clearswift

Frequently Asked Questions

Clearswift SECURE ICAP Gateway v4.2

Version 01

30/07/2015

Copyright

Contents

What is the SECURE ICAP Gateway?

The Clearswift SECURE ICAP Gateway provides deep content inspection features to ICAP clients to extend the functionality of your existing web security platform.

The Clearswift content inspection engine's unique features allow you to create an effective and accurate Data Loss Prevention policy for browsing traffic from your users or to your corporate servers.

The Gateway provides the following key functionality:

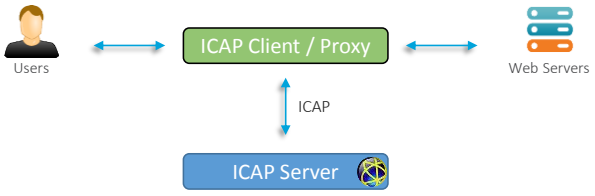
- Clearswift deep content inspection
- Recursive decomposition
- True file type detection
- Lexical expression detection
- Structured and unstructured data detection
- Token detection
- Adaptive redaction[1]
- Information Governance server integration[1]
- URL database
- Anti-malware engine[1]

The full details of the product can be checked in the SECURE ICAP Gateway datasheet.

What is ICAP?

The Internet Content Adaptation Protocol or ICAP is a protocol that was initially developed to offload inspection from existing proxy servers. In an ICAP deployment, there are two elements: an ICAP client and an ICAP server.

The ICAP client sends content to be inspected to the ICAP server, which can respond by accepting the content unmodified, block it or modify the content.



The SECURE ICAP Gateway is an ICAP Server, as it receives the content to be inspected from existing poxy devices.

[1] Cost option

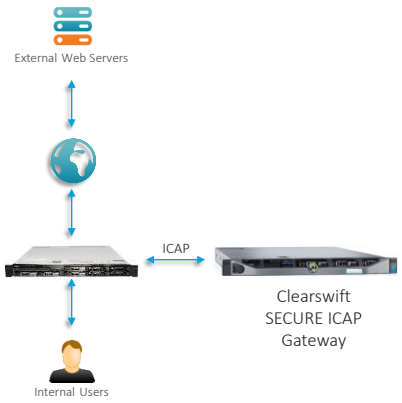
Which products can the SECURE ICAP Gateway be integrated with?

The Clearswift SECURE ICAP Gateway can be integrated with any ICAP compatible ICAP client. The officially supported products are Blue Coat ProxySG, F5 BIG-IP LTM and Squid Proxy.

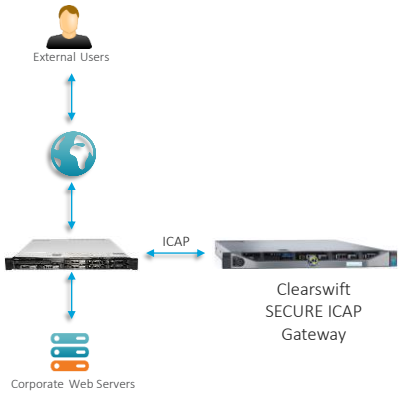
Can the SECURE ICAP Gateway be deployed alongside a forward or reverse proxy?

Yes. The SECURE ICAP Gateway will receive the content to be inspected from an existing proxy, regardless of whether it is a forward or a reverse proxy.

In a forward proxy deployment the aim is to enforce the security policy to browsing traffic.



When the SECURE ICAP Gateway is deployed in a reverse proxy infrastructure, it protects the information exposed through the corporate webservers as well as the content being uploaded to them.



Can several SECURE ICAP Gateways run as a group?

Yes. Several instances of the SECURE ICAP Gateway can be deployed and peered together. One or more ICAP clients will then be able to share the load between the different SECURE ICAP Gateways to provide load balancing and high availability.

From an administration perspective, a peer group of ICAP Gateways can be created to unify the management and reporting through the platform.

What can the Clearswift deep content inspection engine do?

Clearswift's award winning Content Inspection Engine is able to decompose the communication flow recursively to identify and understand its contents.

The engine is capable of performing true data type detection to identify more than 180 different data types, even if they are embedded, renamed, or obfuscated.

It is also able to extract the information from within the data type and analyze it against managed or user created expression lists. These expressions might contain simple words or phrases, regular expressions, or even tokens like credit cards or social security numbers where checksums must be generated to validate them.

Structured data sources like databases usually contain critical information such as customers' contact information. The content inspection engine can be fed with information from these sources to look for it in the communication flow. As a result, an accurate detection is performed to protect your critical information.

Can the SECURE ICAP Gateway inspect HTTPS traffic?

Yes. HTTPS traffic inspection needs to be enabled proxy device. Then, it will redirect the decrypted traffic to the Clearswift SECURE ICAP Gateway for inspection.

Does the SECURE ICAP Gateway provide URL filters?

Yes. The Clearswift SECURE ICAP Gateway includes a URL database that can be used to perform URL filtering of web browsing traffic.

Within the categories included in the product there are security risk related ones which act as an additional layer of threat protection.

It must be noted though that a URL database is often present within the proxy device. In this case, it should be decided by the administrator where these filters are to be applied to reduce administration overlap.

Does the SECURE ICAP Gateway provide anti-malware engines?

Yes, as an additional option. Clearswift SECURE ICAP Gateway clients can choose between Kaspersky or Sophos anti-malware engines.

Can the SECURE ICAP Gateway apply Adaptive Redaction?

Yes, as an additional option. The Clearswift SECURE ICAP Gateway contains the Clearswift Content Inspection engine, so all the common features of it are available in the product. This includes the ones applicable in a web environment:

- Data Redaction
- Document Sanitization
- Structural Sanitization

What does Data Redaction do?

Data Redaction is the process of looking for words, phrases or tokens in a piece of textual data and replacing the detected text items with an asterisk character. So if the keywords to redact were "fox" and "dog", we would have the phrase:

> "The quick brown *** jumped over the lazy ***."

This process can help to reduce the chance of data leakage.

What does Document Sanitization do?

Document Sanitization looks at the documents and detects meta data held as document properties or change tracking and allows a client to remove either or both of these elements.

This process can help to reduce the chance of data leakage.

What does Structural Sanitization do?

Structural Sanitization is inspecting the documents for potential active code such as macros, scripts and embedded objects and will remove them from the file/message/webpage. This can help protect clients from Advanced Persistent Threats (APT) as they often use common file formats to embed the malicious payload as active content.

What file formats are supported by these features?

The following table defines what formats are supported by each feature.

Format	Structural Sanitization	Document Sanitization	Data Redaction
HTML	Yes	N/A	Yes
XML	N/A	N/A	Unsupported in 4.0
Microsoft Office 97-2003	Detection only, therefore On Unsuccessful Action Triggered	Detection only, therefore On Unsuccessful Action Triggered	Detection only, therefore On Unsuccessful Action Triggered
Microsoft Office 2007+	Yes	Yes	Yes
Open Office	Yes	Yes	Yes
PDF	Yes	Yes	Yes
RTF	Yes	Unsupported in 4.0	Yes
RTF Encoded HTML	Yes	Unsupported in 4.0	Yes

How are these features licensed?

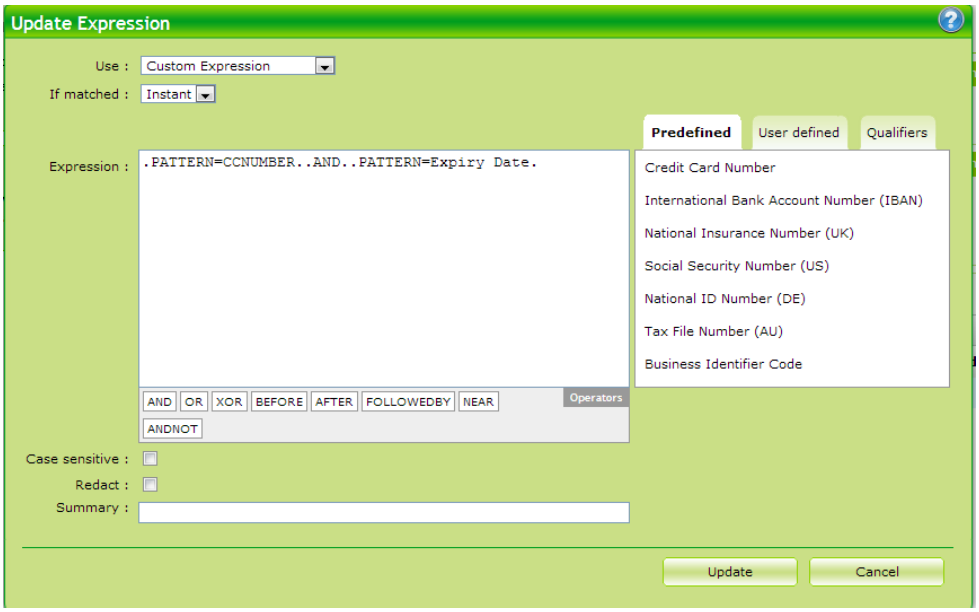
Each feature is charged for separately. There is a discount if a client purchases all three of the Data Redaction + Document Sanitization + Structural Sanitization options.

Where can I find out more about the Adaptive Redaction features?

There is a separate FAQ for these features and datasheets are available. Please check our website for more information:
http://www.clearswift.com/solutions/adaptive-redaction

What are custom tokens?

The Gateway is delivered with a number of predefined tokens to help detect common data types such as credit card and social security numbers. However clients may have specific data types that might be appropriate for their environment such as "Part Number" or "Patient Number". The custom token features allow a client to build up a list of tokens that they use and be able to incorporate them in keyword searches.



In this example we have defined an "Expiry Date" using a regular expression of

[0-9]{2}/[0-9]{2}\s

to find a format of mm/yy to assist our keyword search to find credit card details in some piece of data.