clearswift

Product Information Bulletin

Clearswift SECURE Email Gateway 4.2

Issue 1.0

July 2015

Contents

Overview

This new release brings additional security features to the Clearswift SECURE Email Gateway.

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

- Sophos Live Protection
- Secure backup support
- Revised installation and upgrade procedure
- TLS enhancements
- Reporting enhancements
- Network stack hardening
- Processing failure rule priority
- Text analysis results

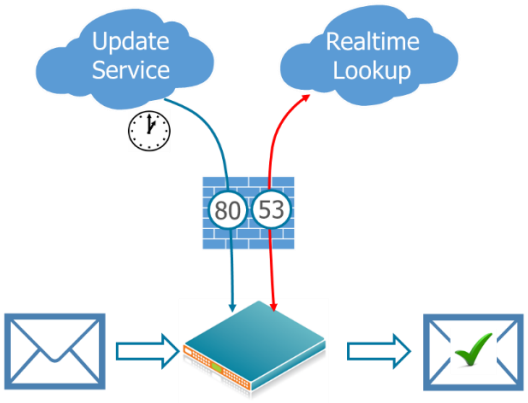
Sophos Live Protection

Key points:

- Reduces the risk of Zero-day threats
- Supplements the standard Anti-virus methods
- No configuration required

As well as receiving updates every 15 minutes, the SEG can utilise a new DNS based lookup service to reduce the window of opportunity between a new virus being analysed by Sophos and the publication time of the latest virus definitions.

If a file is scanned and there is no malware found, a secure DNS lookup is also performed using a hash of the file and if that finds a match then the file will be held as being malicious. If nothing is found then the message and attachments are delivered.



This feature is only available to customers using Sophos AV. Clearswift is looking to release similar functionality with Kaspersky AV in a future release.

Secure backup support

Key points:

- Provides secure method to backup/restore and export
- Wide choice of secure methods

This release allows System Administrators to utilise secure connections to FTP servers for:

1. Backup & Restore
2. Transaction Log export

The enhanced security mode provides support for:

- S/FTP – FTP over SSH
- FTPS (implicit) – FTP over SSL. Implicit SSL mode requires an SSL session to be established between client and server before any data is exchanged over Port 990.
- FTPS (explicit) – FTP over SSL. Explicit SSL mode allows client to optionally switch from unencrypted mode to SSL, typically on Port 21.

As well as standard FTP.

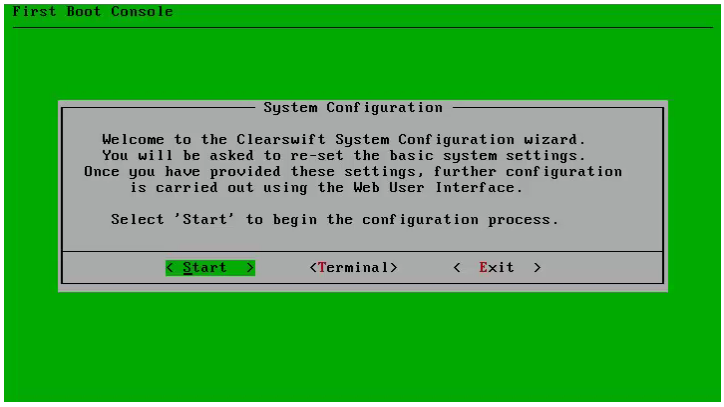
Revised Installation and Upgrade Process

Key points:

- Simplifies the installation process
- More flexibility to apply OS updates without waiting for a product update
- More information about updates available from the product UI

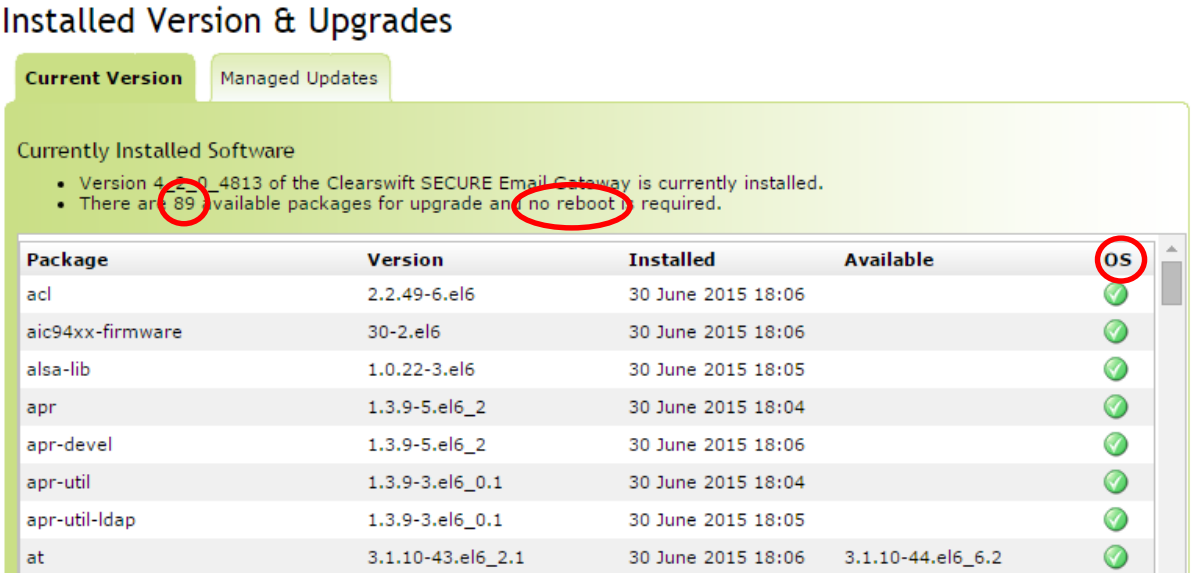
The installation process has been simplified to provide a more streamlined installation process.

Booting the standard Clearswift ISO starts the process to install Red Hat 6.6 and the Gateway. With 4.2 the packages are installed without questions which are now deferred to the installation wizard where the hostname, IP, timezone and locale are all defined before the rest of the configuration settings are defined.

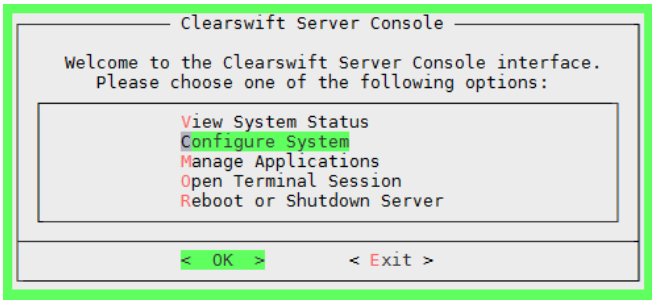


In this release, the system will automatically poll for updates to both operating system and application. These are displayed in the "Installed Version and Updates" in the System Center.

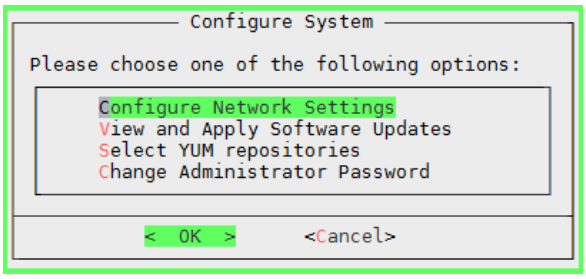
The system shows which packages have updates, which ones are OS updates, total number of updates and whether a reboot is required.



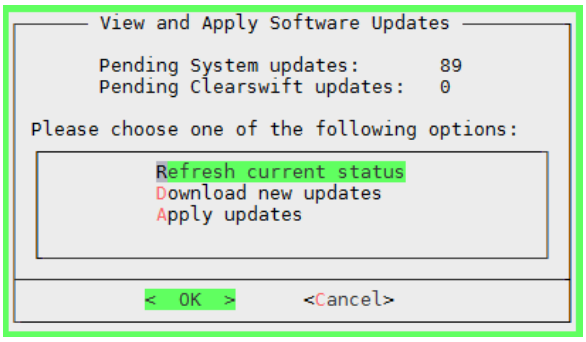
In order to apply the packages, you would still use the Admin console via "Configure System".



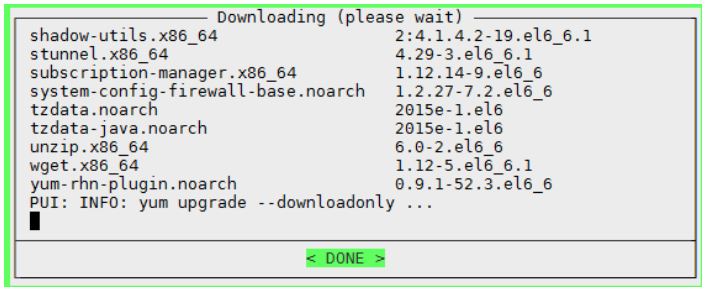
Select "View and Apply Software Updates".



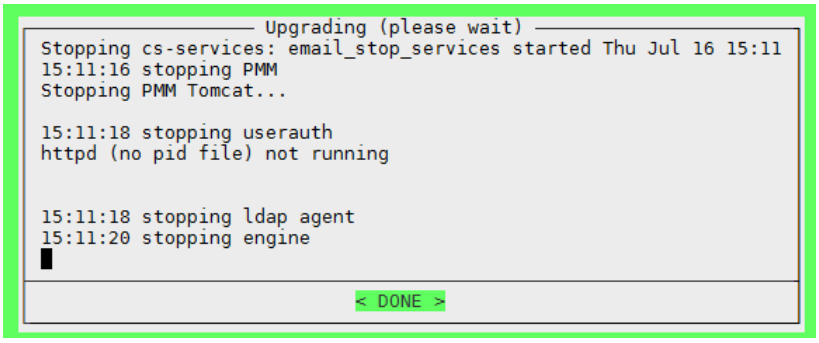
It is also possible to force an update check using "Refresh Current Status".



The new updates can be fetched by "Download new updates".



Applying the outstanding packages can be performed at the administrator's convenience by using the "Apply updates".



Once completed the system may require a reboot as per the "Installed Versions and Updates" page.

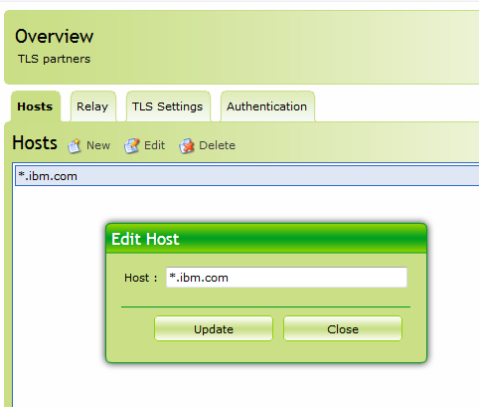
Upgrading from 4.1 to 4.2 is a similar process, whereby a 4.1 customer will download the updates from either the network repositories, or a local DVD based repository and will then apply the updates from the console.

TLS enhancements

Key points:

- Enhances TLS capabilities
- Simplifies secure message configuration
- Support for domain and sub-domains

It is now possible to create TLS endpoints that encapsulate a domain and any sub-domains of that organization. This is achieved by using a wildcard prefix on the domain name to support the parent and any sub-domains.



Reporting changes

Key points:

- Available for customers with Adaptive Redaction features
- Summary of redaction and sanitization events over a time period
- Drill down options to view message detail

If the customer has any of the Adaptive Redaction features licensed, another report category is available in the Report Center. The "Remediation" category provides a report on how many messages have been automatically modified to make them acceptable to the security policy.

This report does allow drill down by either redaction or sanitization to show individual senders and recipients whose messages have been modified.

Network stack hardening

Key points:

- Reduces the chance for system exploitation

Various network parameters have been set to match security best practice and vulnerabilities occasionally found by certain network penetration tools.

Processing failure rule prioritization

Key points:

- Customers can now define what failures take priorities
- Eliminates issues where malware could be quarantined in the wrong quarantine area
- Covers Malware, Spam and Encryption failure scenarios

In previous versions of product, if a message had 2 attachments where one attachment was corrupted and the other attachment was found to have a virus, then the message processing failure rule would determine the disposal for this message. We are aware that some customers allow end-users to release these messages and the risk is that they may release a message that contains malware.

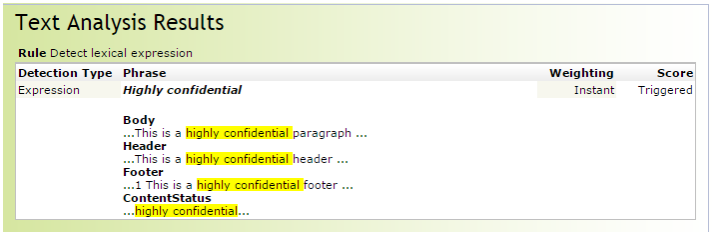
In 4.2 the priority order of policy rules in the content route now determines what happens when a message has both bad data and malware. So the previous example would follow the "Virus" rule.

Text analysis results

Key points:

- Provides more feedback where keywords were found in messages and their attachments

When checking a held message in the message center, the UI now provides information showing where in the message and attachments the detected text was found.



Enhancement requests

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

ER#	Summary
MAIL-7077	Support the use of wildcards on domain names for TLS Connections
MAIL-4305	Network Stack Hardening
MAIL-741	Appliance does not detect virus content in Message Processing Failure message
MAIL-648	Backup/restore option to use SFTP

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	28th July 2015

Interoperability

The Version 4.2 Gateway can be peered with existing Version 3.x Gateways where it will be possible to share some of the management capabilities such as message management and reporting.

It will be possible to import a 3.8 configuration into a V4.2 system thus saving deploying a V4.0 (or 4.1) and then upgrading that to V4.2.

However, due to the changes in the underlying functionality it will not be possible to create a peer group of V3 and V4 servers with a consistent policy defined on a single peer therefore any change made that affects the V3 peers will have to be replicated on the V4 servers.

End of life

This release will signal the start of both SEG 3.7 and SEG 4.0 end of life programs. They will last 12 months (as defined in the Support Services handbook) and both versions will reach their end of life on 31st July 2016.

SEG Version 3.8 will be unaffected by this release.

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.

Clients using 4.0/4.1 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.