clearswift

Product Information Bulletin

Clearswift SECURE Email Gateway 4.5

Issue 1.0

November 2016

Contents

Overview

This new release delivers a number of customer enhancement requests, as well as additional security features for the Clearswift SECURE Email Gateway.

The new features are briefly summarized below, and examined in more detail on the following pages.

- Branding
- Expose Anti-virus heuristics & behavioral settings
- Anti-spoof enhancements
- External Command
- Route Selectors
- Message Reprocess option
- Key server enhancements
- Increased Lex Threshold

Branding

Key points:

- Refreshed UI, new colors and new branding
- Remove Shockwave flash from UI
- Improved performance

The user-interface has modified to not only reflect new Clearswift branding, but more importantly to improve the usability, security and performance.

All usage of Shockwave flash have not been removed from the product following the ever increasing number of emergency updates published by Adobe. The latest security update (CVE-2016-7855[1]) is given a Priority 1 category. Flash was previously used in the System Health page, Reports and various QuickCharts in the product.

[1] https://helpx.adobe.com/security/products/flash-player/apsb16-36.html

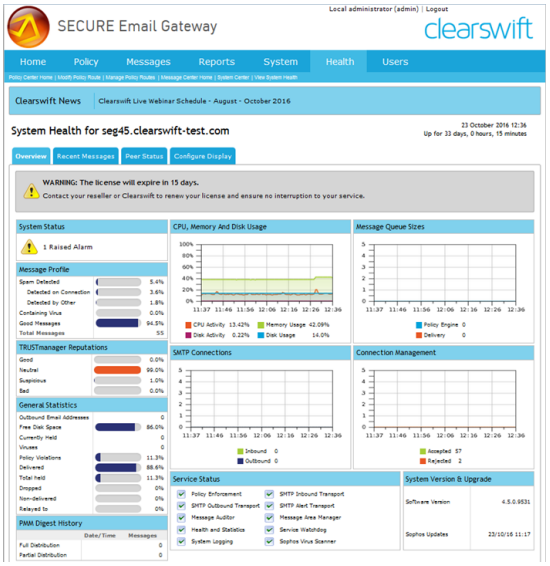

Figure 1 New System Health

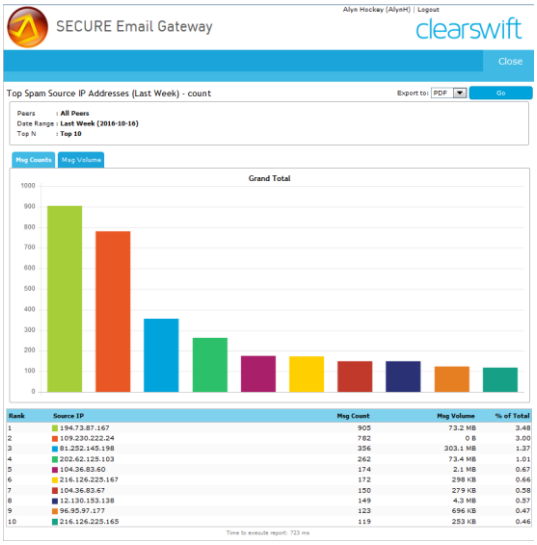

Figure 2 New Report style

Expose Anti-virus heuristics & behavioral settings

Key points:

- Allow customers to select levels of scanning they wish to use
- Heuristics and Behavioral scanning by default

Given the speed and growth of new malware, the Gateways can now exploit the Sophos and Kaspersky engines to their fullest levels. This release allows the customer to determine how aggressive they want to inspect files for malware.

The Gateways already use signatures which are checked every 15 minutes, but also using a HTTP/DNS Cloud based lookup to see if the file in question has malware so

new it hasn't been listed in the latest signature update. The Cloud lookup can bring the window of time from when the vendor detects the message as malicious down to the point where a Gateway can use that signature down to just 3 minutes.

Not only are signatures used to identify malware, but the Gateways can now inspect the file being scanned using heuristic algorithms to see if the file shares any similarity to other known items of malware and also perform behavioral analysis to try and understand what the file will do when it does execute, in a similar way to how a Sandbox works, but only much faster.

This release allows customers to enable or disable scanning options from within the user interface.

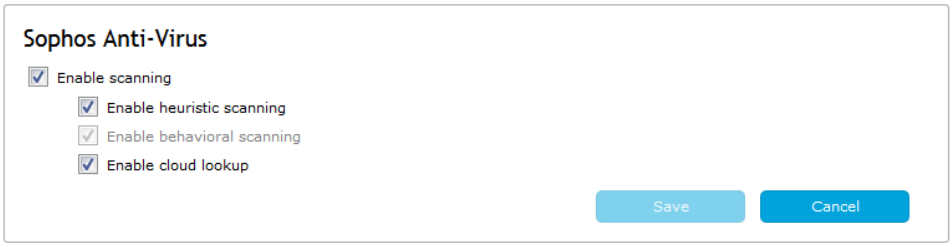

Figure 3 - AV Scanning options

Anti-spoof enhancements

Key points:

- Ability to hold spoofed messages in quarantine
- New algorithms to detect spoofed messages

Spoofed messages are examples of social engineering and are very common with Phishing and "whaling[2]" and as such it is very important to be able to detect these particular messages and stop them arriving at their intended destination before the recipient either compromises themselves or their company[3].

The Spoof detection rule has been extended to allow customers to not simply reject spoofed messages but also hold them in quarantine to allow analysis of the message and record it source.

Along with this change, additional algorithms have been put into place that would prevent a number phishing emails from being successful.

[2] https://www.techopedia.com/definition/28643/whaling
[3] http://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/

External Command

Key points:

- Allow customers and partners to create plugins to extend Gateway functionality
- Supports shell script, python script and executable
- Can be used to detect or modify data

There are times when customers have requirements that we may not be able to fulfill and as a result they may consider moving to a different product. Rather than lose a customer we have provided an easy way to extend the functionality without necessarily have to write complex code.

The Run External Command means to allow customers to add their own components to perform some specialized detection or modification of messages and their attachments.

They can use any Shell scripts, Python scripts and Linux executables that can be executed on a linux command line that does not need any user interaction to be configured.

The external command can be configured to only run on certain policies and on specific data types. The invoked command can also modify data, but the modification of data is restricted to keeping the file type the same, although the contents may differ, for example

Color image converted to monochrome

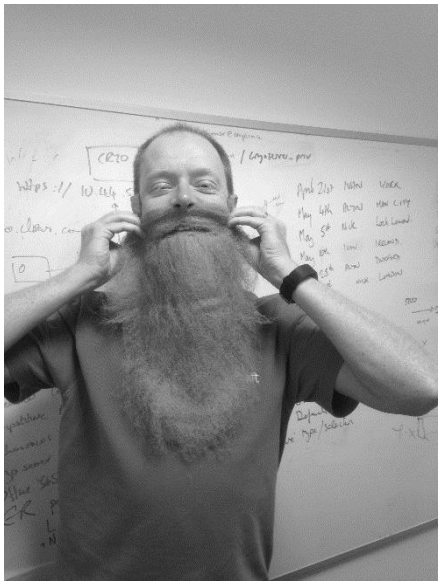

Figure 4 - External Command

This feature is not recommended to support time consuming operations on the data as that could have significant issues on overall message processing. Ideally any processing should be counted in milliseconds and seconds, not minutes.

Route Selectors

Key points:

- Create routes within routes
- Maintains separation of sources and destinations
- Helps to reduce the size of policy files

Policy routes define what rules will be applied to specific senders and recipients. The senders and recipients are defined in one or more address lists.

In most cases the collection of senders and recipients does not cause conflict, but potentially the collection of address lists may provide an opportunity for someone to be able to send email to someone that they shouldn't.

For example, if you have 2 groups of Account Managers who deal with different groups of customers, but the account managers should only be able to mail their own customers. This could easily be created using a policy like

	Action	From	To	Rules
1.	Deliver the message	Account Managers (Alpha)	Customers List 1	2
2.	Deliver the message	Account Managers (Beta)	Customers List 2	2

The downside of this approach is that you'd need a number of routes, making the policy large, so potentially harder to visualize and also tedious when adding a common rule to lots of policy routes.

In 4.5 we use route selectors, or "routes within routes" which permits individual separation of senders and recipients and means that adding new rules to the routes is much simpler.

	Action	From	To	Rules
1.	Deliver the message	Account Managers (Alpha) Account Managers (Beta)	Customers List 1 Customers List 2	2

Customers who upgrade will not see any behavioral change in policy routes until they start to separate their address lists.

Message Reprocess options

Key points:

- Extends the functionality of the reprocess feature
- Option to reprocess both original and modified message
- Option to select which route the message is reprocessed through

Currently when a message has been blocked, the SysAdmin may want to re-process it to either

1. Rectify policy configuration and verify any changes made to policy so that the message isn't blocked
2. Verify that the message is still safe to be delivered by reprocessing the message which will repeat the virus scans (with hopefully newer malware signatures)

In both cases the message is reprocessed using the same policy route. A number of customers wanted the ability extend this to allow them to override the route and allow them select a special route which could perform different operations on the message.

In this following example, inbound mail is normally processed by Route 1 and the message is checked for various rules. In this case some has received a message with an image attachment which is banned. This has caused the message to be blocked and inspected.

The SysAdmin decides that the message is ok, but the image is not, so they have have created a special dummy route with rules to remove offending attachments. They can use the Reprocess feature to have the message reprocessed using the rules in the other policy route where the offending items are striped from the message.

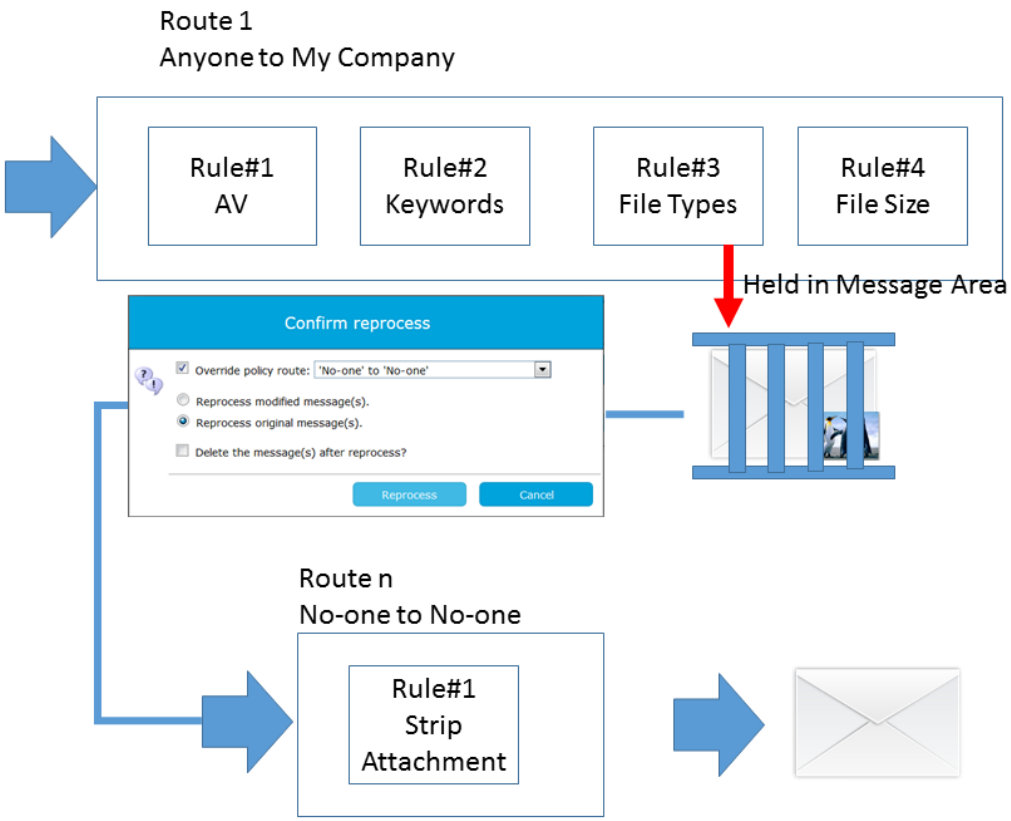

Figure 5 - Message Reprocessing

The reprocess message manage feature has been extend to allow either the original or modified message to be reprocessed. This maybe important as the original message may have an active document that had been sanitized and delivered in its modified format.

Key Server enhancements

Key points:

- Secure connectivity to external key servers
- Support for AD servers to be supported as key servers
- Support for binary certificates

For customers using the Email Encryption feature we have made some enhancements to provide greater support for retrieving certificates from external key servers.

We now support HTTP/S and LDAP/S as a communications protocol to key servers so that credentials used to query key servers is not compromised.

The gateway can now also support binary mode certificates which are typically served by Windows AD (Windows 2008R2 and Windows 2012) which is also supported.

Increased Lex Thresholds

Key points:

- Increased the threshold for keyword search functions
- Maximum threshold now 10,000

The previous threshold for use in a keyword search rule was 100, and to allow for greater granularity when dealing with complex search criteria where it is necessary to use multiple words and phrases to calculate whether material should be stopped has now been extend to 10,000.

Enhancement requests

The following customer reported enhancement requests have been implemented in this release.

ER#	Summary
Mail-10082	Option to hold messages with spoof detection
Mail-8402	Run external command with access to attachments in SEG
Mail-6549	Key server must support certificates in binary format
Mail-6548	Key server lookup needs to support AD
Mail-6421	Request for Key Server Query via LDAP/S & HTTP/S
Mail-8404	Allow multiple 'Mail Sent' routes per Mail Policy Route
Mail-10026	Support higher lex threshold limits

Bug fixes

A number of client-reported bugs have been fixed in this release. Please see the release notes for more information.

Availability

Phase	Date
General Availability	1st November 2016

Interoperability

It is possible[4] to peer a Version 4.5 Gateway with an existing Version 3.x Gateway although it will not be possible to share policy due to the different levels of functionality in the later products.

It will be possible to import a 3.8 configuration into a V4.5 system thus saving deploying a V4.0 (or 4.1 to 4.3) and then upgrading that to V4.5.

End of life

This release will signal the start of the SEG 4.3 end of life program. Version 4.3's EOL program will last 12 months (as defined in the Support Services handbook) and will reach end of life on 1st November 2017.

Platform support

Clients with low memory and low disk space systems may find that their hardware is no longer suitable and may need to refresh their hardware / virtual systems.

Clearswift recommends that systems have a minimum of 4Gb RAM, multi-core processors that support 64bit instructions and over 250Gb+ of disk space for low volume production environments.

For customers with a greater workload the recommended minimum would be 6-8Gb RAM, single or dual multi-core processors and 250Gb+ of redundant disk storage.

Packaging

This release will NOT be available as a patch for all systems running 3.x to automatically download.

[4] In orde to peer a V4.4 or later with SEG 3.8 does require some modification of the TLS ciphers used for Peer communications

Clients using 4.0 to 4.4 will be able to upgrade their system through the Admin console.

Clients who want to migrate from 3.x must install a new system and migrate their existing configuration to the new system. They will typically deploy the solution in a test mode initially and then deploy a production system.

Clients will be able to import a V3.8.* policy file to replicate their policy or a V3.8.* full system backup if they want to import reporting data, quarantine messages, logs and policy.

To make the installation process easier, clients will be able to request professional services from Clearswift to assist in the deployment of this new version.