



## **TEKNIikka JA LIIKENNE**

**Tietotekniikka**

**Tietoverkot**

## **INSINÖÖRITYÖ**

**Blue Coat -sisällönsuodatus ja -kompressointi**

**Työn tekijä: Anssi Suokas  
Työn ohjaaja: Janne Salonen**

**Työ hyväksytty: 11. 5. 2009**

**Janne Salonen  
Yliopettaja**



## **ALKULAUSE**

Tämä insinöörityö tehtiin Metropolia Ammattikorkeakoululle. Työn valvojana ja ohjaajana toimi yliopettaja Janne Salonen. Kiitän häntä hyvin sujuneesta yhteistyöstä lopputyön sekä opintojen osalta. Kiitän myös lehtori Jussi Alhorinnettä kieliasun tarkistuksesta.

Helsingissä 24.4.2009

Anssi Suokas

## TIIVISTELMÄ

|   |   |
|---|---|
| <b>Työn tekijä:</b> Anssi Suokas  |   |
| <b>Työn nimi:</b> Blue Coat -sisällönsuodatus ja -kompressointi   |   |
| <b>Päivämäärä:</b> 24.4.2009  | <b>Sivumäärä:</b> 42 s. + 6 liitettä          |
| <b>Koulutusohjelma:</b><br>Tietotekniikka   | <b>Suuntautumisvaihtoehto:</b><br>Tietoverkot |
| <b>Työn ohjaaja:</b> Yliopettaja Janne Salonen  |   |
| <b>Työn ohjaaja:</b>  |   |
| <p>Tämä työ tehtiin Metropolia Ammattikorkeakoululle. Työssä selvitettiin Blue Coat ProxySG -laitteiden ominaisuuksia ja mahdollisuuksia verkon välityspalvelimena suodattamaan ja optimoimaan verkon HTTP-liikennettä. Työssä esitellään Blue Coat ProxySG -laitteistoa, sisällönsuodatuskompressointi, sekä Applications Delivery Network -sisältökytkentää. ADN-sisältökytkentä on tarkoitettu WAN-verkossa sijaitsevien toimipisteiden väliseen ohjelmien kiihdytykseen ja verkon kaistanleveyden säästämiseen. Työn tavoitteena oli tehdä laitteilla sisällönsuodatusratkaisu ja ADN-sisältökytkentä.</p> <p>Työn teoriaosassa esitellään sisällönsuodatus teknologioita ja niiden toteutustapoja sekä ongelmakohtia. Teoriaosassa esitellään myös laitteiden välille muodostettava sisältökytkentä ja sen edut. Käytännön osuus on jaettu kahteen osaan, ja ensimmäinen osa käsittelee sisällönsuodatuksen käyttöön ottamisen ja sääntöjen luomisen. Toisessa käytännön osassa käsitellään ADN-kytkennän käyttöönotto.</p> <p>Työn lopputuloksena saatiin kaksi toimivaa ratkaisua, joista ensimmäisessä otettiin käyttöön sisällönsuodatusratkaisu halutuin määrityksin ja toisessa osuudessa HTTP-liikenteen kiihdytys ja kaistankäytön säästöratkaisu.</p> |   |
| <b>Avainsanat:</b> Proxy, HTTP-liikenne, ADN, sisällönsuodatus, kompressio  |   |

## ABSTRACT

|  |  |
|--|--|
| <b>Name:</b> Anssi Suokas  |  |
| <b>Title:</b> Blue Coat Content Filtering and Compression  |  |
| <b>Date:</b> 24 April 2009   | <b>Number of pages:</b> 42               |
| <b>Department:</b><br>Information Technology   | <b>Study Programme:</b><br>Data Networks |
| <b>Instructor:</b> Janne Salonen, Principal lecturer   |  |
| <b>Supervisor:</b>   |  |
| <p>This study was done for the Helsinki Metropolia University of Applied Sciences. In this study, the properties and possibilities of Blue Coat ProxySG equipment as a network proxy server to filter and optimize HTTP traffic across the network was examined. As a part of the study, the Blue Coat ProxySG equipment, content compression and Applications Delivery Network content switching are described. ADN content switching is intended to accelerate program execution and to preserve bandwidth between work nodes in WAN networks. The goal of the study was to find content filtering and ADN content switching solutions using this equipment.</p> <p>In the theoretical part of this study, content filtering techniques and implementations as well as related problem areas are described. Also, the advantages of content switching between connected equipment are described. The practical part of this study is divided into two parts: The first part covers the procedures for creating content filtering and creating the necessary rules for it. The second part covers ADN switching configuration and implementation.</p> <p>The end result of this study consists of two working solutions. The first result is the implementation of content filtering with desired configurations, and the second is a solution that accelerates HTTP traffic and preserves bandwidth.</p> |  |
| <b>Keywords:</b> Proxy, HTTP traffic, AND, Content Filtering, Compression  |  |

## **SISÄLLYSLUETTELO**

### **ALKULAUSE**

### **TIIVISTELMÄ**

### **ABSTRACT**

## **KÄSITELUETTELO**

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>JOHDANTO</b>   | <b>1</b>  |
| <b>2</b> | <b>PROTOKOLLAPINO JA TCP/IP-PROTOKOLLAPERHE</b>         | <b>2</b>  |
| 2.1      | OSI-viitemalli  | 2         |
| 2.2      | TCP/IP-viitemalli                                       | 5         |
| 2.3      | TCP/IP-protokollaperhe                                  | 5         |
| <b>3</b> | <b>VÄLITYSPALVELIN</b>                                  | <b>7</b>  |
| <b>4</b> | <b>SISÄLLÖNSUODATUS</b>                                 | <b>9</b>  |
| 4.1      | Sisällönsuodatustekniikat                               | 10        |
| 4.2      | Layer 4 ja 7 -tason suodatus                            | 11        |
| <b>5</b> | <b>KOMPRESSOINTI</b>                                    | <b>13</b> |
| <b>6</b> | <b>BLUE COAT -LAITTEET</b>                              | <b>16</b> |
| <b>7</b> | <b>PROXYSG 200: SISÄLLÖNSUODATUS JA HTTP-KOMPRESSIO</b> | <b>18</b> |
| 7.1      | Käyttöönotto ja käyttöjärjestelmä                       | 19        |
| 7.2      | Sisällönsuodatus  | 23        |
| 7.3      | Politiikat  | 24        |
| 7.4      | Sisällönsuodatuksen ja HTTP-kompression toteutus        | 27        |
| <b>8</b> | <b>PROXYSG: SISÄLTÖKYTKENTÄ</b>                         | <b>33</b> |
| <b>9</b> | <b>JOHTOPÄÄTÖKSET</b>                                   | <b>41</b> |
|          | <b>VIITELUETTELO</b>                                    | <b>42</b> |
|          | <b>LIITTEET</b>   |           |

Liite 1. Sisällönsuodatuksen ja -kompression konfiguraatiot laitteelle ProxySG200.

Liite 2. Cisco reitittimen konfiguraatiot ADN-kytkennän etätoimiston LAN-verkolle.

Liite 3. Cisco reitittimen konfiguraatiot ADN-kytkennän palvelinpuolen LAN-verkolle.

Liite 4. ADN konfiguraatiot ProxySG200 laitteelle.

Liite 5. ADN konfiguraatiot ProxySG400 laitteelle.

Liite 6. Blue Coat ProxySG200 ja ProxySG400 laitteiden tekniset tiedot.

## KÄSITELUETTELO

|       |  |
|-------|--|
| ADN   | <i>Application Delivery Network</i> . Blue Coat Inc. kehittämä ProxySG-laitteiden välille muodostettava sisältökytkentä.   |
| CIFS  | <i>Common internet Files System</i> . Microsoftin kehittämä verkkotiedostojärjestelmä, joka aikaisemmin tunnettiin nimellä SMB.  |
| DHCP  | <i>Dynamic Host Configuration Protocol</i> . Protokolla, jonka avulla tietokoneelle voidaan määrittää IP-osoite automaattisesti.   |
| DNS   | <i>Domain Name System</i> . Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.   |
| FTP   | <i>File Transfer Protocol</i> . TCP-protokollaa käyttävä tiedonsiirtomenetelmä kahden tietokoneen välillä.   |
| HTTP  | <i>Hypertext Transfer Protocol</i> . Protokolla jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.  |
| HTTPS | <i>Hypertext Transfer Protocol Secure</i> . HTTP-protokollan salattu versio. HTTPS-protokollaa käytetään tiedon suojattuun siirtoon webissä. Tiedot salataan ennen lähettämistä SSL-protokollan avulla.    |
| IM    | <i>Instant Messaging</i> . Teknologia mikä mahdollistaa tosi-aikaisen kommunikoinnin kahden ja useamman osanottajan välillä internetin ylitse tai joissakin muodoissa sisäisessä verkossa ja intranetissä. |
| ISO   | <i>International Organization of Standardization</i> . Kansainvälinen standardoimisjärjestö, jonka määrittelemiä standardeja on otettu laajasti käyttöön.  |
| LAN   | <i>Local Area Network</i> . Tietoliikenneverkko rajoitetulla maantieteellisellä alueella. Esimerkiksi yhden talon koneiden muodostama tietokoneverkko tai yrityksen yhden toimipisteen verkko.             |
| MACH5 | <i>Multiprotocol Accelerated Caching Hierarchy</i> . Blue Coat Inc. kehittämä teknologia, mikä mahdollistaa usean kiihdytysteknologian yhdistämisen yhdeksi.   |
| MAPI  | <i>Messaging Application Programming Interface</i> . Viestintä arkkitehtuuri ja komponenttien objekti malli.   |
| NAT   | <i>Network Address Translation</i> . Prosessi verkko-osoitteiden informaation muokkaamiseen ja liikenteen reititykseen yhdestä verkosta toiseen muuntaen osoitteen.  |
| OSI   | <i>Open System Interconnection Reference Model</i> . Tapa kuvata tiedonsiirto-protokollien yhdistelmä seitsemässä kerroksessa.   |
| SOCKS | SOCKS on internetprotokolla mikä, reitittää verkkopaketteja välityspalvelimen kautta asiakas- palvelin -ohjelmille.  |

|        |   |
|--------|---|
| SSL    | <i>Secure Socket Layer</i> . Kryptograafinen protokolla, mikä tarjoaa turvallisuutta ja tiedonsiirron salaamista TCP/IP-yhteyksissä esimerkiksi internetiin.  |
| TCP    | <i>Transmission Control Protocol</i> . Protokolla jolla luodaan yhteydet tietokoneiden sovellusten välille käyttämällä IP-paketteja.  |
| IP     | <i>Internet Protocol</i> . Verkkokerroksen protokolla jota voidaan pitää TCP/IP protokollan ytimenä.  |
| TCP/IP | <i>Transmission Control Protocol / Internet Protocol</i> . TCP/IP-protokolla ei varsinaisesti ole yksi protokolla, vaan kyseessä on useista eri tarkoituksiin suunnitelluista protokollista muodostuva protokollaperhe. |
| URL    | <i>Uniform Resource Locator</i> . Internetissä olevan sivuston tai tiedoston sekä näiden käyttöön tarvittavan yhteyskäytännön yksilöivätunnus. WWW-sivun osoite.  |
| WAN    | <i>Wide Area Network</i> . Laajaverkko on tiedonsiirtoverkko, joka peittää laajola maantieteellisiä alueita.  |
| WCCP   | <i>Web Cache Communication Protocol</i> . Cisco Systemsin kehittämä sisällönreititys-protokolla.  |
| VPM    | <i>Visual Policy Manager</i> . VPM on graafisesti toteutettu politiikka editori mikä sisältyy Proxy SG-laitteisiin.   |
| VPN    | <i>Virtual Private Network</i> . Tapa jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.   |
| WWW    | <i>World Wide Web</i> . Internet-verkossa toimiva hajautettu hypertekstijärjestelmä.  |



## 1 JOHDANTO

Tässä insinöörityössä tutkitaan internetliikenteen sisällönsuodatusta, verkkojen välistä sisällönkompressointia ja -kytkentää. Työssä käsitellään ensin luvussa 2 tietotekniikan perusasioita lähtien protokollapinon rakenteesta ja tavasta, miten dataliikenne kuljetetaan eri verkkokerroksilla. Työssä käsitellään välityspalvelimen tehtävät ja tarkoitus luvussa 3, jonka jälkeen on saatu pohja asioille, joita aletaan käsitellä dataliikenteen sisällönsuodatuksessa ja sen tarjoamissa mahdollisuuksissa ja ongelmakohtissa. Työ on rajattu tutkimaan vain HTTP-liikennettä, mikä käyttää TCP/IP-protokollia liikennöintiin.

Tarkoitus on tutustua Blue Coat Systems Inc. tarjoamaan HTTP-liikenteen suodatus- ja verkon optimointiratkaisuun ja sen tarjoamiin mahdollisuuksiin käyttämällä Blue Coatin ProxySG-sarjan laitteita. Nykypäivänä internetliikenteen suodatus on välttämätöntä tietoturvan kannalta lisääntyvien tietoturvariskien takia, ja suodatus onkin herättänyt paljon puheenaihetta ja ihmetystä sen ongelmakohtien takia.

Luvussa 4 käsitellään sisällönsuodatusta ja sen teoriaa. Luku 5 käsittelee HTTP-liikenteen kompressointia Blue Coat ProxySG -laitteilla ja ADN-sisältökytkennän teoriaosuuden. Luvussa 6 tutustutaan Blue Coat Systems Inc. tarjoamiin välityspalvelimiin ja käydään läpi työssä myöhemmin käytettävien ProxySG200 ja ProxySG400 -laitteiden tekniset tiedot ja ominaisuudet. Työn luvussa 7 käsitellään internetliikenteen sisällönsuodatuksen ja HTTP-kompressoinnin käyttöönottoaminen ProxySG200-laitteella ja siinä määritetään laitteen käyttöjärjestelmän asetukset ja ominaisuudet sekä luodaan suodatusratkaisu ja siihen säännöt sekä politiikat. Luku 8 käsittelee ADN-sisältökytkennän käyttöönottoamisen ja asetukset WAN-verkon eripuolilla sijaitsevien toimipisteiden välille. Toimipisteiden välille luodaan HTTP-liikenteelle oma tunneli, mitä pitkin HTTP-liikennettä kuljetetaan pakattuna verkkojen välillä ja näin saadaan nopea sisältökytkentä verkkojen välille.

Käytettävien laitteiden valmistaja BlueCoat Systems Inc. on vuonna 1996 perustettu osakeyhtiö, joka sijaitsee Kalifornian Sunnyvalessa. Yhtiö tarjoaa tietoturvaa web-tietoliikenteeseen. Yrityksille yhtiö tarjoaa erilaisia mahdollisuuksia nopeuttaa ja hallita tietoliikennettä yrityksen sisäisten verkkojen välillä sekä internetin ylitse. Blue Coatin tarjoamat ratkaisut soveltuvat käytet-

täviksi yritysten sivukonttoreissa oletusyhdyskäytäväksi, niin kuin myös yritysten palvelinkeskuksissakin. Yhtiö tarjoaa organisaatioille turvallisuuden ja verkonsuorituskyvyn hallinnointi- ja optimointipalveluja. Blue Coatin laitteita ja palveluja löytyy tällä hetkellä yli 15 000 asiakkaalta maailmanlaajuisesti. Blue Coat on yksi johtavista sisällönsuojaus ja ohjelmistopalveluiden tarjoajista markkinoilla. [1.]

## 2 PROTOKOLLAPINO JA TCP/IP-PROTOKOLLAPERHE

Tässä luvussa käsitellään verkon protokollien sijoittumisen esitystapoja protokollapinon avulla ja TCP/IP-verkon protokollien toiminta ja tehtävät. Nämä tiedot luovat perusteet tukemaan myöhemmin käsiteltäviä asioita.

Protokollapinoa kuvataan yleensä kahdella eri viitemallilla, joista yleisempi on OSI-malli (Open Systems Interconnection Reference Model). Siinä kuvataan tiedonsiirtoprotokollien yhdistelmä seitsemässä kerroksessa. Kaikki kerroksista käyttävät yhtä alemman kerroksen palvelua ja tarjoavat palveluja yhtä kerrosta ylemmäs. Toinen tapa, millä kuvataan protokollapinoa, on TCP/IP-malli (Transmission Control Protocol / Internet Protocol), mikä koostuu neljästä kerroksesta ja soveltuu lähinnä vain TCP/IP-tiedonsiirron mallintamiseen. Seuraavaksi käsitellään OSI-viitemalli ja TCP/IP-viitemalli sekä niiden eroavaisuudet toisistaan. [2, s.181-182.]

### 2.1 OSI-viitemalli

OSI-mallissa tietojärjestelmälle on määritelty seitsemän perustehtävää ja tehtävät on kuvattu kerroksina, jotka ovat numeroitu yhdestä seitsemään. Kerrokset 1-3 määrittelevät laitteistojen ja niihin läheisesti liittyvien protokollien toiminnan ja niitä kutsutaan alakerroksiksi. Ylemmät kerrokset määrittelevät puolestaan asiakas-palvelinsovelluksen ohjelmallisen toiminnan. Ylemmistä kerroksista käytetään nimitystä isäntäkerrokset. OSI-viitemalli on kehitetty 1980-luvun alussa ja se on ISO:n kansainvälinen standardi. Seuraavaksi käsitellään OSI-mallin eri kerrokset ja niiden tehtävät protokollapinossa lyhyesti.

### *1. Fyysinen kerros (Physical layer)*

Mallin alinta kerrosta kutsutaan fyysiseksi kerrokseksi. Tämä kerros määrittelee kaapelointiin ja signaalinsiirtoon liittyvät sähköiset ja mekaaniset arvot. Yleisempiin määrittelyihin kuuluvat käytettävät liitin- ja kaapelityypit sekä signaalien jännitetasot. Verkon aktiivilaitteista keskittimet, toistimet ja mediamuuntimet kuuluvat fyysisen kerroksen laitteisiin.

### *2. Siirtokerros (Data Link layer)*

Siirtokerroksen toinen kutsumanimi on siirtoyhteyshierarkia, johon usein viitataan termillä layer 2. Siirtokerros on mallin toinen kerros, mikä määrittelee miten lähetettävästä datasta muodostetaan kaapelointijärjestelmässä siirrettäviä yksiköitä, kuten kehyksiä (frame) tai soluja (cell). Kerros määrittelee myös lähetettävän ja vastaanottavan laitteen fyysiset osoitteet (MAC-osoitteet). Kerroksen tärkeimpiä aktiivilaitteita ovat verkkokortit, sillat ja kytkimet.

### *3. Verkkokerros (Network layer)*

Verkkokerros määrittelee verkkojen välisessä tietoliikenteessä reitityksen sekä huolehtii eri liikennöintimuotojen välisestä priorisoinnista. Kerrosta kutsutaan myös termillä layer 3, ja sen keskeisin aktiivilaite on reititin.

### *4. Kuljetuskerros (Transport layer)*

Ensimmäinen ohjelmallisista kerroksista on kuljetuskerros. Kerroksen tehtävistä huolehtivat kuljetusprotokollat. Kuljetusprotokollat pilkkovat sovellusten lähetettävän datavirran käsittelykokoisiin yksiköihin eli segmentteihin tai paketteihin. Datan pilkkominen, lähetettävän pakettikoon määrittely ja kuittaus muodostavat tehtäväkokonaisuuden, jota kutsutaan vuonohjaukseksi.

### 5. Istuntokerros (Session layer)

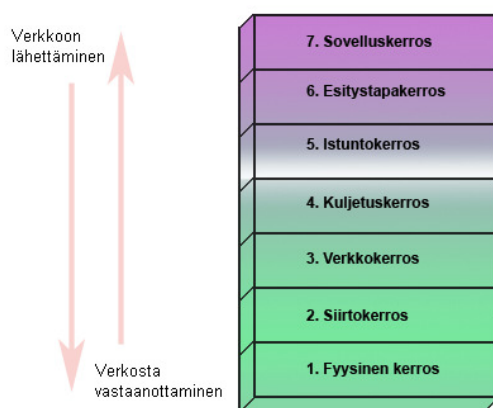
Istuntokerroksen tehtäviin kuuluvat käyttöoikeuksien tarkistukset sekä muut järjestelmän suojauksiin liittyvät tehtävät. Salausohjelmistot ja tietokantojen hallintajärjestelmät toimivat osittain tämän kerroksen ohjelmistoina.

### 6. Esitystapakerros (Presentation layer)

Esitystapakerros määrittelee asiakkaan ja palvelimen välisen sanomaliikenteen muodon. Kerroksen määrittelyihin kuuluvat erilaiset koodausjärjestelmät. Järjestelmien välillä tiedonsiirto tapahtuu binäärimerkkijonoina ja koska siirrossa käytetään vain yhtä tietotyyppiä, joudutaan sanomarakenteeseen määrittelemään tietotyyppien koodaaminen binäärimerkkijonoksi ja vastaanottavassa sovelluksessa takaisin alkuperäisiksi tietotyypeiksi.

### 7. Sovelluskerros (Application layer)

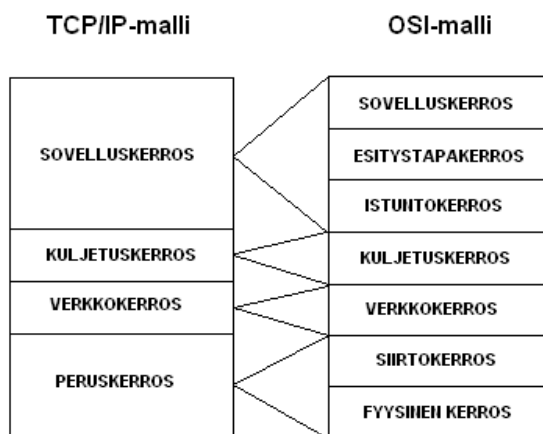
Ylintä kerrosta kutsutaan sovelluskerrokseksi ja kerroksen tehtävinä on määritellä sovellusten ja käyttöjärjestelmien toiminnasta ne osat, joita alemmissa kerroksissa ei ole määritelty. [2, s.138-142.]



Kuva 1. Protokollapino kuvaa eri verkkokerroksia ja tapaa miten dataliikenne kerroksilla siirtyy. [lähde 2, s. 138 mukaillen.]

## 2.2 TCP/IP-viitemalli

TCP/IP-protokollapino on yksinkertaisempi viitemalli kuin OSI-malli eikä siinä ole huomioitu kaikkia OSI-mallin mukaisia tehtäviä. Yksittäinen TCP/IP-kerros huolehtii useamman kerroksen tehtävistä protokollapinossa. Malli koostuu neljästä kerroksesta ja soveltuu lähinnä vain TCP/IP-tiedonsiirron mallintamiseen. Mallissa alin kerros sisältää OSI-mallin fyysisen- ja siirtokerroksen ja sitä kutsutaan peruskerrokseksi. Verkkokerros on protokollapinossa toisena, kolmantena kerroksena on kuljetuskerros ja ylin kerroksista on nimeltään sovelluskerros, joka sisältää OSI-mallin kerroksista istuntokerroksen, esitystapakerroksen ja sovelluskerroksen. [2, s.180-184.]



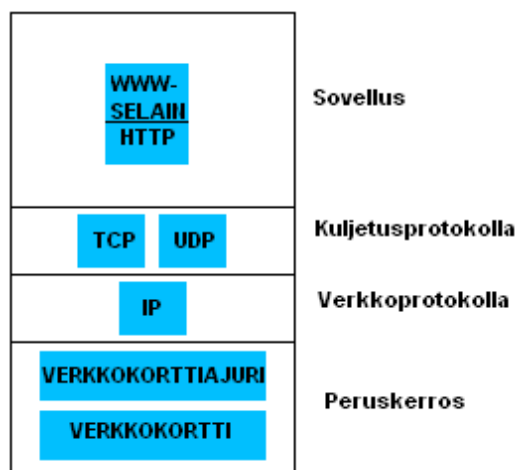
Kuva 2. TCP/IP-malli eroaa OSI-mallista kerrosten lukumäärässä. Yksi kerros hoitaa useampaa tehtävää, joten kerroksia on vain neljä. [lähde 2, s.184 mukailen.]

## 2.3 TCP/IP-protokollaperhe

TCP/IP-protokolla ei varsinaisesti ole yksi protokolla, vaan kyseessä on useista eri tarkoituksiin suunnitelluista protokollista muodostuva protokollaperhe. Nämä protokollat voidaan kuvata TCP/IP-viitemallin verkkokerroksilla. Jäsenprotokollat voidaan karkeasti jakaa käyttötarkoituksensa mukaan eri kerroksiin. Lähiverkkoprotokoliin verrattuna suurin ero on nimi ja osoitejärjestelmien hierarkkisuus. TCP/IP-verkossa toiminnan lähtökohtana on verkkojen välinen tietoliikenne. Verkon sijainnin internetissä, sekä koneen sijainnin verkon sisällä määrittelee hierarkkiset nimi- ja osoitejärjestelmät. Nimien

ja osoitteiden yhdistämiseksi käytetään nimipalveluita, jotka muodostavat TCP/IP-verkon tärkeimmän ydinpalvelun.

Reititys on toinen tärkeä ydinpalvelu, joka mahdollistaa tiedonsiirron eri arkkitehtuurereja noudattaen Internetin osaverkkojen välillä. IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden osoitteista ja pakettien reitittämisestä verkossa. IP-protokollan päällä voidaan ajaa useita muita verkko- tai kuljetuskerroksen protokollia ja näistä TCP-protokolla on yleisin. Se vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä sekä hukkuneiden pakettien uudelleenlähetyksestä. TCP/IP-protokollaperheeseen kuuluu monia muitakin protokollia kuten yhteydetön UDP-protokolla (User Datagram Protocol), mutta pääosa liikennöinnistä tapahtuu TCP-yhteyksinä IP-protokollien päällä ja tässä työssä käsitellään lähinnä TCP/IP-protokollia ja tiedon siirtymistä liittyen näihin protokolleihin. Kuvasssa 3 näkyy mitä alemman kerroksen protokollia WWW (World Wide Web) -selain käyttää liikennöidessään. [2, s.178-180.]



Kuva 3. WWW-selaimen asema TCP/IP-viitemallissa [lähde: 2, s.297 mukaillen.]

### HTTP-protokolla

HTTP-protokolla (HyperText Transfer Protocol) on sovellustason protokolla ja se määrittelee esitettävän tiedon muodon ja koodaustavan, jotta eri käyttöjärjestelmät ja laitealustat pystyvät tulkitsemaan tietoa. Käytettäessä WWW (World Wide Web) -selainta, käyttää se sovelluskerroksen protokollana HTTP:tä. [2, s.296.]

### *TCP-protokolla*

TCP-protokolla on protokollaperheen toinen ydin protokolla. Se luo yhteydet tietokoneiden sovellusten välille käyttämällä IP-paketteja. TCP-protokollan tehtäviin kuuluu vuonhallinta, luotettavuudesta ja kuittauksista huolehtiminen sekä pakettien laittaminen oikeaan järjestykseen. TCP-protokolla huolehtii luotettavan päästä päähän –yhteyden muodostamisesta kahden koneen välille. Sitä kutsutaan myös yhteydelliseksi tiedonsiirtoprotokollaksi, jonka tehtävänä on sopia yhteyden muodostamisesta ja liikennöinnin ehdoista kahden koneen välillä. Käytettäessä WWW-selainta tarvitaan kuljetustason TCP-protokolla huolehtimaan sovelluksen lähettämän tietovirran paloittelusta selaisiin osiin, joita verkon laitteet pystyvät käsittelemään. [2, s.296-298.]

### *IP-protokolla*

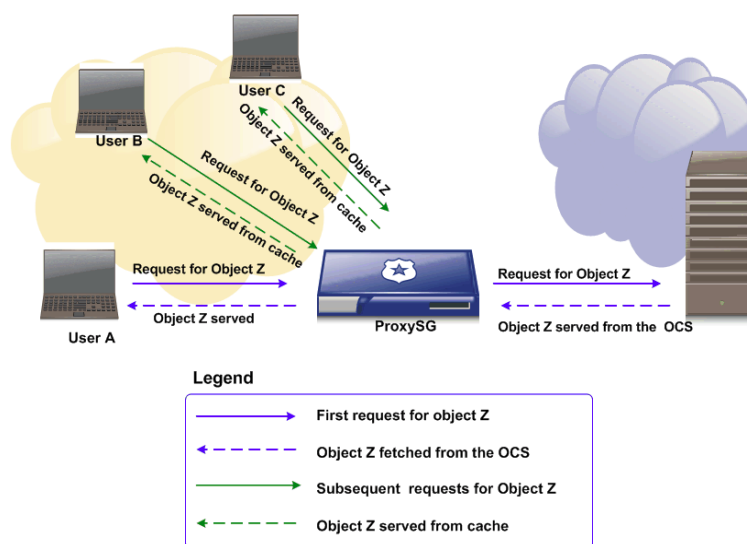
Verkkokerroksen IP-protokollaa voidaan pitää TCP/IP-protokollan ytimenä. Verkossa tietoa välittävät reitittimet lähettävät ja vastaanottavat ainoastaan IP-paketteja eivätkä tutki paketin sisällä olevaa protokollaa. Tyypillisesti verkkoyhteydet tehdään vasta IP-pakettien sisällä olevan TCP-protokollan avulla eikä verkko tästä syystä tiedä käytettävistä yhteyksistä mitään. IP-protokolla on melko monipuolinen protokolla, koska sitä voidaan ajaa melkein minkä tahansa verkon päällä ja lähes mitä tahansa sovellusta voidaan ajaa internet-protokollan päällä. WWW:n tapauksessa IP-protokolla huolehtii siitä, että lähetettävät paketit löytäisivät oikeaan kohdeverkkoon. [2, s.296-298.]

## **3 VÄLITYSPALVELIN**

Välityspalvelimesta käytetään myös englanninkielistä nimitystä proxy. Sen tehtävänä on varastoida ja suodattaa verkossa siirrettäviä tiedostoja. Tyypillisesti välityspalvelimia käytetään WWW-sivujen varastoimiseen. Sivujen varastoiminen nopeuttaa latausaikoja ja vähentää tiedon lataamisen aiheuttamaa kuormitusta verkossa. Tiedostot saadaan varastoimalla lähemmäksi niiden hakijoita. Välityspalvelimia on kahdenlaisia, määriteltyjä ja läpinäkyviä. Yksinkertaisimmat versiot välityspalvelimista ”Circuit level proxies” eivät

tarkista ollenkaan pakettien sisältöä vaan jakavat yhteyden käyttäjän ja palvelimen välille. Jos tämä proxy sijaitsee palvelimen, mikä ei autentikoi käyttäjiä edessä, niin on mahdollista lisätä autentikointikerros. Yleisemmät proxyt, kuten web-liikenteeseen tarkoitettut pystyvät suorittamaan käyttäjän autentikointia, säilömään web-sivuja ja todentamaan joitakin protokollia. Proxyilla pystytään myös pitämään yllä sallittujen osoitteiden ja kiellettyjen osoitteiden listoja, millä voidaan rajoittaa käyttäjien ja palvelimien pääsyä niihin. Osa proxyistä ovat turvallisempia, ja ne pystyvät myös havaitsemaan hyökkäyksiä ja estämään niitä. [3.]

Kuvassa 4 havainnollistetaan välityspalvelimen toimintaa. Käyttäjä A hakee välityspalvelimelta sisältöä, joka välittää pyynnön palvelimelle. Palvelin lähettää pyydetyn sisällön välityspalvelimelle, mikä tarjoilee sen käyttäjä A:lle. Käyttäjät B ja C hakevat samaa sisältöä, mitä käyttäjä A haki hetkeä aikaisemmin ja saavat sisällön nopeasti suoraan välityspalvelimen muistista, eikä sisältöä tarvitse hakea uudelleen palvelimelta asti. Tämä nopeuttaa sisällön saamista ja vähentää sisällön noutamiseen käytettyä aikaa. [4, s.120.]



Kuva 4. Välityspalvelimen toimintamalli [4, s.120.]



### *Määritelty välityspalvelin*

Käytettävä välityspalvelin voidaan määrittää erikseen muodostettaessa internet-yhteyttä jolloin kaikki liikenne välittyy välityspalvelimen kautta. Palvelimen tapahtumarekisteriin, eli lokiin jää merkinnät kaikista yhteyksistä ja niiden liikenteestä. Välityspalvelin voi myös piilottaa käyttäjän henkilöllisyyden, jolloin sivustot millä käyttäjä vierailee näkyvät sivuston tapahtumarekisterissä vain välityspalvelimen osoitteena. Välityspalvelimia ei yleensä kuitenkaan voida käyttää niiden intranetien ulkopuolella. [3.]

### *Läpinäkyvä välityspalvelin*

Läpinäkyvää välityspalvelinta käytettäessä käyttäjän ei tarvitse määritellä välityspalvelimen osoitetta muodostaessaan internet-yhteyttä, käyttäjä ei voi myöskään kiertää tätä palvelinta. Välityspalvelimella voidaan määrittää sallittuja ja kiellettyjä -sivustoja. Välityspalvelimen loki-tiedostosta voidaan seurata sen välittämää liikennettä ja tarvittaessa myös rajoittaa sitä. [3.]

## **4 SISÄLLÖNSUODATUS**

Sisällönsuodatus ja sen rooli internetselainliikenteen tietoturvassa, hallinnoinnissa ja kontrolloinnissa on kasvanut, ja sen kysyntä on lisääntynyt internetin ja uusien URL-osoitteiden määrän kasvamisen seurauksena. Internetselailun sisällönsuodatusohjelmilla pyritään estämään käyttäjän pääsy valitunaiheisille internetsivuille. Suodatusohjelmat sisältävät yleensä muitakin ominaisuuksia millä voidaan seurata internetin käyttöä ja kontrolloida siihen käytettävää kapasiteettia. Sisällönsuodatus ohjelmista yleensä löytyy myös erilaisia raportointi ominaisuuksia ja niitä voidaan säätää käyttötarkoituksen mukaan. Sisällönsuodatusohjelmalla voidaan luoda erilaisia politiikoita ja määrittää kiellettyjä tai sallittuja sivuja yksinkertaisimmillaan IP-osoitteen tai nimipalvelimen (domain) mukaan. Kehittyneemmällä ohjelmalla suodatusta voidaan tehdä tiedon sisällönanalyysin mukaan.

Sisällönsuodatus voidaan ostaa myös palveluna, joka korvaa erillisen sisällönsuodatus ohjelman. Sisällönsuodatusta käytetään esimerkiksi yrityksissä tuottavuuden nostamiseen ja tietoturvaan. Internetin käytön rajoittamisella pyritään yleensä varmistamaan henkilökunnan keskittyminen työntekoon ei-

kä internetissä surffailemiseen työajalla. Toinen käyttötarkoitus sisällön-suodattamisella on estää kielletyille tai haitallisille sivuille pääsy julkisissa käyttöympäristöissä. Yrityksissä voidaan käyttää suodattimia myös tietoturvasyistä. Web-sisältö uhat ovat nopeiten kasvava vaara tietokoneelle, koska selainliikenteen takia yritykset jättävät yleensä portit 80 (HTTP) ja 443 (HTTPS) avoimiksi palomuuereista. Internetselaimen käytön salliminen yrityksen verkon ulkopuolelle kohdistuvaan liikenteeseen tekee selaimesta turvallisuusriskin ja tämä vaatii sen huomioimista asianmukaisin menetelmin. [5.]

#### 4.1 Sisällönsuodatustekniikat

Sisällönsuodatusteknologiat sijaitsevat työaseman web-selaimen ja internet-yhteyden välissä estääkseen suodatukseen määriteltäviä sisältöjä näkymästä käyttäjälle. Yrityksessä suodatusratkaisu voidaan sijoittaa esimerkiksi internetin ja kytkimen tai reitittimen väliin, jolloin kyseistä suodatusta käytetään kaikkiin kytkimeen liitettyihin työasemiin ja laitteisiin tai reitittimen ohjaaman liikenteen suodattamiseen. Suodatettavan sisällön määrittelyyn käytetään sivuluokitusta, automaattista analyysiä ja ihmisen tekemää analyysiä. Internetin sisällöntuottajat voivat tehdä vapaaehtoisen sivun arviointiin vaikuttavan luokittelun verkkosivuilleen. Kaikki sisällöntuottajat eivät luokittele sivujaan, ja luokittelua voidaan käyttää myös tarkoituksenmukaisesti harhaanjohtavasti. Internetin sisällönsuodatukseen käytetään kahdenlaista tekniikkaa: estotekniikkaa ja sisällön analyysiä. Estotekniikoilla tarkoitetaan reititinyhdistelmiä ja porttiasetuksia, joilla tapahtuu tietoliikenteen estäminen tiettyihin IP-osoitteisiin ja portteihin. Tämä tekniikka on kuljetustasolla, eli layer 4-kerroksella tapahtuvaa suodatusta.

Sisällönanalyysiin perustuvat tekniikat kontrolloivat tietoon pääsyä sivujen sisällön, kuten tiettyjen avainsanojen esiintymisen perusteella. Sanojen esiintymistiheyttä sivulla voidaan mitata ja näille sanoille voidaan asettaa painoarvoja, joiden mukaan sivu arvioidaan. Tämä tekniikka on sovellustasolla, eli layer 7-kerroksella tapahtuvaa suodatusta. [6 s.13-14.]

Seuraavaksi käsitellään internetin sisällönsuodatuksen menetelmät.

#### *Sulkumenetelmä (exclusion filtering)*

Sulkumenetelmä perustuu osoitelistoihin ja sillä estetään käyttäjien pääsy yksittäisille sivuille tai nimipalvelimiin, jotka ovat mustalla listalla. Näitä listoja joudutaan päivittämään jatkuvasti, jotta tietokanta pysyy ajan tasalla.

#### *Sisällyttämismenetelmä (inclusion filtering)*

Sisällyttämismenetelmä edellyttää, että on olemassa lista web-sivuista, joilla käyttäjä pystyy vierailemaan ja vain nämä sivut ovat sallittuja. Menetelmä on hyvin rajoittunut ja sen käyttö soveltuu vain erityisiin käyttötarkoituksiin.

#### *Sisällön analyysi (content analysis)*

Sisällön analyysi-menetelmässä tietoa kontrolloidaan analysoimalla web-sivusta tai URL-osoitteesta tiettyjä avainsanoja ja niiden perusteella tehdään päätös päästetäänkö käyttäjä sivulle vai ei. Näiden avainsanojen lisäksi voidaan määritellä erilaisia kriteerejä ja sääntöjä, joiden mukaan estäminen sivulle tehdään. Ohjelmat perustuvat tekoälyyn ja pystyvät tulkitsemaan sivuilla esiintyviä kuvia ja tekstiä sekä tiedostojen formaatteja. [6 s.14-15.]

## **4.2 Layer 4 ja 7 -tason suodatus**

Internetin käyttäminen webselaimella on yleisesti sallittua palomuurien läpi, ja tästä syystä lähes kaikki ohjelmat tarjoavat mahdollisuuden tunneloida viestintä kuin se olisi web-liikennettä ja käyttävät porttia 80, mikä on varattu web-palvelinten käyttöön. Toiset ohjelmat tunneloivat datan viestinnän HTTP-protokollaan ja näkyvät samanlaisena liikenteenä kuin selaimella otettaisiin yhteyttä palvelimeen. Koska suuri osa internetliikenteestä käyttää web-liikenteen portteja ja näyttää web-liikenteeltä, layer 4-tason palomuri, minkä liikenteen suodatus perustuu vain TCP/IP-osoitteisiin ja portteihin, on riittämätön suoja internetin tarjoamia uhkia vastaan. Yhteyttä muodostettaessa ei voida luottaa vain lähteen IP-osoitteeseen, sallitaanko liikenne vai ei, koska lähes kaikkialla on käytössä palveluita identiteetin salaamiseksi, kuten Network Access Translation (NAT), Virtual Private Networks (VPN) ja tunnelointi. Tästä syystä myös viruksia, matoja ja muita haittaohjelmia levitetäes-

sä pystytään oikea lähdeosoite muuttamaan. Layer 4-tasolla toimiva palomuuuri ei pysty analysoimaan pakettien sisältöä. Tästä syystä nykyajan hyökkäykset tehdään ohjelmistotasolla, jota palomuuuri ei pysty estämään. [5.]

Layer 7-tason suodatus tapahtuu tutkimalla jokaisen TCP/IP-paketin oikea sisältö, eli analysoidaan liikenteen sisältöä. Layer 7-tason suodatusta on yleisesti tehty välityspalvelimilla tai ohjelmisto tason yhdyskäytävällä (application level gateway). Käyttäjän ja palvelimen välisessä yhteydessä välityspalvelin kuuntelee paketteja ja käyttäytyy käyttäjälle kuin se olisi suoraan yhteydessä palvelimeen ja palvelimelle kuin yhteys olisi suoraan käyttäjään. Välityspalvelin täten katkaisee yhteyden näiden kahden välillä ja se mahdollistaa, että voidaan tutkia jokaisen paketin sisältö niiden kulkiessa tämän kautta. Vain harva välityspalvelin kuitenkaan tarkistaa jokaisen paketin sisällön mahdollisilta hyökkäyksiltä. [5.]

Tärkeimmät ongelmakohdat layer 7-tason suodatuksessa ovat:

### 1. Nopeus

Jokaisen paketin porttinumero voidaan tarkistaa nopeasti, mutta kaiken datan analysointi, minkä paketti on kuljettanut, on suuri työ, ja se voi haitata ja hidastaa yhteyttä huomattavasti sekä kuormittaa palomuuria.

### 2. Protokollan analysointi

On mahdollista rajoittaa analysointia jolla voidaan varmistaa, että kuljetetun datan formaatti vastaa ohjelman sallittua HTTP-protokollaa. Tämä pakottaa ohjelmat käyttämään liikennöintiin vain porttia 80. Tämä ei kuitenkaan suojaa hyökkäyksiltä ohjelmia vastaan, mitkä käyttävät liikennöintiin HTTP-protokollaa.

### 3. Sisällönsuodatus

Koko sisällön analysoiminen olisi todellinen turvallisuusratkaisu, mutta sen toteuttaminen on lähes mahdotonta. Lähes mitä tahansa liikennettä voidaan

tunneloida HTTP:n kautta, mutta ongelmaksi tulee millä tavalla saadaan eroteltua hyvä sisältö huonosta. Jos tarkastellaan esimerkiksi Skype-liikennettä, mikä on salattu päästä päähän -menetelmällä ja voidaan tunneloida HTTPS (HTTP-protokollan salattu versio, portti 443) -liikenteeksi. On melko vaikeaa kieltää vain Skype-liikennettä ja sallia kaikki muu HTTPS-protokollaa käyttävä liikenne. Koko sisällön analysoinnin sijasta voidaan suorittaa sisällön-suodatusta, mikä tarkoittaa että suodatetaan pois liikenne, minkä joko tiedetään olevan ”huonoa”, se on epäilyttävää tai ei standardin mukaista. Tämä vaatii silti, että koko paketin sisältö analysoidaan, mutta siitä etsitään vain jo tunnettuja hyökkäysuhkia tai uusia malleja. [5.]

## 5 KOMPRESSOINTI

Kompressointi on menetelmä, joka pienentää tiedon kokoa muuttamalla sen muotoon, mikä tarvitsee vähemmän bittijä. Yleisimmin kompressointia eli tiedon pakkaamista käytetään tallennustilan minimoimiseksi esimerkiksi tietokoneen kiintolevyllä tai vähentämään kuljetettavaa dataa verkon ylitse. Vähentämällä kuljetettavan datan kokoa saavutetaan enemmän kaistanleveyttä käytettäväksi ja siirtoajat lyhenevät. Blue Coatin kompressointitekniikat on suunniteltu parantamaan kaistankäyttöä ja vähentämään kuljetettavan datan määrää verkossa. Kompressointitekniikka käyttää algoritmeja, joilla poistetaan ylimääräistä tietoa ja hyödynnetään toistuvaa tietoa. Kun kompressointi on käytössä, esitetään alkuperäinen tieto tiiviimmässä ja tehokkaammassa muodossa. Tämä pakattu data voidaan lähettää verkon ylitse ja päästessään määränpäähän se puretaan algoritmeilla alkuperäiseen muotoonsa mikä se oli ennen kompressointia. Blue Coat ProxySG -laitteissa käytetään standardeja gzip ja deflate -algoritmeja tiedon pakkaamiseen. Laitteet tukevat käyttöjärjestelmästä riippuen kahdenlaisia kompressointimetodeja: HTTP-kompressointia ja ADN-kompressointia.

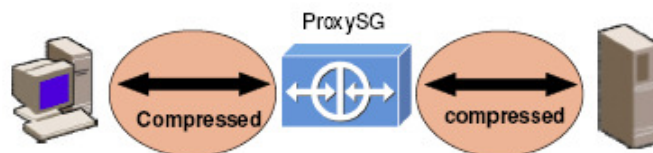
### HTTP-kompressointi

HTTP-kompressointi Blue Coat ProxySG-laitteissa on täysin yhteensopiva HTTP 1.1 -standardin kanssa. ProxySG pystyy noutamaan kompressoitua sisältöä alkuperäiseltä web-palvelimelta ja tarjoilemaan sen kompressoituna sisältönä asiakkaille, jotka tukevat kompressointialgoritmejä tai purkavat pakatun sisällön ennen kuin lähettää sen muille asiakkaille. Laitteet pystyvät taltioimaan sisältöä pakatussa muodossa ja puretussa muodossa. Taltioitujen objektien pakkausta ja purkamista määritellään politiikoilla. Politiikoilla määritetään miten kaistaa käytetään ja halutaanko menetelmällä nopeuttaa käyttäjien vai palvelimien käyttämää kaistanleveyttä. Blue Coatin mukaan kompressoinnilla saavutetaan 30 % - 40 % säästöä kaistan käytössä. Ylempi kuva 5 havainnollistaa liikennöintiä, kun käytössä ei ole kompressointia välityspalvelimessa. [7.]



Kuva 5. Kompressoimaton liikenne [7.]

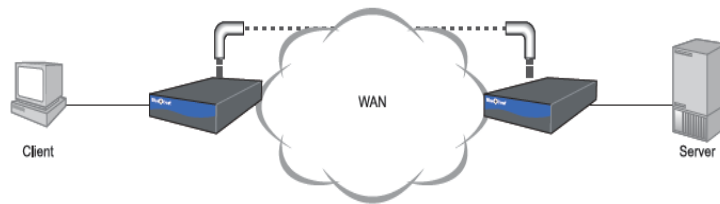
Käytettäessä kompressointia sama sisältö voidaan kuljettaa verkon ylitse pakattuna datana, jolloin saman tiedon siirtämiseen käytetään vähemmän kaistanleveyttä. Kompressoitun dataliikenteen siirtyminen on kuvattu kuvassa 6.



Kuva 6. Kompressoitu liikenne [7.]

### *ADN-kompressointi*

Application Delivery Network (ADN) -ominaisuus mahdollistaa tiedon kompressoimisen ja lähettämisen ADN-tunnelia pitkin WAN:n eri puolilla sijaitsevien ProxySG-laitteiden välillä. Tämä sisältökytkentä vaatii, että käytössä on vähintään kaksi ProxySG-laitetta, ja ne on sijoitettu eri puolille WAN:ia ja ovat saman ADN-verkon jäseniä. Laitteen, joka sijaitsee lähimpänä palvelimia, tulee myös mainostaa reitiryksiä palvelimille, jotta WAN:in toisella puolella olevalla laitteella on pääsy niihin. ProxySG voidaan myös sijoittaa suoraan linjalle mahdollistaen läpinäkyvät ADN-tunnelit. Tämä liikenne käyttäjien ja palvelimien välillä on automaattisesti kompressoitua ennen datan lähettämistä, jotta kaistan käyttö on pienempää ja latausajat loppukäyttäjille pienemmät. ADN-kompressointia käytetään useimmiten sisällön bittien varastoimisen (Byte Caching) kanssa, jolloin päästään optimaalisiin tuloksiin. Ensin suoritetaan bittien varastoiminen ja siitä saatu data pakataan kompressoimalla se. Molemmat toiminnot ovat oletusasetuksina käytössä ADN-liikenteen optimoimisessa. [8.]

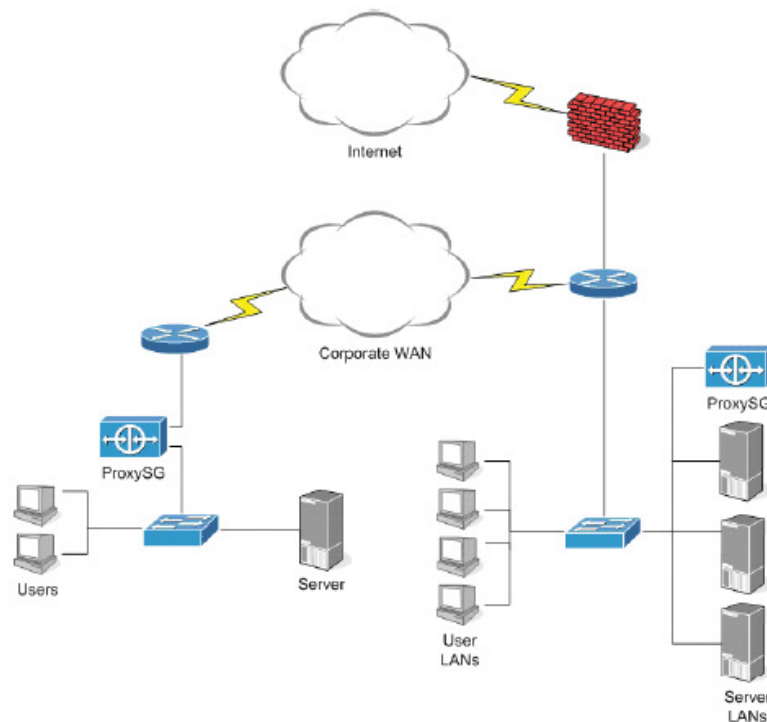


*Kuva 7. ADN-tunneli asiakkaan ja palvelimen välissä [8.]*

Etätoimistoista voidaan ADN-ominaisuuden avulla luoda päätoimipisteen palvelimiin etäyhteys ja käyttää niitä myös etätoimiston palvelimina. Tällä ratkaisulla voidaan vähentää huomattavasti IT-kuluja ja vähentää tarvetta paikanpäällä hoidettaville huolto- ja päivitystöille. Päätoimipisteen ProxySG sijoitetaan mahdollisimman lähelle palvelinverkkoja, ja se toimii ADN-managerina etätoimiston ProxySG-laitteelle mikä sijoitetaan suoraan yhteyden väliin linjalle, jolloin sillä suodatetaan myös liikennettä sisältökytkennän lisäksi verkkoon ja verkosta pois päin.

Kuvassa 8 on esitetty ADN-kytkentä verkkojen välillä ja verkkoon liitetyt laitteet. Päätoimipisteessä sijaitsevat reitittimen takana kytkin, mihin on liitetty työsemille tarkoitetut lähiverkot ja palvelimien verkot. ProxySG-laite on liitetty

verkkoon ja sen kautta liikenne kulkee palvelimille. Etätoimisto on resursseiltaan pienempi ja siellä on lähiverkossa käyttäjiä, palvelin ja ProxySG-laite. Näiden ProxySG-laitteiden välillä muodostuu ADN-sisältökytkentä ja tiedon siirto ja nopea palvelimien käyttäminen onnistuu myös etätoimiston verkossa.



Kuva 8. ADN-verkon laitteet [lähdettä 9 mukailen.]

## 6 BLUE COAT -LAITTEET

Blue Coat tarjoaa erilaisia ratkaisuja yritysten tarpeisiin ja laitteet kuvataan tuoteperheinä, jotka tarjoavat IT-alan yrityksille vaihtoehtoisen ratkaisun turvalliseen web-kommunikointiin ja yrityksen tärkeiden ohjelmien nopeaan käyttämiseen. Laitteet ovat niiden käyttötarkoituksen mukaan luokiteltu omiin laiteryhmiin.

Blue Coat tuoteperheet ovat lueteltu seuraavana:

- Blue Coat ProxySG
- Blue Coat Packet Shaper
- Blue Coat ProxyRA
- Blue Coat ProxyAV



- Blue Coat Web Filter
- Blue Coat Reporter
- Blue Coat Director
- Blue Coat ProxyClient [10.]

Tässä työssä käsitellään Blue Coat ProxySG -laitteita, niiden ominaisuuksia ja suoritetaan laitteiden käyttöönotto testiympäristössä.

### *Blue Coat ProxySG -laitteet*

Blue Coat ProxySG -laiteryhmä tarjoaa skaalautuvan välityspalvelin alustan web-liikenteeseen sekä yritysohjelmien kiihdytyksen ja kompressointimenetelmän. ProxySG on rakennettu objekti-pohjaiselle käyttöjärjestelmälle mikä hyödyntää jo olemassa olevia autentikointi tapoja tarjoten joustavan määritteiden ja sääntöjen toimeenpanon koskien sisältöä, käyttäjiä, ohjelmia ja protokollia. Laitteilla voidaan suorittaa web-liikenteen sisällönsuodatusta, estää vakoiluohjelmia ja haittaohjelmia leviämistä verkkoon, skannata viruksia ja valvoa verkkoliikennettä. Blue Coat ProxySG -laitteet on suunniteltu yhden välityspalvelimen arkkitehtuuria noudattamalla, missä yksi välityspalvelin käsittelee eri välityspalvelinten vaatimukset yrityksen verkossa. Työssä käytetään ProxySG-tuoteperheen laitteista ProxySG200-C- ja ProxySG400-1- laitteita, joiden tekniset tiedot löytyvät liitteestä 6. Työssä käytetään käyttöjärjestelmänä ProxySG200-laitteen mukana tullutta versiota SGOS 5.3.2.1, joka tukee sisällönsuodatus- ja kompressointimenetelmiä. Menetelmien käyttöönoton käsitellään tarkemmin ProxySG200-laitteelle seuraavassa luvussa internetliikenteen käsittelyyn. SGOS 5.3.2.1 tukee myös ADN-sisältökytkentää ja tämä versio on myös käytössä luvussa 8 tehtävässä laitteiden välisessä sisältökytkennässä. [11.]

Blue Coat ProxySG -laitteet soveltuvat ominaisuuksiltaan eri tarkoituksiin ja niitä on tarjolla etätoimiston pienistä ja vähemmälle käyttäjämäärälle suunnatuista laitteista aina datakeskuksen ydinverkkoon, missä käyttäjiä on todella paljon ja laitteiston suorituskykyä vaaditaan paljon. Kuvassa 9 on ProxySG-laitteiden käyttötarkoituksen mukainen esitys.



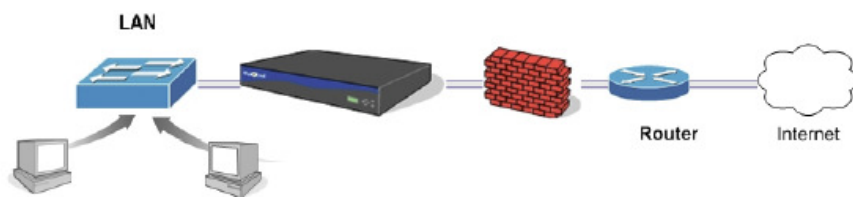
Kuva 9. Blue Coat ProxySG- tuoteperheen laitteiston valinta riippuu käyttötarkoituksesta ja käyttäjämäärästä. [11.]

## 7 PROXYSG 200: SISÄLLÖNSUODATUS JA HTTP-KOMPRESSIO

Verkon optimoinnin ja hallinnan takia verkon ja internetin väliin asennetaan Blue Coat ProxySG200 toimimaan välityspalvelimena ja hallintalaitteena. Tämä mahdollistaa liikenteen hallinnoimisen ja suorituskyvyn parantamisen käyttöympäristössä. Työssä ProxySG200-laitteelta haetaan määritetyille käyttäjäryhmälle kohdistuvaa kaistanhallintaa, internetliikenteen sisällönsuodatusta ja käyttäjien pääsyn rajoittamista ei-toivotuille sivustoille. Tässä luvussa käytetään yhtä Blue Coat ProxySG200-laitetta. Laite toimii välityspalvelimena käyttäjäryhmälle ja karsii internetliikenteestä HTTP-protokollaa hyödyntävää ei toivottua liikennettä sekä suodattaa dataliikennettä, mikä on suunnattu porttia 80 käyttäväksi liikenteeksi. Laite tukee HTTP-liikenteen kuuntelemisen lisäksi seuraavia protokollia: CIFS:iä, FTP:tä, IM:ää, MAPI:a, Shell:iä, SOCKS:ia, SSL:ää ja Streamingiä. HTTP Proxyn pääasiallinen käyttökohde on web-liikenteen kontrolloiminen tarjoten turvallisuutta, autentikointia, virusturvaa ja suorituskykyä. Seuraavaksi käsitellään laitteen asennus verkkoon ja laitteella HTTP-liikenteen suodatusratkaisu sekä verkon optimointia.

## 7.1 Käyttöönotto ja käyttöjärjestelmä

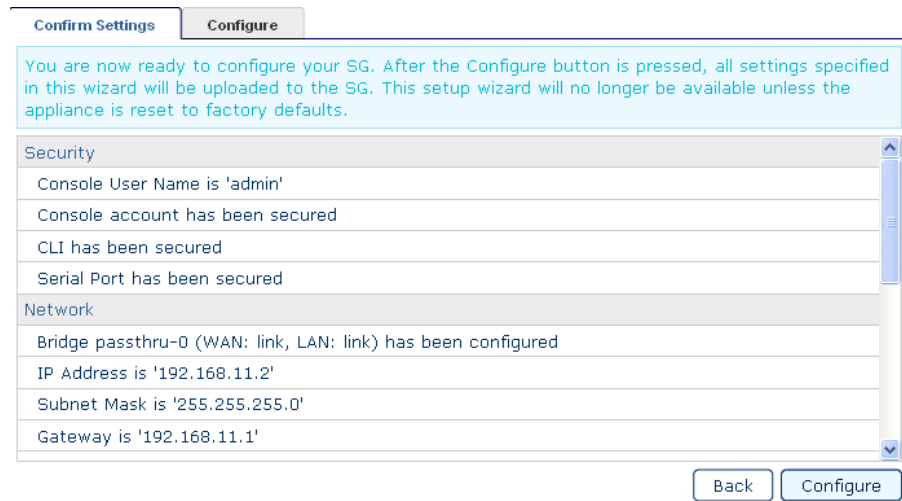
Blue Coat ProxySG200 sijoitetaan verkkoon reitittimen ja kytkimen väliin siltaamaan liikennettä, jolloin laite on fyysisesti linjalla laitteiden yhteyden välissä tai virtuaalisesti linjalle, jolloin laite kytketään LAN-portista reitittimeen ja hyödynnetään WCCP (Web Cache Communication Protocol) -ominaisuutta. Laite näkyy läpinäkyvänä välityspalvelimena, jonka kautta liikennettä ohjataan reitittimellä. Tässä työssä laite kytketään suoraan linjalle siltaamaan liikenteen internetin ja lähiverkon välistä jolloin liikenteen kuunteleminen ja rajoittaminen mahdollistuu.



Kuva 10. ProxySG-laitteen sijoitus verkkoon [12, s.25.]

Asennus aloitetaan laitteen alkuasennuksella. Tämä on mahdollista suorittaa kolmella eri tavalla, ja tässä työssä käytetään laitteen alkuasetuksien määrittämiseen selainta. Vaihtoehtoisina menetelminä olisi kytkemällä sarjakaapeli suoraan laitteeseen ja konfiguroimalla terminaalipäätteellä asetukset tai etäasennus verkon ylitse. Alkuasennuksessa määritellään laitteelle tunnus ja salasana käyttöjärjestelmää varten, sekä tekstipohjaisen (CLI) terminaalin ja sarjaportin salasanat. Seuraavaksi syötetään verkonparametrit, kuten IP-osoite, aliverkon maski, oletusyhdykskäytävä ja DNS-palvelimen ip-osoite. Käytettäessä useampaa ProxySG-laitetta voidaan konfiguroida Application Delivery Network (ADN) -ominaisuus molempiin ProxySG-laitteisiin, jolloin näiden laitteiden välille syntyy sisältökytkentä optimoimaan verkkoliikennettä. ADN-sisältökytkentä käsitellään kappaleessa 8 eikä sitä käytetä tämän luvun konfiguraatioissa. Asennuksen yhteydessä valitaan mitä liikennettä halutaan tutkia ja optimoida sekä oletusasetus liikenteen kieltämisestä tai sallimisesta. Valitaan kuunneltaviksi protokolliksi CIF, FTP ja HTTP. Työssä optimoidaan vain HTTP-liikennettä ja tutkitaan kaikki liikenne mikä käyttää HTTP-protokollaa liikennöintiin. Oletukseksi valitaan kaiken liikenteen salliminen, mikä tarkoittaa sitä, että jos liikennettä halutaan rajoittaa, on se teh-

tävä politiikoilla ja säännöillä erikseen. Blue Coat ProxySG200 sijoitetaan lähiverkkoon 192.168.11.0 /24 kuvan 11 mukaisilla asetuksilla.



Confirm Settings | **Configure**

You are now ready to configure your SG. After the Configure button is pressed, all settings specified in this wizard will be uploaded to the SG. This setup wizard will no longer be available unless the appliance is reset to factory defaults.

| Security                         |
|----------------------------------|
| Console User Name is 'admin'     |
| Console account has been secured |
| CLI has been secured             |
| Serial Port has been secured     |

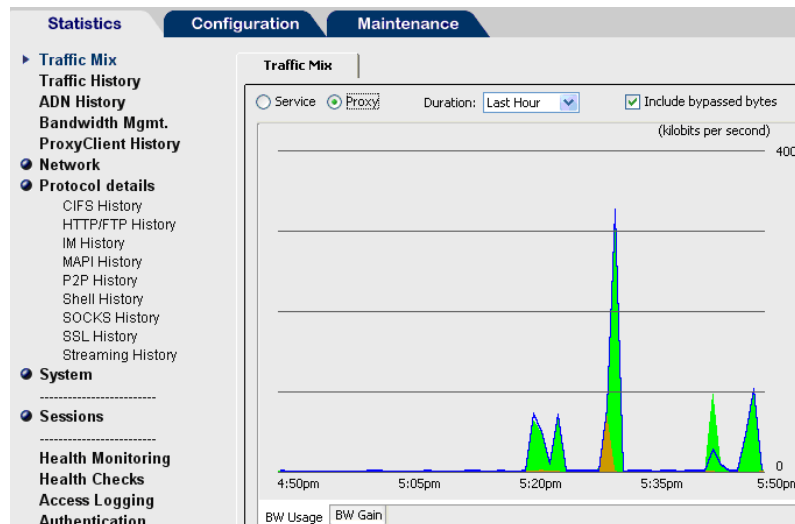
| Network  |
|--|
| Bridge passthru-0 (WAN: link, LAN: link) has been configured |
| IP Address is '192.168.11.2'                                 |
| Subnet Mask is '255.255.255.0'                               |
| Gateway is '192.168.11.1'                                    |

Back | Configure

Kuva 11. ProxySG-laitteen alkuasetukset

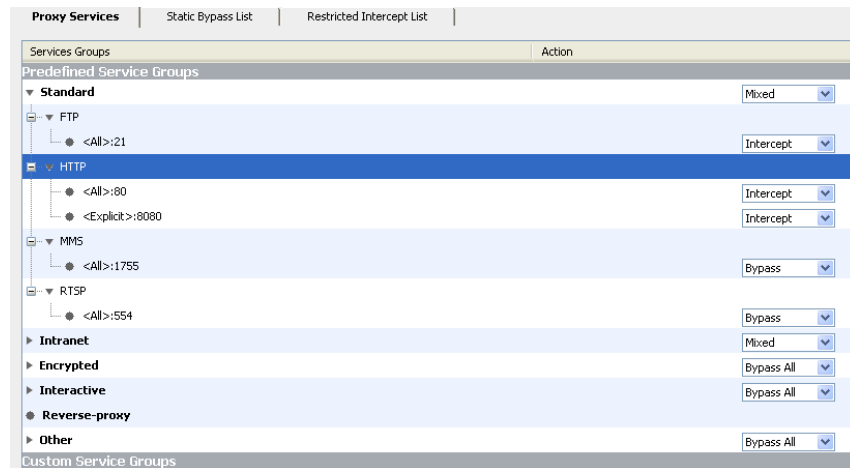
Alkuasetusten jälkeen otetaan selaimella yhteys laitteen käyttöjärjestelmään syöttämällä selaimen laitteelle alkuasetusten yhteydessä annettu IP-osoite: 192.168.11.2 ja portin numeroksi 8082.

Sisäänkirjautumisen jälkeen aukeaa selaimen etusivu, mikä sisältää laitteesta kuvan, mallin sekä käytettävän käyttöjärjestelmän tiedot. Sivulta löytyy valikko, josta päästään tarkastelemaan laitteen tietoja ja asettamaan laitteelle erilaisia toimintoja, asetuksia ja seuraamaan verkkoliikennettä. Valitsemalla Management Console -valinta aukeaa laitteen käyttöjärjestelmä. Käyttöjärjestelmästä löytyy kolme välilehteä. Ensimmäinen välilehti on Statistical, ja se tarjoaa useita tilastien seurantamahdollisuuksia mukaan lukien yksittäisten protokollien liikenteen tarkkailemisen. Toinen välilehti on Configuration, joka sisältää laitteen asetukset ja määritelmät, millä tavalla liikennettä tutkitaan ja suodatetaan sekä käytetäänkö sisällönsuodatukseen valmiita suodatusratkaisuja. Kolmas välilehti Maintenance sisältää laitteen laitekoonpanon tiedot, päivitysominaisuuksia, lisenssin hakuominaisuuksia, laitteen toiminnan seurannan ja lokitietoja. Laitteelle haetaan käyttöönnoton yhteydessä voimassa oleva lisenssi automaattisella haku ominaisuudella tai manuaalisesti, jonka jälkeen laitteelle asetetaan välityspalvelimen ominaisuudet toimimaan.



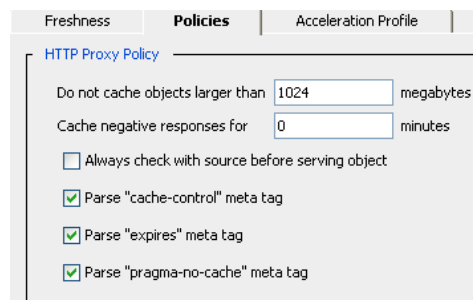
Kuva 12. SGOS-käyttäjärjestelmän etusivu

Välityspalvelimen ominaisuudet ProxySG-laitteilla antavat käyttömukavuutta ja tehokkuutta, koska useiden käyttäjien hakiessa samoja tietoja samasta osoitteesta pystyy laite taltioimaan näitä tietoja kiintolevyllä hakematta niitä joka kerta erikseen sivun alkuperäisestä osoitteesta ja näin ollen vähentää verkon käyttökapasiteettia ja nopeuttaa latausaikoja. Välityspalvelin ominaisuuksissa voidaan määritellä portteja ja osoitteita mistä ProxySG kuuntelee tulevia pyyntöjä ja tekee määriteltäviä ratkaisuja sääntöjen ja politiikoiden mukaan. Oletuksena laitteella on kaksi HTTP-palvelu kuuntelijaa, toinen kaikille IP-osoitteille kuuntelemassa läpinäkyvästi porttia 80 ja toinen määriteltä kuuntelija portille 8080. Valintoja liittyen protokoliin ja käytettäviin portteihin on mahdollista muokata määriteltujen tarpeiden mukaisiksi sekä lisätä myös jälkikäteen protokollia kuunneltavien listalle. Valintojen muokkaaminen voidaan suorittaa Configuration välilehdeltä valitsemalla Services valikosta proxy services.



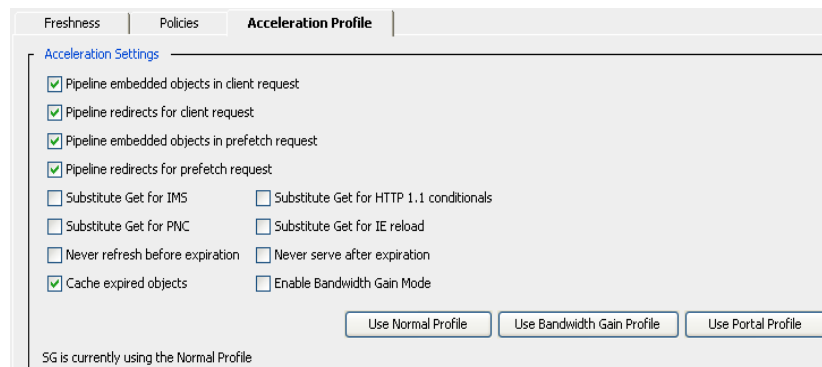
Kuva 13. Välityspalvelimen asetusten valinta ikkuna

Määritetään välityspalvelimelle asetukset valitsemalla välilehdeltä Configuration kohdasta Proxy Settings valinta HTTP Proxy, mistä voidaan määrittää välityspalvelimen toimintamalli ja tapa miten se käsittelee pyyntöjä ja mitä sisältöä taltioidaan ja mitä ei. Työssä käytetään oletusasetuksia politiikoiden määrittelyssä. Välityspalvelin ei varastoi tiedostoja, minkä koko on enemmän kuin 1024 bittiä sekä noudattaa haluttuja valintoja.



Kuva 14. HTTP Proxyn asetukset

Acceleration Profile välilehdeltä voidaan valita millä tavalla proxy toimii ja mitä profiilia käytetään. Valittavina ovat Normal Profile, Portal Profile ja Bandwith Gain Profile. Työssä käytetään valintana normaalia profiilia, koska se on oletus profiili ja käytettävissä tilanteissa kun, ProxySG on käytössä tavallisena eteenpäin välittävänä välityspalvelimena. Tämä valinta on tyypillisesti käytössä ympäristöissä missä objektien tuoreus on tärkeämpää kuin palvelin puolen kaistanleveyden hallitseminen. Valinta tukee HTTP-standardeja ottaen huomioon objektien uudistamisen ja toimivuuden. Profiilissa on lisätty tiedonsiirto toimintoja (pipeline) , jotka vähentävät käyttäjien latausaikoja.



Kuva 15. Tiedonsiirron käsittelyominaisuudet

Välityspalvelin asetukset ovat nyt laitteen osalta kunnossa. Seuraavaksi käsitellään sisällönsuodatusratkaisuja.

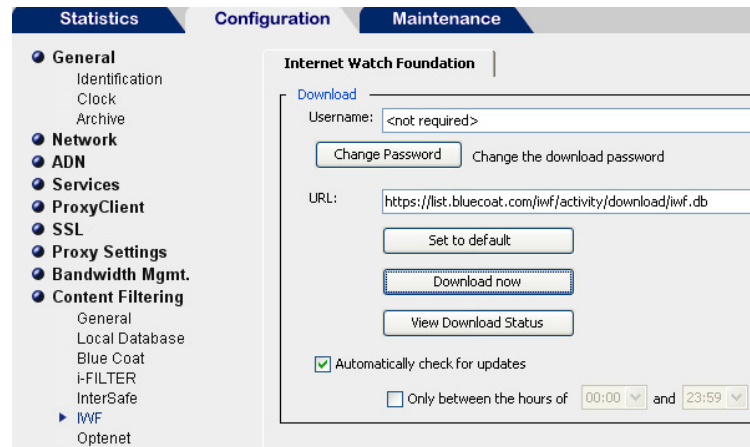
## 7.2 Sisällönsuodatus

BlueCoat ProxySG200 tarjoaa sisällönsuodatuksen useita vaihtoehtoja. Valittavana ovat Blue Coatin oman Web Filter ratkaisun lisäksi seuraavat kolmannen osapuolen tarjoamat lisenssin vaativat ratkaisut i-Filter, InterSafe, Optonet, Proventia, SmartFilter, SurfControl, Websense ja Webwasher. Laitte tukee myös Internet Watch Foundationin tarjoamaa ilmaista suodatusratkaisua. Työssä käytetään suodatuksen Internet Watch Foundationin tarjoamaa suodatusratkaisua, mikä sisältää estolistan haitalliseksi havaituista osoitteista.

Internet Watch Foundation (IWF) on ei-valtiollinen säätiö mikä perustaa toimintansa hyväntekeväisyyteen. Sen kotipaikka on Iso-Britannia, ja se tarjoaa julkisia online-palveluita joihin IT- ammattilaiset ilmoittavat internetin sisällöstä, mikä on mahdollisesti laitonta. IWF suodattaa sisältöä, joka käsittää lapsen seksuaalista hyväksikäyttöä maailmanlaajuisesti ja rikosoikeudellisesta ja epäsiiveellisestä sisällöstä rotuvihan yllyttämään sisältöön Isossa Britanniassa. Lisätietoja IWF:stä on saatavissa osoitteesta <http://www.iwf.org.uk>.

Suodatuslistan ottaminen käyttöön tehdään valitsemalla Content Filtering-kohdasta valinta General, josta valitaan ruksilla IWF:n suodatus päälle. Seuraavaksi valitaan Content Filtering ja IWF-valinta ja ladataan oletusosoitteesta laitteelle tietokanta Download-painikkeella, kuten kuvassa 16 on havain-

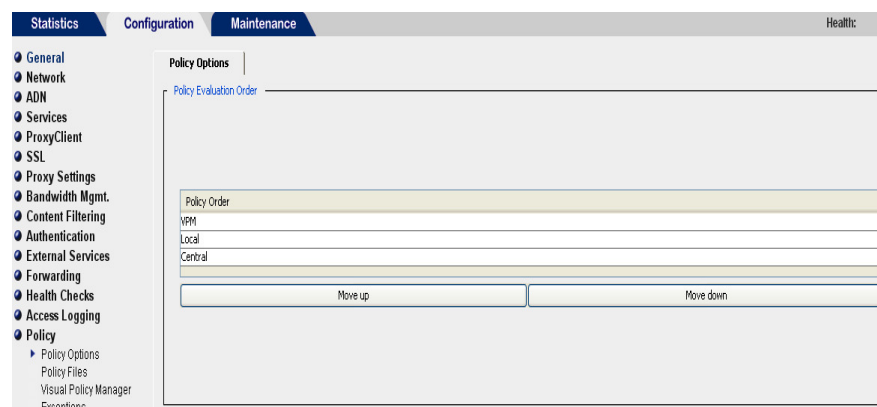
nollistettu. Kun lautus on suoritettu onnistuneesti loppuun, on tietokanta latautunut kiintolevylle ja on valmiina käytettäväksi osana suodatusratkaisua.



Kuva 16. IWF sisällönsuodatuksen käyttöönottoaminen ja tietokannan lataaminen osoitteesta <https://list.bluecoat.com/iwf/activity/download/iwf.db>.

### 7.3 Politiikat

Seuraavaksi käsitellään laitteeseen määriteltäviä politiikoita ja niiden järjestyksen vaikutusta. Laitteen käyttöjärjestelmästä valitaan Configuraton, Policy, minkä alapuolelta löytyy neljä valintaa: Policy Options, Policy Files, Visual Policy Manager sekä Exeptions. Politiikoita määritettäessä ensin määritetään politiikoiden arvojärjestys Policy Options-kohdasta, jossa valittavana ovat VPM (Visual Policy Manager), Local (lokaali tiedosto) ja Central (yleinen tiedosto). Valinta tapahtuu siirtämällä ylös- tai alaspäin valittua politiikkaa niin, että viimeisenä listassa oleva politiikka on tärkein ja ohittaa muissa politiikoissa määritetyt säännöt.



Kuva 17. Politiikkatiedostojen arvojärjestys



Sääntöjä hallitaan neljän politiikka tiedoston avulla ja nämä tiedostot ovat:

#### *Central Policy File*

Central Policy File sisältää globaalit asetukset suorituskyvyn ja toiminnan lisäämiseksi. Central Policy File sisältää myös suodattimet haitallisia viruksia vastaan, kuten Code Red ja Nimda. Code Red oli tietokoneelle suunnattu matovirus, joka hyökkäsi Microsoft IIS Web-palvelinta käyttäviin työasemiin heinäkuussa 2001. Nimda taas oli vastaavasti nopeasti leviävä matovirus joka löydettiin syyskuussa 2001 ja sen kohteina olivat Windows-työasemat ja palvelimet. Central Policy -tiedostoa hallitsee yleensä Blue Coat, vaikka tämän tiedoston tilalle on mahdollista osoittaa laitteelle kustomoitu Central Policy -tiedosto alkuperäisen tilalle.

#### *Forward Policy File*

Forward Policy File -tiedostoa käytetään täydentämään jo aikaisemmin luotuja toisia kolmea politiikkaa. Tämä politiikka tiedosto sisältää huolintasäannot, kun järjestelmää päivitetään uudempaan versioon.

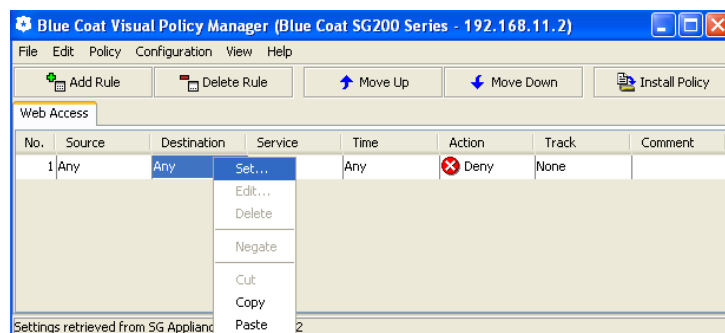
#### *Local Policy File*

Local Policy File on tiedosto, jonka laitteen ylläpitäjä luo itse. Kun VPM ei käytetä päätyökaluna politiikkojen määrittämiseen, niin lokaali tiedosto sisältää suurimman osan järjestelmän politiikka säännöistä. Jos VPM on päätyökalu politiikoiden luomiseen, niin tämä lokaali tiedosto on joko tyhjä tai sisältää jotakin laajennettuja politiikka ominaisuuksia, jotka eivät ole käytettävissä VPM:lla.

#### *Visual Policy Manager*

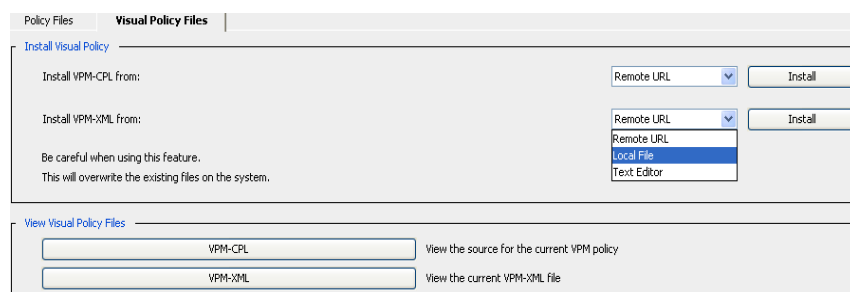
Visual Policy Manager, eli VPM, on graafisesti toteutettu politiikka editori joka sisältyy Proxy SG-laitteisiin. Politiikoilla ja säännöillä, joita luodaan tämän ohjelman avulla, voidaan tukea muita politiikoita tai ylittää niitä. Tällä ohjelmalla määritetään pääsyylistoja sekä kontrolloidaan politiikoita ja sääntöjä ilman, että käyttäjän tarvitsee tuntea syvällisemmin Blue Coat Content Policy Languagea (CPL), eikä käyttäjän tarvitsee manuaalisesti editoida politiikoita. Tässä työssä toteutetaan Visual Policy Managerilla HTTP-liikenteen optimointia ja politiikoiden luominen tietyin määrittein. Ohjelma käynnistetään valitsemalla Configuration, Policy, Visual Policy Manager ja painamalla

Launch-painikkeesta. Työpöydälle aukeaa Java-pohjainen sovellus mihin eri tasojen ja sääntöjen luominen tehdään. Ensin luodaan Policy-valikosta haluttava taso, mikä tässä tapauksessa on Web Access, jonka jälkeen voidaan tehdä määritteet lähteestä (Source), kohteesta (Destination), palvelusta (Service), ajasta (Time), toimenpiteestä (Action) sekä siitä halutaanko suorittaa seuranta loki-tiedostoihin. Lisääminen tapahtuu painamalla hiiren oikeanpuoleista painiketta halutun kohdan päällä ja valitsemalla tarvittavat toimenpiteet. Sääntöjä voidaan luoda useita erilaisia, ja näistä ylempänä oleva sääntö ohittaa alempana olevan säännön.



Kuva 18. Sääntöjen lisääminen Visual Policy Managerilla

Valmiita politiikoita laitteeseen tuodaan valitsemalla Policy Files ja välilehti liittäväen politiikan mukaan. Välilehdeltä Policy Files tuodaan politiikoita lokaaliin tiedostoon, välittävään tiedostoon tai yleiseen tiedostoon. Välilehdellä Visual Policy Files voidaan tuoda Visual Policy Managerilla luotuja sääntöjä ja määritteitä ProxySG-laitteeseen. Exeptions valinnasta voidaan lisätä politiikoihin poikkeus-sääntöjä, joiden lisäys tapahtuu joko URL-osoitteesta, lokaalista tiedostosta tai luomalla sääntö tekstieditoria käyttämällä.

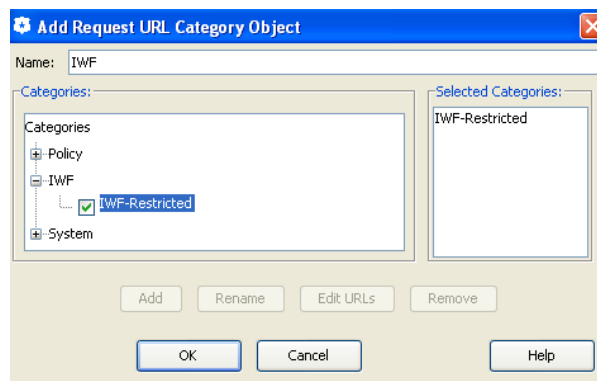


Kuva 19. VPM-tiedostojen tuonti

## 7.4 Sisällönsuodatuksen ja HTTP-kompression toteutus

Tämä luku käsittelee aikaisemmin käyttöön otetun ProxySG200-laitteen politiikoiden ja sääntöjen toteutuksen. Työssä käytetään aikaisemmin luvussa määriteltyjen välityspalvelimen ominaisuuksien lisäksi Internet Watch Foundationin (IWF) julkaisemaa suodatuslistaa haitallisista osoitteista ja haitallisesta sisällöstä. Estetään tietyille internetsivuille pääseminen kategoroidulla estolistalla sekä sallitaan osaan kielletyistä sivuista pääseminen öisin ja viikonloppuisin. HTTP-liikenteen optimoimiseksi kompressoidaan kaikki http-protokollaa käyttävä liikenne.

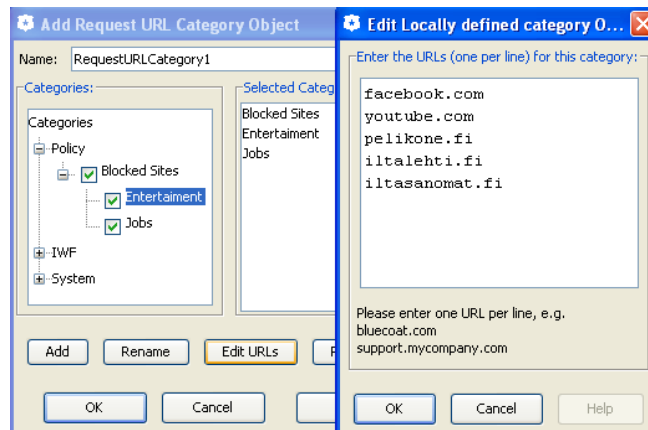
IWF-sisällönsuodatus otetaan käyttöön lisäämällä Web Access-tasolle uusi sääntö ja säännön kohteeseen valitaan URL-kategorian mukaan valinta. Valitaan kategorioista IWF-Restricted ja annetaan säännölle nimeksi IWF ja hyväksytään luotu sääntö. Nyt IWF-estolista on käytössä ja estää liikenteen mikä kohdistuu luvussa 7.2 ladatuntietokannan määrittelemiін sivustoihin.



Kuva 20. IWF-suodatuksen käyttöönotto

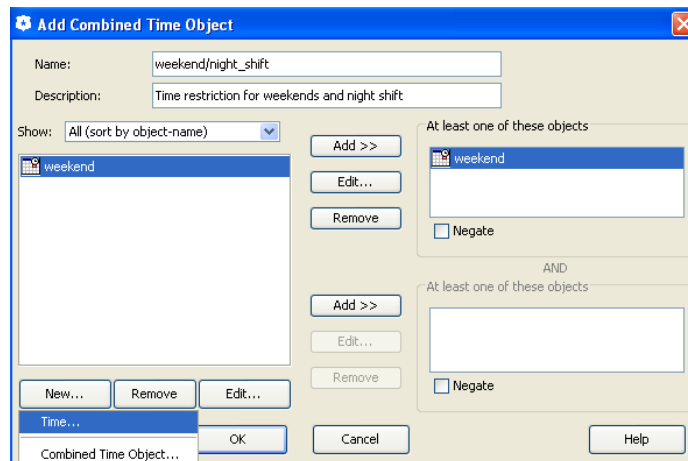
Seuraavaksi suoritetaan kategoroidun estolistan luominen lisäämällä uusi sääntö Web Access-tasolle ja valitaan kohteeseen (Destination) Request URL Category -valinta ja lisätään uusi kategoria, jolle annetaan nimeksi Blocked Sites. Lisätään tälle kategorialle alikategoria Entertainment ja Jobs. Entertainment kategoriaan lisätään URL-osoitteiksi osoitteet, jotka kielletään työaikana. Kieltämällä sivustoja tehostetaan työajankäyttöä ja vähennetään turhaa kaistankäyttöä verkkoliikenteestä. Työssä kielletyiksi sivuiksi ovat valittu kuvassa 21 olevat internetsivut. Vastaavasti Jobs-alikategoriaan tehdään lista kielletyistä osoitteista kuten [www.monster.com](http://www.monster.com) ja [www.hotjobs.com](http://www.hotjobs.com), joilla käyminen työaikana halutaan kieltää. Annetaan ka-

tegoria ryhmälle nimeksi BlockedSites ja hyväksytään kategoria. Lisätään säännön lähteeseen (Source) objekti Client IP/Subnet ja osoitteeksi 192.168.11.0 /24, mikä on lähiverkon osoiteavaruus. Lähiverkosta ei ole säännön hyväksymisen jälkeen mahdollista kirjautua kategorian mukaisille sivustoille.



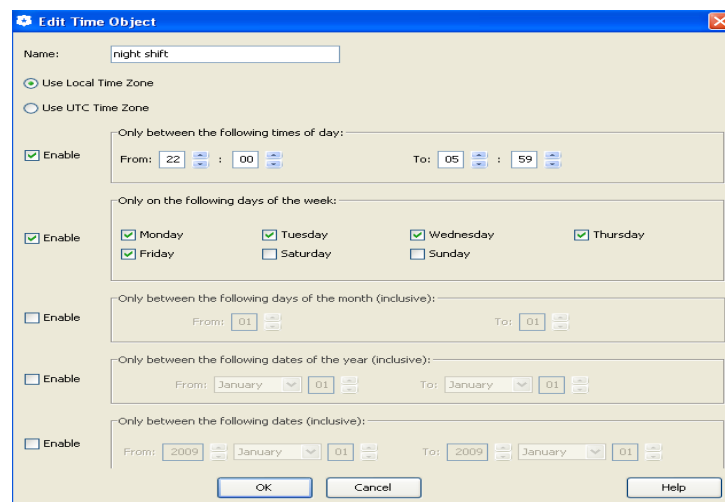
Kuva 21. Kiellettyjen sivujen lisääminen kategoriaan.

Öisin ja viikonloppuisin sallitaan kuitenkin osalle kielletyistä sivuista pääseminen, joten luodaan uusi sääntö, missä sallitaan aikaisemmin kielletyistä sivuista osaan pääsyn arkipäivinä öisin aikaan 22.00-06.00 sekä viikonloppuisin. Säännön luominen tapahtuu lisäämällä lähteeseen (Source) objekti Client IP / Subnet ja osoitteeksi 192.168.11.0 /24. Lisätään kohteeseen (Destination) uusi URL- kategoria ja nimetään Allowed Sites -nimiseksi ja annetaan kategoriaan lisättävälle objektille nimi AllowedSites. Tähän kategoriaan lisätään sivut ja osoitteet, joihin pääseminen sallitaan määritettyyn aikaan ja lopuksi hyväksytään kategoria. Käyttäjien pääsy Entertainment-kategoriassa estetyille sivustoille www.iltasanomat.fi ja www.iltalehti.fi sallitaan edellä määritettyihin aikoihin, joten luodaan aikamääritys säännölle valitsemalla aika (Time) kohtaan Combined Time Object -valinta ja lisäämällä tähän rajoitus arkipäiville ja viikonloppulle. Ensin luodaan sääntö-objekti, joka koskee vain viikonloppua. Säännön lisääminen näkyy kuvassa 22.



Kuva 22. Aika-objektin lisääminen viikonlopulle

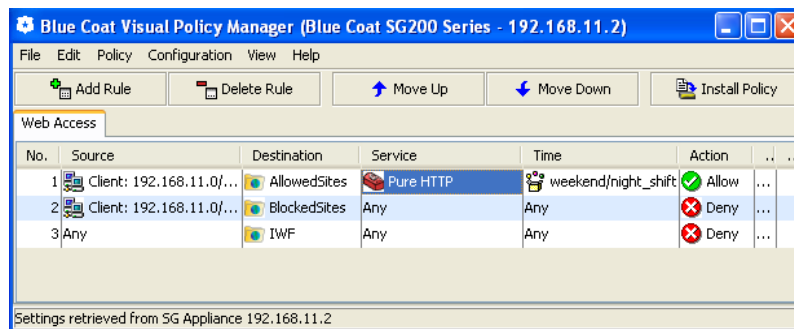
Seuraavaksi luodaan sääntö-objekti arkipäiville. Yhdistetyillä objekteilla voidaan luoda useita sääntöjä ja erilaisia yhdistettyjä määritteitä missä usean ehdon pitää toteutua, jotta rajoitus otetaan käyttöön. Aika-objekteissa määritykset tehdään ottamalla käyttöön halutut rajoitusvaihtoehdot ja valitsemalla tarkemmat määritteet niiden oikealta puolelta.



Kuva 23. Aikaobjektin määrittelyvaihtoehdot

Lisätään aikaobjekti yhdistettyyn objektiin ja hyväksytään yhdistetty objekti-sääntöön. Oletuksena säännön toiminto kohdassa on aina Deny-valinta, joka muutetaan tässä tapauksessa Allow-valinnaksi, jolloin säännön eri määritteet sallitaan säännössä määrätystä lähteestä valittuihin kohteisiin tiettyinä aikoina. Lisätään palvelukohdasta vielä säännölle käytettäväksi protokollaksi

HTTP ja vain puhdas HTTP-liikenne. Nyt luotu sääntö sallii Allowed Sites-kategorian sivuille pääsyn aikamääritteen mukaan ja vain pelkkänä puhtaan HTTP-liikenteenä. Koska sääntö numero 1 on ylempänä kuin sääntö numero 2, joka kieltää kyseisille sivuille pääsemisen ohittaa ylempänä numerolla 1 oleva sääntö sen ja mahdollistaa [www.iltasanomat.fi](http://www.iltasanomat.fi) ja [www.iltalehti.fi](http://www.iltalehti.fi) sivustoille kirjautumisen aikamääritteen mukaan.

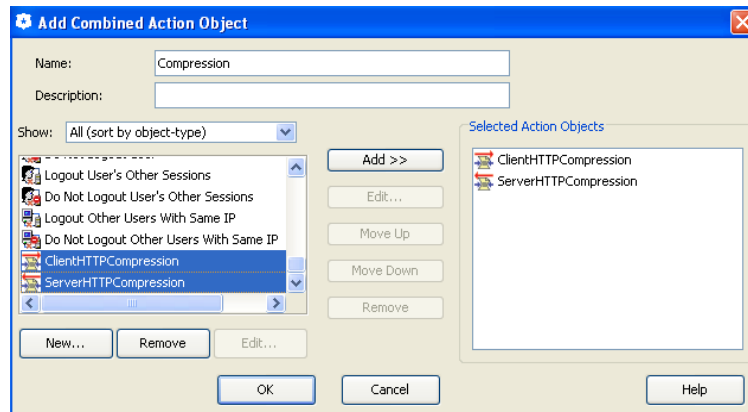


Kuva 24. VPM-säännöt

Säännöt sivustoille pääsemiseen ja estämiseen on luotu ja seuraavaksi halutaan suorittaa HTTP-liikenteen kompressoiminen, jolla säästetään kaistaa ja voidaan tarjota käyttäjille suoraan välityspalvelimella sijaitsevia tiedostoja joko pakatussa muodossa tai purettuna. Lisätään uusi Web Access layer-taso ja annetaan sille nimeksi Compression. Valitaan toiminto (action) -kohdasta hiiren oikeaa nappia painamalla set ja lisätään uusi toiminto-objekti. Valitaan objektiksi ClientHTTPCompression-valinta. Suoritetaan valinta käyttäjän hakiessa pakattua sisältöä, laitteelta löytyessä vain pakkaamatonta sisältöä pakkaa laite sisällön ennen kuin tarjoaa sitä käyttäjälle. Käyttäjän hakiessa pakkaamatonta sisältöä laitteen kiintolevyllä ollessa sisältö vain pakattuna, purkaa laite sen ennen käyttäjälle tarjoamista. Nimetään objekti ClientHTTPCompression nimiseksi ja hyväksytään objekti. Seuraavaksi lisätään uusi toiminto-objekti ja valitaan siihen ServerHTTPCompression-valinta. Valitaan, että pyynnöt suoritetaan aina käyttämällä HTTP-kompressiota ja sisällytetään valintaan myös ei-tuettujen muotojen pakkaaminen. Annetaan objektille nimeksi ServerHTTPCompression ja hyväksytään se.

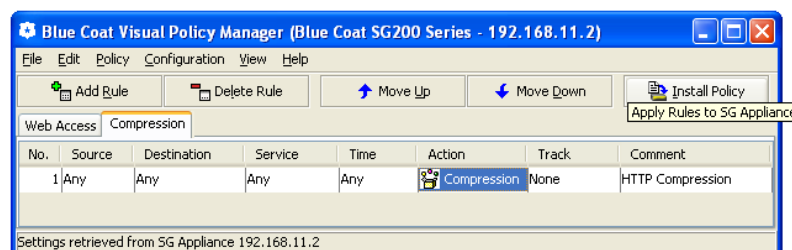
Edellä tehtyjen kompressointi objektien yhdistäminen yhdeksi toiminnoksi tapahtuu valitsemalla lisää toiminto objekti (Add Combined Action Object) ikkunasta uusi ja valitsemalla Combined Action Object -valinta ja valitsemalla

vasemmanpuoleisesta laatikosta aikaisemmin tehtyt ClientHTTPCompression ja ServerHTTPCompression -objektit ja lisäämällä ne yhdistettyyn objektiin painamalla add-painiketta. Annetaan yhdistetylle objektille nimeksi Compression ja hyväksymällä tämä objekti sääntöön.



Kuva 25. Yhdistettyjen sääntöjen luominen

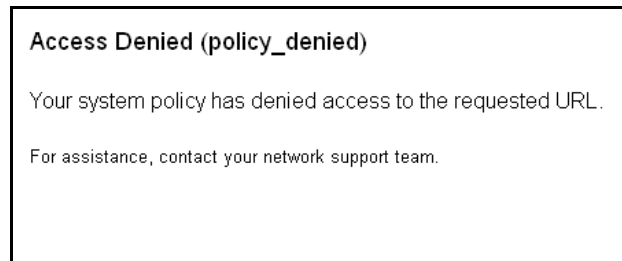
Kaikki tarvittavat sääntöjen määritykset on nyt toteutettu määritellyllä tavalla ja näiden sääntöjen käyttöönotto tapahtuu painamalla kuvassa 26 olevaa Install Policy -painiketta jolloin laite tallentaa politiikat VPM-tiedostoihin.



Kuva 26 Poliitikoiden hyväksyminen

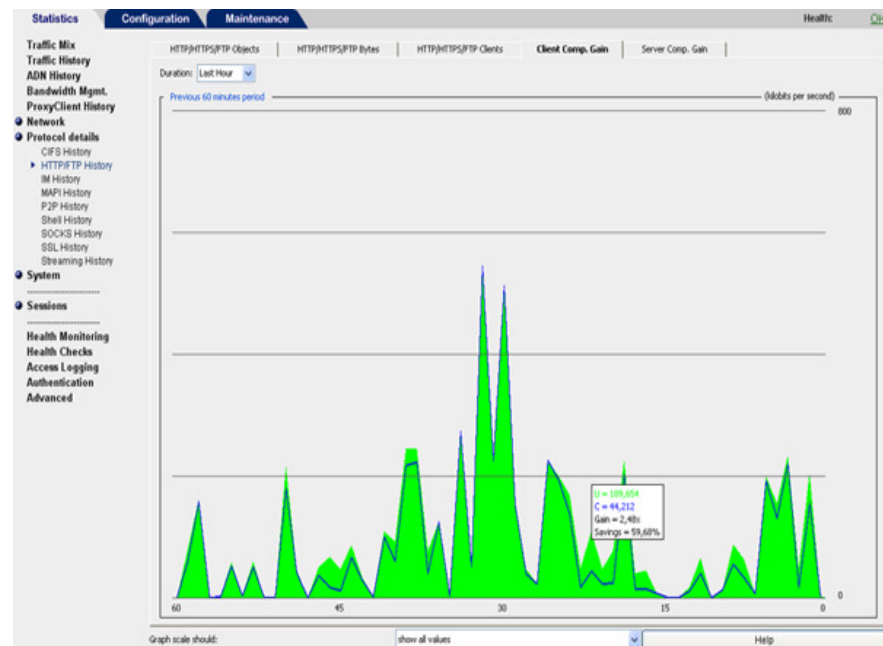
Sisällön suodatuksen ja kompression testaaminen suoritettiin selailemalla useilla eri internetsivustoilla useaan kertaan ja toistamalla samoille sivustoille menemistä. Tästä voitiin havaita, että ensimmäisen kerran sivustolle mentäessä lataus aika kesti pidempään kuin uudelleen samalle sivustolle mentäessä. ProxySG200 säilöä välityspalvelimen ominaisuuksillaan sisältöä laitteen kiintolevylle tehtyjen asetusten mukaisesti ja nopeuttaa sivustojen selailemistä, kun kohteena on toistuvasti samat sivustot ja sisältö. Tehtyjen politiikoiden takia sivustolle [www.youtube.com](http://www.youtube.com) pääsy ei onnistu mihinkään ai-

kaan vaan laite herjaa aina sinne yritettäessä kuvan 27 mukaisella tavalla. Saman herjan laite antoi myös yritettäessä muille kielletyille sivuille ja kategoriassa AllowedSites oleville sivuille muuhun aikaan kuin viikonloppuisin ja arkipäivisin kello 22.00 - 5.59 välisenä aikana.



Kuva 27. Kirjautuminen sivulle estetty

Kompression testaaminen suoritettiin selailemalla useita eri internet sivustoja useaan kertaan, jolloin voitiin ProxynSG:n käyttöjärjestelmästä seurata HTTP-protokollan liikennöinti historiaa ja havaittiin, miten kompressio oli liikennöintiin vaikuttanut ja minkä verran. Tämä ilmenee alla olevasta kuvasta 28, missä tarkastellaan käyttäjälle kompression aiheuttamaa kaistan säästöä. Kuvassa vihreällä on kaistantarve ja sinisellä viivalla siihen käytetty kapasiteetti.

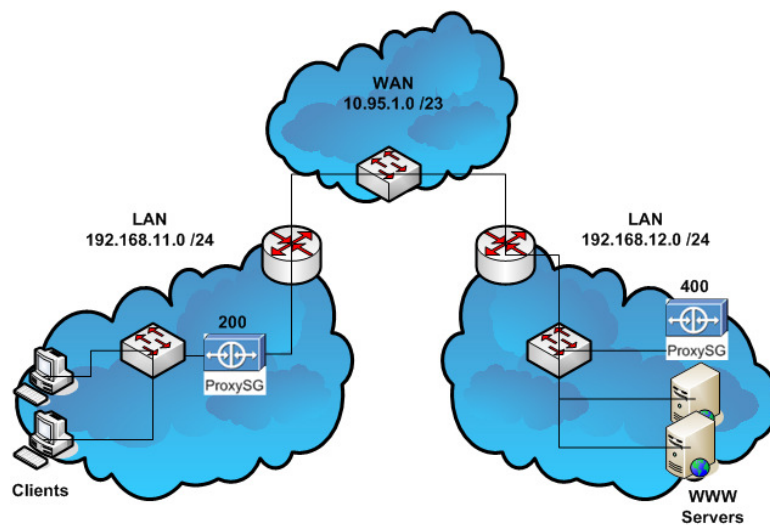


Kuva 28. Kompression statistiikasta voidaan seurata pakatun datan kaistankäyttöä ja kompression aiheuttamaa kaistansäästöä. Kuvassa nähdään, että kaistaan leveyttä on säästetty matalammilla verkkoliikenteen osilla.



## 8 PROXYSG: SISÄLTÖKYTKENTÄ

Tässä työn osassa tehdään Metropolia Ammattikorkeakoulun laboratoriotiloissa kahden verkon välille sisältökytkentä käyttäen Blue Coat ProxySG -laiteryhmän ProxySG200 ja ProxySG400 -laitteita. Sisältökytkennän ominaisuuksia ja sijoitusmahdollisuuksia käsiteltiin jo aikaisemmin luvussa 5, joten tässä osiossa käsitellään ADN-sisältökytkennän (Application Delivery Network) käyttöönottoaminen. Työssä käytetään runkoverkon rakentamiseen kahta Cisco 2811 -reititintä, jotka toimivat omissa verkoissaan DHCP-palvelimina, kahta Cisco Catalyst 3560 sarjan PoE-24 layer3-tason kytkintä sekä laitteita Blue Coat ProxySG200-C ja Blue Coat ProxySG400-1. Laitteet asennetaan verkkoon kuvan 29 mukaisella tavalla, ja laboratorioverkko on työssä toimipisteiden välinen WAN-verkko. ProxySG200 toimii etätoimiston välityspalvelimena millä muodostetaan päätoimipisteen välityspalvelimeen eli ProxySG400 laitteeseen ADN-sisältökytkentä optimoimaan ja kompressoimaan verkkojen välistä HTTP-liikennettä.



Kuva 29. Verkon rakenne

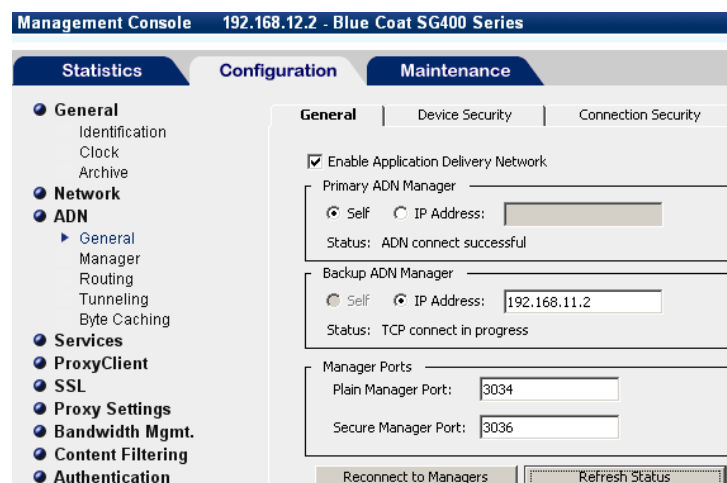
Reitittimille annetaan liitteiden 2 ja 3 mukaiset asetukset, jotta saadaan runkoverkko toimimaan työhön soveltuvalla tavalla ja muodostettua kahden eri verkon välille WAN-verkko. Kytkimiin työssä ei tule konfiguraatioita, vaan ne toimivat oletusasetuksillaan välittäen liikennettä. ProxySG400-laitteelle annetaan sarjakaapelia käyttämällä alkuasetukset, ja käytettävä rajapinta on laitteesta kytkimeen liitetty portti 0:0. Laitteelle annetaan kuvan 30 mukaiset

konfiguraatit, jonka jälkeen laitteeseen saadaan otettua selaimella yhteys osoitteesta <https://192.168.12.2:8082>.

```
You have entered the following IP addresses:
IP address: 192.168.12.2
IP subnet mask: 255.255.255.0
IP gateway: 192.168.12.1
DNS server: 10.95.254.253
Would you like to change any of them? Y/N [No]
```

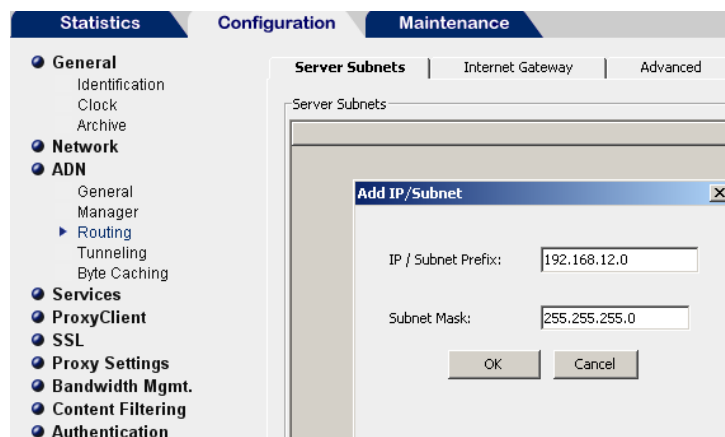
Kuva 30. ProxySG400-laitteelle annetut alkuasetukset

Koska ProxySG400 on sijoitettu lähimmäksi palvelimia, mainostaa se muille laitteille palvelinten verkkoja, mikä työssä on sama verkko, missä välityspalvelinkin sijaitsee. Lähimpänä palvelimia oleva laite konfiguroidaan ADN-manageriksi, ja se tulee konfiguroida ensimmäiseksi käyttökuntoon jonka jälkeen siihen yhdistetään kauempana sijaitsevia laitteita. Tässä verkkojen välisessä kytkennässä ProxySG200 yhdistetään päätoimipisteessä sijaitsevaan ProxySG400-laitteeseen ADN-kytkennällä. Kytkennän käyttöönoton tapahtuu asetuksien määrittämisellä. Valitaan configuration-välilehdeltä valinta ADN ja otetaan general-valinnoista ADN käyttöön tekemällä kuvan 31 mukaiset valinnat. Seuraavaksi yhdistetään laite muihin kytkettäviin laitteisiin. Ensisijainen ADN-manageri on ProxySG400 ja varamanagerin osoitteeseen syötetään ProxySG200 laitteen IP-osoite.



Kuva 31. ADN-sisältökytkennän määrittäminen

Yhdistämisen jälkeen voidaan havaita, että vara-ADN-managerin (Backup ADN Manager) status jää tilaan TCP connect in progres, koska vara-managerina toimivaa ProxySG200 laitetta ei ole vielä konfiguroitu tämän ADN-verkon jäseneksi. ADN-verkkoon liittyminen tapahtuu vasta WAN-verkon molempien laitteiden ollessa konfiguroituina. Seuraavaksi valitaan routing ja mainostetaan siellä Server subnets -välilehdeltä verkot, missä on palvelimia. Tässä työssä palvelimet sijaitsevat verkossa 192.168.12.0 255.255.255.0 kuvan 32 mukaisesti.



Kuva 32. Palvelimen verkon mainostus

HTTP proxy processing otetaan käyttöön valitsemalla tunneling ja välilehti Proxy processing, mistä päästään lisäämään rasti kohtaan "Enable proxy processing for incoming ADN tunnel connections for the following protocol: HTTP". Tämä mahdollistaa välityspalvelin ominaisuuksien hyödyntämisen ADN-tunnelissa kuljetettavalle datalle.

Palvelimien puolella sijaitseva välityspalvelin ei kuuntele liikennettä eikä ole suoraan linjalla asiakkaan ja palvelimen välissä, vaan toimii ADN-kytkennän manageri laitteena mainostaen liikennettä www-palvelimille. Koska suodatus tapahtuu jo aikaisemmin laitteeseen kytketyillä ADN-verkon ProxySG laitteilla ei ADN-managerin tarvitse kuunnella tai tutkia siihen tulevaa dataliikennettä. ProxySG400-laitteen välityspalvelimen asetukset asetetaan tilaan bypass all kuvan 33 mukaisella tavalla, jolloin laite ei tutki sen läpi kulkevaa liikennettä. ADN-managerin asetukset ovat nyt kunnossa ja seuraavaksi asetukset suoritetaan vara managerille WAN-verkon toisella puolella sijaitsevalle ProxySG200-laitteelle.

| Proxy Services            |  | Static Bypass List | Restricted Intercept List |
|---------------------------|--|--------------------|---------------------------|
| Services Groups           |  |                    | Action                    |
| Predefined Service Groups |  |                    |                           |
| Standard                  |  |                    | Bypass All                |
| Intranet                  |  |                    | Bypass All                |
| Encrypted                 |  |                    | Bypass All                |
| Interactive               |  |                    | Bypass All                |
| Reverse-proxy             |  |                    |                           |
| Other                     |  |                    | Bypass All                |
| Custom Service Groups     |  |                    |                           |

Kuva 33. Välityspalvelut-valinnat

Määritetään proxysg200-alkuasetukset antamalla laitteelle verkko-osoite ja aliverkon maski sekä oletusyhdykäytävä ja DNS Serverin osoite. Kuvassa 34 esitetään käytettävät osoitteet.

| SG Setup Wizard      |                   |
|----------------------|-------------------|
| Introduction         | Network > Address |
| Security             | Address           |
| Network              |                   |
| App Delivery Network |                   |
| Services             |                   |
| Finish               |                   |

Configure Bridge passthru-0 (WAN: link, LAN: link)

IP Address: 192.168.11.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.11.1

DNS Server: 10.95.254.253

Back Next

Kuva 34. ProxySG200 alkuasetukset

Kun ProxySG200-laitteelle on määritetty alustavat verkkoasetukset, päästään konfiguroimaan ADN-verkon asetukset syöttämällä ensisijaisen ADN-managerin osoitteeksi 192.168.12.2, mikä työssä on ProxySG400-laitteen rajapinnan osoite. Nyt konfiguroitavasta ProxySG200-laitteesta valitaan vara-ADN-manageri kuvan 35 mukaisella tavalla ottamalla käyttöön valinta "This is the backup ADN Manager". Näin saadaan lisättyä kytkennän vikasietoisuutta.

| App Delivery Network > ADN Manager |                |
|------------------------------------|----------------|
| Introduction                       | Configure      |
| Security                           | ADN Manager    |
| Network                            | Server Subnets |
| App Delivery Network               |                |
| Services                           |                |
| Finish                             |                |

There must be a ProxySG designated as the primary ADN Manager that maintains Server Subnets between participating ProxySG appliances.

☒ Enter the primary ADN Manager IP address

192.168.12.2

☐ This is the primary ADN Manager

☒ Configure a backup ADN Manager

☐ Enter the backup ADN Manager IP address

☒ This is the backup ADN Manager

Back Next

Kuva 35. ADN managerin konfigurointi

Etätoimiston välityspalvelin on sijoitettu suoraan linjalle kuuntelemaan liikennettä, joten sen ei tarvitse mainostaa palvelimien verkkoja ja kohdat välilehdellä Server Subnets jätetään tyhjiksi. Asiakaspuolella sijaitseva välityspalvelin kuuntelee liikennettä ja ohjaa ADN-tunnelin kautta valittua HTTP-protokollaa käyttävää dataliikennettä kompressoidea sitä ProxySG400 laitteelle ja sen mainostamille www-palvelimille. Valinta tehdään kuvassa 36 esitetyn mukaisesti HTTP-liikenteelle.

Kuva 36. Kuunneltavan protokollan valinta

Oletusasetuksiksi valitaan Blue Coatin kehittämä MACH5 (Multiprotocol Accelerated Caching Hierarchy) -teknologia ja sen asetukset. Valittavat vaihtoehdot näkyvät kuvassa 37. MACH5 teknologia mahdollistaa organisaatioiden nopeuttaa käytössä olevia avainsovelluksia mukaan lukien tiedostojen käsittelyn, sähköpostin, nettiohjelmat, videot ja SSL salatut web-ohjelmistot. MACH5 ratkaisussa yhdistyy viisi kiihdytys teknologiaa yhdeksi. Näitä teknologioita ovat kaistanhallinta, Protokollien optimointi, objektien taltioiminen, bittien säilöminen ja pakkaaminen. MACH5-ratkaisu tarjoaa enemmän vaihtoehtoja yleisten verkkohaasteiden hoitamiseen. [13.]

**Services > Default Settings**

**Intercepted Traffic** **Default Settings**

When the SG is first configured, certain default settings need to be specified. If the SG will be used primarily as a WAN accelerator, use of the MACH5 Edition default settings is recommended. However, if the SG is used for security enforcement, leaving the defaults at their more secure settings is recommended.

☒ Use the MACH5 Edition default settings  
☐ Set these values individually

[Default Policy](#)

☒ Allow all intercepted traffic  
☐ Deny all intercepted traffic

[Destination IP](#)

☒ Trust the client-provided destination IP  
☐ Look up the server's destination IP using DNS

[HTTP Request Errors](#)

☒ Tolerate errors in HTTP requests  
☐ Reject HTTP requests with errors

Back Next

Kuva 37. MACH5-valinta

Asetukset ovat ProxySG200-laitteelle valmiit ja lopuksi saadaan yhteenveto valituista konfiguraatioista, jonka jälkeen valitaan asetusten konfigurointi laitteelle. Kuvassa 38 on yhteenveto tehdyistä asetuksista. Kun laite on saanut asetukset valmiiksi, päästään laitteiden välistä liikennöintiä tarkastelemaan kirjautumalla selaimella laitteen rajapinnan osoitteeseen ja antamalla määritetty tunnus ja salanana.

**Finish > Confirm Settings**

**Confirm Settings** **Configure**

You are now ready to configure your SG. After the Configure button is pressed, all settings specified in this wizard will be uploaded to the SG. This setup wizard will no longer be available unless the appliance is reset to factory defaults.

**App Delivery Network**

Application Delivery Network has been configured

Primary ADN Manager is '192.168.12.2'

This is the Backup ADN Manager

**Services**

CIFS is not being intercepted or optimized

FTP is not being intercepted or optimized

HTTP is being intercepted and optimized

Instant Messenger Traffic (AOL, MSN and Yahoo) is not being intercepted or optimized

Microsoft Exchange / Outlook is not being intercepted or optimized

Back Configure

Kuva 38. Yhteenveto asetuksista

Kirjautumisen jälkeen sisältökytkennän onnistuminen tarkistetaan Proxysg 200-laitteelta ja valitaan Configuration-päävälilehdeltä ADN-valinta ja General välilehdeltä huomataan että ADN-tunneli on nyt onnistuneesti yhdistetty nä ProxySG200 ja ProxySG400 -laitteiden välille jolloin ensisijaisen ADN-

managerin ja varamanagerin molemmat statukset ovat "ADN connect successful" -tilassa.

**General** | Device Security | Connection Security

☒ Enable Application Delivery Network

Primary ADN Manager

☐ Self ☒ IP Address: 192.168.12.2

Status: ADN connect successful

Backup ADN Manager

☒ Self ☐ IP Address:

Status: ADN connect successful

Manager Ports

Plain Manager Port: 3034

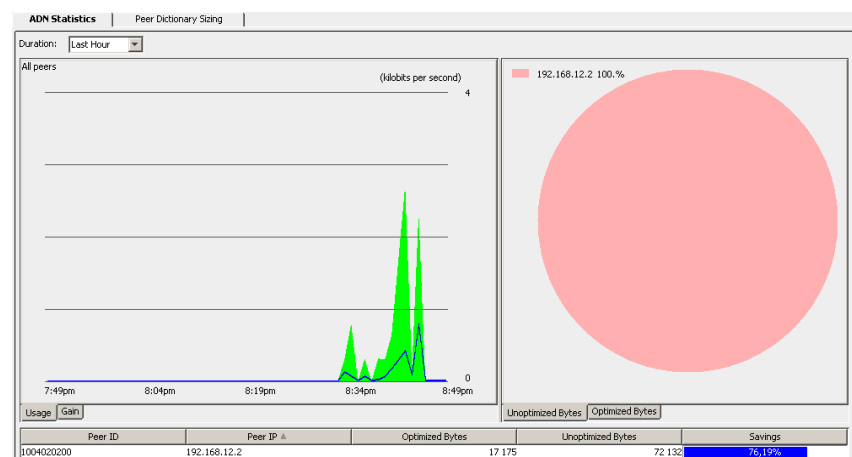
Secure Manager Port: 3036

Reconnect to Managers Refresh Status

Kuva 39. ADN-kytkennän yhdistäminen

Molemmilla käytettävillä laitteilla optimoidaan HTTP-liikennettä, joten valitaan lopuksi myös ProxySG200-laitteelta tunneling ja välilehti Proxy processing ja otetaan käyttöön HTTP proxy processing laittamalla rasti kohtaan "Enable proxy processing for incoming ADN tunnel connections for the following protocol: HTTP". Sisältökytkentä hyödyntää nyt HTTP-liikenteen kompressointia kahden laitteen välisessä sisältökytkennässä.

ADN-kytkennän statistiikkaa ja kaistanleveyden säästöä voidaan seurata molemmilta ProxySG-laitteilta. ProxySG200-laitteelta liikennettä tarkasteltaessa kytkennän jälkeen ympyrä-diagrammi näyttää SG400-laitteen osoitetta 192.168.12.2 ja 100% käytetyn protokollan osuudelle, mikä työssä on HTTP-liikennettä. Käyrä diagrammista voidaan havaita datan vaatima kaistanleveys ja sen siirtämiseen käytetty kaistanleveys tietyllä ajanhetkellä.



Kuva 40. ADN-statistiikka

ProxySG200-laitteelta tarkasteltaessa ADN-verkkoonliitettyjä laitteita ”Peer Dictionary Sizing” -välilehdeltä huomataan että tunnelin vastakkaisen laitteen ID-tunnus ja IP-osoite löytyy tietoineen tältä välilehdeltä. Jos käytössä olisi useampia laitteita liitettyä samaan sisältökytkentään, löytyisi kaikista verkon jäsenistä samat tiedot.

| Rank | Peer ID    | Peer IP      | Byte Cache Score | Peer Traffic (GB/Day) |
|------|------------|--------------|------------------|-----------------------|
| 1    | 1004020200 | 192.168.12.2 | 100000000        | 0,0000                |

Kuva 41. ADN-verkon jäsen laitteiden seuranta

ProxySG400-laitteelta tarkasteltaessa ADN-tunnelin liikennöintiä Statistics välilehden Traffic Mix valinnasta nähdään ”Inbound ADN” -palvelun kohdasta luodun tunnelin kuljettamaa bittimäärää asiakas- ja palvelinpuolelta sekä kaistanleveyden säästöä, mikä tässä työssä on ADN-tunnelia pitkin kuljetettua HTTP-liikennettä.

| Service Name                 | Proxy Type      | Client Bytes                 | Server Bytes | Bypassed Bytes                | Savings |
|------------------------------|-----------------|------------------------------|--------------|-------------------------------|---------|
| Inbound ADN                  | Inbound ADN     | 75,882                       | 19,253       | 0                             | 74,62%  |
| CIFS                         | CIFS            | 0                            | 0            | 0                             | n/a     |
| Endpoint Mapper              | Endpoint Mapper | 0                            | 0            | 0                             | n/a     |
| FTP                          | FTP             | 0                            | 0            | 0                             | n/a     |
| HTTP                         | HTTP            | 0                            | 0            | 0                             | n/a     |
| RTSP                         | RTSP            | 0                            | 0            | 0                             | n/a     |
| HTTPS                        | SSL             | 0                            | 0            | 0                             | n/a     |
| Citrix ICA                   | TCP Tunnel      | 0                            | 0            | 0                             | n/a     |
| Default                      | TCP Tunnel      | 0                            | 0            | 0                             | n/a     |
| IMAP                         | TCP Tunnel      | 0                            | 0            | 0                             | n/a     |
| Total Client Bytes: 74,10 KB |                 | Total Server Bytes: 18,80 KB |              | Total Bypassed Bytes: 0 bytes |         |
|                              |                 |                              |              | Total Gain: 74,62%            |         |

Kuva 42. Saapuvan liikenteen kaistan säästö



## 9 JOHTOPÄÄTÖKSET

Työssä onnistuttiin Blue Coat ProxySG -laitteiden toimintamallin selvittämisessä, sisällönsuodatuksen ja kompression konfiguroinnissa ja käyttöön otossa. Laitteet olivat aluksi melko hankalia käyttää, mutta ne ovat tarkemman tutustumisen jälkeen melko loogisia ja selkeätoimintoisia.

Blue Coat ProxySG-laitteet ovat melko monipuolisia välityspalvelimia tarjoten ratkaisuja erilaisiin käyttötarkoituksiin ja mahdollistaen verkon liikennöinnin optimoinnin ja erilaisia suodatusratkaisuja erilaisiin tarpeisiin. Poliitikoiden luominen on helppoa ja melko selkeää Visual Policy Manageria käyttämällä. Laitteet vaativat lisenssin toimiakseen ja ilman lisenssejä tarvittaville ominaisuuksille on niillä mahdotonta tehdä mitään. Välityspalvelimina laitteet nopeuttavat internetin selaamista usein toistuvilla sivustoilla ja vähentävät merkittävästi latausaikoja tehostaen ajankäyttöä ja tarjoten miellyttävämmän tavan sivujen selaamiselle. HTTP-kompressio vähentää kaistanleveyden käyttöä, jolloin verkosta tulee optimoitu. ADN-sisältökytkentää käytettäessä voidaan eri paikoissa sijaitsevien toimipisteiden välille rakentaa nopea yhteys, sekä vähentää kuluja käyttämällä etätoimipisteissä päätoimipisteen palvelimia. Sisältökytkentää olisi mahdollista käyttää muiden liikennöinti protokollien dataliikenteeseen ja nopeuttaa eri ohjelmien käyttämistä verkon ylitse palvelimilta. Blue Coat mainostaakin sisältökytkennälle erilaisia ratkaisuja useiden ohjelmien käytön nopeuttamiseksi mukaan lukien Microsoft Office tuoteperheen Word ja Excel, Microsoft Exchange -palvelu etätoimipisteisiin, Oracle sekä SAP. [14.]

Blue Coat ProxySG -laitteet soveltuvat hyvin pieniin ja suuriin yrityksiin käyttötarkoituksen mukaan. Tuoteperheessä on paljon valinnan varaa ja laitteita on tarjolla erikokoonpanoilla yhdestä kiintolevystä useampaan kiintolevyyn. Suurempiin verkkoympäristöihin soveltuu useampi laite käytettäväksi.

Työssä tutkittiin, millaisia ominaisuuksia ja ratkaisuja Blue Coat ProxySG -laitteet tarjoavat HTTP-liikenteen sisällönsuodatuksen ja ProxySG-laitteiden väliseen sisältökytkentään. Työlle asetetut tavoitteet saavutettiin ja projekti oli onnistunut tavoitteiden mukaisesti.

## VIITELUETTELO

- [1] Blue Coat, [verkkodokumentti, viitattu 14.4.2009] About Blue Coat Systems. Saatavissa <http://www.bluecoat.com/company/aboutbluecoat>.
- [2] Hakala, Mika - Vainio, Mika. Tietoverkon rakentaminen, 2005
- [3] Proxy, [verkkodokumentti, viitattu 10.12.2008]. Saatavissa [http://en.wikipedia.org/wiki/Proxy\\_server](http://en.wikipedia.org/wiki/Proxy_server).
- [4] Proxy, [verkkodokumentti, viitattu 10.1.2009] Configuration and Management Suite Volume 2: Proxies and Proxy Services. Saatavissa [http://www.bluecoat.co.jp/downloads/manuals/SGOS\\_Vol2\\_ProxiesPortServices\\_5.3.1.pdf](http://www.bluecoat.co.jp/downloads/manuals/SGOS_Vol2_ProxiesPortServices_5.3.1.pdf).
- [5] Sisällönsuodatus, [verkkodokumentti, viitattu 8.1.2009] From Network Security To Content Filtering. Saatavissa <http://www.ucci.it/docs/CFS-200705.pdf>.
- [6] Björkman, Taru. Suojelua vai suodatusta? Internetin sisällönsuodatus yleisissä kirjastoissa, 2008
- [7] Kompresio, [verkkodokumentti, viitattu 10.2.2009] ProxySG TechBrief – HTTP Compression. Saatavissa [http://www.onixnet.com/Blue%20Coat/ImportMedia/downloads/support/BCS\\_tb\\_HTTP\\_compression.pdf](http://www.onixnet.com/Blue%20Coat/ImportMedia/downloads/support/BCS_tb_HTTP_compression.pdf)
- [8] ADN, [verkkodokumentti, viitattu 12.2.2009] Technology Primer - Compression. Saatavissa <http://www.bluecoat.com/doc/365>.
- [9] ADN, [verkkodokumentti, viitattu 10.3.2009] EdgeCorps ADN Deployment Scenario. Saatavissa <http://www.bluecoat.com/doc/8659>.
- [10] Blue Coat Product Suite, [verkkodokumentti, viitattu 10.11.2008]. Saatavissa <http://www.bluecoat.com/products/overview/>.
- [11] Blue Coat ProxySG, [verkkodokumentti, viitattu 10.11.2008]. Saatavissa <http://www.bluecoat.com/products/sg>.
- [12] Proxy Guide, [verkkodokumentti, 10.3.2009] SSL Proxy Reference Guide for SGOS 5.3.1. Saatavissa [http://www.bluecoat.co.jp/downloads/manuals/SGOS\\_5.3.x\\_SSL\\_Proxy\\_Reference\\_Guide.pdf](http://www.bluecoat.co.jp/downloads/manuals/SGOS_5.3.x_SSL_Proxy_Reference_Guide.pdf).
- [13] MACH5, [verkkodokumentti, viitattu 14.4.2009] MACH5 Acceleration Technology. Saatavissa <http://www.bluecoat.com/doc/797>.
- [14] ADN White Paper, [verkkodokumentti, viitattu 24.4.2009] Application Delivery Networks: The New Imperative for IT Visibility, Acceleration and Security. Saatavissa <http://www.bluecoat.com/doc/direct/8791>.

## SISÄLLÖNSUODATUKSEN JA KOMPRESSION KONFIGURAATIOT LAITTEELLE PROXYSG200

```
!- Version: SGOS 5.3.2.1 Proxy Edition
!- BEGIN ssl
ssl ;mode
exit
!- END ssl
!- BEGIN proxies
general ;mode
trust-destination-ip enable
exit
!- END proxies
!- BEGIN content_filtering
content-filter ;mode
provider iwf enable
websense ;mode
no log-forwarded-client-address
exit
exit
!- END content_filtering
!- BEGIN proxies
http tolerant-request-parsing
!- END proxies
!- BEGIN services
management-services ;mode
edit "SNMP" ;mode
remove all 161
exit
exit
management-services ;mode
exit
proxy-services ;mode
edit "FTP" ;mode
intercept all 21
exit
edit "HTTP" ;mode
intercept all 80
intercept explicit 8080
exit
edit "CIFS" ;mode
intercept transparent 139
intercept transparent 445
exit
exit
!- END services
!- BEGIN policy
policy proxy-default allow
policy order L C V F
!- END policy
!- BEGIN policy
inline policy vpm-cpl end-417013418-inline
;; CPL generated by Visual Policy Manager: [Thu Mar 19 14:57:31 EET 2009]
```

```

*****
;
; WARNING:
;   THIS FILE IS AUTOMATICALLY GENERATED - DO NOT EDIT!
;   ANY MANUAL CHANGES TO THIS FILE WILL BE LOST WHEN VPM
;   POLICY IS REINSTALLED.
*****
;

define category "AllowedSites"
    iltasanomat.fi
    iltalehti.fi
end category "AllowedSites"

define category "Jobs"
    monster.com
    hotjobs.com
end category "Jobs"

define category "Entertainment"
    facebook.com
    youtube.com
    pelikone.fi
    iltalehti.fi
    iltasanomat.fi
end category "Entertainment"

define category "Blocked Sites"
    category="Jobs"
    category="Entertainment"
end category "Blocked Sites"

define condition "Allowed Sites"
    url.category=("AllowedSites")
end condition "Allowed Sites"

define condition __PROTO_1
    client.protocol=http url.scheme=http p2p.client=no streaming.client=no
end condition __PROTO_1

define condition "night shift"
    time=(2200..0559) weekday=(1..5)
end condition "night shift"

define condition weekend
    time=(0000..2359) weekday=(6..7)
end condition weekend

;; Description: Time restriction for weekends and night shift
define condition __CondList1weekend/night_shift
    condition="night shift"
    condition=weekend
end condition __CondList1weekend/night_shift

define condition weekend/night_shift
    condition=__CondList1weekend/night_shift
end condition weekend/night_shift

```

```
define condition BlockedSites
    url.category=("Blocked Sites")
end condition BlockedSites
```

```
define condition IWF
    url.category=("IWF-Restricted")
end condition IWF
```

```
:: Tab: [Web Access]
```

```
<Proxy>
    client.address=192.168.11.0/24 condition="Allowed Sites" condi-
tion=__PROTO_1 condition=weekend/night_shift Allow ; Rule 1
    client.address=192.168.11.0/24 condition=BlockedSites Deny ; Rule 2
    condition=IWF Deny ; Rule 3
```

```
:: Tab: [Compression]
```

```
<Proxy>
    http.allow_compression(yes) http.allow_decompression(yes)
    http.server.accept_encoding(all)
http.server.accept_encoding.allow_unknown(yes) ; Rule 1 ; HTTP
Compression
```

```
end-417013418-inline
inline policy vpm-xml end-417013418-inline
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- *****-->
<!-- WARNING: -->
<!-- THIS FILE IS AUTOMATICALLY GENERATED - DO NOT EDIT! -->
<!-- MANUALLY EDITING THIS FILE MAY PREVENT VPM FROM BEING -->
<!-- ABLE TO LOAD POLICY. -->
<!-- *****-->
<vpmapp>
<vpmxml-info
version="531">
</vpmxml-info>
<conditionObjects>
<vpm-cat>
<node
n="AllowedSites"
u-l="iltasanomat.fi&#10;iltalehti.fi">
</node>
<node
n="Jobs"
u-l="monster.com&#10;hotjobs.com">
</node>
<node
n="Entertainment"
u-l="facebook.com&#10;youtube.com&#10;pelikone.fi&#10;iltalehti.fi&#10;iltasanomat.fi">
```

```

</node>
<node
n="Blocked Sites"
u-l="">
<child
n="Jobs">
</child>
<child
n="Entertainment">
</child>
</node>
</vpm-cat>
<ipobject
name="__Client IP Address/Subnet1"
single="true"
type="1"
value="192.168.11.0/24">
</ipobject>
<time
UTC="false"
days="1..5"
name="night shift"
single="true"
time="2200..0559"
value="night shift">
</time>
<time
UTC="false"
days="6..7"
name="weekend"
single="true"
time="0000..2359"
value="weekend">
</time>
<comb-obj
d="Time restriction for weekends and night shift"
n-1="false"
n-2="false"
name="weekend/night_shift"
t="6">
<c-l-1
n="night shift">
</c-l-1>
<c-l-1
n="weekend">
</c-l-1>
</comb-obj>
<time
name="weekend/night_shift"
single="false"
upgraded="true">
<item>
night shift</item>
<item>
weekend</item>

```

```

</time>
<categorylist4
name="BlockedSites"
typ="r">
<sel>
<i>
Blocked Sites</i>
</sel>
<excl>
</excl>
<sel-p>
</sel-p>
</categorylist4>
<clnt-http-compres
cmpr="al-c"
name="ClientHTTPCompression"
uncmpr="al-d">
</clnt-http-compres>
<svr-http-compres
i-u-cc="true"
name="ServerHTTPCompression"
opt="all">
</svr-http-compres>
<comb-obj
d=""
n-1="false"
n-2="false"
name="Compression"
t="5">
<c-l-1
n="ClientHTTPCompression">
</c-l-1>
<c-l-1
n="ServerHTTPCompression">
</c-l-1>
</comb-obj>
<categorylist4
name="IWF"
typ="r">
<sel>
<ai
a="iw1"
n="IWF-Restricted">
</ai>
</sel>
<excl>
</excl>
<sel-p>
</sel-p>
</categorylist4>
<protocol
name="__PROTO_1"
subtype="pure-http"
t="http">
</protocol>

```

```

<categorylist4
name="Allowed Sites"
typ="r">
<sel>
<i>
AllowedSites</i>
</sel>
<excl>
</excl>
<sel-p>
</sel-p>
</categorylist4>
</conditionObjects>
<layers>
<layer
layertype="com.bluecoat.sgos.vpm.WebAccessPolicyTable">
<name>
Web Access</name>
<numRows>
3</numRows>
<rowItem
enabled="true"
num="0">
<colItem
col="0"
id="no"
value="1">
</colItem>
<colItem
col="1"
id="so"
name="__Client IP Address/Subnet1"
negate="false"
type="Condition">
</colItem>
<colItem
col="2"
id="de"
name="Allowed Sites"
negate="false"
type="Condition">
</colItem>
<colItem
col="3"
id="se"
name="__PROTO_1"
negate="false"
type="Condition">
</colItem>
<colItem
col="5"
id="ti"
name="weekend/night_shift"
negate="false"
type="Condition">

```



```

</collItem>
<collItem
col="4"
id="ac"
name="Allow"
negate="false"
type="Condition">
</collItem>
<collItem
col="7"
id="tr"
name="None"
type="String">
</collItem>
<collItem
col="6"
id="co"
name=""
type="String">
</collItem>
</rowItem>
<rowItem
enabled="true"
num="1">
<collItem
col="0"
id="no"
value="2">
</collItem>
<collItem
col="1"
id="so"
name="__Client IP Address/Subnet1"
negate="false"
type="Condition">
</collItem>
<collItem
col="2"
id="de"
name="BlockedSites"
negate="false"
type="Condition">
</collItem>
<collItem
col="3"
id="se"
name="Any"
type="String">
</collItem>
<collItem
col="5"
id="ti"
name="Any"
type="String">
</collItem>

```

```

<collItem
col="4"
id="ac"
name="Deny"
negate="false"
type="Condition">
</collItem>
<collItem
col="7"
id="tr"
name="None"
type="String">
</collItem>
<collItem
col="6"
id="co"
name=""
type="String">
</collItem>
</rowItem>
<rowItem
enabled="true"
num="2">
<collItem
col="0"
id="no"
value="3">
</collItem>
<collItem
col="1"
id="so"
name="Any"
type="String">
</collItem>
<collItem
col="2"
id="de"
name="IWF"
negate="false"
type="Condition">
</collItem>
<collItem
col="3"
id="se"
name="Any"
type="String">
</collItem>
<collItem
col="5"
id="ti"
name="Any"
type="String">
</collItem>
<collItem
col="4"

```

```

id="ac"
name="Deny"
negate="false"
type="Condition">
</collItem>
<collItem
col="7"
id="tr"
name="None"
type="String">
</collItem>
<collItem
col="6"
id="co"
name=""
type="String">
</collItem>
</rowItem>
</layer>
<layer
layertype="com.bluecoat.sgos.vpm.WebAccessPolicyTable">
<name>
Compression</name>
<numRows>
1</numRows>
<rowItem
enabled="true"
num="0">
<collItem
col="0"
id="no"
value="1">
</collItem>
<collItem
col="1"
id="so"
name="Any"
type="String">
</collItem>
<collItem
col="2"
id="de"
name="Any"
type="String">
</collItem>
<collItem
col="3"
id="se"
name="Any"
type="String">
</collItem>
<collItem
col="5"
id="ti"
name="Any"

```

```
type="String">
</collItem>
<collItem
col="4"
id="ac"
name="Compression"
negate="false"
type="Condition">
</collItem>
<collItem
col="7"
id="tr"
name="None"
type="String">
</collItem>
<collItem
col="6"
id="co"
name="HTTP Compression"
type="String">
</collItem>
</rowItem>
</layer>
</layers>
</vpmapp>
```

end-417013418-inline  
!- END policy

**CISCO REITITTIMEN KONFIGURAATIOT ADN-KYTKENNÄN ETÄTOIMISTON LAN-  
VERKOLLE**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterSg200
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$m0uS$aI9Gknd11fkDnUF3eHLXd.
!
no aaa new-model
memory-size iomem 15
!
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp excluded-address 192.168.11.0 192.168.11.10
ip dhcp pool verkko11
    network 192.168.11.0 255.255.255.0
    default-router 192.168.11.1
    dns-server 10.95.254.253
!
!
!
!
voice-card 0
no dspfarm
!
!
!
interface FastEthernet0/0
ip address 10.95.1.11 255.255.254.0
duplex auto
speed auto
no shut
!
interface FastEthernet0/1
ip address 192.168.11.1 255.255.255.0
duplex auto
speed auto
no shut
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
```

```
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
router eigrp 1234  
  network 10.95.0.0 0.0.1.255  
  network 192.168.11.0  
  no auto-summary  
!  
!  
!  
ip http server  
no ip http secure-server  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
  no login  
!  
scheduler allocate 20000 1000  
!  
end
```

**CISCO REITITTIMEN KONFIGURAATIOT ADN-KYTKENNÄN PALVELINPUOLEN  
LAN-VERKOLLE**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterSg400
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$ccL/$D3oFGQCFVkb63kDD9MREX1
!
no aaa new-model
memory-size iomem 15
!
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp excluded-address 192.168.12.0 192.168.12.10
ip dhcp pool verkko12
    network 192.168.12.0 255.255.255.0
    default-router 192.168.12.1
    dns-server 10.95.254.253
!
!
!
!
voice-card 0
no dspfarm
!
!
!
interface FastEthernet0/0
ip address 10.95.1.12 255.255.254.0
duplex auto
speed auto
no shut
!
interface FastEthernet0/1
ip address 192.168.12.1 255.255.255.0
duplex auto
speed auto
no shut
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
```

```
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
router eigrp 1234  
  network 10.95.0.0 0.0.1.255  
  network 192.168.12.0  
  no auto-summary  
!  
!  
!  
ip http server  
no ip http secure-server  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
  no login  
!  
scheduler allocate 20000 1000  
!  
end
```



**ADN KONFIGURAATIOT PROXYSG200 LAITTEELLE**

```
!- Version: SGOS 5.3.2.1 Proxy Edition
!- BEGIN ssl
ssl ;mode
exit
!- END ssl
!- BEGIN proxies
general ;mode
trust-destination-ip enable
exit
!- END proxies
!- BEGIN application_delivery_network
adn ;mode
manager ;mode
primary-manager 192.168.12.2
backup-manager self
exit
tunnel ;mode
proxy-processing http enable
exit
enable
exit
!- END application_delivery_network
!- BEGIN content_filtering
content-filter ;mode
websense ;mode
no log-forwarded-client-address
exit
exit
!- END content_filtering
!- BEGIN proxies
http tolerant-request-parsing
!- END proxies
!- BEGIN services
proxy-services ;mode
edit "HTTP" ;mode
intercept all 80
intercept explicit 8080
exit
exit
!- END services
!- BEGIN policy
policy proxy-default allow
!- END policy
```

**ADN KONFIGURAATIO PROXYSG400 LAITTEELLE**

```

!- Version: SGOS 5.3.2.1 Proxy Edition
!- BEGIN ssl
ssl ;mode
exit
!- END ssl
!- BEGIN application_delivery_network
adn ;mode
manager ;mode
primary-manager self
backup-manager 192.168.11.2
exit
routing ;mode
server-subnets ;mode
add 192.168.12.0/24
exit
exit
tunnel ;mode
proxy-processing http enable
exit
enable
exit
!- END application_delivery_network
!- BEGIN content_filtering
content-filter ;mode
websense ;mode
no log-forwarded-client-address
exit
exit
!- END content_filtering
!- BEGIN services
management-services ;mode
edit "HTTPS-Console" ;mode
attribute ssl-versions SSLv2v3
attribute cipher-suite rc4-md5 rc4-sha des-cbc3-sha des-cbc3-md5 rc2-cbc-md5 rc4-64-
md5 des-cbc-sha des-cbc-md5 exp1024-rc4-md5 exp1024-rc4-sha exp1024-rc2-cbc-md5
exp1024-des-cbc-sha exp-rc4-md5 exp-rc2-cbc-md5 exp-des-cbc-sha
exit
exit
!- END services
!- BEGIN policy
policy proxy-default allow
!- END policy
!- BEGIN authentication
!
inline authentication-forms end-417034195-inline
(exception.auth
(exception.authentication_form
(properties
(form_type "authentication_form")
)
(http

```

```

        (code "200")
        (format <<--18db6fd3.4c74e--
<HTML>
<HEAD>
<TITLE>Enter Proxy Credentials for Realm $(cs-realm)</TITLE>
</HEAD>
<BODY>
<H1>Enter Proxy Credentials for Realm $(cs-realm)</H1>
<P>Reason for challenge: $(exception.last_error)
<P>$(x-auth-challenge-string)
<FORM METHOD="POST" ACTION=$(x-cs-auth-form-action-url)>
$(x-cs-auth-form-empty-domain-field)
<P>Username: <INPUT NAME="PROXY_SG_USERNAME" MAXLENGTH="64"></P>
<!-- To prepopulate the Username field with a previously entered username, set the VA-
LUE field to the cs-username substitution -->
<P>Password: <INPUT TYPE="PASSWORD" NAME="PROXY_SG_PASSWORD" MAX-
LENGTH="64"></P>
<INPUT TYPE="HIDDEN" NAME="PROXY_SG_REQUEST_ID" VALUE=$(x-cs-auth-
request-id)">
<INPUT TYPE="HIDDEN" NAME="PROXY_SG_PRIVATE_CHALLENGE_STATE" VA-
LUE=$(x-auth-private-challenge-state)">
<P><INPUT TYPE="SUBMIT" VALUE="Submit"> <INPUT TYPE="RESET"></P>
</FORM>
<P>$(exception.contact)
</BODY>
</HTML>
--18db6fd3.4c74e--
    )
  )
)
(exception.new_pin_form
  (properties
    (form_type "new_pin_form")
  )
  (http
    (code "200")
    (format <<--18db6fd3.4c78c--
<HTML>
<HEAD>
<TITLE>Create New PIN for Realm $(cs-realm)</TITLE>
<SCRIPT LANGUAGE="JavaScript"><!--
function validatePin() {
var info;
var pin = document.pin_form.PROXY_SG_PASSWORD;
if (pin.value != document.pin_form.PROXY_SG_RETYPE_PIN.value) {
    info = "The PINs did not match. Please enter them again.";
} else {
    // Edit this regular expression to match local PIN definition
    var re=/^[A-Za-z0-9]{4,16}$/
    var match=re.exec(pin.value);
    if (match == null) {
        info = "The PIN must be 4 to 16 alphanumeric characters";
    } else {
        return true;
    }
}

```

```

}
alert(info);
pin.select();
pin.focus();
return false;
} // -->
</script>
</HEAD>
<BODY>
<H1>Create New PIN for Realm $(cs-realm)</H1>
<P>$(x-auth-challenge-string)
<FORM NAME="pin_form" METHOD="POST" ACTION=$(x-cs-auth-form-action-url) ON-
SUBMIT="return validatePin()">
$(x-cs-auth-form-empty-domain-field)
<P> Enter New Pin: <INPUT TYPE=PASSWORD NAME="PROXY_SG_PASSWORD"
MAXLENGTH="64"></P>
<P>Retype New Pin: <INPUT TYPE=PASSWORD NAME="PROXY_SG_RETYPE_PIN"
MAXLENGTH="64"></P>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_USERNAME" VALUE=$(cs-username)>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_REQUEST_ID" VALUE=$(x-cs-auth-
request-id)>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_PRIVATE_CHALLENGE_STATE" VA-
LUE=$(x-auth-private-challenge-state)>
<P><INPUT TYPE=SUBMIT VALUE="Submit"></P>
</FORM>
<P>$(exception.contact)
</BODY>
</HTML>
--18db6fd3.4c78c--
)
)
)
(exception.query_form
(properties
(form_type "query_form")
)
(http
(code "200")
(format <<--18db6fd3.4c7d6--
<HTML>
<HEAD>
<TITLE>Query for Realm $(cs-realm)</TITLE>
</HEAD>
<BODY>
<H1>Query for Realm $(cs-realm)</H1>
<P>$(x-auth-challenge-string)
<FORM METHOD="POST" ACTION=$(x-cs-auth-form-action-url)>
$(x-cs-auth-form-empty-domain-field)
<INPUT TYPE=HIDDEN NAME="PROXY_SG_USERNAME" VALUE=$(cs-username)>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_REQUEST_ID" VALUE=$(x-cs-auth-
request-id)>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_PRIVATE_CHALLENGE_STATE" VA-
LUE=$(x-auth-private-challenge-state)>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_PASSWORD">

```

```
<P><INPUT TYPE=SUBMIT VALUE="Yes" ON-  
CLICK="PROXY_SG_PASSWORD.value='Y'">  
<INPUT TYPE=SUBMIT VALUE="No" ON-  
CLICK="PROXY_SG_PASSWORD.value='N'"></P>  
</FORM>  
<P>$(exception.contact)  
</BODY>  
</HTML>  
--18db6fd3.4c7d6--  
)  
)  
)  
)  
end-417034195-inline  
!  
!- END authentication
```

## BLUE COAT PROXYSG200 JA PROXYSG400 LAITTEIDEN TEKNISET TIEDOT

### Blue Coat ProxySG200

[http://www.bluecoat.co.jp/downloads/manuals/200\\_InstallGuide\\_4.x\\_5.x.pdf](http://www.bluecoat.co.jp/downloads/manuals/200_InstallGuide_4.x_5.x.pdf)

|  |  |
|--|--|
| Enclosure (Einschließung)                                      | 19 inch rack-mountable with optional brackets, desktop, wall mount |
| Height (Höhe)  | 43.7 mm (1.72 in); 1 rack unit                                     |
| Width (Breite)   | 191 mm (7.5 in)  |
| Length (Länge)   | 356 mm (14 in)   |
| Weight (Gewicht)   | System 2.5 kg (5.6 lb), Power adapter 0.5 kg (1 lb)                |
| Power Input, AC<br>(for external adapter)<br>(Stromversorgung) | 100-240V, 1.8 A, 50/60 Hz  |
| DC (for Server)  | 19V 3.42A  |
| Disk Drives (Festplatte)                                       | 1 x 40 GB IDE ATA-100  |
| Processors (Prozessor)   | Transmeta TM5900 Crusoe Family                                     |
| RAM (Speicher)   | 256 MB, 512 MB   |
| Network (Netzwerk)   | (2 on board) 10/100 Base-T Ethernet                                |
| <b>Regulations (Regelungen)</b>                                |  |
| Safety (Schutz)  | CSA C22.2 No. 60950-1/ UL60950-1 First edition, EN60950-1          |
| Emissions (Emissionen)   | FCC Class A, EN55022 Class A, VCCI Class A No. 1247859             |
| <b>Environmental (Umweltsmäßig)</b>                            |  |
| Temperature (Betriebstemperatur)                               | 5° C to 35° C (41° F to 95° F)                                     |
| Relative Humidity (Relative<br>Luftfeuchte)                    | Less than 90% relative humidity, non-condensing                    |
| Maximum Altitude (Maximale Höhe)                               | Up to 2000 m (6561 ft)   |

### Blue Coat ProxySG400

[http://www.afina.com.mx/download/docs/bluecoat/SG400\\_Datasheet\\_021803.pdf](http://www.afina.com.mx/download/docs/bluecoat/SG400_Datasheet_021803.pdf)

#### Configuration & Specification Chart

| Configuration A Specifications - Model 400-0 |  | Model 400-1           |
|--|--|-----------------------|
| <b>System</b>                                |  |                       |
| Disk drives                                  | 1 x 40 GB IDE ATA-100  | 2 x 40 GB IDE ATA-100 |
| RAM  | 256 MB   | 512 MB                |
| Network Interfaces                           | (2 on board) 10/100 Base-T Ethernet  |                       |
| <b>Operating System</b>                      | SGOS   |                       |
| <b>Operating Environment</b>                 |  |                       |
| Power  | AC power 100-240V, 50-60Hz, 2A   |                       |
| Temperature                                  | 5°C to 35°C (41°F to 95°F)   |                       |
| Humidity                                     | Less than 90% relative humidity, non-condensing  |                       |
| Altitude                                     | Up to 3048 M (10,000 ft)   |                       |
| <b>Dimensions and Weight</b>                 |  |                       |
| Enclosure                                    | 19" Rack-mountable   |                       |
| Height                                       | 43.7 mm (1.72 in); 1 rack unit   |                       |
| Width  | 443 mm (17.4 in)   |                       |
| Depth  | 350 mm (13.75 in); mounting depth  |                       |
| Weight (maximum)                             | 7.1 kg (15.6 lb)   |                       |
| <b>Regulations</b>                           |  |                       |
| Emissions                                    | FCC Class A, EN55022 Class A   |                       |
| Safety                                       | CSA C22.2 No. 950 M95, UL 1950 3 Edition, EN60950  |                       |
| <b>Support</b>                               | Standard warranty: 90-day software & phone support with 1-year hardware support; extended and upgraded support plans available |                       |