Trustwave®

TECHNICAL REFERENCE

Trustwave MailMarshal 11.3.0 Default Rules

Table of Contents

About This Document **2**

1 Connection Policy **3**

1.1 Policy Group: Connection Policies 3

1.2 Policy Group: TLS Connection Properties 5

2 Content Analysis Policy **6**

2.1 Policy Group: Anti-Malware (Inbound) 6

2.2 Policy Group: Anti-Malware (Outbound) 8

2.3 Policy Group: Anti-Spam 8

2.4 Policy Group: Anti-Phishing 12

2.5 Policy Group: Business Email Compromise 12

2.6 Policy Group: DMARC (Disabled) 13

2.7 Policy Group: Blended Threats 14

2.8 Policy Group: Attachment Management (Inbound) 15

2.9 Policy Group: Attachment Management (Outbound) 18

2.10 Policy Group: Policy Management (Inbound) 21

2.11 Policy Group: Policy Management (Outbound) 24

2.12 Policy Group: Automated Responses 27

2.13 Policy Group: Message Archiving 28

3 Dead Letter Policy **30**

3.1 Policy Group: Spam Management 30

About Trustwave **31**

About This Document

This document provides a text listing of the default email processing rules that are installed by default with a new installation of Trustwave MailMarshal (formerly Trustwave SEG), versions 10.2.5 through 11.2.0.

Administrators running older versions of the product, as well as new users, will be able to review the latest recommended policy in a convenient format.

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

Read the notes on each rule for detailed information.

Changes in release 11.3.0:

- **Rule condition negations** are available for many conditions. Wording of some conditions has been updated to reflect the options such as “is/is not” or “was/was not”. There are no changes to default rule processing.

Changes in release 10.2.5:

- **The Connection rule “**Reject non-domain matching TLS client certificates” is disabled by default.

Changes in release 10.1:

- **Move Message actions** now include a “Category” selection used to generate Dashboard data.
- **A rule to ignore DANE validation for specific domains** is added to Policy Management (Outbound). This rule is only effective if DANE (DNS-based Authentication of Named Entities) validation is enabled. DANE is disabled by default in 10.1.0.
- **The Image Analyzer rule condition** is updated to support the availability of multiple image categories. The effect of the default rule is not changed.

1 Connection Policy

1.1 Policy Group: Connection Policies

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

Rule: Deny Junk Mailers in IP Block List
This rule denies any messages from IP addresses listed in the IP Block List IP group. If a match in the group occurs, the message will be denied by the Receiver, prior to being downloaded to the gateway. Keep the rule up to date by adding to the 'IP Block List' group.
Where message is from 'IP Block List'
Refuse message and reply with 550 Rule imposed mailbox access for {Recipient} refused

Rule: Deny Trustwave Reputation Service Blocklisted on connection
This rule denies messages from hosts listed on the Trustwave Email IP Reputation Service Blocklist. If you wish to quarantine email, as opposed to outright deny during the connection, use the associated Content Analysis rule.
Except where message is from 'Global Allow List'
Where sender's IP address is listed by 'Marshal IP Reputation Service'
Refuse message and reply with 550 Rule imposed as {Sender} is listed on Trustwave Email IP Reputation Service - see rbladmin.trustwave.com/?ip={SenderIP}

Rule: Deny Spamhaus Blocklisted Senders during connection (Disabled)
This rule denies messages from hosts listed on a DNS Blocklist, in this case the ZEN blocklist from Spamhaus. (Note: Before enabling, refer to Spamhaus's terms and conditions, see http://www.spamhaus.org/organization/dnsblusage.html). Hosts can be wrongly listed on blocklists so use with care. If you wish to quarantine email, as opposed to outright deny during the connection, use the associated Content Analysis rule.
Except where message is from 'Global Allow List'
Where sender's IP address is listed by 'Spamhaus ZEN'
Refuse message and reply with 550 Rule imposed as {Sender} is listed on Spamhaus -see www.spamhaus.org

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

Rule: Sender Policy Framework check - Log Only (Disabled)
This rule performs a Sender Policy Framework check against the incoming message and connecting server. The Sender Policy Framework result is logged in the message header and performs no further actions.
Where message is incoming
Where the SPF evaluation is set to log only
Continue processing rules

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

Be aware that turning on this rule may also get you blocklisted - for more information see <http://www.rfc-ignorant.org/policy-dsn.php>.
Except where message is to 'Postmaster Addresses'
Or except where message is from '*@*.*'
Refuse message and reply with 550 Message rejected - user unknown.

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

Rule: Deny Messages Over 30MB during connection (Disabled)
This Connection rule will deny any message that enters the gateway, except where addressed either to or from the Information technology user group, and is identified by the foreign ESMTP server as being over 30MB in size. The foreign mail server must be ESMTP compliant for this rule to trigger. While most email systems today are ESMTP compliant, you should also create a Standard Rule (or use the Attachment Management rule called "Block Messages Over 30MB") that stops messages of a similar size from non-ESMTP compliant servers.
Except where addressed either to or from 'Information Technology'
Where the message size is greater than '30720 KB'
Refuse message and reply with 550 Rule imposed mailbox access for {Recipient} refused

9 Rule(s)

1.2 Policy Group: TLS Connection Properties

Rule: Enforce the use of TLS for specific email senders
This rule will reject messages from specific senders when the connection is not secured using TLS.
Where message is from 'TLS-Enforced Senders'
Where message was not received via TLS
Refuse message and reply with 550 The use of TLS is required to send this message

Rule: Enforce TLS client certificate usage for specific senders
This rule will reject messages that are message is from a specific sender in the "TLS Trusted Partners" group, but no client certificate was provided.
Where message is from 'TLS Trusted Partners'
Where the TLS client certificate was not presented
Refuse message and reply with 550 The use of a client certificate is required to send this message

Rule: Reject non-client TLS Certificates
This rule will reject connections when a client certificate was presented and the intended uses do not include client authentication.
Where the TLS client certificate was presented with options: 'Intention not valid'
Refuse message and reply with 550 TLS client certificate is not intended for client authentication

Rule: Reject expired TLS Client Certificates
This rule will reject connections when a client certificate was presented and the current datetime is not within the certificate's validity period. (The certificate is expired or not yet valid.)
Where the TLS client certificate was presented with options: 'Date not valid'
Refuse message and reply with 550 TLS client certificate is expired or not yet valid

Rule: Reject non-domain matching TLS Client Certificates (Disabled)
This rule will reject connections when a client certificate was presented and the sender's domain does not match the certificate's domain. This rule should only be enabled with user matching for specific domains where the certificate is known to match the domain. It will provide an extra layer of protection against spoofed connections from these domains.
Where the TLS client certificate was presented with options: 'Domain does not match'
Refuse message and reply with 550 TLS client certificate subject does not match sender domain

Rule: Reject untrusted TLS Client Certificates
This rule will reject connections when a client certificate was presented and the certificate chain is untrusted.
Where message is from 'TLS Trusted Partners'
Where the TLS client certificate was presented with options: 'Issuer not trusted'
Refuse message and reply with 550 TLS client certificate not trusted

Rule: Reject revoked TLS Client Certificates
This rule will reject connections when a client certificate was presented and the certificate has been revoked.
Where message is from 'TLS Trusted Partners'
Where the TLS client certificate was presented with options: 'Certificate Revoked'
Refuse message and reply with 550 TLS client certificate revoked

7 Rule(s)

2 Content Analysis Policy

2.1 Policy Group: Anti-Malware (Inbound)

Rule: Block Malware – Email Threat Detection
This rule invokes the Email Threats category script, which targets traits of malware-sending bots and suspicious email attachments. The script is updated automatically, with new updates regularly in response to new threats.
Where message is incoming
Where message does trigger category script(s) 'Email Threats'
Move the message to 'Malware - Suspected' and categorize as 'Malware' with release action "continue processing"

Rule: Block Malware - Advanced Malware and Exploit Detection
This rule invokes the Yara Analysis Engine AMAX (Advanced Malware and Exploit detection) script which scans attachments for suspicious code. AMAX uses a combination of heuristic and specific exploit rules to identify possible malware. This script is updated automatically by Trustwave SpiderLabs regularly in response to new threats.
Where message is incoming
Where message is identified as containing malware by Yara Analysis Engine script AMAX
Send a 'AMAX In' notification message
And move the message to 'Malware - AMAX' and categorize as 'Malware' with release action "continue processing"

Rule: Block Malware - Virus Scanner (Disabled)
This rule will invoke all virus scanners that have been installed and defined within the gateway. All messages inbound to the organization will be scanned. If a virus scanner detects a virus the rule will quarantine the message. Note: You must install a supported virus scanner, define the scanner within the configurator and then enable this rule in order to check for viruses.
Where message is incoming
Where the result of a virus scan is 'Contains Virus'
Move the message to 'Malware' and categorize as 'Malware' with release action "continue processing"

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

Rule: Block Windows Shortcut Files
This rule blocks Windows Shortcut files, which are commonly used by malware authors in email attacks. If the rule detects a file of this type it will quarantine the message and notify the local recipient(s).
Where message is incoming
Where message attachment is of type 'LNK' or 'URL'

Send a 'Suspect File in' notification message
And move the message to 'Suspect' and categorize as 'None' with release action "continue processing"

Rule: Block Highly Suspect Filename Extensions
This rule blocks a few highly suspect filename extensions which are commonly used by malware authors in email attacks. If the rule detects a file with a listed extension it will quarantine the message and notify the local recipient(s).
Where message is incoming
Where message does contain attachments named '*.scr' or '*.cpl' or '*.com' or '*.pif'
Send a 'Suspect File in' notification message
And move the message to 'Suspect' and categorize as 'None' with release action "continue processing"

Rule: Block Executable Files embedded in Documents
This rule blocks messages with executable attachments embedded in Documents, which is highly suspicious. This type of rule uses Trustwave's attachment decoder technology to detect executables irrespective of their filenames.
Where message is incoming
Where message attachment is of type 'EXECUTABLE'
And where attachment parent is of type: 'DOCUMENT'
Send a 'Executable in' notification message
And move the message to 'Attachment Type - Executables' and categorize as 'None' with release action "continue processing"

Rule: Block Executable Files
This rule blocks messages with executable attachments, except where message is to users listed in the 'Information Technology' group. This type of rule uses Trustwave's attachment decoder technology to detect executables irrespective of their filenames. While strict, blocking all executables at the email gateway is a good way of preventing many mass and targeted attacks.
Where message is incoming
Except where message is to 'Information Technology'
Where message attachment is of type 'EXECUTABLE'
Send a 'Executable in' notification message
And move the message to 'Attachment Type - Executables' and categorize as 'None' with release action "continue processing"

Rule: Block Malformed PDF Documents (Disabled)
This rule scans messages with the Yara Analysis Engine script named Malformed PDF, which identifies and quarantines malformed and corrupt PDF documents that could have a possibility of being malicious. Note: This is a strict policy that may also block malformed, but otherwise legitimate PDFs.
Where message is incoming
Where message is identified as containing malware by Yara Analysis Engine script Malformed PDF
Send a 'Malformed PDF In' notification message
And move the message to 'Malformed PDF' and categorize as 'None' with release action "continue processing"

Rule: Block Virus Hoaxes (Disabled)
This rule invokes the TextCensor script Generic Virus Hoaxes to search the message for words and phrases associated with typical virus hoax messages. If the rule triggers it will quarantine the message and notify local recipient(s).
Where message is incoming
Where message does trigger text censor script(s) 'Generic Virus Hoaxes'
Send a 'Potential Junk Mail in' notification message
And move the message to 'Junk' and categorize as 'None' with release action "continue processing"

10 Rule(s)

2.2 Policy Group: Anti-Malware (Outbound)

Rule: Block Malware – Email Threat Detection
This rule invokes the Email Threats category script, which targets traits of malware-sending bots and suspicious email attachments. The script is updated automatically, with new updates regularly in response to new threats.
Where message is outgoing
Where message does trigger category script(s) 'Email Threats'
Move the message to 'Malware - Suspected' and categorize as 'Malware' with release action "continue processing"

Rule: Block Malware - Virus Scanner (Disabled)
This rule will invoke all virus scanners that have been installed and defined within the gateway. All messages outbound to the organization will be scanned. If a virus scanner detects a virus the rule will quarantine the message. Note: You must install a supported virus scanner, define the scanner within the configurator and then enable this rule in order to check for viruses.
Where message is outgoing
Where the result of a virus scan is 'Contains Virus'
Move the message to 'Malware' and categorize as 'Malware' with release action "continue processing"

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

Rule: Block Virus Hoaxes (Disabled)
This rule invokes the TextCensor script Generic Virus Hoaxes to search the message for words and phrases associated with typical virus hoax messages. If the rule triggers it will quarantine the message and notify the local sender.
Where message is outgoing
Where message does trigger text censor script(s) 'Generic Virus Hoaxes'
Send a 'Potential Junk Mail out' notification message
And move the message to 'Junk' and categorize as 'None' with release action "continue processing"

4 Rule(s)

2.3 Policy Group: Anti-Spam

Rule: Allow Senders in Global Allow List
This rule allows messages from any sender listed in the Global Allow List to be excluded from the remainder of the 'Anti-Spam' Policy Group. Add trusted or wanted sources of email to this Allow List.
Where message is incoming
Where message is from 'Global Allow List'
Pass the message on to the next policy group

Rule: Allow Senders in IP Allow List
This rule allows messages sent from any IP address listed in the IP Allow List to be excluded from the remainder of the 'Anti-Spam' Policy Group. Add trusted or wanted IP addresses of senders to this Allow List.
Where message is incoming
Where message is from 'IP Allow List'
Pass the message on to the next policy group

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

Rule: Block Senders in Recipient Block List
This rule allows messages from any sender listed in the Recipients 'Block List' to be immediately quarantined to the Spam folder. Users can create their own Block List via the End User Management web console.
Where message is incoming
Where the sender is in the recipient's blocked senders list
Move the message to 'Spam - Confirmed' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - SpamBotCensor AND SpamProfiler
This rule uses both the SpamBotCensor and SpamProfiler to identify spam messages. (Note: In order for the SpamBotCensor to work, the gateway must be at the perimeter receiving email directly from the Internet). As both these anti-spam engines must detect the message as spam, there is a higher degree of confidence that the message is spam, avoiding the need for end user management on the Spam - Confirmed quarantine folder.
Where message is incoming
Where message is detected as spam by SpamBotCensor and SpamProfiler (Spam, Suspected Spam)
Move the message to 'Spam - Confirmed' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - SpamCensor AND SpamProfiler
This rule uses both the SpamCensor and SpamProfiler to identify spam messages. As both these anti-spam engines must detect the message as spam, there is a higher degree of confidence that the message is spam, avoiding the need for end user management on the Spam - Confirmed quarantine folder.
Where message is incoming
Where message is detected as spam by SpamCensor and SpamProfiler (Spam, Suspected Spam)
Move the message to 'Spam - Confirmed' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - SpamProfiler
This rule uses the SpamProfiler to identify spam messages based on advanced spam 'fingerprint' signatures that are continuously updated by Trustwave SpiderLabs.
Where message is incoming
Where message is detected as spam by SpamProfiler (Spam, Suspected Spam)
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - SpamBotCensor
This rule identifies spam with the SpamBotCensor, which analyzes SMTP transactions looking for spambot traits (Note: In order for this to work, the gateway must be at the perimeter receiving email directly from the Internet). Messages that trigger are quarantined to the 'Spam - Suspected' folder. The SpamBotCensor filter is a special type of Category Script that is automatically updated by Trustwave SpiderLabs.
Where message is incoming
Where message is detected as spam by SpamBotCensor
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - SpamCensor
This rule uses the SpamCensor to identify spam messages based on a scoring system. Messages that exceed 60 points are quarantined to the 'Spam - Suspected' folder. The SpamCensor filter is a special type of Category Script that is automatically updated by Trustwave SpiderLabs.
Where message is incoming
Where message is detected as spam by SpamCensor
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - Marshal RBL Blocklisted (Disabled)
This rule uses the category script 'Marshal Blocklisted' to perform a query of the IP addresses found in the message header against the Marshal RBL Blocklist. By default only the first IP address found in the header is checked.
Where message is incoming
Where message does trigger category script(s) 'Marshal RBL Blocklisted'
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - Spamhaus Blocklisted (Disabled)
This rule uses the category script 'Spamhaus Blocklisted' to perform a query of the IP addresses in the message header against the Spamhaus ZEN blocklist. (Note: Before enabling, refer to Spamhaus's terms and conditions, see http://www.spamhaus.org/organization/dnsblusage.html). The complete ZEN blocklist, including the PBL, is used to validate the connecting server only. Other IP addresses found in the header are validated against the SBL and XBL databases (see www.spamhaus.org/zen). If the query returns positive, the message will be quarantined to the Spam folder.
Where message is incoming
Where message does trigger category script(s) 'Spamhaus Blocklisted'
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - URLCensor (by domain) (Disabled)
This rule invokes the URLCensor to parse the message in order to extract URLs and Web links. The gateway then takes the top-level domains found in those links and performs a query against a URL Blocklist - by default it uses the URIBL blocklist (see www.uribl.com for terms and conditions of use). If the query returns positive, the message will be quarantined to the Spam folder.
Where message is incoming
Where message does trigger category script(s) 'URLCensor Blocklisted'
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Spam - Administrator Maintained Keyword list
This rule uses a locally maintained TextCensor script to identify specific problematic spam and keywords and quarantine them to the 'Spam' folder. To use, simply add a unique identifying phrase to the TextCensor script to block incidents of the same message.
Where message is incoming
Where message does trigger text censor script(s) 'Spam - Administrator maintained keyword list'
Move the message to 'Spam - Suspected' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Scams
Uses a TextCensor script to identify words and phrases associated with 419, Lottery and other scams.
Where message is incoming
Where message does trigger text censor script(s) 'Scams'
Move the message to 'Spam - Scams' and categorize as 'Spam' with release action "continue processing"

Rule: Sender Policy Framework check (Disabled)
This rule performs a Sender Policy Framework check against the first Received: header line in the message. The behavior of the Sender Policy Framework check can be modified by changing settings in the SPF.xml file. Please refer to the documentation and the SPF.xml file for more information on how to customize the Sender Policy Framework check.
Where message is incoming
Where message does trigger category script(s) 'Sender Policy Framework'
Move the message to 'Junk' and categorize as 'Spam' with release action skip to next policy group

Rule: Block Specific Character Sets (Disabled)
This rule will block messages which declare the usage of specific character sets in the message header. By default it targets a selection of character sets, including those often used in Russia, China and Korea.
Where message is incoming
Where message does trigger text censor script(s) 'Suspect Character Sets'
Move the message to 'Junk' and categorize as 'None' with release action skip to next policy group

Rule: Modify Subject Line of Spam (Disabled)
Do not use this rule if you already use the SpamCensor to block email. this rule should only be enabled after disabling the regular SpamCensor rule. The rule uses the SpamCensor to identify spam messages and modifies them by appending "[SPAM]" to the subject line. This allows end users to set email client rules to move any message that contains the phrase [SPAM] in the subject line to another folder for later viewing or discarding.
Where message is incoming
Where message is detected as spam by SpamCensor
Rewrite message headers using 'Rename Spam Subject'
And continue processing.

Rule: Block failed DKIM Verification (Disabled)
This rule identifies messages that were signed using the DomainKeys Identified Mail specification but failed to pass signature verification. DKIM permits verification of the signer of a message, as well as the integrity of its content. To enforce DKIM checking for specific domains or senders, add them to the "DKIM-Enforced Senders" user group and enable this rule.
Where message is incoming
Where message is from 'DKIM-Enforced Senders'
Where the DKIM verification result is fail
Move the message to 'DKIM Failures' and categorize as 'Spam' with release action skip to next policy group

Rule: Block SenderID Failures (Disabled)
This rule checks the From: domain against the relevant SenderID records for that domain, and quarantines the message if it fails. To enforce SenderID checking for specific domains or senders, add them to the "SenderID-Enforced Senders" user group and enable this rule. (Note: In order for this to work, the gateway must be at the perimeter receiving email directly from the Internet).

Where message is incoming
Where message is from 'SenderID-Enforced Senders'
Where message does appear to be spoofed based on where Sender ID evaluation fails with Strict Settings
Move the message to 'SenderID Failures' and categorize as 'Spam' with release action 'continue processing'

19 Rule(s)

2.4 Policy Group: Anti-Phishing

Rule: Block Phishing - PhishFilter
This will block messages categorized as phishing. The PhishFilter is a heuristic filter that is aimed specifically at phishing. It looks at many structural and content traits of an email, and incorporates URLDeep, a phishing URL Classifier.
Where message is incoming
Where message does trigger category script(s) Phishing
Move the message to 'Phishing' and categorize as 'Phishing' with release action 'continue processing'

Rule: Warn Phishing – PhishFilter (Disabled)
This will stamp messages categorized as phishing with a warning. The PhishFilter is a heuristic filter that is aimed specifically at phishing. It looks at many structural and content traits of an email, and incorporates URLDeep, a phishing URL Classifier.
Where message is incoming
Where message does trigger category script(s) Phishing
Stamp message with Warn Phishing
And continue processing.

2 Rule(s)

2.5 Policy Group: Business Email Compromise

Rule: Block – BEC Fraud Filter
This rule checks messages for multiple traits associated with 'Email Compromise' or 'CEO' fraud, such as names or email addresses of company executives, intentionally misspelled domain names, and other suspicious traits. The BEC Fraud script is updated automatically by Trustwave as required to enhance performance.
Where message is incoming
Where message does trigger category script(s) 'BEC Fraud v8'
Send a 'Potential Fraud' notification message
And move the message to 'BEC – Fraud Filter' and categorize as 'Phishing' with release action "skip to the next policy group"

Rule: Block – Spoofed Messages
This rule will attempt to detect messages that are spoofed by ensuring that a sender domain matching a local domain does in fact originate from an IP address in the local domains table. Messages that appear to be spoofed will be quarantined and a notification sent to the intended recipient. The TextCensor script is used to allow spoofing exclusions based on text found in the message header for any third party services that may use your domains.
Where message is incoming
Where message does trigger text censor script(s) 'Spoofing Exclusions'
And where message does appear to be spoofed based on anti-relay
Send a 'Spoofed Message In' notification message
And move the message to 'Spoofed' and categorize as 'Spam' with release action skip to next policy group

Rule: Block – Executive Name Match (Disabled)
Blocks inbound messages where the From: line contains a name listed in the Executive Name settings.
Where message is incoming
Where message does trigger category script(s) 'Executive Name'
Send a 'Potential Fraud' notification message
And move the message to 'BEC – Executive name' and categorize as 'Phishing' with release action skip to next policy group

Rule: Block – Domain Similarity Match (Disabled)
This rule uses the Domain Similarity category script and blocks inbound messages where the From: domain is similar to a local domain.
Where message is incoming
Where message does trigger category script(s) 'Domain Similarity'
Send a 'Potential Fraud' notification message
And move the message to 'BEC – Domain Similarity' and categorize as 'Phishing' with release action skip to next policy group

Rule: Warn – From Reply-To Mismatch (Disabled)
This rule checks for Reply-To domain that is different to the From domain and stamps the message with a warning.
Where message is incoming
Where message does trigger category script(s) 'From ReplyTo Mismatch'
Stamp message with From Reply-To Mismatch
And continue processing.

Rule: Warn – External Email (Disabled)
This rule stamps all messages from an external source with a warning for users to be wary of clicking links and opening attachments.
Where message is incoming
Stamp message with External Email
And continue processing.

Rule: Warn – Modify Subject with External (Disabled)
This rule prepends [EXTERNAL] to the subject line for all messages from an external source.
Where message is incoming
Prepend [External] to message subject
And continue processing.

7 Rule(s)

2.6 Policy Group: DMARC (Disabled)

Rule: Apply DMARC Quarantine policy
This rule identifies messages that failed to pass DMARC verification, where the DMARC policy for message disposition is "quarantine". DMARC allows a domain owner to define a policy to authenticate mail sent “from” their domain based on SPF and DKIM. The DMARC policy specifies a disposition for messages that do not meet the policy, or have been modified during transport.
Where message is incoming
Where message was checked with DMARC and a result of quarantine applied
Move the message to 'DMARC Failures - Quarantine policy' and categorize as 'Spam' with release action "continue processing"

Rule: Apply DMARC Reject policy
This rule identifies messages that failed to pass DMARC verification, where the DMARC policy for message disposition is "reject". DMARC allows a domain owner to define a policy to authenticate mail sent “from” their domain based on SPF and DKIM. The DMARC policy specifies a disposition for messages that do not meet the policy, or have been modified during transport.

Where message is incoming
Where message was checked with DMARC and a result of reject applied
Move the message to 'DMARC Failures - Reject policy' and categorize as 'Spam' with release action "continue processing"

Rule: Detect incoming DMARC Reports
This rule attempts to identify messages with attached incoming DMARC reports for the local domains, and move them into the DMARC Reports quarantine folder for later processing.
Where message is incoming
Where message is incoming
Where message attachment is of type 'GZ' or 'ZIP' or 'TEXT'
And where message does contain attachments named '*!*!*!*.xml' or '*!*!*!*!*.xml' or '*!*!*!*.xml.gz' or '*!*!*!*!*.xml.gz' or '*!*!*!*.xml.zip' or '*!*!*!*!*.xml.zip'
And where message does contain one or more headers 'DMARC Report Subject'
And where message was checked with DMARC and a result of pass applied
Move the message to 'DMARC Reports' and categorize as 'None' with release action "continue processing"

3 Rule(s)

2.7 Policy Group: Blended Threats

Rule: Block Suspect URLs
This rule will scan a message for URLs and query a web service to determine if any of them is suspect. All messages inbound to the organization will be scanned. If a suspect URL is detected the rule will quarantine the message and notify the local recipient(s). Note: You must have valid maintenance to perform the check for suspect URLs. It is recommended that this rule is executed after the message is checked by a Spam engine, and before any rule that rewrites URLs for Blended Threat Scanning.
Where message is incoming
Where message does contain suspect URLs
Send a 'Suspect URLs' notification message
And move the message to 'Suspect URLs' and categorize as 'Phishing' with release action "continue processing"

Rule: Rewrite URLs for Blended Threat Scanning (Disabled)
This rule allows you to check messages for Blended Threats, which are URL links that lead to malicious content on websites. The rule action rewrites URLs in the body of incoming email messages, so that the linked page will be submitted for scanning when the email recipient clicks the link. To enable this rule you must have a valid license for Blended Threat scanning.
Where message is incoming
Rewrite URLs in the message for Blended Threat Scanning
And continue processing.

2 Rule(s)

2.8 Policy Group: Attachment Management (Inbound)

Rule: Block Suspect Attachments
This rule will block any attachment by matching the filename extension with a list of file types that could potentially contain suspect or malicious content. If the rule detects a file with a listed extension it will quarantine the message and notify the local recipient(s).
Where message is incoming
Where message does contain attachments named '*.bat' or '*.chm' or '*.cmd' or '*.hlp' or '*.hta' or '*.inf' or '*.ins' or '*.js' or '*.jse' or '*.lnk' or '*.reg' or '*.sct' or '*.shs' or '*.url' or '*.vb' or '*.vbe' or '*.vbe' or '*.vbs' or '*.wsc' or '*.wsf' or '*.wsh' or '*.nws' or '*.{*}'
Send a 'Suspect File in' notification message
And move the message to 'Suspect' and categorize as 'None' with release action "continue processing"

Rule: Block Password Protected Attachments
This rule will block any message containing password-protected attachments. This is important, as this type of data cannot be virus checked or content managed at the gateway. If the rule detects password protected attachments it will quarantine the message and notify the local recipient(s).
Where message is incoming
Where message attachment is of type 'SEAEncrypt' or 'ARJsfxcrypt' or 'RARsfxcrypt' or 'ZIPsfxcrypt' or 'DOCcrypt' or 'PDFcrypt' or 'SITEncrypt' or 'ARJcrypt' or 'RARcrypt' or 'ZIPcrypt'
Send a 'Password Protected in' notification message
And move the message to 'Attachment Type - Encrypted' and categorize as 'None' with release action "continue processing"

Rule: Block Unknown Attachments (Disabled)
This rule will block any message containing attachments that are unrecognizable by the gateway. This is important, as some users will try to modify attachments to make them unrecognizable to the gateway in order to allow data into the organization. If the rule detects unrecognizable attachments it will quarantine the message and notify the Administrator and local recipient(s).
Where message is incoming
Where message attachment is of type 'BIN'
And where attachment parent is not of type: 'DOC' or 'Word2' or 'DOC6' or 'DOCIRM' or 'DOCX' or 'MCW' or 'DOCcrypt' or 'XLS' or 'XLSX' or 'XLSB' or 'PPT' or 'PPS' or 'PPTX' or 'PPSX' or 'PDF'
Send a 'Administrator Generic (With message attached)' and a 'Unrecognized Attachment in' notification message
And move the message to 'Attachment Type - Unknown' and categorize as 'None' with release action "continue processing"

Rule: Block Double Extension Filenames (Disabled)
This rule will block any attachment with a double extension filename. This is a common method to disguise malicious email attachments. Because Windows hides the extra extension, the real nature of these files is able to remain hidden until the file is executed. Many viruses and worms generate email attachments with double executable extensions to disguise themselves as legitimate files. NOTE: Users often name their documents with double (or more) extensions, so you may want to change this rule to "copy" to a file for a test period prior to implementing.
Where message is incoming
Where message does contain attachments named '*.??.??' or '*.??.???' or '*.??.????' or '*.???.??' or '*.???.???' or '*.???.????'
Send a 'Suspect File in' notification message
And move the message to 'Suspect' and categorize as 'None' with release action "continue processing"

Rule: Block Suspected Pornographic Images (Disabled)
This rule utilizes the Image Analyzer module to scan attached images for suspected pornographic content. Image Analyzer must be licensed for this rule to work correctly.
Where message is incoming
Where the attached image matches the category 'pornography'
Send a 'Suspect Image In' notification message
And move the message to 'Suspect Images' and categorize as 'None' with release action "continue processing"

Rule: Block EXECUTABLE Files (unless zipped) (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where the executable files are actually archived within a zip file or similar.
Where message is incoming
Where message attachment is of type 'EXECUTABLE'
And where attachment parent is not of type: 'ARCHIVE'
Send a 'Executable in' notification message
And move the message to 'Attachment Type - Executables' and categorize as 'None' with release action "continue processing"

Rule: Block SMIME and PGP Encrypted (Disabled)
This rule will block any message containing PGP or S/MIME encrypted data. This is important, as this type of data cannot be virus checked or content managed at the gateway (unless you have MailMarshal Secure email server installed). If the rule detects PGP or S/MIME data it will quarantine the message and notify the local recipient(s).
Where message is incoming
Where message attachment is of type 'P7M' or 'PGP'
Send a 'Encrypted in' notification message
And move the message to 'Attachment Type - Encrypted' and categorize as 'None' with release action "continue processing"

Rule: Block VIDEO Files (Disabled)
This rule blocks messages with VIDEO attachments, except where message is to users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses Trustwave's attachment decoder technology, which detects video files irrespective of what they are called.
Where message is incoming
Except where message is to 'Information Technology' or 'Marketing'
Where message attachment is of type 'VIDEO'
Send a 'Multimedia in' notification message
And move the message to 'Attachment Type - Video and Sound' and categorize as 'None' with release action "continue processing"

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

And where message attachment size is greater than '15 KB'
Send a 'Multimedia in' notification message
And move the message to 'Attachment Type - Images' and categorize as 'None' with release action "continue processing"

Rule: Block SOUND Files (Disabled)
This rule blocks messages with SOUND attachments, except where message is to users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses Trustwave's attachment decoder technology, which detects sound files irrespective of what they are called.
Where message is incoming
Except where message is to 'Information Technology' or 'Marketing'
Where message attachment is of type 'SOUND'
Send a 'Multimedia in' notification message
And move the message to 'Attachment Type - Video and Sound' and categorize as 'None' with release action "continue processing"

Rule: Block IMAGES (unless fingerprint is known) (Disabled)
This rule blocks messages with IMAGE attachments, except where the fingerprint for that image is known to the gateway. This can be a useful way to allow company logos to be excluded from an image-blocking rule.
Where message is incoming
Where message attachment is of type 'IMAGE'
And where attachment fingerprint is not known
Send a 'Multimedia in' notification message
And move the message to 'Attachment Type - Images' and categorize as 'None' with release action "continue processing"

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

Rule: Block more than 10 Attachments (Disabled)
This rule blocks any message where the number of attachments is greater than 10. This rule does not count files contained within an archive such as a Zip file. A high number of attachments may be a signal that the message is non-business related.
Where message is incoming
Where number of attachments is greater than '10'
Send a 'Generic in' notification message
And move the message to 'Junk' and categorize as 'None' with release action "continue processing"

Rule: Block Messages Over 30MB (Disabled)
This is a Standard rule to quarantine messages, except where message is to the 'Information Technology' user group, that are over 30MB in size. This rule is used in conjunction with the 30MB Connection rule to block messages from non-ESMTP mail servers. Please note that this rule uses Message size, not attachment size. For example, at 28MB attachment would typically push the Message size well above 30MB. This is normal and expected behavior for MIME encoding.
Where message is incoming
Except where message is to 'Information Technology'
Where message size is greater than '30720 KB'
Send a 'Generic in' notification message
And move the message to 'Oversize' and categorize as 'None' with release action "continue processing"

14 Rule(s)

2.9 Policy Group: Attachment Management (Outbound)

Rule: Block Password Protected Attachments
This rule will block any message containing password-protected attachments. This is important, as this type of data cannot be virus checked or content managed at the gateway. If the rule detects password protected attachments it will quarantine the message and notify the local sender.
Where message is outgoing
Where message attachment is of type 'SEAEncrypt' or 'ARJsfxcrypt' or 'RARsfxcrypt' or 'ZIPsfxcrypt' or 'DOCcrypt' or 'PDFcrypt' or 'SITEncrypt' or 'ARJcrypt' or 'RARcrypt' or 'ZIPcrypt'
Send a 'Password Protected out' notification message
And move the message to 'Attachment Type - Encrypted' and categorize as 'None' with release action "continue processing"

Rule: Block Unknown Attachments (Disabled)
This rule will block any message containing attachments that are unrecognizable by the gateway. This is important, as some users will try to modify attachments to make them unrecognizable to the gateway in order to allow data into the organization. If the rule detects unrecognizable attachments it will quarantine the message and notify the Administrator and local sender.
Where message is outgoing
Where message attachment is of type 'BIN'
And where attachment parent is not of type: 'DOC' or 'Word2' or 'DOC6' or 'DOCIRM' or 'DOCX' or 'MCW' or 'DOCcrypt' or 'XLS' or 'XLSX' or 'XLSB' or 'PPT' or 'PPS' or 'PPTX' or 'PPSX' or 'PDF'
Send a 'Administrator Generic (With message attached)' and a 'Unrecognized Attachment out' notification message
And move the message to 'Attachment Type - Unknown' and categorize as 'None' with release action "continue processing"

Rule: Block Suspected Pornographic Images (Disabled)
This rule utilizes the Image Analyzer module to scan attached images for suspected pornographic content. Image Analyzer must be licensed for this rule to work correctly.
Where message is outgoing
Where the attached image matches the category ‘pornography’
Send a 'Suspect Image Out' notification message

And move the message to 'Suspect Images' and categorize as 'None' with release action "continue processing"

Rule: Block EXECUTABLE Files (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where message is from users listed in the 'Information Technology' group. This type of rule uses Trustwave's attachment decoder technology to detect executables irrespective of what they are called.
Where message is outgoing
Except where message is from 'Information Technology'
Where message attachment is of type 'EXECUTABLE'
Send a 'Executable out' notification message
And move the message to 'Attachment Type - Executables' and categorize as 'None' with release action "continue processing"

Rule: Block EXECUTABLE Files (unless zipped) (Disabled)
This rule blocks messages with EXECUTABLE attachments, except where the executable files are actually archived within a zip file or similar.
Where message is outgoing
Where message attachment is of type 'EXECUTABLE'
And where attachment parent is not of type: 'ARCHIVE'
Send a 'Executable out' notification message
And move the message to 'Attachment Type - Executables' and categorize as 'None' with release action "continue processing"

Rule: Block SMIME and PGP Encrypted (Disabled)
This rule will block any message containing PGP or S/MIME encrypted data. This is important, as this type of data cannot be virus checked or content managed at the gateway (unless you have MailMarshal Secure email server installed). If the rule detects PGP or S/MIME data it will quarantine the message and notify the local sender.
Where message is outgoing
Where message attachment is of type 'P7M' or 'PGP'
Send a 'Encrypted out' notification message
And move the message to 'Attachment Type - Encrypted' and categorize as 'None' with release action "continue processing"

Rule: Block VIDEO Files (Disabled)
This rule blocks messages with VIDEO attachments, except where message is from users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses Trustwave's attachment decoder technology, which detects video files irrespective of what they are called.
Where message is outgoing
Except where message is from 'Information Technology' or 'Marketing'
Where message attachment is of type 'VIDEO'
Send a 'Multimedia out' notification message
And move the message to 'Attachment Type - Video and Sound' and categorize as 'None' with release action "continue processing"

Rule: Block IMAGE Files (Disabled)
This rule blocks messages with IMAGE attachments, except where message is from users listed in the 'Executive Team', 'Sales', 'Information Technology' and 'Marketing' groups. The rule also has a size condition, so that any images under 15KB are excluded - images this small are typically business-related

logos. The rule uses Trustwave's attachment decoder technology, which detects image files irrespective of what they are called.
Where message is outgoing
Except where message is from 'Information Technology' or 'Marketing' or 'Sales' or 'Executive Team'
Where message attachment is of type 'IMAGE'
And where message attachment size is greater than '15 KB'
Send a 'Multimedia out' notification message
And move the message to 'Attachment Type - Images' and categorize as 'None' with release action "continue processing"

Rule: Block SOUND Files (Disabled)
This rule blocks messages with SOUND attachments, except where message is from users listed in the 'Information Technology' and 'Marketing' groups. This type of rule uses Trustwave's attachment decoder technology, which detects sound files irrespective of what they are called.
Where message is outgoing
Except where message is from 'Information Technology' or 'Marketing'
Where message attachment is of type 'SOUND'
Send a 'Multimedia out' notification message
And move the message to 'Attachment Type - Video and Sound' and categorize as 'None' with release action "continue processing"

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

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

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

Rule: Block Messages Over 30MB (Disabled)
This is a Standard rule to quarantine messages, except where message is from the 'Information Technology' user group, that are over 30MB in size. This rule is used in conjunction with the 30MB Connection rule to block messages from non-ESMTP mail servers. Please note that this rule uses Message size, not attachment size. For example, at 28MB attachment would typically push the Message size well above 30MB. This is normal and expected behavior for MIME encoding.
Where message is outgoing
Except where message is from 'Information Technology'
Where message size is greater than '30720 KB'
Send a 'Generic out' notification message
And move the message to 'Oversize' and categorize as 'None' with release action "continue processing"

12 Rule(s)

2.10 Policy Group: Policy Management (Inbound)

Rule: Block Pornographic Language
This rule invokes a TextCensor script to search the message for pornographic and sexually explicit words and phrases. It does not specifically target Spam messages, rather it searches for any sexually explicit content. This rule uses the "Language - Pornographic" TextCensor script but you can create your own, or use our scripts as a template.
Where message is incoming
Where message does trigger text censor script(s) 'Language - Pornographic'
Send a 'Language in' notification message
And move the message to 'Language' and categorize as 'None' with release action "continue processing"

Rule: Block Common & Mild Profanity (Disabled)
This rule invokes a TextCensor script to search the message for common profanities and mildly abusive words and phrases. This rule uses the "Language - Mild Profanity" TextCensor script but you can create your own, or use our scripts as a template.
Where message is incoming
Where message does trigger text censor script(s) 'Language - Mild Profanity'
Send a 'Language in' notification message
And move the message to 'Language' and categorize as 'None' with release action "continue processing"

Rule: Block Chain Letters (Disabled)
This rule invokes the TextCensor script 'Generic Chain Letters' to search the message for words and phrases associated with typical Chain Letters.
Where message is incoming
Where message does trigger text censor script(s) 'Generic Chain Letters'
Send a 'Potential Junk Mail in' notification message
And move the message to 'Junk' and categorize as 'None' with release action "continue processing"

Rule: Social Security Number detection (Disabled)
This rule searches the message body for numbers in the format of a US Social Security Number. To trigger, the rule also requires the presence of word(s) like "social", "ssn" or "soc num" in the subject or body.
Where message is incoming

Where message does trigger text censor script(s) 'Social Security Number'
Send a 'Policy Risk in' notification message
And move the message to 'Policy Breaches' and categorize as 'None' with release action "continue processing"

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

Rule: HIPAA Compliance Rule (Disabled)
This rule checks for health and medical-related keywords along with other parameters which would indicate possible HIPAA compliance issues. This rule archives all messages with such content for one year. If you enable this rule please review the retention time on the folder, as you may need longer than one year. Also, consider the storage requirements that arise as a result of archiving large volumes of email for long periods. The original message is allowed through to the intended recipient.
Where message is incoming
Where message does trigger text censor script(s) 'Social Security Number'
And where message does trigger category script(s) 'HIPAA'
Copy the message to 'Policy Breaches - HIPAA' with release action "continue processing"
And continue processing.

Rule: Credit Card Number detection (Disabled)
This rule searches the message body for numbers in the format of a Credit Card number. To trigger, the rule typically requires the presence of word(s) like "credit", "card" or "expiry" in the subject or body.
Where message is incoming
Where message does trigger text censor script(s) 'Credit Card Number'
Send a 'Policy Risk in' notification message
And move the message to 'Policy Breaches' and categorize as 'None' with release action "continue processing"

Rule: PCI Data Security Standard detection (Disabled)
This rule searches the message subject, body, and attachments for numbers in the format of a Credit Card number. To trigger, the rule also requires the presence of related keywords like "creditcard", "cvv", and names of well-known credit card issuers.
Where message is incoming
Where message does trigger text censor script(s) 'Payment Card Industry Data Security Standard'
Send a 'Policy Risk in' notification message
And move the message to 'Policy Breaches' and categorize as 'None' with release action "continue processing"

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

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

Rule: Weapons related content (Disabled)
This rule monitors email for weapons-related content. If the TextCensor script triggers then a copy of the message is held for review, and the original message is allowed through to the original recipient.
Where message is incoming
Where message does trigger text censor script(s) 'Weapons related content'
Copy the message to 'Policy Breaches' with release action "continue processing"
And continue processing.

Rule: Delete Read Receipts & Return Receipts (Disabled)
This rule removes common Read Receipt and Return Receipt fields from the message header.
Where message is incoming
Rewrite message headers using 'Delete Read Receipt fields'
And continue processing.

Rule: Block if 'Subject:' Field Missing or Blank (Disabled)
This rule will block any message that arrives with a missing or blank 'Subject:' field. It is not configured to send any notifications.
Where message is incoming
Where message does trigger category script(s) 'Blank Subject'
Move the message to 'Junk' and categorize as 'None' with release action "continue processing"

Rule: Block greater than 50 Recipients (Disabled)
This rule blocks any message where the number of recipients is greater than 50. A high number of recipients may be a signal that the message is non-business related.
Where message is incoming
Where number of recipients is greater than '50'
Send a 'Administrator Generic (With message attached)' notification message
And move the message to 'Junk' and categorize as 'None' with release action "continue processing"

14 Rule(s)

2.11 Policy Group: Policy Management (Outbound)

Rule: Block Pornographic Language
This rule invokes a TextCensor script to search the message for pornographic and sexually explicit words and phrases. It does not specifically target Spam messages, rather it searches for any sexually explicit content. This rule uses the "Language - Pornographic" TextCensor script but you can create your own, or use our scripts as a template.
Where message is outgoing
Where message does trigger text censor script(s) 'Language - Pornographic'
Send a 'Language out' notification message
And move the message to 'Language' and categorize as 'None' with release action "continue processing"

Rule: Block Common & Mild Profanity (Disabled)
This rule invokes a TextCensor script to search the message for common profanities and mildly abusive words and phrases. This rule uses the "Language - Mild Profanity" TextCensor script but you can create your own, or use our scripts as a template.
Where message is outgoing
Where message does trigger text censor script(s) 'Language - Mild Profanity'
Send a 'Language out' notification message
And move the message to 'Language' and categorize as 'None' with release action "continue processing"

Rule: Social Security Number detection (Disabled)
This rule searches the message body for numbers in the format of a US Social Security Number. To trigger, the rule also requires the presence of word(s) like "social", "ssn" or "soc num" in the subject or body.
Where message is outgoing
Where message does trigger text censor script(s) 'Social Security Number'
Send a 'Policy Risk out' notification message
And move the message to 'Policy Breaches' and categorize as 'None' with release action "continue processing"

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

Rule: HIPAA Compliance Rule (Disabled)
This rule checks for health and medical-related keywords along with other parameters which would indicate possible HIPAA compliance issues. This rule archives all messages with such content for one year. If you enable this rule please review the retention time on the folder, as you may need longer than one year. Also, consider the storage requirements that arise as a result of archiving large volumes of email for long periods. The original message is allowed through to the intended recipient.
Where message is outgoing
Where message does trigger text censor script(s) 'Social Security Number'

And where message does trigger category script(s) 'HIPAA'
Copy the message to 'Policy Breaches - HIPAA' with release action "continue processing"
And continue processing.

Rule: Credit Card Number detection (Disabled)
This rule searches the message body for numbers in the format of a Credit Card number. To trigger, the rule typically requires the presence of word(s) like "credit", "card" or "expiry" in the subject or body.
Where message is outgoing
Where message does trigger text censor script(s) 'Credit Card Number'
Send a 'Policy Risk out' notification message
And move the message to 'Policy Breaches' and categorize as 'None' with release action "continue processing"

Rule: PCI Data Security Standard detection (Disabled)
This rule searches the message subject, body, and attachments for numbers in the format of a Credit Card number. To trigger, the rule also requires the presence of related keywords like "creditcard", "cvv", and names of well-known credit card issuers.
Where message is outgoing
Where message does trigger text censor script(s) 'Payment Card Industry Data Security Standard'
Send a 'Policy Risk out' notification message
And move the message to 'Policy Breaches' and categorize as 'None' with release action "continue processing"

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

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

Rule: Racist and Hate content (Disabled)
This rule monitors email for racist and hate content. If the TextCensor script triggers then a copy of the message is held for review, and the original message is allowed through to the original recipient.
Where message is outgoing
Where message does trigger text censor script(s) 'Language - Racist and Hate'
Copy the message to 'Policy Breaches' with release action "continue processing"
And continue processing.

Rule: Weapons related content (Disabled)
This rule monitors email for weapons-related content. If the TextCensor script triggers then a copy of the message is held for review, and the original message is allowed through to the original recipient.
Where message is outgoing
Where message does trigger text censor script(s) 'Weapons related content'
Copy the message to 'Policy Breaches' with release action "continue processing"
And continue processing.

Rule: Remove sensitive header information (Disabled)
This rule removes selected header fields which may give away too much information about internal mail systems. Fields like X-MimeOLE can contain information about the type and version of mail server used internally. Even the Received lines which are added locally can reveal too much information about internal systems. This rule should only be applied to messages which are leaving your company, and are bound for the internet.
Where message is outgoing
Rewrite message headers using 'Remove selected Header fields'
And continue processing.

Rule: Delete Read Receipts & Return Receipts (Disabled)
This rule removes common Read Receipt and Return Receipt fields from the message header.
Where message is outgoing
Rewrite message headers using 'Delete Read Receipt fields'
And continue processing.

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

Rule: Ignore DANE Validation
This rule skips DANE validation for messages message is to the domains specified in the DANE Excluded Domains group. This rule is only relevant when processing of DANE (DNS-based Authentication of Named Entities) is enabled.
Where message is outgoing
Where message is to DANE Excluded Domains
Ignore DANE Validation
And continue processing.

Rule: Apply DKIM signature (Disabled)
This rule applies a digital signature to a message according to the DomainKeys Identified Mail specification. For the signature to be applied the local domain of the sender must have a DKIM private key associated with it, and the public key must be published in a DNS record. The signature can be validated by the recipient.
Where message is outgoing
Apply DKIM signature; if signing fails pass through and send a 'DKIM Signing Failure' notification message
And continue processing.

16 Rule(s)

2.12 Policy Group: Automated Responses

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

Rule: Auto Allow List - Harvest Outbound Recipients (Disabled)
This rule will automatically harvest all outbound external recipient email addresses for the purposes of excluding these recipients from spam filtering. The assumption is that any external recipients to whom you send email will be legitimate. Even if you unintentionally allow a Spammers address with this rule, that should not be a big issue, as Spammers rarely reuse addresses. On the other hand it is key to allow as many legitimate users as possible.
Except where message is to 'Global Allow List'
Or except where message is from 'Postmaster Addresses'
Where message does trigger text censor script(s) 'NOT Out of Office Reply'
Add message recipients into 'Auto Harvested Allow List'
And continue processing.

Rule: Challenge - Response Successful (Disabled)
This rule is designed to trigger on responses to the initial Challenge - Response rule. Senders who successfully answer the challenge message will have their original message released, and have their email address added to the harvested Allow List.
Where message is to 'Postmaster Addresses'
Except where message is from 'Global Allow List'
Where message does contain one or more headers 'Challenge Subject Keyword'
And where the external command 'Message Release' is triggered
Send a 'Challenge - Response Successful' notification message
And delete the message
And add message sender into 'Auto Harvested Allow List'

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

The rule applies to a specific group only as it is a very aggressive means of blocking Spam. In this case it only applies to those local users for whom total Spam blocking is a primary requirement, and for whom the Challenge / Response mechanism is acceptable.
Where message is to 'Executive Team'
Except where message is to 'Postmaster Addresses'
Or except where message is from 'Global Allow List'
Send a 'Challenge - Response Block' notification message
And move the message to 'Awaiting Challenge - Response' and categorize as 'None' with release action "continue processing"

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

The rule is a very aggressive means of blocking Spam and should be used only after taking due consideration of the consequences. Note that the Challenge \ Response system can generate a high volume of NDRs, and that messages from legitimate listservers will be blocked by default.
Where message is incoming
Except where message is to 'Executive Team' or 'Postmaster Addresses'
Or except where message is from 'Global Allow List'
Send a 'Challenge - Response Block' notification message
And move the message to 'Awaiting Challenge - Response' and categorize as 'None' with release action "continue processing"

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

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

7 Rule(s)

2.13 Policy Group: Message Archiving

Rule: Archive All Inbound Messages
This rule archives all inbound messages to a special Archive folder. By default, messages are kept for 3 months.
Where message is incoming
Copy the message to 'Archive In' with release action "continue processing"
And continue processing.

Rule: Archive All Outbound Messages
This rule archives all outbound messages to a special Archive folder. By default, messages are kept for 3 months.
Where message is outgoing

Copy the message to 'Archive Out' with release action "continue processing"
And continue processing.

2 Rule(s)

3 Dead Letter Policy

3.1 Policy Group: Spam Management

Rule: Move spam messages to DeadLetter:Spam Folder
If the message could not be unpacked by the gateway, but has been identified as spam by the SpamProfiler module, it is moved to a special dead-letter folder to separate spam that is malformed from legitimate malformed messages.
Where message is detected as spam by SpamProfiler
Move the message to 'Dead Letters: Spam' with release action "pass message through to recipient(s)"

1 Rule(s)

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.