Trustwave®

USER GUIDE

MailMarshal Cloud (SEG Cloud) Available Policy and Features

Table of Contents

About This Document **2**

1 Non-Rule Functionality **3**

1.1 Disclaimers (Message Stamps) 3
1.2 Keywords Detection 3
1.3 Administrative Email Addresses 3
1.4 Notifications 3
1.5 Digests 3
1.6 Blended Threats Exclusions 3
1.7 Executive Names List 3
1.8 Connector Agent 3
1.9 DKIM Signing 4

2 Processing Policies **5**

2.1 Package: Trustwave Sandbox Filtering 5
2.1.1 From Trustwave Sandbox (Inbound) 5
2.2 Package: Standard Protection – Outbound Rules 6
2.2.1 Malware Protection (Outbound) 6
2.2.2 Customer Blacklist (Outbound) 8
2.2.3 Anti-Spam (Outbound) 9
2.2.4 Size and Bandwidth Control (Outbound) 11
2.2.5 Transport Layer Security (Outbound) 13
2.2.6 Attachment Control (Outbound) 14
2.2.7 Message Content (Outbound) 17
2.2.8 Dead Letter Handling (Outbound) 19
2.3 Package: Standard Protection – Inbound Rules 19
2.3.1 Malware Protection (Inbound) 19
2.3.2 Invalid Recipient Handling (Inbound) 21
2.3.3 Customer Blacklist (Inbound) 22
2.3.4 Anti-Spam (Inbound) 22
2.3.5 Business Email Compromise (Inbound) 27
2.3.6 DMARC Policy (Inbound) 28
2.3.7 Size and Bandwidth Control (Inbound) 30
2.3.8 Transport Layer Security (Inbound) 33

2.3.9 Domain Reputation (Inbound) 34
2.3.10 Attachment Control (Inbound) 35
2.3.11 Message Content (Inbound) 38
2.3.12 Dead Letter Handling (Inbound) 41
2.4 Package: Blended Threats 41
2.4.1 Blended Threats Protection (Inbound) 41
2.5 Package: Data Protection 41
2.5.1 Sensitive Material (Outbound) 41
2.5.2 Sensitive Material (Inbound) 44
2.6 Package: Acceptable Use 45
2.6.1 Objectionable Material (Outbound) 45
2.6.2 Objectionable Material (Inbound) 47
2.7 Package: Advanced Image Analysis 48
2.7.1 Image Analyzer (Outbound) 48
2.7.2 Image Analyzer (Inbound) 49
2.8 Package: Trustwave Sandbox Routing 49
2.8.1 To Trustwave Sandbox (Inbound) 49
2.9 Package: Data Retention – 31 days 49
2.9.1 31 day retention outbound 49
2.9.2 31 day retention inbound 50
2.10 Package: Data Retention – 90 days 50
2.10.1 90 day retention outbound 50
2.10.2 90 day retention inbound 50
2.11 Package: Trustwave Secure Email Encryption 51
2.11.1 Secure Email Encryption (Outbound) 51

About This Document

This document provides detail of the policy and feature configuration available to MailMarshal Cloud (SEG Cloud) customers.

Use this listing along with the MailMarshal Cloud Customer Guide to understand the available features and functions of MailMarshal Cloud.

If you have a business need that you believe is not covered by the polices and features listed, contact Trustwave to discuss your requirements.

The policy listing has been updated with current rules and offerings as of April 2024.

- Messages containing suspicious URLs detected by URL Categorizer are logged in a unique classification.
- Additional Credit Card and Social Security rules are available that apply additional keyword checks to reduce false positive triggering.
- The Phishing detection rule is now applied before other spam blocking rules. This rule quarantines messages (previous versions stamped a warning)
- Additional packages are available to retain messages for 31 or 90 days (purchased separately).

1 Non-Rule Functionality

1.1 Disclaimers (Message Stamps)

Two configurable disclaimer texts are available, one for inbound messages and one for outbound messages. Disclaimers can be stamped at the top or bottom of messages. If a disclaimer is enabled, all messages for the direction will be stamped (User Matching and other conditions are not supported).

1.2 Keywords Detection

Customers can block (quarantine) messages that contain keywords or phrases. Keyword entries can be combined using Boolean and proximity operators. Separate keyword lists are available for inbound and outbound messages. For details, see the Customer Guide and Help.

1.3 Administrative Email Addresses

The Server address and Administrator address can be set for each configured domain. It is not possible to configure specific addresses for each notification.

1.4 Notifications

Notification templates and notification rules cannot be customized. Only the templates and notifications configured in existing rules can be used.

1.5 Digests

Default Digest Templates and Quarantine Digests are configured. Additional Digest Templates and Digests can be configured.

1.6 Blended Threats Exclusions

Customers using Blended Threats Protection can maintain a list of domains that will never be subject to Blended Threats scanning. URLs in these domains will not be rewritten by the Blended Threats functionality.

1.7 Executive Names List

Customers can provide a list of names and email addresses of company executives. This list is used to assist in prevention of email fraud, by identifying messages from external sources that may appear to come from trusted internal users.

1.8 Connector Agent

Customers can synchronize user and group information (for rule User Matching) to MailMarshal Cloud from their Active Directory or LDAP server.

1.9 DKIM Signing

Outbound mail from customers can be DKIM signed. For more information, see MailMarshal Cloud Knowledgebase article Q21085.

2 Processing Policies

- Unless otherwise noted, individual rules can be enabled or disabled.
- Where noted, User Matching can be applied to policy groups (rulesets) and rules. User Matching allows you to apply policy based on groups of email addresses, including wildcard entries. User Matching allows you to apply any combination of the following conditions:
    - Where Addressed To
    - Where Addressed From
    - Except Where Addressed To
    - Except Where Addressed From

2.1 Package: Trustwave Sandbox Filtering

Note: The Filtering package is part of the Trustwave Sandbox offering. This package applies only to messages returned from the Sandbox service. To enable Sandboxing (if provisioned), see the Trustwave Sandbox Routing package below.

2.1.1 From Trustwave Sandbox (Inbound)

This ruleset evaluates the results of Sandbox inspection, and blocks messages identified as malicious.

Rule: Trustwave Sandbox Block Malware

Cannot be disabled

This rule quarantines messages that are identified as Malware by the Trustwave Sandbox Service.

When a message arrives
And the message is incoming
Where addressed from 'IP Trustwave Sandbox'
Where message is categorized as 'Trustwave Sandbox Malicious Attachment'
Then
Write log message with 'Malware - Trustwave Sandbox'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Trustwave Sandbox Block Suspected Malware

This rule quarantines messages that are identified as Suspected Malware by the Trustwave Sandbox Service

When a message arrives
And the message is incoming
Where addressed from 'IP Trustwave Sandbox'
Where message is categorized as 'Trustwave Sandbox Suspect Attachment'
Then
Write log message with 'Malware - Suspect - Trustwave Sandbox'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Trustwave Sandbox Block Spam

Cannot be disabled

This rule moves to the Spam folder messages that are identified as spam by the Trustwave Sandbox Service. These messages can be managed by end users

When a message arrives
And the message is incoming
Where addressed from 'IP Trustwave Sandbox'
Where message is categorized as 'Trustwave Sandbox Spam'
Then
Write log message with 'Spam - Trustwave Sandbox'
And move the message to 'Spam - General (Incoming)' with release action "continue processing"

Rule: Trustwave Sandbox Block Suspect URL

This rule quarantines messages that are identified as containing suspect URLs by the Trustwave Sandbox Service

When a message arrives
And the message is incoming
Where addressed from 'IP Trustwave Sandbox'
Where message is categorized as 'Trustwave Sandbox Suspect URL'
Then
Write log message with 'Suspect URL - Trustwave Sandbox'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Trustwave Sandbox Error

This rule quarantines messages that were forwarded to the Trustwave Sandbox Service but could not be fully analyzed

When a message arrives
And the message is incoming
Where addressed from 'IP Trustwave Sandbox'
Where message is categorized as 'Trustwave Sandbox Error'
Then
Write log message with 'Sandbox - Error'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.2 Package: Standard Protection – Outbound Rules

2.2.1 Malware Protection (Outbound)

This ruleset scans outgoing messages for malicious code and content, blended threats, and suspicious attachments.

Rule: Block Malware - Email Threat Detection (Notify)

Cannot be disabled

This rule targets traits of malware-sending bots and suspicious attachments. The heuristic detection script is updated regularly to detect emerging threats.

When a message arrives
And the message is outgoing
Where message is categorized as 'Known Threats'
Then
Send a 'Malware Out' system notification message
  And write log message with 'Malware - Threats'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Suspect File Attachments

This rule scans messages for suspicious file attachments. These attachments are rarely transferred via email, and can harbor malicious content.

When a message arrives
And the message is outgoing
Where message contains attachment(s) named '*.bat' '*.chm' '*.cmd' '*.com' '*.pif' '*.hlp' '*.hta' '*.inf' '*.ins' '*.js' '*.jse' '*.lnk' '*.one' '*.reg' '*.scr' '*.sct' '*.shs' '*.url' '*.vb' '*.vbe' '*.vbs' '*.msc' '*.wsf' '*.wsh' '*.nws' '*.{*}' '*.cpl'
Then
Write log message with 'Malware - Suspect File Attachments'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Suspect File Attachments (Notify)

This rule scans messages for suspicious file attachments. These attachments are rarely transferred via email, and can harbor malicious content. The sender is notified about the message being blocked.

When a message arrives
And the message is incoming
Where message contains attachment(s) named '*.bat' '*.chm' '*.cmd' '*.com' '*.pif' '*.hlp' '*.hta' '*.inf' '*.ins' '*.js' '*.jse' '*.lnk' '*.one' '*.reg' '*.scr' '*.sct' '*.shs' '*.url' '*.vb' '*.vbe' '*.vbs' '*.msc' '*.wsf' '*.wsh' '*.nws' '*.{*}' '*.cpl'
Then
Send a 'File Extension Out' system notification message
  And write log message with 'Malware - Suspect File Attachments'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Signature Scanner

Cannot be disabled

This rule scans messages for malware using traditional, signature-based AV technology. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is outgoing
Where the result of a virus scan , when scanning with all scanners, is 'Contains Virus'

Then
Write log message with 'Malware - Known Malware'
And move the message to 'Quarantine (Outgoing)' with release action “continue processing”

Rule: Block Malware - Signature Scanner Error

Cannot be disabled

This rule sends a notification to the system administrator if the AV scanner experiences an unexpected failure. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is outgoing
Except where addressed from 'TEMP XLS Senders'
Where the result of a virus scan , when scanning with all scanners, is 'Virus scanner signature is out of date' or 'Unexpected scanner error'
Then
Send a 'Malware - AV Scanner Error' notification message
And write log message with 'Malware - AV Scanner Error'
And move the message to 'Quarantine (Outgoing)' with release action “continue processing”

Rule: Block Malware - Signature Scanner File Error

Cannot be disabled

This rule sends a notification to the system administrator if the AV scanner experiences a failure analyzing a file. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is outgoing
Except where addressed from 'TEMP XLS Senders'
Where the result of a virus scan , when scanning with all scanners, is 'File is corrupt' or 'Could not fully unpack or analyze file'
Then
Send a 'Malware - AV Scanner Error out (Sender)' notification message
And write log message with 'Malware - AV Scanner Error'
And move the message to 'Quarantine (Outgoing)' with release action “continue processing”

2.2.2 Customer Blacklist (Outbound)

Rule: Block Blacklisted Email Addresses (Senders)

This rule blocks outgoing mail addressed from addresses in the Preset Group - Blacklisted Senders (Internal)

When a message arrives
And the message is outgoing
Where addressed from 'Preset Group - Blacklisted Senders (Internal)'
Then
Write log message with 'Message - Blacklisted'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Blacklisted Email Addresses (Recipients)

This rule blocks outgoing mail addressed to addresses in the Preset Group - Blacklisted Recipients (External)

When a message arrives
And the message is outgoing
Where addressed to 'Preset Group - Blacklisted Recipients (External)'
Then
Write log message with 'Message - Blacklisted'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.2.3 Anti-Spam (Outbound)

User Matching Allowed

This ruleset blocks outgoing spam messages using a variety of technologies.

Rule: Block Spam - Signatures and Behavior

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and botnet characteristics. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware)) and SpamBotCensor
Then
Write log message with 'Spam - High Certainty'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Spam - Signatures and Heuristics

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and heuristic analysis of content. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamCensor and SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - High Certainty'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Signatures

User Matching Allowed

This rule blocks messages identified as spam by a signature based technology. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Suspect Spam - Heuristics

User Matching Allowed

This rule blocks messages identified as spam by heuristic analysis of content. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamCensor
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Suspect Spam - URL Blacklist

User Matching Allowed

This rule blocks messages identified as spam because they contain web links that are associated with spam. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where message is categorized as 'URLCensor Blacklisted'
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Keywords

User Matching Allowed

This rule blocks messages identified as spam because they contain keywords associated with spam (a list manually maintained by Trustwave). These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where message triggers TextCensor script(s) 'ISP-Maintained Keyword List'
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - High Volume

User Matching Allowed

This rule blocks messages that have similar signatures and high volume. Please note it may trigger false positives if you have mass mailings originating from your system.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamProfiler (Spam Bulk Mail, Suspected Spam, Confirmed (Malware), High (Probable Malware))
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Suspect Spam - Suspicious URLs in message

User Matching Allowed

This rule blocks messages that contain URLs identified as suspicious (phishing, malware, or spam) by the Trustwave URL Categorizer.

When a message arrives
And the message is outgoing
Where the message contains suspect URLs
Then
Write log message with ‘Suspect URL - Trustwave URL Categorizer’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

2.2.4 Size and Bandwidth Control (Outbound)

This ruleset blocks outbound messages based on their size and bandwidth requirements.

Rule: Block Messages over 50 MB

User Matching Allowed

Block outbound messages over 50MB.

When a message arrives
And the message is outgoing
Where message size is Greater Than '51200 KB’
Then
Write log message with ‘Message - Exceeds Size Limit’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Messages over 100MB (Notify)

Block outbound messages over 100MB (System Limit).

When a message arrives
And the message is outgoing
Where message size is Greater Than '102400 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And delete the message

Rule: Block Messages over 50MB (Notify)

User Matching Allowed

Block outbound messages over 50MB and provide a notification to the sender.

When a message arrives
And the message is outgoing
Where message size is Greater Than '51200 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Messages over 40MB (Notify)

User Matching Allowed

Block outbound messages over 40MB and provide a notification to the sender.

When a message arrives
And the message is outgoing
Where message size is Greater Than '40960 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Messages over 30MB (Notify)

User Matching Allowed

Block outbound messages over 30MB and provide a notification to the sender.

When a message arrives
And the message is outgoing
Where message size is Greater Than '30720 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Messages over 20MB (Notify)

User Matching Allowed

Block outbound messages over 20MB and provide a notification to the sender.

When a message arrives
And the message is outgoing
Where message size is Greater Than '20480 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
And write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Messages over 10MB (Notify)

User Matching Allowed

Block outbound messages over 10MB and provide a notification to the sender.

When a message arrives
And the message is outgoing
Where message size is Greater Than '10240 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
And write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Messages over 5MB (Notify)

User Matching Allowed

Block outbound messages over 5MB and provide a notification to the sender.

When a message arrives
And the message is outgoing
Where message size is Greater Than '5120 KB'
Then
Send a 'Message Size - Over Limit (Outgoing)' notification message
And write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.2.5 Transport Layer Security (Outbound)

Provides the ability to ensure messages are sent by industry standard security mechanisms.

User Matching Allowed

Rule: Deliver using TLS only

User Matching Allowed

Requires a TLS (secure) connection for delivery of messages to external domains you specify. If a message cannot be delivered over TLS, it is returned to the local sender.

When a message arrives
And the message is outgoing
Where addressed to 'Preset Group – TLS – Enforce Delivery Recipients'
Then
Deliver the mail via TLS only

2.2.6 Attachment Control (Outbound)

Rule: Block unknown attachments

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious.

When a message arrives
And the message is outgoing
Where message attachment is of type 'BIN'
Then
Write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block unknown attachments (Notify)

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'BIN'
Then
Send a 'Attachment Type – Unrecognized (out)' notification message
And write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block executable files

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives.

When a message arrives
And the message is outgoing
Where message attachment is of type 'EXECUTABLE'
Then
Write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block executable files (Notify)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'EXECUTABLE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type – Executable (out)'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block executable files (unless in Archive File)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. This rule notifies the sender of the message that it was blocked. Executable files inside standard archives, such as ZIP, RAR, or ARJ will not be blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'EXECUTABLE'
And where attachment parent type is not of type: ' ARCHIVE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Video files

User Matching Allowed

This rule blocks messages which contain video attachments. Files in this category include AVI, MP4, Flash, and Quicktime files.

When a message arrives
And the message is outgoing
Where message attachment is of type 'VIDEO'
Then
Write log message with 'Attachment Type - Video'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Video files (Notify)

User Matching Allowed

This rule blocks messages which contain video attachments. Files in this category include AVI, MP4, Flash, and Quicktime files. A notification is sent to the sender.

When a message arrives
And the message is outgoing
Where message attachment is of type 'VIDEO'
Then
Send a 'Video out' system notification message
  And write log message with 'Attachment Type - Video'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Sound files

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files.

When a message arrives
And the message is outgoing
Where message attachment is of type 'SOUND'
Then
Write log message with 'Attachment Type - Sound'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Sound files (Notify)

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'SOUND'
Then
Send a 'Attachment Type - Sound out' notification message
  And write log message with 'Attachment Type - Sound'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block encrypted attachments

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents.

When a message arrives
And the message is outgoing
Where message attachment is of type 'ENCRYPTED'
Then
Write log message with 'Attachment Type - Encrypted'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block encrypted attachments (Notify)

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'ENCRYPTED'
Then
Send a 'Attachment Type - Encrypted out' notification message
And write log message with 'Attachment Type - Encrypted'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Office Macro Documents

User Matching Allowed

This blocks messages that contain Office documents having macros included in them.

When a message arrives
And the message is outgoing
Where message is categorized as 'Office Document Macros'
Then
Write log message with 'Attachment Type – Office Macros'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Office Macro Documents (Notify)

User Matching Allowed

This blocks messages that contain Office documents having macros included in them. A notification is sent to the sender.

When a message arrives
And the message is outgoing
Where message is categorized as 'Office Document Macros'
Then
Send a 'Office Macro Document (Out)' system notification message
Write log message with 'Attachment Type – Office Macros'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.2.7 Message Content (Outbound)

Rule: Strip read receipts from messages

User Matching Allowed

This rule removes read receipt requests from messages. The messages content is otherwise unaffected.

When a message arrives
And the message is outgoing
Then

Write log message with 'Strip Read Receipt Headers'
And rewrite message headers using 'Strip Read Receipt Request'

Rule: Strip sensitive information from headers

User Matching Allowed

This rule strips information from a message's header which might leak information about your internal network environment. This includes information about the network hosts that handled the message during delivery, and the software package and version information that may be in use by your organization. The messages content is unaffected.

When a message arrives
And the message is outgoing
Then
Rewrite message headers using 'Remove selected Header fields'

Rule: Block Spoofed Messages

User Matching Allowed

This rule blocks outbound messages from being sent from one of your domains, which were sourced from an unknown IP address, from a client that has not authenticated with the MailMarshal Cloud service, or from a host not designated in your SPF records.

When a message arrives
And the message is outgoing
Where message spoofing analysis is based on anti-relay
Then
Write log message with 'Message - Spoofed Message'

Rule: Block Fragmented Messages

User Matching Allowed

Fragmented messages are messages that come in one or more parts, and are re-assembled at the delivery point to read the entire content. Fragmented messages are very rarely used for legitimate purposes today, and can be an indicator that an attacker is attempting to bypass content scanning filters..

When a message arrives
And the message is outgoing
Where message contains one or more headers 'Detect Fragmented Messages'
Then
Write log message with 'Message - Fragmented Message'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Encrypted Messages

User Matching Allowed

This rule prevents messages which contain S/MIME or PGP encrypted material from being sent to your organization. Internal employees may receive confidential information in encrypted form, to prevent detection by automated systems.

When a message arrives
And the message is outgoing
Where message attachment is of type 'P7M; PGP'
  And where message spoofing analysis is based on anti-relay and where Sender ID evaluation fails with Moderate Settings
Then
Write log message with 'Message - Encrypted'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.2.8 Dead Letter Handling (Outbound)

Quarantines malformed or otherwise unscannable or undeliverable mails.

No customer configuration is allowed.

2.3 Package: Standard Protection – Inbound Rules

2.3.1 Malware Protection (Inbound)

This ruleset scans inbound messages for malicious code and content, blended threats, and suspicious attachments. Our Base offering will use the Sophos Anti-Malware engine, which will be included for all customers as part of the basic package.

Rule: Block Malware - Email Threat Detection (Notify)

This rule targets traits of malware-sending bots and suspicious attachments. The heuristic detection script is updated regularly to detect emerging threats.

When a message arrives
And the message is incoming
Where message is categorized as 'Known Threats'
Then
Write log message with 'Malware - Threats'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware - Suspect File Attachments

This rule scans messages for suspicious file attachments. These attachments are rarely transferred via email, and can harbor malicious content.

When a message arrives
And the message is incoming
Where message contains attachment(s) named '*.bat' '*.chm' '*.cmd' '*.com' '*.pif' '*.hlp' '*.hta' '*.inf' '*.ins' '*.js' '*.jse' '*.lnk' '*.one' '*.reg' '*.scr' '*.sct' '*.shs' '*.url' '*.vb' '*.vbe' '*.vbs' '*.msc' '*.wsf' '*.wsh' '*.nws' '*.{*}' '*.cpl'
Then
Write log message with 'Malware - Suspect File Attachments'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware - Signature Scanner

This rule scans messages for malware using traditional, signature-based AV technology. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is incoming
Where the result of a virus scan , when scanning with all scanners, is 'Contains Virus'
Then
Write log message with 'Malware - Known Malware'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware - Signature Scanner Error

This rule sends a notification to the system administrator if the AV scanner experiences an unexpected failure. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is incoming
Where the result of a virus scan , when scanning with all scanners, is 'Virus scanner signature is out of date' or 'Unexpected scanner error'
Then
Send a 'Malware - AV Scanner Error out' notification message
And write log message with 'Malware - AV Scanner Error'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware - Signature Scanner File Error

This rule sends a notification to the system administrator if the AV scanner experiences an unexpected failure. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is incoming
Where the result of a virus scan , when scanning with all scanners, is 'File is corrupt' or 'Could not fully unpack or analyze file'
Then
Send a 'Malware - AV Scanner (recipient)' notification message
And write log message with 'Malware - AV Scanner Error'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware – Advanced Malware Exploit Detection

User Matching Allowed

This rule blocks messages that contain files that trigger the Trustwave SEG Advanced Malware Engine. A notification is sent to the recipient.

When a message arrives
And the message is incoming
Where message is identified as containing malware by Yara Analysis Engine AMAX
Then
Send a 'AMAX In' notification message

And write log message with 'Malware – Advanced Malware Detection'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware – Malformed PDF Detection

User Matching Allowed
Disabled by default. Trustwave recommends you enable this rule.

This rule blocks messages that contain PDF files that are malformed and cannot be opened and scanned. They could potentially be malicious. A notification is sent to the recipient. (This rule may be subject to a small amount of false positives)

When a message arrives
And the message is incoming
Where message is identified as containing malware by Yara Analysis Engine Malformed PDF
Then
Send a 'Malformed PDF In' notification message
And write log message with 'Malware – Suspect File Attachments'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.2 Invalid Recipient Handling (Inbound)

The rules in this policy can refuse or block emails to invalid (unknown) addresses. IMPORTANT: Before enabling the included rules, you must set up User Matching with a group that includes all valid email addresses.

Important: All rules in this policy are currently optional in all regions (this is a change for the Australia and Europe regions). These rules are still recommended to reduce unwanted traffic to customer servers.

Rule: Refuse emails to invalid addresses

User Matching Allowed (Required)

This rule blocks messages to invalid users. IMPORTANT: This rule denies all messages to any address. It can only be used with a manually created User Group Exception that includes all valid email addresses in your environment. Please contact your Service Provider before you use this rule.

When a message arrives
And the message is incoming
Except where addressed to…{User Group exception must be completed}
Then
Refuse message and reply with '550 Mailbox access for {Recipient} refused: address invalid.'

Rule: Block emails to invalid recipients

User Matching Allowed (Required)

This rule blocks messages to invalid users. IMPORTANT: This rule denies all messages to any address. It can only be used with a manually created User Group Exception that includes all valid email addresses in your environment. Please contact your Service Provider before you use this rule.

When a message arrives
And the message is incoming
Then
Write log message with 'Message - Invalid Address'
And move the message to ‘Quarantine (Incoming)’ with release action "skip all remaining rules"

2.3.3 Customer Blacklist (Inbound)

Rule: Block Blacklisted Email Addresses (Senders)

This rule blocks incoming mail addressed from addresses in the Preset Group - Blacklisted Senders (External)

When a message arrives
And the message is incoming
Where addressed from 'Preset Group - Blacklisted Senders (External)'
Then
Write log message with 'Message - Blacklisted'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Blacklisted Email Addresses (Recipients)

This rule blocks incoming mail addressed from addresses in the Preset Group - Blacklisted Recipients (Internal)

When a message arrives
And the message is incoming
Where addressed to 'Preset Group - Blacklisted Recipients (Internal)'
Then
Write log message with 'Message - Blacklisted'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

2.3.4 Anti-Spam (Inbound)

User Matching Allowed

This ruleset block incoming spam messages using a variety of technologies.

Rule: Refuse Messages from blacklisted IP addresses

User Matching Allowed

This rule refuses delivery of messages from source systems that are identified as spam senders by a proprietary listing. The rule returns a failure code to the sending system. The message is completely rejected and not quarantined.

When a message arrives
And the message is incoming
Where sender's IP address is listed by 'Marshal IP Reputation Service'
Then
Refuse message and reply with '550 IP address listed by Marshal IP Reputation Service. Refusing message.'

Rule: Refuse senders which fail SPF check

User Matching Allowed

This rule refuses delivery of messages from source systems that fail a check using the Sender Policy Framework (SPF). The rule returns a failure code to the sending system. The message is completely rejected and not quarantined..

When a message arrives
And the message is incoming
Where the SPF evaluation fails a Relaxed check
Then
Refuse message and reply with '550 SPF relaxed check failed.'

Rule: Allow users on Global Whitelist

Bypasses Spam check for trusted addresses (managed by Trustwave).

When a message arrives
And the message is incoming
Where addressed from 'Global Whitelist'
Then
Write log message with 'Info - Safe Sender'
And pass the message on to the next policy group

Rule: Allow Users on Safe Senders list

User Matching Allowed

Bypasses Spam check for trusted addresses (managed by each end user).

When a message arrives
And the message is incoming
Where the sender is in the recipient's safe senders list
Then
Write log message with 'Info - Safe Sender'
And pass the message on to the next policy group

Rule: Block Users on Blocked Senders list

User Matching Allowed

This rule blocks messages based on the recipient's Blocked Senders list (managed in the SQM console). Before using this rule, request enablement of the Blocked Senders feature. This option is intended to allow users to block material that is unwanted but not malicious, such as newsletters.

When a message arrives
And the message is incoming
Where the sender is in the recipient's blocked senders list
Then
Write log message with 'Spam – End user blacklist'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Phishing

User Matching Allowed

This rule blocks suspected phishing messages. Messages blocked by this rule are monitored by the threat evaluation team. Trustwave strongly recommends you do not enable SQM management of the Spam – Phishing category.

When a message arrives
And the message is incoming
Where message is categorized as 'Phishing'
Then
Write log message with 'Spam - Phishing'
And move the message to 'Spam - General' with release action "continue processing"

Rule: Block Spam - Signatures and Behavior

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and botnet characteristics. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware)) and SpamBotCensor
Then
Write log message with 'Spam - High Certainty'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Spam - Signatures and Heuristics

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and heuristic analysis of content. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamCensor and SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - High Certainty'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Signatures

User Matching Allowed

This rule blocks messages identified as spam by a signature based technology. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Behavior

User Matching Allowed

This rule blocks messages identified as spam due to characteristics typical of spambot origin. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamBotCensor
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Heuristics

User Matching Allowed

This rule blocks messages identified as spam by heuristic analysis of content. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamCensor
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam – Newly Registered Domain

User Matching Allowed

Blocks mail containing URLs referencing domains that were registered in the past 24 hours.

When a message arrives
And the message is incoming
Where message is categorized as 'Newly registered domain'
Then
Write log message with 'Spam – Domain Age Detection'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Suspect Spam - IP Blacklist

User Matching Allowed

This rule blocks messages from source systems that are identified as spam senders by a proprietary listing. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where message is categorized as 'Marshal RBL Blacklisted'
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - URL Blacklist

User Matching Allowed

This rule blocks messages identified as spam because they contain web links that are associated with spam. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where message is categorized as 'URLCensor Blacklisted'
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Keywords

User Matching Allowed

This rule blocks messages identified as spam because they contain keywords associated with spam (a list manually maintained by Trustwave). These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where message triggers TextCensor script(s) 'ISP-Maintained Keyword List'
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - Foreign Character Sets

User Matching Allowed

This rule blocks messages that use foreign character sets.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Suspect Character Sets'
Then
Write log message with 'Spam - Foreign Character Sets'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Suspect Spam – Suspicious URLs in message

User Matching Allowed

This rule blocks messages that contain URLs identified as suspicious (phishing, malware, or spam) by the Trustwave URL Categorizer.

When a message arrives
And the message is incoming
Where message contains suspect URLs
Then
Write log message with 'Suspect URL - Trustwave URL Categorizer'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.5 Business Email Compromise (Inbound)

This ruleset helps detect and manage Business Email Compromise Fraud emails.

Rule: Block BEC - BEC Fraud Filter

User Matching Allowed

Trustwave strongly recommends you do not disable this rule

This rule blocks messages with multiple traits associated with BEC fraud.

When a message arrives
And the message is incoming
Where message is categorized as 'BECFraud v8'
Then
Send a 'Business Email Compromise - In' system notification message
And write log message with "BEC - Filter'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block – Executive Name Match

User Matching Allowed

Blocks emails when a name in the From: header matches one of those configured in the Executive Names List.

When a message arrives
And the message is incoming
Where message is categorized as 'Executive Name'
Then
Send a 'Business Email Compromise - In' system notification message
And write log message with "BEC – Executive Name'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block – Domain Similarity Match

User Matching Allowed

Blocks emails where the domain in the From: header closely resembles one of your local domains.

When a message arrives
And the message is incoming
Where message is categorized as ‘Domain Similarity’
Then
Send a 'Business Email Compromise - In' system notification message
  And write log message with "BEC – Domain Similarity’
  And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Warn – From Reply-To Mismatch

User Matching Allowed

Adds a warning to the message where the From and Reply-To email addresses are mismatched.

When a message arrives
And the message is incoming
Where message is categorized as ‘From Reply-To Mismatch’
Then
Write log message with "BEC – From Reply-To Mismatch’
  And stamp message with "BEC – From Reply-To Mismatch’

Rule: Warn – External Email

User Matching Allowed

Adds a warning to the message indicating that the message was received from an external source.

When a message arrives
And the message is incoming
Then
Stamp message with "External Email Warning’

2.3.6 DMARC Policy (Inbound)

This ruleset allows you to mark or block mail based on the result of DMARC evaluation. Only available if DMARC is properly configured for your domain(s). By default the Monitor rules are enabled and Quarantine rules are disabled.

Rule: DMARC Policy Reject (Quarantine)

User Matching Allowed

This rule quarantines messages that failed DMARC evaluation where the sending domain owner requests that messages be rejected. Only company Administrators can release messages quarantined by this rule.

When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'reject' applied
Then
Write log message with ‘DMARC – Reject'
  And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”
  And report the DMARC disposition of 'reject' for this message

Rule: DMARC Policy Quarantine (Quarantine)

User Matching Allowed

This rule quarantines messages that failed DMARC evaluation where the sending domain owner requests that messages be quarantined.

When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'quarantine' applied
Then
Write log message with 'DMARC – Quarantine'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"
  And report the DMARC disposition of 'quarantine' for this message

Rule: DMARC - Error

User Matching Allowed

This rule quarantines messages where DMARC evaluation encountered an error and could not be completed.

When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'error' applied
Then
Write log message with 'DMARC – Error'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: DMARC Policy Reject (Monitor)

User Matching Allowed

This monitoring rule rewrites the message subject to alert the recipient that the message failed DMARC evaluation and the sender domain requests "reject" action. The message is not quarantined or rejected.
When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'reject' applied
Then
Write log message with 'DMARC – Policy Reject (Monitor)'
  And prepend [DMARC Failed (Reject)] to message subject
  And continue processing rules

Rule: DMARC Policy Quarantine (Monitor)

User Matching Allowed

This monitoring rule rewrites the message subject to alert the recipient that the message failed DMARC evaluation and the sender domain requests quarantine action. The message is not quarantined.

When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'quarantine' applied
Then

Write log message with ‘DMARC – Policy Quarantine (Monitor)'
And prepend [DMARC Failed (Quarantine)] to message subject
And continue processing rules

Rule: DMARC Policy None (Monitor)

User Matching Allowed

This monitoring rule rewrites the message subject to alert the recipient that the message failed DMARC evaluation and the sender domain does not request any specific action. The message is not quarantined.

When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'none' applied
Then
Write log message with ‘DMARC – Policy None (Monitor)'
And prepend [DMARC Failed (None)] to message subject
And continue processing rules

Rule: DMARC Error (Monitor)

User Matching Allowed

This monitoring rule rewrites the message subject to alert the recipient that DMARC evaluation encountered an error and could not be completed.

When a message arrives
And the message is incoming
Where message was checked with DMARC and a result of 'error' applied
Then
Write log message with ‘DMARC – Error (Monitor)'
And prepend [DMARC Error] to message subject
And continue processing rules

2.3.7 Size and Bandwidth Control (Inbound)

This ruleset blocks inbound messages based on their size and bandwidth requirements.

Rule: Block Messages over 50 Megabytes

User Matching Allowed

Block inbound messages over 50MB.

When a message arrives
And the message is incoming
Where message size is Greater Than '51200 KB’
Then
Write log message with ‘Message - Exceeds Size Limit’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Messages over 40 Megabytes

User Matching Allowed

Block inbound messages over 40MB.

When a message arrives
And the message is incoming
Where message size is Greater Than '40960 KB'
Then
Write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 30 Megabytes

User Matching Allowed

Block inbound messages over 30MB.

When a message arrives
And the message is incoming
Where message size is Greater Than '30720 KB'
Then
Write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 20 Megabytes

User Matching Allowed

Block inbound messages over 20MB.

When a message arrives
And the message is incoming
Where message size is Greater Than '20480 KB'
Then
Write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 10 Megabytes

User Matching Allowed

Block inbound messages over 10MB.

When a message arrives
And the message is incoming
Where message size is Greater Than '10240 KB'
Then
Write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 5 Megabytes

User Matching Allowed

Block inbound messages over 5MB.

When a message arrives
And the message is incoming
Where message size is Greater Than '5120 KB'
Then
Write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 50MB (Notify)

User Matching Allowed

Block inbound messages over 50MB and provide a notification to the recipient.

When a message arrives
And the message is incoming
Where message size is Greater Than '51200 KB'
Then
Send a 'Message Size - Over Limit (Incoming)' notification message
And write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 40MB (Notify)

User Matching Allowed

Block inbound messages over 40MB and provide a notification to the recipient

When a message arrives
And the message is incoming
Where message size is Greater Than '40960 KB'
Then
Send a 'Message Size - Over Limit (Incoming)' notification message
And write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 30MB (Notify)

User Matching Allowed

Block inbound messages over 30MB and provide a notification to the recipient

When a message arrives
And the message is incoming
Where message size is Greater Than '30720 KB'
Then
Send a 'Message Size - Over Limit (Incoming)' notification message
And write log message with 'Message - Exceeds Size Limit'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 20MB (Notify)

User Matching Allowed

Block inbound messages over 20MB and provide a notification to the recipient

When a message arrives
And the message is incoming
Where message size is Greater Than '20480 KB'
Then
Send a 'Message Size - Over Limit (Incoming)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 10MB (Notify)

User Matching Allowed

Block inbound messages over 10MB and provide a notification to the recipient

When a message arrives
And the message is incoming
Where message size is Greater Than '10240 KB'
Then
Send a 'Message Size - Over Limit (Incoming)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Messages over 5MB (Notify)

User Matching Allowed

Block inbound messages over 5MB and provide a notification to the recipient

When a message arrives
And the message is incoming
Where message size is Greater Than '5120 KB'
Then
Send a 'Message Size - Over Limit (Incoming)' notification message
  And write log message with 'Message - Exceeds Size Limit'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.8 Transport Layer Security (Inbound)

Provides the ability to ensure messages are received by industry standard security mechanisms.

User Matching Allowed

Rule: Message not received via TLS (Block)

Blocks (quarantines) messages from domains you specify, if they are not received over a TLS (secure) connection.

When a message arrives
And the message is incoming
Where addressed from 'Preset Group – TLS – Enforce TLS Senders'
Where message was not received via TLS
Then

Write log message with 'TLS – Not received via TLS'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.9 Domain Reputation (Inbound)

User Matching Allowed

Rule: DKIM - Signature verification failed (Monitor)

User Matching Allowed

Logs messages that are DKIM signed if the signature is not verified. Does not change or block the messages.

When a message arrives
And the message is incoming
Where the DKIM verification result is 'Fail'
Then
Copy the message to 'Monitor (Incoming)' with release action "continue processing"
And write log message with 'DKIM - Signature failed'

Rule: DKIM - Signature verification failed (Stamp)

User Matching Allowed

Stamps the text of messages with a warning when they are DKIM signed and the signature is not verified.

When a message arrives
And the message is incoming
Where the DKIM verification result is 'Fail'
Then
Write log message with 'DKIM - Signature failed'
And stamp message with 'DKIM Signature Failed'

Rule: DKIM - Signature verification failed (Block)

User Matching Allowed

Blocks (quarantines) messages when they are DKIM signed and the signature is not verified.

When a message arrives
And the message is incoming
Where the DKIM verification result is 'Fail'
Then
Write log message with 'DKIM - Signature failed'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: DKIM - Signature not present (Block)

User Matching Allowed

Blocks (quarantines) messages from domains you specify, if they are not DKIM signed.

When a message arrives
And the message is incoming
Where addressed from 'Preset Group – DKIM – Enforce Senders'
Where the DKIM verification result is 'Not Present'
Then
Write log message with 'DKIM - Signature not present'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.10 Attachment Control (Inbound)

Rule: Block unknown attachments

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious.

When a message arrives
And the message is incoming
Where message attachment is of type 'BIN'
Then
Write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block unknown attachments (Notify)

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'BIN'
Then
Send a 'Attachment Type - Unrecognized' notification message
And write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block executable files

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives.

When a message arrives
And the message is incoming
Where message attachment is of type 'EXECUTABLE'
Then
Write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block executable files (Notify)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'EXECUTABLE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block executable files (unless in Archive File)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. Executable files inside standard archives, such as ZIP, RAR, or ARJ will not be blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'EXECUTABLE'
And where attachment parent type is not of type: ' ARCHIVE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Video files

User Matching Allowed

This rule blocks messages which contain video attachments. Files in this category include AVI, MP4, Flash, and Quicktime files.

When a message arrives
And the message is incoming
Where message attachment is of type 'VIDEO'
Then
Write log message with 'Attachment Type - Video'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Sound files

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files.

When a message arrives
And the message is incoming
Where message attachment is of type 'SOUND'
Then
Write log message with 'Attachment Type - Sound'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Sound files (Notify)

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'SOUND'
Then
Send a 'Attachment Type - Sound' notification message
And write log message with 'Attachment Type - Sound'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block encrypted attachments

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents.

When a message arrives
And the message is incoming
Where message attachment is of type 'ENCRYPTED'
Then
Write log message with 'Attachment Type - Encrypted'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block encrypted attachments (Notify)

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'ENCRYPTED'
Then
Send a 'Attachment Type - Encrypted' notification message
And write log message with 'Attachment Type - Encrypted'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Archive attachments (Notify)

User Matching Allowed

This rule blocks messages which contain archived attachments. Files in this category include ZIP, ARJ, TAR and other formats. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'ARCHIVE'
Then
Send a 'Archive in' system notification message
And write log message with 'Attachment Type - Archive'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Office Macro Documents

User Matching Allowed

This blocks messages that contain Office documents having macros included in them.

When a message arrives
And the message is incoming
Where message is categorized as 'Office Document Macros'
Then
Write log message with 'Attachment Type – Office Macros'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Office Macro Documents (Notify)

User Matching Allowed

This blocks messages that contain Office documents having macros included in them. A notification is sent to the recipient.

When a message arrives
And the message is incoming
Where message is categorized as 'Office Document Macros'
Then
Send a 'Office Macro Document (In)' system notification message
Write log message with 'Attachment Type – Office Macros'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.11 Message Content (Inbound)

Rule: Strip read receipts from messages

User Matching Allowed

This rule removes read receipt requests from messages. The message content is otherwise unaffected.

When a message arrives
And the message is incoming
Then

Write log message with 'Strip Read Receipt Headers'
And rewrite message headers using 'Strip Read Receipt Request'

Rule: Monitor Spoofed Messages

User Matching Allowed

This rule monitors inbound messages sent from one of your domains, sourced from unknown IP addresses or unauthenticated users. The rule doesn't block any messages.

When a message arrives
And the message is incoming
Where message spoofing analysis is based on anti-relay
Then
Copy the message to 'Archive (Incoming) - 2 weeks' with release action “continue processing”
And write log message with 'Message - Spoofed Message'

Rule: Block Spoofed Messages

User Matching Allowed

This rule blocks inbound messages sent from one of your domains, sourced from unknown IP addresses or unauthenticated users.

When a message arrives
And the message is incoming
Where message spoofing analysis is based on anti-relay
Then
Write log message with 'Message - Spoofed Message'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Fragmented Messages

User Matching Allowed

Fragmented messages are messages that come in one or more parts, and are re-assembled at the delivery point to read the entire content. Fragmented messages are very rarely used for legitimate purposes today, and can be an indicator that an attacker is attempting to bypass content scanning filters.

When a message arrives
And the message is incoming
Where message contains one or more headers 'Detect Fragmented Messages'
Then
Write log message with 'Message - Fragmented Message'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Encrypted Messages

User Matching Allowed

This rule prevents messages which contain S/MIME or PGP encrypted material from being sent to your organization. Internal employees may receive confidential information in encrypted form, to prevent detection by automated systems.

When a message arrives
And the message is incoming
Where message attachment is of type 'P7M; PGP'
And where message spoofing analysis is based on anti-relay and where Sender ID evaluation fails with Moderate Settings
Then
Write log message with 'Message - Encrypted'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Monitor Spoofed Messages (via SPF check)

User Matching Allowed

This rule monitors messages where the IP address used does not match an entry in the sender's SPF records.

When a message arrives
And the message is incoming
Where message spoofing analysis is based on where Sender ID evaluation fails with Custom Settings
Then
Copy the message to 'Archive (Incoming) - 2 weeks' with release action "continue processing"
And write log message with 'Message - Spoofed Message'

Rule: Monitor Local Domain Spoofed Messages

User Matching Allowed

This rule monitors messages sent from one of your domains, where the IP address used does not match an entry in your SPF records or the IP relay table.

When a message arrives
And the message is incoming
Where message spoofing analysis is based on anti-relay and where Sender ID evaluation fails with Custom Settings
Then
Copy the message to 'Archive (Incoming) - 2 weeks' with release action "continue processing"
And write log message with 'Message - Spoofed Message'

Rule: Block Local Domain Spoofed Messages

User Matching Allowed

This rule blocks messages sent from one of your domains, where the IP address used does not match an entry in your SPF records or the IP relay table.

When a message arrives
And the message is incoming
Where message spoofing analysis is based on anti-relay and where Sender ID evaluation fails with Custom Settings
Then
Write log message with 'Message - Spoofed Message'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.3.12 Dead Letter Handling (Inbound)

Quarantines malformed or otherwise unscannable or undeliverable mails.

No customer configuration is allowed.

2.4 Package: Blended Threats

Note: This package is optional and incurs an additional fee.

2.4.1 Blended Threats Protection (Inbound)

This ruleset allows you to check messages for Blended Threats, which are URL links that lead to malicious content on websites. Blended Threat checking includes two parts: rewriting of URLs by the included rule, and scanning by a cloud service when the URL link is clicked.

Rule: Bypass Rewrite for SMime Signed Messages

User Matching Allowed

This rule skips the Blended Threat URL rewriter when the message contains SMime signed data. Customers who need to maintain the check on signed mail at the internal server can choose to use this rule. CAUTION: URLs in the affected messages will not be scanned for malicious content at time of click. Recipients cannot be notified by a modification to affected messages because that would also prevent later validation of the signature. Set user matching to affect the minimum possible number of messages.

When a message arrives
And the message is incoming
Where message attachment is of type 'P7S'
Then
Pass the message on and skip the next rule

Rule: Blended Threats Scanner

User Matching Allowed

This rule rewrites URLs in the body of incoming email messages, so that the linked page will be submitted to a cloud service for scanning when the email recipient clicks the link.

When a message arrives
And the message is incoming
Then
Rewrite URLs in the message for Blended Threats scanning

2.5 Package: Data Protection

2.5.1 Sensitive Material (Outbound)

This ruleset scans outbound messages for potentially sensitive content, such as credit card numbers, US Social Security numbers or keywords for the financial/medical industry.

Rule: Block Credit Card Numbers – Extensive (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. The message recipient is notified. NOTE: This rule triggers on the presence of any string of numbers that matches the format of a card number. It is likely to cause some false triggers on documents containing many numbers.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Credit Card Number - Plain'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Credit Card Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of word(s) like "credit", "card" or "expiry" in the message. The message sender is notified.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Credit Card Number - Keywords'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Social Security Numbers – Extensive (with Notification)

User Matching Allowed

This rule looks for indications that US Social Security numbers are embedded in an email message or its attachments. The message recipient is notified. NOTE: This rule triggers on the presence of any string of numbers that matches the format of a Social Security Number. It is likely to cause some false triggers on documents containing many numbers. The message sender is notified.

When a message arrives
And the message is outgoing
Where message is categorized as 'SocialSecurity'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Social Security Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Social Security Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that US Social Security numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of related keyword(s) in the message. The message recipient is notified.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Social Security Number - Keywords'
  And where message is categorized as 'SocialSecurity'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Social Security Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Copy Messages with HIPAA Content

User Matching Allowed

This rule archives messages that contain keywords which might fall under the US HIPAA act. The messages should be reviewed by the administrator to verify their content. Sending a digest to the administrator is recommended.

When a message arrives
And the message is outgoing
Where message is categorized as 'HIPAA'
Then
Copy the message to 'Archive (Outgoing)' with release action "continue processing"
  And write log message with 'Policy Breaches - HIPAA Content'

Rule: Copy Messages with SEC Content

User Matching Allowed

This rule archives messages that contain keywords which might be a violation of the US Securities and Exchange Commission's regulations. The messages should be reviewed by the administrator to verify their content. Sending a digest to the administrator is recommended.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Keyword List - SEC'
Then
Copy the message to 'Archive (Outgoing)' with release action "continue processing"
  And write log message with 'Policy Breaches - SEC Content'

Rule: Copy Messages with Sarbanes-Oxley Content

User Matching Allowed

This rule archives messages that contain keywords which might be a violation of the US Sarbanes-Oxley act. The messages should be reviewed by the administrator to verify their content. Sending a digest to the administrator is recommended.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Keyword List - SOX'
Then
Copy the message to 'Archive (Outgoing)' with release action "continue processing"
  And write log message with 'Policy Breaches - SOX Content'

2.5.2 Sensitive Material (Inbound)

This policy scans inbound messages for potentially sensitive content, such as credit card numbers, US Social Security numbers or keywords for the financial/medical industry.

Rule: Block Credit Card Numbers – Extensive (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. The message recipient is notified. NOTE: This rule triggers on the presence of any string of numbers that matches the format of a card number. It is likely to cause some false triggers on documents containing many numbers.

When a message arrives
And the message is incoming
Where message triggers system text censor script(s) 'Credit Card Number - Plain'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk in' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (incoming)' with release action "continue processing"

Rule: Block Credit Card Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of word(s) like "credit", "card" or "expiry" in the message. The message recipient is notified.

When a message arrives
And the message is incoming
Where message triggers system text censor script(s) 'Credit Card Number - Keywords'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk in' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (incoming)' with release action "continue processing"

Rule: Block Social Security Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that US Social Security numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of related keyword(s) in the message. The message recipient is notified.

When a message arrives
And the message is incoming
Where message triggers system text censor script(s) 'Social Security Number - Keywords'
  And where message is categorized as 'SocialSecurity'
Then
Send a 'Policy Risk in' system notification message
  And write log message with 'Policy Breaches - Social Security Numbers'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.6 Package: Acceptable Use

2.6.1 Objectionable Material (Outbound)

This ruleset scans outbound messages for objectionable content, such as offensive language, pornography, or hate speech.

Rule: Block Vulgarity

User Matching Allowed

This rule blocks messages containing common obscenities and vulgarities.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Mild Profanity'
Then
Write log message with 'Policy Breaches - Vulgarity'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Racist and Hate Language

User Matching Allowed

This rule blocks messages containing especially offensive language, such as racist or hate speech.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Racist and Hate'
Then
Write log message with 'Policy Breaches - Racist and Hate Language'
  And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Pornographic Language

User Matching Allowed

This rule blocks messages containing sexually explicit or pornographic language.

When a message arrives
And the message is outgoing

Where message triggers system TextCensor script(s) 'Language - Pornographic'
Then
Write log message with 'Policy Breaches - Pornographic Language'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Pornographic Language (Notify)

User Matching Allowed

This rule blocks messages containing sexually explicit or pornographic language. The sender is notified about the message being blocked.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Pornographic'
Then
Send a ‘Language Out’ system notification message
And write log message with 'Policy Breaches - Pornographic Language'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Chain Letters

User Matching Allowed

This rule blocks messages which have the appearance of an Internet chain letter.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Generic Chain Letters'
Then
Write log message with 'Policy Breaches - Chain Letter'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Virus Hoaxes

User Matching Allowed

This rule blocks messages which have the appearance of a hoax virus warning chain letter.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Generic Virus Hoaxes'
Then
Write log message with 'Policy Breaches - Virus Hoax'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Script and Code

User Matching Allowed

This rule looks for indications that script and code in embedded in an email message, which could potentially be dangerous.

When a message arrives
And the message is outgoing

Where message triggers system TextCensor script(s) 'Script and Code'
Then
Write log message with 'Policy Breaches - Script and Code'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

2.6.2 Objectionable Material (Inbound)

This ruleset scans inbound messages for objectionable content, such as offensive language, pornography, or hate speech.

Rule: Block Vulgarity

User Matching Allowed

This rule blocks messages containing common obscenities and vulgarities.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Language - Mild Profanity'
Then
Write log message with 'Policy Breaches - Vulgarity'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Racist and Hate Language

User Matching Allowed

This rule blocks messages containing especially offensive language, such as racist or hate speech.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Language - Racist and Hate'
Then
Write log message with 'Policy Breaches - Racist and Hate Language'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Pornographic Language

User Matching Allowed

This rule blocks messages containing sexually explicit or pornographic language.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Language - Pornographic'
Then
Write log message with 'Policy Breaches - Pornographic Language'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Chain Letters

User Matching Allowed

This rule blocks messages which have the appearance of an Internet chain letter.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Generic Chain Letters'
Then
Write log message with 'Policy Breaches - Chain Letter'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Virus Hoaxes

User Matching Allowed

This rule blocks messages which have the appearance of a hoax virus warning chain letter.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Generic Virus Hoaxes'
Then
Write log message with 'Policy Breaches - Virus Hoax'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Script and Code

User Matching Allowed

This rule looks for indications that script and code in embedded in an email message, which could potentially be dangerous.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Script and Code'
Then
Write log message with 'Policy Breaches - Script and Code'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

2.7 Package: Advanced Image Analysis

2.7.1 Image Analyzer (Outbound)

Deep Image Analysis

Rule: Image Scanner

User Matching Allowed

This rule scans outbound messages for attached images that are identified as potentially offensive (pornographic) by a deep image analysis module.

When a message arrives
And the message is outgoing
Where the attached image is inappropriate
Then
Write log message with 'Policy Breaches - Inappropriate Image'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

2.7.2 Image Analyzer (Inbound)

Deep Image Analysis

Rule: Image Scanner

User Matching Allowed

This rule scans inbound messages for attached images that are identified as potentially offensive (pornographic) by a deep image analysis module.

When a message arrives
And the message is incoming
Where the attached image is inappropriate
Then
Write log message with 'Policy Breaches - Inappropriate Image'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.8 Package: Trustwave Sandbox Routing

2.8.1 To Trustwave Sandbox (Inbound)

This ruleset identifies messages that should be scanned by the Trustwave Sandbox, and routes them for scanning.

Rule: Send to Trustwave Sandbox

This rule detects incoming messages that have not been sent to the Sandbox Service and routes them to the service. Only messages that have components that can be processed through the Sandbox are accepted for routing. To enable the service (if provisioned), enable this rule. The instance of the Trustwave Sandbox Service used varies by region.

When a message arrives
And the message is incoming
Except where addressed from 'IP Trustwave Sandbox'
Where message is categorized as 'Sandbox Prefilter'
Then
Write log message with 'Sandbox - Sent to Sandbox Service'
And set message routing to *(regional sandbox instance)*
And pass the message on and do not process any additional rules

2.9 Package: Data Retention – 31 days

2.9.1 31 day retention outbound

Rule: Retain messages

User Matching Allowed

Copies outbound messages to a folder with 31 day retention

When a message arrives
And the message is outgoing
Then
Write log message with 'Message – Data Retention'
And copy the message to ‘Data Retention (Outgoing) – 31 days’ with release action “continue processing”

2.9.2 31 day retention inbound

Rule: Retain messages

User Matching Allowed

Copies inbound messages to a folder with 31 day retention

When a message arrives
And the message is incoming
Then
Write log message with 'Message – Data Retention'
And copy the message to ‘Data Retention (Incoming) – 31 days’ with release action “continue processing”

2.10 Package: Data Retention – 90 days

2.10.1 90 day retention outbound

Rule: Retain messages

User Matching Allowed

Copies outbound messages to a folder with 90 day retention

When a message arrives
And the message is outgoing
Then
Write log message with 'Message – Data Retention'
And copy the message to ‘Data Retention (Outgoing) – 90 days’ with release action “continue processing”

2.10.2 90 day retention inbound

Rule: Retain messages

User Matching Allowed

Copies inbound messages to a folder with 90 day retention

When a message arrives
And the message is incoming
Then
Write log message with 'Message – Data Retention'
And copy the message to ‘Data Retention (Incoming) – 90 days’ with release action “continue processing”

2.11 Package: Trustwave Secure Email Encryption

2.11.1 Secure Email Encryption (Outbound)

Rule: Encrypt messages based on user matching

User Matching Allowed

Route messages to the Trustwave Secure Email Encryption service if specified users match. Note: You MUST configure user matching before enabling this rule.

When a message arrives
And the message is outgoing
Then
Write log message with 'Encrypted Message - by Recipient'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages using keyword

User Matching Allowed

Sends the message to the Trustwave Secure Email Encryption service if it matches a keyword specified for encryption.

Note: This rule triggers if any of the following words are found in the message subject (not case sensitive): encrypt, safe, secure, secured. To avoid false triggering, use the more specific rules available below.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – Keyword in subject line'
Then
Write log message with 'Encrypted Message - Keyword'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages with keyword in subject

User Matching Allowed

Sends the message to the Trustwave Secure Email Encryption service if the subject contains any of the keywords [encrypt], [secure], or [confidential]

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – Trustwave Essential Triggers'
Then
Write log message with 'Encrypted Message - Keyword'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages with [encrypt] in subject

User Matching Allowed

Sends the message to the Trustwave Secure Email Encryption service if it matches the keyword [encrypt]

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – [encrypt] in subject line'
Then
Write log message with 'Encrypted Message - Keyword'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages with [secure] in subject

User Matching Allowed

Sends the message to the Trustwave Secure Email Encryption service if it matches the keyword [secure]

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – [secure] in subject line'
Then
Write log message with 'Encrypted Message - Keyword'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages with [confidential] in subject

User Matching Allowed

Sends the message to the Trustwave Secure Email Encryption service if it matches the keyword [confidential]

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – [confidential] in subject line'
Then
Write log message with 'Encrypted Message - Keyword'
And rewrite message headers using 'Add encryption routing header'
And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages containing Credit Card Data

User Matching Allowed

Sends the message to Trustwave Secure Email Encryption service if credit card information is found in the message.

Note: This rule triggers if both the “categorized” and TextCensor conditions trigger.

The “categorized” component checks for well-formed credit card numbers in the subject, body, and top level attachments of a message, using a proprietary method.

The TextCensor component searches the subject, body, and attachments (not case sensitive).

- It triggers immediately if one of the following words or phrases is found: JCB, American Express, Amex, credit card, Diners Club, DiscoverCard, Mastercard, Visa
- It triggers if more than one of the following words is found: card, credit, Diners, Discover, number, No., Num

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Keyword list – Credit Card'
  And where messages is categorized as ‘CreditCard’
Then
Write log message with 'Encrypted Message – Credit Card Number'
  And rewrite message headers using 'Add encryption routing header'
  And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages containing SSN data and keyword

User Matching Allowed

Sends the message to Trustwave Secure Email Encryption service if it matches SSN data and associated keyword information.

Note: This rule triggers if both the “categorized” and TextCensor conditions trigger.

The “categorized” component checks for well-formed US Social Security numbers in the subject, body, and top level attachments of a message, using a proprietary method.

The TextCensor component searches the subject, body, and attachments (not case sensitive).

- It triggers immediately if one of the following words or phrases is found: SSN, Social Security
- It triggers if more than one of the following words is found: Security, Social, number, No., Num

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Keyword list – Social Security'
  And where messages is categorized as 'SocialSecurity'
Then
Write log message with 'Encrypted Message – Social Security Number'
  And rewrite message headers using 'Add encryption routing header'
  And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

Rule: Encrypt Messages containing SSN data

User Matching Allowed

Sends the message to Trustwave Secure Email Encryption if it matches a SSN number. Warning: Since SSN numbers are not unique, this is subject to a high rate of false positives.

Note: This rule triggers on the presence of strings that look like US Social Security Numbers, in the message subject or body.

This rule is subject to false positives (excessive triggering) because Social Security Numbers are not uniquely distinguishable from other groups of nine digits such as telephone numbers.

The TextCensor component searches the subject, body, and attachments (not case sensitive).

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Encryption – Social Security Number Anywhere'
Then
Write log message with 'Encrypted Message – Social Security Number'
  And rewrite message headers using 'Add encryption routing header'
  And set message routing to 'smtp-partner.encryption.twsegcloud.com:25,IPv4'

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave Fusion® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.