



realtimepublishers.com<sup>tm</sup>

# *The Administrator Shortcut Guide<sup>tm</sup> To*



# Blocking Spam with Sender Validation



**SpamLion<sup>TM</sup>**  
Anti Spam Gateway

*Alan Sugano*

Chapter 3: Implementing a sender validation Solution in Your Company.....	36
Cost Justification Compared with Other Methods.....	36
Software Cost.....	37
Implementation Benefits and Cost Justification .....	37
Ongoing Administrative Costs.....	39
Minimal User Support Costs.....	39
Implementation Steps for a Sender Validation Service .....	40
Select a Sender Validation Service.....	41
Select an Implementation Strategy .....	41
Train End Users .....	41
Select an Initial Implementation Date.....	41
Upload a Pre-Approved Senders List .....	41
Change Your MX Record .....	42
Follow Up .....	42
Set Up a Quarantine Period.....	42
Sender Validation Internal Server Implementation Steps.....	42
Select a Sender Validation Package.....	43
Select an Implementation Strategy .....	43
Plan End-User Training .....	43
Decide on Sender Validation Server Placement.....	44
Purchase the Server Hardware .....	44
Install the OS on the Server .....	44
Install the Sender Validation Software on the Server.....	44
Select an Initial Implementation Date(s) .....	45
Upload a Pre-Approved Senders List .....	45
Reconfigure the Firewall.....	45
Make Mail Server Modifications.....	50
Activate the Sender Validation Server.....	50
Test the Sender Validation Server .....	51
Establish a Quarantine Period.....	51
Backup .....	51
Post Installation Tasks and Best Practices .....	52
Summary.....	54

## Copyright Statement

© 2004 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at [info@realtimedpublishers.com](mailto:info@realtimedpublishers.com).

## Chapter 3: Implementing a Sender Validation Solution in Your Company

Sender validation is the only spam solution I know of that has the potential to eliminate 100 percent of a company's spam. There are many ways to implement a sender validation solution in your company. Sender validation can be implemented as a service or a dedicated server. The dedicated server can be installed in your company's DMZ, local area network (LAN), or in a co-location facility. Each configuration has its advantages and disadvantages. Your email environment will dictate the best sender validation configuration for your company.

In this chapter, we'll take a look at the cost justification of a sender validation solution, the estimated startup and maintenance costs, and the implementation steps necessary to set up a sender validation solution as a service or dedicated server. In addition, I'll provide best practices to follow after the sender validation solution is up and running.

### Cost Justification Compared with Other Methods

Ideally, a sender validation solution should be installed on a dedicated server for the best performance and stability. If you have more than 100 users in your company, you probably want to implement any server-based anti-spam solution on a dedicated server.

Remember that any anti-spam solution will increase the load on an existing server. Often mail servers are already heavily loaded, and installing an anti-spam solution on the server will just make the situation worse. By installing a sender validation solution on a dedicated server, you ensure compatibility with other SMTP mail servers and reduce the risk of having the sender validation software conflict with existing mail services, such as antivirus software.

Expect to pay \$1000 to \$3000 for a name brand (such as Hewlett-Packard and Dell) server capable of handling a server-based sender validation solution for more than 100 users. Make sure to budget the time and cost to install the operating system (OS) on the anti-spam server. In addition, make sure you have adequate backup capacity to backup this additional server, an available port on your Ethernet switch, and the physical room to hold the server.

## Software Cost

Of course, you must factor in the cost of the sender validation software. Most vendors sell their software by the number of users. For larger installations, many vendors offer a quantity discount. You can contact the software vendor directly to get the best deal. Expect to pay \$5 to \$30 per user for a sender validation solution. This option is less expensive than a spam filtering service but more than a non-sender validation spam solution.

The software cost is typically a one-time purchase cost. However, some sender validation vendors require an annual license renewal. This fee usually includes free technical support and upgrades during the maintenance period. Expect to pay 15 to 25 percent of the purchase price for maintenance and upgrades.

## Implementation Benefits and Cost Justification

Fortunately, a sender validation solution is one of the easiest IT projects to cost justify, especially if you have more than 100 email users in your company. The return on investment (ROI) is usually less than a year, and in some cases, as little as several weeks.


### An ROI Example

The biggest selling point of a sender validation solution is the time savings secured by the end users. Consider the following simple example: A company with 200 email users implements a sender validation solution that costs \$8000. On average, each employee of the company is paid \$25 per hour. After implementing the sender validation solution, each employee saves 10 minutes per day because the employees do not have to wade through junk mail, are not constantly interrupted by “ding—new message” every 15 minutes, and are less likely to accidentally delete valid email messages. Based on these assumptions, the company’s savings per day is:

$200 \text{ users} \times \$25 \text{ per hour} \times (10 \text{ minutes}/60 \text{ minutes}) = \$833.33 \text{ savings per day}$

If you take the total cost of \$8000 for the sender validation implementation and divide it by \$833.33, it takes roughly 10 days to pay for the sender validation solution. Let’s assume that this company works 5 days per week. In this example, the company will have an ROI of 2 weeks! It is difficult to identify any IT project that has a shorter ROI period.

Based on this simple example, the short ROI period should cost justify any sender validation project. The elimination of undesirable spam messages (pornographic ads) should also reduce coworker tension, and reduce the likelihood of a lawsuit issued against the company.

 The ROI for a company implementing a sender validation spam solution can be as little as 2 weeks.

In addition to the increased user productivity, there are other benefits of a sender validation solution. Reduced storage on your internal mail server is one such benefit.

## Reduced Storage on Your Internal Mail Server

A sender validation solution will reduce the storage requirements on your mail server because the junk mail will never reach the server in the first place. Reducing the amount of mail on the server has the following benefits:

- Better mail server performance—Reduced mail storage increases performance of the mail server—especially when performing searches.
- Reduced mail store size—A significant percentage of a company’s mail store contains spam. Although spam might reside in the deleted items folder, it still takes up space on the server before it is permanently deleted. Failed non deliverables (NDRs) and bad mail items can consume significant space on a mail server. Some companies estimate that spam takes up half of their current mail storage space.
- Reduced backup/restore times—The backup and restore times on any mail server will be reduced because of the decreased mail store size.
- Reduced backup storage requirements—If your tape backup is close to capacity, implementing an anti-spam solution might eliminate the need to purchase a higher-capacity backup system. Even if a company must back up the sender validation server, the company will still have a net reduction in backup capacity requirements.
- Reduced mail store maintenance time—With a reduced mail store size, defragmentation of the mail store and mail store repair utilities will run faster. In the event of a mail store corruption, downtime will be reduced because repair utilities do not have to deal with a large volume of junk mail on the server.
- Reduced stress on your WAN links—Sender validation reduces the amount of spam traffic on your WAN links to internal remote mail servers.
- Sender validation has the potential to eliminate 100 percent of spam—Sender validation can be implemented as your company’s first anti-spam solution or as an upgrade to replace an outdated anti-spam solution.

### **Ongoing Administrative Costs**

Although there are many benefits that enable an organization to easily cost-justify a sender validation solution implementation, to truly compare sender validation solutions, you must consider the ongoing administrative costs. The following list highlights these considerations:

- Sender validation service solutions require annual re-licensing—Some sender validation solutions require annual re-licensing of as much as 100 percent of the product cost per year. Although this cost can be very expensive in the long run, it might be the best solution for your company—such is especially true of smaller companies that use a sender validation service and do not have an internal server.
- Sender validation dedicated server annual maintenance costs—For most sender validation server solutions, expect to pay 15 to 30 percent in maintenance fees for ongoing technical support and software upgrades.

However, after the sender validation product is in place, there is very little ongoing maintenance. The most important maintenance item on the sender validation server is the backup of the sender validation database. This database contains all of the company's "approved senders." As long as this database is backed up, you should be able to quickly recover from any hardware problem.

### **Minimal User Support Costs**

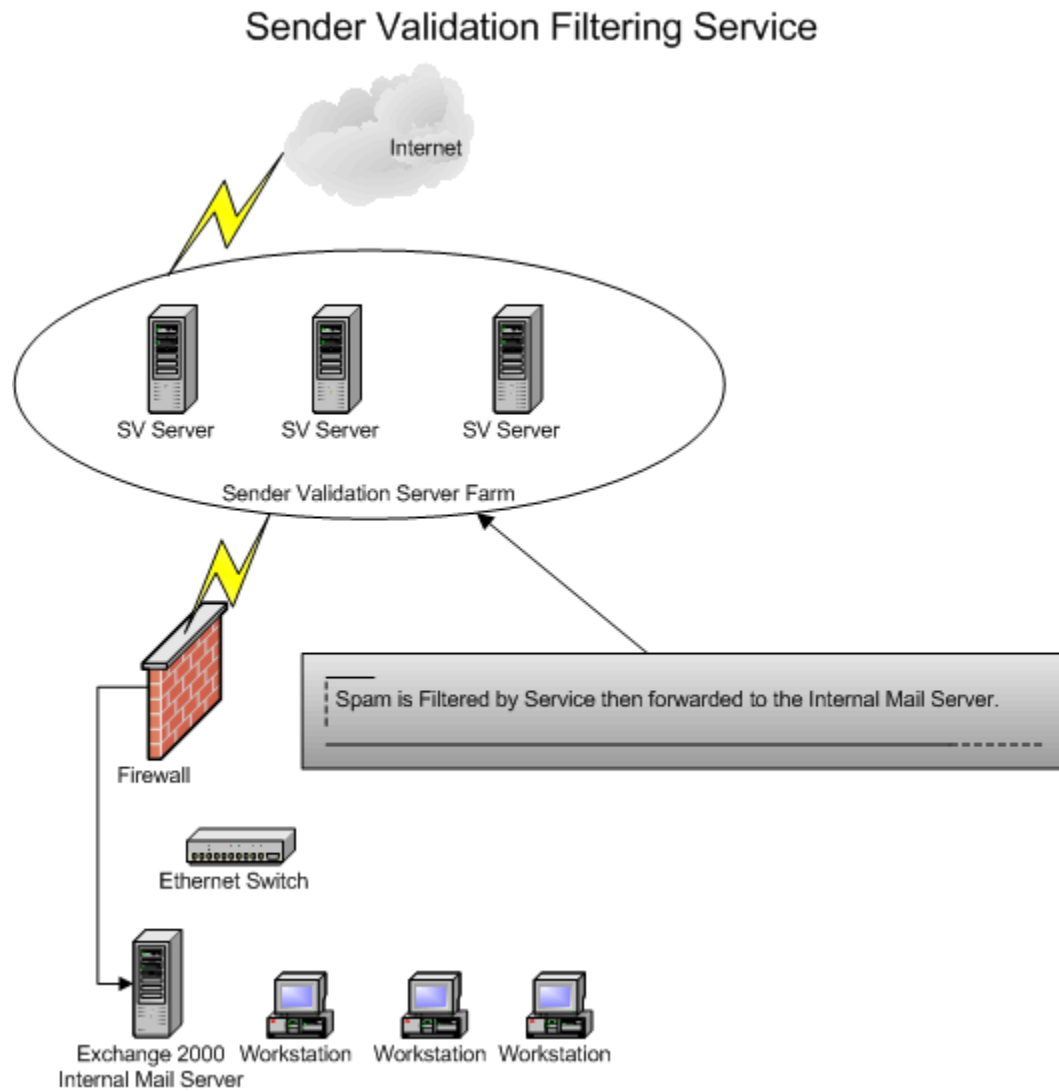
Most of the sender validation solutions include an integrated junk mail box or Web interface to manage their junk mail. The initial training on a sender validation solution should be minimal. An hour training session to explain how sender validation works and how a user manages junk email should be more than adequate. Some users might not require any training.

After the initial end-user training costs, ongoing training costs are minimal:

- New hires might require a brief training session.
- Existing users might require some training on a new release of the software so that they can take advantage of any new or enhanced features of the software.
- Help desk support and desktop costs are minimal because everything is managed at the server level.

## Implementation Steps for a Sender Validation Service

Figure 3.1 illustrates a typical sender validation service implementation.



**Figure 3.1: Sender validation filtering service implementation.**

The following sections walk you through the sender validation service implementation steps.



### **Select a Sender Validation Service**

Decide on the service to use. Make sure users are comfortable with the user interface. Ideally, test the service with your company's email to make sure it is a good fit for the company. Carefully review the administrative capabilities of the sender validation service before selecting a solution. During the evaluation phase, some sender validation companies can only filter certain email accounts with any remaining accounts set to a bypass mode. This setup allows the company to try before they buy so that they can identify any issues that might arise during the trial phase.

### **Select an Implementation Strategy**

Decide whether you want to move the entire company over to the sender validation solution all at once or roll out the sender validation service in phases. The larger the company, the more likely you'll use a phased approach.

### **Train End Users**

Depending on the skill level of your users, it might be necessary to train your users on how to use the sender validation service. Ideally, the training should take place just before their mailboxes are cut over to the service so that they will retain as much of the training as possible before using the actual service.

### **Select an Initial Implementation Date**

Select an initial cut-over date—ideally, on a weekend. This selection should allow enough time for the MX record change to propagate over the Internet. Before you make the change, consider reducing the time to live (TTL) for your existing MX record so that the change will propagate faster throughout the Internet.

### **Upload a Pre-Approved Senders List**

If the service allows an upload of pre-approved senders, I suggest using this feature to reduce the number of messages in quarantine. Alternatively, if the service has a “learning mode,” you can redirect all outgoing messages to the sender validation service and have any sender addresses automatically added to the approved senders list before turning on the sender validation service. Some services require a module on your existing server to forward the email addresses to their server for the approved list. This learning strategy will work better if your company sends mail to a set number of users on a frequent basis. I strongly suggest employing either one of these methods to upload a pre-approved sender list; otherwise, each sender must be manually validated. Manual validation is one of the reasons why early sender validation solutions developed a bad reputation.

### ***Change Your MX Record***

You must redirect your MX record to the sender validation service's servers. The sender validation service's servers will then redirect your email to your internal server. I suggest setting up a backup MX record to your ISP's mail server so that the ISP can hold your mail if the sender validation service goes down. You can set a backup MX record directly to your internal server; however, if the service does not respond in a timely manner, mail will be directly delivered to your mail server, bypassing the sender validation service. In addition, if a spammer figures out that the backup MX record points directly to your mail server, the spammer can use the backup MX record to completely bypass your sender validation service.

### ***Follow Up***

Expect some issues to arise when turning on the sender validation service. Some users will require help adding users to their approved senders lists, and senders might have difficulty completing the validation process. Prepare your users for a dramatic reduction in mail messages. Some users think their mail might be broken because they don't receive any messages in their Inboxes.

### ***Set Up a Quarantine Period***

You might want to increase or decrease the quarantine period for your messages based on your company's requirements.

## **Sender Validation Internal Server Implementation Steps**

If you have more than 100 users, consider a sender validation server-based solution. Running an internal sender validation server inside the company is usually more cost effective than paying a recurring monthly or annual fee for a sender validation service. The following list highlights steps for a sender validation internal server implementation:

### **Select a Sender Validation Package**

To do so, you will need to answer the following questions:

- Does the sender validation solution offer a product evaluation?
- Is it possible to evaluate the product for some users in your company or is it an all-or-nothing implementation?
- Does the product evaluation have any time or user limits?
- Does the sender validation solution offer the product as a service with the option to migrate to an in-house server in the future?

Answers to these questions should help you determine the correct sender validation solution for your company. In addition, make sure users are comfortable with the user interface. Carefully review the administration capabilities of the sender validation package before selecting a solution:

- Does the software package have a planning guide to assist in the implementation?
- What type of support does the company offer during the transition period?
- Does the software vendor have expertise only in the software package they support?

Ideally the vendor is familiar with your mail server, firewall, ISP, and MX record changes. The more familiar the vendor is with your network, the smoother the transition.

### **Select an Implementation Strategy**

Decide whether you want to move the entire company over all at once or rollout the sender validation server in phases. The larger the company, the more likely you will use a phased approach.

### **Plan End-User Training**

Depending on the skill level of your user base, it might be necessary to train your users to use the sender validation software. Ideally, the training should take place just before their mailboxes are cut over to the service so that they will retain as much of the training as possible.

### ***Decide on Sender Validation Server Placement***

You can place the sender validation server behind the firewall, in the DMZ, in front of the firewall, or in a co-location facility. If your firewall has the capability, install the sender validation server in the DMZ. Doing so allows the sender validation server to become the “sacrificial lamb” in case the server is attacked by hackers. This setup increases security because there is no direct email communication with your internal email server and the Internet for incoming mail.

### ***Purchase the Server Hardware***

Based on the sender validation software recommendations, order the server hardware that will safely support your company’s email load and number of users. Don’t forget to include a provision to backup the server, either with a dedicated tape drive or existing backup resource. Make sure you have an open Ethernet port on your switch and the physical space to accommodate the server.

### ***Install the OS on the Server***

Install the OS according to the sender validation solution vendor’s recommendations. Some packages are sensitive to OS version and service pack levels. Install any critical security patches on the server to protect it from hackers. Make sure that the OS configuration matches the sender validation requirements.

### ***Install the Sender Validation Software on the Server***

Install the sender validation server software on the server. Be sure to follow any special requirements during the installation process. After you install the software, test the sender validation server to make sure it’s not an open relay. You can use the testing tool at <http://www.ordb.org/submit/> for verification. Performing the open relay test will ensure that the new sender validation solution is not entered into an open relay database.

---

### **Select an Initial Implementation Date(s)**

Select an initial cutover date that is on a weekend. Doing so will give you more time to reconfigure your firewall and test the sender validation server implementation. It also gives you more time to restore the firewall and servers to their original configurations in case something goes wrong. Make sure that the cutover dates coincide with end-user training.

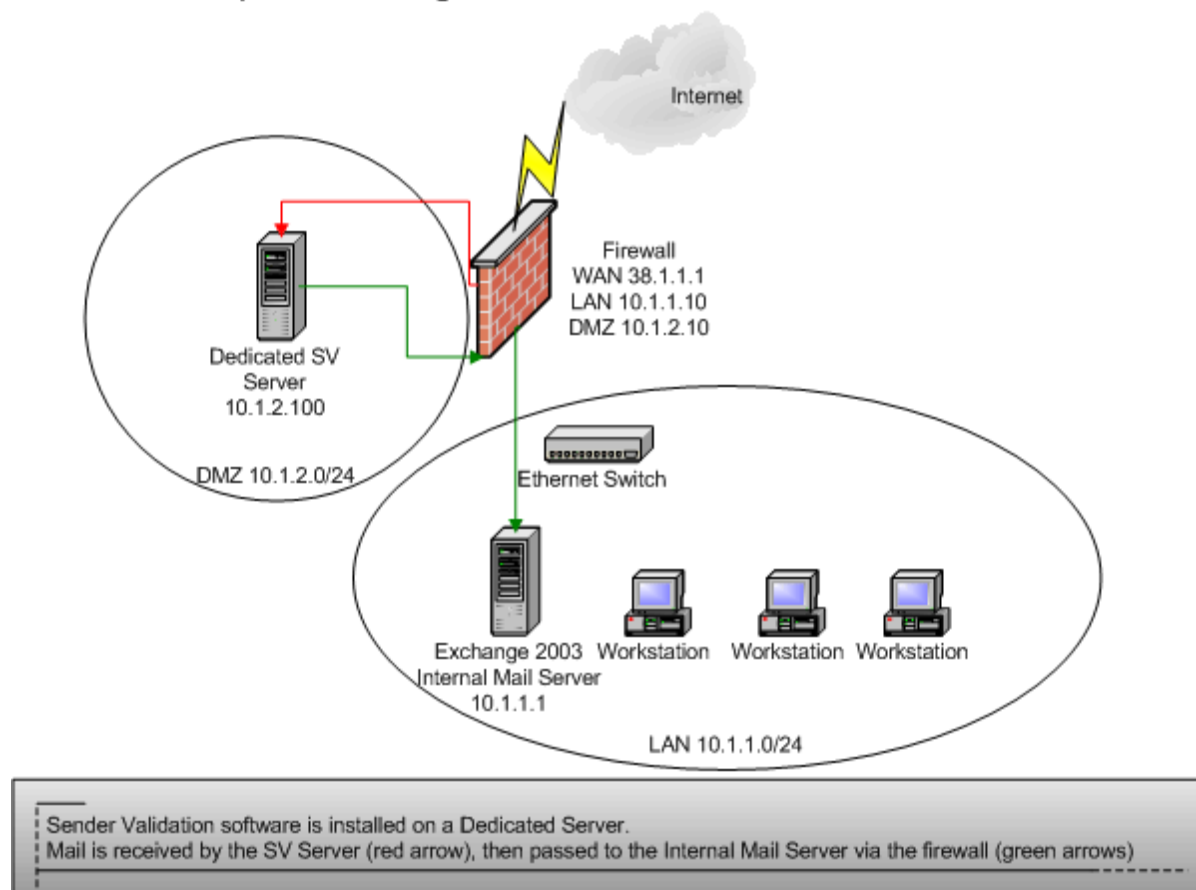
### **Upload a Pre-Approved Senders List**

Use the pre-approved senders list feature to reduce the amount of messages in quarantine. Alternatively, if the service has a “learning mode,” you can redirect all outgoing messages to the sender validation service and have any sender addresses automatically added to the approved senders list before activating the sender validation server. Some services require a module on your existing server to forward the email addresses to the server so that the addresses can be added to the approved list. This learning strategy will work better if your company sends mail to a set number of users on a frequent basis. Without a pre-approved senders list, each sender must be validated manually. Manual validation is one of the reasons why early sender validation solutions developed a bad reputation. Create the list well in advance of uploading it to the server so that you have enough time to ensure the list is complete and accurate.

### **Reconfigure the Firewall**

Before making any changes to the firewall, make sure you have a good backup of the firewall configuration. Doing so will allow you to quickly restore your current mail configuration if issues arise during the implementation. Figure 3.2 illustrates a sender validation server implementation in the DMZ.

## Spam Filtering on a Dedicated Server in the DMZ



**Figure 3.2: Sender validation dedicated server in the DMZ.**

Create the following NAT rule on the firewall for the sender validation server (assume that the MX record points to 38.1.1.1 and the internal address of the sender validation server in the DMZ is 10.1.2.100):

Public Address: MX record for the mail server (38.1.1.1) on the WAN

DMZ Address: Private address of the sender validation server (10.1.2.100) in the DMZ

Description: One-to-one NAT rule to translate the public IP address of the mail server (MX record) to private IP address of the sender validation server.

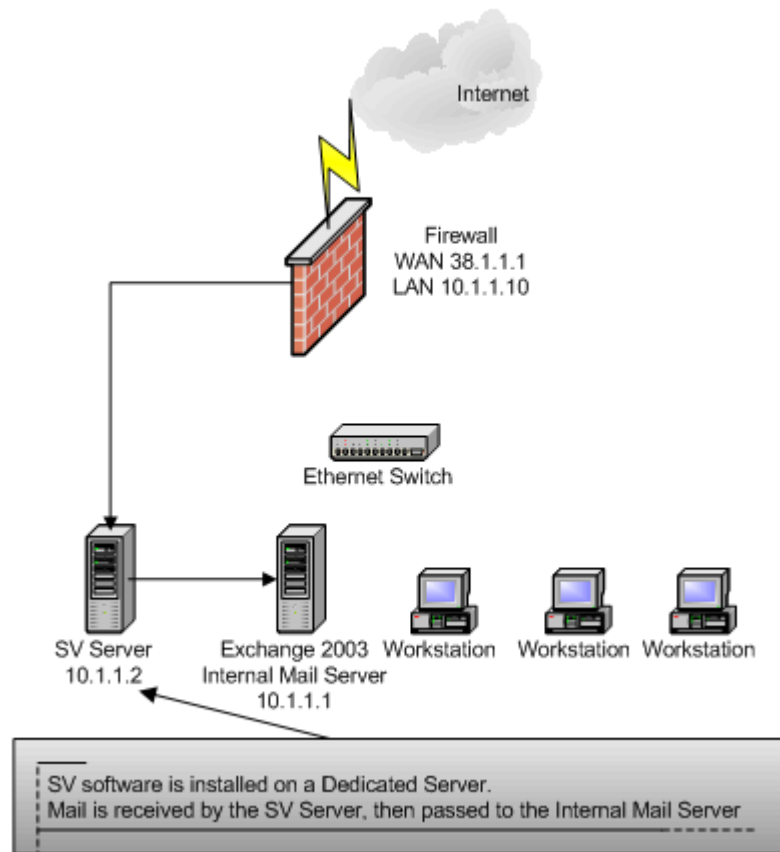
Create the rules on the firewall for the sender validation server that Table 3.1 shows (assume the IP address of the internal mail server is 10.1.1.1).

Source	Destination	Port(s)	Port and Description
Any from the WAN	Sender validation server in the DMZ (10.1.2.100)	25 (SMTP) and 80 (Web)	Allow incoming mail and Web traffic (Web-based validation) to the sender validation server from the public Internet
Sender validation server in the DMZ (10.1.2.100)	Internal mail server (10.1.1.1) on the LAN	25 (SMTP)	Allow the sender validation server to send mail to the Internal mail server
Any from the LAN	Sender validation server in the DMZ (10.1.2.100)	80 (Web)	Allow users to manage their quarantined mail using a Web-based interface
Internal mail server on the LAN (10.1.1.1)	Sender validation server in the DMZ (10.1.2.100)	25 (SMTP)	Allow internal mail server to send mail to the sender validation server in the DMZ
Sender validation server in the DMZ (10.1.2.100)	Any on the WAN	25 (SMTP) 53 (DNS) 80 (Web)	Allow sender validation server to send out mail to the Internet

**Table 3.1: Rules on the firewall for the sender validation server.**

These rules might vary depending on the type of firewall and the specific requirements of your sender validation server package. These rules assume that the outgoing mail is forwarded by the internal mail server to the sender validation server so that the sender validation server can inspect the outgoing addresses and add them automatically to the approved senders list. Figure 3.3 shows a sender validation server on the LAN.

## Spam Filtering on a Dedicated Server on the LAN



**Figure 3.3: Sender validation dedicated server on the LAN.**

Create the following NAT rules on the firewall for the sender validation server (assume that the MX record points to 38.1.1.1 and the internal address of the sender validation server in the DMZ is 10.1.1.2):

Public Address: 38.1.1.1 on the WAN interface

LAN Address: 10.1.1.2 on the LAN interface

Description: One-to-one NAT rule to translate the public IP address of the mail server (MX record) to the private IP address of the sender validation server.



Create the rules on the firewall for the sender validation server that Table 3.2 shows.

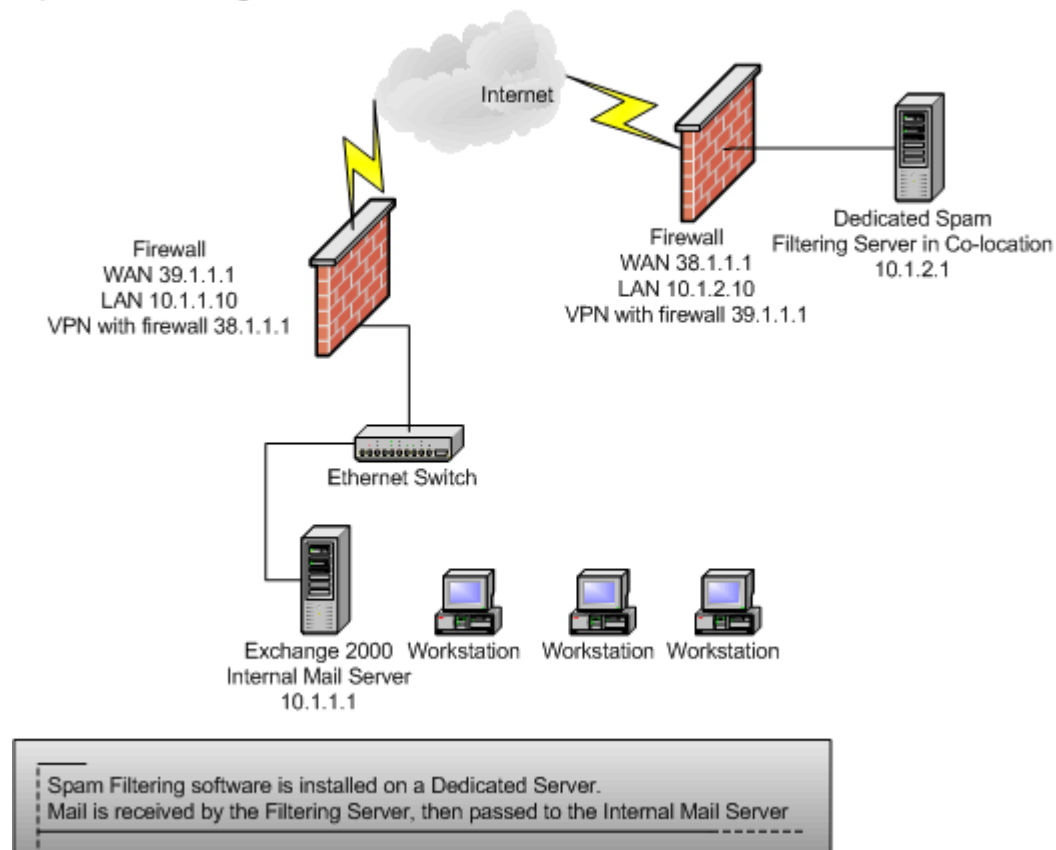
Source	Destination	Port(s)	Port and Description
Any from the WAN	Sender validation server on the LAN (10.1.1.2)	25 (SMTP) and 80 (Web)	Allow incoming mail and Web traffic (Web-based validation) to sender validation server from the public Internet
Sender validation server on the LAN (10.1.1.2)	Any on the WAN	25 (SMTP) 53 (DNS) 80 (Web)	Allow sender validation server to send out mail to the Internet.

**Table 3.2: Rules on the firewall for the sender validation server.**

These rules might vary depending on the type of firewall and the specific requirements of your sender validation server package.

If the sender validation server is in a co-location facility, establish a VPN connection to the server. That way, all traffic will be encrypted between your internal mail server, LAN, and the sender validation server. Figure 3.4 shows a sender validation server in a co-location facility.


### Spam Filtering on a Dedicated Server on the WAN



**Figure 3.4: Sender validation dedicated server in a co-location facility.**

Create a VPN between the co-location firewall and the company firewall. It might be necessary to change your MX record to point to the public IP address of the sender validation server. Make sure to add a Reverse (PTR) record for your sender validation server to avoid mail delivery problems with other mail servers. Some mail servers perform a reverse lookup from the receiving mail server as a way to combat spam. If an MX record change is necessary, make sure to allow enough time for the MX change to propagate throughout the Internet.

As with the previous configurations, these rules might vary depending on the type of firewall and the specific requirements of your sender validation server package.

 Any of these firewall changes can cause serious disruption in service and/or security holes if they are not created properly. If you do not feel comfortable with these changes, budget some time to have the firewall vendor, sender validation server vendor, or a qualified consultant assist you in the sender validation server implementation. Make sure to get a good backup of any firewall configuration before you begin so that you can quickly restore the original configuration if necessary.

### ***Make Mail Server Modifications***

Depending on the sender validation software requirements, you might have to re-route your outgoing mail through the sender validation server—especially if you want to take advantage of any auto-learning features. Some sender validation servers require that a module is installed on the mail server to enable this functionality. Check the sender validation server documentation for any other mail server modifications.


### ***Activate the Sender Validation Server***

Activate the sender validation server for the desired number of users. Unless the company is very small, I suggest a two-phase approach. Turn on the sender validation software for a select number of users, then fine-tune the system. Create a document to address any of the questions. Before you activate the sender validation software for the remaining users, distribute this document to your end users to reduce the number of Help desk calls. When you activate the remaining users, the system should be fine-tuned to your company's email environment.

### ***Test the Sender Validation Server***

Have someone send you mail from a test account to test the following scenarios. You can use the same test mail account by simply adding/removing the email address from your approved senders list:

- **Preloaded list test.** If you decide to upload a pre-approved list of senders, make sure the test account is in the list and mail is accepted from anyone on the pre-approved senders list. Remove the test account from the approved senders list after this test is completed.
- **Manual validation test.** Have an end user manually add the test account to the approved senders list. Doing so will set up the next test.
- **Approved senders list test.** Make sure that a test message from the user added in the previous step is delivered properly.
- **Manual deletion from the approved senders list test.** Manually delete the test user from the approved senders list.
- **Auto-add to the approved senders list test.** If you are using the auto-add to the approved senders list feature, send a message to the test account and verify that the email address is auto-added to the approved senders list. After you verify this addition, delete the test account to prepare for the next test.
- **Sender validation test.** Send a message from the test account and make sure that you receive the validation request. Have the test user complete the validation process and verify that the mail is delivered correctly.
- **Quarantine test.** This test cannot be done initially—ensure that the messages in quarantine are deleted when they reach the proper age. For testing purposes, you can reduce the quarantine period to a shorter time to ensure that the messages are properly deleted from quarantine.

 Proper testing of the sender validation server will ensure a successful implementation.

### ***Establish a Quarantine Period***

You might want to increase or decrease the quarantine period for your messages based on your company's requirements.


### ***Backup***

Make sure to check the backup status of the server to ensure that the server and sender validation databases are properly backed up.


## Post Installation Tasks and Best Practices

After installation is complete, there are some additional tasks to be done. If you use best practices for these tasks, you will enjoy a successful sender validation implementation:


- Document firewall changes—Make sure to document any firewall changes. Record the IP addresses of the sender validation server and mail servers. You might want to keep a copy of the original approved senders list just in case you need to restore it. Create contact information for any key personnel involved in the installation.

 Save the pre-sender validation firewall configuration in case you must bypass the sender validation server in the future.


- Back up the sender validation server—Make sure to incorporate a backup of the sender validation server into your existing backup strategy.

 Ideally the entire sender validation server should be backed up; however if you're short on backup space, the approved senders database is the most critical information on the sender validation server.

- Develop a failover plan—In the event of a hardware failure of the sender validation server, create a failover plan to temporarily bypass the sender validation server. This plan might require firewall reconfiguration, mail server reconfiguration, and MX record changes depending on your environment.
- Perform end user follow up—Survey a sample of users, gain feedback, and address any outstanding issues. Train end users how to send a test mail from a test account or other “approved sender” so that they can verify whether the mail is still working.

 Some users might experience such a dramatic decrease in spam they may think their incoming mail is not working.

- Check quarantine daily—For the first 30 days of the sender validation activation, check the quarantine location daily. Even with a preloaded approved senders list, users might still have a few senders in their quarantine list that they might want to manually add to the approved senders list. After 30 days, users can probably reduce the quarantine check to once every few days. Even with daily quarantine checking, users should still save a significant amount of time with the sender validation solution. When reviewing quarantine, train users to read the sender’s name rather than looking at subject line.

 Typically a user’s “mental filter” looking at quarantine is 10 times faster than looking through an Inbox filled with spam.

- Monitor logs, performance, and data backups—Review the logs on a regular basis and address any issues that arise. It’s a good idea to become familiar with the logs so that you get a feeling for what is normal and what is an exception.

Performance of the sender validation server is critical to ensure that mail is delivered in a timely manner and that the validation process is working. Make sure that the sender validation server has adequate disk space, processing power, and memory. Identify any bottlenecks by using tools such as the Windows Server Performance Monitor, and address bottlenecks as necessary.

In addition, review the backup logs to ensure that the sender validation server is properly backed up.

- Install upgrades, patches, and hotfixes—Install maintenance releases of the software when necessary.

### ***Dealing with eCommerce and Other Legitimate First-Contact Situations***

eCommerce and other first-contact situations can lead to false-positives because the senders typically do not respond to these emails. Train users to pre-approve the sender as well as to manage their quarantine to manually add these types of first contact senders to the “approved list.” Some sender validation vendors are working on enhanced features to automate this process in the future.

### ***Troubleshooting***

In rare instances, a user might get a spam message. Some sender validation solutions can track who or how a sender was validated. This feature is a good place to start when tracking down how a spammer was added to the approved senders list. Make sure that your internal mail server will only accept incoming mail from the sender validation server; otherwise, a spammer can bypass the sender validation server to deliver spam.

## Summary

Some sender validation solutions might support installation directly on the mail server in the future. Of course, you must be running a mail server that is supported by the sender validation solution. This option is attractive for companies with fewer users, because such companies do not have to purchase a dedicated server in order to implement a sender validation solution.

Another development on the horizon is the coexistence of a sender validation solution with firewall or anti-virus software. This develop will eliminate the need for a dedicated server for the sender validation solution. However, installing any service on top of a firewall will make the firewall less secure. It is less fault tolerant because you will lose multiple services if the firewall fails. If your firewall is already heavily loaded, a dedicated server is still the best solution.

Finally, a sender validation lite solution might become available on the market. Such a solution simply verifies that an email address belongs to a valid user and domain. It does not require a response from the sender. Although this option requires less processing power, it is easier to get messages past the spam filter by simply spoofing the sender's address.