clearswift

Product Information Bulletin

Clearswift SECURE ICAP Gateway v4.4

Version 01

05/07/2016

Copyright

Version 1.0, July, 2016

Published by Clearswift Ltd.

Contents

1 Overview

This new release of the SECURE ICAP Gateway brings several enhancements to the product as well as a number of security features.

The additional features included in this release of the SECURE ICAP Gateway are listed below:

- Transaction log improvements
- Extended detection of potentially malicious files
- System password strength
- System console upgrades

2 Transaction Logs improvement

Key points:

- Additional information related server responses
- Includes reference to the triggered policy

The SECURE ICAP Gateway includes an option to generate a log of the transactions processed by the Gateway. This log is generally only used when clients need to analyze information with external tools instead of using the on-box reporting engine.

The transaction log includes, amongst others, information on the user that made the request, the destination of the request, the total size of information being uploaded and downloaded. In this release, the following additional information has been added to the transaction log:

- x-result: Result of applying the policy, which could be "allowed" or "blocked"
- x-destination: IP address of the web server. This field is included for consistency with the SECURE Web Gateway, but as the SECURE ICAP Gateway doesn't access the destination server, it will always be empty.
- x-rule: Unique ID of the content rule triggered, if any, as a result of enforcing the policy
- x-route: Unique ID of the web policy route selected by the engine to analyze the transaction

Additionally, the sc-status field has been modified to show the response from the web server if the result of applying the policy, shown in the x-result field, is to allow the traffic. In case of blocking the traffic, the proxy response is provided.

The transaction log file follows the W3C extended log file format standard to simplify the integration with third party tools. However, that restricts the contents of the file to single byte characters.

```
#Version: 1.0
#Software: Clearswift SECURE ICAP Gateway
#Fields: date  time    sc-status      x-req-size     bytes   c-ip    c-dns   s-ip    x-category
       x-user  x-remoteuser   x-result       x-destination  x-rule  x-route cs-uri
2016-07-14     12:33:06       0       439     0       192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/static/adaptive-
redaction/dr/index.html
2016-07-14     12:33:06       200     0       1666    192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/static/adaptive-
redaction/dr/index.html
2016-07-14     12:33:06       0       470     0       192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/static/adaptive-
redaction/dr/style.css
2016-07-14     12:33:06       200     0       1940    192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/static/adaptive-
redaction/dr/style.css
2016-07-14     12:33:07       0       459     0       192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/static/adaptive-
redaction/dr/RedactAll.jpg
2016-07-14     12:33:07       200     0       40580   192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/static/adaptive-
redaction/dr/RedactAll.jpg
2016-07-14     12:33:07       0       411     0       192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/favicon.ico
2016-07-14     12:33:07       200     0       7756    192.168.250.1   -
       "'Technology & Telecommunication'"    "-"     false   allowed 0.0.0.0 -       58486c7d-
5f19-4f0b-811d-f3ba2cd57526   https://www.clearswift.com/favicon.ico
```

3 Script and malware detection enhancements

Key points:

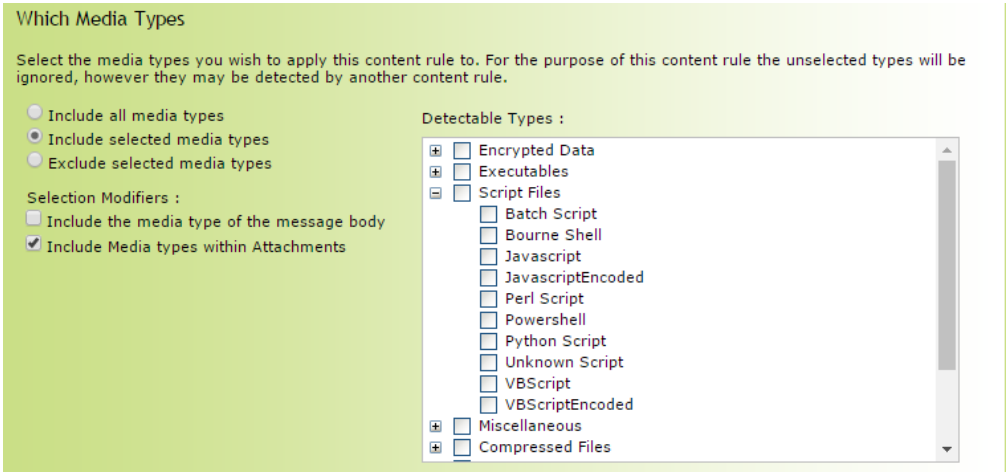
- Recognition of new script formats
- Support for MSO files
- Scan scripts using Detect Lexical Expression

Malware, especially ransomware and spyware, has been actively spreading through the use of standard data types with active content on them. Once the content is opened, an action is triggered that will either download or activate the malicious payload.

To prevent those threats from hitting organizations, Clearswift keeps improving the detection and remediation techniques of the deep content inspection engine. In this release, there have been a number of enhancements regarding active code detection

in MS Office formats, including the addition to the undocumented MSO data type to the supported data types.

Additionally, the Gateways now recognise more file formats to prevent malicious scripts from getting into organizations. The detect media types content rule has been extended to display the new specific script formats.



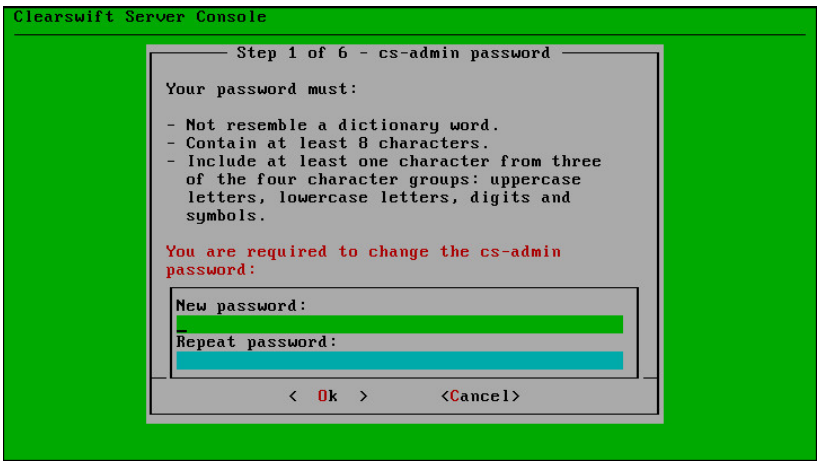
4 Strong admin password

Key points:

- Strong password strength policy applied to all new installations
- Not implemented for software installs (when the product is installed on an existing RHEL deployment)
- The feature can be disabled if not required
- Can be enabled for customers upgrading from an earlier version

During the installation process, you are asked to setup the console UI admin password. In this release, a strong password policy is enforced to ensure the chances of the password being guessed are highly reduced.

Although it is possible to disable this feature after the initial installation, Clearswift strongly recommends the use of strong passwords for system and administration accounts.



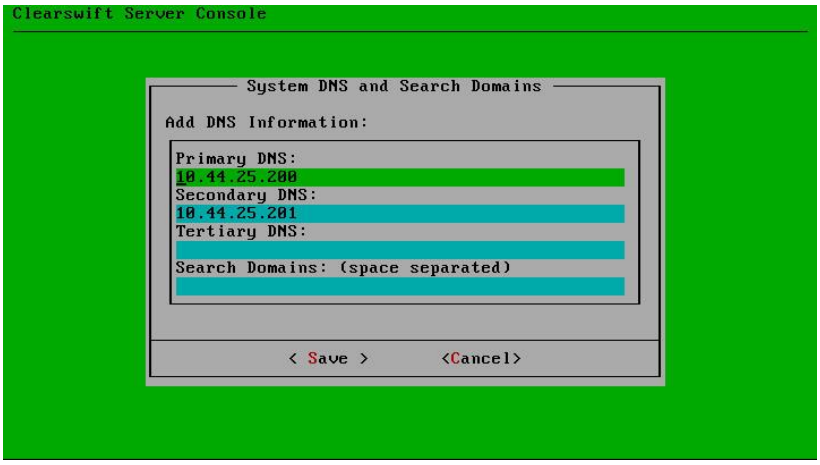
If you wish to disable an installed system or enable on an upgraded system, please see the online help article:
http://clearswifthelp.clearswift.com/SWG/440/en/SWG.htm#Sections/ConceptTopics/CONCEPTPasswordPolicyManualChange.htm

5 System console changes

Key points:

- Improved DNS servers
- Tagged interfaces

The system console has been improved in this release in the data validation and usability areas. In particular, fulfilling the DNS server configuration has been made easier and interfaces are now annotated, making identification easier.



6 Enhancement requests

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

ER #	Summary
WEB-3778	Ability to show In the transaction logs, when a site has been blocked by policy.

7 Fixed issues

A number of client reported issues have been fixed in his release. Please see the release notes for more information.

8 Availability

Phase	Date
General Availability	5th July 2016

9 Interoperability

The Clearswift SECURE ICAP Gateway 4.4 can be peered with existing version 3.2.8 ICAP Gateways to share reporting between both systems. Due to changes to the policy between both versions, it won't be possible to share policies between both versions, though.

It is also possible to import the configuration and backup from a SECURE ICAP Gateway 3.2.8 directly into the version 4.4 of the Gateway to simplify the migration to the newest version.

The version 4.4 of the SECURE ICAP Gateway can also be peered with the Information Governance Server version 1.2 and version 1.3.

10 End of life

The availability of this release will not start the end of life program of any older version of the SECURE ICAP Gateway.

11 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 6GB RAM, multi-core

processors that support 64-bit instructions and over 250GB of disk space for low volume production environments. For customers with a greater workload the recommended minimum would be 8-16GB RAM, dual multi-core (at least quad-core) processors and 250GB of redundant disk storage with a performance similar to 15k rpm SAS drives.

12 Packaging

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

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 v3.2.8 policy file to replicate their policy or a v3.2.8 full system backup if they want to import reporting data, 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.