

SurfControl Web Filter
for Blue Coat

Integration Guide

rev1.0, May 2004

ACKNOWLEDGEMENTS

SurfControl wishes to acknowledge the following people for their contributions to this integration guide:

Role	Name
Technical Contributor	Josh Wolfer, Technical Support Engineer
Author	Shawn Titus, Technical Communications Manager

NOTICE

© 2004 SurfControl. All rights reserved. SurfControl, SurfControl E-mail Filter, SurfControl Web Filter, Virtual Control Agent, Anti-Spam Agent, Anti-Virus Agent, Virtual Learning Agent, Virtual Image Agent, and the LexiMatch logos are registered trademarks and trademarks of SurfControl plc. All other trademarks are properties of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

This integration guide provides general information on SurfControl Web Filter for Blue Coat (SurfControl for Blue Coat). SurfControl for Blue Coat utilizes pass-through filtering technology and seamlessly integrates with Blue Coat's ProxySG secure proxy appliance. Policies are created using Blue Coat and web sites are categorized using SurfControl's industry-leading URL Category database.

With this latest offering from SurfControl, Blue Coat users also gain functionality from SurfControl's robust monitoring and reporting capabilities.

This document discusses the following:

- Network architecture.
- Filtering process.
- Pre-installation requirements.
- Set up and configuration.

NETWORK ARCHITECTURE

SurfControl for Blue Coat requires the Blue Coat ProxySG secure proxy appliance (which provides Internet Filtering) and includes the software for SurfControl Web Filter for Microsoft Windows (SurfControl WF), which provides monitoring and reporting capabilities. Figure 1 shows the basic network architecture for SurfControl for Blue Coat.

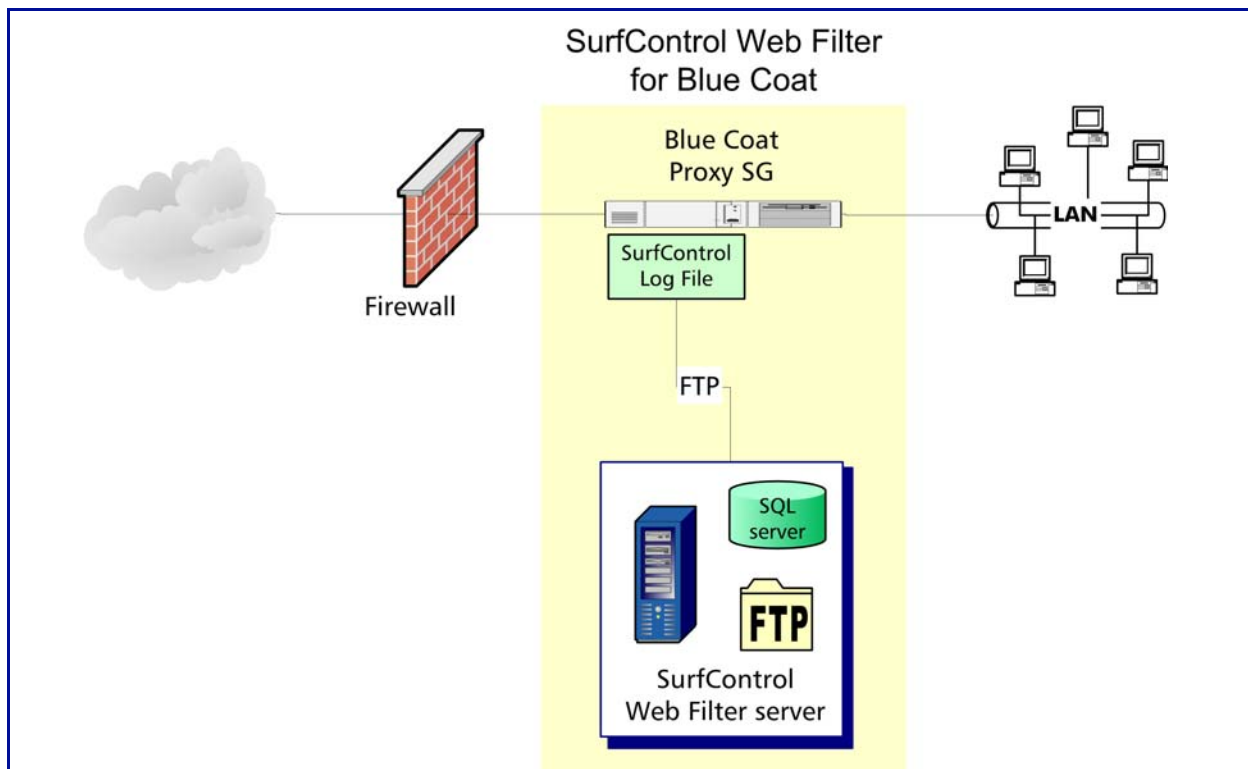


Figure 1 SurfControl for Blue Coat architecture

FILTERING PROCESS

With SurfControl for Blue Coat, the Blue Coat ProxySG appliance filters Internet traffic using SurfControl's URL Category database and then writes the data to a SurfControl-formatted log file. The following steps outline the filtering, monitoring, and reporting process:

- 1 Client issues an HTTP request
- 2 Browser configuration directs request to Blue Coat ProxySG.
- 3 Blue Coat filters the request using SurfControl Categories database.
- 4 Blue Coat writes the data associated with the transaction into a SurfControl-formatted log file. (SurfControl calls these log files "flat files.")
- 5 Once the active log file reaches the maximum size (configured by the administrator), Blue Coat creates a new log file.
- 6 Using FTP, the preconfigured Blue Coat "Custom Client" moves the file to the specified location on the SurfControl server.
- 7 The SurfControl Scheduler imports data to the SurfControl database (SurfControl_WebFilter) residing on the specified SQL server .
- 8 Data is now available for monitoring and reporting.

PRE-INSTALLATION REQUIREMENTS

Before installing SurfControl for Blue Coat, perform the following:

- 1 Download SurfControl for Blue Coat from <http://www.surfcontrol.com>.
- 2 Obtain a user name and password to enable Blue Coat's usage of the SurfControl categories database. See "Evaluation of SurfControl for Blue Coat" and "Purchase of SurfControl for Blue Coat" for additional information.
- 3 Make sure an FTP server, such as Microsoft's IIS, is installed on the SurfControl server.
- 4 Make sure a Microsoft SQL server (MSDE, SQL7.0 or SQL2000) is available for the SurfControl database. SurfControl recommends installing the SQL server onto the SurfControl server.

Evaluation of SurfControl for Blue Coat

If you are downloading an evaluation copy of the software, SurfControl will send you an e-mail containing your evaluation user name and password (required to enable the SurfControl URL Category database on the Blue Coat appliance). No keys are required to enable the SurfControl monitoring and reporting evaluation.

Purchase of SurfControl for Blue Coat

If you have purchased SurfControl for Blue Coat, the Blue Coat user name and password will be included in the fulfillment e-mail from SurfControl (and will also include the SurfControl product keys).

SETUP AND CONFIGURATION

This section outlines the basic set up for configuring SurfControl for Blue Coat. Before creating filtering policies, you should perform the steps outlined below.

SURFCONTROL

On the SurfControl WF server, perform the following:

- 1 Install MSDE or SQL.
- 2 Configure the FTP server.
- 3 Install SurfControl WF.
- 4 Disable the SurfControl Web Filter service.
- 5 Create a directory named TMP in the C:\Program Files\SurfControl\Web Filter directory.
- 6 Using the Scheduler, create a Database Update event to import the log data into the SurfControl database.
- 7 Using the Scheduler, create events for database maintenance (purge, archive, and compact).
- 8 Using the Scheduler, create Report events to meet your company's requirements.

Please note, SurfControl for Blue Coat does not support manual categories or the Virtual Control Agent.

BLUE COAT

From the Management Console, choose Configuration and perform the following:

- 1 Choose Blue Coat to use SurfControl as your content filtering provider (Configuration→Content Filtering→General).
- 2 Set up SurfControl categories (Configuration→Content Filtering→SurfControl). For additional information, see page 432 of the *Blue Coat ProxySG Configuration and Management Guide*.

To complete this step you will need the URL Category database user name and password you received.

- 3 Schedule updates to the SurfControl Categories database (Configuration→Content Filtering→Automatic Download). For additional information, see page 440 of the *Blue Coat ProxySG Configuration and Management Guide*.
- 4 Create a new log file (Configuration→Access Logging→Logs) to use the SurfControl format.
SurfControl recommends setting the maximum remote file size to 1 MB and the early upload value to 20 MB.
- 5 Configure the client for uploading log files to the SurfControl server (Configuration→Access Logging→Upload Client). For additional information, see page 504 of the *Blue Coat ProxySG Configuration and Management Guide*.

The Upload Client must use FTP to upload files to the SurfControl server. Enter the IP address of the SurfControl server, the path (\TMP\), and the user name required by the FTP server. The transfer type must be set to Text File.

- .
- .
- .
- Setup and Configuration**

- 6 Set up the upload schedule (Configuration→Access Logging→Upload Schedule). For additional information, see page 507 of the *Blue Coat ProxySG Configuration and Management Guide*.

The upload schedule should be set to periodically.

- 7 Create filtering policies by launching the filtering policies manager (Configuration→Policy→Visual Policy Manager). To log transactions, you must add a Web Content Layer to the policy. To do this, set a new Modify Access Logging action and enable logging to the log file you created in step 3.