clearswift
by HelpSystems

Clearswift & Sandbox Technology

Version 1.1

01/08/2017

Copyright

Contents

1 Introduction

With the introduction of Sandbox technology to address targeted threats and malicious active code, a new problem has arisen. The main issues around Sandbox technology are the following:

- Cost of per message to be scanned
- Hardware cost & throughput requirement
- Virtual aware malware
- Time Released malware

The use of Clearswift's Adaptive Redaction – Structural Sanitization, will mitigate all active code from Microsoft Office formats, Open Office, HTML, RTF and PDF files.

The best practice of the using the Structural Sanitization is to hold a copy of messages that have been successfully redacted of active content. An annotation is also advised to inform users both internally and externally that the message has been amended according to the company policy.

The risk is apparent when the user contacts the IT department to ask for the message with the active code. This can occur when the user either does not understand the risk of the active code or when the original message is a well formatted phishing email / attachment.

In addition to the above risks, users may be tempted to ask for the original message with the active code if the sender is 'trusted'. This is where the insider threat can occur if the trusted sender has been compromised.

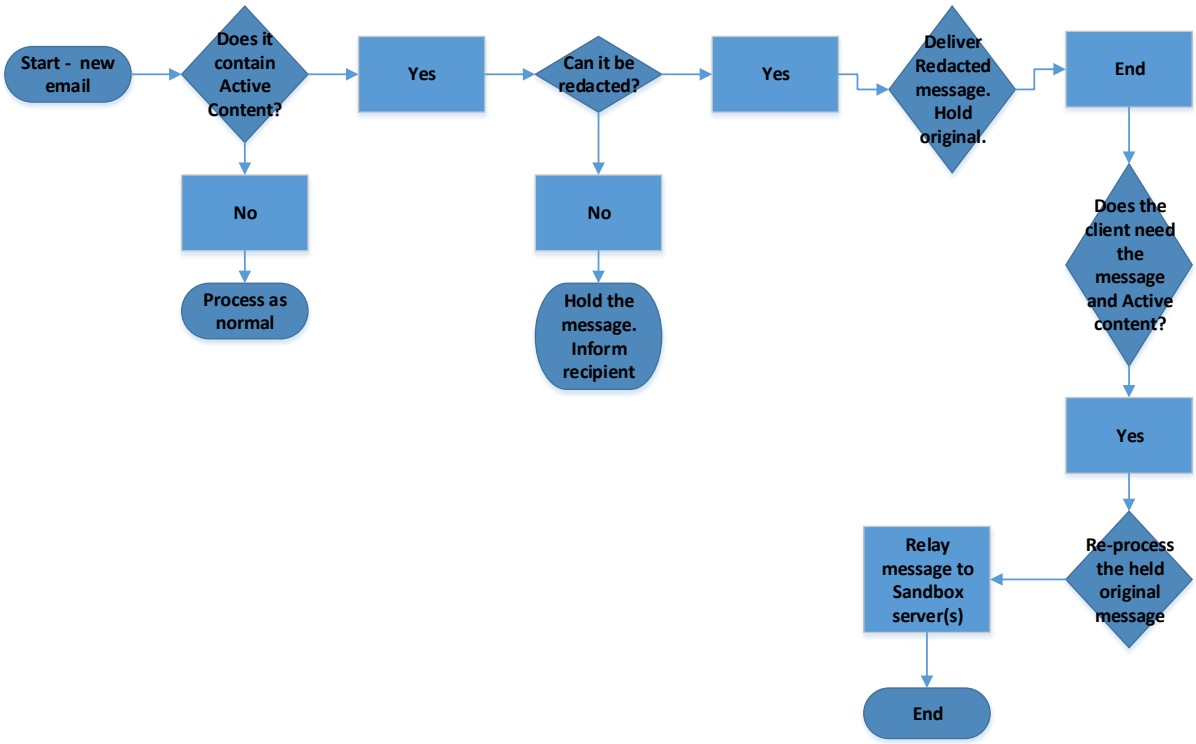
As with all security approaches there is no 'silver bullet' to address all security risks. This combined with the need for business communications to continue can cause compromising risks within security policies.

By utilizing either Clearswift's award winning SECURE Email Gateway OR Clearswift ARgon for Email in conjunction with a Sandbox technology, a proper balance can be achieved.

This document outlines how using both technologies can protect the organization whilst reducing costs, time and false positives on active code.

2 Mail Flow process

The below diagram shows the mail flow process of using both Clearswift and Sandbox technology:



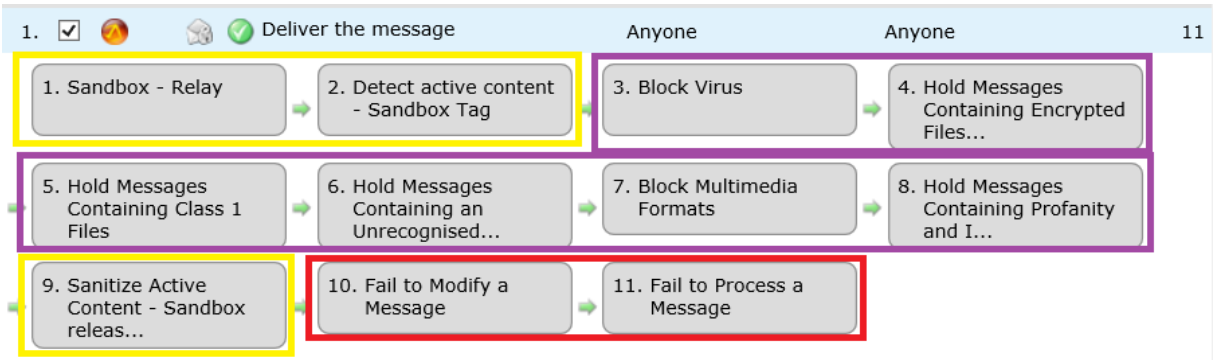
The mechanism for the relay to the sandbox server is that all mails are tagged with an X-Header regardless of whether the message contains active content or not.

When the message is 'reprocessed' the message goes through the evaluation of the rules again and an additional content rule will be triggered looking for the X-Header added in the first processing of the message.

2.1 SECURE Email Gateway Policy configuration

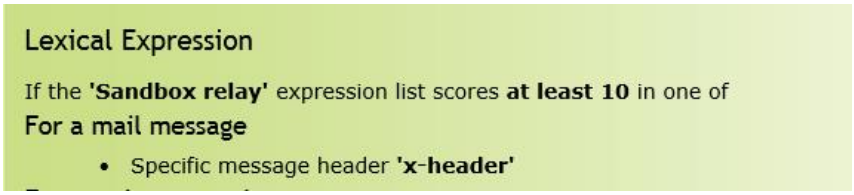
The SECURE Email Gateway policy has to have another triggered content rule for the "reprocessed" messages to add a different action whilst allowing normal messages not be triggered for the relay to Sandbox content rule.

The simple design from the content rules aspect is:

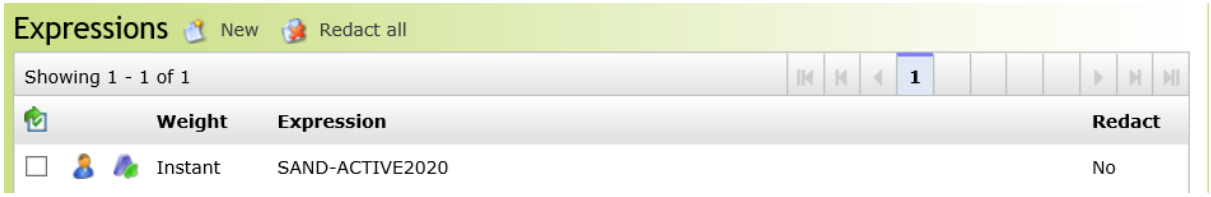


The processing flow is as follows:

Rule 1 "Lexical Expression" content rule. This rule is only triggered when the message is 'Reprocessed'. The rule is a Lexical based content rule looking for the X-Header added from rule 2 below. The action is to relay the message to the Sandbox server.



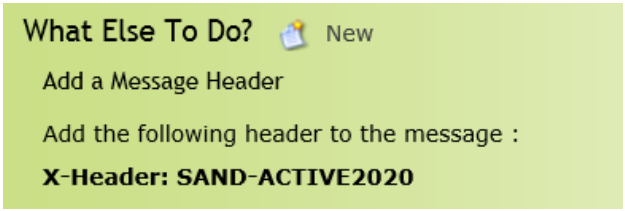
The "**Sandbox relay"** is adding the below X-Header to the message:



The action of detecting the X-Header is:

The Disposal action of the Relay is set as "Original Message"

Rule 2 – "Detect Active Content" content rule. Adds the X-Header e.g. SAND-ACTIVE2020 (this value could be anything required):



The X-Header is added to all messages that contain active code only.

Rules 3 to 8 are normal mail flow scanning

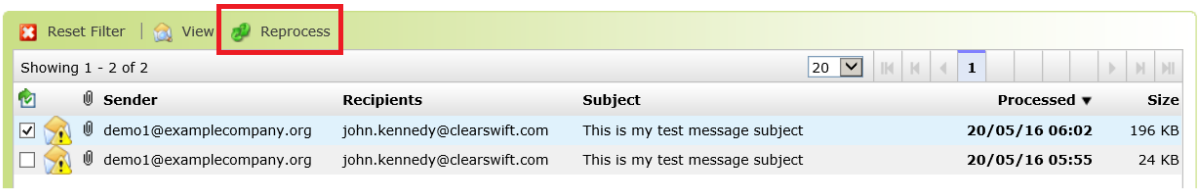
Rule 9 is the Structural Sanitization rule that removes the active content then delivers as normal. A copy of the message is then held.

Rule 10 & 11 are standard rules for non-RFC compliance, System failure

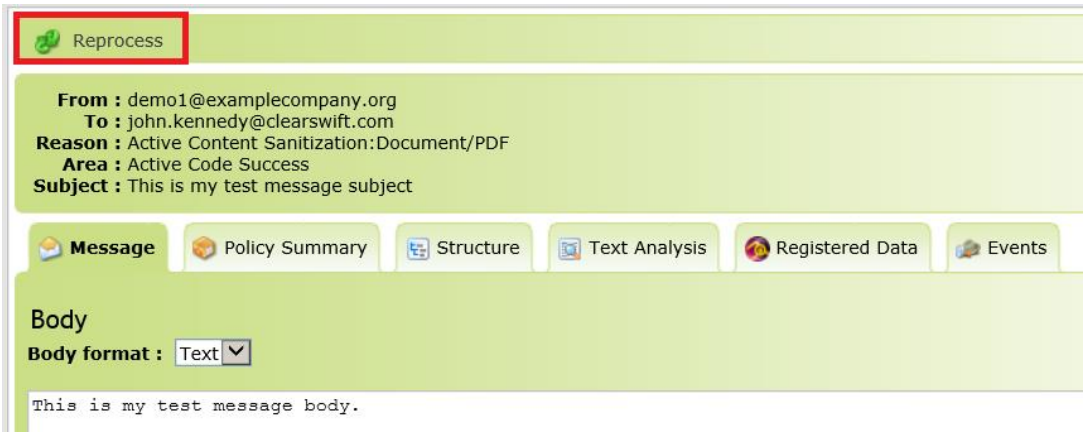
2.2 Active Code release

For any message that has been redacted and a copy has been held a user can request the original message with the active code to be released. This mechanism would also be valid for messages that the active code could not be redacted for any reason.

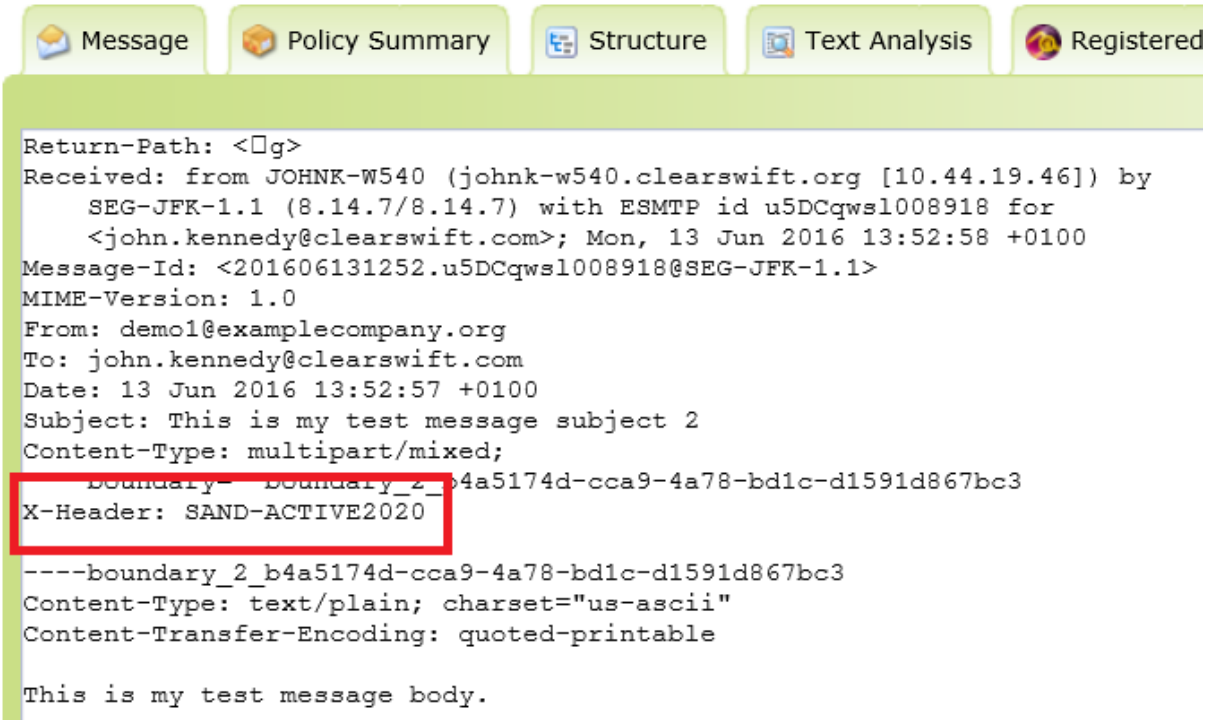
The system administrator can then select the required message and 'Reprocess' it e.g.



OR through the message view itself:



By taking the action of reprocessing the message, the message will now go through all content rules again. The second scan will now show the X-Header added by content rule 2. This can be seen in the raw message:



Content rule 1 will now match this X-Header and route the message to the Sandbox server for additional scanning.

3 Benefits

The benefit of utilizing both technologies means that the mail flow is not delayed needlessly. The organisation is protected by the removal of the active content BUT allowing the message and attachments through to the recipients.

If the Sandbox server solution is priced per message the final cost would be greatly reduced as only messages that are identified as business mail by the recipient and the requirement for the active code will be sent to the Sandbox solution.

4 Outgoing messages

The solution was designed around inbound messages. However the same principle could be applied to outbound messages.

The policy could redact active code. Then, if required, reprocess the message and relay to the Sandbox server. The criteria would be that the Sandbox server can deliver messages to the Internet.