VisNetic MailServer

AntiSpam QuickStart Guide

Version 9.1

Contents

CHAPTER 1

VisNetic MailServer Antispam Quick Start

In This Chapter

Introduction

Well, you installed VisNetic MailServer, you defined your Domains, added your User Accounts and it's sat there delivering mail as required.

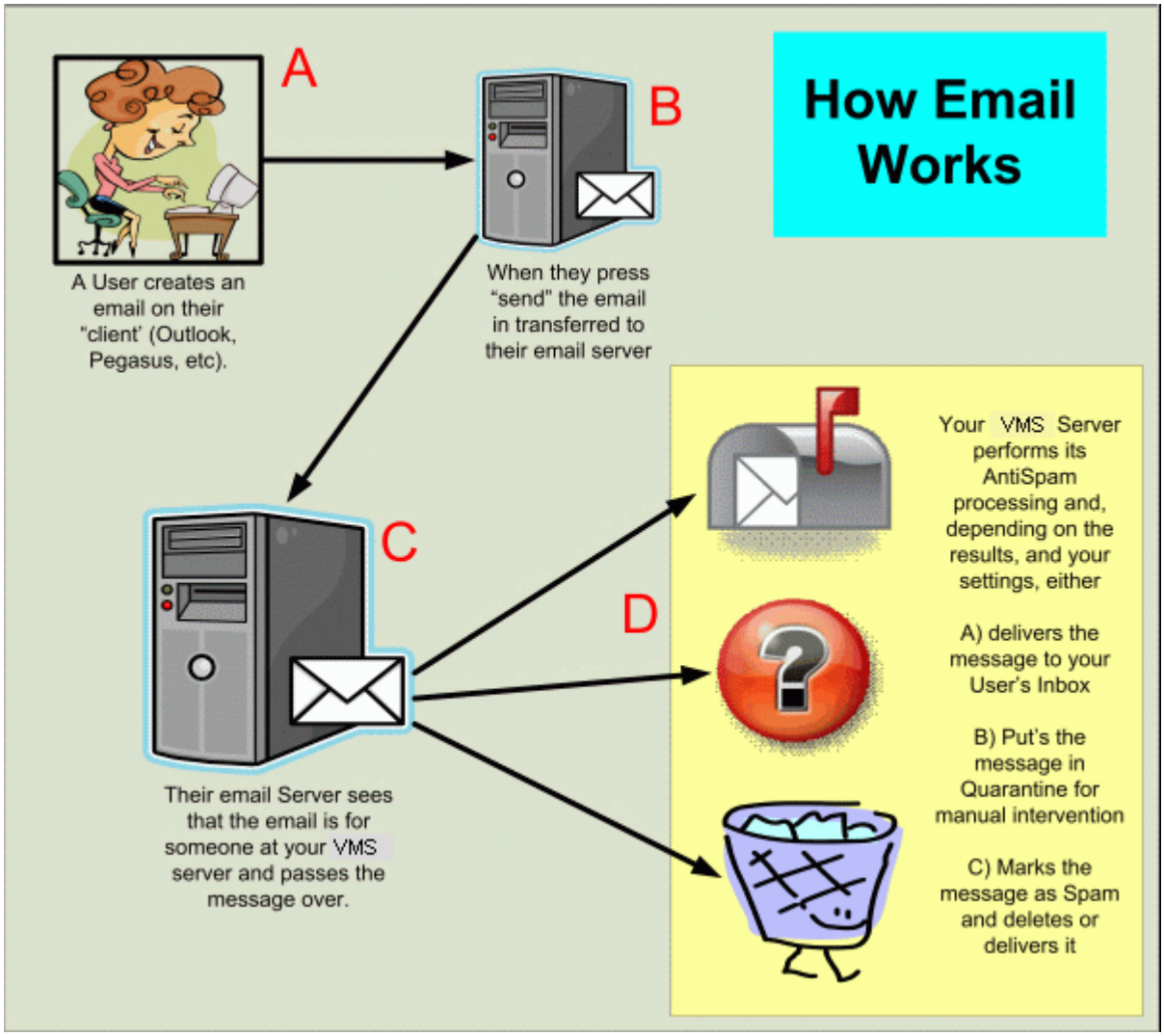
But – your Users are getting Spam! They don't want Spam. You are using VisNetic MailServer because it has the best AntiSpam technology in the world.

What are you doing wrong?

Don't Panic – this Guide will talk you through the AntiSpam options of VisNetic MailServer and how to set them up so your Users are as protected as they can be.

The Email Process, simply put

The first thing is to look at a very simplified description of how the Email Process works.



Hopefully, the picture is self-explanatory. The User uses her Client software to create a message. When she tells the client to send the message, it passes it to the Server (like a Post Office), which works out which other server to pass the message to (the recipients "Post Office"), and does so. The recipients server then holds the message until the recipient logs in with their client to collect their messages.

The main points to remember are:

- VisNetic MailServer is contacted by other Email Servers with messages destined for your Users.

- VisNetic MailServer can make a guess (more later!) as to whether the message is Spam or not.
- VisNetic MailServer can take different delivery actions based on whether it thinks the message is Spam.

So let's move on to the Processing within VisNetic MailServer.

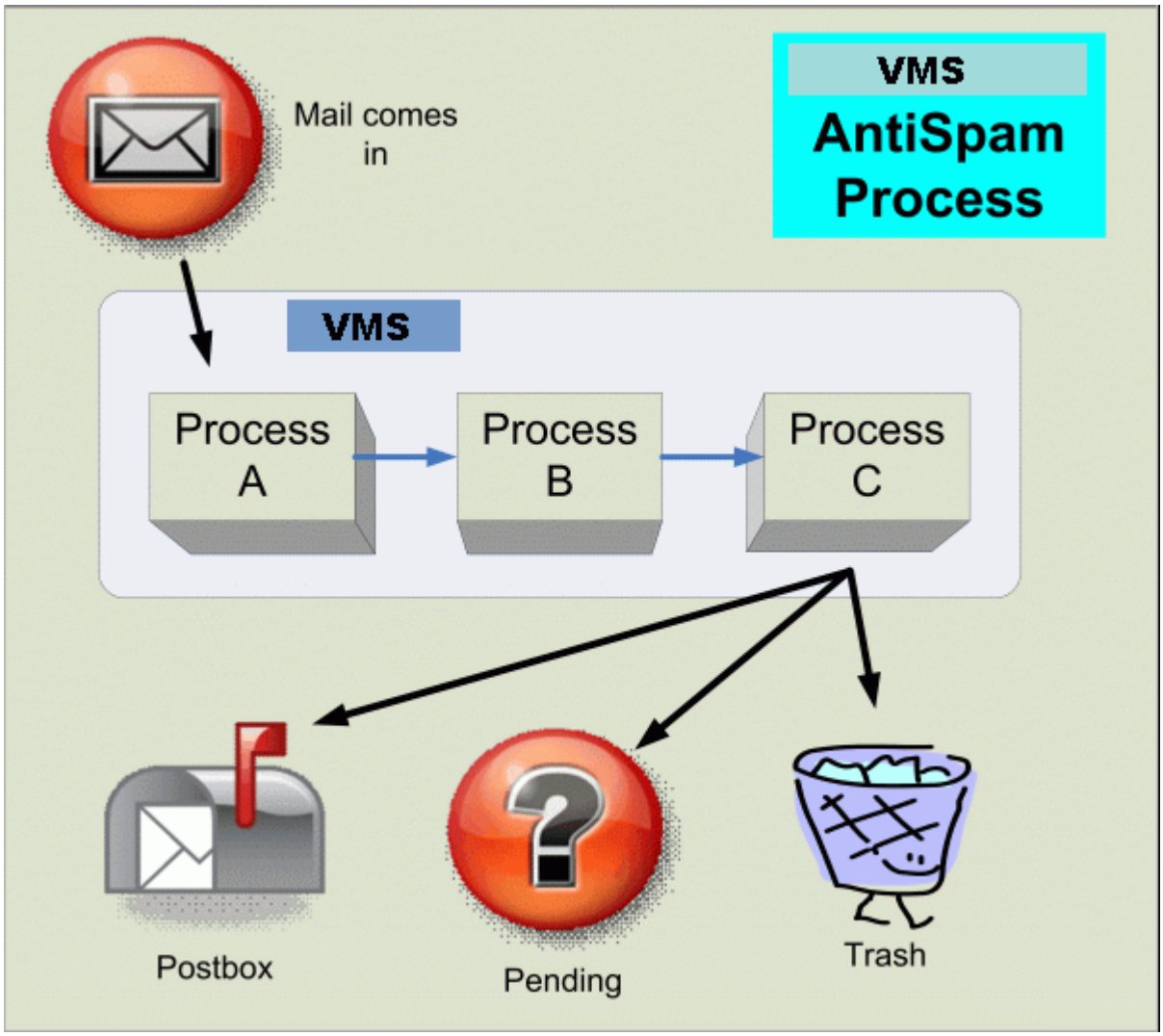
VisNetic MailServer as a Process Model

We are going to keep this manual really easy.

By the time you have read all of it you will have a basic understanding of how VisNetic MailServer deals with Spam.

You will know where to find the AntiSpam settings within VisNetic MailServer, have an idea of what each setting does, and know how changing or tweaking that setting will affect the messages coming in for your Users.

Lets have another simple diagram, Just for VisNetic MailServer itself - don't be put off, this book is structured to teach!



Well - I said it was going to be simple!

When a message is destined for one of your Users the sending mail server will contact your VisNetic MailServer installation to attempt to deliver that message. VisNetic MailServer processes the incoming message via the three Processes A, B, and C.

By the time VisNetic MailServer has finished it's processing one of the following will have occurred:

- The message will have been delivered to your User.
- The message will be held in a "Quarantine" system (Don't worry, we'll explain later).
- The message will not have been accepted for delivery.

That's it! No other options. Nothing magical or mysterious. We have a result!

So let's look at those processes.

Process C - Message delivery (or not!)

Yes, I know we are going backwards here but there is method in our madness. By explaining what happens to a message at the end and why it happens, you will be better prepared to understand why VisNetic MailServer is doing all it's processing in boxes A and B, so read on -

By the time a message gets to Process C VisNetic MailServer will have made some decisions - it will know some, or all, of the following

- Who the message is from.
- Who the message is for.
- Who the message says it's from.
- Where the message is from (the sending server).
- Whether the message is coming from a source that is allowed to send messages from the sender.
- Whether the message comes from a source known for Spam.
- Whether the message contains links to sites known for Spam.
- Whether the message contains words that are normally associated with Spam
- Whether the message contains words that are normally associated with your (or your User's) business.
- And much more

All this information will have been used by VisNetic MailServer to assign a Spam Score to the message, which is worth talking about right now, as it is the key to the whole AntiSpam process within VisNetic MailServer.

SPAM SCORES - The Spam Score of a message is a value assigned by VisNetic MailServer that indicates **how likely** it is that the message is Spam.

The Spam Score takes a value from 0.00 to 10.00, with 0.00 meaning the message is highly unlikely to be Spam, and 10.00 meaning the message is highly likely to be Spam.

Keep in mind at all times that VisNetic MailServer can never be **certain** that a message is Spam!

For example, one of the biggest subjects for Spam messages in this day and age is cheap medication, so you could say that messages containing the words Viagra or Cialis are certain to be spam, but this just isn't true for a pharmaceutical company that produces Viagra and/or Cialis!

So VisNetic MailServer cannot be perfect, no AntiSpam system can be perfect, they can just get very close to perfection (which, of course, VisNetic MailServer does!)

So we get to Process C with a Spam Score assigned to our message, and it it this Spam Score that governs what happens to that message -

- The message is delivered.
- The message is "Quarantined".
- The message is refused or rejected.

Let's talk about these -

The message is delivered.

Seems simple, the message is delivered to your user, but there are additional actions that can be taken

- The message can be "marked" as possible spam (usually by adding some specific text to the subject of the message).
- If the message is "marked" it can be delivered to a specific Spam "queue" or "folder" (so your Users can deal with it as a secondary priority).

The message is "Quarantined".

You can set VisNetic MailServer to Quarantine a message when the Spam Score is within a certain range - So it's time for quick talk about Quarantine -

QUARANTINE

A Quarantined message is "parked" by VisNetic MailServer until human action is taken to tell VisNetic MailServer what to do with the message (or it is released as Spam by the system).

Quarantined messages can be "un-parked" by:

The Sender responding correctly to a "Challenge Response" message (more later!), proving he/she is human.

The recipient of the message actions it via Webmail or the automatic Quarantine Report VisNetic MailServer can generate.

A Spam Administrator actions the message.

That's all you need to know for now - keep it in the back of your head!

The message is refused or rejected.

As it says, the message does not get to your user - its Spam Score is so high that you have decided it is definitely Spam.

NOTE - that this is considered a dangerous option - remember, VisNetic MailServer cannot be **certain** that a message is Spam, so rejecting messages could lead to your users losing legitimate messages.

So there it is - Process C explained!

You now know what can happen to a message that comes into your VisNetic MailServer Installation

Process B - Is it Spam or not?

Well - it's time to open Process B.

This is where all the "heavy" processing happens. VisNetic MailServer uses many technologies in its fight against Spam. Each of these technologies has its good points and bad points, and only you, as the System Administrator, will know (eventually) whether each technology is right for you.

The fight against Spam is an on-going one. As pointed out in this manual already, there are no 100% effective AntiSpam solutions!

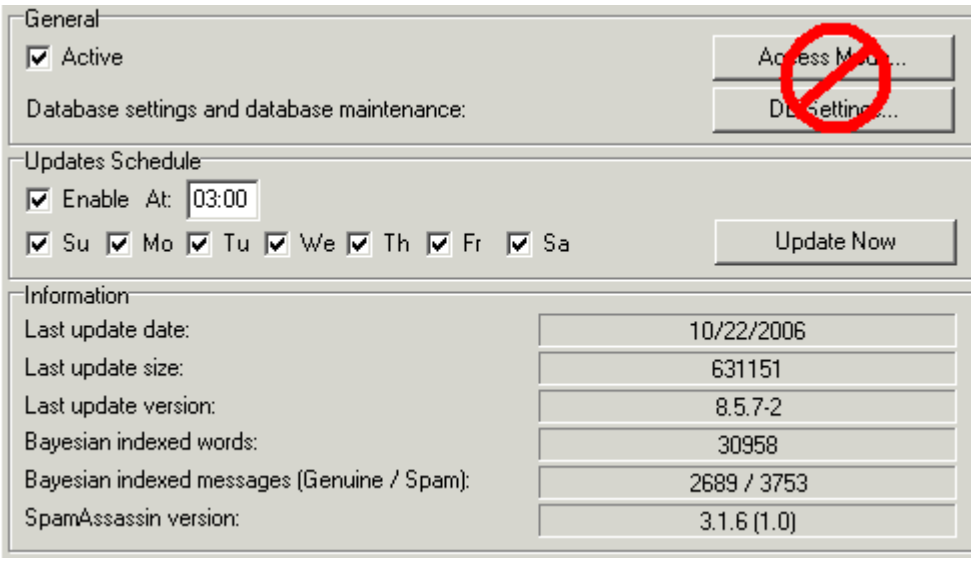
Spammers are clever - they learn the technologies being used to fight Spam and find ways around them. The fight is continuous and changing. As new Spamming techniques are introduced, so are new ways to fight them. VisNetic MailServer is constantly being updated to integrate new AntiSpam technologies, so you can be sure you have the right tools at your disposal. But only you can tell if those tools are working!

As the System Administrator, it is your job to tune and tweak VisNetic MailServer so that is does the best job it possibly can. You need to check what Spam messages are getting through to your Users and what Genuine messages are being marked as Spam - and find out why - and fix it!

Anyway, enough of all that. Let's go through VisNetic MailServer's AntiSpam arsenal and see what you can do, why you would want to do it, and why you might **not** want to do it (You'll see!).

General Settings

The General settings area allows you to activate or deactivate AntiSpam and set an update Schedule



Let's do it -

- Check that Active Box

Ignore the Access Mode and DB Settings buttons for now - we can learn about those when we need to.

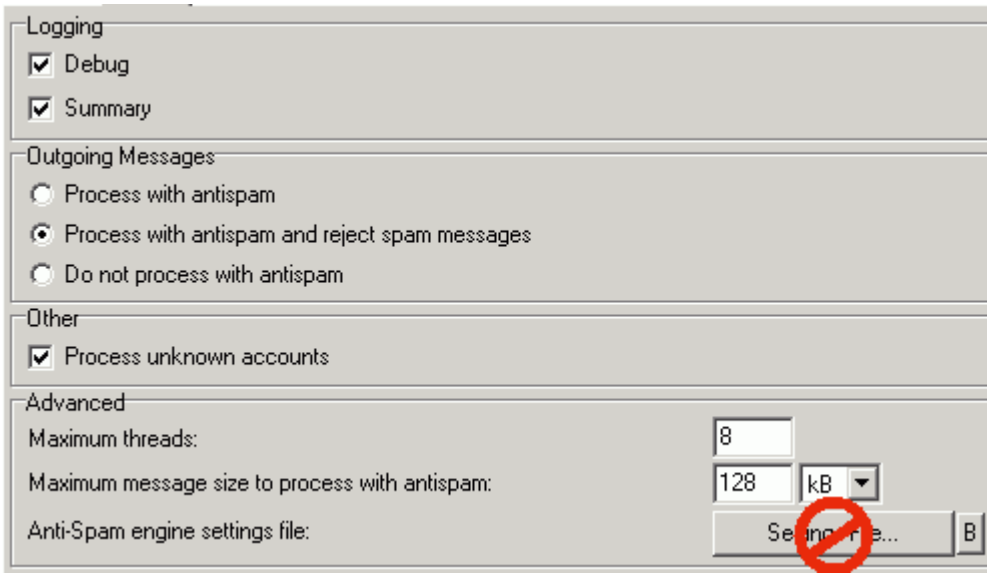
- Set an update schedule to make sure your AntiSpam is always up to date
- Check the Enable box
- Enter a time for your update to happen
- Check the box for each day you want the update to happen

And we'll ignore the Information box - it's just information!

Congratulations - you just started protecting your users.

Other Settings

Here we are going to set settings related to the System, Outgoing messages and "Unknown Accounts".



Logging

- Check both boxes

Initially, while you are tuning your AntiSpam Settings, you are very likely to have messages that are incorrectly classified. Having full logging options allows you to investigate the reasons behind the incorrect classification and tweak your settings accordingly.

Outgoing Messages

We are sorry, but this one is up to you

- Do you trust your Users?
- Do you want your server using resources to check outgoing messages?
- Are you a corporate installation or an ISP?

If you trust your users not to send Spam then you do not need this checking.

If you don't care what the rest of the world thinks about your server's reputation regarding Spam then you don't need this checking.

If you are providing Email services for the masses (maybe as an ISP) and you care about your server's reputation then you want to check outgoing messages, and probably reject outgoing Spam.

Only you know your user-base!

Other

Check the box to process unknown accounts - This is for messages destined for an email address that does not exist on your server, but may be delivered to an account via some filter or rule.

Advanced

Leave these at the standard installation defaults -

Maximum threads 8

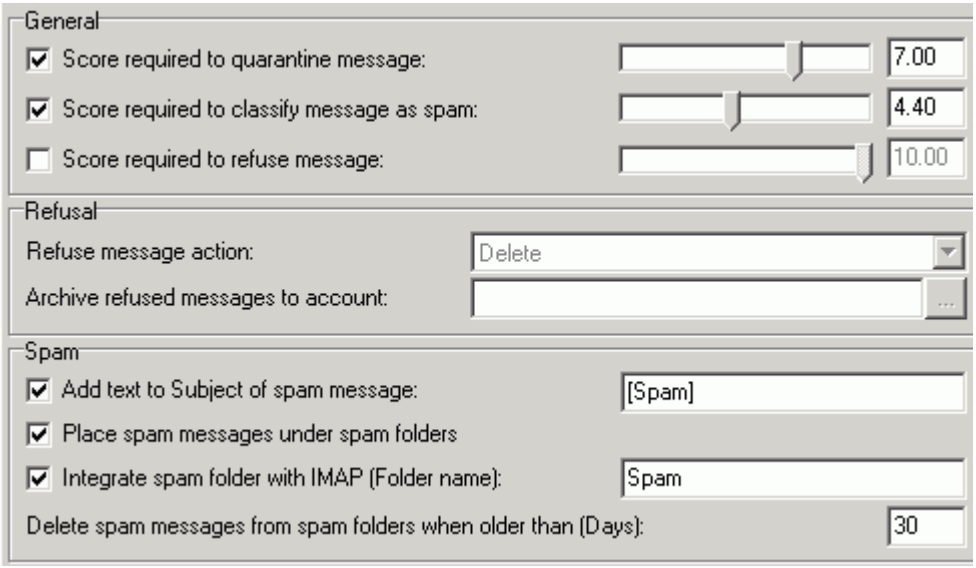
Maximum message size to process 128 kB

And don't even think about touching the **Settings File** button - we're about three manuals away from that :)

Action Settings

Remember Process C? If you don't, go back to and read the chapter again, (see "Process C - Message delivery (or not!)" on page 7)

This is where you set what happens to a message after all the heavy work is done and a Spam Score is assigned to the message.



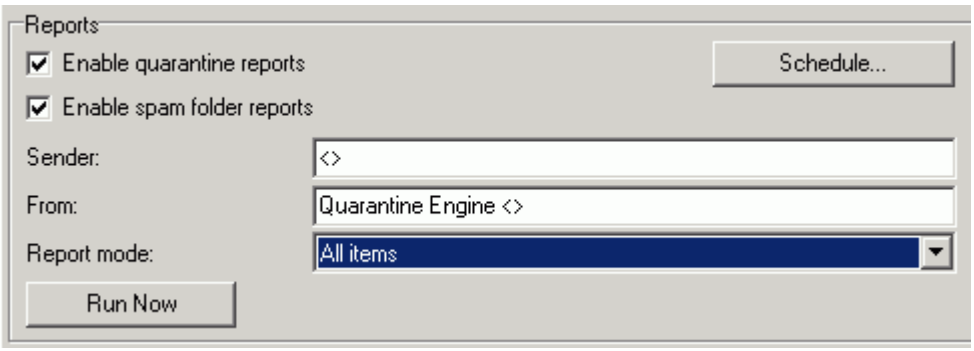
So let's tell VisNetic MailServer how to treat messages - these are our recommendations for an initial setup:

- Check the box to Quarantine Messages - let's have your Users helping you.
- Slide the slider or enter a value in the box - we recommend 7.00 initially.
- Check the box to classify messages as spam - this is, after all, why he are doing all this.
- Slide the slider or enter a value in the box - we recommend 4.40 initially.
- Uncheck the refuse message box - remember, VisNetic MailServer can't be certain a message is Spam! Don't activate this until you are confident you are not losing genuine messages.
- "Refuse message action" and "Archive refused messages..." are greyed out because we didn't check the Refuse message box, so ignore them.
- Check the Add text to Subject button - it's a good idea, your users can see that VisNetic MailServer thinks that this message is spam, and take action if it isn't spam. It also means that Spam messages that get through are identifiable by the fact they don't have this text.
- Enter the text you want to add to the subject of the message - make it something meaningful so your Users understand it!
- Check the box to have Spam messages stored in the User's Spam Folder (if you defined one when you set up the User Account!).
- Check the box to integrate the Spam Folder with an IMAP folder.
- Enter a value to have Spam messages deleted by the system after the specified number of days - we recommend 30 initially

NOTE - having the system delete spam is great, but you must be sure to give you Users enough time to maintain their Spam before deleting it. Having a value of 7 days here could mean that a User that goes on a two week vacation loses an important genuine message that was incorrectly marked as Spam

Reports

The Reports tab allows you to have VisNetic MailServer send Automated reports to your Users listing Quarantined and Spam messages that they should action. This is a great way of getting your Users to help setting up your system for you. They can decide whether Quarantined items are accepted or not.

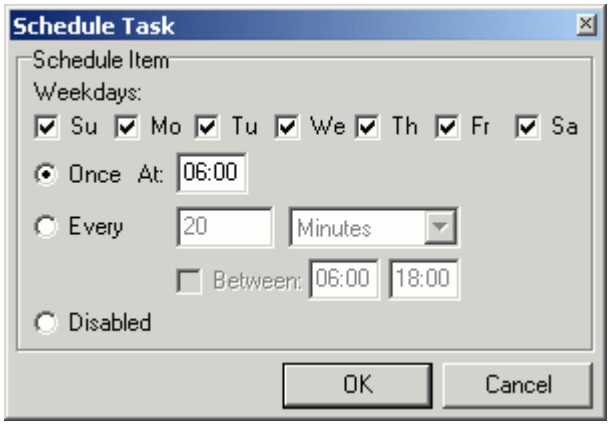


So let's set this up:

- Check the box to Send email reports to quarantine users - this will send an email to all users who have messages in quarantine listing the messages with clickable actions. This allows you users to administer their own quarantine queue.
- Press the Schedule button to define a Schedule for quarantine reports to be sent - a dialog will open:

  Click Add.

  Check each day and select a time for the report to be generated.



  Click OK.

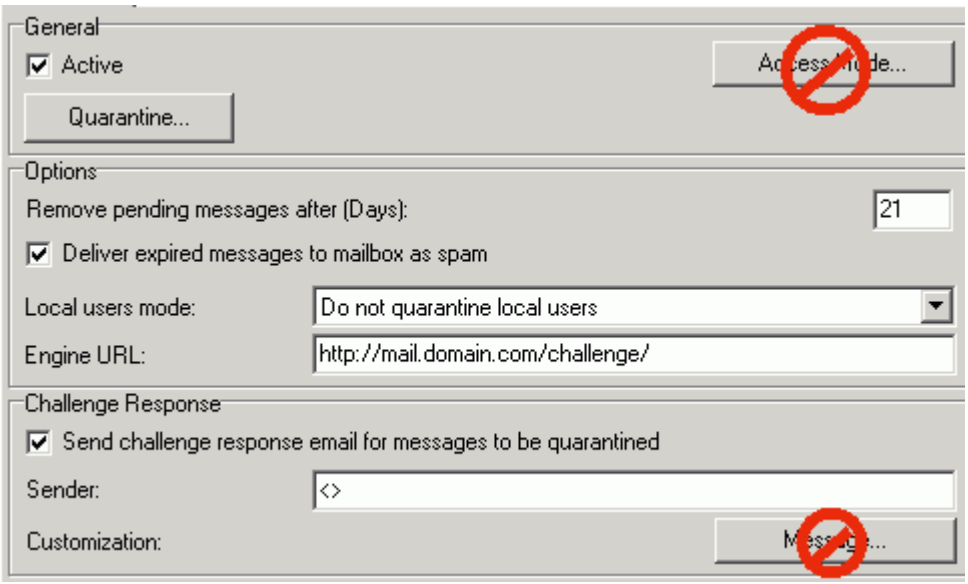
  Click OK.

- Leave the Sender field as it is.
- Leave the From field as it is (Although there is no harm in changing it, but make it something meaningful!).
- Select All Items from the Report mode drop-down - the New items mode only lists messages quarantined since the last report was run, this can be confusing to your Users at first.
- Press the Run now button if you want to run the report right now (not necessary if you are just setting up).
- Check the box to send Challenge response emails - this will send an email to the sender of a quarantined message asking him to confirm he is human by visiting a web page and entering some information. This takes some effort away from your Users and Administrators.
- Leave the Sender field as it is.
- Ignore the Message button (you can customize the message sent but for now we needn't bother).

Quarantine

Remember Quarantine? If not, refresh your memory by looking at "Process C - Message delivery (or not!)" on page 7.

This is where we tell VisNetic MailServer how to handle messages that are to be quarantined. Remember, quarantined messages are held in a quarantine queue awaiting manual intervention by the intended recipient, an administrator, or the original sender.



So here goes -

- Check the Active box to use the quarantine function.

- Ignore the Access Mode button for now - its default setting is All Accounts, meaning all our accounts will have quarantine options enabled.
- Ignore the Quarantine button - it will take you to the Quarantine Queue view.
- Enter a value in the box next to Remove pending messages after (Days). If a message goes into Quarantine and is not manually actioned within this time it will be moved on - Recommended setting 21.
- Check the box to have removed messages delivered as Spam - so after the 21 days in Quarantine the message will be marked as Spam and delivered to the User. If you do not check this option the message is permanently deleted and you run the risk of losing legitimate messages.
- Select "Do not quarantine local users" from the Local users mode drop-down - this means that messages sent from one of your Users to another of your Users will not be Quarantined.
- Modify the Engine URL to point to your domain - so if your domain is MyDomain.com, modify this field to http://www.MyDomain.com/challenge - this is used for the challenge Response system (see below)
- Check the box to send Challenge response emails - this will send an email to the sender of a quarantined message asking him to confirm he is human by visiting a web page and entering some information. This takes some effort away from your Users and Administrators.
- Leave the Sender field as it is.
- Ignore the Message button (you can customize the message sent but for now we needn't bother).

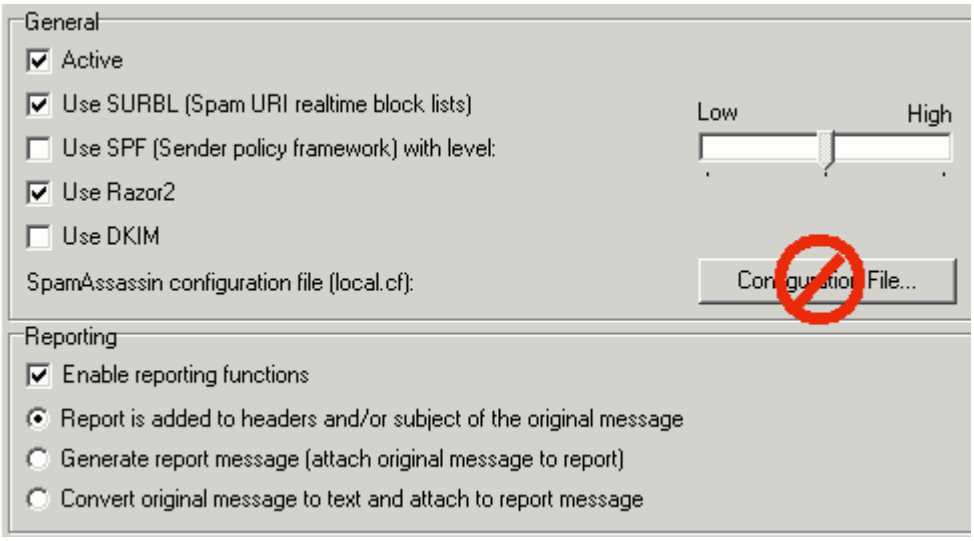
And that's it, Quarantine is all set up and working for you.

SpamAssassin

SpamAssassin is a third-party AntiSpam technology that is incorporated within VisNetic MailServer.

SpamAssassin itself incorporates a number of differently named technologies, each of which can be used in your fight against Spam.

If you want full information about SpamAssassin then you should visit ***SpamAssassin*** http://spamassassin.apache.org.



Let's get on with your initial settings -

- Check the Active box - this switches on SpamAssassin processing. If this box is unchecked, all the other boxes will be grayed out and unusable.
- Check the box to Use SURBL.
- Do not check the box to use SPF.
- Check the box to Use Razor2.
- Do not check the box to Use DKIM.
- Check the Enable reporting functions box.
- Select the Report is added to headers option.

EXPLANATION

SURBL checks the links found within a message to see if they are known to be Spammer target sites.

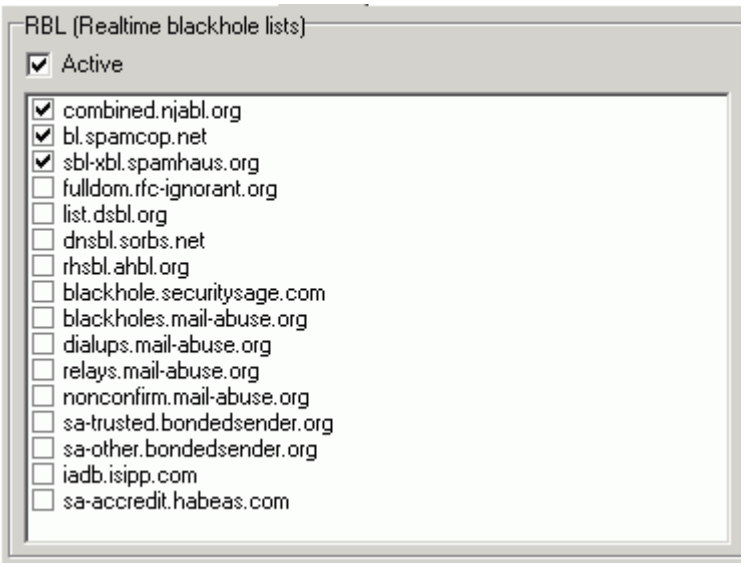
SPF is not widely used as yet and can lead to many genuine messages being classified as Spam.

Razor2 (Vipul's Razor Version 2) is a new technology that checks a random part of the message against a database of known spam. It is difficult for Spammers to beat because of the random aspect of the check.

DKIM is not widely in use as yet and can lead to many genuine messages being classified as Spam.

RBL

RBL is a system whereby VisNetic MailServer can check whether a message has been sent from a known source of Spam.



You would probably have this option switched on in the Mail Service - Security Node, in which case you don't need to switch it on here as well (why check twice?).

If you don't have this enabled in the Security Node then you should enable it here:

- Check the Active box
- Check the boxes for combined.jabl.org, bl.spamcop.net and sbl-xbl.spamhaus.org (recommended settings).

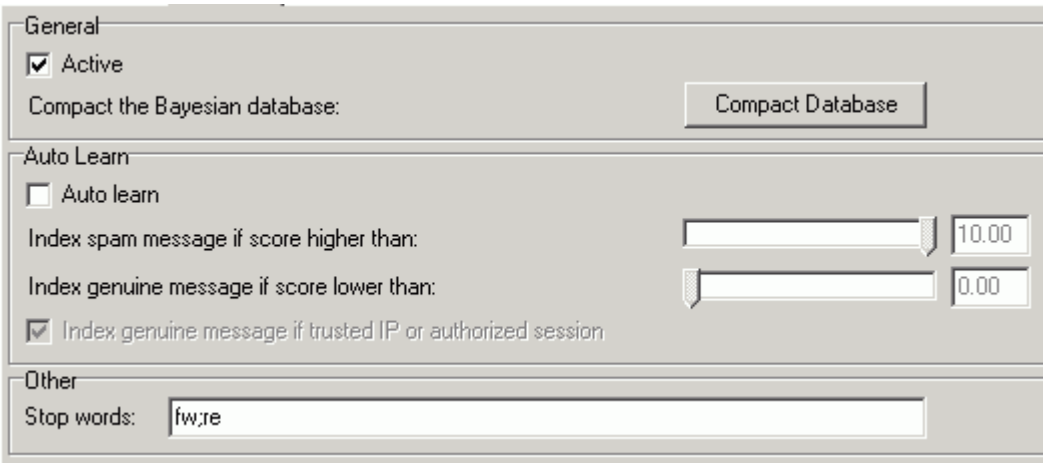
Bayesian Filters

Bayesian filters are based on a statistical method that says "the probability that something will happen in the future is the same as the frequency that it happened in the past".

When applied to Spam, it collects the frequency of spam messages and genuine messages, and the frequency of the words occurring in those messages. When a new message comes in, it checks the words in the new message against the statistics in the database, and makes an "informed guess" as to whether the new message is Spam.

Well, that was a mouthful! It is difficult to explain in less than a whole book, so suffice it to say that it works well enough to help VisNetic MailServer in its decision making.

Let's do it



Check the Active box - let's switch it on

Uncheck the Auto Learn box - we don't want to do that yet!

That's it - done!

EXPLANATION

VisNetic MailServer comes with a Bayesian database built in. This database has been built by analysing millions of emails over the last few years and is a good starting point.

The Auto Learn feature for the Bayesian database is designed to add a server specific database to the system that will understand the messages passing through that server, and will grow more and more accurate as time goes on. At the start of your server's life, however, you will probably be getting many messages incorrectly classified, and these messages will do more damage than good to your Bayesian filters and you will have to work hard to fix that damage. So our recommendation is to leave Auto Learn off initially until you are comfortable with your server's AntiSpam performance.

Learn Rules

The Learn Rules node is used to define message repositories that VisNetic MailServer can interrogate to update its ***Bayesian database*** (see "Bayesian Filters" on page 17), ***Whitelists*** (on page 21), and ***Blacklists*** (on page 24), making them more accurate in the long term.

Don't worry, by the way, we haven't learned about White or Black lists yet, they are in Process C.

There are 6 queues available for Indexing:

- Spam - messages sent here are indexed as Spam
- Genuine - messages sent here are indexed as Genuine
- Genuine-Spam - messages sent here are de-indexed as Genuine and indexed as Spam

- Spam-Genuine - messages sent here are de-indexed as Spam and indexed as Genuine
- Whitelist - messages sent here have their senders added to the Whitelist
- Blacklist - messages sent here have their senders added to the Blacklist

So, having said all that, our recommendation is **Do Not Use This** yet!

Ignore this until your system is running nicely, until you are confident that messages are being processed correctly and your Users are happy and Confident they know what they are doing!

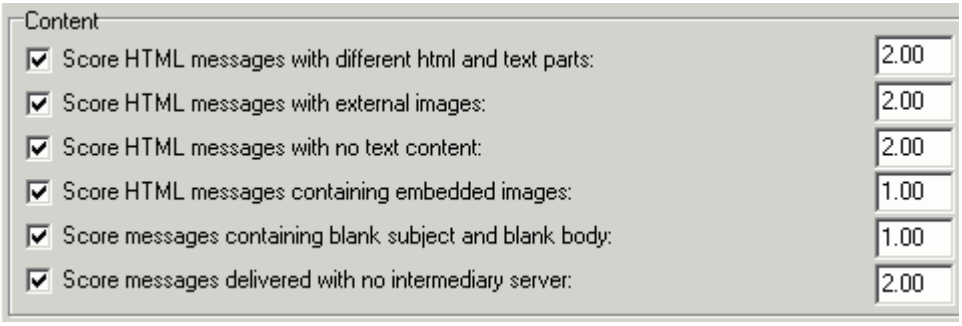
Using this option too soon can cause majors headaches for you, chasing Spam that isn't, and genuine messages that are. One false move with Indexing can lead to hours of work trying to work out what went wrong, and why.

So don't bother yet!

Content

A lot of the Spam "bombing" software that spammers uses do not format messages correctly, i.e. according to the rules.

VisNetic MailServer can take advantage of this in it's fight against Spam.



The values that you specify are used to modify the Spam Score of a message. So if you check "Score HTML messages with external images" and enter a value of 4.55 then any message with external images with have 4.55 added to it's Spam Score.

We recommend that you use all the checks with the following values:

- Score with different html and text parts - 2.00
- Score with external images - 2.00
- Score with no text content - 2.00
- Score containing embedded images - 1.00
- Score containing blank subject and body - 1.00

- Score with no intermediary server - 2.00

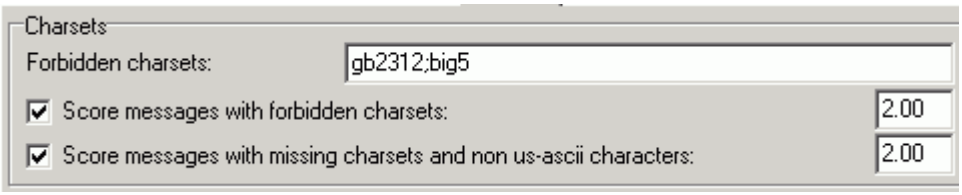
Charset

A Charset is a shortened name for the Character set used within a message.

Every message, according to the rules, should have a charset defined so the message client knows how to display that message.

There are dozens of character sets available on the internet, used by people to display text in their own language, e.g. Chinese.

Whilst these character sets are quite legitimate in use you may decide that your users will not be expecting any messages written in Japanese, and that these messages are likely to be Spam.



NOTE that you can get a list of character sets by pressing F1 whilst in this Node.

You can specify character sets that you want to distrust and a Spam Score Modifier value for the following options:

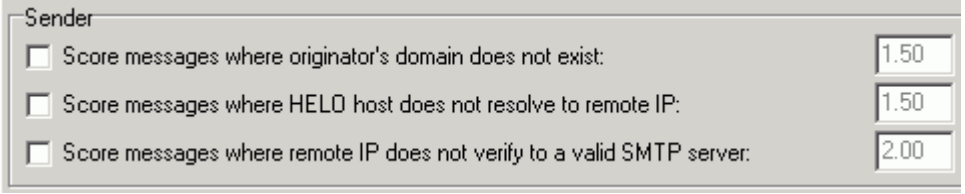
- Score messages with forbidden charsets (the ones listed)
- Score messages with missing charsets and non us-ascii characters (the message doesn't follow the rules)

Whether you use these options and the values you assign are really down to your discretion and what you feel your Users want. You can be quite aggressive with these options and score suspect messages high so they are marked as spam or quarantined based just on this scoring alone.

But it really is up to yourself, sorry.

Sender

The Sender section allows you to modify the Spam Score according to the sender information of the message.



There are three conditions you can check for:

Score messages where originator's domain does not exist

If a message being delivered is reported as coming from john@somedomain.com, VisNetic MailServer can check that somedomain.com exists and, if it doesn't, modify the Spam Score according to the value you set.

Score messages where HELO host does not resolve to remote IP

When VisNetic MailServer is initially contacted by a server to deliver messages that server will declare a hostname for itself (e.g. mail.somedomain.com). VisNetic MailServer can check that mail.somedomain.com exists and modify the Spam Score if it doesn't.

Score messages where remote IP does not verify to a valid SMTP server

In a case where the contacting servers declared hostname **does** exist, e.g. mail.somedomain.com, VisNetic MailServer can check to see whether that host is a real Mail Server and modify the Spam Score if it isn't.

Our recommendation is not to use these options initially and use them at your discretion in the future.

Process A - An instant Decision

Ok - so we've finally got to the start of VisNetic MailServer's black boxes.

We have seen all this wonderful processing that VisNetic MailServer can do to try and determine whether an incoming message is likely to be Spam or not, but it all takes time and resources!

Every incoming message is subjected to the same round of tests, and when you server gets big it can be a real problem of processing power.

So we have Whitelists, Blacklists, and a Greylist function, all of which allow VisNetic MailServer to make an "instant" decision as to whether a message is spam or not - well, it's not so instant with the Greylist, but with minimal processing.

Whitelists

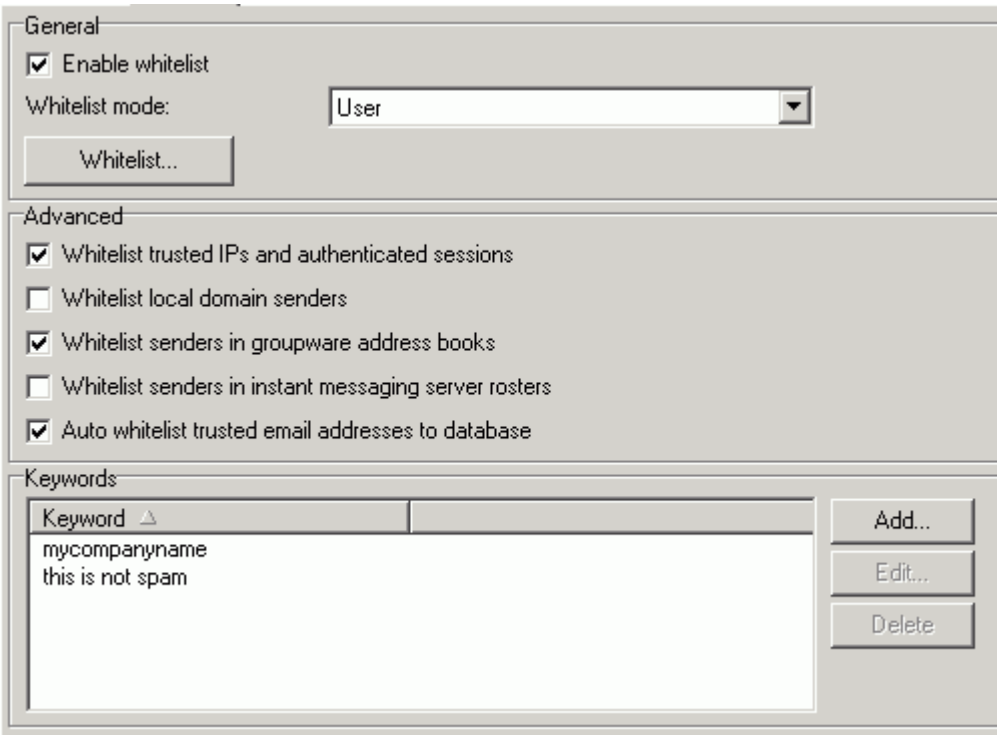
Whitelists are a way of saying "these are good guys, they don't send Spam".

For example, you receive daily update messages on a daily basis from your friend/colleague who is touring the world on vacation/business - why spend all that server time and effort checking whether his message is Spam?

You know it isn't, you want his messages, just pass them through.

Enter the Whitelist - put his email address on the whitelist and VisNetic MailServer will simply pass it through unchecked.

So let's set it up:



Check the box to Enable Whitelist processing.

Now you need to make a decision for the Whitelist mode:

- **User** - select this and addresses will be whitelisted for User who whitelists it.
- **Domain** - select this and the addresses will be whitelisted for the Domain of the User who Whitelists it.
- **System** - select this and the addresses will be whitelisted for the whole VisNetic MailServer.

Ignore the Whitelist button - it takes you to the Whitelist tab in the Spam Queues node.

The first four check boxes in the Advanced section are at your discretion based upon your User community. For the Corporate installation it is probably safe to switch all options on, for the ISP environment, it needs some careful thinking.

- **Whitelist trusted IP's and authenticated sessions**

  This refers to IP addresses that you have defined as "trusted" in the Mail Service - Security Node. These IP's are automatically added to the whitelist so any messages originating from them are passed through.

- **Whitelist Local Domain senders**

  Messages from any Domain on this installation are automatically Whitelisted.

- **Whitelist senders in Groupware address books**

  If you have set up any Groupware address books then VisNetic MailServer can automatically add the addresses to the Whitelist.

- **Whitelist senders in instant messaging server rosters**

  If you have any Instant Message Server rosters (address book equivalent) set up then these addresses can be automatically added to the Whitelist.

Ignore the Whitelist button for now - it will take you to the Spam queues - Whitelist Node, where you can administer your Whitelist entries.

Check the box to Auto whitelist - this will add trusted addresses to your Whitelist.

Select a mode for the Whitelist - sorry, another decision for you here:

- **User**

  When a User Whitelists something then it is only whitelisted for that User (most useful in ISP-type scenarios with unconnected Users)

- **Domain**

  When a User Whitelists something it is Whitelisted for that User's Domain (useful in installations where each Domain is a separate, trusted entity e.g. mulple corporate domains)

- **System**

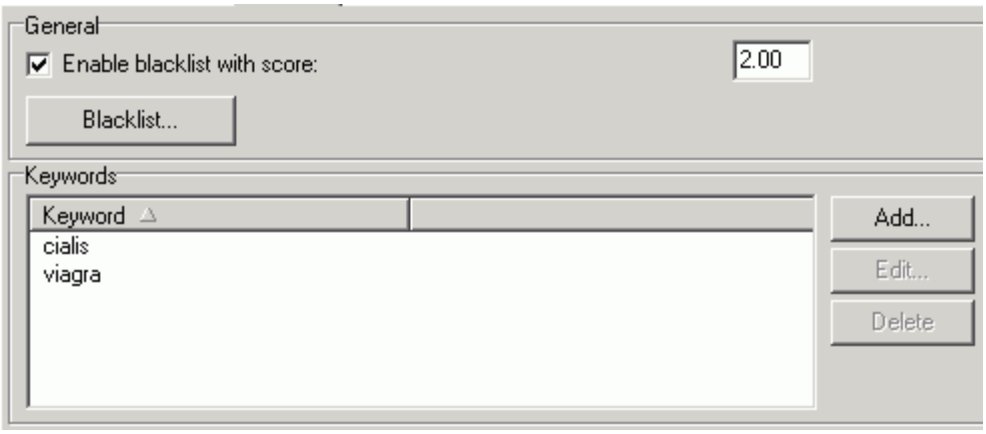
  When a User Whitelists something it is Whitelisted for the whole VisNetic MailServer Installation (useful where VisNetic MailServer is running multiple domains for a single corporate entity)

The Keywords section allows you to add a list of phrases or characters that, if found within a message, will cause that message to be whitelisted.

For example, you could add the string "asecretwayin" and tell your friends to put the string within their messages to save on VisNetic MailServer's processing power. This is another area for your discretion.

Blacklists

You might have guessed by now - a blacklist is pretty much the opposite of a whitelist, except it is not an instant rejection. If a message originates from an address or domain on the blacklist then it is instantly treated with some mistrust and its Spam Score modified by the amount you specify



You can't directly add addresses to your Blacklist from here, that is done by your users and Spam administrators as they receive unwanted messages.

You can, however, add words to your Blacklist that will cause any message containing one of those words to have its spam score altered by the amount specified.

Greylisting

Greylisting works on the fact that Spammers want to get their emails out at the speed of light. They can't be bothered waiting for servers, they just want to send their 14 million messages in the next two minutes or give up trying - so we let them give up!

In the case of "real" servers,

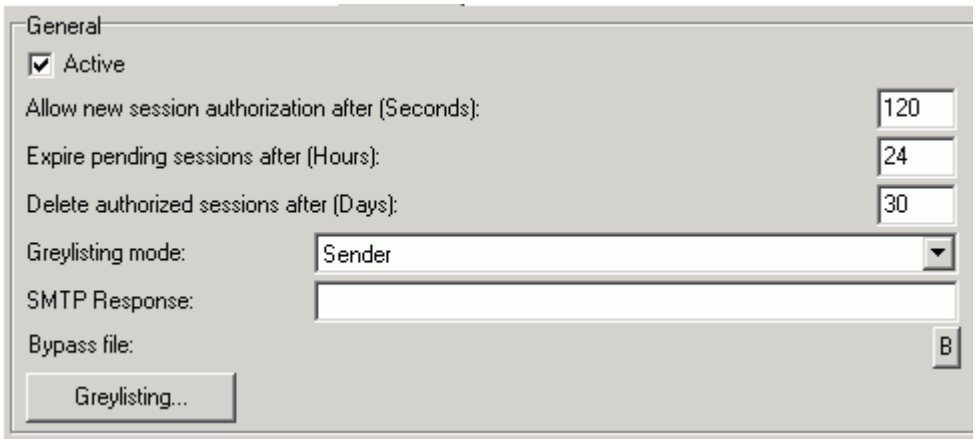
- if ServerB is busy when ServerA tries to connect and send messages, ServerB will respond with a "busy" message.
- ServerA will give up and queue those undelivered messages for retry at a later time.
- ServerA will keep retrying at set intervals (usually minutes at first, later hours) for an extended period (usually days).

In the case of many Spam "bombing" Servers.

- if ServerB is busy when SpamServerA tries to connect and send messages, ServerB will respond with a "busy" message.
- SpamServerA will give up and go away - no Spam!

So we tell VisNetic MailServer to tell incoming servers that it is busy, and the majority of Spam bombers leave us alone.

Here's how to do it:



- Check the box to activate Greylisting
- Set the Allow new session authorization to 60
- Set Expire pending sessions to 24
- Set delete authorized session to 30
- Select Sender for the Greylisting mode
- Put something meaningful in the SMTP Response, like "Greylisted - come back later" - so "real" administrators can see why their server could not get through.
- Ignore the Bypass file for now
- Ignore the Greylisting button - it takes you to the Spam Queues - Greylisting Node, where you can administer your greylisting queues.

EXPLANATION

The above settings have the following effect:

A session from a new sender will be "busied" and put on the Greylisting queue as pending.

If the session is retried within 120 seconds of initial contact it will be busied again.

If the session is retried after 120 seconds it will be accepted and it's status in the queue changed to authorized.

If the session is not retried within 24 hours it will be deleted from the queue.

The session remains authorized for 30 days, during which time any incoming sessions are accepted.

After 30 days the authorized session is deleted from the queue and the whole process must be done again for further sessions.

And finally

Take a break, you deserve it.

You now have VisNetic MailServer's AntiSpam system up and running and protecting your Users.

You can be confident that you are offering the best service and protection that is available.

You have learnt the basics about the technology that is in place and hopefully you feel more comfortable with what you can change and how you can help tweak the system for best performance.

So don't forget - keep an eye on it! Ask your Users if they are having problems - Genuine messages marked as Spam, Spam messages not marked at all.

Get into those logs and understand them. Why are messages being incorrectly classified - what is going wrong.

As the System Administrator, you have a duty to your Users. Make sure you are doing them proud. They have the best email server, give them the best Administrator to go with it.

If you have any comments or suggestions about this manual, please direct them to feedback@deerfield.com and they will be dealt with.

If you have any technical questions regarding VisNetic MailServer you should try the Users Forum at http://forum.deerfield.com, where there are dozens of people helpful and willing to help, or go directly to the Support pages at http://www.deerfield.com/support/ where you will find links to free email support and to the FAQ.

Thanks for taking the time to read this manual.

Index