



Deploying SurfControl E-mail Filter for SMTP

rev1.1, February 2004

ACKNOWLEDGEMENTS

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

Role	Name
Technical Contributor	Dan Femino, Senior Systems Engineer
Technical Contributor	Keith Chomentowski, Senior Systems Engineer
Technical Contributor	Scott Stanney, Systems Engineer
Technical Editor	Shawn Titus, Technical Communications Manager
Technical Editor	Stanley Wilson, Technical Trainer
Author	Karen Hepner, Technical Writer

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 white paper provides a general foundation for implementing SurfControl E-mail Filter by examining pre-installation considerations and by illustrating four common deployment scenarios. You can deploy SurfControl E-mail Filter in a number of ways. Each scenario described in this paper contains elements that may be individually deployed or combined to support your specific network configuration.

PRE-INSTALLATION CONSIDERATIONS

This section discusses the following pre-installation considerations:

- Inbound and outbound filtering.
- Database considerations (size and placement).
- Load balancing methods.
- Server size.

INBOUND AND OUTBOUND FILTERING

SurfControl E-mail Filter is extremely effective at stopping spam, and many customers purchase SurfControl E-mail Filter for this reason. SurfControl stops spam at the gateway, freeing up network resources.

Spam is typically an inbound problem. If you simply want to stop spam (and other unwanted content) from entering your network, configure SurfControl E-mail Filter for inbound filtering only.

However, SurfControl E-mail Filter provides significant benefits if you configure it to perform outbound filtering as well. Outbound filtering can scan for confidential or potentially liable information before routing the e-mail to the intended recipient. Also, SurfControl can add customizable footers or banners to an e-mail before it leaves your network.

In addition, many policies can apply to both inbound and outbound traffic. For example, with a single policy, you can stop inbound and outbound viruses.

If you are using SurfControl E-mail Filter for its powerful spam protection, you may want to consider the benefits of outbound filtering, too.

DATABASE CONSIDERATIONS

SurfControl E-mail Filter stores all configuration data and filtering policies in a SQL database called STEMConfig. All logging data is stored in a SQL database called STEMLog.

SQL vs. MSDE

MSDE, included with the SurfControl E-mail Filter download, is the run-time version of SQL. MSDE databases have a 2 GB size limit and few management tools, but is an effective database for small environments.

Although you can install a SQL database onto the SurfControl server, SurfControl recommends that large environments install a fully licensed version of SQL onto a separate, dedicated server.

Dedicated vs. Centralized

If your network requires multiple SurfControl servers, you have two database options: dedicated or centralized. A dedicated database stores data for a single SurfControl server in a single database; a centralized database stores the data for multiple SurfControl servers in a single database.

Many customers choose to use the centralized database option, which provides the advantages of centralized policy management and message administration, plus the ability to run reports from a single repository.

However, the size of a centralized database grows in direct relation to the number of SurfControl servers that write to it. Depending on the size of your environment and the number of e-mails that pass through your network, a centralized database can require additional administration. In this case, you may choose to use a dedicated database for each SurfControl server.

Database Size

The size of the database correlates to the number of e-mails your organization receives per day, and to the length of time you plan to retain the logged data (used for message administration and reporting purposes). To size your database appropriately, SurfControl estimates that each e-mail generates approximately 1KB of log data stored in the database. (This calculation can also be helpful when determining whether MSDE is sufficient for your environment.)

No matter where you store the SurfControl E-mail Filter data, make sure the server has as much RAM as the anticipated size of the database (for example, a one GB database requires one GB of RAM). (This is in accordance with Microsoft's recommendations for optimal performance.)

LOAD BALANCING METHODS

You can load balance SurfControl E-mail Filter using MX records. On the DNS server hosting your domain, create an MX record for each primary SurfControl server using the same MX preference, while giving the failover server a higher number (which gives it a lower preference). Table 1 provides an example of MX preference assignments for load-balancing and failover using MX records. Figure 1 further shows this method.

Table 1 MX Records for Load Balancing.

Mail Exchanger	IP Address	MX Preference
Site A		
mx1.siteA.com	208.126.216.20	5
mx2.siteA.com	208.126.216.21	5
mx3.siteA.com	208.126.216.22	5
mx4.siteA.com	197.201.56.201	10
Site B		
mx1.siteB.com	197.201.56.201	5
mx2.siteB.com	197.201.56.202	5
mx3.siteB.com	197.201.56.203	5
mx4.siteB.com	208.126.216.20	10

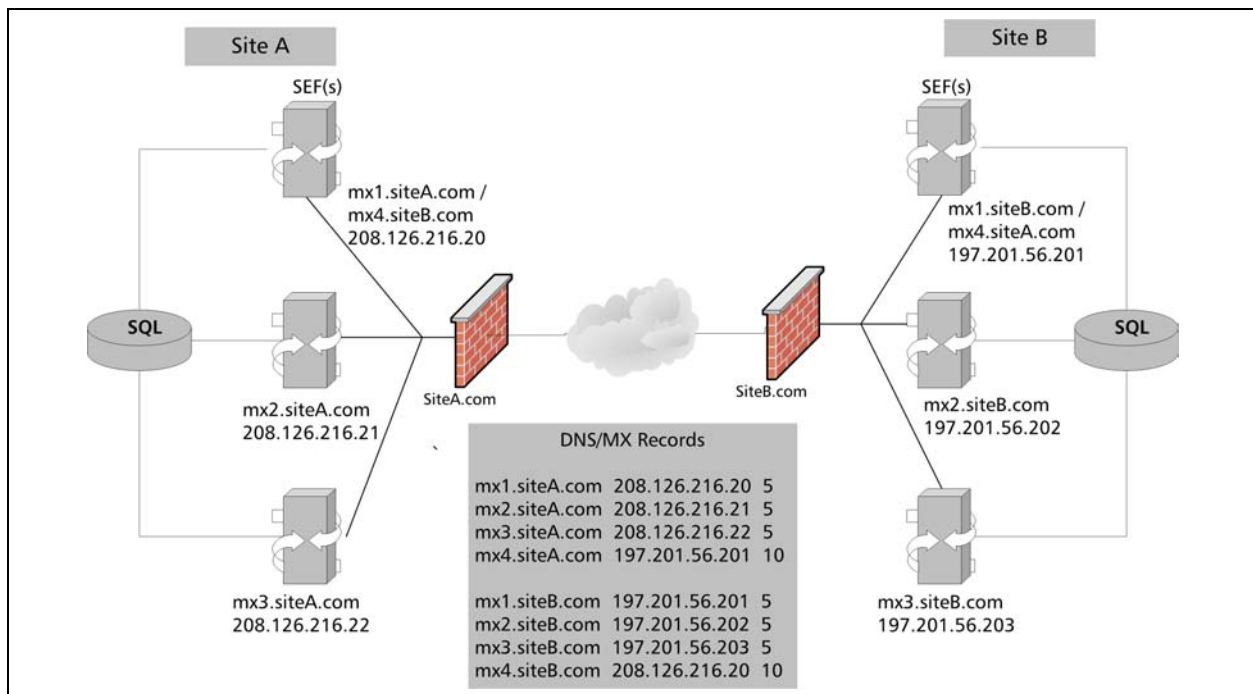


Figure 1 Using MX records for load balancing.

Pre-Installation Considerations

In Figure 1, e-mail sent to siteA.com round-robins between mail exchangers 1, 2, and 3, because each SurfControl server has the same MX preference of 5. (A lower MX preference number means that it has a higher priority -- 5 having a higher priority than 10.) The same thing happens for e-mails sent to siteB.com. If siteA is down (e.g., with a network failure), the sending mail server will route e-mail to the fourth (failover) MX record, which is the address of a server in a different physical location.

For the described failover to work properly, SurfControl servers in siteA are configured to accept messages for siteB, and SurfControl servers in siteB are configured to accept messages for siteA. The failover servers also have static routes configured so that SurfControl knows where to route the e-mails.

In addition to load balancing and failover using MX records, there are also advanced load balancing switches that can be used for these purposes. These switches offer a variety of load balancing algorithms, in addition to round-robin delivery, which provide efficient load distribution and timely failover. Although this is not a required component for a SurfControl implementation, the use of load balancing switches may improve the overall efficiency of your SMTP infrastructure.

SERVER SIZE

SurfControl E-mail Filter requires Windows 2000 Server SP3 or greater, or Windows 2003 Server. Advanced Server is recommended for high-volume e-mail environments. Table 2 shows SurfControl's server recommendations, depending on how many e-mails per hour your organization typically handles.

Table 2 Server Recommendations.

E-mails Per Hour	Server Recommendations
< 10K e-mails	PIII, 1Ghz processor with 1 GB RAM.
< 25K e-mails	Dual-Xeon processor with 2 GB RAM.
<40K e-mails	Quad-Xeon processor with 2 GB RAM, 3 or more HDDs (10,000 + RPM) for e-mail processing.
< 120K e-mails	3-Quad Xeon, 2GB RAM, 3 or more HDDs (10,000 + RPM) for e-mail processing.
< 240K e-mails	6-Quad Xeon, 2GB RAM, 3 or more HDDs (10,000 + RPM) for e-mail processing.

Actual processing speeds are dependent on several factors: number of rules processing threads, number of enabled rules, size of e-mails, and complexity of the e-mails (e.g., attachments, embedded files, etc.).

Partitioning the Server

Because SurfControl frequently reads from and writes to disk as it processes e-mail, you can optimize SurfControl's performance by installing onto a server capable of fast disk I/O and configured to support multiple hard disk drives (HDDs). Figure 2 shows the optimal HDD and partitioning configuration for SurfControl.

Figure 2 shows a server with five SCSI HDDs. Two of the HDDs are in a RAID1 configuration and are divided into three partitions: a partition for the operating system, a partition for the page file, and a partition for the SurfControl application.

The other three HDDs each have a single partition and are capable of fast disk I/O. The first drive contains the In folder where SurfControl stores the received e-mails. The second drive contains the Work folder. SurfControl retrieves e-mails from the In folder and moves them to the Work folder, where the e-mails are processed against the configured rule set. SurfControl then moves the e-mail to a quarantine folder for review or to the Out folder for delivery. The third drive contains the Out folder where SurfControl relays processed messages to the intended recipient.

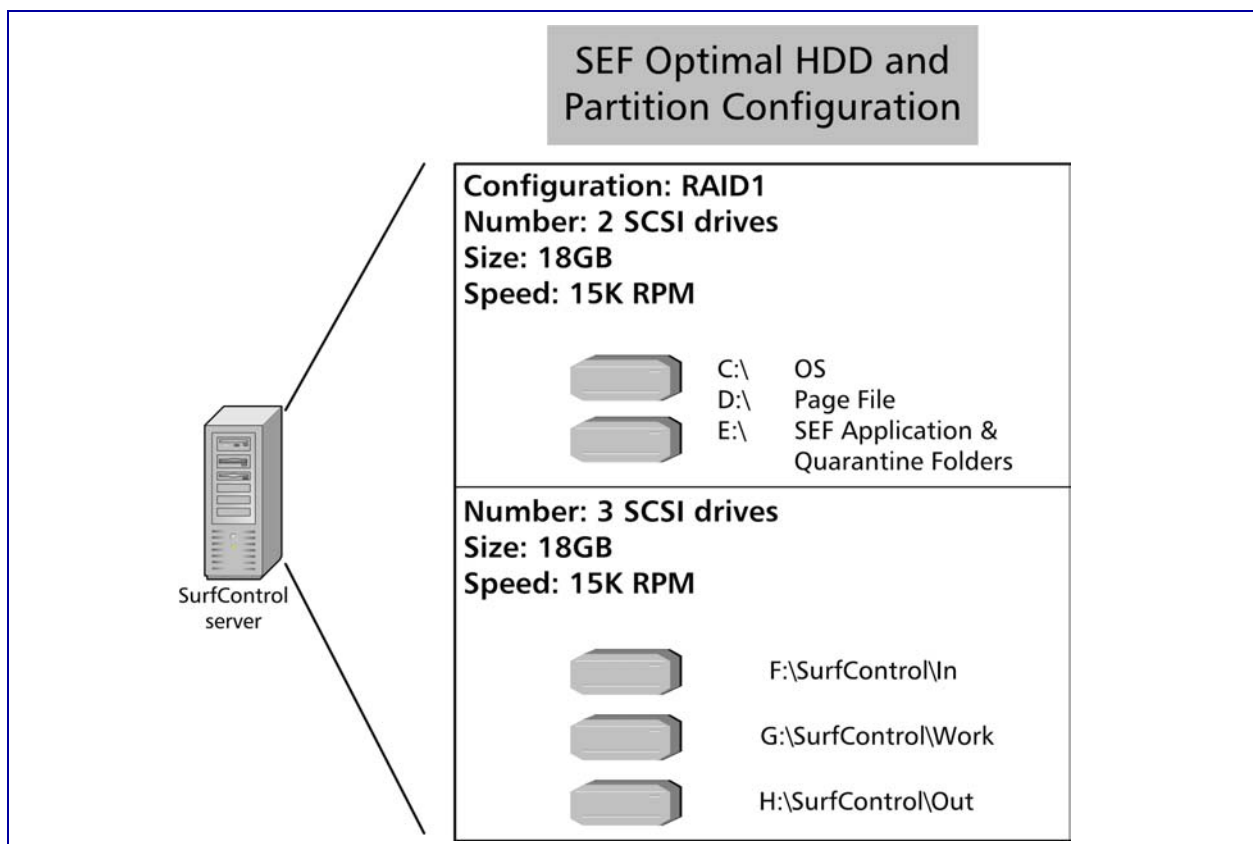


Figure 2 Partitioning the SurfControl server.

DEPLOYMENT SCENARIOS

This section outlines the following deployment scenarios:

- Scenario 1: Simple installation (on the protected network for a small to medium environment).
- Scenario 2: DMZ installation (for a large environment).
- Scenario 3: Protected network installation (for a large environment).
- Scenario 4: Multiple site installation (in a geographically distributed network).

SCENARIO 1: SIMPLE INSTALLATION

Many small- to medium-sized organizations deploy SurfControl E-mail Filter in a protected network, as shown in Figure 3.

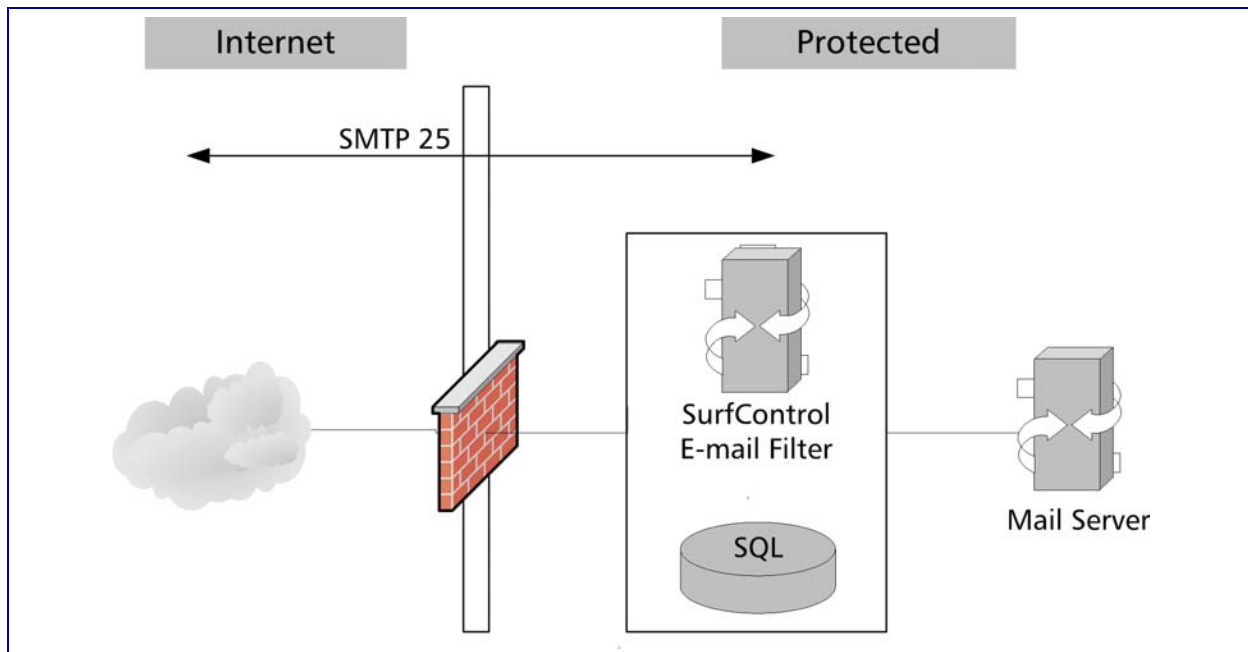


Figure 3 Simple installation for small- to medium-sized environments.

In this scenario, all SurfControl components (including the SQL database) are installed on a single server. SurfControl is filtering all inbound and outbound SMTP traffic.

Inbound e-mail travels from the Internet to SurfControl for filtering. SurfControl then routes the e-mail to the next host, which is typically the SMTP service/daemon of the internal mail server.

Outbound e-mail flows from the SMTP service/daemon of the internal mail server to SurfControl for filtering. SurfControl uses available DNS to resolve MX records and route the SMTP traffic.

SCENARIO 2: IN A DMZ

Many large organizations deploy SurfControl E-mail Filter in the DMZ, as shown in Figure 4.

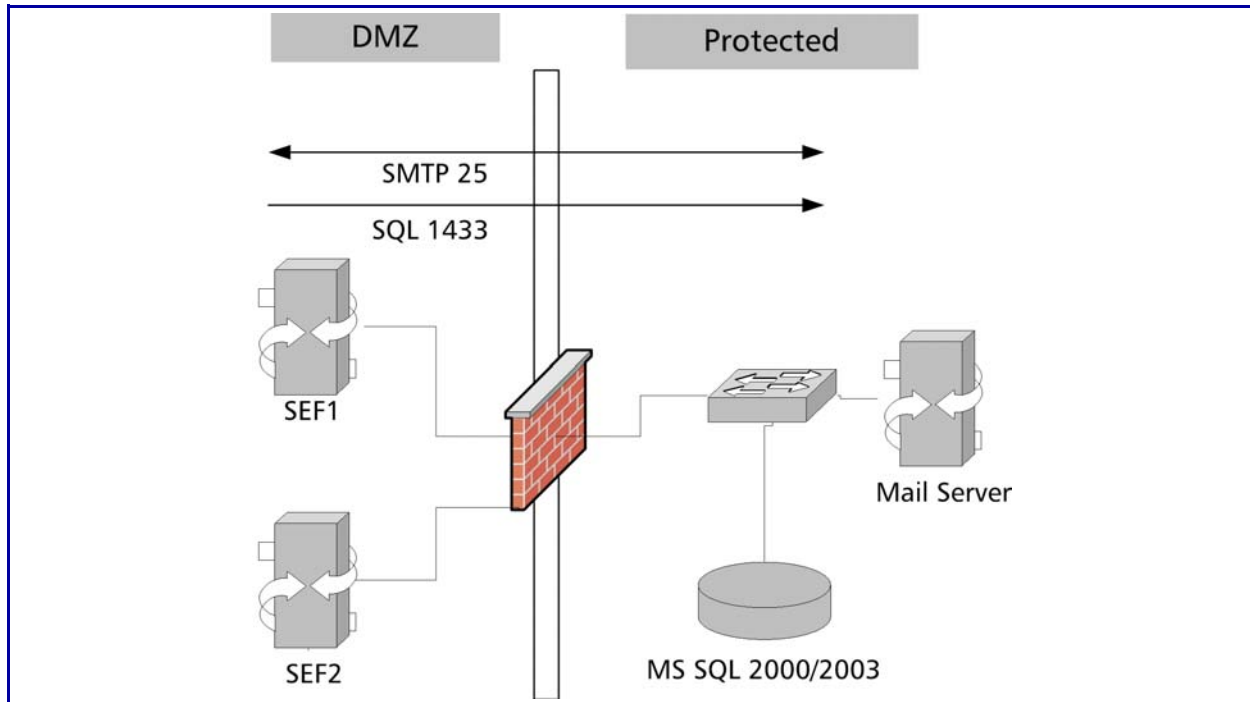


Figure 4 SurfControl E-mail Filter in the DMZ.

Figure 4 shows the SurfControl servers on a hardened server in the DMZ. In this scenario, the SurfControl servers receive SMTP traffic for the organization, filter the e-mail accordingly, then route it to the next host, which is typically a mail server, gateway, or bridgehead on the protected network.

Many deployment scenarios include two or more SurfControl servers, with no single point of failure. In these scenarios, load balancing is typically achieved using DNS MX records with the same preference.

There are several different ways that SurfControl routes SMTP traffic in this type of deployment:

- **SurfControl filters both inbound and outbound traffic.** In this configuration, SEF1 or SEF2 receives inbound SMTP traffic, depending on the MX record. SEF1 or SEF2 statically delivers all "allowed" messages to the internal mail server. When the mail server receives outbound e-mail, it routes the e-mail to SEF1 or SEF2 for outbound DNS name resolution and delivery.
- **SEF1 primarily filters inbound traffic; SEF2 primarily filters outbound traffic.** In this configuration, the SEF1 acts as a back-up for outbound traffic (based on internal configuration). SEF2 acts as a back-up for inbound traffic (based on higher MX preference).
- **SEF1 and SEF2 for inbound filtering only.** In this configuration, load balance SurfControl using MX records. Outbound mail is completely separate and can be routed through additional SurfControl servers, or through any existing outbound mail gateways. This configuration is typically used when there is a high requirement to filter inbound e-mail (e.g., spam), but little or no requirement to filter outbound e-mail.

SQL Placement

In Figure 4, the SQL server is placed inside the protected network. Firewall rules permit SEF1 and SEF2 to communicate with the SQL server over port 1433. SEF1 and SEF2 share a single SQL database for policy management and logging, allowing SurfControl to be managed as a single entity.

Alternatively, you could install SQL or MSDE directly onto each SurfControl server, though policy management and message administration would not be centralized with this configuration. However, you can easily export policies from one SurfControl server and import them to any other SurfControl servers. This configuration is commonly used when SurfControl's main objective is to discard spam, and you have no need for centralized reporting.

Security Considerations

Because of its placement in a DMZ, install SurfControl E-mail Filter onto a hardened Windows 2000 or Windows 2003 server, following Microsoft's OS hardening recommendations for a stand-alone server. SurfControl servers are stand-alone servers (not part of a domain or AD) and use local accounts for services. When communicating with the SQL database, SurfControl uses SQL authentication.

SCENARIO 3: A PROTECTED NETWORK

Depending on your environment, there can be specific advantages to installing SurfControl E-mail Filter on your protected network, such as enabling SurfControl to interact with existing user directories and filter outbound e-mail. Figure 5 depicts this deployment, where an organization's e-mail is routed to a mail relay or anti-virus gateway and then routed to SurfControl servers on the protected network for additional filtering.

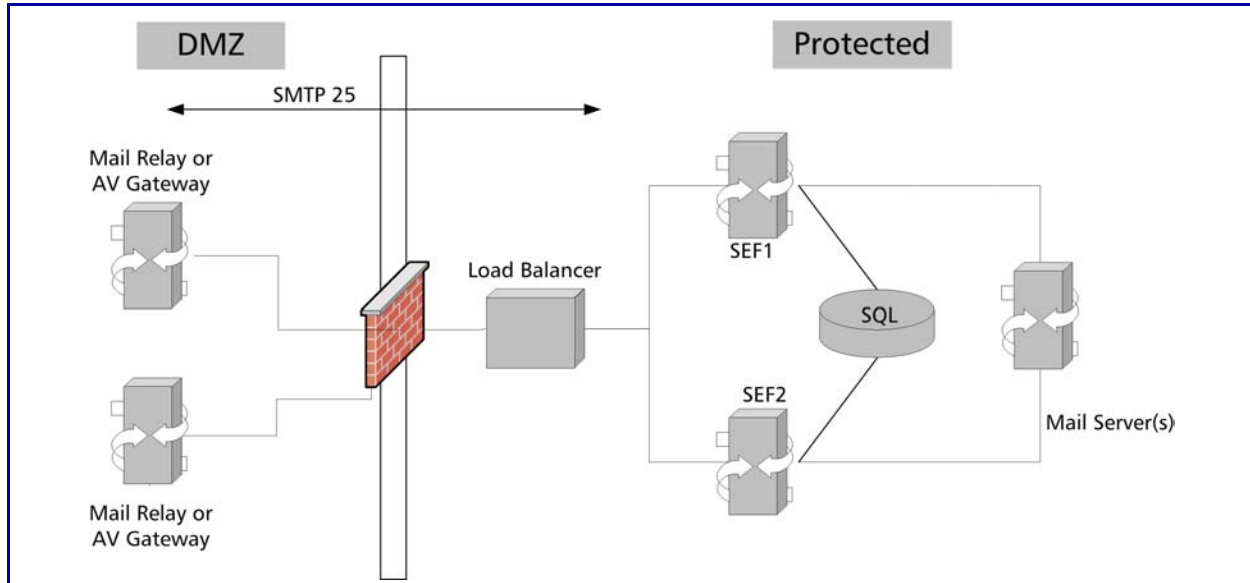


Figure 5 SurfControl E-mail Filter on the protected network.

This example includes an optional load balancing switch to help distribute the SMTP traffic evenly across the SurfControl servers. These servers share a centralized policy database and log database. The SurfControl servers deliver any "allowed" messages to the next host.

As with installing in the DMZ, there are numerous ways that SMTP traffic is routed in this type of deployment:

- **The gateway in the DMZ receives inbound e-mail and routes the e-mail to SEF1 or SEF2 using a load balancer.** SurfControl servers filter the content according to policy, then route any "allowed" e-mails to the next internal mail host. Mail servers route outbound mail to SEF1 or SEF2 for filtering. SEF1 or SEF2 can either resolve DNS to route outbound traffic, or route messages to the DMZ for any additional filtering and delivery.

For inbound traffic, designate one (or more) SurfControl servers to primarily filter inbound e-mail. For outbound traffic, designate one (or more) SurfControl servers to primarily filter outbound e-mail. When receiving an increased volume of traffic, the load balancing hardware/software dynamically utilizes any other available resources. In addition, you can use the load balancer to dynamically route outbound e-mail to SurfControl depending on server availability, or other load balancing algorithms specific to the device.

- **Inbound e-mail is the same as above.** Outbound SMTP traffic can bypass SurfControl. Internal mail servers may route mail directly to the Internet, or relay to the mail server/AV gateway for outbound delivery.

-
-
- **Deployment Scenarios**

SQL Placement

The database can be installed on a separate server or server cluster, on one of the SurfControl servers, or on each of the SurfControl servers. Once again, server requirements depend entirely on message volume and reporting requirements.

SCENARIO 4: MULTIPLE SITES

Some larger organizations may have more than one geographic location responsible for mail processing. If one site is unavailable or is seeing an increased volume of traffic, you can route overflow to a different site for processing. This is often accomplished with MX records using different preferences, as shown in Figure 6.

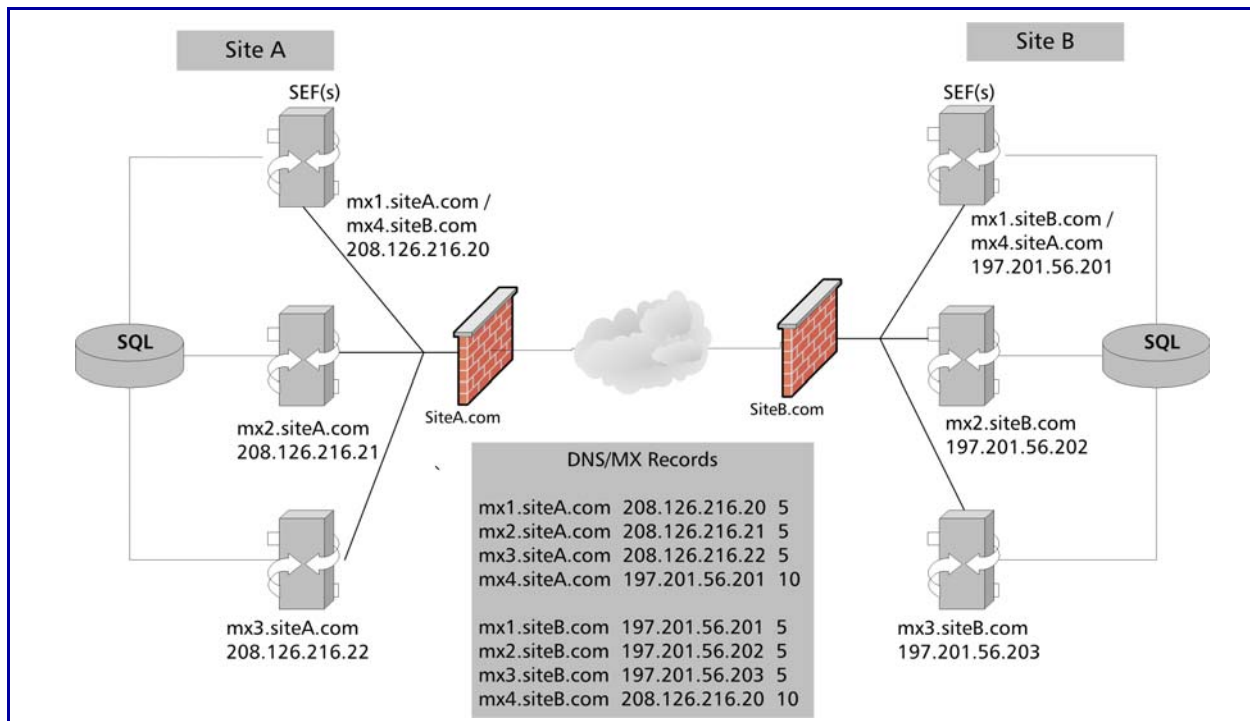


Figure 6 SurfControl E-mail Filter at multiple sites.

In Figure 6, e-mail intended for SiteA is primarily delivered to the SurfControl servers physically residing at SiteA. However, in the unlikely event that SiteA is unavailable, messages intended for SiteA will be delivered to SiteB, because of the failover configuration (specified by the lower MX preference).

SurfControl servers at both sites need to have static routes that identify where to route e-mail intended for both SiteA and SiteB.