VisNetic MailServer

# AntiSpam Tools Overview

# Introduction

**VisNetic MailServer** is a full-featured mail server software package that includes a comprehensive set of security and anti-spam technologies. In order to effectively fight spam, several features and technologies are necessary as spam techniques are vast, no one feature or technology is effective on its own. Some of the features are configured in the AntiSpam section of the VisNetic MailServer configuration utility, and others are configured in various other areas of the mail server configuration screens. Configuring VisNetic MailServer to effectively fight spam for your organization is very much an individual effort, as **no two organizations are exactly the same** when it comes to determining what is spam, and what is legitimate email, however there are many similarities. There are also certain types of spam that are considered spam to almost everyone (except, maybe spammers), and VisNetic MailServer has the ability to detect and perform actions on these types of messages rather easily.

# Technologies

At the heart of VisNetic MailServer's ability to fight spam are two popular technologies: **Bayesian Filtering** and **SpamAssassin**. These options are readily available in the AntiSpam section of the configuration utility and are enabled by default. Usually no manual configuration is required outside reviewing and becoming familiar with the options in AntiSpam. Such as, Scoring, Spam Folders, Greylisting, Challenge Response, Message Content, and Logging.

Some of the other options available in VisNetic MailServer are **DNSBL**, **Intrusion Prevention**, **rDNS**, **Relay Checking**, **IP Blocking**, **Content Filters**, and **Black & White Lists**. These options are very much a part of fighting spam but not located in the AntiSpam options, mainly because these options can also be used for mail routing, filtering, accepting or rejecting mail they deserve their own configuration section outside of the AntiSpam section which is used to primarily control the behavior of Bayesian and SpamAssassin technologies.

We will first discuss options available in the AntiSpam section and then focus on the other options.

# Techniques

## Setting up scoring for messages

In this section we will cover verifying that messages are getting scored as spam and learn how to identify how the message reached its final score.

To enable message scoring follow these steps:

1) Open the VisNetic MailServer Administration *(Start / Programs / Deerfield.com / VisNetic MailServer / VMS Configuration)*
2) Click on **AntiSpam** on the left hand side
3) Click on the **SpamAssassin** Tab
4) Verify that SpamAssassin is **Active**
5) Verify that **Enable SpamAssassin Reporting Functions** is selected
6) Verify that ***"Report is added to headers and or subject of original message"*** is selected at the bottom.
7) Select the **Other** tab and **enable Debug and Summary logging**.

Enabling Debug and Summary logging will ensure that while you are learning how the AntiSpam system works you can make required changes based on accurate logging information. All logs are saved to the \logs\ sub-folder of your installation path for VisNetic MailServer. Logs can be viewed with any text editor, such as Notepad.

## Verifying scoring is enabled

*Now that the ability to score messages is enabled, we will now verify that messages are getting scored correctly*

Verifying the steps above will ensure that the following **X-SPAM headers** are added to each message:

**X-Spam-Status:**

**X-Spam-Level:**

**X-Spam-Checker-Version:**

The **X-Spam-Status header** will show if the message was identified as spam and what the message scored and what spam tests the message went through to reach its final score.

The **X-Spam-Level header** will be filled with asterisks per each point that the message scores. If the message scored a 3.5 then there would be 3 asterisks in this header.

The **X-Spam-Checker-Version** is where VisNetic MailServer identifies which version of AntiSpam software is being used as well as the domain name of the AntiSpam system.

To **view** the X-Spam headers in your email client you would typically show all headers or view the Properties of the message. In VisNetic WebMail you select the 'Full headers' icon after selecting a message.

Now that the X-Spam Headers are added to the messages we can start to see what messages are scoring in relation to the score that is configured to mark a message as spam. This can be configured under the Action tab of the AntiSpam section of VisNetic MailServer.

By default VisNetic MailServer is going to classify a message as spam at a score of 5.00. The lower the score to classify a message as spam, the more spam will get caught as well as the more valid messages could be marked as spam.

## Scoring Options

The best practice in getting SpamAssassin to classify more spam messages correctly as spam is to collect 20 or more messages that were not marked as spam, and get an **average score** from the messages via the headers of the message. Then lower the score required to classify a message as spam accordingly. However, lowering the Score Required to Classify a Message as spam could cause valid messages to be marked as spam. Generally lowering this score to anything lower than 2.00 is not suggested.

**Note:** If spam messages are scoring low one possible cause for this are the **Bayesian Filters**. These filters, if corrupt in anyway, could throw off the score of a spam message

dramatically. Bayesian Filters add or subtract from the overall SpamAssassin score that a message reaches.

## Spam Actions

Once message are marked as spam there are a number of actions you can take to **filter the messages** away from the inbox. From within the AntiSpam Action Tab you can configure the spam messages to be placed in the **Spam Folder**. This Spam Folder is accessible via WebMail or any mail client as long as the Account in the mail client is configured as an **IMAP** account.

Another option is to have the AntiSpam engine **add a prefix** to the subject of the message. This allows an Email Client to be able to filter on this subject and place it in whichever folder the end user wants the spam messages to go to. This can also be used via the **Content Filter**. This would allow the Admin to filter on the subject and perform any actions via the Content Filter directly at the MailServer level.

VisNetic MailServer has two actions that can be enabled and will act based upon the spam score. Under the Action Tab of the AntiSpam Settings, you can **Quarantine** messages if they reach higher than a specific score. This will take the spam message and instead of giving it to the original recipient the message will go to the account that is specified in the “Quarantine Email Address” field. Multiple accounts can be specified by separating the addresses via a semicolon.

The second option that VisNetic MailServer can be configured to do from within the AntiSpam settings is to **Delete Message** if the message reaches higher then a specified score. This option will do just as it’s named. If a message reaches over a specific score the message will be deleted directly at the mail server during the session itself. This option should only be enabled and set to a high enough score that the messages are guaranteed to be spam as the message is deleted. If this score is too low then valid messages might be deleted (depending on their score).

# Additional Spam Options

## Greylisting

There are other ways that the AntiSpam can fight spam besides the SpamAssassin scoring. **Greylisting** allows the mail server to silently reject all SMTP connections made to VisNetic MailServer. This will force the sending mail server to retry the message. This is useful because most spammers will not retry messages that come back to them - thus stopping those spam messages from being delivered. One potential downside of Greylisting is that there is a slight delay in receiving mail (the time it takes for the sending server to retry the message).

Greylisting can be enabled by selecting the Greylisting tab under the AntiSpam section of VisNetic MailServer. Simply check the box Active. Additional configurations for Greylisting are detailed in the VisNetic MailServer Help Files.

## Challenge Response

Challenge Response is a very effective way to stop a good portion of spam from coming in. When initially using Challenge Response, the recommended approach is to Enable Challenge Response but **do not** Challenge anything. What this allows is for the mail server to build up a **white list** of entries that in the future will not be challenged. After a small period of time (a month or so) this white list should contain a list of friendly senders. Then, enabling Challenge Response to challenge messages marked as spam and to challenge messages not marked as spam is the suggested setting. This way spam messages that score too low to be considered spam would still be challenged.

Challenge Response can be enabled and configured by selecting the Challenge Response tab under the AntiSpam section of VisNetic MailServer. Additional Configuration for Challenge Response can be found in the VisNetic MailServer Help Files.

## DNSBL

DNSBL is a very important part of helping fight spam, it uses **real-time IP blocking services** that provides VisNetic MailServer with an **accept or reject** reply based on known spamming IP addresses. There are hundreds of free services that provide an accurate database of known spam IP's, such as, **sbl-xbl.spamhaus.org** and **bl.spamcop.net**. You can also use DNSBL's to reject known open relays, one such service is **relays.ordb.org**. This service provides a real-time list of open relays that are typically used by spammers. The DNSBL option can use several different DNSBL hosts but we don't recommend using more than three as doing so could put a heavy demand on your DNS servers. DNSBL rejects messages during the SMTP session making it extremely efficient and effective.

## Relay Checking

Relay checking ensures that connecting clients or servers (**based on IP address**) are trusted or authenticated before they are allowed to send to remote domains. This security option is vital to the security of your mail server. At no point should your mail server allow unauthorized relaying, doing so would allow spammers to send spam messages to other servers without being trusted or authenticated. By default VisNetic MailServer is configured as a **closed relay**.

## Content Filtering

Content Filtering is a very flexible filtering system that provides the admin with a **condition / action** filtering response. You can use content filtering to take certain action on message senders, recipients, whether marked as spam, etc… or you can create custom logs based on any available condition. VisNetic MailServer provides numerous **system variables** that can be used in content filtering. For example, if you create a content filter designed to write to a text file or create a special X-header in each message, you can use

variables to populate your file or header. For example, %%date%%, %%recipient%%, %%IP%%.

A complete list of System Variables is available in the **variables.dat** file in the …\VisNetic MailServer\examples directory.

## Black and White list

An important part of spam protection is based on effective use of **Black & White Lists**. A sender whose address is white listed will always have their email delivered to the recipients, while black listed users are denied. Unfortunately it is not always possible to use black lists for spam protection as most spammers are **not using their true identity** in the email headers, but the identity of another or one made up entirely.

Given this, the most important item pertaining to White and Black lists is proper white listing. Being able to configure your mail server so that it only accepts messages from approved senders.

Black & White lists are included in each VisNetic MailServer, regardless of version. They are:

- Global – for the entire server
- Domain – for the domain
- Individual – for each user

## Logging

When troubleshooting, or simply trying to learn how the system works, it's important to familiarize yourself with the logs. Debug and Summary logging provides the most logging information but will require more disk space. Debug logging is required if you want to view sessions using the VisNetic Admin. The logs are saved in the \logs\ sub-folder of the VisNetic MailServer installation path. The logs start with a letter representing the associated service, for example,

SMTP = sYYMMDD.log
POP3 = pYYMMDD.log

IMAP = mYYMMDD.log
AntiSpam = \logs\antispam\YYMMDD.log

The logs can be viewed with any text editor, such as, Notepad. Since VisNetic MailServer is a multi-thread server it does not log sessions by session ID but by order received. On a busy server this can make viewing the logs a very difficult task. Using the **Log Analyzer** will help make this task much easier.

**Real-time session reporting** is available from the VisNetic Admin and can help troubleshoot spam problems. When viewing **SMTP Session History** double click the session to view the associated log. The success or failure of the session will be reported in the log, as well as the message ID, if the message is accepted. The **message ID**, in bold below,

>>> 250 2.6.0 5759 bytes received in 00:00:05; Message id **ICU78140** accepted for delivery

can be used to track a message reported in the Antispam logs, example,

IP [03B0] 11:16:46 **ICU78140** '<user@spammer>' '<user@your_domain.com >' score 10.00 reason [SpamAssassin=10.00,Bayes=100.00,Body=12] action SPAM

This message ID makes it traceable to the SMTP log so you can determine IP, sender and recipient information.

## Intrusion Prevention

Intrusion Prevention provides a way to **automatically block** IP addresses that meet certain criteria that spammers would typically use, such as, **harvesting email addresses**, establish X number of connections in a minute, or block after X unknown users, or even if the message exceeds a certain message size. Once an IP is on the block list the next time it connects it will immediately be blocked.

# Conclusion

Whatever antispam solution is employed, a layered approach is recommended. When spammers adjust to overcome popular antispam solutions, additional antispam technologies must be employed to thwart their advances. Following the guidelines in this document, VisNetic MailServer can reduce your current spam load to an acceptable level, and keep you prepared for the evolution of spam.