SpamLion, Inc.
Sender Validation Gateway™

SpamLion, Inc.
P.O. 549
Cotati, CA 94931

Phone (707) 585-1200
Fax (707) 585-6206

SpamLion Sender Validation Gateway™

Easy Installation Guide for version 1.60

SpamLion Sender Validation Gateway™ - Easy Installation Guide v1.60

Tell Us What You Think

As the reader of this publication, you are our most important critic and commentator. We want to know what we're doing right, what we could do better, and any other comments you're willing to pass our way.

Please include the following information:
Title: SpamLion Sender Validation Gateway – Easy Installation Guide for version 1.60

Send all correspondence to:
John Swanson, Technical Editor
SpamLion, Inc.
P.O. 549
Cotati, CA 94931
(707) 585-1200
(707) 585-6206 Fax
mail to: jswanson@spamlion.com

Technical questions, mail to: support@spamlion.com
Corporate Web Site: www.spamlion.com

Table of Contents

INTRODUCTION **5**

Overview **5**

Benefits **5**

Requirements **5**

Placement **5**

Support **7**
Purchased SpamLion Solution 7
Trial Installation 7
Network Engineering Services 8

EASY SETUP **9**

1. Complete the Easy Installation Network Diagram **9**

2. Prepare your SpamLion Server **10**

3. Download SpamLion Gateway installation software to the SpamLion computer **10**

4. Locate the SpamLion license file **10**

5. Run the SpamLion Installer program **10**

6. Start the SMTP and W3 services **11**

7. Set appropriate NTFS file permissions **11**

8. Complete the Initial Database Configuration **11**

9. Set the Operating mode **11**

10. Start SpamLion service **11**

11. Finalize the appropriate SpamLion settings **12**

12. Synchronize Receivers to Mail Server **12**

13. Export Active Directory Contacts as Receivers (Optional) **12**

14. Export Active Directory Distribution Lists to create Senders (Optional) **13**

15. Import Outlook and/or Outlook Express contacts as valid senders (Optional)..... 13

16. Enable Dictionary Harvest Attack defense 13

17. Configure SpamLion Logging Settings 13

18. Configure SMTP Mail Delivery Settings 14

19. Send outbound mail through SpamLion..... 14

20. Allow inbound mail flow through SpamLion 14

21. Insure SpamLion is operational 14

22. Set up housekeeping tasks 14

23. Rollout Anti-Spam Protection 14

24. Check for trial license expiration 15

25. Relax 15

Introduction

Overview

A SpamLion Sender Validation Gateway™ is an anti-spam solution that is placed in your corporate network to protect your email recipients from receiving unsolicited commercial email. SpamLion is software that must be installed on a computer in your corporate network. Once the software is in place, simply personalize the response message that each first-time sender receives and synchronize mail addresses on your mail server with SpamLion. Enable mail to flow through SpamLion at your firewall and mail server and SpamLion will begin protecting your users while automatically learning and validating the addresses of everyone to whom you send mail.

Benefits

What are the Customer Benefits to a SpamLion solution? The top five reasons we hear from satisfied customers are:

- Increased employee productivity as well as corporate security.
- Limit legal liability resulting from a possible 'hostile work environment'.
- Saves disk space and processing cycles on your existing Mail Server.
- Keeps unwanted traffic off your private network, preserving your bandwidth.
- Strong, effective defense against Dictionary Harvest Attacks (DHA).

Requirements

SpamLion is a server-based product that requires its own computer. The computer must be running one of the following operating systems:

- Windows 2000 Server,
- Windows 2000 Professional,
- Windows XP or
- Windows Server 2003.

The computer hardware must be scaled to the message traffic that it will process. An installation protecting under 300 mailboxes with moderate message traffic will run adequately on a workstation class computer: Pentium 4, 1GHZ processor, 256MB RAM, 60G HDD, 10/100 Mbit Network Interface Card. Larger messaging situations will require a faster processor, 512MB RAM, and a hardware RAID solution for the disk system.

An email network with fewer than 50 mailboxes will generally run on Windows 2000 Professional or Windows XP. A mail network consisting of more than 50 mailboxes requires a server-class operating system such as Windows 2000 Server Standard Edition or Windows Server 2003 Standard or Web Editions.

Placement

The SpamLion Anti-Spam Gateway is software that is composed of 3 major components:

- A web site used for Administration, Sender Validation and Quarantine Management,
- A Mail Examiner which provides the interface with the SMTP mail transport and the rest of the SpamLion system, and
- The SpamLion Engine (NT Service) and Database.

SpamLion will protect any mail server (Exchange, GroupWise, Lotus Notes) regardless of the Operating System that it runs on (Unix, Linux, Windows, Novell); however, you must be using a mail server that is not a virtual server hosted by an Internet Service Provider (ISP). In other words, you must own your e-mail domain name and the mail server must be an independent machine (dedicated IP address) capable of forwarding mail. If the last condition is not met, you shouldn't be using this product.

Many smaller companies have their ISP provide Web and Mail hosting services and want the benefits of a SpamLion Sender Validation solution. If you find yourself in this situation, you may still deploy a SpamLion on a computer in your office, provided you have an available fixed IP address available or you may have your ISP host the solution in their co-location facility for you. If this is the case, then you loose the functionality of having SpamLion automatically "learn" and validate to whom you send mail. Other than that, SpamLion will work for you protecting your recipients from the intrusion of inbound unsolicited commercial email.

The following illustrations show a typical email network in increasing levels of detail. The first section shows simple mail server to mail server communication using SMTP transport over the Internet.

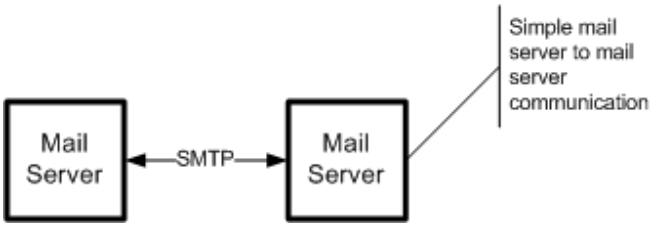

Figure 1, Simple Mail Server to Mail Server

Next we see computers with their e-mail client software such as Outlook, Outlook Express, Netscape Mail, GroupWise, or Eudora, to name a few, connecting to their mail servers which in turn, connect to other mail servers on the Internet.

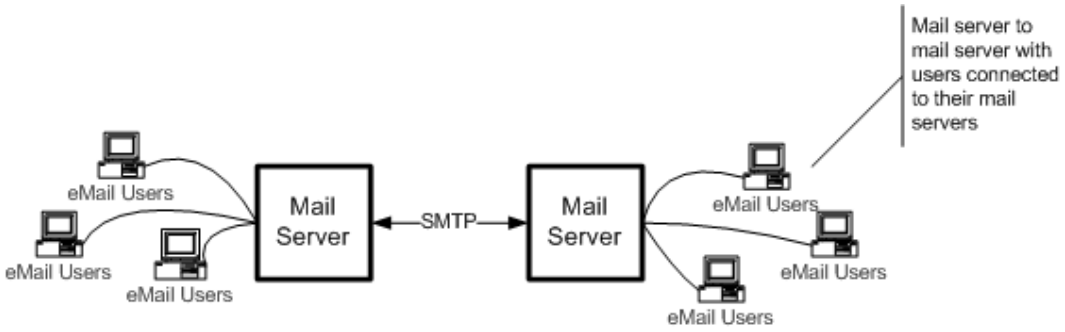

Figure 2, Mail Server to Mail Server with email clients

The third section shows the network from your company's perspective. Here, a firewall separates your network from the Internet.

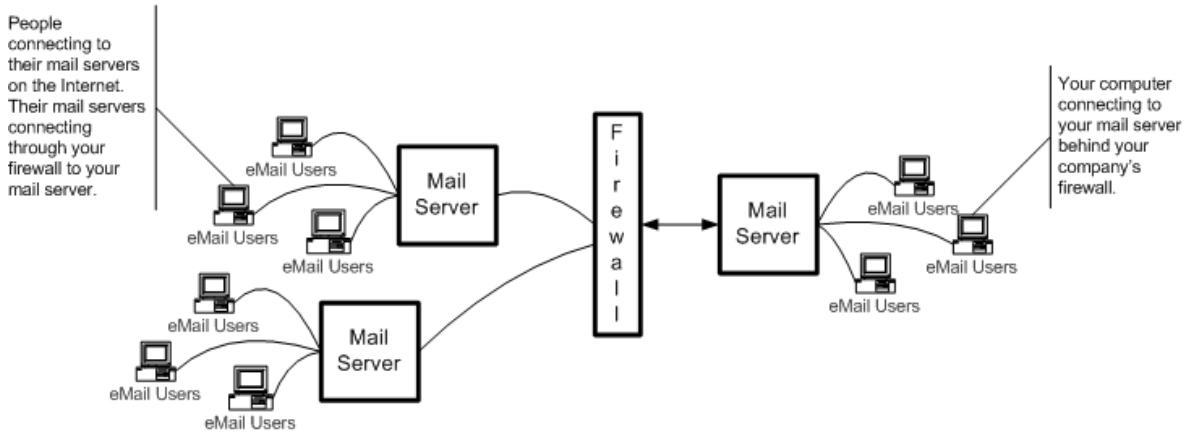

Figure 3, Typical corporate email network

The SpamLion Gateway may be positioned anywhere between the Internet and your mail server. The most popular placement of the SpamLion computer is on the inside LAN portion of your company's network; that is, behind the firewall. This is shown in Figure 4.

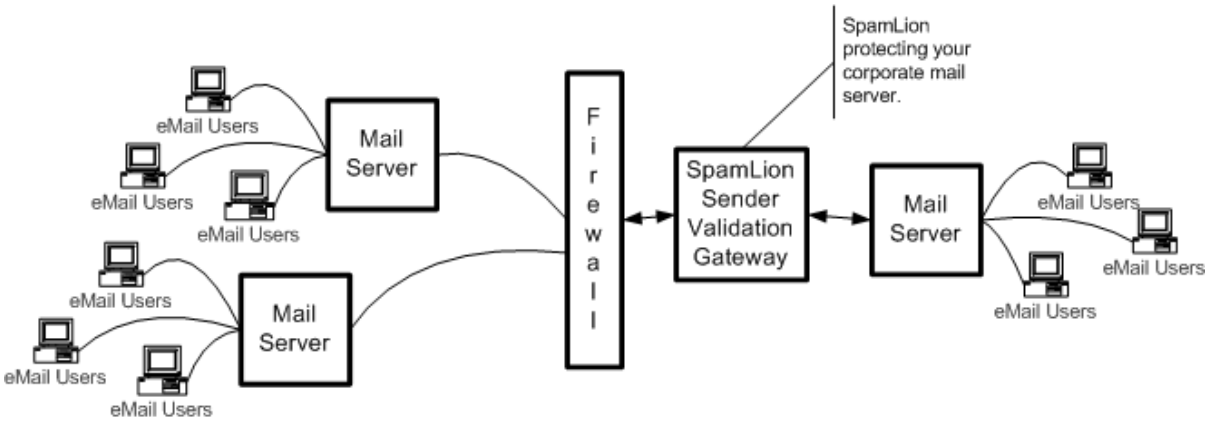

Figure 4, SpamLion placement in typical company network

With this configuration all IP Addressing will be in terms of the private IP Address range. The Firewall provides network address translation to the mail server. The most common way to route incoming mail to the SpamLion computer is to change the firewall's routing to forward all SMTP traffic to the SpamLion computer instead of the protected mail server. This technique involves no DNS changes. Next, HTTP traffic, commonly on port 80, needs to be forwarded to the SpamLion computer to enable administrator, user and first time sender validation access.

SpamLion is designed to forward all inbound mail destined for your registered domain(s) to the protected mail server and to only accept outbound mail from your protected mail server. Likewise, you protected mail server or bridgehead must be configured to deliver all outbound mail to the SpamLion Gateway server. This provides a "secure" mail relay mechanism that will not exploited by spammers.

Support

The installation model that has just been presented covers over 90% of all situations where SpamLion is currently deployed. Review your network to determine if it fits the model described here. If it does then proceed to the next section which will take you step by step through the installation and configuration of your SpamLion Sender Validation solution.

Purchased SpamLion Solution

If you have already purchased a SpamLion solution, then a free Support Incident is included in the purchase price. It may be used to assist you in your installation and configuration, provided that your situation fits the model currently under discussion.

To open a support ticket, visit our web site at http://www.spamlion.com and select Support from the main menu or call our corporate office at 707 585-1200. Tell the attendant that you have purchased a SpamLion solution and you would like to open a support ticket on a paid installation. Be sure to provide your serial number when requested.

Trial Installation

If you have chosen to run SpamLion in a 45 day Trial, then you may open a support incident by visiting our web site or calling the corporate office as described in the previous section. The charge will be $250. Alternatively, we suggest that you work with your SpamLion Authorized Partner or Reseller.

Network Engineering Services

If your situation does not fit within the deployment model under consideration, then call our Sales department at 800 761-7899 to discuss your situation. Based on an initial consultation with one of our support engineers, we will suggest a remote installation service plan that will fit your situation.

Remote installation services are pre-paid and non-refundable. They consist of from 1 to 4 contact hours of professional services. You will be working directly with a support engineer who will assist you with the installation and configuration of your SpamLion. It also includes recipient address synchronization with your mail server, import of contacts from your mail server or mail clients, and administrator training.

Remote installation service uses remote control software such as PC Anywhere, Remote Desktop, Net Meeting or VNC to work on your SpamLion directly across the Internet while in a phone conversation with your IT provider. Working with one of our consultants, guarantees that you are up and running in minimum time with little if any disruption to your mail services.

Note that in all instances, SpamLion support engineers are not in a position to assist you with the configuration or modification of your firewall or with modifications to DNS.

Easy Setup

The following sections take you through the installation tasks in chronological order, step by step.

1. Complete the Easy Installation Network Diagram

Fill in the sheet with the name(s) of your protected email domain(s), the IP address of the SpamLion computer and mail server.

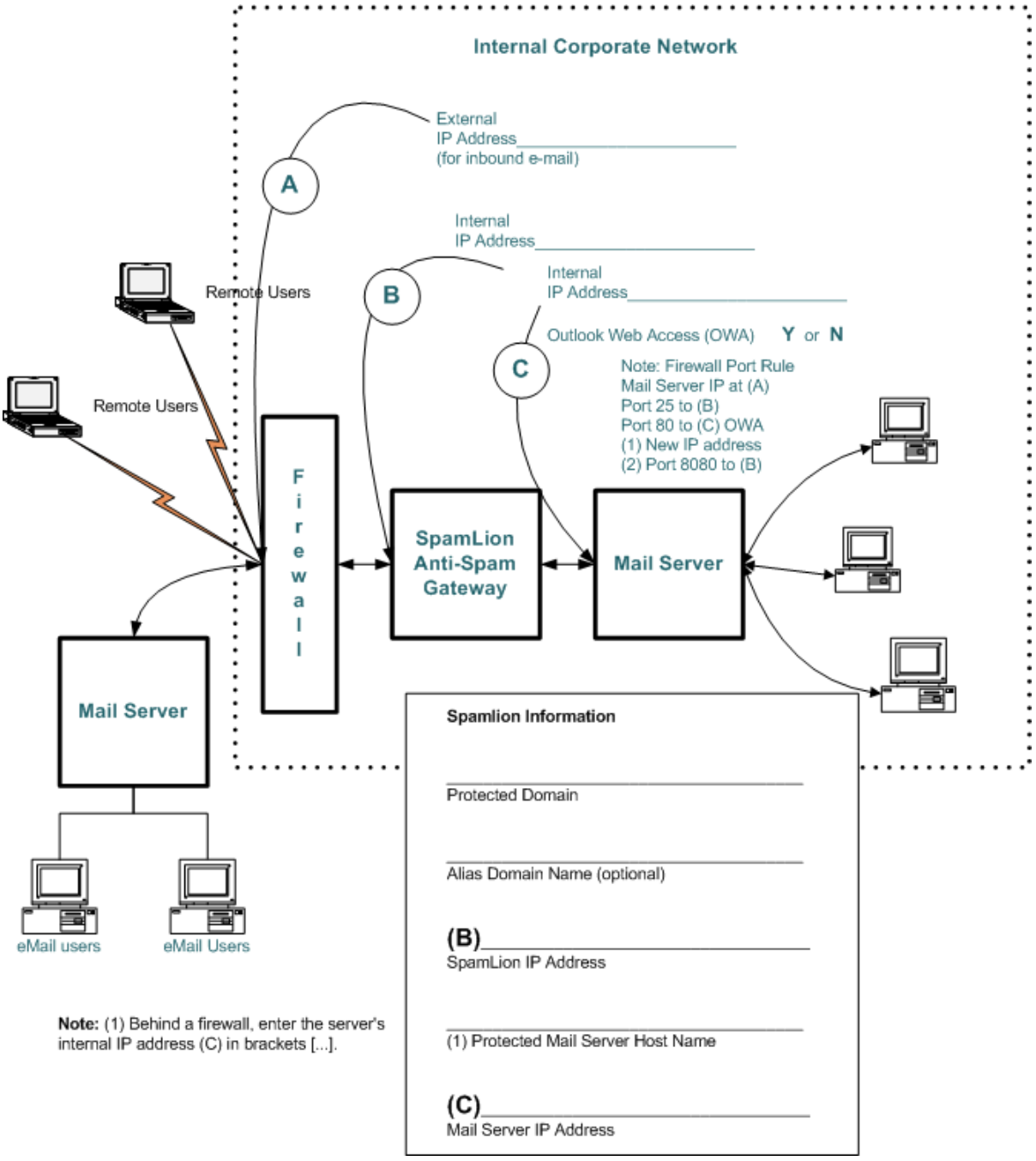

Figure 5, SpamLion Settings

The SpamLion Gateway solution includes a web site to process sender registrations and to provide a

login for the Administrator and protected receivers. If you are NOT using Exchange Server's Outlook Web Access (OWA), then the firewall routing is straightforward, forward HTTP, port 80 traffic to the SpamLion computer. If you are using OWA, then the SpamLion Web site must be configured to use a port other than 80, for example, 8080. The firewall NAT may then forward HTTP port 8080 traffic to the SpamLion computer; while directing port 80 traffic to the protected mail server where the OWA web site is generally located. Use the Internet Information Services Manager to configure the SpamLion web site to use a port other than the default port 80 and include that port number in the Inside and Outside URLs that are specified on the Initial Database Configuration web page. You will perform these steps after SpamLion installer program completes.

2. Prepare your SpamLion Server

Select a computer system that meets the criteria described in the previous section, "Requirements". We recommend that you do not use computers that have been configured by the computer vendor from an image unless you are familiar with the contents of the software contained within that image. When in doubt, format the hard drive and begin with a fresh installation of the operating system.

Install the Windows operating System. Your Operating System choices are:

- Windows 2000 Server, Professional,
- Windows XP and
- Windows Server 2003 Standard, Enterprise and Web Editions.

For Windows 2000 Server, Professional and XP, install Internet Information Server 5.0 (IIS), the latest Windows 2000 Service Pack, and the appropriate Critical and Security Update(s) from the Microsoft Windows Update site. The IIS 5.0 components include ONLY: Common Files, IIS Manager SnapIn mmc, SMTP Service and World Wide Web Service. You are limited to 10 IIS sessions; choose this in low-traffic environments.

For Windows Server 2003 (all Editions), install Internet Information Server 6.0 (IIS), the latest Windows 2000 Service Pack, and the appropriate Critical and Security Update(s) from the Microsoft Windows Update site. IIS 6.0 components include ONLY: Common Files, IIS Manager SnapIn (mmc), SMTP Service and World Wide Web Service.

Do <u>no</u>t make the computer a member of a security domain. All security will be in the context of the local machine.

Once the OS is installed, ping servers on the Internet and your mail server by IP address and hostname to insure that you have reliable network connectivity through your firewall.

3. Download SpamLion Gateway installation software to the SpamLion computer

Download the SpamLion product from the SpamLion FTP site, ftp://ftp.spamlion.com/download. Navigate to the Installation-Gateway-v1.60 folder. You can run the self-extracting archive file directly from the FTP site or you can download the zip or the exe file to your hard disk and extract from there. Tip: Create a folder to contain all downloaded components such as C:\Install. When you run the self-extracting archive (exe), the software will expand into its own sub-folder. If you manually unzip the contents make sure that you retain the folder structure.

4. Locate the SpamLion license file

Place the product license file, "spamlion.lic", into the root of the product installation sub-folder referred to in the previous step. The license file is an attachment to the Product Purchase or Trial e-mail message that was sent to you or provided to you by your SpamLion Authorized Partner or Reseller.

5. Run the SpamLion Installer program

Navigate to the product installation folder referred to previously. Double-click the Installer.exe. The installer program does the following:

- Ask for and verify the drive letter of the volume where SpamLion will be installed,

- Check for available space on the volume (at least 8G recommended),
- Verify the existence of the license file (spamlion.lic),
- Create the SpamLion folder structure,
- Install and register the components.
- Create and configure the SpamLion Web site and the SMTP Virtual Server.

The Installer program will ask for the following information:

1. **Protected e-mail domain name**,
2. **Alias domain name** (Optional)
3. **SpamLion IP Address** in dot notation ex., xxx.xxx.xxx.xxx
4. **Fully Qualified Domain Name** of the protected mail server (mail.mycompany.com) or the Private IP Address of the mail server in square brackets [xxx.xxx.xxx.xxx] if you are behind a firewall.
5. **Protected mail server IP Address** ex., xxx.xxx.xxx.xxx

6. Start the SMTP and W3 services

Use a command window and type "net start smtpsvc" and "net start w3svc" or use the Administrative Tools Services application.

7. Set appropriate NTFS file permissions

Open a command prompt in the \SpamLion1\Utility folder. Run the updacls.bat file, type "updacls /set". For full syntax, type "updacls /?".

8. Complete the Initial Database Configuration

Open a web browser and connect to the SpamLion Administrative web site, (http://<yourserver>). The SpamLion Login screen appears. Click the SpamLion Administrator box and press the enter key. Enter "Administrator" into the Username field and "spamlion" into the Password field and then press Enter.

You will be positioned at the Initial Settings screen where you enter the following:

1. IP Address in decimal dot notation of the protected mail server ex. xxx.xxx.xxx.xxx,
2. Inside URL that resolves to your SpamLion Web site on your private network. This is used by SpamLion to generate One_Click_Logins for Quarantine Status Notification.
3. Outside URL that resolves to your SpamLion web site on the Internet. This is used by SpamLion to generate One_Click_Logins for Sender Validation e-mail messages.
4. Administrator e-mail address. This address must exist in your mail domain.

Once you press the save button, additional setting pages become available for you to use in subsequent sessions.

9. Set the Operating mode

Set the operating mode when SpamLion is not available to either Bypass or Queue. When the SpamLion1 service is not running, mail may be held on the SpamLion server waiting for the service to become available. This is known as "Queuing". Alternatively, mail may simply flow through the SpamLion computer. This is known as "Bypass".

10. Start SpamLion service

Start the SpamLion service using the command prompt "net start spamlion1" or the Services applet in the Administrative Tools. SpamLion service is set to start automatically every time your computer starts. If the NT service fails to start, check to see if the SpamLion1 service has been installed correctly by checking the \SpamLion1\Database folder. If you see a file called spamliontemp.mdb, then the SpamLion failed to install as a service. Use the Event Viewer to open the Application Log and look for the SpamLion log entries recorded there. Once you correct the problem, install the SpamLion service by using a Command Prompt. Navigate to the \SpamLion\Engine folder and type "spamlion1 –u 1" then "spamlion1 –i 1".

11. Finalize the appropriate SpamLion settings

Review the settings described in the Administrator manual that best server your company environment. Use the administrator web console to make appropriate changes. Help is available for each Administrator page. All SpamLion operational settings are located in the Settings Page. Sections under this page include:

- Main Settings
- Accounts
- Notices
- Processing.

The Notices page allows you to customize the SpamLion email challenge message sent to first-time senders and to set SpamLion to act as an "email firewall" rejecting mail to non-existent Receivers, or addresses on your domain.

The Processing section contains a setting band called **New Receivers Default Settings** that allows you to configure the default capabilities that your Receivers will have when their records are created. The next section discusses using Address List Synchronization to create the Receiver records. You need to review this setting band before proceeding to the next step because the values set will be used when the Receiver records are created in the SpamLion database.

12. Synchronize Receivers to Mail Server

In order to protect against Dictionary Harvest Attacks, synchronize your server address list with SpamLion and enable the "**Reject mail from non-existent receivers**" setting. Before creating Receiver records from your Exchange address list, determine if the majority of the Receivers will be "Protected" or "Bypassed". Set the appropriate default value for "**SpamLion Protection"** which is found in the Administrator console – Settings – Processing – New Receivers' Default Settings band before performing the initial synchronization.

Once you have determined the default settings then follow these steps:

1. Create a local security account for the GALSync, example: GALSync.
2. Set the NTFS permission, Modify, on the SpamLion1\Xfer\Sync folder to include the GALSync security account.
3. Create a share called "Sync$" on the SpamLion1\Xfer\Sync folder and set share permissions to "Full Control".
4. Copy the SpamLion1\GALSync\GALSyncEX2K folder to the \Exchsrvr folder on the Exchange Server. The Exchange Server by default is installed in Program Files. The utility batch files you will work with assume that Exchange binaries were installed in \Exchsrvr. Either create a new folder \Exchsrvr and copy the GALSyncEX2K folder there or modify the batch files to insert the 8.2 style "progra~1" identifier in all the file paths.
5. Modify the ADE.BAT file to the correct share, userid and password that you have created previously.
6. Initial Receivers update using the ADE.Bat file.
7. Run the initial export, type: "ade /extract user"

Check for successful completion: SLConverted.txt file created in Export subfolder, receivers visible in the Administrator console Receivers Page. Use the System tool Schedule task to run the user export on a regular basis.

Troubleshooting: Permissions appropriate to run LDAP query, create files, connect to network share and transfer file.

13. Export Active Directory Contacts as Receivers (Optional)

Some organizations define mail-enabled identities in their Active Directory. These identities do not have a mailbox on the Exchange Server; however, they have a mail identity on the mail domain. The purpose of these identities is to forward mail to another address. Inbound email sent to this type of identity is immediately forwarded to another email address. If you want to protect this type of entity you may either

enter the address manually in the Receivers page or use the ADE utility to transfer them from AD to SpamLion. The following steps rely on the share, permissions and user login id created in the previous step:

1. Modify the ADE.BAT file to use the correct share (Sync$), userid (GALSync) and password that you have created previously.
2. Type: "ade /export user contactasreceiver"

Check for successful completion: SLConverted.txt file created in Export subfolder, receivers visible in the Administrator console Receivers Page. Use the System tool Schedule task to run the user with contactasreceiver export on a regular basis.

Troubleshooting: Permissions appropriate to run LDAP query, create files, connect to network share and transfer file.

14. Export Active Directory Distribution Lists to create Senders (Optional)

Some organizations have the list of external contacts organized as distribution lists within their Active Directory. You can use the ADE utility to export the addresses and place them as valid senders in the SpamLion database. Follow the steps listed below:

1. Using the SpamLion Administrator console Receivers page insure that you have a protected receiver with Validation set to "Company". It may be the Administrator account, for example: administrator@mycompany.com.
2. Set the NTFS permission, Modify, on the SpamLion1\Xfer\Xfer folder to include the GALSync security account.
3. Create a share called "Xfer$" on the SpamLion1\Xfer\Xfer folder and set share permissions to "Full Control".
4. Modify the ADE.BAT file to use the correct share (Xfer$), userid (GALSync) and password that you have created previously.
5. Type: "ade /export contact administrator@mycompany.com".

Check for successful completion. The SpamLionContacts.txt file is created in the Export folder.

Troubleshooting: Permissions appropriate to run LDAP query, create files, connect to network share and transfer file.

15. Import Outlook and/or Outlook Express contacts as valid senders (Optional)

In the event that your contacts are not in Active Directory, you will need to import Outlook and/or Outlook Express contacts from the address book to SpamLion. Refer for detailed instruction in the KB200302-1 Contact Import.pdf. Note for the Senders to be created as valid the last entry in the file specifying the domain receiver as the "x-sender" must be in protected mode. Ask your SpamLion Authorized Partner or Reseller for it or contact SpamLion corporate at 707 585-1200 or send an email to support@spamlion.com requesting that the KB article be sent to you via email.

16. Enable Dictionary Harvest Attack defense

Log in to the Administrator console – Settings – Notices – Non-Deliverable Inbound Mail band. Enable (check) the "**Reject mail to non-existent Receivers**" feature.

17. Configure SpamLion Logging Settings

By default, SpamLion installs with Full logging enabled to allow you to troubleshoot any problems with mail flow. Once you are assured that SpamLion is processing mail correctly, use the Admin Console to change the Log Level to "Medium" or "Minimum". In high traffic environments, a "Maximum" setting will result in a performance hit and may even result in messages bypassing SpamLion processing.

18. Configure SMTP Mail Delivery Settings

In companies with a large number of protected mailboxes, and high traffic volumes, the outbound mail re-try queue may grow to a size that impacts performance. IN order to prevent this from happening, make the following adjustment to the settings found in IIS Manager, SMTP Virtual Server Delivery property. Open IIS Manager. Locate the SMTP virtual server and bring up the properties. Open the Delivery tab. Change the settings to correspond to the ones in Figure 6.

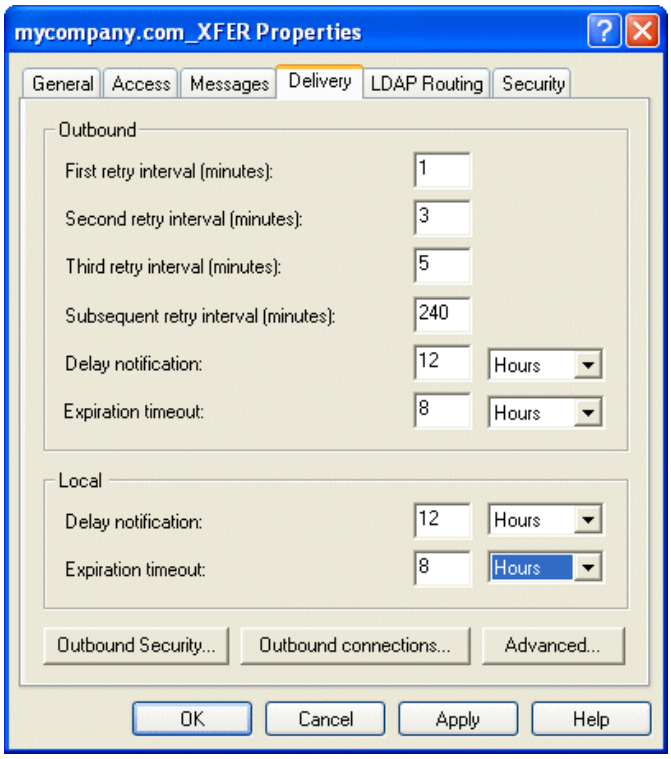

Figure 6. SMTP Delivery properties

19. Send outbound mail through SpamLion

Change the Smart Host entry on the Exchange Server to route outbound mail to SpamLion.

20. Allow inbound mail flow through SpamLion

At this point, you are ready to send email through the SpamLion computer by changing the firewall port rule to route mail on port 25 to the SpamLion computer.

21. Insure SpamLion is operational

Validate that SpamLion is operational by performing the following tests:

- Send e-mail from an un-protected post office to your SpamLion Administrator mailbox.
- Send e-mail to demo@spamlion.com. Respond to the validation request. Receive response.
- Access the website to request a login code. Login using the code in the e-mail sent to you.

22. Set up housekeeping tasks

Set up and configure the FileCleanup utility to automatically delete SpamLion log files and database backups to prevent you from running out of space. Alternatively, monitor the LogFiles and Database sub folders manually. Tip: Keep the most recent 5 days of files for referral use.

23. Rollout Anti-Spam Protection

There are a number of deployment options available from a pilot project to full-scale deployment. Make sure the users have sufficient training in the validation process operation of the Quarantine Manager. On-Line assistance is available by clicking the Help button on there web-page. A user guide template written in Microsoft Word is available in the SpamLion1\Documentation folder for you to customize.

In a passive rollout scenario, you want SpamLion to allow all inbound mail to continue to flow to your receivers in "bypass" mode while it is recording the email addresses of everyone to whom you're sending mail. SpamLion is said to be "learning" and this is its native operating mode with respect to outbound mail. With the receiver protection set to "bypass", all mail, spam included, continues to flow into the

protected domain mail server and mailboxes. From the user's perspective nothing has changed.

There is one caveat. The **Skip Outbound AutoValidate for Bypassed Receivers** setting is checked (enabled) by default. This means that SpamLion will not learn the sender addresses from the outbound mail messages of the receivers that are in bypass mode.

The setting was created to prevent people that are in bypass mode with an out of office auto response from validating all inbound mail addresses. While the vast majority of your receivers are in "bypass" mode, it is recommended that you uncheck this setting and accept the validated senders that are from spammers.

Once you have all mailboxes configured to the appropriate protection setting, you can change the setting back to its default. However, if you are performing a mass mailing from a bypassed mailbox, you may want to change the mailbox's AutoValidate setting to either validate the outbound sender addresses or not. You can also go back and "void" the senders that were validated as a result of the learning phase.

As the Administrator can take the time to train the users and rollout the capability to individuals in a measured way. You may also allow the user to make unrestricted changes to their settings or you may lock down the settings that are available to them in their Quarantine Management. Refer to the Administrator console – Settings – Processing – Receivers' User Interface Settings band.

24. Check for trial license expiration

Periodically check the SpamLion Administrator's mailbox for an initialization message that shows the number of days remaining in the current license. Purchasing a SpamLion will insure uninterrupted spam protection. Upon payment, you will receive a permanent, non-expiring license. Simply stop the SpamLion service. Replace the existing trial license found in C:\SpamLion1\Engine with the permanent license. Start the SpamLion service. Make sure that you save this new license in a secure place as part of your backup procedure.

25. Relax

Your spam problems are over!