



Deploying SurfControl Web Filter for Windows in a Cisco PIX Environment

rev. 1.0, January 2005

ACKNOWLEDGEMENTS

SurfControl wishes to acknowledge the following people for their contributions to this white paper:

Role	Name
Technical Contributor	Scott Stanney, Systems Engineer
Editor	Karen Hepner, Technical Writer
Author	Shawn Titus, Technical Communications Manager

NOTICE

© 2005 SurfControl. All rights reserved. SurfControl, SurfControl E-mail Filter, SurfControl Web Filter, 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 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 white paper provides a general foundation for implementing SurfControl Web Filter for Microsoft Windows in a Cisco PIX environment.

Instead of directly integrating with PIX, Web Filter utilizes pass-by filtering technology on a stand-alone server. This implementation off-loads the intense web filtering processes from the PIX system, allowing the firewall to perform more efficiently. Furthermore, pass-by technology eliminates the possibility for interruption of Internet access (a common issue with integrated solutions).

Additional advantages include:

- Transparency to the end-user.
- Open failure.
- The ability to monitor all TCP/IP-based protocols.

This white paper identifies pre-installation considerations and common deployment scenarios, covering the following topics:

- Network placement.
- Database considerations.
- Functional components
- Deployment scenarios.

NETWORK PLACEMENT

Web Filter uses a sniffer engine to monitor Internet traffic; therefore, placement within the network is critical. Web Filter can only monitor and block Internet traffic that passes by the server. In most cases, you should deploy Web Filter at the Internet gateway, as all outbound requests will pass through the gateway.

In order for Web Filter to access the data it's filtering, the switch it connects to must support the SPANning of ports. Specifically, you must perform a bi-directional SPAN the PIX Firewall port. This configuration ensures that the port on which Web Filter resides receives copies of all packets sent to or from the PIX Firewall.

If your network has multiple Internet gateways, you will need to deploy at least one Web Filter server at each gateway. In general, a single Web Filter server can monitor and block at least 10,000 users in an environment where you are monitoring HTTP, HTTPS, and FTP.¹

¹ The number of users that a single Web Filter server can monitor is dependent on the number of protocols you decide to monitor and the amount of traffic the users generate.

-
-
- **Database Considerations**

Figure 2 shows an example of Web Filter placement within a network.

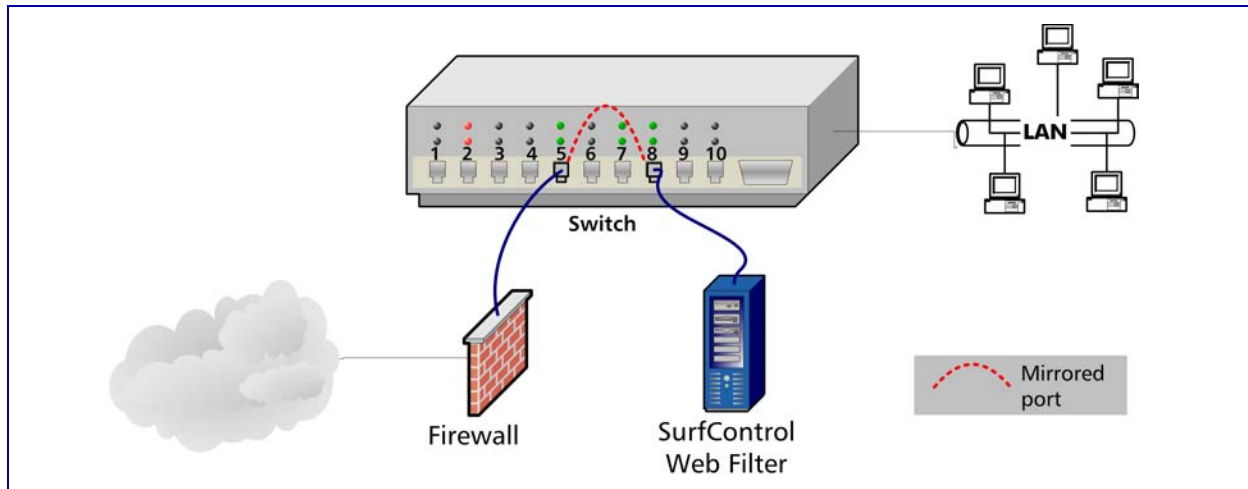


Figure 2 Network placement

In general, use the following guidelines for placing Web Filter within your network:

- Always place Web Filter downstream of NATting firewalls, proxy servers, and caching devices. These network devices alter the HTTP request and render Web Filter unable to determine which user initiated the request.
- Always place Web Filter in a location where it can see all the traffic that needs to be filtered. In general, deploy Web Filter at the Internet gateway.
- Span or mirror the gateway port (firewall, proxy server, caching device, etc.).

DATABASE CONSIDERATIONS

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

SQL vs. MSDE

MSDE, included with the Web Filter download, is based on Microsoft SQL Server technology. An MSDE database has a 2 GB size limitation and does not include management tools, but is an effective database for small environments. MSDE should only be used in environments with fewer than 500 users.

For environments with more than 500 users, SurfControl recommends using a fully licensed version of SQL, which allows more flexibility and the ability to fine-tune database performance.

ONBOARD VS. OFFBOARD DATABASE

If your network requires multiple Web Filter servers, you have two database options: onboard or offboard. An onboard database stores data for a single Web Filter server in a single database on the Web Filter server; an offboard database stores the data from one or more Web Filter collectors in a single database on a separate server.

Many customers choose to use the offboard database option, which provides the advantages of centralized policy management, plus the ability to run reports from a single repository. If you choose this option, then 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 an offboard 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, an offboard database can require more frequent database administration. SurfControl recommends using Windows Authentication for performance and security reasons. Therefore, offboard databases require specific security settings for communication between the Web Filter server and the database.

DATABASE SIZE

The size of the database correlates to:

- The amount of traffic your employees generate.
- The amount of traffic Web Filter is monitoring.
- The number of protocols Web Filter is monitoring.
- The number of users Web Filter is monitoring.

SurfControl estimates that 5000 users generate approximately 1 GB of data per month. Make sure the SQL server has as much RAM as the anticipated size of the database (for example, a 1 GB database requires 1 GB RAM). This recommendation is in accordance with Microsoft's policy for optimal performance.

FUNCTIONAL COMPONENTS

SurfControl offers several products that can work together to provide additional filtering functionality. Some of these components are Web Filter-specific; some are stand-alone products.

SRC

SRC is Web Filter's reporting module, and allows you to run a wide range of reports through a web interface. SRC installs during the Web Filter installation, and most customers place SRC on the Web Filter server. If you want to install SRC on a separate server, make sure that server meets the minimum [SRC system requirements](#).

-
-
- **Functional Components**

VCA

The VCA is an optional component that dynamically categorizes URLs that are not in SurfControl's URL Category List. The VCA runs as a service, typically on the Web Filter server. However, you can install the VCA on a separate server. This is done by installing the full version of Web Filter on a separate server and disabling all other services.

SMC

SMC allows you to manage different Web Filter applications (e.g., SurfControl Web Filter for MS Windows, SurfControl Web Filter for ISA Server) from a single console.

MOBILE FILTER

SurfControl Mobile Filter allows you to filter “remote” employees, such as employees on business using company laptops. Mobile Filter is deployed on a server in the DMZ, and on the client computers to be filtered by Mobile Filter.

Once the Mobile Filter server is installed and configured, SurfControl Web Filter detects these users and displays them as objects in the Who tab of the Rules Administrator. Using either the Mobile Filter server or the Web Filter Rules Administrator, you can add these users to your filtering rules.

IM FILTER

The SurfControl Instant Message Filter restricts users' access to IM and P2P applications based on the protocol digital signature of the application.

You may install the IM Filter on the Web Filter server. If your database is onboard, SurfControl recommends this deployment only if you have disabled the Identity Server.

TYPICAL DEPLOYMENT

SRC and the VCA are typically installed on the Web Filter server, though you may choose to install these on separate servers. For example, you may want to move the individual components offboard if you are already using a remote database, and your user count is nearing the maximum of what your Web Filter server can handle.

DEPLOYMENT SCENARIOS

This section describes two common scenarios, based on the database deployment.

ONBOARD DATABASE

If you choose the onboard SQL server option, install SQL onto the Web Filter server (see Figure 3).

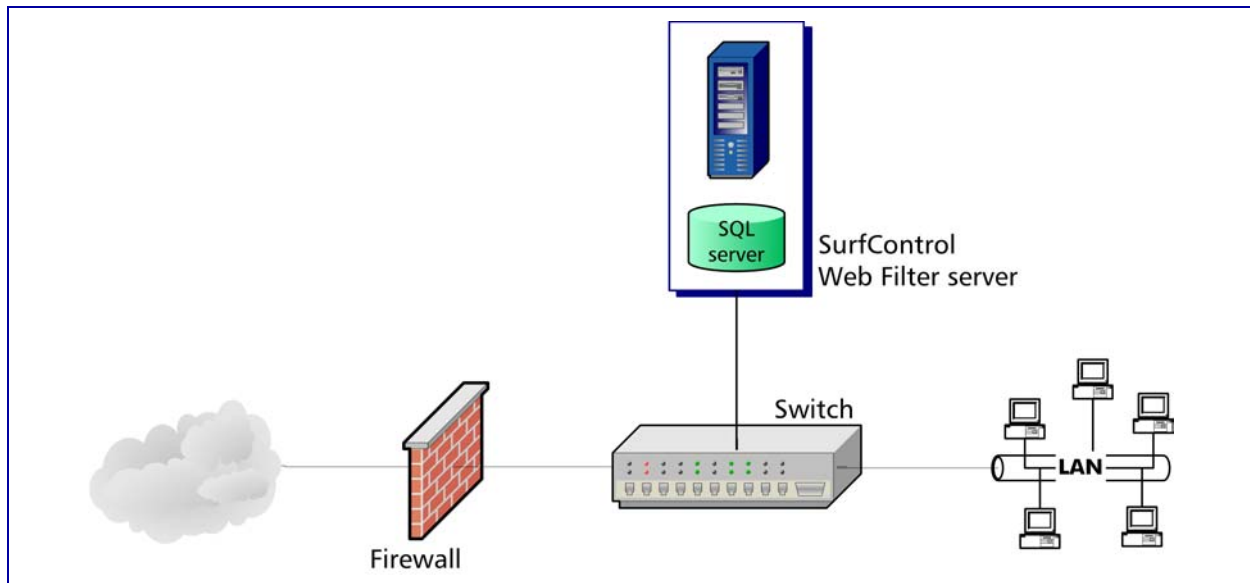


Figure 3 Scenario 1: Web Filter with an onboard SQL server

If you have an onboard database, follow the server recommendations listed in this section. These recommendations are based on number of users and server resources.

-
-
- **Deployment Scenarios**

Web Filter Components

Each scenario can include additional Web Filter components. Table 1 outlines how to deploy each component if the database is onboard.

Note: These are basic guidelines. Actual recommended deployment also depends on Internet usage patterns, which can vary significantly from company to company.

Table 1 Web Filter Components: Onboard Database

Web Filter Component	Recommendation
SRC	Install on the Web Filter server.
VCA	Install on the Web Filter server.
SMC	Install on the Web Filter server.
IM Filter	Install on the Web Filter server (with the Identity Server disabled).
Mobile Filter	Install on a separate server, and place it in the DMZ.

Table 2 shows SurfControl's server recommendations.

Table 2 Server Recommendations (Onboard Database)

Server Component	Recommendation: <500 Users	Recommendation: 500-2,500 Users	Recommendation: 2,500-5,000 Users
Processor	Pentium IV, 2.0 GHz	2 x Pentium IV, 2.0 GHz	2 x Pentium IV Xeon, 2.0 GHz
RAM	1 GB	1.5 GB or more	2 GB or more
NICs	Single Ethernet	2 Ethernet (1 for monitoring, 1 for blocking)	2 or 3 Ethernet (at least 1 for monitoring, 1 for blocking)
Hard drive	HDD (10,000+ RPM) 9 GB free (SCSI)	HDD (10,000+ RPM), 18 GB free (SCSI)	HDD (10,000+ RPM), 36 GB free (SCSI)
Operating System	Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, or Microsoft Windows Server 2000	Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, or Microsoft Windows Server 2003	Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, or Microsoft Windows Server 2003
Database	MSDE, installed on the Web Filter server	Microsoft SQL Server 2000, installed on the Web Filter server	Microsoft SQL Server 2000, installed on the Web Filter server

OFFBOARD DATABASE

Figure 4 shows the offboard database option in a single collector environment.

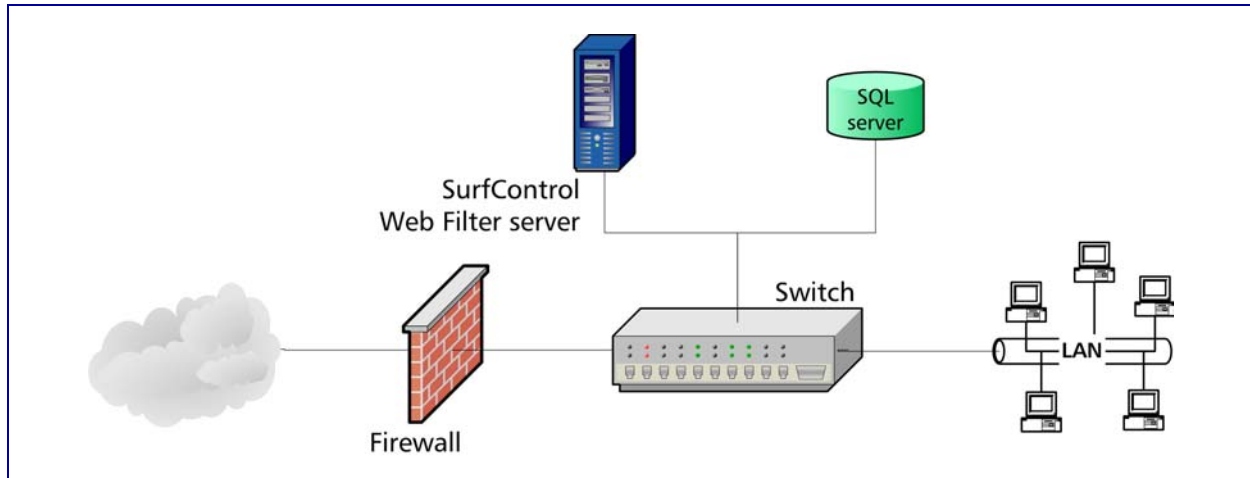


Figure 4 Scenario 2: Single Web Filter server with an offboard database

Web Filter Components

If you have a remote database, you may have the system resources that allow for multiple Web Filter components. Follow the recommendations listed in this section for sizing guidance.

Table 3 outlines whether you can install each Web Filter component on the Web Filter server when you have an offboard database.

Table 3 Web Filter Components: Offboard Database

Web Filter Component	Recommendation
SRC	Install on the Web Filter server.
VCA	Install on the Web Filter server.
SMC	Install on the Web Filter server.
IM Filter	Install on the Web Filter server (with the Identity Server enabled).
Mobile Filter	Install on a separate server, and place it in the DMZ.

-
-
- **Deployment Scenarios**

Table 4 outlines SurfControl’s recommendations the SurfControl Web Filter server when the SQL database is offboard.

Table 4 Web Filter Server Recommendations (Offboard Database)

Server Component	Recommendation: 500-1,000	Recommendation: 1,000-5,000 Users	Recommendation: 5,000-10,000 Users
Processor	Pentium IV, 2.0 GHz	P IV Xeon, 2.8 GHz	2 x Pentium IV Xeon, 2.8 GHz
RAM	1.5 GB	1.5 GB	2 GB or more
NICs	2 Ethernet (1 for monitoring, 1 for blocking)	2 Ethernet (at least 1 for monitoring, 1 for blocking)	2 or 3 Ethernet (at least 1 for monitoring, 1 for blocking)
Hard drive	HDD (10,000+ RPM) 9 GB free (SCSI)	HDD (10,000+ RPM), 9 GB free (SCSI)	HDD (10,000+ RPM), 9 GB free (SCSI)
Operating System	Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, or Microsoft Windows Server 2000	Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, or Microsoft Windows Server 2003	Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, or Microsoft Windows Server 2003

LOAD BALANCING

Web Filter can be load balanced by subnet or by using a Layer 4-7 switch. For details on load balancing, refer to the [SurfControl Web Filter for Windows Deployment Guide](#).