CONFIDENTIAL

Reference	20201120/SD/1
Author	Spyros Delimpasis
Updated	2021-12-15
Comments	Clearswift SEG

CLEARSWIFT SECURE EMAIL GATEWAY

BEST PRACTICES CONFIGURATION

AGAINST ZERO-HOUR MALWARE

This document aims to provide the reader a configuration guide on how Clearswift Secure Email Gateway appliance can contribute to protection of an organization against zero-hour malware.

1. Antivirus Detection

Implement a 'Detect Virus' content rule for blocking malware.

Enable All Engines

It is highly recommended that you enable all available AV engines (Avira, Kaspersky and Sophos) for achieving the best possible detection rates.

Note: Enabling an additional antivirus engine requires an extra license option.

Heuristics and Cloud Lookups

It is highly recommended to enable all scanning methods (heuristics, behavioral, cloud lookup).

Although it is not expected and there have not been any reports from the field, enabling more than one AV engines might have an impact on the system performance. So it is recommended to monitor the performance of SEG for the first few days and ensure there is no performance degradation.

More details:

https://hstechdocs.helpsystems.com/manuals/clearswift/seg/english/5_4_0/SEG.htm#Sections/SystemsCenter/SYCAntiVirusScanners.htm

Virus Outbreak Detection

It is highly recommended that 'Virus Outbreak Detection' is enabled in the 'Detect Virus' content rule. This is typically enabled in inbound policy routes. If enabled for outbound routes, the administrator may notice false positive detections.

Sandbox

This is a cost option feature which uses the Sophos Sandbox service. When enabled, a hash-check is performed on the attachment and the engine consults *Sophos AV* scan results to identify whether to submit the attachment for sandboxing. One or more attachments can then be submitted for Sandboxing, which takes place in a cloud facility operated by Sophos.

Actions on Unsuccessful Scan

If an email or an attachment cannot be scanned then the Unsuccessful Scan condition is triggered. The administrator must keep failed messages in a dedicated message area (eg Virus Scan Failed).

Note: This content rule is included by default in the starter policy.

2. Block Malicious URLs

Implement a 'Sanitize Message' content rule to detect and block the 'Real-time Malicious URL-lists' from Mailshell and Sophos. These are managed lists that it contain URLs that are known to deliver malicious content.

It is recommended that in this rule 'All Messages' are scanned and not only on specific message classes.

3. Block Executables files and scripts (media type)

Create one or more 'Detect Media Type' content rule that will block Executable files and Script files. 'Detect Media Type' content rule will block media types based on the structure of data and not just the filename extension of an attachment.

The recommended media types for blocking are:

Executable Files

INCLUDED Media Types

- 32 Bit Unknown Windows
- DLL - 32 Bit Library
- ELF - Executable and Linkable Format
- EXE - 16 Bit Windows

Script Files

INCLUDED Media Types

- Batch Script
- Bourne Shell
- Javascript Files
- JavascriptEncoded Script

- EXE - 32 Bit Windows
- EXE - ActiveX Object embedded within Excel
- EXE - DOS Executable
- JAVA - Java Executable
- XPT - XPCOM Type Library
- Perl Script
- Powershell
- Python Script
- Unknown Script
- VBScript
- VBScriptEncoded

Note: This content rule is included by default in the starter policy.

4. BLOCK MICROSOFT CLASS1 FILES (FILENAME DETECTOR)

In addition to the above rule implement the pre-built "Hold Messages Containing Class 1 Files" content scenario. It will block executable and script files based on filename ("Detect Filenames" content rule). Clearswift has a pre-built "Microsoft Class1 Files" filename list which contains the following entries:

```
*.???*.bat
*.???*.chm
*.???*.cmd
*.???*.com
*.???*.cpl
*.???*.dll
*.???*.eml
*.???*.exe
*.???*.grp
*.???*.hlp
*.???*.hta
*.???*.inf
*.???*.js
*.???*.jse
*.???*.lnk
*.???*.mdb
*.???*.mht
*.???*.msi
*.???*.ocx
*.???*.pif
*.???*.reg
*.???*.scr
*.???*.shs
*.???*.swf
*.???*.vb
*.???*.vbe
*.???*.vbn
*.???*.vbs
*.???*.wsc
*.???*.wsf
*.???*.wsh
*.???*.{*
*.bat
*.chm
*.cmd
*.com
*.cpl
*.dll
*.eml
*.exe
*.grp
*.hlp
*.hta
*.inf
*.js
*.jse
*.lnk
*.mdb
*.mht
*.msi
*.ocx
*.pif
*.reg
*.scr
*.shs
*.swf
*.vb
*.vbe
*.vbs
*.wsc
*.wsf
*.wsh
*.{*
~*.???*.asd
~*.asd
```

Note: This content rule is included by default in the starter policy.

5. DETECT/SANITIZE ACTIVE CONTENT

Implement a 'Detect Active Content' content rule in all incoming routes. This content rule can detect active content (scripts and macros) in document files (MS Office, PDF, etc.). Blocking documents that carry active content can mitigate threats from zero-hour malware that is not yet detected by the other SEG methods and methods (Antivirus engines, Virus outbreak, etc).

Note: 'Detect Active Content' will block ANY document containing active content (malicious or not). So, the administrator might notice legitimate documents being held (especially with PDF attachments). Therefore, it is highly recommended to implement an inform mechanism (inform messages) towards the recipient or/and administrator. By doing so management of false positives can be greatly simplified.

Sanitize Active Content

The 'Sanitize Active Content' type content rule reduces administration overhead caused by false positives. This rule removes active content detected in document files. The attachment is rendered harmless and safe to be delivered to recipient's mailbox. This feature is part of the Adaptive Redaction technology which is developed by Clearswift.

In case the Active Content is required for the file to work correctly (e.g. Excel file with macros that perform calculations), the rule can be configured to hold a copy of the original message. The administrator can then release the original message to the internal recipient.

More details on Adaptive Redaction:

https://www.clearswift.com/resources/datasheets/adaptive-redaction-structural-document-sanitization

Note: 'Sanitize Active Content' content rule is available as additional license option.

6. SPAMLOGIC

Content Rule

Implement SpamLogic content rule ('Detect Spam' content rule) within incoming policy routes. This allows precise positioning of the antispam detection priority compared to other content rules of the inbound policy. It is highly recommended that SpamLogic content rules are positioned after content rules that detect malware threats (like blocking executables or scripts). For example if a message is carrying both an executable file but also is detected as spam by the SpamLogic engine, it is desired to end up in 'Executables' message area and not in Spam message area, because the Spam message area may be accessible directly from the end-user via PMM management.

It is recommended to create at least two "Detect Spam" content rules. The first one will handle spam for which the level of confidence for the detection is high and the quarantine will be accessed only by an administrator.

The second rule will handle spam for which the level of confidence is lower. There may be false positives and the quarantine for these emails can be accessed by PMM users, so they can handle quarantined spam emails that were sent to them.

In some environments a third rule may be required to quarantine emails that were marked as phishing emails.

Global Spamlogic Configuration

Enable secondary antispam engine (Rspamd) in Policy > Spamlogic settings > tab Antispam Engines.

Disable all methods, except:

- Validate Sender Domain
- Greylisting

Local SpamLogic Configuration

Create two "Detect Spam" content rules.

a. Hold Confirmed Spam that will include these detection methods

- Bad Reputation returned by TRUSTManager
- Real-time IP Blocklist
- Spoof Detection
- SPF Hard Fail
- DMARC Reject
- Confirmed Spam

The disposal action can be set either to Reject or preferably to Hold. By quarantining it will be possible to handle false positives, but more storage may be required because the Area of this rule will hold a lot of messages.

b. Hold Probable Spam that will include these detection methods

- BATV
- SPF Soft Fail
- DMARC Quarantine
- DKIM Hard Fail
- DKIM Soft Fail
- Suspected Spam Email

The disposal action must be set to Hold. The Area used must be different from the one used in the previous rule.

More details on SpamLogic methods can be found here:

https://hstechdocs.helpsystems.com/manuals/clearswift/seg/english/5_4_0/SEG.htm#Sections/PolicyCenter/PCSpamConfigureSpamPolicy.htm

Phishing Detection in SpamLogic

SpamLogic can distinguish phishing messages from Spam messages. Phishing messages are considered dangerous and their goal is to steal credentials or initiate a social engineering attack (BEC attacks, CEO fraud etc.).

If Rspamd is enabled Spamlogic can use the advanced phishing detection feature provided by PhishTank (Policy > Spamlogic settings).

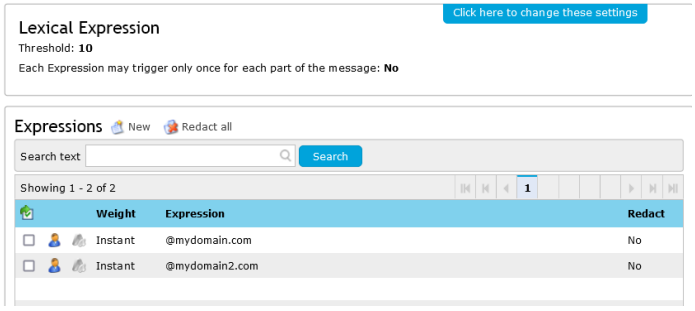
It is highly recommended to implement SpamLogic as multiple content rules in the same incoming policy routes, that will quarantine 'Phishing' messages separately from 'Junk' messages.

The SpamLogic content rule can further differentiate between 'Confirmed Phishing' and 'Suspected Phishing' messages. This can allow even further separation of these two message classes for storing into different quarantines. Please note that 'Suspect Phishing' may have false positive detections, so the administrator may want to apply different policy/management from 'Confirmed Phishing'.

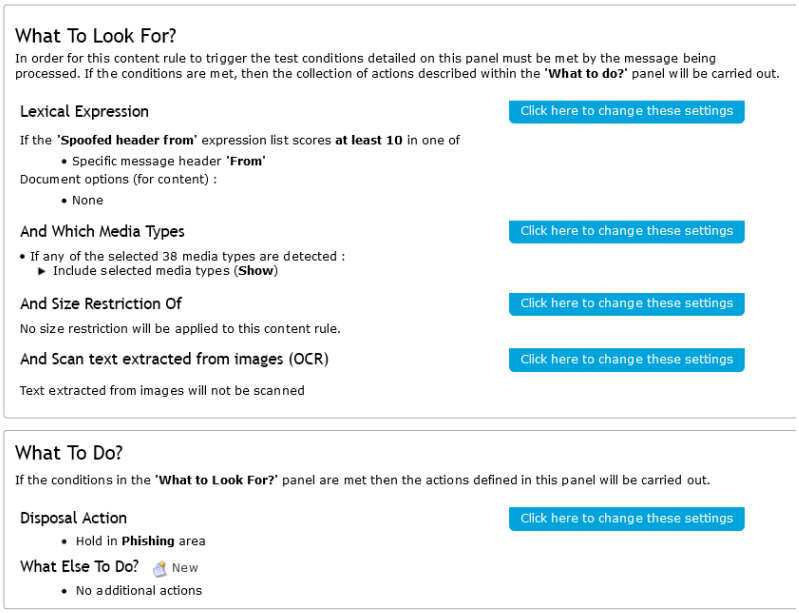
7. HOLD SPOOFED "FROM" HEADER

Implement a lexical detection rule that detects internal email addresses into the From header of emails originating from the Internet. This header can be easily spoofed to an internal address and make users think that they are receiving emails from a trusted source.

First you must create a lexical expression list and add in it all protected (internal) email domains:



The list must be assigned to a lexical detection rule, that will search in header "From" and hold emails that trigger this rule in the Phishing Area.



The rule must be added to all routes that process incoming email traffic.

8. BLOCK ENCRYPTED & PASSWORD PROTECTED MEDIA TYPES

Implement the pre-built 'Hold Messages Containing Encrypted Files and Inform the Recipient' content rule. It is a 'Detect Media Type' content scenario that detects and blocks media types that are encrypted/password-protected. Clearswift SEG analysis engine is not able to analyze these files, thus as a security precaution they should be blocked for manual inspection.

The pre-built content rule INCLUDES the following media types:

- Encrypted Data > PEM Message > Digital Signed and Encrypted
- Encrypted Data > PGP Message > Digital Signed and Encrypted
- Encrypted Data > PGP Message > Encrypted
- Encrypted Data > PKCS Message
- Encrypted Data > PKCS Signature
- Script Files > JavascriptEncoded
- Script Files > VBScriptEncoded
- Miscellaneous > Unrecognized type > Encrypted
- Compressed Files > 7-zip > Encrypted
- Compressed Files > RAR - RAR compressed Archive > Encrypted
- Compressed Files > ZIP - PKware ZIP Compressed Archive > Digital Signed and Encrypted
- Compressed Files > ZIP - PKware ZIP Compressed Archive > Encrypted
- Documents > Microsoft Excel Spreadsheet (XLS XLSX) > Digital Rights Protected
- Documents > Microsoft Excel Spreadsheet (XLS XLSX) > Encrypted
- Documents > Microsoft Powerpoint Presentation (PPT PPTX) > Digital Rights Protected
- Documents > Microsoft Powerpoint Presentation (PPT PPTX) > Encrypted
- Documents > Microsoft Word Document(DOC DOCX) > Digital Rights Protected
- Documents > Microsoft Word Document(DOC DOCX) > Encrypted
- Documents > Open office Calc Document (ODS) > Encrypted
- Documents > Open office Graphic Document (ODG) > Encrypted
- Documents > Open office Impress Document (ODP) > Encrypted
- Documents > Open office Master Document (ODM) > Encrypted
- Documents > Open office Math Document (ODF) > Encrypted
- Documents > Open Office Writer Document (ODT) > Encrypted
- Documents > PDF - Adobe Portable Document Format > Encrypted
- Message Formats > Microsoft Outlook Document (TNEF) > Digital Rights Protected

Note: This content rule is included by default in the starter policy.

9. BLOCK UNKNOWN BINARY

It is highly recommended to block media types that SEG is not able to recognize and analyze. This can be achieved with the pre-built 'Hold Messages Containing an Unrecognized Media Type' content rule. It is a 'Detect Media Type' content rule which detects the following media type:

```
Miscellaneous > Unrecognized Type > Not Signed, Encrypted or DRM protected
```

This content rule is expected to produce false-positive detections with messages and attachments that are not recognized by the SEG analysis engine. The false positive cases are expected to rise if the route includes a 'Structural Validation' rule. Therefore, it is recommended to implement an inform mechanism (inform messages) towards the recipient and/or the administrator. By doing so management of false positives can be greatly simplified.

Note: This content rule is included by default in the starter policy.

10. SANITIZE SUSPICIOUS or ALL URLs

The 'Sanitize Message' content rule allows also for the sanitization (removal) of suspicious URLs in message bodies.

Suspicious URLs are URLs that the Clearswift engine can detect based on specific patterns (e.g. URL that redirects to another URL, IP instead of hostname, etc.). Not all patterns signify a malicious attempt, so there may be false-positives.

It is recommended to setup a 'Suspicious URLs' URL list that has enabled all the rules for detecting suspicious URLs. Then implement a 'Sanitize Message' content rule that will sanitize the suspicious URLs in body and deliver the message. Just like with Active Content sanitization, it is possible to retain the original message in case the internal recipient needs it.

By sanitizing URLs the engine will actually replace the URL with asterisks. In rich text the actual anchor element will also be sanitized. In essence, clicking the link does not allow navigation to the URL.

In environments where elevated security is a must (e.g. military and financial institutions) the 'Sanitize Message' content rule can be configured to sanitize all URLs for incoming messages. This may add administration overhead due to increased numbers of false positives and release requests coming from internal users. In that case the administrator can create a custom URL list of allowed (whitelisted) URLs that will not be sanitized when detected in incoming messages.

The 'Sanitize Message' content rule offers a variety of options on how and what to sanitize in a message. For example there is the possibility to remove URLs that have to do with styling and images in rich text message bodies.

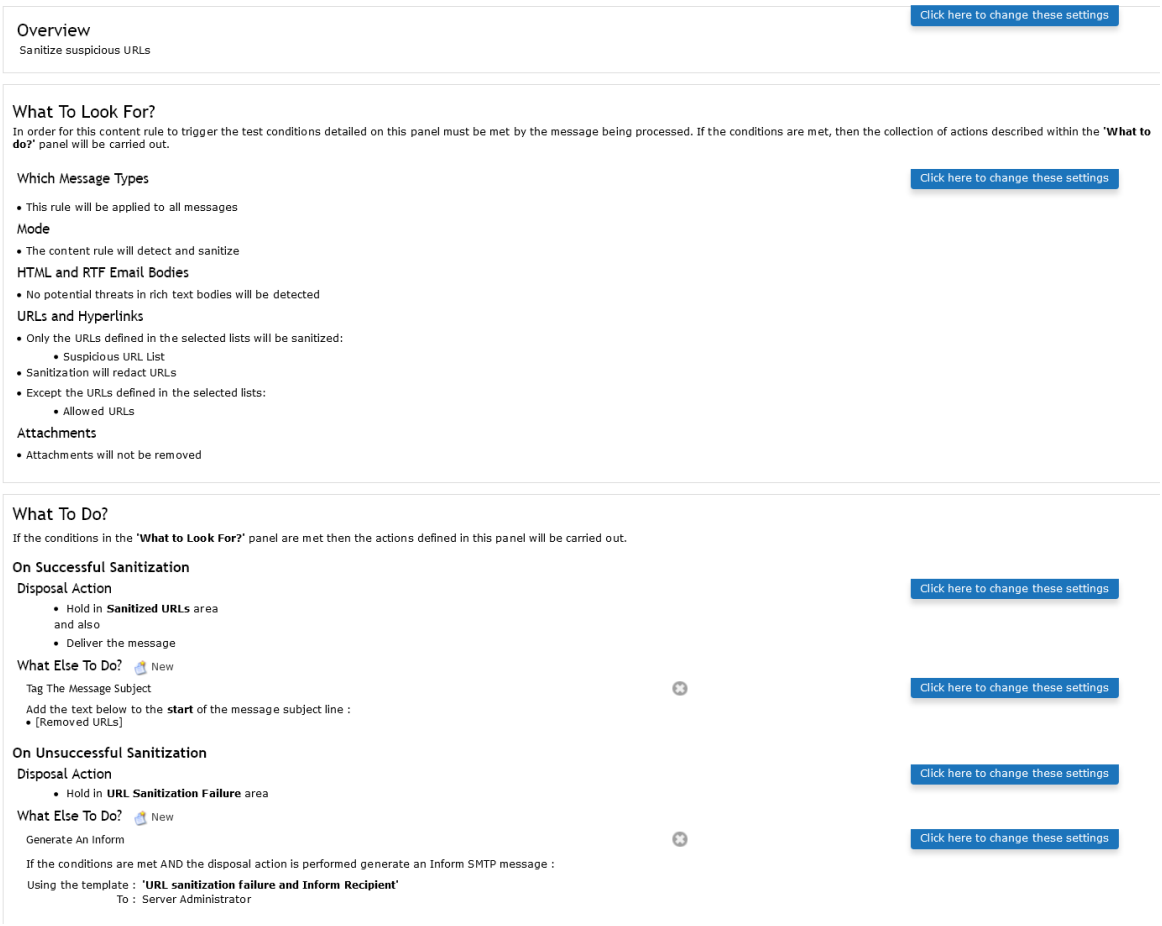
It can also remove or convert a message body in pure plain from rich text, for even more proactive security (plain text cannot carry active content, or URLs that are downloaded automatically). But of course, this affects the display of the message content.

The optimal balance point between security and usability differs for each organization. So it will not be attempted in current document, to go into more details on how to use this content rule.

It is highly recommended to read more details on the 'Sanitize Message' content rule, to identify any further needs that this content rule can cover for your organization.

More details can be found here:

https://hstechdocs.helpsystems.com/manuals/clearswift/seg/english/5_4_0/SEG.htm#Sections/PolicyCenter/PCAboutSanitization.htm



11. STRUCTURAL VALIDATION

'Structural Validation' content rule will look for data and files appended to image files (GIF, JPG, PNG, TIF). This is a technique where an attacker tries to mask a malicious file to image files, in an attempt to bypass scanning. Structural Validation can identify if there are appended data in the afore-mentioned media types and make them available to the analysis engine for further inspection according to the content rules in the policy route.

This content rule is expected to produce false-positive detections, especially in combination with the 'Detect Unknown Binary' content rule above.

PDF Image Extraction

If Structural Validation should be applied against images that are embedded in PDF files, then the following setting must be enabled:

```
System > Policy Engine Settings > Advanced > PDF Image Extraction = enabled
```

Turning on this feature will impose performance overhead. This is due to the creation process of most virtual PDF printers that are available on the Internet. The process includes the transformation of each document page to an image which is also compressed in order to minimize size of the resulting PDF file. When such a file is examined by the Policy Engine, all images need to be decompressed and then scanned. This process is very demanding in memory and CPU cycles and in effect may slow down message flow. If this setting is enabled it is recommended to monitor system performance during the first few days.

12. BLOCK MALFORMED DATA

Implement in all incoming routes the 'Detect Malformed Data - Email' content rule. Default disposal action for these rules must be set to 'Hold to Message Area'. Malformed data is any information that cannot be read or correctly processed. It can often go unnoticed in message attachments and might contain a hidden threat to the organization.

The content rule operates on selected Media Types. The administrator can exclude or include certain types (such as PDF) using a combination of Detect Malformed Data content rules.

Note: This content rule is included by default in the starter policy.

13. BLOCK FAIL TO PROCESS/FAIL TO MODIFY

Implement in all incoming routes the 'Failed to Process' and 'Failed to Modify' content rules. Default disposal action for these rules must be set to 'Hold to Message Area'. These content rules trigger when a message fails to be analyzed or modified. This means that the message might have undetected malicious content, therefore such message must be quarantined. Manual inspection of these message is required before releasing them to internal recipients.

Note: This content rule is included by default in the starter policy.

CONTENT RULES PRIORITY

Based on the information of current document, we provide sample list for rules in incoming policy routes. The key concept is that the higher a risk a rule represents, the higher must be placed in the list. Also, if a rule includes a Delivery disposal action, it must be placed as low as possible. Rules with action set to "Perform no action" can be placed wherever the administrator wants in the list. Even if these rules trigger, no action will be applied to the message.

16 Rules on route (applied in the order shown)

		Rules	Rule Type
1.	☐	Structural Validation Perform no action	Validation
2.	☐	Drop Messages Containing a Virus Hold in **Virus** area	Virus
3.	☐	Hold malicious URLs Hold in **Malicious URLs** area	Sanitize Message
4.	☐	Hold Executables Hold in **Executables** area	Media Types
5.	☐	Hold Class 1 Files Hold in **Executables** area	Media Types
6.	☐	Hold Encrypted Files and Inform the Recipient Hold in **Encrypted** area	Media Types
7.	☐	Hold Messages Containing an Unrecognised Media Type Hold in **Unknown Binary** area	Media Types
8.	☐	Hold active content Hold in **Active Content** area	Active Content
9.	☐	Hold Phishing Hold in **Phishing** area	SpamLogic
10.	☐	Hold confirmed spam Hold in **Spam** area	SpamLogic
11.	☐	Hold probable spam (PMM enabled) Hold in **Probable spam** area	SpamLogic
12.	☐	Sanitize Active Content Hold in **Sanitized Active Content** area , and also Deliver the message	Active Content
13.	☐	Sanitize Suspect URLs Hold in **Sanitized URLs** area , and also Deliver the message	Sanitize Message
14.	☐	Fail to Modify a Message Hold in **Message Processing Failure** area	Error
15.	☐	Detect Malformed Data - Email Hold in **Message Processing Failure** area	Error
16.	☐	Fail to Process a Message Hold in **Message Processing Failure** area	Error

Rules 2-8 are considered a kind of ‘threat’ zone. These content rules detect messages that may have malicious content. Therefore, they must be placed above other rules.

Other content rules that fulfill other kind of policy requirements (e.g. message sizing, multimedia files, etc.) can be placed after the threat-bearing content rules. SpamLogic content rule can be positioned among them accordingly.

In a typical scenario either a ‘Hold Active Content’ (Rule 8) or ‘Sanitize Active Content’ (Rule 12) content rule is implemented but not both. ‘Detect Active Content’ rule is positioned in ‘threat’ zone as it can detect potentially malicious content. ‘Sanitize Active Content’ and ‘Sanitize Suspect URLs’ sanitize and deliver a message so they are positioned towards the end, as to not override other content rules.