University of Guelph Co-op Program
Work Term Nearing Completion S05

Work Term Report

"The Quality Assurance Process at Blue Coat Systems"

Document Metadata

Current Author: Dave Heppenstall	**Last Modified:** 19 August 2005
Institution: Blue Coat Systems	**Creation Date:** 9 August 2005
Intended Audience: Any Interested Parties	**Security:** University of Guelph, Co-op Program Blue Coat Systems

Goal and Scope

The purpose of this document is to explore and demonstrate the unique challenges presented with a member of the Quality Assurance team at Blue Coat Systems inc. The audience of this document is twofold, the co-op department at the university of Guelph to evaluate the work term through this report and new QA hires at Blue Coat as a reference manual for common tasks which may be unfamiliar during the initial phase.

1.1 Introduction

Blue Coat Systems is the world leader in web-based proxy appliances. Blue Coat Systems endeavors to maintain corporate productivity while making the web good for business. One of the chief goals of Blue Coat Systems is control; to keep "good" employees from doing "bad" things on the internet.

The current position held by the student is Quality Assurance Test Engineer. The student works with the Quality Assurance department to contribute to product testing to seek out defects and deficiencies, in addition to verifying and validating that product repairs and fixes were effective – and didn't affect other aspects negatively concurrently. It is with this guise that the student proceeds to contribute to Blue Coat Systems.

1.2 Ongoing Learning

At the onset of the term, the student outlined certain goals to strive to attain in order to have a greater degree of self-directed learning while working in a hands-on environment. Base Competencies, as described through extensive research by Evers, Rush, and Berdrow (1998) are the general skills that students need to succeed in today's workplace. The skills are grouped under four base competencies which are most desired by employers:

1. Managing Self
2. Communicating
3. Managing People and Tasks
4. Mobilizing Innovation and Change

By developing these competencies, students can decrease the gap between the classroom and work, translating into lifelong employability.

1.3 Perspective

As much as a contradiction as the following statement may seem, quality assurance is very much an alien ideal in the Computing and Information Science program at the University of Guelph. That is to say, quality is expected and so are the deadlines - but at this point in my program, work is all completed independently with no one to review your code but yourself. Up until now, this essentially demonstrates my sum experience with the field.

Quality Assurance at Blue Coat requires testing of products which you did not design and evaluating work which is not your own. To reiterate, this is indeed a very alien concept for a student of computer science in second year. In upper year courses, group work does begin to take shape, but this is still all within the development process. In QA, I did not have to look at almost any code at all. In a nutshell, high level black box testing, exhaustive analysis and sanity checks.

1.4 Overview

Pursuant to Blue Coat's goal of control and internet security, we have developed a line of proxy appliances for a variety of purposes to fit neatly within an existing network infrastructure. Hardware proxy appliances are much faster than software based control and filtering.

Interface to the product is twofold, a GUI (Graphical User Interface) and a CLI (Command Line Interface). Typically, an end-user customer will only use the GUI aspects, but the CLI is still utilized (with the exception described below). Both of these interfaces must be thoroughly examined by the QA team as well as the behavior of the product itself when put through certain tests.

1.4.1 The Proxy SG™

"The Proxy SG™ family of appliances includes the award-winning ProxySG 400 Series, 800 Series and 8000 Series. Based on Blue Coat SGOS™, a custom, object-based operating system with integrated caching, these proxy appliances leverage existing authentication systems to enable granular policy enforcement down to the individual user. Blue Coat's end-to-end product portfolio includes powerful reporting, policy and configuration management software - delivering a scalable proxy system architecture for centralized or distributed enterprise environments. Delivered as a rack mountable appliance for simple installation and management, these ICSA-certified solutions easily integrate with existing security and network infrastructure."

Stop IM file transfers, disable access to websites with certain content, and allow users to authenticate access through NTLM and/or LDAP servers. With the Proxy SG™, you call the shots.

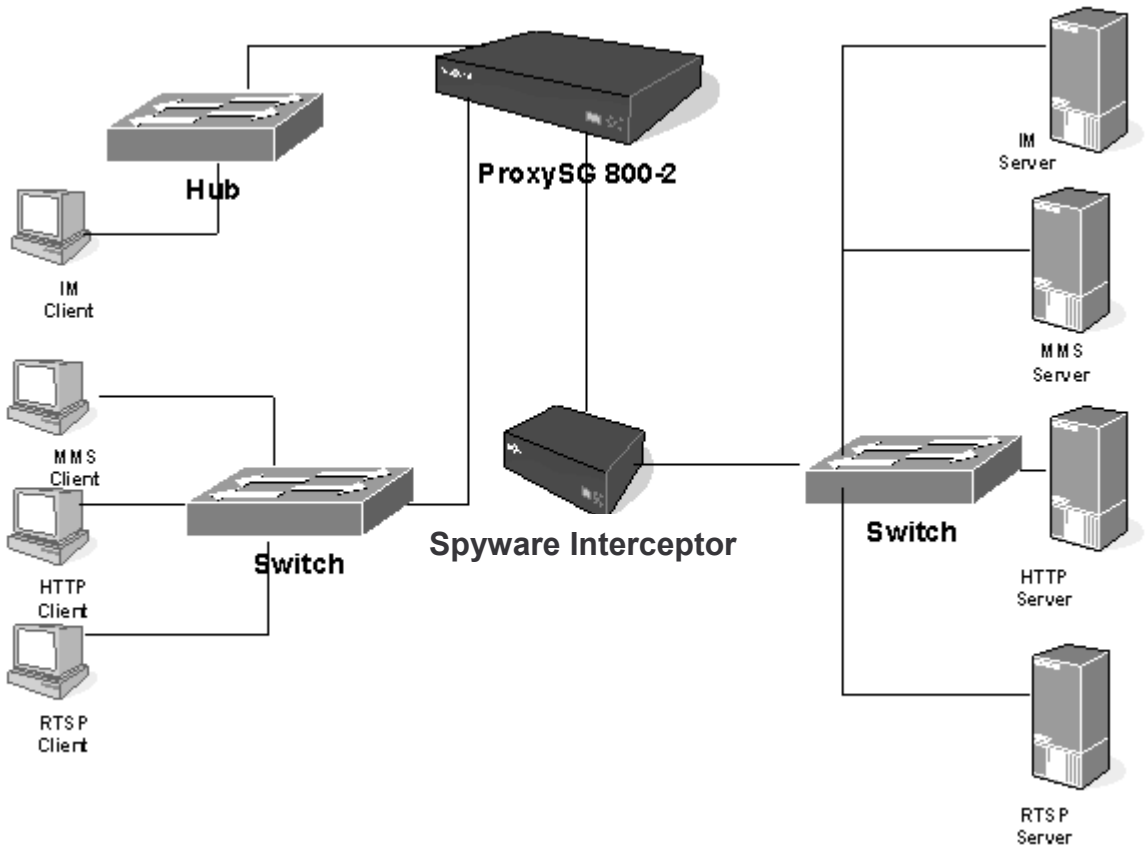
1.4.2 Spyware Interceptor™

"Blue Coat Spyware Interceptor™ is an easy-to-deploy anti-spyware appliance for networks of up to 1000 users. Interceptor prevents known and unknown spyware while enabling legitimate applications via proven proxy technology. Interceptor's patent-pending SCOPE™ anti-spyware engine optimizes its ten methods of protection daily to minimize the need for cleaning spyware, keyloggers and adware from your desktops."

In this world, prevention is key. Reports indicate that IT departments spend more time cleaning spyware from user's machines than anything else. The solution of choice was simply to reimage a computer. For a home user, this usually involves reformatting the computer and installing an operating system from scratch. With the Spyware Interceptor, the appliance blocks these types of applications from gaining entry in the first place. The SI is constantly adapting to meet the changing ways in which spyware programs secretly install.

1.4.3 Co-Operation

A Network Illustration

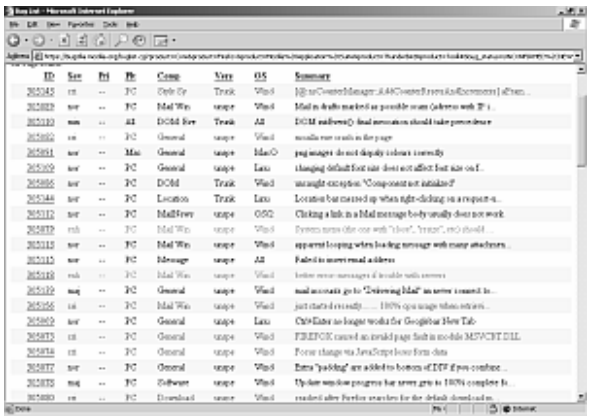


2 Quality Assurance Procedures

2.1 Task Distribution

In the QA Team at Blue Coat, there are several key team members working under the guidance of the QA team leader. Communication between each member of this team is very important as the completion of tasks could not be complete without this. Communication does not simply mean, "reading and responding to e-mail." There are key tools which exist to implement the communication and exchange of information between all employees at Blue Coat.

2.1.1 CacheZilla *(BugZilla)*



CacheZilla is a modified version of web-based tool based on the open-source tool "BugZilla," used specifically for implementing bug reports and monitoring the research, development and problem solving surrounding the issue(s) with our products.

Scenario One: Your e-mail informs you that you have had several new bugs assigned to you. What does this mean? Check CacheZilla and place a query for any bugs whose QA Contact is you. Take a look at the list. Typically from the QA point of you, you have been assigned some bugs which have been resolved. It is now your job to make sure that these bugs are actually corrected. Run the test cases provided by the developer who corrected the problem and also try to reproduce the problem using the instructions by the original reporter. If the bug has indeed been fixed, mark the bug as "Verified," if the problem persists, mark it as "Reopened" and enter details on your observations.

Scenario Two: You are running product tests, perhaps to check if another resolved bug has been verified and you encounter irregular activity or unexpected behavior. It is time to report a bug.

View all bugs

Mozilla

- Open CacheZilla
- Enter `SI` as the key query term

Reporting a new bug

Mozilla

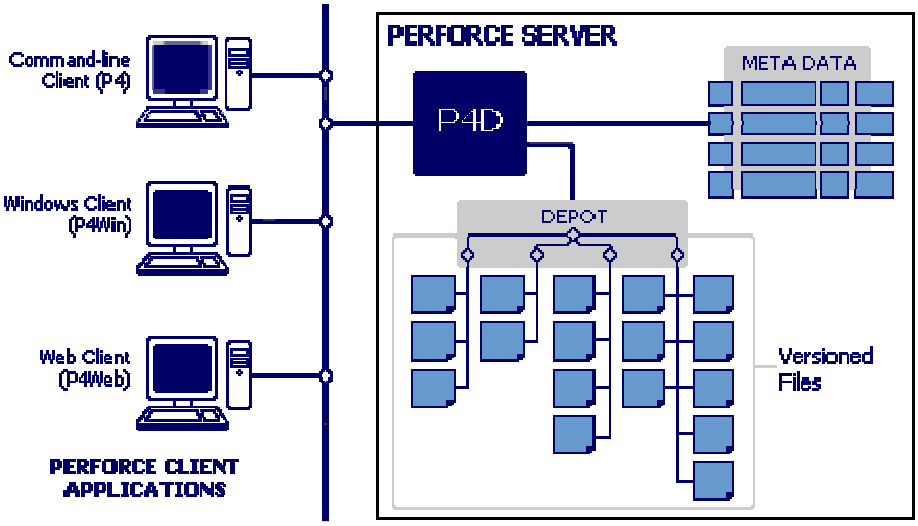
- Open CacheZilla
- Enter the key query terms
- Scroll to the footer and click “Enter New Bug”, select the product name you are testing.
- Select a component; write a one-line summary that is simple to search for, choose a severity level, enter the build number (corresponding to the main branch) and write a description which contains the symptoms, the steps to recreate and possibly a recommended solution.
- Click Commit.
- If desired, revisit the bug and enter yourself as the QA contact.

Verifying a fixed bug

Mozilla

- Open CacheZilla
- Enter a new query for `FIXED` and `RESOLVED` bugs.
- Enter your username as the QA contact.
- Select the product, highlight all branches.
- Click Submit Query.

2.1.2 Perforce 4



Perforce is the central development utility at Blue Coat. It maintains source code, documentation, test worksheets, test result whitepapers and other general information and specifications.

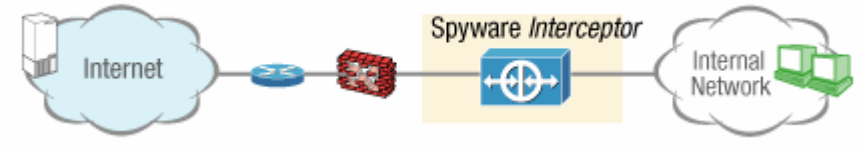
P4D stores file revisions in depot(s). File status and change metadata are maintained in the built-in database.

"Typically each user has his or her own client workspace, and may also use other special-purpose or project workspaces. The client workspace specification defines a view, or subset, of files from the repository that are of interest to the user. The workspace itself contains physical copies of the files in its view.

P4D comprises three main sub-components: a request handler, a data manager and a file librarian. The request handler acts as an executive, sequencing actions to carry out client requests and managing communication with the client. The data manager implements database services optimized for multi-user SCM operations. It maintains a meta-database describing the status and history of versioned files in the depot and transactions against the depot. The librarian is a highly efficient file archiver that stores repository files on disk local to the server. It writes text file versions in an RCS-compatible, reverse-delta format; binary file versions are stored in a standard compressed format."

2.2 Working with the Spyware Interceptor™

2.2.1 Remanufacturing



On any given day, chances are that overnight a new compilation of all the code changes from the previous day will be built. In order to achieve the most up to date and accurate testing, you should upgrade the Spyware Interceptor box you are using.

Training Material Focus

Local

Mozilla

- Open *Build List*
- Navigate to *product's working directory*
- Select build based on your product specification (ie, an 800 box)
- Copy entire path of build to use.

Mozilla

- Open *Caches*
- Find a the appliance you are using and establish a serial connection.

PuTTY

- `en` → "admin"
- `con t`
- `upgrade-path` *"copied path of build to use (from above)"*
- `exit`
- `load upgrade`
- `restart upgrade`
- *Wait for system to reboot*
- Hit [`ENTER`] three times

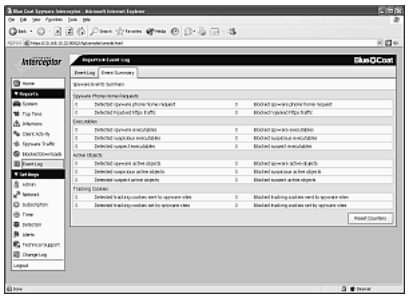
Remote Desktop

- Connect to a desktop downstream from the Spyware Interceptor

Remote

Internet Explorer

- Open https://si.bluecoat.com:**8083**/
- *Wait for wizard to launch*
- Admin – enter a username and password
- Network – Hostname: `SI`, Use DHCP data
- Activation – Enter key
- Time – Specify time zone and track with Blue Coat NTP server
- Detection – Desired settings dependant on task
- Alerts – SMTP: *`smtp server`*, E-mail: *`your email`*
- *Finish and Log in*



For the Spyware Interceptor to function, the computers which are to be protected must be "downstream" from the appliance. To achieve this, place the Spyware Interceptor between the outside and your terminal. The appliance is specially designed to respond to http://si.bluecoat.com:8083 (or 8082)/, for management console access.

2.2.2 Establishing and Configuring Content Filtering

`Training Material Focus`

Local

Mozilla

- Open *Caches*
- Find your appliance and establish serial connection.

PuTTY

- `en` → "admin"
- `con t`
- *For content information and testing…*
  - `content-filter`
  - *To view current database info…*
    - `bl`
    - `view`
    - `exit`
  - *To test urls based on the database…*
    - `test url <address>` (i.e. coolwebsearch.com)
  - `exit`
- *To access content configuration on the SI box in the GUI…*
  - `services`
  - `http-console`
  - `enable 8081`
  - `exit`
  - `exit`
- `exit`

Remote Desktop

- Connect to a box downstream from SI.

Remote

Internet Explorer

- Open https://si.bluecoat.com:**8082**/
- *Log in as* user: `admin`, pass: `test`

Local

Mozilla

- Open http:// si.bluecoat.com:**8081**/
- Click close
- *Log in as* user: `admin`, pass: `test`
- Click "Management Console" → "Content Filtering" → "General"
- Enable "Use Blue Coat Web Filter"

2.3 Working with the Proxy SG™

2.3.1 Remanufacturing

(See 2.2.1, same process exactly)

2.3.2 Configuring Inline Policy

Training Material Focus

Add local policy

PuTTY

- `en` → "admin"
- `con t`
- `inline policy local foo`
  - *Example 1:*
    - **<proxy>**
      `url.domain=www.ibdprince.com action.strip_active_content(yes)`

      `define active_content strip_with_indication`
      `tag_replace` **`applet`** `<<EOT`
      `<APPLET code=lake.class id=Lake WIDTH=80 HEIGHT=50><PARAM name=image value="image.gif"></APPLET>`
      `EOT`
      `end`

      `define action strip_active_content`
      `transform strip_with_indication`
      `end`
  - *Example 2*:
    - `define category "unavailable"`
      `perl.com`
      `end`
      <proxy>
      `exception (content_filter_denied, "$(cs-categories-unqualified)")`
  - *Example 3*:
    - **<proxy>**
      `url.domain=//perl.com ALLOW`
      `exception …`
      <proxy>
      `url.extension=.gif DENY`
- *`foo` (Record terminator)*

Change Proxy Behavior

Internet Explorer

- Open https://si.bluecoat.com:**8082**
- Policy > Policy Options
  - Default Proxy Policy: Select Allow or Deny
- Content Filtering > General
  - Use Local Database, Enable Category Review message in exceptions

2.3.3 Authentication: Realms

`Training Material Focus`

1) Create a new Realm

Internet Explorer

- Open Management Console
- Navigate: Configuration > Authentication > IWA (or LDAP)
- Click "New"
  - Enter any realm name
  - IWA (NTLM): Enter Primary Server host
  - LDAP: Enter Primary Server host

PuTTY

- Serial connect to the SG Box
- Install proxy to enable authentication checks:
  - `<proxy>`
    `allow authenticate(`***`realm_name`***`)`

2) Manage NTLM Users

Remote Desktop

- Connect to: **`The ntlm server`**
- Open "Local Users and Groups" snap-in in the mmc.
- Open "Services" snap-in in the mmc.
- Ensure "BCAAA" is started and running.

2b) Manage LDAP Users

Remote Desktop

- Connect to: **`The ldap server`**
- Run Active Directory to Manage Users

3) Test Authentication in the Realm

Mozilla

- Set explicit proxy to the SG box. Open a web page, note the login prompt.