**Symantec Web Filter - Support Guide**

2011-07-05

Michael Spence

**Audience:**

Currently this documentation is for Field Support officers and Service Desk staff. This document may be useful for explanation purposes to clients; however it has not been designed for this purpose. It is expected that the user of this guide has practical knowledge of proxies.

**Preamble:**

This document describes how users are to be setup.

This document describes the notable "issues" with this setup

This document DOES NOT describe the configuration of rules, although it does demonstrate how to diagnose which rules are being enforced.

This document does describe the differing levels of the Web Filter.

This document DOES NOT list the proxy exceptions.

**Topics of Discussion**

1. General Overview

2. Internal CSPs

3. WSP Synchronisation

4. Security Groups

5. Automatic Proxy Set

6. Blocked Pages

**Topics in Detail**

**1. General Overview**

The Symantec Web Filter is a proxy for web browsers although not in the same manner as typical Microsoft ISA proxy servers. The system consists of a Client Side Proxy (CSP) and a Web Side Proxy (WSP). The CSP has access to the internal network and using this connectivity can gather information about the users, such as security groups. This information is synchronised with the WSP. As users attempt to access websites, their username is added by the CSP to their request and passed to the WSP. The WSP then filters the request based on the information it has about the user and the requested website.



**2. Internal CSPs**

Currently there are two CSPs within APEagers, the number of these machines has no limit and they all point directly at the one WSP. The current CSPs are:

qld-csp

nsd-csp

The proxy functionality is accessed through port 3128.

There is future intention to roll out this proxy to other APEagers' networks. As such, it could be expected that the following CSPs may exist.

dwn-csp

klo-csp

bb-csp

adt-csp

**3. WSP Synchronisation**

On the qld-csp machine there is a program installed which regularly interrogates the Active Directory system based on a number of configured rules. The rules have been configured to synchronise users who are in the Internet Control Groups.

This synchronisation occurs approximately every 4 hours. Due to this timeframe, when a new user is created, it is expected that they may not have internet access for some time.

**4. Security Groups**

The internet control groups created for use with the Symantec Web Filter are:

Internet L0 - No Access

Internet L1 – Manufacturer Only

Internet L2 – Whitelist Only

Internet L5 – Standard Access

Internet L7 - plus Social Networking

Hopefully it is easy to see that the names have been created to denote a "Level" of access. The levels up to L5 are exclusive to each other, meaning that if a user is in more than one group, the one with the lowest level is enforced.

Levels L6 and above are designed to be Additive. For a user to have Social Networking for example the user must be a member of level 5 also.



**L0 - No Access**

Users in this group have ABSOLUTELY no access to use the web via this system. Exceptions to this are proxy exceptions (access to extranets), \*.apeagers.com.au and \*.outlook.com.

**L1 - Manufacturer Only**

Over time a list of the Brand specific sites has been compiled. In this setup this acts like a whitelist, and users in this group have access ONLY to this list and the sites listed in the previous rule.

**L2 - Whitelist Only**

Websites with a deemed business function have been requested from various GM’s in the past. These sites are not brand specific. Users of this group have access ONLY to this list and the sites in the previous rules.

**L5 - Standard Access**

The Symantec system has categorized 80+% (reportedly) of all web sites on the internet. A number of categories have been granted access to users of this group. Websites listed in previous rules are also allowed.

**L7 - Social Networking**

Users in this group gain access to a list of allowed social networking sites (including Facebook, Twitter and Linked In). This group does not grant them access to the websites listed in previous rules.

Please note that during the setup process of this system the "Old" internet control groups, which corresponded vaguely to the above groups, were added to the above groups to aid in mass deployment.

**5. Automatic Proxy Set**

An Active Directory Group Policy has been created to force the proxy of machines within APEagers to be automatically configured to "qld-csp:3128". This policy requires that a user is a member of an Internet Control Group. Even if a user changes their proxy, it will be reverted back to "qld-csp:3128" within 40 minutes.

**6. Blocked Pages**

The following example image shows a "Blocked Page" message. This is generated by the WSP and is the result of the rules defined.

When diagnosing blocked pages, please note the URL, Category and Rule, stated in the block page.

A standard user, when blocked, will have the rule "L9 - Block (Default)"; gaining the "Category" in this case is essential for diagnosis.

A whitelist user (either Manufacturer or Whitelist) will be blocked at their level of access.

