



Version 5.5

SurfControl Web Filter

Best Practices Guide



NOTICES

© 2007 SurfControl. All rights reserved. SurfControl, SurfControl E-mail Filter, SurfControl Web Filter, SurfControl Enterprise Threat Shield, SurfControl RiskFilter, SurfControl Mobile Filter, SurfControl Report Central, Single Management Console, Virtual Control Agent, Anti-Spam Agent, Anti-Virus Agent, Virtual Learning Agent, Virtual Image Agent, and the Personal E-mail Manager 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.

August 2007

1

Notices

TABLE OF CONTENTS

Notices	i
Table of Contents	iii
Introduction	1
How to use this Guide	2
General Best Practices	4
Database Configuration	5
SQL vs. SQL Server Express	5
Database Size	5
Local vs. Remote Database	6
Database Permissions	7
System Configuration	12
Rules Creation	12
Exclude the Web Filter directory from Real-Time Scanning	12
Performance Optimization	13
Monitor Settings	13
Web Filter Service Settings	14
Maintenance Plan	17
Best Practices for Web Filter for Windows	19
Introduction	20
System Configuration	21
NIC Configuration	21
NIC Teaming	23
Performance Optimization	24
Monitor Settings	24
Web Filter Service Settings	27
Ignored Ports	28
Subnet Monitoring	29
Best Practices for Web Filter for ISA Server	31
Introduction	32
Enhancing ISA Server Security with Web Filter	32
System Configuration	34
Username and Domain Name Enumeration	34
Rules Creation	35
Content Scanning	36
Creating ISA Firewall Policy Access Rules	37
Deployment	41
Deployment Recommendations	41
DMZ Considerations	42
Appendix	44
Comments on this Guide?	45
Technical Support	46

1

Table of Contents

SurfControl Sales47

Introduction

How to use this Guide.....page 2

HOW TO USE THIS GUIDE

This guide provides specific recommendations for configuring your system, and can help you optimize performance in most environments.

SurfControl recommends that you read this document fully before you make any modifications to your system. This guide has been functionally organized, as you may want to perform multiple functions in single areas (for example, you may want to perform two procedures in the Service Settings dialog box at the same time, even though they are organized separately in this document).

This guide contains references to the SurfControl Knowledge Base. Each referenced article is hot-linked to the Knowledge Base as [KBarticlenumber](#) (for example, [KB1977](#)). Click the link to view the correlating article.

General Best Practices

Database Configurationpage 5
System Configurationpage 12
Performance Optimizationpage 13

DATABASE CONFIGURATION

Web Filter stores all configuration data, filtering policies, and log data in a Microsoft SQL database. Web Filter provides robust reporting capabilities and is very data intensive (stores large amounts of data). Some of the stored data includes (but is not limited to): URL, category, requesting IP, user name, protocol, first seen/last seen data, and filtering rules.

In Services (from the Windows Control Panel), ensure the SurfControl Web Filter service is configured to:

- Run as a Windows user with correct permissions on the SQL database. See [Database Permissions on page 7](#) for more information.
- Start automatically.

SQL VS. SQL SERVER EXPRESS

Web Filter uses SQL Server Express, or a fully-licensed version of SQL Server 2000 or 2005. You should ensure your choice of database platform is installed and running, before attempting to install Web Filter. SurfControl recommends that you use SQL Server rather than SQL Server Express for the following reasons:

- SQL Server allows greater scalability.
- SQL Server enables you to fine-tune database performance.
- SQL Server is more suitable for environments with heavy Web traffic.
- SQL Server does not have a specified database size limitation, whereas SQL Server Express has a maximum database size of 4GB.

For customers using SQL Server Express, SurfControl recommends downloading a free Microsoft management tool called SQL Server Management Studio Express to manage instances of your SQL Server Database Engine. You can download the tool from the following link: [SQL Server Management Studio Express](#)

DATABASE SIZE

The size of the database is directly related to:

- The amount of traffic your employees generate.
- The amount of traffic Web Filter is monitoring (including file type and page level monitoring).
- The number of protocols Web Filter is monitoring.
- The number of users Web Filter is monitoring.



Note: SurfControl estimates that 5,000 users generate approximately 1 GB of data per month.

Database size in relation to disk space

Ensure there is ample disk space available for purging. A good general rule is that you should allocate disk space that is twice the size of the database.

Database size in relation to RAM

The recommended RAM in relation to the size of the database for specific database platforms are dependent on the following:

- **SQL Server 2000 (Standard Edition)** - SQL Server 2000 can only use a maximum of 2GB RAM, so if the Web Filter database grows beyond 2GB in size, response times for data retrieval may be affected, but are considered to be satisfactory for databases up to 10GB in size.
- **SQL Server 2000 (Enterprise Edition)** - If the Enterprise edition of SQL Server 2000 is installed on Windows 2000 Advanced Server, it can be configured to utilize more than 4GB RAM. SurfControl recommends this configuration if the database is likely to grow beyond 10GB in size.
- **SQL Server 2005 (Standard and Enterprise Editions)** - SQL Server 2005 will secure and release as much memory as it requires, and therefore does not have a limit on the amount of RAM it can utilize.

LOCAL VS. REMOTE DATABASE

If your network requires multiple Web Filter servers, you have the option to install the database in a location which is local or remote to the Web Filter server.

- **Local database** - Stores data for a single Web Filter server in a single database on the Web Filter server.
- **Remote database** - Stores the data from one or more Web Filter collectors in a single database on a separate server. If you choose to use the remote database option, you can manage your policy from one location, plus you have the ability to run reports from a single repository. This means that policy changes made on one collector are replicated to the other collectors, removing the need for separate policy creation at each collector.

However, the size of a remote database grows in direct relation to the number of Web Filter servers that write to it. Depending on the size of your environment and the amount of Internet traffic, a remote database can require more frequent database administration. SurfControl recommends using Windows Authentication for performance and security reasons. Therefore, remote databases require specific security settings for communication between the Web Filter server and the database.

DATABASE PERMISSIONS

The Web Filter service connects to the database to perform various different tasks. Certain tasks require individual database permissions depending on which users are responsible for performing those activities (see [Table 2-1 on page 8](#)). SurfControl recommends having two different types of user to undertake Web Filter activities; An Administrator and a standard user. These are defined as follows:

- **Administrator** - This user should be the database owner (DBO). This type of user will perform database maintenance, such as purging and restoring data, and operating Web Filter services. (By default, the SQL account that you used to create the Web Filter database is the DBO).
- **User** - A standard user should be able to define rules and objects in the Rules Administrator as well as operate Web Filter Manager applications.

The correct properties for Web Filter database Administrators and users are illustrated in the figures below:

Figure 2-1 Database User Properties - Administrator (dbo)

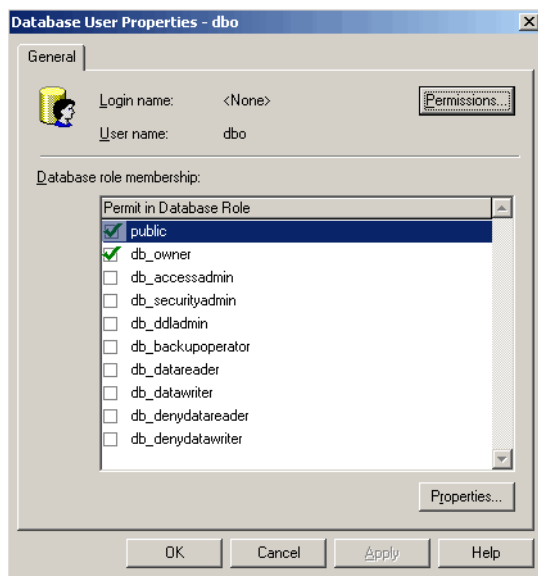
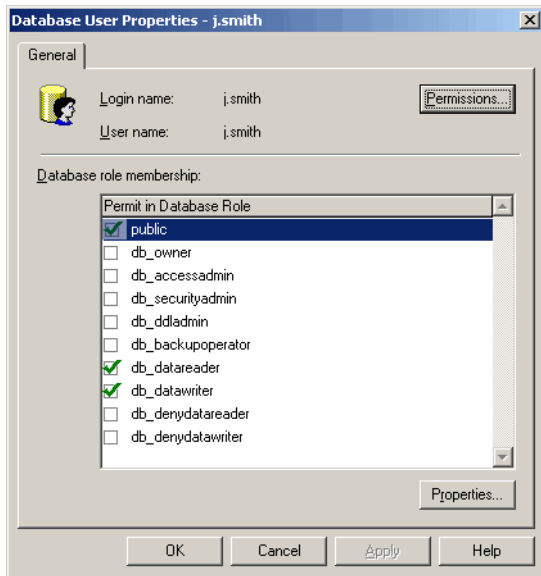


Figure 2-2 Database User Properties - Standard User



The table below shows the minimum database permissions required for the SurfControl Web Filter service to perform specific tasks:

Table 2-1 Database Permissions

Task	db_reader	db_writer	db_owner	Information
Write automatically to the database			✓	Requires execute permissions on the database Stored Procedures.
Manually import flat files			✓	Requires execute permissions on the database Stored Procedures.
Create Rules	✓	✓		
Modify Rules	✓	✓		
Database maintenance			✓	Requires execute permissions on the database Stored Procedures.

Database permissions for Web Filter Services

The Web Filter scheduler application can be configured to run automated tasks at specific times, and in order to initiate some of these tasks, the Scheduler service will require dbo permissions to access the database and run stored procedures. These are namely;

- Database management tasks.
- Database updates.

Additionally, if you have configured Network Group updates in the Scheduler, the Scheduler service will need to log on with a domain user account, so that it has permissions for the Domain Controller to return group membership information.

For the database scheduled tasks, the service will need to log on as the dbo account you have setup. To ensure the Scheduler uses the dbo logon account, perform the following:

- 1 Click **Start**, point to **Programs, Administrative Tools** and click **Services**.
- 2 Right-click **SurfControl Web Filter Scheduler Service**, and click **Properties**.
- 3 Click the **Log On** tab.
- 4 Select **This account** and click **Browse**.
- 5 Type in the name of the dbo user name, and click **OK**.
- 6 Type the password in the **Password** box, and again in the **Confirm Password** box.
- 7 Click **Apply**, and **OK**.
- 8 In order for the changes to take effect, restart the Scheduler service.

Configuring Database permissions

There are various ways to configure database permissions. These are listed below from easiest to most difficult:

- Assign Database Reader and Database Writer Permissions to standard users.
- Assign permissions for running stored procedures.
- Change Database ownership.

These are discussed in more detail in the following sections:

Assigning Database Reader and Database Writer Permissions. To give permissions to other users to edit the Rules and/or Monitor Database using a trusted connection to the database, follow the steps below.



Caution: Having multiple copies of the Rules Administrator open and making changes will corrupt the database. SurfControl recommends that users should always co-ordinate their changes.

- 1 Open SQL Server Enterprise Manager.
 - 2 Navigate to your SQL Server in the directory tree, expand **Security** and click **Logins**.
 - 3 Right-click the user account that needs to be modified, and click **Properties**.
-

- 4 Click the **Database Access** tab.
- 5 In the **Specify which databases can be accessed by this login** section, make sure the SurfControl database is selected. In the bottom half of the screen, in the **Database Roles** section, ensure the public **db_datareader** and **db_datawriter** are selected.



Caution: Do not add roles in the **Permit in Database Role** section for **db_owner**. If you make this change, previous rules or categories will not be displayed under the **Where** objects of categories when that user attempts to access the Rules Administrator. Duplicate tables will also be created in the database associated with that user.

Assigning Permissions to Run Stored Procedures. Regardless of whether you choose Trusted or SQL Authentication, there are two ways to make authentication work successfully. The user account associated with the database is either:

- The database owner (the account used to create the database is automatically the database owner). Check this in the SQL Enterprise Manager by right clicking the database name, and selecting **Properties**.
OR
- The account has a server role of System Administrator (SA).



Note: The SA account and accounts that have local administrator privileges on the SQL Server (this usually includes Domain Administrators), have this server role because they are part of the Builtin\Administrators group. Make sure the Builtin\Administrators group has not been deleted from SQL.

However, some SQL Administrators do not like to assign this role because it is so powerful. Check the server role by following these steps:

- 1 Open SQL Enterprise Manager.
- 2 Expand the Security folder.
- 3 Select **Logins**.
- 4 Right-click the user account in question and select **Properties**.
- 5 Click the **Server Roles** tab.

Troubleshooting. If the user account is encountering permission problems, you may notice the following symptoms:

- Collected Data is not imported into the database - If the service is configured to be automatic in the monitor to database settings (in the Advanced tab of the Web Filter service settings), you can go into the SurfControl TMP directory with the service running, and see if the .tmp files are being successfully imported (and disappearing), or being renamed to .err extension which implies a permission problem.
- If database ownership is not assigned correctly, it can result in duplicate rules tables being created. Therefore, after making changes, try to open the Rules Administrator. Do you still see your rules or have they disappeared? Confirm this in the SQL Enterprise Manager by ensuring that you do not have duplicate tables.
- Running a Purge all on the database fails with an error message about being unable to truncate tables.

Changing Database Ownership. If you do not want to make the DBO account a System Administrator, you can change the database ownership by following these steps:

Perform the following steps to confirm database ownership:

- 1 Open SQL Enterprise Manager, right-click the Surfcontrol Database and select **Properties**.
- 2 Click the **General** tab and look for the owner.
 - If it is a Windows user account, use **Trusted Connections**.
 - If it is a SQL account, it needs to be the SQL account you plan to use.
 - If it displays a different SQL account (such as SA) then follow the next set of steps below to change the database owner:
 - i Firstly, remove the desired SQL account from any relationship with the database by clicking **Security > Logins**.
 - ii Right-click the account in the right-hand pane and select **Properties**.
 - iii Click the **Database Access** tab.
 - iv Clear the check box associated with the database in question and click **OK**.
 - v To change the database owner, open SQL Query Analyzer and point to the Surfcontrol database in question.
 - vi Type in the following command: `sp_changedbowner [sqlaccount]`
(where the value in [sqlaccount] is the account you want).
 - vii Press Enter.

The account should now be **dbowner**. If you see a message that says the account is associated with the database, follow the steps above to remove that user's association with the database.

SYSTEM CONFIGURATION

The following sections describe recommendations for configuring your Web Filtering policies, and settings for third party anti-virus software.

RULES CREATION

When your Web Filter and operating system settings are aligned for optimal filtering, you can implement your filtering policies. Web Filter policies are created in the Rules Administrator.

General guidelines for creating Web Filter Rules

For best results, make sure your rules adhere to the following guidelines:

- Remember that rules are processed from the top down in the Rule Panel list.
- Place rules to be applied to individuals or small groups near the top of the list.
- Use When and Allowance objects carefully. Use reports such as Protocol Data Analysis or Protocol Time Analysis, to narrow down who these rules should apply to before creating them. See the *SRC Administrators Guide* for more details.
- Keep the number of rules to a minimum to ensure Web Filter maximum efficiency.
- Create, test and activate any global rules you create before creating user or group specific rules.
- Ensure that only one person modifies rules at a time.
- Always add the Translators and Proxies object to a Disallow rule that is meant to block any specific categories.

EXCLUDE THE WEB FILTER DIRECTORY FROM REAL-TIME SCANNING

If your anti-virus software uses real-time virus scanning, SurfControl recommends that you configure your anti-virus software to exclude the following directories:

- The directory used to store flat files (by default, C:\Program Files\SurfControl\Web Filter\TMP). For information on how to store flat files in a different directory, refer to [KB1301](#).
- For local SQL installations, the SQL directory (by default, C:\Program Files\Microsoft SQL Server).

PERFORMANCE OPTIMIZATION

Below are some recommended general best practices for Web Filter, in order to maintain an ideal level of performance. This section covers the following areas:

- Monitor Settings
- Service Settings
- Maintenance Plan

MONITOR SETTINGS

There are certain monitor settings you can configure to disregard network traffic transmitted to and from your corporate Web sites or intranet, which you may not want to see reported or recorded in the Web Filter Manager.

Ignoring Web Sites

In the Web Filter Manager, you can enter the sites you want Web Filter to ignore (in most cases, your internal sites). This list supports domain names, numbers, and wild cards. For example, enter *.yourcompany.* to disregard all corporate sites. When a user accesses an ignored site, the data is not recorded in the database.

Follow the instructions below to configure your corporate Web sites to be ignored by the Web Filter service:

- 1 From the **Start** menu, point to **Programs, SurfControl Web Filter**, and click **SurfControl Web Filter Manager**.
- 2 From the Navigation panel, select **Monitored Data**, then click **Monitor Settings** in the Information Tasks pane.
- 3 In the **Unmonitored Destinations** tab, enter the Web sites you would like Web Filter to ignore, and click **OK**.
- 4 Click the **Update Confirmation** button at the top of the screen.

WEB FILTER SERVICE SETTINGS

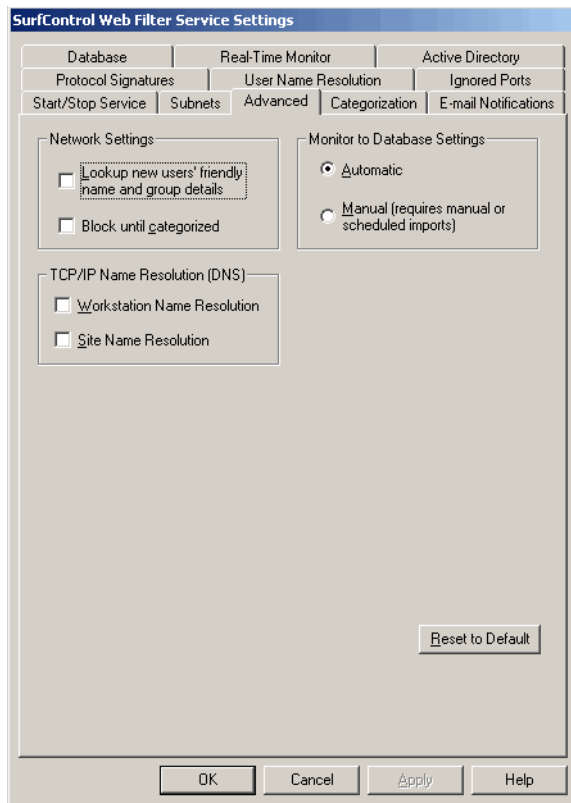
After the installation, SurfControl recommends configuring the following settings in the Web Filter Service Settings dialog box:

Advanced Settings

Configure the following settings in the **Advanced** tab (Figure 2-3):

- Under **Monitor to Database Settings**, select **Automatic**. This enables SurfControl Web Filter to write automatically to flat file before saving the data to the database.
- Under **TCP/IP Name Resolution (DNS)**, make sure that **Workstation Name Resolution** and **Site Name Resolution** are not selected.

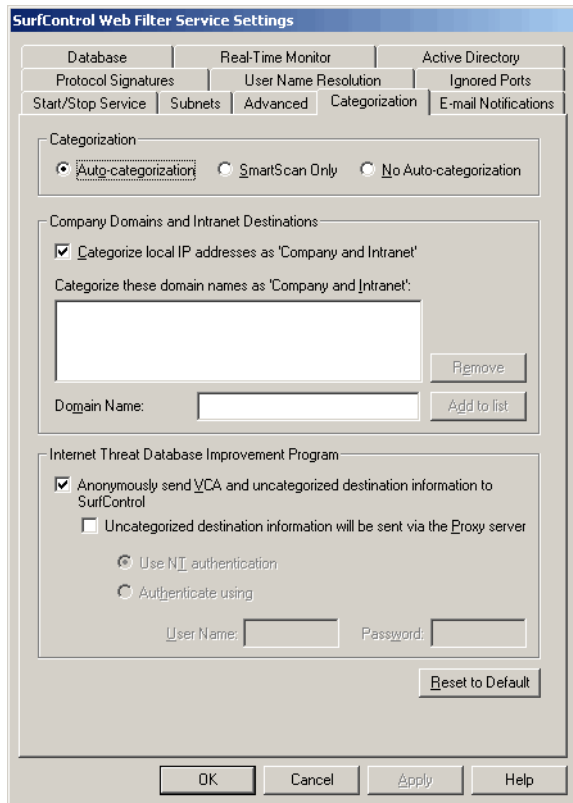
Figure 2-3 Advanced Tab



Categorization Settings

In the **Categorization** tab, ensure that **Auto-Categorization** is selected, as shown in [Figure 2-4](#):

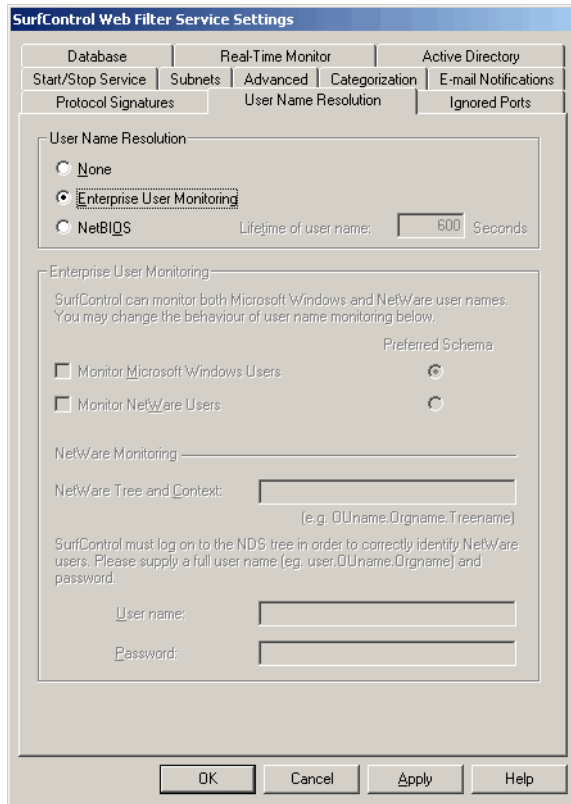
Figure 2-4 Categorization tab



User Name Resolution Settings

In the **User Name Resolution** tab (Figure 2-5), select **Enterprise User Monitoring** if you are using Enterprise User Monitoring (EUM) to resolve user names. If you do not use EUM, select **None**.

Figure 2-5 User Name Resolution tab



MAINTENANCE PLAN

In order to maintain SurfControl Web Filter at its optimum level of performance, SurfControl recommends that you execute the following tasks on a regular basis.

These specifications and configuration guidelines are for environments of over 1,000 users. Smaller environments may perform these tasks less frequently.

Table 2-2 Maintenance Plan

Action	Servers	Frequency
Update Category List	Web Filter servers	Daily
Export Rules (from the Rules Administrator)	SQL Server	Monthly
Archive Web Filter Database	SQL Server	Monthly
Purge Web Filter Database	SQL Server	Monthly
Compact Web Filter Database	SQL Server	Monthly (to occur after the purge)



Note: Before you purge the Monitor database, make an archive copy of the database.

2

GENERAL BEST PRACTICES *Performance Optimization*

Best Practices for Web Filter for Windows

Introductionpage 20

System Configurationpage 21

Performance Optimizationpage 24

INTRODUCTION

The purpose of this chapter is to provide best practice recommendations for the fine tuning and configuration of SurfControl Web Filter for Windows. This guide provides specific recommendations for:

- Network Interface Card (NIC) configuration.
- Service settings.
- Monitor settings.

For information on network placement, monitoring users, and deployment scenarios, consult the *Web Filter for Windows Deployment Guide*. For details on monitoring by user name using Enterprise User Monitoring, refer to the *EUM Deployment Guide*.

SYSTEM CONFIGURATION

This section contains information about how to configure the network interface cards (NICs) on the Web Filter server, and briefly discusses NIC teaming.

NIC CONFIGURATION

When you install SurfControl Web Filter, you must configure one or more NICs on the Web Filter server. In order for SurfControl to analyze data passing through a switch. Your switch must support uni- or bi-directional spans. A switch that supports bi-directional spans allows the SurfControl server to receive and send data through the spanned port. If your switch supports bi-directional spans, the SurfControl server requires a minimum of one NIC.

However, a switch that only supports uni-directional spans allows only the recipient server to receive data from the spanned port. Therefore, with a uni-directional span, SurfControl is unable to block Internet access using a single NIC. If your switch supports uni-directional spans, the SurfControl server requires at least two NICs.

In these cases, SurfControl recommends that you install Web Filter onto a server with two NICs. If you are installing two NICs, one (N1) is the monitoring NIC, and the other (N2) is the blocking NIC.

The monitoring NIC (N1) does not need an IP address. Unbind the TCP/IP stack. During installation, the Install Shield Wizard prompts you to bind a NIC to the Web Filter service; choose this NIC. This NIC is responsible for sniffing network traffic. The blocking NIC (N2) requires an IP address. Make sure the TCP/IP stack is bound to the NIC. This NIC is responsible for blocking Internet access, EUM activity, DNS queries, and writing to the database.



Note: The blocking NIC (N2) and its source port must be a member of the same VLAN as the monitoring NIC (N1). On a Web Filter for Windows v5.5 SP2 installation, SurfControl recommends increasing the number of receive buffers on your installed NICs.

Testing has shown that if the number of receive buffers on the NIC are increased, the number of dropped packets is reduced. For more information, see [KB2259](#).

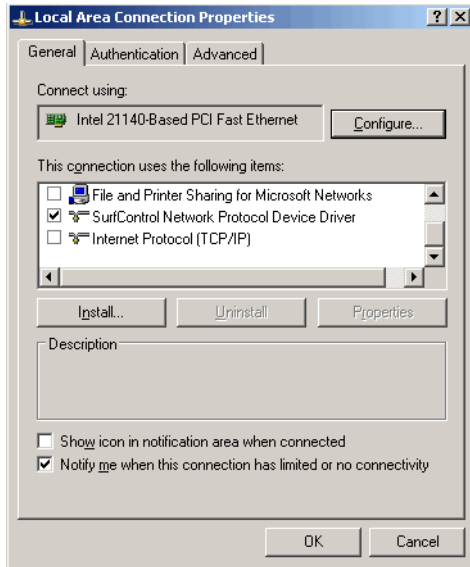
NIC configuration consists of the following steps:

- Configuring the monitoring NIC
- Configuring the blocking NIC

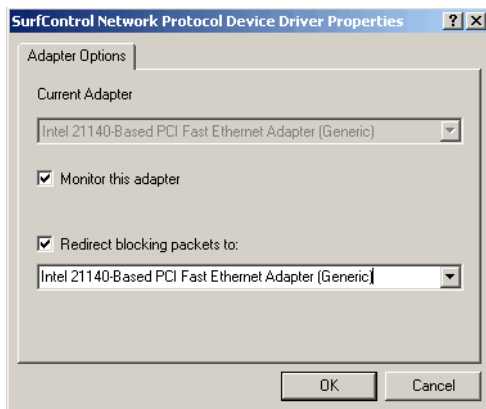
Configuring the monitoring NIC

To configure the monitoring NIC, perform the following:

- 1 Open the dialog box for the monitoring NIC (this is the NIC you bound to the Web Filter service):



- 2 Clear all components (including **Internet Protocol**), except **SurfControl Network Protocol Device Driver**:
- 3 Open the dialog box for the SurfControl Network Protocol Device Driver:

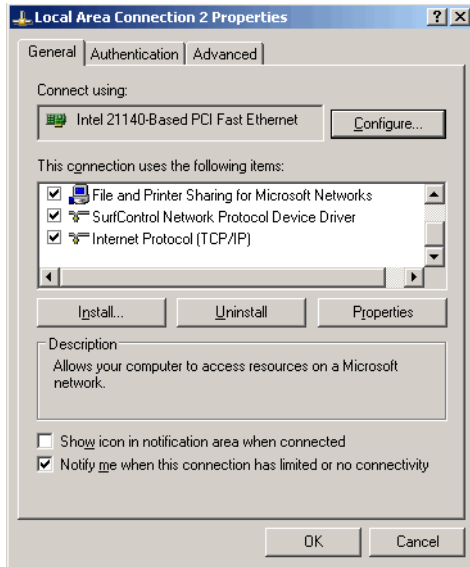


- 4 Make sure **Monitor this adapter** is selected; this indicates that this NIC is responsible for monitoring.
- 5 Select **Redirect blocking packets to**, and select the second NIC. The second NIC is now responsible for blocking.
- 6 Click **OK**.

Configuring the blocking NIC

To configure the blocking NIC, perform the following:

- 1 Open the dialog box for the blocking NIC:



- 2 Make sure **Internet Protocol** is selected. This NIC is responsible for blocking, for performing all DNS queries, for transferring data to the database, and for receiving EUM data.
- 3 Click **OK**.

NIC TEAMING

Teaming Network cards on a single server is a configuration that is supported by Web Filter v5.5 SP2. Currently, both Broadcom and Intel NICs have been tested and are known to work with Web Filter on Windows 2000 and 2003 servers. For more information and configuration recommendations, please refer to KB articles [KB2157](#) and [KB2258](#).

PERFORMANCE OPTIMIZATION

This section contains information about how to achieve optimal performance from your Web Filter installation. This includes making changes to the following areas of the product:

- Monitor settings
- Service Settings
- Subnet monitoring

MONITOR SETTINGS

You can perform additional modifications in the Web Filter Monitor settings, as described in the following sections:

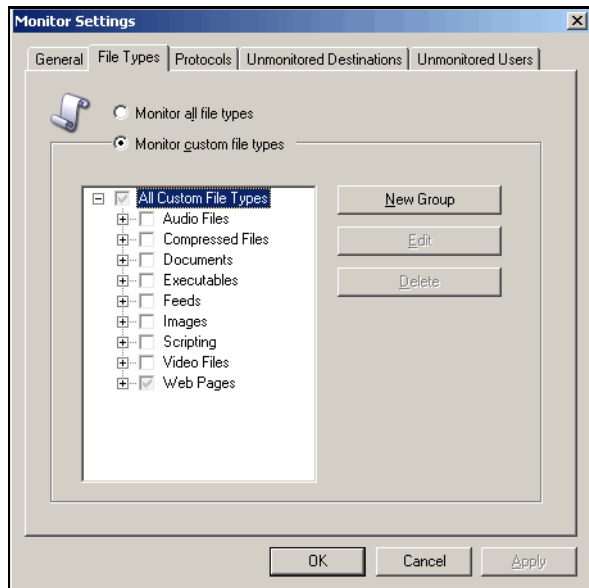
Monitoring Levels

By default, Web Filter is configured to monitor Web Pages only, rather than the complete range of available file types, and also does not record the full page level of URL requests. This increases the overall efficiency of the system and is recommended by SurfControl.

File Types. To access Web Filter's monitored file types:

- 1 In the Web Filter Manager, click **Monitored Data** in the Navigation panel, click **Monitor Settings** in the Information panel, and click the **File Types** tab.
- 2 Select or clear file types to be monitored.
- 3 Click **OK**.

Figure 3-1 Monitor Settings - File Types

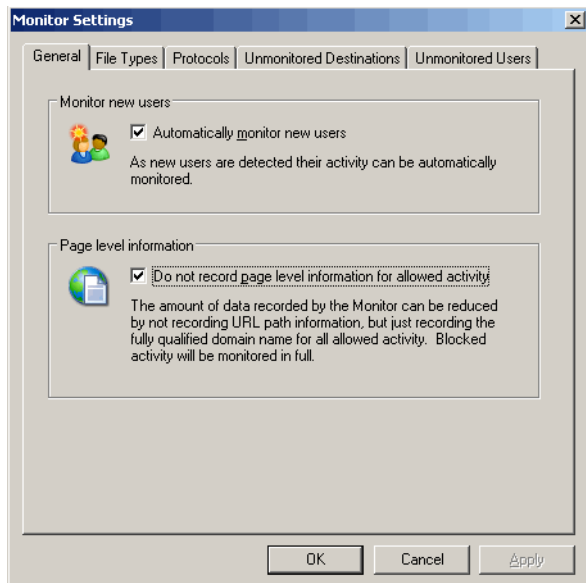


Page Level Information. After installing Web Filter, Page level monitoring is automatically selected so that it does not record the full URL path of allowed Web pages (see [Figure 3-2](#)). However, any URLs for blocked Web pages are recorded in full, regardless of this setting. This means that only the fully qualified domain name of the URL is written to the database, and may result in less available information to view or report on.

To access the Page level information setting:

- 1 In the Web Filter Manager, click **Monitored Data** in the Navigation panel, click **Monitor Settings** in the Information panel, and click the **General** tab.
- 2 Select or clear the **Do not record page level information for allowed activity** check box depending on the desired amount of recorded information required.
- 3 Click **OK**.

Figure 3-2 Monitor Settings - General



Monitored Protocols

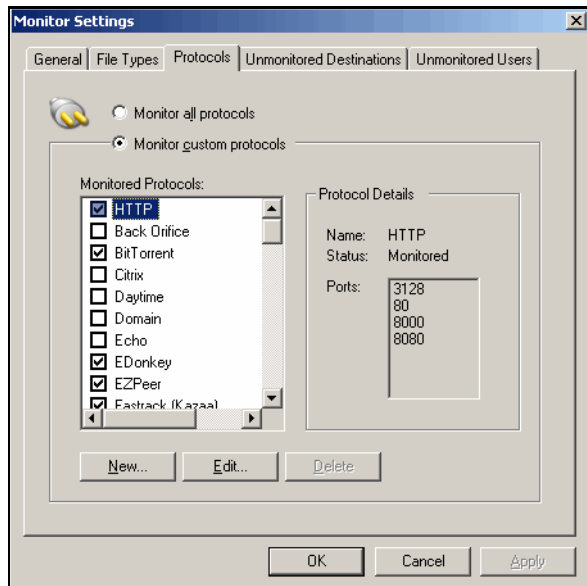
Web Filter has the ability to monitor a variety of protocols, and is configured to monitor over twenty by default. Deciding which protocols to monitor is dependent on the following:

- If protocol signature scanning is disabled, overall efficiency can be increased by monitoring web traffic only. In this case, the recommended configuration is to only select FTP, HTTP and HTTPS in the list, and then navigate to the Ignored Ports tab and ensure these are the only ports the Web Filter service will monitor. Refer to [Ignored Ports on page 28](#) for more details.
- If protocol signature scanning is enabled, it is recommended that the default set of monitored Web, IM and P2P protocols are left unchanged in the Monitored Protocols list.

To access monitored protocols:

- 1 In the Web Filter Manager, click **Monitored Data** in the Navigation panel, and click **Monitor Settings** in the Information panel.
- 2 Click the **Protocols** tab.
- 3 Click **Monitor all protocols** to automatically select all protocols in the list, or click **Monitor custom protocols** and individually select protocols to monitor.
- 4 Click **OK**.

Figure 3-3 Monitor Settings - Protocols



WEB FILTER SERVICE SETTINGS

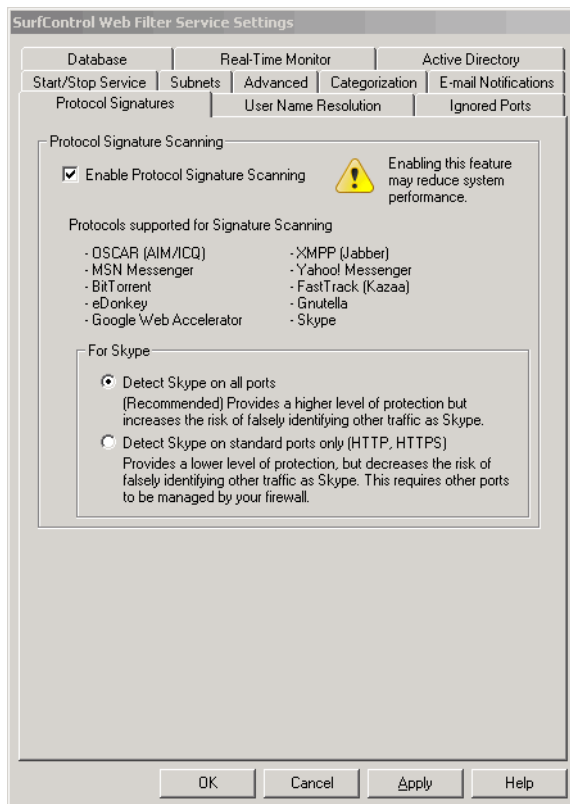
After the installation, SurfControl recommends configuring the following settings in the Web Filter Service Settings dialog box:

Protocol Signature Scanning Settings

Web Filter for Windows has the ability to monitor and filter the Skype protocol by signature. If you have enabled Protocol Signature scanning in the **Protocol Signatures** tab (Figure 3-4), ensure **Detect Skype on all ports** is selected (this option is selected by default after installation). This option is recommended by SurfControl and provides a higher level of protection, but can increase the risk of falsely identifying other traffic as Skype.

You can select **Detect Skype on standard ports only (HTTP, HTTPS)** to detect Skype on ports 80 and 443 only. However, this scanning method provides a lower level of protection, but decreases the risk of falsely identifying other traffic as Skype. To identify all possible Skype connections, you must ensure other ports are managed by your firewall.

Figure 3-4 Protocol Signatures tab



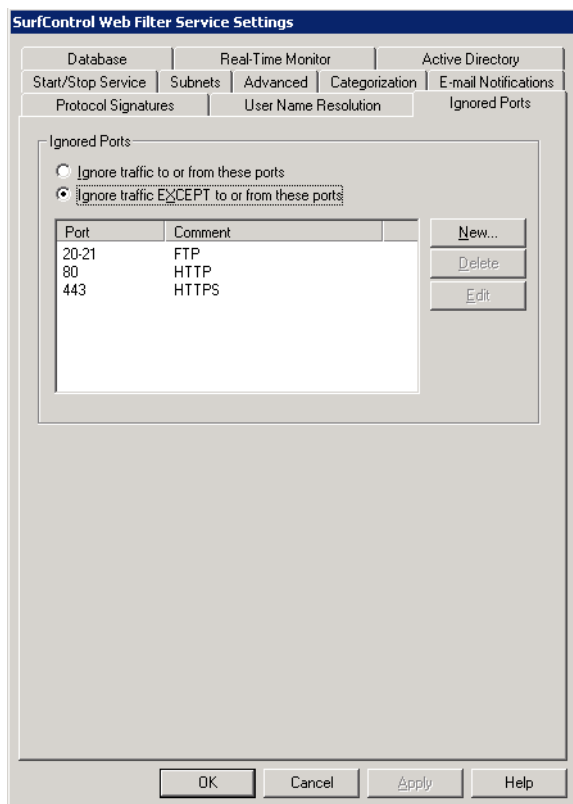
IGNORED PORTS

Web Filter detects all network traffic through the driver and passes relevant information to the Web Filter service, even though certain protocols and ports may not be set up to be monitored in the Web Filter monitor settings. To improve the performance of Web Filter, network ports can be identified for the driver to ignore in order to ensure that network activity on those ports is not passed to the Web Filter service.

To effectively control the levels of network traffic that the Web Filter service monitors, use the Ignored Ports tab in the Service settings. SurfControl recommends a best practice of configuring this feature to monitor and filter network ports that you are interested in. However, this is dependent on whether you are also utilizing protocol signature scanning. For example:

- If you are not using protocol signature scanning, only add Web and FTP ports to the list to be monitored. To do this, perform the following:
 - i Select **Ignore traffic EXCEPT to or from these ports**.
 - ii Click **New**.
 - iii Enter a port range of 20-21 for FTP and click **OK**.
 - iv Repeat this process by entering single port numbers of 80 for HTTP, and 443 for HTTPS.
 - v The ports list should be populated with the data as illustrated in [Figure 3-5](#). Click **OK**. (You will have to restart the Web Filter service, if the service is running).

Figure 3-5 Ignored Ports



- If protocol signature scanning is enabled, all network traffic will be scanned for protocol signatures and if a signature is found, Web Filter will then determine if the port should be ignored. In this situation, it is more effective to select **Ignore traffic to or from these ports** and enter the port numbers you are not interested in monitoring or filtering.

SUBNET MONITORING

If you have installed Web Filter in a network location where it can monitor internal traffic, such as Web services, FTP servers, or e-mail servers, you should ensure traffic being transmitted to your internal subnets is ignored by Web Filter. This will help to improve network performance by reducing the load on the Web Filter service.

Follow the instructions below to configure internal subnets to be ignored by the Web Filter service:

- 1 Stop the Web Filter service.
- 2 Launch the Web Filter Service Settings.
- 3 Click the **Subnets** tab.
- 4 In the **Ignore Subnets** section, click **Add**.
- 5 In the **Subnet** dialog box, enter the IP Address and Subnet Mask you want Web Filter to ignore.
- 6 Click **OK**.
- 7 On the Web Filter Service Settings dialog box, click **OK**.
- 8 Start the Web Filter service.

Repeat this process for all your internal IP Address ranges.

Best Practices for Web Filter for ISA Server

Introduction	page 32
System Configuration	page 34
Deployment	page 41

INTRODUCTION

SurfControl's Web Filter for Microsoft Internet and Security Acceleration (ISA) Server enables customers to significantly improve the security of mission critical information, and maximize IT resources through a powerful "defense in depth" approach. The purpose of this chapter is to provide best practice recommendations for the fine tuning and configuration of SurfControl Web Filter for ISA Server. This chapter provides specific recommendations for:

- System configuration including:
 - Content Scanning
 - Rules creation
 - Deployment

For more information about Microsoft ISA Server 2004 and 2006, refer to the following Microsoft ISA Server TechNet web sites:

- <http://www.microsoft.com/technet/isa/2004/default.aspx>
- <http://www.microsoft.com/technet/isa/2006/default.aspx>

Because your ISA Server is a proxy through which your enterprise accesses the Internet, it is a potential bottleneck. To help prevent this, refer to the following Best Practices for Performance articles:

- <http://www.microsoft.com/technet/isa/2004/plan/bestpractices.aspx>
- http://www.microsoft.com/technet/isa/2006/perf_bp.aspx

After installation, complete the modifications discussed in this chapter to enable optimal Web Filter performance.

ENHANCING ISA SERVER SECURITY WITH WEB FILTER

During a Web Filter for Microsoft ISA Server installation, an Internet Server Application Program Interface (ISAPI) filter is added to the ISA Server configuration. While ISA Server can control access to ports and protocols for users and select sites, the ISAPI filter delivers SurfControl's industry-leading categorization and rules engine for more granular and comprehensive access control than ISA Server can provide by itself.

SurfControl Web Filter takes ISA firewall security to the next level with these features:

- **Real-time Monitoring.** Web Filter makes it easier to keep tabs on user activity by filtering out extraneous data and provides the ability to shut down a user in real-time from the console.
- **Time and Bandwidth Control.** Web Filter provides added value by enabling you to control how much time a user is allowed to spend on the internet and how much and what type of content a user can transfer over the internet.
- **Internet Threat Database.** Instead of having to manually enter URLs and domain name sets, Web Filter's Internet Threat Database does it all for you. The Internet Threat Database not only contains millions of undesirable web sites, but categorizes them so that you can control access by site category, and is updated on a daily basis. Additionally, Web Filter uses artificial intelligence (AI) technologies - the Virtual Control Agent (VCA) - to evaluate the sites that users visit in real-time, and blocks the sites

dynamically if they meet the VCA's specifications. You can even review the sites captured by the VCA by running a report of the activity.

- **Notification.** Web Filter sets up automatic e-mail notification to alert network security administrators, compliance managers, or others of policy violations.
- **Mobile Filter.** This add-on to Web Filter allows you to install an agent on managed devices (such as corporate laptops) in order to enforce the same web usage policies you have in place for corporate network devices. You can also create a custom ruleset that applies only to these mobile clients.

SYSTEM CONFIGURATION

When you set up Web Filter's system configuration enhancements for ISA Server, SurfControl recommends that you implement changes in the following areas:

- Username and Domain Name Enumeration.
- Creating Rules.
- Content Scanning.
- Creating ISA Firewall Policy Access Rules.
- Deployment.

This section covers these areas in further detail.

USERNAME AND DOMAIN NAME ENUMERATION

Web Filter for ISA server must be able to enumerate users on the network for monitoring and reporting purposes. The enumeration process involves finding the correct domain controllers to query, authenticating to these if required by the security policy, and then querying them to obtain the user names belonging to groups used in rules. This process is dependent on the following:

Web Filter's ability to access the associated domain and user names from the domain controllers.

ISA Server's ability to gather those domain and user names.

Configuring enumeration of usernames and domain names

To configure Web Filter and ISA Server to be able to enumerate users and domains:

- 1 Enable client connections to use the Web Proxy filter by configuring the browser's LAN settings to use a proxy server, ensuring that **Automatically detect settings** is not selected.
- 2 Enable username resolution by either ensuring all users authenticate when connecting to the ISA server, or adding users and/or Active Directory group domain objects to an allow access rule.

To configure all users to authenticate:

- i In the ISA server management console, click **Firewall Policy** in the server tree.
- ii Click the **Toolbox** tab and click the **Network Objects** rule element.
- iii In the list, expand **Networks**, right-click **Internal** and click **Properties**.
- iv Click the **Web Proxy** tab and click **Authentication**.
- v Select **Require all users to authenticate**. If a different domain is responsible for authentication, click **Select Domain** to enter a different domain name.
- vi Click **OK** in the **Authentication** dialog box.
- vii Click **OK** in the **Internal Properties** dialog box.
- viii Click **Apply** to save the changes.

To add users to an allow access rule:

- i In the ISA server management console, click **Firewall Policy** in the server tree.

- ii Right-click the allow access rule and click **Properties**.
 - iii Click the **Users** tab, click **All Users** and click **Remove**.
 - iv Click **Add**, click **All Authenticated users** and click **Add**.
 - v Click **Close** in the **Add Users** dialog box.
 - vi Click **OK** in the **Allow Properties** dialog box.
 - vii Click **Apply** to save the changes.
- 3 Enable NETBIOS over IP on the internal NIC:
 - i In the **Local Area Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and click **Properties**.
 - ii On the **General** tab, click **Advanced**.
 - iii Click the **WINS** tab, and select **Enable NetBIOS over TCP/IP**.
 - iv Click **OK** in the **Advanced TCP/IP Settings** dialog box.
 - v Click **OK**.
 - vi Click **Close**.
- 4 Configure all client browser settings which use a GPO Policy to point to the ISA Server as a web proxy.
- 5 Configure the SurfControl Web Filter service to log on with a domain Admin account which is able to enumerate users and domains.

RULES CREATION

Now that your Web Filter and ISA Server system settings are aligned for optimal filtering, you can implement your filtering policies. Web Filter policies are created in the Rules Administrator.

ISA Rules Considerations

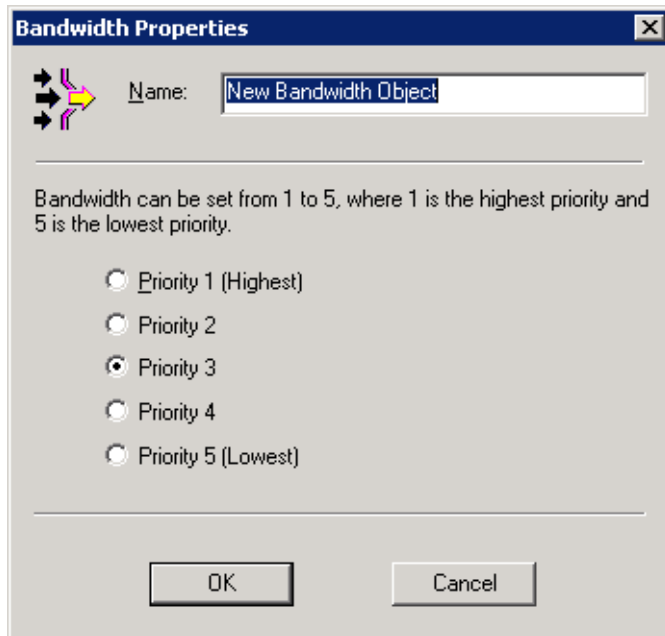
While very similar in functionality to the version of the Rules Administrator that is included with Web Filter for Windows (standalone), the version of the Rules Administrator that is included with Web Filter for ISA includes the following changes and additions:

Protocol support. For ISA Server 2000, when constructing rules with the Rules Administrator, only the FTP, HTTP, and HTTPS protocols are available. (ISA Server 2004 and 2006 support the same set of protocols as the Web Filter for Windows product).

Override Rules. In addition to the standard Allow, Disallow, and Allowance rules, Web Filter for ISA Server adds the Override rule. Override rules block initial access to a network resource but allow the user to override the block. An Override rule serves to notify users of potential policy violations while allowing access to incorrectly blocked material such as a miscategorization without explicit intervention.

Bandwidth throttling. Web Filter for ISA adds a Bandwidth tab to the Rules Administrator interface. This seamlessly integrates the bandwidth throttling capabilities of ISA Server to produce a non-stop filtering and blocking solution. A bandwidth object, pictured below, consists of a list of throughput options from one to five, with one being the most permissive and five being the most restrictive. By specifying bandwidth properties, work related material can be configured to have a higher priority, while personal network traffic is assigned a lower priority. This speeds access for work-related material while allowing access for personal traffic, albeit more slowly.

Figure 4-1 Bandwidth Properties



CONTENT SCANNING

Web Filter for ISA has an optional Anti-Virus Agent (AVA) component, which works in conjunction with Microsoft ISA Server to virus scan HTTP traffic. It scans all Web traffic for known viruses and can also be configured to use heuristic analysis to detect unknown viruses. The comprehensive inspection process used to identify virus content may have an impact on the performance of Web Filter. To maintain effective performance:

- Ensure you have the minimum hardware required for when the Anti-Virus Agent is enabled (*see the ISA Starter Guide*)
- Use the AVA Whitelist feature.

Configuring the AVA Whitelist

Adding Web site addresses to a whitelist enables you to prevent certain URLs from being scanned by the Anti-Virus Agent. The whitelist is stored in the Windows Registry and requires the URLs to be entered manually.

Entries in the whitelist inherit sub-domains automatically. For example, if the connections you want to ignore are for 'windowsupdate.com' (regardless of sub-domain), then the entry should be added as 'windowsupdate.com'. To prevent connections to 'www.windowsupdate.com' from being scanned, then the entry should be added as 'www.windowsupdate.com', however this will only ignore connections to 'www.windowsupdate.com' and not 'downloads.windowsupdate.com'.

To add URLs to the whitelist, perform the following:

- 1 To stop the Web Filter service, right-click the SurfControl icon in the notification area, and then click **Stop Web Filter Service**.
- 2 To open Services click **Start**, point to **Programs, Administrative Tools** and click **Services**. Stop the Microsoft ISA firewall service.
- 3 Launch the registry by clicking **Start** and **Run**. Type in **regedit** and click **OK**.
- 4 Navigate to [HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControl Scout\Content\AVA]
- 5 Right-click the **WhiteList Sites** key, and click **Modify**.
- 6 Enter the required URLs into the **Value data** field.
- 7 Click **OK**.
- 8 In Services, start the Microsoft ISA firewall service.
- 9 Right-click the SurfControl icon in the notification area, and click **Start Web Filter Service**.

CREATING ISA FIREWALL POLICY ACCESS RULES

Microsoft ISA Server blocks all client access unless it is explicitly allowed. Before SurfControl Web Filter can be used, you must create firewall policy rules in ISA Server 2004 or 2006 which enable client access to the Internet.

ISA Server's performance is related to the type of information it requires to evaluate the rules. Because rules are evaluated in order, it is recommended that you place rules that are processed quickly at the top of the rule list, if it doesn't interfere with the behavior of the firewall policy you've designed. Performance is subsequently enhanced because if a request matches a rule that is high in the order, ISA Server does not have to compare the request to rules that might take longer to process. For more information about ISA Server rules best practices, see the following Best Practices Firewall Policy articles:

- http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/firewall_policy.msp
- http://www.microsoft.com/technet/isa/2006/BP_Firewall_Policy/default.msp?mfr=true

On a Web Filter installation for ISA Server 2004 or 2006 installation, you must create ISA firewall policy access rules to enable several Web Filter features:

- Virtual Control Agent (VCA)
- Remote Administration Client
- Remote Access to SurfControl Report Central (SRC)

These are discussed further in the following sections:

Virtual Control Agent (VCA)

The VCA is a Web Filter component that runs as a service, and dynamically categorizes new web sites which are not contained in the SurfControl Internet Threat Database. Whenever a user browses to a site that is not categorized, the VCA performs a 10 page deep scan of the site's HTML, and uses artificial intelligence to make the most appropriate categorization of that site.

Configuring a VCA Firewall Policy Access Rule. If you are using the VCA, in addition to configuring your LAN settings to use a proxy server, you must enable the VCA spiders to gain outbound access to the internet when installed locally. To configure the spider settings:

- 1 Make sure that the ISA server web browser can access the internet.
- 2 From the **Start** menu, select **Programs, SurfControl Web Filter, Virtual Control Agent**.
- 3 Click the **Settings** tab. In the Spider Settings field, the path to the VCA spider files is displayed.
- 4 Select the **Impersonate Internet Explorer** check box.
- 5 Select the **Use Proxy** check box.
- 6 If your proxy allows for integrated authentication, select the **Use NT Authentication** check box, (otherwise, you must supply a user name and password for VCA to present to the proxy). Click **OK**.

To configure LAN Settings:

- 1 Open a browser window. From the **Tools** menu, click **Internet Options**.
- 2 Open **Connections, LAN Settings**. (Do not enter anything in the Automatic Configuration section).
- 3 Select the **Use a proxy server for your LAN** check box.
- 4 Select the **Bypass proxy server for local addresses** check box and click **OK**.

The VCA spiders should now have outbound access to the Internet. If they do not, a firewall policy rule needs to be created to allow ISA (Localhost) to External (anywhere). This does not usually need to be set, but security hardened ISA servers are generally not allowed Internet access by the local host.

The Remote Administration Client

The Web Filter Remote Administrator is a client that is installed on the desktop to allow you to create reports, design or edit rules, and view the database without being physically present at the server.

Configuring a Remote Administration Firewall Policy Access Rule. In order to allow the Remote Administration client to access Web Filter on ISA Server, you must create an ISA firewall policy access rule to allow the Remote Administration Client to access the Web Filter server:

- 1 Begin a typical SurfControl Web Filter installation.
- 2 When prompted, choose **Remote Administration**.
- 3 Proceed with the installation and choose whether your connection is to a **Pass By/Proxy** or to a **Microsoft ISA Server**.
- 4 Choose **Web Filter ISA Server**.
- 5 Enter your database connection credentials.

- 6 Complete the installation.
- 7 Open the Rules Administrator from the client.
- 8 Click **Connect to Collector**.
- 9 Enter the name of the ISA Server on which Web Filter is installed.
- 10 Make sure that you have enabled NETBIOS and RPC services on both the remote and the local server.
- 11 On the ISA Server, create a New Access Rule and assign it a name.
- 12 Change to **Allow**.
- 13 Change to **Selected Protocols**, and click **Add**.
- 14 Click **New > Protocol** and assign the protocol a name.
- 15 Click **New**.
- 16 Change the protocol type to **UDP**.
- 17 Direction: **Send**.
- 18 Port range: **1024 - 65535**.
- 19 Do not add a secondary connection.
- 20 Add the protocol created in steps 13 - 19.
- 21 Source: **Remote Management Computer(s) and Localhost**.



Note: If the workstation you plan to use is not a part of the RMC group, add a Host object to define it.

- 22 Destination: **Remote Management Computer(s) and Localhost**.
- 23 Optional: For User Sets, select **All Users** or specify only those users that are allowed to use the Web Filter Real-Time Monitor.
- 24 Start the Web Filter service. You should now be able to connect with the Real-Time Monitor.

After configuring the firewall policy access rule, ensure that file and print sharing is enabled on the ISA server(s).

Remote Access to SurfControl Report Central (SRC)

SurfControl Report Central (SRC) is Web Filter's reporting module that allows you to run a wide range of reports through a web interface.

Configuring a Remote SRC Access Firewall Policy Rule. Although you can install SRC on any server, if you install it on the ISA Server, you must create a user-defined port and then add it to a new or existing Allow rule to enable remote access to SRC:

- 1 Open the ISA Management Console.
- 2 Highlight **Firewall Policy**.
- 3 Click the **Toolbox** tab to the right of the management console.

- 4 In the list of protocols, highlight the **User-Defined** folder.
- 5 Click **New Object**.
- 6 For Protocol type, choose **TCP**.
- 7 For Direction, type: **Outbound**.
- 8 For From, type: **8888**.
- 9 For To, type: **8888**.
- 10 Do not add a secondary connection.
- 11 Click **Next**.
- 12 Click **Finish**. The object is now ready to be applied to a new or existing Allow rule. The Allow rule must be one that affects the internal clients you've designated to access SRC remotely.
- 13 In the **From** box, add the name of the internal object that you want to allow.
- 14 In the **To** box, add localhost (for example, the name of the ISA server).



Note: The firewall policy rule outlined above, sets remote access for the HTTP connection to SRC. If you want to use the HTTPS connection, you need to substitute port number 8888 with 8443.

DEPLOYMENT

You can install SurfControl on a single ISA Server or in multi-server arrays. (An array is a method for storing information on multiple devices). In an ISA 2004 Standard Edition installation, Web Filter is installed on a single ISA Server connected to one or more clients. In an ISA 2004 Enterprise Edition environment, Web Filter is installed on multiple servers.

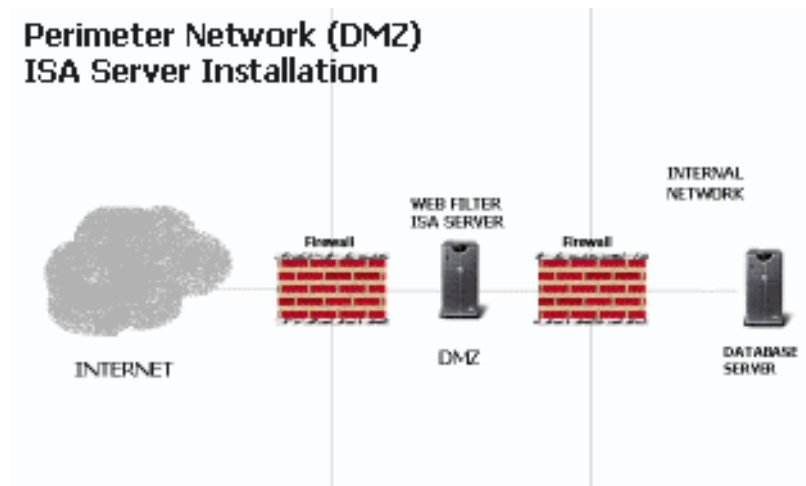
An array is used for the following purposes:

- Redundancy
- Scalability
- Load balancing

Arrays are also recommended in situations where you have multiple Internet portals and want to have the same ISA rules implemented on each portal.

In a perimeter network (DMZ) installation, Web Filter is installed on one or more ISA 2004 Servers located between a perimeter firewall and an internal firewall as shown in the figure below:

Figure 4-2 ISA Server in the DMZ



DEPLOYMENT RECOMMENDATIONS

SurfControl recommends the following when deploying Web Filter for ISA Server:

- If Web Filter for ISA Server is used as a proxy, it does not need to be installed in a specific location in the LAN. However, if it is used as a firewall, consult the Microsoft ISA templates for network placement recommendations.
- Use a firewall to deny HTTP traffic from all IP addresses except for the ISA server.
- Firewall clients should be configured so that the browser uses a proxy service.

DMZ CONSIDERATIONS

SurfControl recommends the following when deploying Web Filter for ISA Server in the DMZ:

- If the ISA Server is part of the DMZ domain, Web Filter for ISA Server should be a member of the domain that users log into.
- Is there a one-way or two-way trust relationship between the Web Filter ISA Server and the corporate domains? Two-way trust relationships are very reliable. One-way trusts will cause problems if configured to trust the wrong way.
- Are there multiple domain controllers? The ports required to query the domain controllers should already be open via System Policy LDAP to localhost. If not, check to see which ports if any, must be opened for this purpose.

When Web Filter for ISA is deployed in a DMZ, it may be unable to query the domain controllers for a variety of reasons:

- It cannot resolve the IP addresses of the domain controllers.
- It is unable to authenticate to the domain controllers.
- Access is blocked by a firewall, preventing Web Filter from enumerating groups using NT objects.

To Resolve a domain controller name resolution issue:

- Add an entry to the LMHosts file on the Web Filter server(s) for the domain controllers. See the following Microsoft KB article for more information: <http://support.microsoft.com/Default.aspx?kbid=180094>
- Enable NETBIOS over IP on the Web Filter server(s).

To resolve an authentication issue:

- Use a Local Admin account to log into the Web Filter server(s). This account should also be a member of the domain administrators group in the DMZ, and an account with the same name and password should exist in the corporate domain. Use this logon account for the Web Filter services also.

To resolve a firewall access issue:

- Set up a child domain with a trust relationship between the domain controllers with Web Filter for ISA a member of the child domain.
- Open up ports on the internal firewall where necessary.

4

BEST PRACTICES FOR WEB FILTER FOR ISA SERVER *Deployment*

Appendix

Comments on this Guide?	page 45
Technical Support	page 46
SurfControl Sales	page 47

COMMENTS ON THIS GUIDE?

You can view updated documentation and support information at <http://www.surfcontrol.com>

Was this guide helpful? E-mail us at documentation@surfcontrol.com to suggest changes or make a correction.

Version 5.5

August 2007

TECHNICAL SUPPORT

For the latest support information on SurfControl products, visit <http://www.surfcontrol.com>

- Search our Knowledge Base - Our searchable database is constantly being updated and may be the quickest means to answering your questions regarding your SurfControl product.
- Online Support - If you do not find a satisfactory answer to your question in the documentation or the Knowledge base, you can fill out an Online Support Request Form.
- Telephone Support - If you would like to speak to a Technical Support Representative, our excellent SurfControl Technical Support is just a phone call away.

SURFCONTROL SALES

For product and pricing information, or to place an order, contact SurfControl. To find your nearest SurfControl office, please visit our web site: <http://www.surfcontrol.com>