MailMarshal SMTP 6.1 Default Rules (6.1.3.81)

Contents

This document provides a text listing of the default email processing rules that are installed by default with a new installation of MailMarshal SMTP 6.1 (6.1.3.81).

This information is provided in order to allow MailMarshal administrators to review the changes in default rules between product versions.

Note that not all rules are enabled by default. Disabled rules are marked (Disabled).

Read the notes on each rule for detailed information.

MARSHAL™
Secure. Protect. Comply.

Policy Group: Connection Policies

Receiver Rule: Deny Junk Mailers in Global Blacklist
This rule denies any messages from users or domains listed in the Global Blacklist User group. If a match in the group occurs, the message will be denied by the Receiver, prior to being downloaded to the MailMarshal gateway. Keep the rule up to date by adding to the 'Global Blacklist' group.
When a message arrives
Where addressed from 'Global Blacklist'
Refuse message and reply with 550 Rule imposed mailbox access for {Recipient} refused

Receiver Rule: Deny Messages where IP used in HELO String
Spammers frequently use an IP address as their HELO string. This is probably done in order to deliberately place that IP address in the Received line of the header. The IP address used is frequently a legitimate, non-blacklisted address, and the aim is probably to defeat IP blacklist checking.
Legitimate servers almost never use IP addresses in the HELO string - the standard and expected HELO string should be the fully qualified domain name (FQDN) of the server itself. As such this rule should be safe to use without the risk of blocking legitimate email.
When a message arrives
Where message is incoming
Where sender's HELO name is 'an IP address'
Refuse message and reply with 550 HELO name rejected.

Receiver Rule: Reject Messages with Blank Return Path (Disabled)
IMPORTANT - PLEASE READ:
This rule will reject all incoming messages where no return path is provided, I.E. where the connecting server issues a blank MAIL FROM address. However, enabling this rule will make you RFC non-compliant as you are obliged to accept blank return paths for the purposes of handling your own NDRs and returned messages.

Be aware that turning on this rule may also get you blacklisted - for more information see .
When a message arrives
Except where addressed to 'Postmaster Addresses'
Or except where addressed from '*@*.*'
Refuse message and reply with 550 Message rejected - user unknown.

Receiver Rule: Deny Messages to Invalid Addresses (Disabled)
This rule denies all messages to any address not listed in the 'All Employees' group. It saves resources by preventing delivery of messages to invalid users. You may also wish to enable DHA (Directory Harvest Attack) prevention in order to deny Spammers the ability to gain information on your valid email addresses.
NOTE: You must populate the 'All Employees' group with all your users before enabling this rule.
When a message arrives
Where message is incoming
Except where addressed to 'All Employees'
Refuse message and reply with 550 Rule imposed mailbox access for {Recipient} refused: user invalid

Receiver Rule: Deny Messages Over 30MB at Receiver (Disabled)
This Receiver rule will deny any message that enters the gateway, except where addressed either to or from the Information technology user group, and is identified by the foreign ESMTP server as being over 30MB in size. The foreign mail server must be ESMTP compliant for this rule to trigger. While most email systems today are ESMTP compliant, you should also create a Standard Rule (or use the Attachment Management rule called "Block

Messages Over 30MB") that stops messages of a similar size from non-ESMTP compliant servers.
When a message arrives
Except where addressed either to or from 'Information Technology'
Where the message size is greater than '30720 KB'
Refuse message and reply with 550 Rule imposed mailbox access for {Recipient} refused

Receiver Rule: Deny SpamCop Blacklisted Senders at Receiver (Disabled)
This rule denies messages from hosts listed on a DNS Blacklist, in this case SpamCop. Warning: Hosts can be wrongly listed on blacklists so use with care. If you wish to quarantine email, as opposed to outright deny, use the Engine rule. The rule excludes email from people in the Global Whitelist group. To enable a DNS rule you must first enable the DNS Blacklist that you wish to use in Server and Array Properties. You can use this rule as a template for other DNS Blacklists.
When a message arrives
Except where addressed from 'Global Whitelist'
Where sender's IP address is listed in 'SpamCop'
Refuse message and reply with 550 Rule imposed as {Sender} is blacklisted on SpamCop (see www.spamcop.net)

Receiver Rule: Deny Spamhaus Blacklisted Senders at Receiver (Disabled)
This rule denies messages from hosts listed on a DNS Blacklist, in this case Spamhaus. Warning: Hosts can be wrongly listed on blacklists so use with care. If you wish to quarantine email, as opposed to outright deny, use the Engine rule. The rule excludes email from people in the Global Whitelist group. To enable a DNS rule you must first enable the DNS Blacklist that you wish to use in Server and Array Properties. You can use this rule as a template for other DNS Blacklists.
When a message arrives
Except where addressed from 'Global Whitelist'
Where sender's IP address is listed in 'Spamhaus SBL-XBL'
Refuse message and reply with 550 Rule imposed as {Sender} is blacklisted on SpamCop (see www.spamcop.net)

7 Rule(s)

Policy Group: Virus & Threats (Inbound)

Standard Rule: Clean Virus (Disabled)
This rule will invoke all virus scanners that have been installed and defined within MailMarshal. All messages inbound to the organization will be scanned. If a virus scanner detects a virus and it can clean the virus the rule will clean the message and pass it through to the next rule. Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for viruses.
When a message arrives
Where message is incoming
Where the result of a virus scan, when scanning with all scanners, is 'Contains Virus' and 'Cleaned Virus'
Write log message(s) with 'Virus Cleaned'
And pass message to the next rule for processing.

Standard Rule: Block Virus (Disabled)
This rule will invoke all virus scanners that have been installed and defined within MailMarshal. All messages inbound to the organization will be scanned. If a virus scanner detects a virus the rule will quarantine the message and notify the local recipient(s). Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for viruses.
When a message arrives

Where message is incoming
Where the result of a virus scan, when scanning with all scanners, is 'Contains Virus'
Send a 'Virus In' notification message
And move the message to 'Virus'

Standard Rule: Virus Scanning Errors (Disabled)
The purpose of this rule is to correctly handle virus scanner errors if they occur. All messages inbound to the organization will be scanned. If the virus scanner encounters a problem during scanning the rule will quarantine the message and notify the local recipient(s). Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for virus scanning errors.
When a message arrives
Where message is incoming
Where the result of a virus scan, when scanning with all scanners, is 'Password Protected' or 'Corrupt File' or 'Signatures Out Of Date' or 'Could Not Unpack Or Analyze' or 'Unexpected Error'
Send a 'Virus Scanning Errors in' notification message
And move the message to 'Virus Scanner Errors'

Standard Rule: Block Known Virus Attachments
This rule checks for names of attachments associated with known viruses. To keep this rule up to date, subscribe to an alert service and add to the list of attachments when significant new viruses appear.
When a message arrives
Where message is incoming
Where message contains attachments named '????card.id????.cmd' or '????card.id????.bat' or '????card.id????.pif' or '????card.id????.com' or '????card.php????.cmd' or '????card.php????.bat' or '????card.php????.pif' or '????card.php????.com' or 'document_all_*.exe' or 'document_all_*.scr' or 'document_all_*.pif' or 'message_*.exe' or 'message_*.scr' or 'message_*.pif' or 'excel document_*.scr' or 'excel document_*.pif' or 'word document_*.scr' or 'word document_*.pif' or 'screensaver_*.exe' or 'screensaver_*.scr' or 'screensaver_*.pif' or 'screensaver_*.zip' or 'application_*.scr' or 'website_*.scr' or 'website_*.pif' or 'product_*.scr' or 'letter_*.scr' or 'information_*.scr' or 'details_*.scr' or 'document_*.scr' or 'all_document_*.pif' or 'document_4351.pif' or 'document_excel.pif' or 'document_full.pif' or 'document_word.pif' or 'message_details.pif' or 'message_part2.pif' or 'mp3music.pif' or 'my_details.pif' or 'your_archive.pif' or 'your_bill.pif' or 'your_details.pif' or 'your_document.pif' or 'your_file.pif' or 'your_letter.pif' or 'your_picture.pif' or 'your_product.pif' or 'your_text.pif' or 'your_website.pif' or 'yours.pif' or 'party.???.???' or 'disco.???.???' or 'mail2.???.???' or 'ranking.???.???' or 'jokes.???.???' or 'nomoney.???.???' or 'aboutyou.???.???' or 'shower.???.???' or 'topseller.???.???' or 'product.???.???' or 'swimmingpool.???.???' or 'posting.???.???' or 'creditcard.???.???' or 'readme.???.exe' or 'transcript.???.exe' or 'mail.???.exe' or 'letter.???.exe' or 'document.???.exe' or 'message.???.exe' or 'readme.???.com' or 'instruction.???.com' or 'transcript.???.com' or 'mail.???.com' or 'letter.???.com' or 'attachment.???.com' or 'document.???.com' or 'message.???.com' or 'readme.???.bat' or 'instruction.???.bat' or 'transcript.???.bat' or 'readme.???.cmd' or 'instruction.???.cmd' or 'transcript.???.cmd' or 'mail.???.cmd' or 'letter.???.cmd' or 'file.???.cmd' or 'text.???.cmd' or 'attachment.???.cmd' or 'document.???.cmd' or 'message.???.cmd' or 'readme.???.scr' or 'instruction.???.scr' or 'transcript.???.scr' or 'mail.???.scr' or 'letter.???.scr' or 'file.???.scr' or 'text.???.scr' or 'attachment.???.scr' or 'document.???.scr' or 'message.???.scr' or 'readme.???.pif' or 'instruction.???.pif' or 'transcript.???.pif' or 'mail.???.pif' or 'letter.???.pif' or 'file.???.pif' or 'text.???.pif' or 'attachment.???.pif' or 'document.???.pif' or 'message.???.pif' or ''
Send a 'Virus Attachment In' notification message
And move the message to 'Virus Suspected'

Standard Rule: Block Known Threats
This rule invokes an XML Category script to search the message for words and phrases associated with known threats and viruses. To keep this rule effective you can add to the Known Worms script when nasty new viruses appear. If the rule detects keywords associated with Known Worms it will quarantine the message and notify the local recipient(s).
When a message arrives
Where message is incoming
Where message is categorized as 'Known Threats'
Send a 'Worm In' notification message
And move the message to 'Virus Suspected'

Standard Rule: Block Virus - Zero Day Protection Framework (Disabled)
PLEASE NOTE - Enable this rule at your own risk. Because of the nature of Zero Day updates, they are published with more limited quality testing than our normal threat updates.

The rule invokes the ZeroDay Threats category script. This script is automatically updated in response to new threat outbreaks.
When a message arrives
Where message is incoming
Where message is categorized as 'Zero Day Threats'
Send a 'Worm In' notification message
And move the message to 'Virus Suspected'

Standard Rule: Block Virus Hoaxes (Disabled)
This rule invokes the TextCensor script Generic Virus Hoaxes to search the message for words and phrases associated with typical virus hoax messages. If the rule triggers it will quarantine the message and notify local recipient(s).
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Generic Virus Hoaxes'
Send a 'Potential Junk Mail in' notification message
And move the message to 'Junk'

7 Rule(s)

Policy Group: Virus & Threats (Outbound)

Standard Rule: Clean Virus (Disabled)
This rule will invoke all virus scanners that have been installed and defined within MailMarshal. All messages outbound to the organization will be scanned. If a virus scanner detects a virus and it can clean the virus the rule will clean the message and pass it through to the next rule. Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for viruses.
When a message arrives
Where message is outgoing
Where the result of a virus scan, when scanning with all scanners, is 'Contains Virus' and 'Cleaned Virus'
Write log message(s) with 'Virus Cleaned'
And pass message to the next rule for processing.

Standard Rule: Block Virus (Disabled)
This rule will invoke all virus scanners that have been installed and defined within MailMarshal. All messages outbound to the organization will be scanned. If a virus scanner detects a virus the rule will quarantine the message and notify the local sender. Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for viruses.
When a message arrives

Where message is outgoing
Where the result of a virus scan, when scanning with all scanners, is 'Contains Virus'
Send a 'Virus Out' notification message
And move the message to 'Virus'

Standard Rule: Virus Scanning Errors (Disabled)
The purpose of this rule is to correctly handle virus scanner errors if they occur. All messages inbound to the organization will be scanned. If the virus scanner encounters a problem during scanning the rule will quarantine the message and notify the local sender. Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for virus scanning errors.
When a message arrives
Where message is outgoing
Where the result of a virus scan, when scanning with all scanners, is 'Password Protected' or 'Corrupt File' or 'Signatures Out Of Date' or 'Could Not Unpack Or Analyze' or 'Unexpected Error'
Send a 'Virus Scanning Errors out' notification message
And move the message to 'Virus Scanner Errors'

Standard Rule: Block Known Virus Attachments
This rule checks for names of attachments associated with known viruses. To keep this rule up to date, subscribe to an alert service and add to the list of attachments when significant new viruses appear.
When a message arrives
Where message is outgoing
Where message contains attachments named '????card.id????.cmd' or '????card.id????.bat' or '????card.id????.pif' or '????card.id????.com' or '????card.php????.cmd' or '????card.php????.bat' or '????card.php????.pif' or '????card.php????.com' or 'document_all_*.exe' or 'document_all_*.scr' or 'document_all_*.pif' or 'message_*.exe' or 'message_*.scr' or 'message_*.pif' or 'excel document_*.scr' or 'excel document_*.pif' or 'word document_*.scr' or 'word document_*.pif' or 'screensaver_*.exe' or 'screensaver_*.scr' or 'screensaver_*.pif' or 'screensaver_*.zip' or 'application_*.scr' or 'website_*.scr' or 'website_*.pif' or 'product_*.scr' or 'letter_*.scr' or 'information_*.scr' or 'details_*.scr' or 'document_*.scr' or 'all_document_*.pif' or 'document_4351.pif' or 'document_excel.pif' or 'document_full.pif' or 'document_word.pif' or 'message_details.pif' or 'message_part2.pif' or 'mp3music.pif' or 'my_details.pif' or 'your_archive.pif' or 'your_bill.pif' or 'your_details.pif' or 'your_document.pif' or 'your_file.pif' or 'your_letter.pif' or 'your_picture.pif' or 'your_product.pif' or 'your_text.pif' or 'your_website.pif' or 'yours.pif' or 'party.???.???' or 'disco.???.???' or 'mail2.???.???' or 'ranking.???.???' or 'jokes.???.???' or 'nomoney.???.???' or 'aboutyou.???.???' or 'shower.???.???' or 'topseller.???.???' or 'product.???.???' or 'swimmingpool.???.???' or 'posting.???.???' or 'creditcard.???.???' or 'readme.???.exe' or 'transcript.???.exe' or 'mail.???.exe' or 'letter.???.exe' or 'document.???.exe' or 'message.???.exe' or 'readme.???.com' or 'instruction.???.com' or 'transcript.???.com' or 'mail.???.com' or 'letter.???.com' or 'attachment.???.com' or 'document.???.com' or 'message.???.com' or 'readme.???.bat' or 'instruction.???.bat' or 'transcript.???.bat' or 'readme.???.cmd' or 'instruction.???.cmd' or 'transcript.???.cmd' or 'mail.???.cmd' or 'letter.???.cmd' or 'file.???.cmd' or 'text.???.cmd' or 'attachment.???.cmd' or 'document.???.cmd' or 'message.???.cmd' or 'readme.???.scr' or 'instruction.???.scr' or 'transcript.???.scr' or 'mail.???.scr' or 'letter.???.scr' or 'file.???.scr' or 'text.???.scr' or 'attachment.???.scr' or 'document.???.scr' or 'message.???.scr' or 'readme.???.pif' or 'instruction.???.pif' or 'transcript.???.pif' or 'mail.???.pif' or 'letter.???.pif' or 'file.???.pif' or 'text.???.pif' or 'attachment.???.pif' or 'document.???.pif' or 'message.???.pif'
Send a 'Virus Attachment Out' notification message
And move the message to 'Virus Suspected'

Standard Rule: Block Known Threats
This rule invokes an XML Category script to search outbound messages for words and phrases associated with known worms and viruses. To keep this rule effective you can add to the Known Worms script when nasty new viruses appear. If the rule detects keywords associated with Known Worms it will quarantine the message and notify the local sender.
When a message arrives
Where message is outgoing
Where message is categorized as 'Known Threats' and type is ANY except 'DayZero Outbreak'
Send a 'Worm Out' notification message
And move the message to 'Virus Suspected'

Standard Rule: Block Threats - Zero Day Protection Framework (Disabled)
PLEASE NOTE - Enable this rule at your own risk. Because of the nature of Zero Day updates, they are published with more limited quality testing than our normal threat updates.

The rule invokes the ZeroDay Threats category script. This script is automatically updated in response to new threat outbreaks.
When a message arrives
Where message is outgoing
Where message is categorized as 'Zero Day Threats'
Send a 'Worm In' notification message
And move the message to 'Virus Suspected'

Standard Rule: Block Suspect Script and Code (Disabled)
This rule invokes the TextCensor script 'Script and Code' to search the message for suspicious scripting or code associated with known vulnerabilities. Most organizations will have little or no need to send this type of data in an email message. If the script triggers, it will quarantine the message and notify the local sender.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Script and Code'
Send a 'Script and Code out' notification message
And move the message to 'Suspect'

Standard Rule: Block Virus Hoaxes (Disabled)
This rule invokes the TextCensor script Generic Virus Hoaxes to search the message for words and phrases associated with typical virus hoax messages. If the rule triggers it will quarantine the message and notify the local sender.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Generic Virus Hoaxes'
Send a 'Potential Junk Mail out' notification message
And move the message to 'Junk'

8 Rule(s)

Policy Group: Attachment Management (Inbound)

Standard Rule: Block Suspect Attachments
This rule will block any attachment by matching the filename extension with a list of file types that could potentially contain suspect or malicious content. If the rule detects a file with a listed extension it will quarantine the message and notify the local recipient(s).
When a message arrives
Where message is incoming
Where message contains attachments named '*.bat' or '*.chm' or '*.cmd' or '*.com' or '*.pif' or '*.hlp' or '*.hta' or '*.inf' or '*.ins' or '*.js' or '*.jse' or '*.lnk' or '*.reg' or '*.scr' or '*.sct' or '*.shs' or

'*.url' or '*.vb' or '*.vbe' or '*.vbe' or '*.vbs' or '*.wsc' or '*.wsf' or '*.wsh' or '*.nws' or '*.{*}'
Send a 'File Extension in' notification message
And move the message to 'Suspect'

Standard Rule: Block Password Protected Attachments
This rule will block any message containing password-protected attachments. This is important, as this type of data cannot be virus checked or content managed at the gateway. If the rule detects password protected attachments it will quarantine the message and notify the local recipient(s).
When a message arrives
Where message is incoming
Where message attachment is of type 'SEAEncrypt' or 'ARJsfxcrypt' or 'RARsfxcrypt' or 'ZIPsfxcrypt' or 'DOCcrypt' or 'PDFcrypt' or 'SITEncrypt' or 'ARJcrypt' or 'RARcrypt' or 'ZIPcrypt'
Send a 'Password Protected in' notification message
And move the message to 'Attachment Type - Encrypted'

Standard Rule: Block Unknown Attachments
This rule will block any message containing attachments that are unrecognizable by MailMarshal. This is important, as some users will try to modify attachments to make them unrecognizable to the gateway in order to allow data into the organization. If the rule detects unrecognizable attachments it will quarantine the message and notify the Administrator and local recipient(s).
When a message arrives
Where message is incoming
Where message attachment is of type 'BIN'
And where attachment parent is not of type: 'DOC' or 'XLS' or 'PPT' or 'PPS' or 'PDF'
Send a 'Administrator Generic (With message attached)' and a 'Unrecognized Attachment in' notification message
And move the message to 'Attachment Type - Unknown'

Standard Rule: Block Fragmented Messages
This rule checks in the message header to see if the message is fragmented. If it is then it quarantines the message and notifies the local recipient(s). Because fragmented messages and/or attachments could contain dangerous code (virus, trojan or be of a file type that is not allowed by corporate policy) and can not be scanned for these items until it is reassembled, they should be handled with care.
When a message arrives
Where message is incoming
Where message contains one or more headers 'Detect Fragmented Message'
Send a 'Fragmented Message in' notification message
And move the message to 'Suspect'

Standard Rule: Block Double Extension Filenames
This rule will block any attachment with a double extension filename. This is a common method to disguise malicious email attachments. Because Windows hides the extra extension, the real nature of these files is able to remain hidden until the file is executed. Many viruses and worms generate email attachments with double executable extensions to disguise themselves as legitimate files. NOTE: Users often name their documents with double (or more) extensions, so you may want to change this rule to "copy" to a file for a test period prior to implementing.
When a message arrives
Where message is incoming
Where message contains attachments named '*.??.??' or '*.??.???' or '*.??.????' or '*.???.??' or '*.???.???' or '*.???.????'
Send a 'File Extension in' notification message
And move the message to 'Suspect'

Standard Rule: Block EXECUTABLE Files (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where addressed to users listed in the 'Information Technology' group. This type of rule uses MailMarshal's attachment decoder technology to detect executables irrespective of what they are called.
When a message arrives
Where message is incoming
Except where addressed to 'Information Technology'
Where message attachment is of type 'EXECUTABLE'
Send a 'Executable in' notification message
And move the message to 'Attachment Type - Executables'

Standard Rule: Block EXECUTABLE Files (unless zipped) (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where the executable files are actually archived within a zip file or similar.
When a message arrives
Where message is incoming
Where message attachment is of type 'EXECUTABLE'
And where attachment parent is not of type: 'ARCHIVE'
Send a 'Executable in' notification message
And move the message to 'Attachment Type - Executables'

Standard Rule: Block SMIME and PGP Encrypted (Disabled)
This rule will block any message containing PGP or S/MIME encrypted data. This is important, as this type of data cannot be virus checked or content managed at the gateway (unless you have the MailMarshal Secure option installed). If the rule detects PGP or S/MIME data it will quarantine the message and notify the local recipient(s).
When a message arrives
Where message is incoming
Where message attachment is of type 'P7M' or 'PGP'
Send a 'Encrypted in' notification message
And move the message to 'Attachment Type - Encrypted'

Standard Rule: Block VIDEO Files (Disabled)
This rule blocks messages with VIDEO attachments, except where addressed to users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses MailMarshal's attachment decoder technology, which detects video files irrespective of what they are called.
When a message arrives
Where message is incoming
Except where addressed to 'Information Technology' or 'Marketing'
Where message attachment is of type 'VIDEO'
Send a 'Video in' notification message
And move the message to 'Attachment Type - Video and Sound'

Standard Rule: Block IMAGE Files (Disabled)
This rule blocks messages with IMAGE attachments, except where addressed to users listed in the 'Executive Team', 'Sales', 'Information Technology' and 'Marketing' groups. The rule also has a size condition, so that any images under 15KB are excluded - images this small are typically business-related logos. The rule uses MailMarshal's attachment decoder technology, which detects image files irrespective of what they are called.
When a message arrives
Where message is incoming
Except where addressed to 'Information Technology' or 'Marketing' or 'Sales'
Where message attachment is of type 'IMAGE'
And where message attachment size is greater than '15 KB'
Send a 'Image in' notification message
And move the message to 'Attachment Type - Images'

Standard Rule: Block SOUND Files (Disabled)
This rule blocks messages with SOUND attachments, except where addressed to users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses MailMarshal's attachment decoder technology, which detects sound files irrespective of what they are called.
When a message arrives
Where message is incoming
Except where addressed to 'Information Technology' or 'Marketing'
Where message attachment is of type 'SOUND'
Send a 'Sound in' notification message
And move the message to 'Attachment Type - Video and Sound'

Standard Rule: Block IMAGES (unless fingerprint is known) (Disabled)
This rule blocks messages with IMAGE attachments, except where the fingerprint for that image is known to MailMarshal. This is a useful way to allow company logos to be excluded from an image-blocking rule. Fingerprints can be made known to MailMarshal from the Console when processing a quarantined message.
When a message arrives
Where message is incoming
Where message attachment is of type 'IMAGE'
And where attachment fingerprint is not known
Send a 'Image in' notification message
And move the message to 'Attachment Type - Images'

Standard Rule: Strip Executable Attachments (Disabled)
This rule strips EXECUTABLE attachments from messages, except where addressed to users listed in the 'Information Technology' user group. This type of rule uses MailMarshal's attachment decoder technology, which detects executables irrespective of what the file name extension. The rule will take a copy of the original message plus attachments, remove the EXECUTABLE files from the message, and stamp the message indicating what file has been removed.
When a message arrives
Where message is incoming
Except where addressed to 'Information Technology'
Where message attachment is of type 'EXECUTABLE'
Copy the message to 'Attachment Type - Executables'
And strip attachment
And stamp message with 'Removed Attachments'
And pass message to the next rule for processing.

Standard Rule: Block more than 10 Attachments (Disabled)
This rule blocks any message where the number of attachments is greater than 10. This rule does not count files contained within an archive such as a Zip file. A high number of attachments may be a signal that the message is non-business related.
When a message arrives
Where message is incoming
Where number of attachments is greater than '10'
Send a 'Generic in' notification message
And move the message to 'Junk'

Standard Rule: Block Messages Over 30MB (Disabled)
This is a Standard rule to quarantine messages, except where addressed to the 'Information Technology' user group, that are over 30MB in size. This rule is used in conjunction with the 30MB Receiver rule to block messages from non-ESMTP mail servers. Please note that this rule uses Message size, not attachment size. For example, at 28MB attachment would typically push the Message size well above 30MB. This is normal and expected behavior for MIME encoding.
When a message arrives

Where message is incoming
Except where addressed to 'Information Technology'
Where message size is greater than '30720 KB'
Send a 'Generic in' notification message
And move the message to 'Oversize'

15 Rule(s)

Policy Group: Attachment Management (Outbound)

Standard Rule: Block Suspect Attachments
This rule will block any attachment by matching the filename extension with a list of file types that could potentially contain suspect or malicious content. If the rule detects a file with a listed extension it will quarantine the message and notify the local sender.
When a message arrives
Where message is outgoing
Where message contains attachments named '*.bat' or '*.chm' or '*.cmd' or '*.com' or '*.pif' or '*.hlp' or '*.hta' or '*.inf' or '*.ins' or '*.js' or '*.jse' or '*.lnk' or '*.reg' or '*.scr' or '*.sct' or '*.shs' or '*.url' or '*.vb' or '*.vbe' or '*.vbe' or '*.vbs' or '*.wsc' or '*.wsf' or '*.wsh' or '*.nws' or '*.{*}'
Send a 'File Extension out' notification message
And move the message to 'Suspect'

Standard Rule: Block Password Protected Attachments
This rule will block any message containing password-protected attachments. This is important, as this type of data cannot be virus checked or content managed at the gateway. If the rule detects password protected attachments it will quarantine the message and notify the local sender.
When a message arrives
Where message is outgoing
Where message attachment is of type 'SEAEncrypt' or 'ARJsfxcrypt' or 'RARsfxcrypt' or 'ZIPsfxcrypt' or 'DOCcrypt' or 'PDFcrypt' or 'SITEncrypt' or 'ARJcrypt' or 'RARcrypt' or 'ZIPcrypt'
Send a 'Password Protected out' notification message
And move the message to 'Attachment Type - Encrypted'

Standard Rule: Block Unknown Attachments
This rule will block any message containing attachments that are unrecognizable by MailMarshal. This is important, as some users will try to modify attachments to make them unrecognizable to the gateway in order to allow data into the organization. If the rule detects unrecognizable attachments it will quarantine the message and notify the Administrator and local sender.
When a message arrives
Where message is outgoing
Where message attachment is of type 'BIN'
And where attachment parent is not of type: 'DOC' or 'XLS' or 'PPT' or 'PPS' or 'PDF'
Send a 'Administrator Generic (With message attached)' and a 'Unrecognized Attachment out' notification message
And move the message to 'Attachment Type - Unknown'

Standard Rule: Block Fragmented Messages
This rule checks in the message header to see if the message is fragmented. If it is then it quarantines the message and notifies the local sender. Because fragmented messages and/or attachments could contain dangerous code (virus, trojan or be of a file type that is not allowed by corporate policy) and can not be scanned for these items until it is reassembled, they should be handled with care.
When a message arrives
Where message is outgoing

Where message contains one or more headers 'Detect Fragmented Message'
Send a 'Fragmented Message out' notification message
And move the message to 'Suspect'

Standard Rule: Block EXECUTABLE Files (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where addressed from users listed in the 'Information Technology' group. This type of rule uses MailMarshal's attachment decoder technology to detect executables irrespective of what they are called.
When a message arrives
Where message is outgoing
Except where addressed from 'Information Technology'
Where message attachment is of type 'EXECUTABLE'
Send a 'Executable out' notification message
And move the message to 'Attachment Type - Executables'

Standard Rule: Block EXECUTABLE Files (unless zipped) (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where the executable files are actually archived within a zip file or similar.
When a message arrives
Where message is outgoing
Where message attachment is of type 'EXECUTABLE'
And where attachment parent is not of type: 'ARCHIVE'
Send a 'Executable out' notification message
And move the message to 'Attachment Type - Executables'

Standard Rule: Block SMIME and PGP Encrypted (Disabled)
This rule will block any message containing PGP or S/MIME encrypted data. This is important, as this type of data cannot be virus checked or content managed at the gateway (unless you have the MailMarshal Secure option installed). If the rule detects PGP or S/MIME data it will quarantine the message and notify the local sender.
When a message arrives
Where message is outgoing
Where message attachment is of type 'P7M' or 'PGP'
Send a 'Encrypted out' notification message
And move the message to 'Attachment Type - Encrypted'

Standard Rule: Block VIDEO Files (Disabled)
This rule blocks messages with VIDEO attachments, except where addressed from users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses MailMarshal's attachment decoder technology, which detects video files irrespective of what they are called.
When a message arrives
Where message is outgoing
Except where addressed from 'Information Technology' or 'Marketing'
Where message attachment is of type 'VIDEO'
Send a 'Video out' notification message
And move the message to 'Attachment Type - Video and Sound'

Standard Rule: Block IMAGE Files (Disabled)
This rule blocks messages with IMAGE attachments, except where addressed from users listed in the 'Executive Team', 'Sales', 'Information Technology' and 'Marketing' groups. The rule also has a size condition, so that any images under 15KB are excluded - images this small are typically business-related logos. The rule uses MailMarshal's attachment decoder technology, which detects image files irrespective of what they are called.
When a message arrives
Where message is outgoing
Except where addressed from 'Information Technology' or 'Marketing' or 'Sales' or 'Executive Team'

Where message attachment is of type 'IMAGE'
And where message attachment size is greater than '15 KB'
Send a 'Image out' notification message
And move the message to 'Attachment Type - Images'

Standard Rule: Block SOUND Files (Disabled)
This rule blocks messages with SOUND attachments, except where addressed from users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses MailMarshal's attachment decoder technology, which detects sound files irrespective of what they are called.
When a message arrives
Where message is outgoing
Except where addressed from 'Information Technology' or 'Marketing'
Where message attachment is of type 'SOUND'
Send a 'Sound out' notification message
And move the message to 'Attachment Type - Video and Sound'

Standard Rule: Park Large Files for Later Delivery (Disabled)
This rule sets aside messages in a special folder called 'Parked Large Files'. This rule will trigger if the bandwidth required to deliver the messages exceeds a certain value - in this case 20MB. The bandwidth calculation is a product of the actual message size, and the number of individual destination mailservers that MailMarshal will need to connect to in order to deliver the message. These messages will be released automatically after business hours. You can configure the release schedule by altering the properties of the 'Parked Large Files' folder.

This is commonly used to deliver large mail-outs after business hours and only the sender is notified that a message has been parked for later delivery.
When a message arrives
Where message is outgoing
Where the estimated bandwidth required for delivery is greater than '20480 KB'
Send a 'Message Delayed' notification message
And Park the message in 'Parked Large Files'

Standard Rule: Strip Executable Attachments (Disabled)
This rule strips EXECUTABLE attachments from messages, except where addressed from users listed in the 'Information Technology' user group. This type of rule uses MailMarshal's attachment decoder technology, which detects executables irrespective of what the file name extension. The rule will take a copy of the original message plus attachments, remove the EXECUTABLE files from the message, and stamp the message indicating what file has been removed.
When a message arrives
Where message is outgoing
Except where addressed from 'Information Technology'
Where message attachment is of type 'EXECUTABLE'
Copy the message to 'Attachment Type - Executables'
And strip attachment
And stamp message with 'Removed Attachments'
And pass message to the next rule for processing.

Standard Rule: Block Messages Over 30MB (Disabled)
This is a Standard rule to quarantine messages, except where addressed from the 'Information Technology' user group, that are over 30MB in size. This rule is used in conjunction with the 30MB Receiver rule to block messages from non-ESMTP mail servers. Please note that this rule uses Message size, not attachment size. For example, at 28MB attachment would typically push the Message size well above 30MB. This is normal and expected behavior for MIME encoding.
When a message arrives

Where message is outgoing
Except where addressed from 'Information Technology'
Where message size is greater than '30720 KB'
Send a 'Generic out' notification message
And move the message to 'Oversize'

13 Rule(s)

Policy Group: Spam & Junk Mail

Standard Rule: Allow Senders in Global Whitelist
This rule allows message from any sender listed in the Global Whitelist to be excluded from the remainder of the 'Spam & Junk Mail' Policy Group. Add trusted or wanted sources of email to this Whitelist.
When a message arrives
Where message is incoming
Where addressed from 'Global Whitelist'
Pass the message on to the next policy group

Standard Rule: Allow Senders in Recipient Allow List
This rule allows messages from any sender listed in the Recipients 'Allow List' to be excluded from the remainder of the 'Spam & Junk Mail' Policy Group. Users can create their own Allow List via the End User Management web console.
When a message arrives
Where message is incoming
Where the sender is in the recipient's safe senders list
Pass the message on to the next policy group

Standard Rule: Block Senders in Recipient Block List
This rule allows messages from any sender listed in the Recipients 'Block List' to be immediately quarantined to the Spam folder. Users can create their own Block List via the End User Management web console.
When a message arrives
Where message is incoming
Where the sender is in the recipient's blocked senders list
Move the message to 'Spam'

Standard Rule: Block Spam - Pornography
This rule uses the MailMarshal SpamCensor filter to identify Pornographic Spam messages.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spam' and type is 'Adult'
Move the message to 'Spam Type - Pornographic'

Standard Rule: Block Spam - Phishing
This rule uses the MailMarshal SpamCensor filter to identify Phish and identity theft type Spam messages.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spam' and type is 'Phishing'
Move the message to 'Spam Type - Phish'

Standard Rule: Block Spam - SpamCensor
This rule uses the MailMarshal SpamCensor filter to identify spam messages based on a scoring system. Messages that exceed 60 points are quarantined to the 'Spam' folder. The SpamCensor filter is a special type of Category Script that is automatically updated by NetIQ.

When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spam'
Move the message to 'Spam'

Standard Rule: Block Spam - URLCensor (by domain)
This rule invokes the URLCensor to parse the message in order to extract URLs and Web links. MailMarshal then takes the top-level domains found in those links and performs a query against a URL Blacklist - by default we use the SURBL blacklist (see www.surbl.org). If the query returns positive, the message will be quarantined to the Spam folder.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'URLCensor Blacklisted'
Move the message to 'Spam'

Standard Rule: Block Spam - Spamhaus Blacklisted
This rule uses the category script 'Spamhaus Blacklisted' to perform a query of the IP addresses in the message header against the Spamhaus SBL-XBL blacklist server (see www.spamhaus.org). If the query returns positive, the message will be quarantined to the Spam folder.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spamhaus Blacklisted'
Move the message to 'Spam'

Standard Rule: Block Spam - SpamCop Blacklisted
This rule uses the category script 'SpamCop Blacklisted' to perform a query of the IP addresses in the message header against the SpamCop DNS blacklist server (see www.spamcop.net). If the query returns positive, the message will be quarantined to the Spam folder. You can use this rule and its xml file (spamcop.xml) as a template for other DNS Blacklists rules.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'SpamCop Blacklisted'
Move the message to 'Spam'

Standard Rule: Block Spam - Administrator Maintained Keyword list
This rule uses a locally maintained TextCensor script to identify specific problematic spam and keywords and quarantine them to the 'Spam' folder. To use, simply add a unique identifying phrase to the TextCensor script to block incidents of the same message.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message triggers text censor script(s) 'Spam - Administrator maintained keyword list'
Move the message to 'Spam'

Standard Rule: Block Spam - CountryCensor (Disabled)
The CountryCensor can be used to identify the geographical location of the IP addresses listed in the message header. This can be used to eliminate all traffic from heavily Spamming countries. This could be used where you would expect to receive no legitimate email from these countries.
By default CountryCensor is not configured to block mail from any specific countries. Information of the configuration of CountryCensor can be found in CountryCensor.xml, which

is located in the Config folder, by default a subfolder of the MailMarshal install folder. Make your changes on the Array Manager, and then push your changes to all your nodes by hitting "Commit Configuration Changes"
When a message arrives
Where message is incoming
Where message is categorized as 'CountryCensor'
Move the message to 'Spam'

Standard Rule: Block Spam - URLCensor (by IP address) (Disabled)
This rule invokes the URLCensor to parse the message in order to extract URLs and Web links and extract the base domain name from these links. DNS is then used to resolve these domain(s) to their corresponding IP Address(es). MailMarshal then takes these IP Address and performs a second DNS query, this time against an IP Blacklist - by default we use the SpamHaus blacklist (see www.spamhaus.org).
If the query succeeds, the message will be quarantined to the Spam folder. By default, this rule is designed to trigger after the URLCensor so that only the URLs not caught by URLCensor will be subjected to DNS lookup, thereby minimizing resource overhead.
When a message arrives
Where message is incoming
Where message is categorized as 'URLCensor IPBlacklist'
Move the message to 'Spam'

Standard Rule: Block Spam - Zero Day Protection Framework (Disabled)
PLEASE NOTE - Enable this rule at your own risk. Because of the nature of Zero Day updates, they are published with more limited quality testing than our normal SpamCensor updates.

The rule invokes the ZeroDay Spam category script. This script will be automatically updated in response to large scale or worldwide Spam outbreaks. It is intended to be a short-term measure to protect you until the SpamCensor is updated to handle the threat.
When a message arrives
Where message is incoming
Where message is categorized as 'Zero Day Spam'
Move the message to 'Spam Type - Zero Day'

Standard Rule: Block if 'From:' Field is Invalid
This rule will block any message that arrives with a missing or invalid 'From:' field. It is not configured to send any notifications.
When a message arrives
Where message is incoming
Where message is categorized as 'InvalidFrom'
Move the message to 'Junk'

Standard Rule: Block Suspect Script and Code
This rule invokes the TextCensor script 'Script and Code' to search the message for suspicious scripting or code associated with known vulnerabilities. Most organizations will have little or no need to receive this type of data in an email message. If the script triggers, it will quarantine the message and notify the local recipient(s).
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Script and Code'
Send a 'Script and Code in' notification message
And move the message to 'Suspect'

Standard Rule: Block Spoofed Messages
This rule will attempt to detect messages that are spoofed by ensuring that a sender domain matching a local domain does in fact originate from an IP address in the local domains table. Messages that appear to be spoofed will be quarantined and a notification sent to the

intended recipient. The TextCensor script is only used to allow spoofing exclusions based on text found in the message header.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Spoofing Exclusions'
And where message spoofing analysis is based on anti-relay
Send a 'Spoofed Message In' notification message
And move the message to 'Spoofed'

Standard Rule: Block Pornographic Language
This rule invokes a TextCensor script to search the message for pornographic and sexually explicit words and phrases. It does not specifically target Spam messages, rather it searches for any sexually explicit content. This rule uses the "Language - Pornographic" TextCensor script but you can create your own, or use our scripts as a template.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Language - Pornographic'
Send a 'Language in' notification message
And move the message to 'Language'

Standard Rule: Block Common & Mild Profanity (Disabled)
This rule invokes a TextCensor script to search the message for common profanities and mildly abusive words and phrases. This rule uses the "Language - Mild Profanity" TextCensor script but you can create your own, or use our scripts as a template.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Language - Mild Profanity'
Send a 'Language in' notification message
And move the message to 'Language'

Standard Rule: Block Chain Letters (Disabled)
This rule invokes the TextCensor script 'Generic Chain Letters' to search the message for words and phrases associated with typical Chain Letters.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Generic Chain Letters'
Send a 'Potential Junk Mail in' notification message
And move the message to 'Junk'

Standard Rule: Block if 'Subject:' Field Missing or Blank (Disabled)
This rule will block any message that arrives with a missing or blank 'Subject:' field. It is not configured to send any notifications.
When a message arrives
Where message is incoming
Where message is categorized as 'Blank Subject'
Move the message to 'Junk'

Standard Rule: Block greater than 50 Recipients (Disabled)
This rule blocks any message where the number of recipients is greater than 50. A high number of recipients may be a signal that the message is non-business related.
When a message arrives
Where message is incoming
Where number of recipients is greater than '50'
Send a 'Administrator Generic (With message attached)' notification message
And move the message to 'Junk'

Standard Rule: Block Specific Character Sets (Disabled)
This rule will block messages which declare the usage of certain suspect character sets in the

message header. By default it targets a selection of character sets, including those often used in Russia, China and Korea.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Suspect Character Sets'
Move the message to 'Junk'

Standard Rule: Modify Subject Line of Spam (Disabled)
Do not use this rule if you already use the SpamCensor to block email. this rule should only be enabled after disabling the regular SpamCensor rule.

This rule uses the MailMarshal SpamCensor to identify spam messages and modifies them by appending "[SPAM]" to the subject line. This allows end users to set email client rules to move any message that contains the phrase [SPAM] in the subject line to another folder for later viewing or discarding.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spam'
Rewrite message headers using 'Rename Spam Subject'
And pass message to the next rule for processing.

23 Rule(s)

Policy Group: Policy Management (Inbound)

Standard Rule: Social Security Number detection (Disabled)
This rule searches the message body for numbers in the format of a US Social Security Number. To trigger, the rule also requires the presence of word(s) like "social", "ssn" or "soc num" in the subject or body.
When a message arrives
Where message is incoming
Where message is categorized as 'Social Security'
Send a 'Policy Risk in' notification message
And move the message to 'Policy Breaches'

Standard Rule: SEC Compliance Rule (Disabled)
This rule checks for keywords which would indicate possible SEC compliance issues. This rule archives all messages with such content for one year. If you enable this rule please review the retention time on the folder, as you may need longer than one year. Also, consider the storage requirements that arise as a result of archiving large volumes of email for long periods. The original message is allowed through to the intended recipient.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Keyword list - SEC'
Copy the message to 'Policy Breaches - SEC'
And pass message to the next rule for processing.

Standard Rule: Credit Card Number detection (Disabled)
This rule searches the message body for numbers in the format of a Credit Card numbers. To trigger, the rule typically requires the presence of word(s) like "credit", "card" or "expiry" in the subject or body.
When a message arrives
Where message is incoming
Where message is categorized as 'CreditCard'
Send a 'Policy Risk in' notification message
And move the message to 'Policy Breaches'

Standard Rule: Sarbanes-Oxley Compliance Rule (Disabled)
This rule checks for keywords which would indicate possible Sarbanes-Oxley compliance issues. This rule archives all messages with such content for one year. If you enable this rule please review the retention time on the folder, as you may need longer than one year. Also, consider the storage requirements that arise as a result of archiving large volumes of email for long periods. The original message is allowed through to the intended recipient.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Keyword list - SOX'
Copy the message to 'Policy Breaches - SOX'
And pass message to the next rule for processing.

Standard Rule: Racist and Hate content (Disabled)
This rule monitors email for racist and hate content. If the TextCensor script triggers then a copy of the message is held for review, and the original message is allowed through to the original recipient.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Language - Racist and Hate'
Copy the message to 'Policy Breaches'
And pass message to the next rule for processing.

Standard Rule: Weapons related content (Disabled)
This rule monitors email for weapons-related content. If the TextCensor script triggers then a copy of the message is held for review, and the original message is allowed through to the original recipient.
When a message arrives
Where message is incoming
Where message triggers text censor script(s) 'Weapons related content'
Copy the message to 'Policy Breaches'
And pass message to the next rule for processing.

6 Rule(s)

Policy Group: Policy Management (Outbound)

Standard Rule: Block Pornographic Language
This rule invokes a TextCensor script to search the message for pornographic and sexually explicit words and phrases. It does not specifically target Spam messages, rather it searches for any sexually explicit content. This rule uses the "Language - Pornographic" TextCensor script but you can create your own, or use our scripts as a template.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Language - Pornographic'
Send a 'Language out' notification message
And move the message to 'Language'

Standard Rule: Block Common & Mild Profanity (Disabled)
This rule invokes a TextCensor script to search the message for common profanities and mildly abusive words and phrases. This rule uses the "Language - Mild Profanity" TextCensor script but you can create your own, or use our scripts as a template.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Language - Mild Profanity'
Send a 'Language out' notification message
And move the message to 'Language'

Standard Rule: Social Security Number detection (Disabled)
This rule searches the message body for numbers in the format of a US Social Security Number. To trigger, the rule also requires the presence of word(s) like "social", "ssn" or "soc num" in the subject or body.
When a message arrives
Where message is outgoing
Where message is categorized as 'Social Security'
Send a 'Policy Risk out' notification message
And move the message to 'Policy Breaches'

Standard Rule: SEC Compliance Rule (Disabled)
This rule checks for keywords which would indicate possible SEC compliance issues. This rule archives all messages with such content for one year. If you enable this rule please review the retention time on the folder, as you may need longer than one year. Also, consider the storage requirements that arise as a result of archiving large volumes of email for long periods. The original message is allowed through to the intended recipient.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Keyword list - SEC'
Copy the message to 'Policy Breaches - SEC'
And pass message to the next rule for processing.

Standard Rule: Credit Card Number detection (Disabled)
This rule searches the message body for numbers in the format of a Credit Card numbers. To trigger, the rule typically requires the presence of word(s) like "credit", "card" or "expiry" in the subject or body.
When a message arrives
Where message is outgoing
Where message is categorized as 'CreditCard'
Send a 'Policy Risk out' notification message
And move the message to 'Policy Breaches'

Standard Rule: Sarbanes-Oxley Compliance Rule (Disabled)
This rule checks for keywords which would indicate possible Sarbanes-Oxley compliance issues. This rule archives all messages with such content for one year. If you enable this rule please review the retention time on the folder, as you may need longer than one year. Also, consider the storage requirements that arise as a result of archiving large volumes of email for long periods. The original message is allowed through to the intended recipient.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Keyword list - SOX'
Copy the message to 'Policy Breaches - SOX'
And pass message to the next rule for processing.

Standard Rule: Monitor CVs and Resumes (Disabled)
This rule uses the TextCensor script "Resume and CVs" to look for signs of Resumes & CVs in outbound email. It copies the message to the folder called "Policy Breaches" and logs an entry into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Resume and CVs'
Copy the message to 'Policy Breaches'
And write log message(s) with 'Contains a CV'
And pass message to the next rule for processing.

Standard Rule: Racist and Hate content (Disabled)
This rule monitors email for racist and hate content. If the TextCensor script triggers then a

copy of the message is held for review, and the original message is allowed through to the original recipient.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Language - Racist and Hate'
Copy the message to 'Policy Breaches'
And pass message to the next rule for processing.

Standard Rule: Weapons related content (Disabled)
This rule monitors email for weapons-related content. If the TextCensor script triggers then a copy of the message is held for review, and the original message is allowed through to the original recipient.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Weapons related content'
Copy the message to 'Policy Breaches'
And pass message to the next rule for processing.

Standard Rule: Stamp Scanned and Processed (Disabled)
This rule places the MailMarshal Scanned message stamp on every outbound message. This is useful to let the intended recipient(s) know that the message has been content checked and is unlikely to contain material that they would not want to receive.
When a message arrives
Where message is outgoing
Where message is outgoing
Stamp message with 'MailMarshal Scanned'
And pass message to the next rule for processing.

10 Rule(s)

Policy Group: Automated Responses

Standard Rule: Allow Senders in Recipient Allow List
This rule allows messages from any sender listed in the Recipients 'Allow List' to be excluded from the remainder of the 'Automated Responses' Policy Group. Users can create their own Allow List via the End User Management web console.
When a message arrives
Where the message is addressed to or from any user
Where the sender is in the recipient's safe senders list
Pass the message on to the next policy group

Standard Rule: Harvest Outbound Recipients
This rule will harvest all outbound external recipients for the purposes of excluding these recipients from spam filtering. The assumption is that any external recipients to whom you send email will be legitimate. Even if you unintentionally whitelist a Spammers address with this rule, that should not be a big issue, as Spammers rarely reuse addresses. On the other hand it is key to whitelist as many legitimate users as possible.
When a message arrives
Where message is outgoing
Except where addressed to 'Global Whitelist'
Or except where addressed from 'Postmaster Addresses'
Add message recipients into 'Harvested Whitelist'
And pass message to the next rule for processing.

Standard Rule: Challenge - Response Successful (Disabled)
This rules is designed to trigger on responses to the initial Challenge - Response rule. Senders who successfully answer the challenge message will have their original message

released, and have their email address added to the harvested whitelist.
When a message arrives
Where addressed to 'Postmaster Addresses'
Except where addressed from 'Global Whitelist'
Where the external command 'Message Release' is triggered
And where message contains one or more headers 'Challenge Subject Keyword'
Send a 'Challenge - Response Successful' notification message
And delete the message
And add message sender into 'Harvested Whitelist'

Standard Rule: Challenge - Response by Group (Disabled)
This rule applies to a specific local group only (by default the Executive Team group). For all members of that group, all email from the Internet is blocked unless the sender is already known and in the Global Whitelist. For all other senders to this local group a challenge is sent back to the sender. Once the sender responds to the challenge the original message is released and their address is automatically harvested. In the future the same sender will not be challenged in this way again.

The rule applies to a specific group only as it is a very aggressive means of blocking Spam. In this case it only applies to those local users for whom total Spam blocking is a primary requirement, and for whom the Challenge / Response mechanism is acceptable.
When a message arrives
Where addressed to 'Executive Team'
Except where addressed to 'Postmaster Addresses'
Or except where addressed from 'Global Whitelist'
Send a 'Challenge - Response Block' notification message
And move the message to 'Awaiting Challenge - Response'

Standard Rule: Challenge - Response Block Unknown (Disabled)
With this rule, all email from the Internet is blocked unless the sender is already known and in the Global Whitelist. For all others a challenge is sent back to the sender. Once the sender responds to the challenge the original message is released and their address is automatically harvested. In the future the same sender will not be challenged in this way again.

The rule is a very aggressive means of blocking Spam and should be used only after taking due consideration of the consequences. Note that the Challenge \ Response system can generate a high volume of NDRs, and that messages from legitimate listservers will be blocked by default.
When a message arrives
Where message is incoming
Except where addressed to 'Executive Team' or 'Postmaster Addresses'
Or except where addressed from 'Global Whitelist'
Send a 'Challenge - Response Block' notification message
And move the message to 'Awaiting Challenge - Response'

Standard Rule: Product Info Auto Responder (Disabled)
This rule will act as an auto-responder to automatically send information based on a request in the subject line of a message. This can be used to automate the delivery of all kinds of sales and marketing information. You can attach a file to the Product Info Auto Responder email template if required.
When a message arrives
Where addressed to 'productinfo@mydomain.com'
Where message triggers text censor script(s) 'Product Info Auto Responder'
Send a 'Product Info Auto Responder' notification message
And write log message(s) with 'Product Info Request'
And pass message to the next rule for processing.

Standard Rule: Old Domain Name Responder (Disabled)
This rule will respond to a user that sends a message to an old domain name. It will notify them that the domain name is going to be removed and to change their address list to reflect the new domain name.
When a message arrives
Where addressed either to or from '@our.old.domain.com'
Send a 'Old Domain Name Responder' notification message
And write log message(s) with 'Message to Old Domain'
And pass message to the next rule for processing.

7 Rule(s)

Policy Group: Monitoring Only

Standard Rule: Monitor Viruses (Disabled)
This rule is for monitoring/evaluation purposes and will NOT block viruses. This rule will invoke all virus scanners that have been installed and defined within MailMarshal. All messages to and from the organization will be scanned. If a virus scanner detects a virus then the message is copied (not moved) to allow safe reviewing in the Console.
Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for viruses.
When a message arrives
Where the message is addressed to or from any user
Where the result of a virus scan, when scanning with all scanners, is 'Contains Virus'
Copy the message to 'Virus'
And pass the message on to the next policy group

Standard Rule: Monitor Virus Scanning Errors (Disabled)
This rule is for monitoring/evaluation purposes. The purpose of this rule is to correctly handle virus scanner errors if they occur. All messages to and from the organization will be scanned. If the virus scanner encounters a problem during scanning then the message is copied (not moved) to allow safe reviewing in the Console.
Note: You must install a supported virus scanner, define the scanner within MailMarshal and then enable this rule in order to check for viruses.
When a message arrives
Where the message is addressed to or from any user
Where the result of a virus scan, when scanning with all scanners, is 'Password Protected' or 'Corrupt File' or 'Signatures Out Of Date' or 'Could Not Unpack Or Analyze' or 'Unexpected Error'
Copy the message to 'Virus Scanner Errors'
And pass the message on to the next policy group

Standard Rule: Monitor Spam - SpamCensor
This rule is for monitoring/evaluation purposes. It uses the MailMarshal SpamCensor filter to identify spam messages based on a scoring system. Messages that exceed 60 points are copied to the 'Spam' folder, and the original message is allowed through to the intended recipient. The SpamCensor filter is a special type of Category Script that is automatically updated by NetIQ.
When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spam'
Copy the message to 'Spam'
And pass the message on to the next policy group

Standard Rule: Monitor Spam - URLCensor
This rule is for monitoring/evaluation purposes. It invokes the URLCensor to parse the

message in order to extract URLs and Web links. MailMarshal then takes the top-level domains found in those links and performs a query against a URL Blacklist - by default we use the SURBL blacklist (see www.surbl.org). If the query returns positive, the message will be copied to the Spam folder, and the original message is allowed through to the intended recipient.

When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'URLCensor Blacklisted'
Copy the message to 'Spam'
And pass the message on to the next policy group

Standard Rule: Monitor Spam - Spamhaus Blacklisted

This rule is for monitoring/evaluation purposes. It uses the category script 'Spamhaus Blacklisted' to perform a query of the IP addresses in the message header against the Spamhaus blacklist server (see www.spamhaus.org). If the query returns positive, the message will be copied to the Spam folder, and the original message is allowed through to the intended recipient.

When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'Spamhaus Blacklisted'
Copy the message to 'Spam'
And pass the message on to the next policy group

Standard Rule: Monitor Spam - SpamCop Blacklisted

This rule is for monitoring/evaluation purposes. This rule uses the category script 'SpamCop Blacklisted' to perform a query of the IP addresses in the message header against the SpamCop DNS blacklist server (see www.spamcop.net). If the query returns positive, the message will be copied to the Spam folder, and the original message is allowed through to the intended recipient. You can use this rule and its xml file (spamcop.xml) as a template for other DNS Blacklists rules.

When a message arrives
Where message is incoming
Where message size is less than '125 KB'
And where message is categorized as 'SpamCop Blacklisted' and type is 'any'
Copy the message to 'Spam'
And pass the message on to the next policy group

Standard Rule: Monitor if 'From:' Field is Invalid

This rule is for monitoring/evaluation purposes. This rule will take a copy any message that arrives with a missing or invalid 'From:' field - the original message is allowed through to the intended recipient.

When a message arrives
Where message is incoming
Where message is categorized as 'InvalidFrom'
Copy the message to 'Junk'
And pass the message on to the next policy group

Standard Rule: Monitor MP3s

This rule is for monitoring/evaluation purposes. If an MP3 audio file is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.

When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'MP3'

Copy the message to 'Attachment Type - Video and Sound'
And pass the message on to the next policy group

Standard Rule: Monitor Audio
This rule is for monitoring/evaluation purposes. If an audio file (other than MP3) is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'ASF' or 'ASX' or 'AU' or 'MID' or 'WAV' or 'RAM' or 'RA' or 'RMP'
Copy the message to 'Attachment Type - Video and Sound'
And pass the message on to the next policy group

Standard Rule: Monitor Videos
This rule is for monitoring/evaluation purposes. If a video file is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'VIDEO'
Copy the message to 'Attachment Type - Video and Sound'
And pass the message on to the next policy group

Standard Rule: Monitor PDFs
This rule is for monitoring/evaluation purposes. If a PDF file is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where message is incoming
Where message attachment is of type 'PDF' or 'PDFcrypt'
Copy the message to 'Attachment Type - Documents'
And pass the message on to the next policy group

Standard Rule: Monitor Images
This rule is for monitoring/evaluation purposes. If an image file larger than 15Kb is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'IMAGE'
And where message attachment size is greater than '15 KB'
Copy the message to 'Attachment Type - Images'
And pass the message on to the next policy group

Standard Rule: Monitor CVs and Resumes (Outbound) (Disabled)
This rule is for monitoring/evaluation purposes. It uses the TextCensor script "Resume and CVs" to look for signs of CVs and Resumes in outbound email. If the rule triggers then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where message is outgoing
Where message triggers text censor script(s) 'Resume and CVs'
Copy the message to 'Policy Breaches'
And pass the message on to the next policy group

Standard Rule: Monitor Pornographic Language
This rule is for monitoring/evaluation purposes. This rule invokes a TextCensor script to search the message for pornographic and sexually explicit words and phrases. It does not specifically target Spam messages, rather it searches for any sexually explicit content. This rule uses the "Language - Pornographic" TextCensor script but you can create your own, or use our scripts as a template.
When a message arrives
Where the message is addressed to or from any user
Where message triggers text censor script(s) 'Language - Pornographic'
Copy the message to 'Language'
And pass the message on to the next policy group

Standard Rule: Monitor Common Profanity (Disabled)
This rule is for monitoring/evaluation purposes. This rule invokes a TextCensor script to search the message for common profanities and mildly abusive words and phrases. This rule uses the "Language - Mild Profanity" TextCensor script but you can create your own, or use our scripts as a template.
When a message arrives
Where the message is addressed to or from any user
Where message triggers text censor script(s) 'Language - Mild Profanity'
Copy the message to 'Language'
And pass the message on to the next policy group

Standard Rule: Monitor Chain Letters
This rule is for monitoring/evaluation purposes. It uses the TextCensor script "Generic Chain Letters" to look for chain letters. If the rule triggers then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message triggers text censor script(s) 'Generic Chain Letters'
Copy the message to 'Junk'
And pass the message on to the next policy group

Standard Rule: Monitor Bandwidth Exceeding 500KB
This rule is for monitoring/evaluation purposes. It looks for any messages requiring more than 500KB for delivery. If the rule triggers then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where the estimated bandwidth required for delivery is greater than '500 KB'
Copy the message to 'Oversize'
And pass the message on to the next policy group

Standard Rule: Monitor Executables (Disabled)
This rule is for monitoring/evaluation purposes. If an Executable file is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'EXECUTABLE'
Copy the message to 'Attachment Type - Executables'
And pass the message on to the next policy group

Standard Rule: Monitor Virus Hoaxes (Disabled)
This rule is for monitoring/evaluation purposes. It uses the TextCensor script "Generic Virus

Hoaxes" to look for virus hoaxes. If the rule triggers then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message triggers text censor script(s) 'Generic Virus Hoaxes'
Copy the message to 'Junk'
And pass the message on to the next policy group

Standard Rule: Monitor Stock Trading Content (Disabled)
This rule is for monitoring/evaluation purposes. It uses the TextCensor script "Stock Trading" to look for content related to trading stocks, and logs an entry into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message triggers text censor script(s) 'Stock Trading'
Copy the message to 'Policy Breaches'
And pass the message on to the next policy group

Standard Rule: Monitor PGP Encrypted (Disabled)
This rule is for monitoring/evaluation purposes. If a PGP Encrypted file is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'PGP'
Copy the message to 'Attachment Type - Encrypted'
And pass the message on to the next policy group

Standard Rule: Monitor Script and Code (Disabled)
This rule is for monitoring/evaluation purposes. It uses the TextCensor script "Script and Code" to look for scripting or executable code in messages, and logs an entry into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message triggers text censor script(s) 'Script and Code'
Copy the message to 'Suspect'
And pass the message on to the next policy group

Standard Rule: Monitor Unknown Attachments (Disabled)
This rule is for monitoring/evaluation purposes. This rule will look for any message containing attachments that are unrecognizable by MailMarshal. This is important, as some users will try to modify attachments to make them unrecognizable to the gateway in order to allow data into the organization. If a unrecognized file is detected, then the message is copied (not moved) to allow viewing in the Console, and an entry is logged into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where the message is addressed to or from any user
Where message attachment is of type 'BIN'
And where attachment parent is not of type: 'DOC' or 'XLS' or 'PPT' or 'PPS' or 'PDF'
Copy the message to 'Attachment Type - Unknown'
And pass the message on to the next policy group

Standard Rule: Monitor Mail to Hotmail and Yahoo (Disabled)
This rule is for monitoring/evaluation purposes. It looks for messages addressed to Hotmail or Yahoo domains and logs an entry into the database for later reporting. The original message

is allowed through to the intended recipient.
When a message arrives
Where addressed to '*@hotmail.com' or '*@yahoo.com'
Write log message(s) with 'Addressed to Hotmail or Yahoo'
And pass the message on to the next policy group

Standard Rule: Monitor Multiple Recipients (Outbound) (Disabled)
This rule is for monitoring/evaluation purposes. It looks for outbound messages with more than 6 recipients and logs an entry into the database for later reporting. The original message is allowed through to the intended recipient.
When a message arrives
Where message is outgoing
Where number of recipients is greater than '6'
Write log message(s) with 'Has Multiple Recipients'
And pass message to the next rule for processing.

25 Rule(s)

Policy Group: Message Archiving

Standard Rule: Archive All Inbound Messages
This rule archives all inbound messages to a special Archive folder. By default, messages are kept for 6 months.
When a message arrives
Where message is incoming
Copy the message to 'Archive In'
And pass message to the next rule for processing.

Standard Rule: Archive All Outbound Messages
This rule archives all outbound messages to a special Archive folder. By default, messages are kept for 6 months.
When a message arrives
Where message is outgoing
Copy the message to 'Archive Out'
And pass message to the next rule for processing.

2 Rule(s)

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email:emea.sales@marshal.com

Americas
Marshal Inc.
5909 Peachtree Dunwoody Road NE,
Suite 770,
Atlanta,
GA 30328
USA

Phone: +1 404 564-5800
Fax +1 404 564-5801

Email:americas.sales@marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email:apac.sales@marshal.com

info@marshal.com | www.marshal.com