kirjautua Administrative Console-käyttöliittymään, vaan sovellus toimii verkkoselaimella. (Kerio Control Administrator's Guide 2010.)

Kerio StaR kerää tietoja hyvin laaja-alaisesti, tarjoten tarkat tiedot siirretyn datan määrästä, käydyistä verkkosivuista ja käyttäjien toiminnasta. Se myös tallettaa tiedot, perusasetuksilla, 24 kuukauden ajaksi. Tietoja säilytetään välimuistissa ja tallennetaan tietokantaa tunnin välein. Tämä tarkoittaa että aivan reaaliaikaisia tietoja ei tietokannasta ole saatavilla (ks. kuvio 69). (Kerio Control Administrator's Guide 2010.)



KUVIO 68. Kerio StaR Overall



KUVIO 69. Kerio StaR User's Activity

16 YHTEENVETO

Työn tavoitteena oli selvittää Internet-liikenteen ja sisällön suodatukseen käytettyjä tekniikoita ja niiden toimintaa sekä testata eri ratkaisuja käytännössä. Työn aiheen valinnan suurimpana inspiraationa oli oma kiinnostukseni aihetta kohtaa sekä halu kehittää ammatillista osaamistani. Aihe osoittautui haastavaksi ja yllätti laaja-alaisuudellaan. Tästä johtuen aiheen rajaus eli jonkin aikaa omaa elämäänsä työn edetessä.

Suurimpana alkuvaikeutena ja yllätyksenä tuli selkeän ja kattavan taustatiedon löytämisen hankaluus. Uusikin palomuureja käsittelevä kirjallisuus ohitti sovellustason suodatuksen yleensä vain maininnalla, eivätkä suodatusohjelmistojen valmistajat ilmeisesti halua kertoa liikaa käyttämästään tekniikasta. Yksityiskohtaisempaa tietoa suodatustekniikoista ja niiden käytöstä tarjosi valtioiden tai muiden virallisten tahojen suodatushankkeista kiinnostuneiden, sekä yleensä myös huolestuneiden, kansainvälisten järjestöjen julkaisut. Tämän pienen kiertoreitin kautta saatiin kuva siitä mitä tekniikoita suodatuksessa yleisesti käytetään ja voitiin perehtyä tekniikoihin lähemmin.

Tekniikoiden testaus eteni suunnitellusti ja varsin nopeasti työn määrityksiä vastaamattomat tekniikat saatiin pudotettua pois. Lopulta syvempään analysointiin valikoitui varsin kattava paketti erilaisia ohjelmistoja. Huomattava kuitenkin on että testatuista yhdyskäytäväpalvelimista saisi jo itsekseen riittävästi materiaalia useampaankin opinnäytetyöhön, joten ne voitiin tässä työssä käydä läpi vain hyvin pinnallisesti. Kirjoittamisprosessin käynnistäminen otti oman aikansa mutta kun työn lopullinen valmistumispäivämäärä rupesi lähestymään alkoi tuloksia tulla ja työ saatiin valmiiksi aikataulussa.

Työn tekeminen herätti monia ajatuksia. Suodatusta suunnittelevan ylläpitäjän puolelta tärkeimpänä tietona voidaan pitää sitä, että suodatus ei juuri koskaan ole 100 % tehokas. Internetin koko on valtava ja kaiken sisällön luokitteleminen tai luotettava analysoiminen on liki mahdotonta. Lisäksi täytyy ymmärtää että tehokkaan suoda-

tuksen ylläpitäminen vaatii erittäin tarkkaa käyttäjien hallintaa. Jos käyttäjät voivat asentaa tietokoneille ohjelmia tai tehdä muutoksia tietokoneen asetuksiin, kaikki suodatustekniikat voidaan kiertää. Kuten kaikki muukin tietoturvallisuus myös suodatuksen tehokkuus alkaa käyttäjästä ja käyttäjäoikeuksista.

Jos päätös HTTP-sisällön suodatuksesta tehdään, täytyy ymmärtää mitä luotettavan järjestelmän rakentaminen ja ylläpitäminen vaatii. Täytyy myös hyväksyä se tosiasia että osa käyttäjistä tulee suodatuksen kiertämistä yrittämään. Käyttäjien taipumus kiertää asetettuja sääntöjä saattaa olla yrityksen tietoturvalle suurempi riski kuin minkä rajoittamaton Web-sivujen käyttö muodostaa. On myös huomioitava että suodattaminen helposti johtaa yli- tai alisuodatukseen, jolloin suodatus häiritsee normaalia työntekoa tai jättää rajoitettavat Web-sivut estämättä.

Tosiasia kuitenkin on että tarve sisällön suodatukselle ja sisällön-analysoinnille palomuureissa ja yhdyskäytäväpalvelimissa tulee lisääntymään, koska yhä suurempi osa liikenteestä paketoidaan HTTP-protokollalla ja ohjataan sille tarkoitetun portin 80 kautta. Jokaisen tietoverkon ylläpitäjän tulisi olla perillä tästä kehityksestä ja varautua sen vaatimiin muutoksiin niin tekniikassa kuin omassa asennoitumisessa tietoliikenteen tietoturvaan.

Työ täytti sille asetetut tavoitteet ja paransi tekijän taitoja ja osaamista tietoliikenteestä, tietoturvasta ja palvelin ylläpidosta.

LÄHTEET

Access Denied. 2008. Toim. Diebert, R., Palfrey, J., Rohozinski, R. & Zittrain, J. Cambridge, MA, USA: MIT Press.

Björkman, T. 2008. Suojelua vai suodatusta. Suomen kirjastoseura. Viitattu 5.10.2010. HTTP://kirjastoseura.kaapeli.fi/etusivu/seura/mediakasvatus/suodatus_raportti.pdf.

Davies, J. & Northrup, T. 2008. Windows Server 2008 Networking and Network Access Protection (NAP). Redmond, WA, USA: Microsoft Press.

Domain Blacklist Plug-In. 2009. Viitattu 17.6.2010. HTTP://www.simpledns.com/kb.aspx?kbid=1253.

Elharrar, D. 2010. Common Q&A about TMG URL Filtering database. Viitattu 19.11.2010. HTTP://blogs.technet.com/b/isablog/archive/2010/11/15/common-q-amp-a-about-tmg-url-filtering-database.aspx.

Forefront Threat Management Gateway: Overview. 2009. Viitattu 13.8.2010. HTTP://www.microsoft.com/forefront/threat-management-gateway/en/us/overview.aspx.

From Network Security To Content Filtering. 2007. Viitattu 9.9.2010. HTTP://www.ucci.it/docs/CFS-200705.pdf.

Gourley, D. & Totty, B. 2002. HTTP: The Definitive Guide. Viitattu 1.9.2010. HTTP://isys53.informatik.htw-dresden.de/internet/HTTP/ch06.pdf.

Greenfield, P., Rickwood, P. & Tran, H. 2001. Effectiveness of Internet Filtering Software Products. Australia: Commonwealth Scientific and Industrial Research Organisation. Viitattu 14.6.2010. HTTP://www.fbe.unsw.edu.au/cf/staff/peter.rickwood/files/filtereffectiveness.pdf.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. 2. uud. laitos. Jyväskylä: Docendo.

Hassell, J. 2008. Windows Server 2008: the definitive guide. Sebastopol, CA, USA: O'Reilly Media, Inc.

Jyväskylän ammattikorkeakoulu. 2010. Jyväskylän ammattikorkeakoulun kotisivut. Viitattu 28.10.2010. www.jamk.fi.

Kaario, K. 2002. TCP/IP–verkot. Jyväskylä: Docendo.

Kerio Control 7 Datasheet. 2010. Viitattu 8.9.2010. HTTP://www.kerio.com/sites/default/files/Datasheet%20Control_7_US_0610.pdf.

Kerio Control Administrator's Guide. 2010. Viitattu 10.9. HTTP://manuals.kerio.com/control/adminguide/en/.

Microsoft Forefront. 2009. Viitattu 13.8.2010. http://www.microsoft.com/forefront/en/us/default.aspx.

Minasi, M. Gibson, D. Finn, A. Henry, W. & Hynes, B. 2010. Mastering Windows Server 2008 R2. Indianapolis, IN, USA: Wiley Publishing, Inc.

Nevalainen, T. 2010. Valtaosa suuryrityksistä rajoittaa työntekijöidensä Internetin käyttöä. Sanomalehti Karjalainen 5.7.2010. Viitattu 9.7.2010. HTTP://www.karjalainen.fi/Karjalainen/Uutiset_maakunta/valtaosa_suuryrityksist%C3%A4_rajoittaa_ty%C3%B6ntekij%C3%B6idens%C3%A4_internetin_k%C3%A4ytt%C3%B6%C3%A4_6328888.html.

OpenDNS – A Radical Simpler Approach to Web Content Filtering & Security. 2010. Viitattu 17.11.2010. HTTP://www.opendns.com/support/whitepapers/.

PureSight for WinGate. 2010. Viitattu 7.7.2010. HTTP://www.wingate.com/products/puresight-for-wingate/puresight.php.

PureSight 3.0 for WinGate documentation. 2009. Viitattu 8.7.2010. HTTP://downloads.qbik.com/qbiknz2/downloads/PureSight.chm.

RFC 1636. 1994. Report of IAB Workshop on Security in the Internet Architecture. Viitattu 18.8.2010. HTTP://tools.ietf.org/html/rfc1636.

RFC 2616. 1999. Hypertext Transfer Protocol – HTTP/1.1. Viitattu 4.7.2010. HTTP://tools.ietf.org/html/rfc2616.

Simple DNS Plus. 2010. Simple DNS Plus-ohjelman kotisivut. Viitattu 15.6.2010. HTTP://www.simpledns.com.

Turvallisten sisältöjen valikointi ja arviointi. 2006. Opetusministeriö. Viitattu 12.9.2010. HTTP://www.minedu.fi/export/sites/default/OPM/Julkaisut/2006/liitteet/opm_19_tr8.pdf?lang=fi.

Windows Products and Technologies History. 2003. Viitattu 11.10.2010. HTTP://www.microsoft.com/windows/WinHistoryServer.mspx.

WinGate Proxy Server. 2010. Viitattu 7.7.2010. HTTP://www.wingate.com/products/wingate/index.php.

WinGate: The Comprehensive Internet Management Solution for Windows. 2010. Viitattu 8.7.2010. HTTP://www.redline-software.com/eng/support/docs/wingate/.

Zwicky, E., Cooper, S. & Chapman, B. 2001. Internet palomuurien rakentaminen - tehokäyttäjän opas. Helsinki: Satku.