realtimepublishers.com™

The Administrator Shortcut Guide™ To

Blocking Spam with Sender Validation

Alan Sugano

Copyright Statement

Chapter 2: Sender Validation Solutions

In the first chapter, we explored the growing crisis of spam as well as the spam-blocking methods available and being developed to overcome this problem. In this chapter, we'll delve deeper into sender validation solutions—exploring both client-based and server-based solution options. Although I will briefly cover sender validation solutions for individual use, the chapter will focus on business solutions.

The first step in implementing a sender validation solution in your organization is to select a sender validation service or dedicated server. But which solution is right for your environment? We will identify the critical considerations to help you determine the answer. In addition, we'll explore the steps necessary to implement the sender validation solution you select. Let's start by taking a look at client-based sender validation solutions.

Client-Based Sender Validation Solutions

Quite a few sender validation solutions are available for the desktop. Your options in this arena include both services and software that integrates with your existing desktop mail software. The following sections explore these solutions.

Sender Validation Desktop Software

You install sender validation desktop software on each workstation, as this sender validation solution is targeted more towards the end user—rather than a business that has its own internal mail server. Make sure that you pick a package that is compatible with your mail client software. Sender validation desktop software is best suited for POP3 and individual mail users. Figure 2.1 shows how sender validation filtering is performed on each workstation.

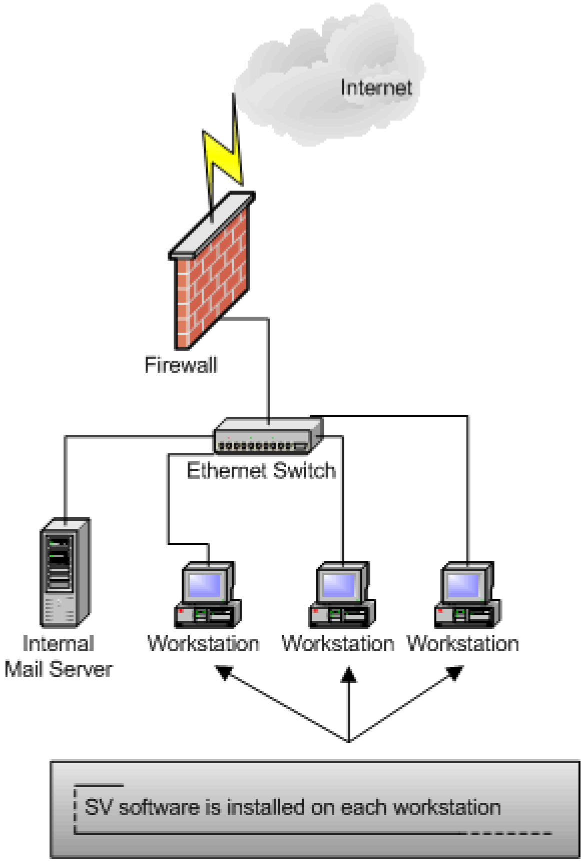


Figure 2.1: Sender validation filtering on each workstation.

The following list highlights desktop packages that use sender validation to fight spam:

- DigiPortal ChoiceMail (http://www.digiportal.com/) spam filtering software
- MailFrontier Matador (http://www.mailfrontier.com/products_matador.html) works with Outlook and Outlook Express
- MYmailSAFE (http://www.mymailsafe.com) offers both a consumer and business anti-spam solution
- Bongosoft (http://www.bongosoft.com/) is a newcomer in the anti-spam market
- Mail Wiper (http://www.mailwiper.com) provides a pop-up blocker with the purchase of the anti-spam software
- Spam Bully (http://www.spambully.com) integrates with Outlook and Outlook express

Remember to pick a package that is compatible with your mail client!

Some of these packages use sender validation in conjunction with other spam filtering methods—such as blacklists, whitelist, and Bayesian filtering—to combat spam.

Advantages

Sender validation desktop software is a useful solution for individual users that do not connect to a corporate mail server and use a single email package to access their mailboxes. It is also useful for users who always access their mail from the same email client. This option is a fairly low-cost solution for the individual user.

Disadvantages

Sender validation desktop software has the following disadvantages:

- It offers no central management.
- Changes/upgrades must be installed individually on each workstation.
- Not a good solution for more than a few users—server-based solutions are usually more cost effective for larger installations.
- Many client-based sender validation solutions require that your desktop computer be running 24 × 7 so that the software can immediately notify the sender of questionable mail; otherwise, this notification is delayed until sender validation is restared. This setup can cause validation delays of as many as 7 days if a user connects only once a day to send/receive mail.
- There is no “master list,” so each user must individually validate mail senders.

In addition to these drawbacks, the package must be compatible with your existing mail client—because this software is client specific, it does not work with a different client to access mail. This requirement is commonly a problem faced by users of Outlook Web Access (OWA) because the spam filtering software is not active when users access their mail though OWA. If such users decide to change their email client, they might need to also change their sender validation software.

Sender Validation Desktop Services

Some companies offer sender validation as a service. These services are also targeted more towards the end user. Figure 2.2 shows how a typical sender validation service is implemented on a workstation. Most services charge by mailbox and/or by megabytes of mail storage.

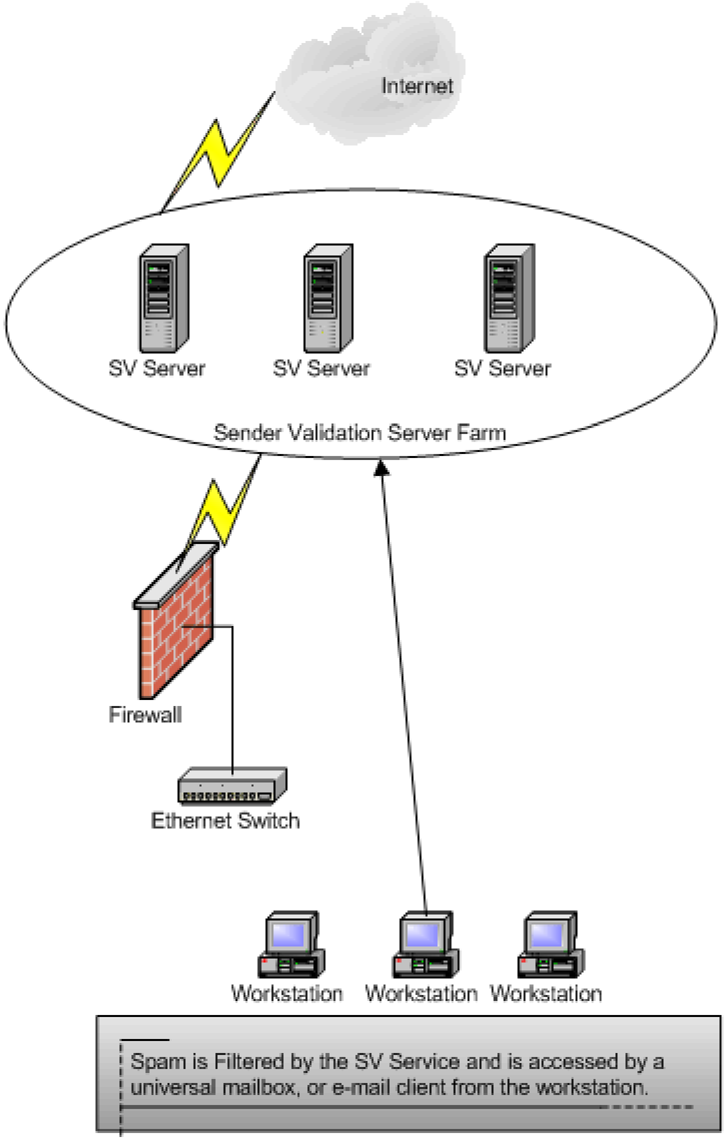

Internet
SV Server
SV Server
SV Server
Sender Validation Server Farm
Firewall
Ethernet Switch
Workstation
Workstation
Workstation
Spam is Filtered by the SV Service and is accessed by a universal mailbox, or e-mail client from the workstation.

Figure 2.2: Sender validation filtering service on a workstation.

The following list highlights companies that provide sender validation desktop services:

- Mailblocks (http://www.mailblocks.com) can consolidate as many as 10 mailboxes
- USOpt (http://www.usopt.com/) offers spam and virus filtering services
- Spam Arrest (http://spamarrest.com/products/individuals.jsp) works with any POP3 mail account

Advantages

These services are very easy to set up. In addition, they require minimal cutover planning and are usually easy to disable if you don't like the service.

Disadvantages

A drawback to this solution is that sender validation desktop services are often more costly in the long run: the typical break even point is 2 to 3 years compared with installing sender validation software on your workstation. In addition, your sender validation list is off-site and is dependant upon the service's and your Internet connection. Also, a service provider will sometimes charge extra for more storage because they have to track your approved sender's list and mail. As a minor security concern, the sender validation service has the addresses to and from which you send and receive email.

Sender Validation Integrated with the Mail Account

Just like some ISPs provide integrated antivirus scanning as part of the email service, some ISPs and application service providers (ASPs) offer sender validation integrated into their email service. This option is a good fit for individual users, but typically does not work well for a business. Figure 2.3 shows how sender validation is integrated with an existing ISP-provided mail account.

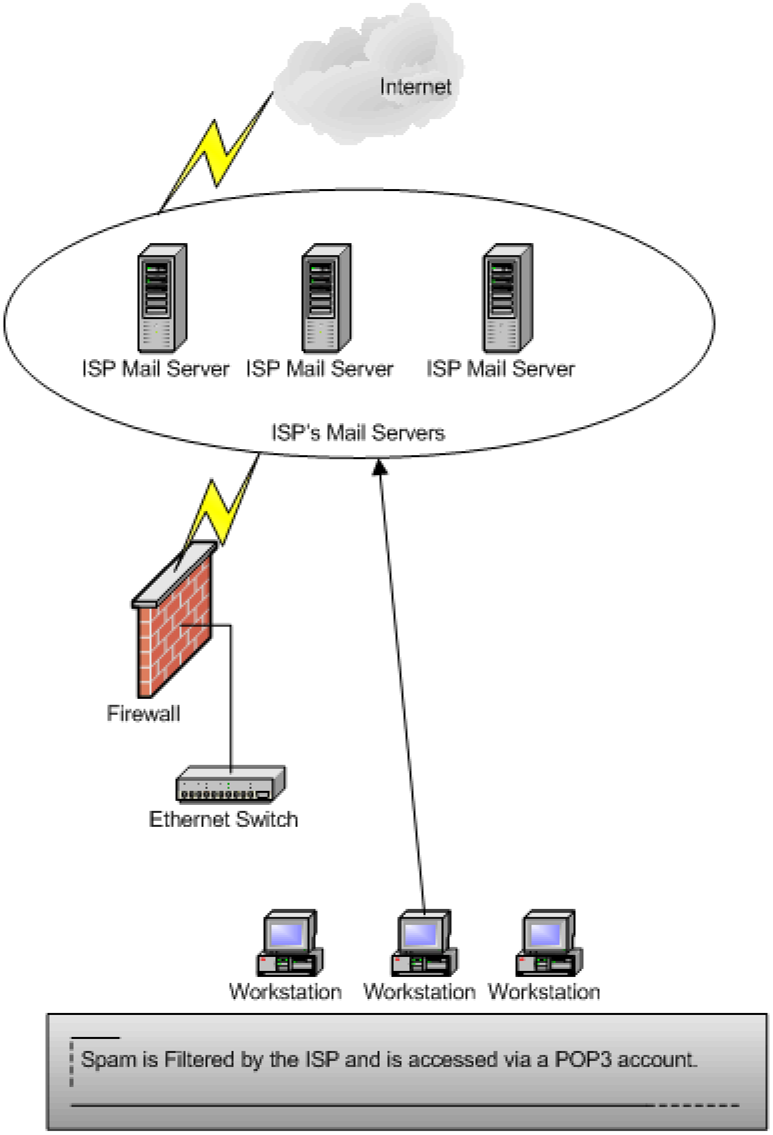


Figure 2.3: Integrated sender validation filtering performed by an ISP.

The following list highlights vendors and ISPs that provide sender validation solutions that are integrated into a mail account provided by the ISP:

- SpamLion (http://www.spamlion.com) offers an ASP version of its software designed to work with an ASP or ISP; this company's service enables you to keep your domain name and share protection among a group
- GoodbyeSpam (https://www.goodbyespam.com/) provides a package specifically designed to work with an ISP's mail service
- EarthLink spamBlocker (http://www.earthlink.net/) offers sender validation features: a sender's email address must be in the recipient's address book in order to for the recipient to receive the message; otherwise, the message is placed in quarantine

Advantages

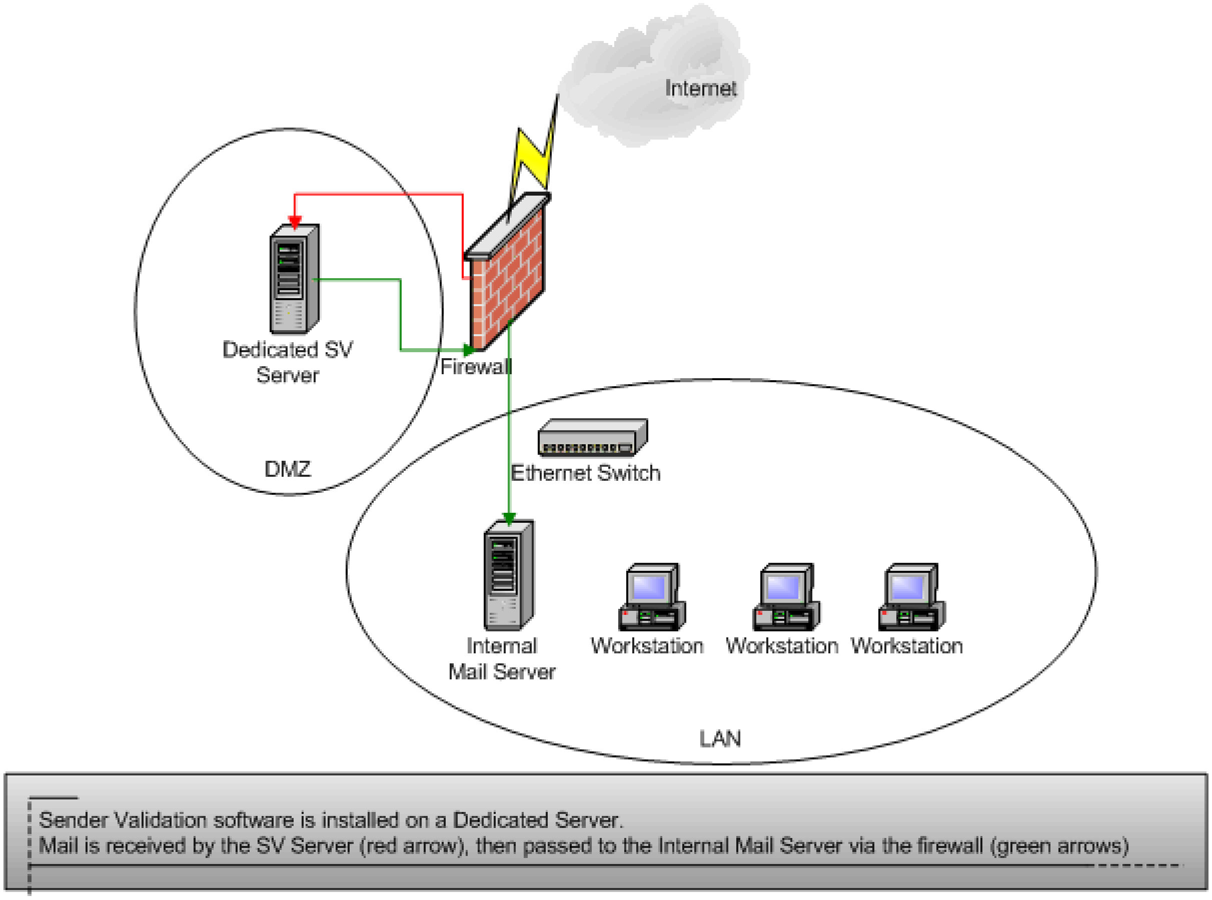
One of the benefits of this solution is that no mail server is required. In addition, some vendors offer Web-based email services that include sender validation protection. Typically the mail is accessed via a POP3 account.

Disadvantages

With the exception of SpamLion, this sender validation solution is for single users—not for business users—and has most of the same disadvantages as the desktop software and service solutions. In addition, typically, you must use the provider's domain name and cannot receive mail under a personalized domain.

Server-Based Sender Validation Solutions

If you're evaluating a sender validation package for your company, consider a server-based solution. For most companies, the server-based sender validation solution is more cost effective and far more practical to use than installing a sender validation solution on each workstation or using a sender validation service. Server-based sender validation solutions are easier to implement in an enterprise environment because no additional software is necessary on the workstation. They're mail client independent, so if a user accesses the mail with a different client—wireless, OWA, or some other method—the anti-spam software still works because it operates at the server—not desktop—level. Figure 2.4 displays how server-based sender validation is integrated into an existing network.



Sender Validation software is installed on a Dedicated Server.
Mail is received by the SV Server (red arrow), then passed to the Internal Mail Server via the firewall (green arrows)

Figure 2.4: Sender validation filtering on a dedicated server.

Sender Validation Business Server Software

The following list highlights vendors that offer server-based sender validation solutions for a business environment. These packages are compatible with any mail server that uses SMTP:

- SpamLion (http://www.spamlion.com/CorporateEdition.asp) is typically installed on a dedicated server and can handle a range from ten to thousands of users
- MailFrontier (http://www.mailfrontier.com/products_asg.html) can be installed on a Windows- or Solaris-based computer; in addition to sender validation, MailFrontier uses blacklists and Bayesian filtering to catch spam

Advantages

If your company has a policy of not allowing mail to be handled by a third-party, a software-based server solution is a good fit. They are locally managed, and, typically, the approved sender list can be backed up with existing tape backup software. In addition, server-based sender validation solutions offer the following advantages:

- There is little maintenance after the system is up and running.
- Depending on your mail volume, these packages are not too resource intensive, so a “super” server is not necessary. Some packages will run on your existing mail server and some will run on Linux and other free OSs. The dedicated server will align with other servers (mail, firewall, file and print) just like any other infrastructure server on your network.
- Software that runs on a dedicated server is typically compatible with any mail server that supports SMTP. Some packages can coexist on an existing Web server for reduced startup costs.
- Most sender validation solutions include a Web-based user interface that ensures compatibility with almost any mail client and OS.
- If you’re running Microsoft Exchange Server, some solutions have enhanced features that integrate specifically with Exchange Server.
- For the enterprise environment, some solutions offer load balancing and failover to reduce the probability of downtime. If they do fail, you can simply redirect traffic on the firewall to bypass the sender validation server.

Disadvantages

Most sender validation packages run best on a dedicated server, so the startup cost is higher than that for software that installs on an existing mail or Web server. In addition, some end-user training may be required for users to manage their quarantine and approved senders lists.

For a dedicated server solution, the OS must be installed before the sender validation software can be implemented. The sender validation will require some maintenance (service packs, bug fixes, software updates, and son on), but will not require blacklist, keyword, or message pattern updates.

Some packages require an annual license and do not offer one-time purchase options. And some packages require ISP support using a secondary email relay server to fully implement their failover solution.

Sender Validation Business Services

Some vendors provide sender validation as a service. A sender validation service offers the advantages of a faster implementation and lower initial investment. However, using a sender validation service will probably cost your company more money in the long run. That said, this option is a good alternative if you're short on IT staff and have less then 50 email users to protect. Figure 2.5 shows how a sender validation service is integrated into an existing network.

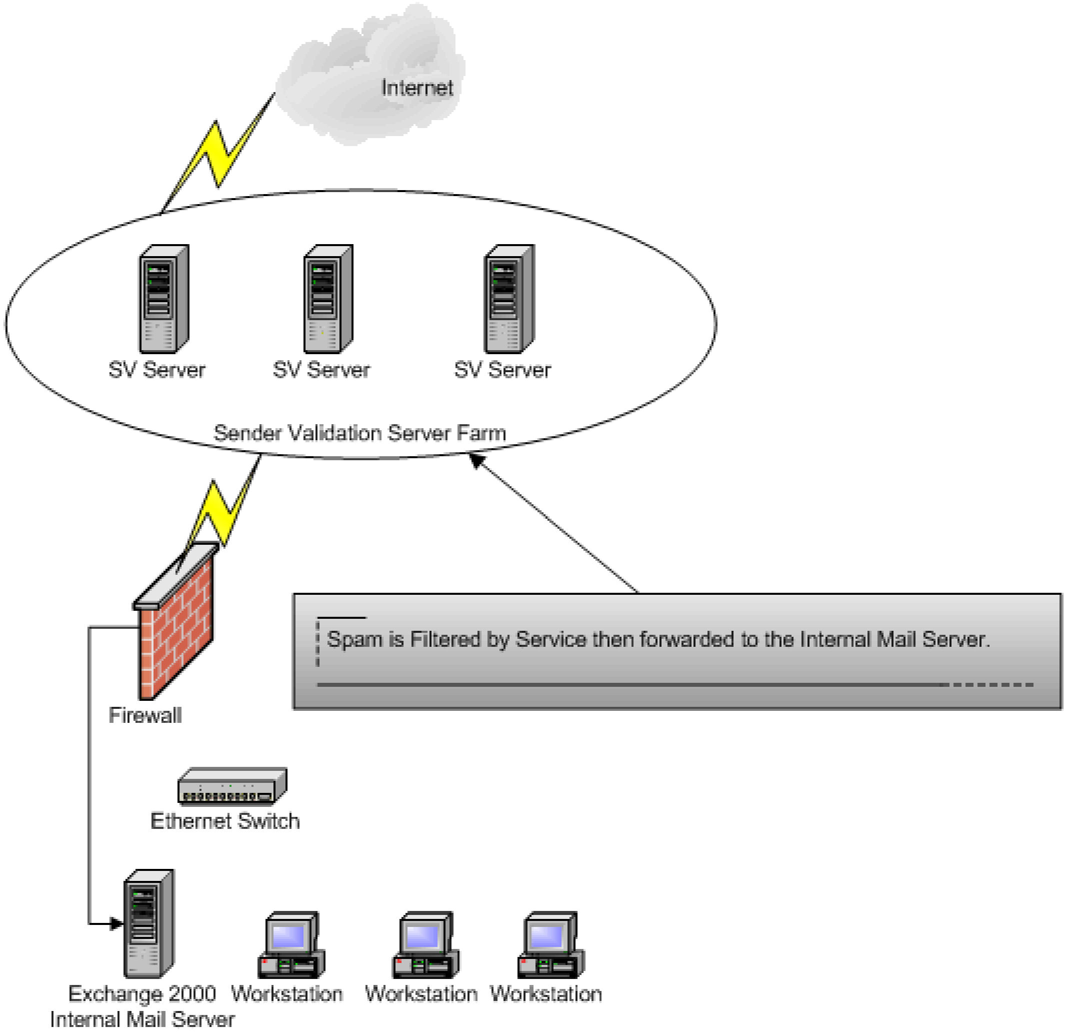


Figure 2.5: Sender validation filtering service.

The following list highlights companies that offer sender validation services for businesses:

- SpamLion (http://www.spamlion.com/SpamLionService.asp) offers a service that has an expandable 10-user license
- Hushmail (https://www.hushmail.com/services.php?PHPSESSID=475a528134b3e892a14b3c083f161107&subloc=identity) offers, in addition to sender validation services for business, 2048 mail encryption and digital signing of mail messages

Advantages

This sender validation solution offers shorter implementation time and lower startup costs. In addition, there is little maintenance after the system is up and running. All of the sender validation services are hosted off-site, so you don't have to worry about maintaining another server: no backup issues or maintenance.

Disadvantages

If your company has a policy of not allowing mail to be handled by a third-party, sender validation business service is not an option. In addition, a service may cost more in the long run: typical payback for a dedicated server is less than 2 years. If the service goes down, you will have no mail or spam filtering until the service comes back up. If the service stays down for an extended amount of time, you must change your MX record in order to receive mail. Most services charge by the user, so each additional user will increase your sender validation filtering expense.

🕮 Need more information? Refer to the following sites about sender validation solution and other spam related topics:

🕮 http://www.spamcon.org/

🕮 http://www.1stopspam.com/stopspam/Anti_Spam_Organizations/

🕮 http://www.spamanti.net/en/news/news200310.php

Sender Validation Planning and Implementation

When considering a sender validation solution for your company, there are a few factors to consider before making your final purchase decision. The following sections explore these additional items that you should consider before purchasing and implementing a sender validation solution in your company. From this point forward, we will focus on sender validation for a business.

🕮 If you're considering a sender validation solution for personal use, take a look at one of the products mentioned earlier.

Evaluating Sender Validation in Your Environment

For any large sender validation implementation, consider a “proof of concept” test to determine how sender validation will work in your environment. Such a test will answer the following questions:

- How will sender validation work with the type of mail my company receives and sends?
- How will my users react to managing their approved senders and quarantine lists?
- How will the sender validation solution handle the anticipated mail load?
- If the sender validation solution is installed on an existing mail server, how will the mail server be able to handle the additional load?
- How will the sender validation solution integrate with my firewall?
- How will the sender validation solution integrate with my mail server?

Consider each of these questions before making a final sender validation purchase decision.

The Right Sender Validation Solution for Your Company

Should you go with a sender validation service or a server-based solution? There are some important factors to consider when making this decision. The following items should help you determine which sender validation solution (service or server-based) is right for your company:

- Number of email users—Sender validation services are a good fit for companies that have 10 to 50 email users. For a larger number of users, it’s generally more cost effective to implement a sender validation server-based solution. With a server-based solution, the larger number of email users, the shorter the payback period, compared with a sender validation service. For example, the typical payback period for 100 users using a sender validation server-based solution is just over 1 year, compared with using a sender validation service. If your company is small but growing rapidly, consider implementing a dedicated server because you will save money in the long run. In general, the greater the number of users, the more cost effective the dedicated server solution will be.
- Company email policy—Some companies have a policy that email must be handled internally. If your company has this requirement, an internal sender validation server-based solution will be your only option.
- Integration with existing mail server and infrastructure—Most sender validation packages integrate with existing mail servers as long as the servers support SMTP. Because the packages work at the server level, you don’t need to worry about email client compatibility. If you’re running products—such as GalSync, Alias Identification, Blackberry Enterprise Server, and Auto NDR—check with the sender validation solution’s vendor to see how well the solution integrates with these or any other email–infrastructure–related packages. This item is an important consideration regardless of whether you select a sender validation service or sender validation server-based solution.

- Product evaluation/demo—For this category, consider the following questions:
    - Does the company offer an evaluation?
    - Is it possible to see a running demonstration of the software package?
    - Is it possible to have the demonstration run with samples of your email?
    - Can you try before you buy?
    - How do the users like the interface?
    - How powerful is the administration interface?
    - Is the package easy to use?
    - Does the sender validation solution offer different ways to handle the validation process?
    - How easy is the validation process for email senders?
    - How easily can a spammer get around the validation process?
    - Will the sender validation solution handle your current and future email load?
    - Is the product scalable?
    - What type of fault tolerance does the solution provide?
    - How easy is it to bypass sender validation filtering in case there is a problem with the sender validation service or sender validation server-based solution?
    - How long has the sender validation solution been around?
    - How do companies that use the sender validation solution like it?
    - How stable is the product (what is the service's historical uptime percentage)?
- Funds—Do you have the budget for a dedicated server, sender validation software, and installation costs? Make sure that you have enough backup capacity on an existing tape drive or consider purchasing a dedicated tape backup and software for the sender validation server. If you're short on capital, the initial startup costs are less with a sender validation service compared with a sender validation server-based solution. The more mail users that you have, the faster you can recoup the cost of a dedicated server. You might want to budget for a consultant to ensure that the sender validation solution is properly integrated with your existing DNS, STMP routing, and firewall configuration.
- Internal IT resources—If your company is short on internal IT resources, a sender validation service might be a better fit. The sender validation service can be implemented with fewer internal resources—both in the initial setup and ongoing maintenance. If you are short on IT resources but still want to implement an internal sender validation server-based solution, budget for consulting work to assist in the implementation to save time spent on incorrect configuration and problem solving.

- Virus scanning—An important item to remember is email-based viruses. Sender validation does not check for viruses! Although less than 99 percent of all email viruses come from spammers, a best-of-breed antivirus solution is a good idea. Check whether your current antivirus solution has a dedicated email virus scanner. Some sender validation services have the option of scanning for viruses, which I highly recommend you purchase. Regardless of which sender validation solution you ultimately decide on, you should still maintain virus protection on your servers. If the sender validation service goes down, you might need to bypass the sender validation/virus scanning and accept email directly into your server. For this reason, you should still maintain virus scanning on the server. If you allow users to check their email from POP3 accounts, you still have virus exposure from this source.

> Don’t think you are immune to viruses just because you have sender validation filtering!

- Availability—If you’re leaning towards the sender validation service, ask the provider about the number of servers, number of users per server, average server utilization, peak server utilization, type of connection, connection redundancy, historical uptime, and a service level agreement (SLA) if the service goes down. In general, you have more control over an internal sender validation server-based solution; you are at the mercy of the sender validation service if the line or server goes down (most sender validation services provide redundant connections, so your email will queue rather than not be delivered). Talk to other companies to see how happy they are with the level of service that the sender validation service vendor provides.
- Licensing—Make sure that the sender validation solution vendor offers product licensing that is a good fit for your company. Find out the following licensing information so that you can compare among vendors:
    - How is the product licensed (per user, per server, per megabyte of storage, per month, per year, one-time license, renewable annually)?
    - Is a maintenance contract required?
    - Are upgrades included in the purchase price?

- Product support—The answers to the following questions are more important if you select a sender validation server-based solution; however they are still important for the sender validation service:
    - Does the company offer 24 × 7 support?
    - Is there an additional cost for extended support?
    - How well does the vendor know their product?
    - Does the vendor have expertise in implementing this package in an enterprise environment?
    - Does the vendor have a staff of implementers that can provide onsite help if necessary?
    - How much does onsite support cost?
    - Does the vendor have experience with your mail server and firewall?
    - What is the average size of their implementations?

> ☞ Particularly for a sever-based sender validation solution implementation, modifications to the firewall, existing mail server, and sometimes MX records must take place in order for the sender validation software to work correctly. Selecting a vendor that is familiar with your environment will prevent problems during the implementation.

- Sender validation service cancellation policy—Obtain the service’s cancellation policy in case you want to move to another solution. It is better to know the answers to the following questions before signing up for a service so that there won’t be any surprises if you decide to cancel the service and move to a dedicated server solution:
    - Before purchasing a solution, get answers to the following questions:
    - Does the vendor need advance notice to cancel the service? If so, how long?
    - If you decide to move to a server-based sender validation solution, can you transfer the approved senders list to an internal server?

Necessary Steps to Implement a Sender Validation Service

Once you've decided to go with a sender validation service, follow these suggested implementation steps (I'll walk you through implementation steps for a server-based sender validation solution in a moment):

- Select a sender validation service—Make sure users are comfortable with the user interface offered by the service. Ideally, test the service with your company's email to make sure the service is a good fit for the company. Carefully review the administration capabilities of the sender validation service before making the final selection. During the evaluation phase, some sender validation companies have the ability to turn on sender validation filtering for certain email accounts with any remaining accounts set to a "by-pass" mode.
- Consider a phased rollout of sender validation—Consider at least a two-phased approach when rolling out the sender validation service. Phase one will be a select number of power users. After phase one, you can fine tune sender validation, address any issues that arise, and provide additional training before rolling out sender validation for the entire company. The last thing you want is a bunch of upset email users as a result of your failure to anticipate all of the potential problems prior to the rollout.
- Train end users—Make sure that your users understand the validation process and can add/delete users from the approved senders list.
- Change your MX record—You must redirect your MX record to the servers of the sender validation services. The service's servers will redirect your email to your internal server. You might want to add a backup MX record to your ISP's mail server in case the sender validation service's mail goes down (so they can hold the mail for you). You can set a backup MX record directly to your internal server; however if the service does not respond in a timely basis, mail will be directly delivered to your mail server bypassing the sender validation service. In addition, if a spammer discovers 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. If you decide to use a backup MX record that points directly to your internal mail server, create a rule on your firewall to only accept incoming mail from the sender validation service's servers and your ISP servers. That way, the firewall will prevent anyone from sending mail directly. If the sender validation service's servers go down, simply disable this rule to bypass the sender validation servers and allow incoming mail to flow directly to your internal mail server. It's much easier to disable a rule on the firewall than calling the ISP to change the MX record for your domain, and waiting for the change to replicate across the entire Internet.
- Mail server modifications—Some sender validation services have the capability of auto-adding outgoing email addresses to the approved senders list. To use this functionality, you must redirect your outgoing mail to the sender validation service's mail server. Alternatively, some sender validation services require installing a "learning" module on your existing mail server. If you don't plan to use the learning feature, no modification of the mail server is usually necessary. Without the learning module, everyone must complete the validation process, which is a big inconvenience. This inconvenience was a major reason why earlier attempts at sender validation were rejected. I strongly suggest turning on the auto-learn feature.

- Follow up—Expect some issues to arise when turning on the sender validation service. Some users will require help adding/deleting users on their approved senders list, and senders might have difficulty completing the validation process.
- Quarantine period—You might want to increase or decease the quarantine period for your messages based on your company's requirements.

Necessary Steps to Implement a Sender Validation Dedicated Server

If you have more than 50 users, consider a sender validation server-based solution. It's usually more cost effective to run an internal sender validation server compared with the cost of a service. The dedicated server will handle the sender validation process. Consider the following suggestions when implementing a dedicated server sender validation solution:

- Select a sender validation package—As with the first step of implementing a sender validation service, make sure users are comfortable with the user interface. In addition, obtain answers to the following questions:
  - Does the software package have a planning guide to assist in the implementation?
  - What type of support does the vendor offer during the transition period?
  - Does the vendor offer support after the initial transition is complete?
  - Does the software vendor have expertise only in the software package they support? (Ideally the vendor should be familiar with your mail server, firewall, ISP, and MX record changes.) The more familiar a vendor is with your network, the smoother the transition should be.
- Consider a phased rollout of sender validation—This consideration follows the same guidelines as with a sender validation service implementation. The phased approach provides a safety net with limited exposure in case unforeseen issues arise.
- Train end users—Depending on the level of experience of your user base, it might be necessary to train your users on how 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/off-site. If you do not have a firewall, I strongly suggest purchasing one before implementing the sender validation server. It will be more difficult and ultimately take more time if you have to install a firewall after you install the sender validation server. If your firewall has the capability, I suggest installing 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. The downside of placing the sender validation server in the DMZ is that the firewall configuration is the most complex with this topology.

- DNS changes—Usually no DNS or MX record changes are necessary to implement the server if you redirect mail by altering your firewall configuration. An MX record change pointing to the sender validation server might be necessary if you want OWA users to retain the same IP address.
- Firewall changes—To set up the sender validation server, you must redirect incoming mail from your internal mail server to the new sender validation server. If you are running Web-based validation, you must redirect port 80 traffic to the sender validation server. Doing so can be problematic if you're self-hosting an existing Web site—although some sender validation servers can coexist with an existing Web site. If you want the sender validation solution on a separate server, you can either set up an additional external IP address to handle the Web-based validation or use port redirection on the firewall to handle inbound Web-based validation. If you are running any VPNs, make sure to test the sender validation server with the remote locations to ensure that they can use the sender validation server.

Summary

Sender validation packages come in various forms: desktop software, desktop services, integrated with an ISP-provided email account, dedicated business server, and business service account. As we explored, each of these sender validation solutions has advantages and disadvantages, and there are many vendors to choose from for each of type of solution.

We also looked at the critical issues to help you select a package that meets your company's needs. A little homework up front will help you with a successful implementation. After addressing the questions in the evaluation section, you should have a good idea which sender validation route to take. Once you decide on the right type of solution, you can follow the suggestions in the related implementation steps section.

In the next chapter, we'll take a look at cost justification of the sender validation solution. Don't worry—sender validation is probably one of the easiest IT projects to cost justify. We'll take an in-depth look at the implementation steps necessary to ensure a successful sender validation rollout for your company. We'll also discuss ongoing support issues, upgrades, maintenance, and how to support additional users. Finally, we'll explore what the future holds for sender validation.