clearswift

Major Features Overview - Version 4 Releases

Clearswift SECURE Gateways

Issue 1.0

September 2016

Copyright

Version 1.0, September, 2016

Published by Clearswift Ltd.

Contents

Introduction

This document describes the major features made available in the Version 4 Releases of the Clearswift SECURE Gateway products, up to and including 4.5 (due for release in November 2016), that are not available in the Version 3.x series of releases.

Platform

Red Hat Enterprise Linux (RHEL)

There are numerous advantages for using RHEL, these include:

- Enterprise grade security
- Reduces customer need for familiarisation with "another" Linux
- Widely used in Fortune 500 (Government, Military and Finance sectors)
- Long life support - RHEL 6.x support till 2021 with standard coverage
- Greater support for new hardware
- 64bit operating system (allowing customer to use more than 4Gb of RAM of physical memory)
- Better support for cloud environments (Public cloud providers such as AWS and Azure)
- Support for 3rd party applications and drivers to allow tools to be loaded onto the platform to aid system operations and management.
- IPv6 ready (not enabled)
- Allows product to be deployed as "Appliance" or as "Software"

Platform console

Management of the networking configuration, external connections (such as NTP, SNMP and SCOM servers), command line access and product updates are now performed via the System console allowing only the system administrator to make changes to these vital system parameters.

Strong console password

For greater security, the system now requires a strong password to be used for console access.

SNMP and SCOM monitoring

Monitoring of the platform via standard system management tools like SNMP and SCOM are now standard.

Hygiene services

Revised Anti-spam engine

There are number of enhancements to improve the spam detection and reduce the false positives. These include:

1. New TRUSTmanager sender IP system, easier to deploy and more accurate
2. New signatures engine looking for messages and classifying based on
    a. Detection of Bulk mail
    b. Message reputation checks
    c. Content checks
    d. Spam tricks detection
3. DKIM support.

Kaspersky Security Network

When Kaspersky detects a new virus, the new signature is made available via a Cloud lookup as well as being added to the next signature. This method significantly improves spam detection of new malware variants as new malware can be detected with minutes of being recognised as malware by Kaspersky.

Cloud based lookups can reduce the time for a virus signature to be made available from many hours to as little as 3 minutes.

Sophos Live Protection

When Sophos detect a new virus, the new signature is made available via a Cloud lookup as well as being added to the next signature. This method significantly improves spam detection of new malware variants as new malware can be detected with minutes of being recognised as malware by Sophos.

Cloud based lookups can reduce the time for a virus signature to be made available from many hours to as little as 3 minutes.

AV heuristics and behavioural analysis

Both AV tools use signature files which are updated regularly, but also real-time lookups to see if it's a new known piece of malware. They can also perform heuristic checks on the file where they inspect the code/structure of the file to see if it is similar to other malware that has been observed before, so whilst it may not 100% guaranteed, it may detect new strains of malware.

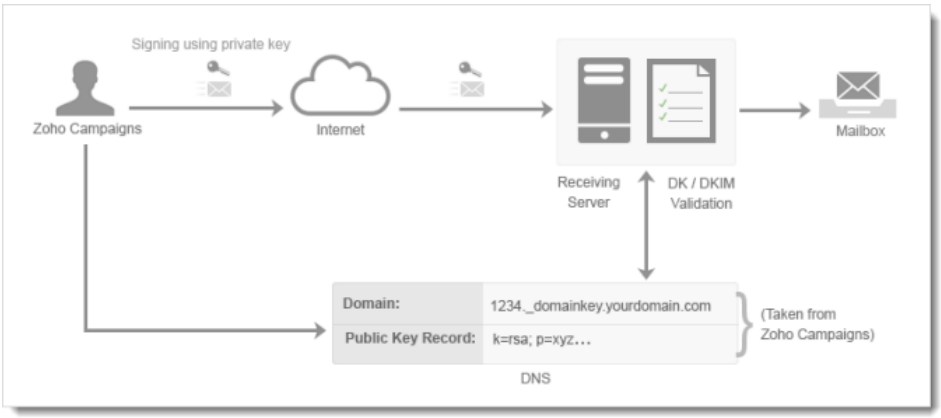
Behavioural analysis involves running portions of code via some code emulation capabilities to understand what the program is doing. If the code is performing activities which are not expected then the AV engine may also flag this file as a concern.

Hold spoofed messages and new spoof detection algorithm

Spoofed messages are a major problem for an organization so providing methods to monitor and detect these are key. The 4.x software permits these to be held in Quarantine and new algorithms have been added to simplify detection.

Domain Keys Identified Mail

DKIM is a method of identifying if an email is authentic and will help to reduce the amount of spoofed messages being sent into an organization.



It also benefits validity to messages that are sent by an organization so their business partners can trust that they are authentic.

Support CIDR based whitelists

A Classless Inter-Domain Routing address is a method used to list a collection of adjacent IP addresses using a simple, shortened fashion making it easier to use in whitelists.

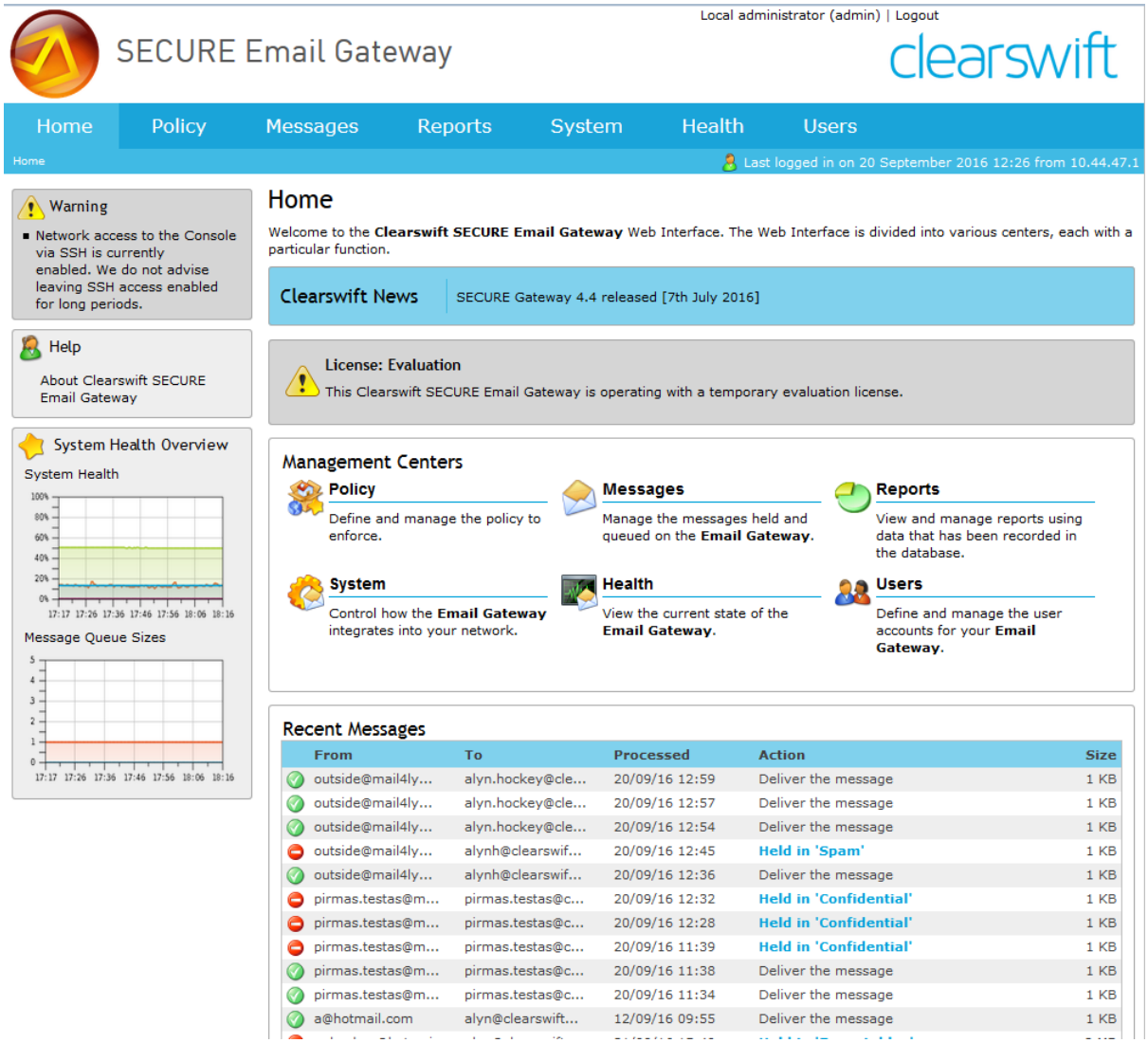
For example the address range 192.168.1.0 to 192.168.1.255 could be represented as 192.168.1.0/24 using CIDR notation which is easier to use.

Newsletter spam option

Newsletters represent a type of message that typically is considered unwanted (spam) for some people but wanted for others. Depending on how companies want to configure their spam detection, if they are happy with this approach they can manage the misclassifications of wanted newsletters using the following instructions:

1. Set Suspected Spam to "Hold in area"
2. Use PMM to manage spam and let users whitelist the newsletters they want to receive

Refreshed User Interface



Available in V4.5 (due November 2016) the UI has been modernised, optimised and all flash objects have been removed.

These changes make the user interface behave more responsively.

Message Processing Enhancements

Adaptive Redaction – Open Office

Support for Data Redaction, Structural Sanitization and Document Sanitization was added to permit searching and remediation of Open Office files formats.

	VBA Macro	Javascript	Vbscript	ActiveX	OO Basic	Python	Beanshell
DocX	y	n/a	n/a	y	n/a	n/a	n/a
PptX	y	n/a	n/a	y	n/a	n/a	n/a
XlsX	y	n/a	n/a	y	n/a	n/a	n/a
HTML	n/a	y	y	y	n/a	n/a	n/a
RTF encoded HTML	n/a	y	y	y	n/a	n/a	n/a
PDF	n/a	y	n/a	y	n/a	n/a	n/a
RTF	n/a	n/a	n/a	y	n/a	n/a	n/a
Calc	n/a	Y	n/a	n/a	Y	Y	Y
Draw	n/a	Y	n/a	n/a	Y	Y	Y
Impress	n/a	Y	n/a	n/a	Y	Y	Y
Writer	n/a	Y	n/a	n/a	Y	Y	Y

Data Redaction – Excel

It is now possible to scan and redact text items in Excel spreadsheets.

Extended range of DLP tokens

Over 90 new tokens have been added to the range of DLP tokens to permit detection of PCI, PII and other useful items in messages such as email address or IP addresses.

Quarantine message in multiple areas

It is now possible to hold a message in multiple message area. Each copy would be independent of the other to allow different administrators to have access and each would be subject to the message areas automatic expiry scheme.

Relay-to rewrite option

When messages are sent to a mail server using a "Relay-to", it is now possible to modify the recipient's domain name. This may be useful for archiving purposes.

External Command

It is possible to extend the capabilities of message processing by allowing customers, partners and System Integrators to write code (or just use a collection of Linux commands) to perform some additional scanning of a message that is not currently possible using a standard SECURE Email Gateway.

For example, you could write an app that looks at image being attached to messages and if it detects a 2D barcode, it could be processed differently (i.e. delivered and sent to an email archive, or sent to a different recipient).

Reprocessing message options

Quarantined Messages can now be reprocessed with a choice of either the original or modified message to see how the message would be re-evaluated again. This is particularly useful when setting up new policies.

By default the message is processed using the same policy route but this can be over-ridden to use a different route.

Address route pairs with the same policy route

A message route is based on a list of senders, recipients and rules. When configured all defined senders can mail to all defined recipients and evaluated against those defined rules.

Depending on your policy this method may require you to have to create multiple routes when there are times when you don't want the risk of all the senders being able to send to all of the recipients. So you would setup a new address route. This has a downside as it makes the policy larger and means a new rule has to be added to multiple routes which introduces the ability for inconsistency.

However it is possible to create a policy route that has multiple route addresses that are isolated, but share the same ruleset.

Outbound Route	
Route Group 1	
Sales, *Marketing*	*Customers*
Route Group 2	
Engineering	*Suppliers*
Rules	
Detect Malware, Check for Confidential Files, Add Disclaimer	

In 3.x the system would merge *Sales*, *Marketing* and *Engineering* to a list of "senders" and match to a combine list of *Customers* and *Supplier* "recipient" addresses.

This may not have the desired effect as it permits *Engineers* to be able to send messages to *Customers*, which may not be permitted.

In 4.5 these lists are used in isolation of their own Routing Groups, which provides the desired level of security and helps to reduce the number of routes required to create a complex policy.

Key Server Enhancements

The latest versions of Gateways supports:

- binary certificates
- provides support to gather certificates from an AD server
- LDAP/S & HTTP/S key retrieval methods

Making the process of using encrypted email simpler.

Networking improvements

Secure protocols

The SEG supports insecure and now secure protocols for allowing the backup and restoration of the system configuration.

The backup/restore and export transaction logs can be transferred to an external source over:

- S/FTP FTP over SSH (TCP 22)
- FTPS (implicit) FTP over SSL (TCP 990)
- FTPS (explicit) FTP over SSL (TCP 21)

The SEG also supports directory server lookups over LDAP/S.

Mandatory TLS support

Mandatory TLS connections are now established bi-directionally as defined and can be defined based on domain name as well as by IP address. Attempts to send/receive without TLS are blocked.

Opportunistic TLS support exceptions

Issues can arise during the TLS handshake which can prevent a connection from being established. It is now possible to offer an exemptions list for sites who claim to support Opportunistic TLS, but repeatedly fail.