clearswift
A HelpSystems Company

Inter Engineering®
World of Data Security!

Critical Information Protection using F5 BIG-IP Local Traffic Manager and Clearswift SECURE ICAP Gateway.

SECURE ICAP Gateway

Clearswift technology provides the ability to dissect communication flows and inspect content to identify threats like viruses and scripts or detect critical information and perform the appropriate mitigation actions as defined by the organizations corporate compliance policies. The SECURE ICAP Gateway technology has been developed to utilize the industry ICAP protocol interface, enabling advanced content inspection and adaptive redaction.

Content Inspection

SECURE ICAP Gateway can apply hygiene policies to clean Internet traffic of un-wanted or malicious content like dangerous file types, tracking cookies and malware. Examples of this type of threat include virus infections and Internet email/social media message attachments that could execute potentially damaging payloads. SECURE ICAP Gateway can use two different antivirus engines for malware checking to ensure accurate detection.

Adaptive Redaction

Adaptive Redaction removes the compliance burden on organizations by deleting only the non-compliant information from being shared, allowing the rest of the information to continue without disruption and false positives.

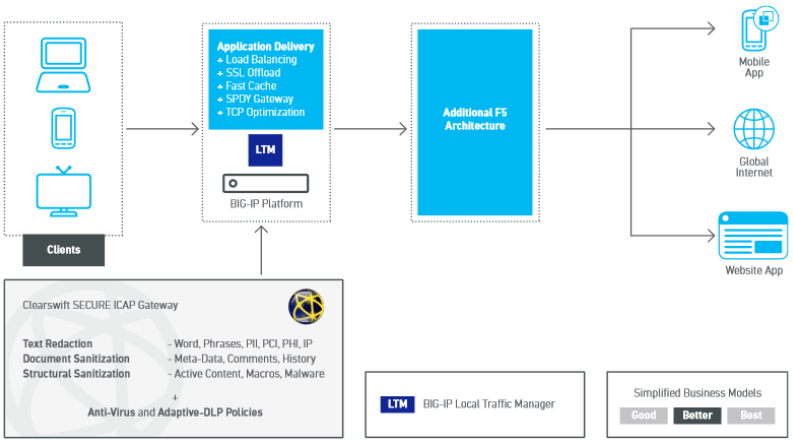
Structural sanitization detects and removes potential threats like scripts, macros, embedded executables and other active content items that are included in files like Word, Excel, PowerPoint, PDF etc.

Data Redaction removes sensitive content or details from a document. The textual analyzer can search for terms, patterns (Credit Cards, PII etc.), custom regular expressions or even information from internal databases.

Document Sanitization will automatically remove from office documents hidden data that could be sensitive. This could be the document properties, which can disclose both the author and the true date of the document; or change histories, which can leak sensitive data that the author or authors believe they have removed – such as project details, new product names and prices.

Products Integration

The SECURE ICAP Gateway can be installed in environments where BIG-IP LTM is already in place or in new deployments. Both appliances communicate using the ICAP protocol (https://tools.ietf.org/html/rfc3507). BIG-IP LTM sends to SECURE ICAP Gateway HTTP requests from clients or HTTP responses from web servers, all of which are analyzed by the ICAP Gateway according to configurable content rules.



Use Cases

Internal users browsing

With the SECURE ICAP Gateway the organization can enforce policies for internal users regarding:

Inbound threat protection with Kaspersky or/and Sophos antimalware and antispyware protection.

Flexible Web2.0 policy controls for social media, allowing policies to be defined according to each website's content and features (eg allow specific YouTube and block all others).

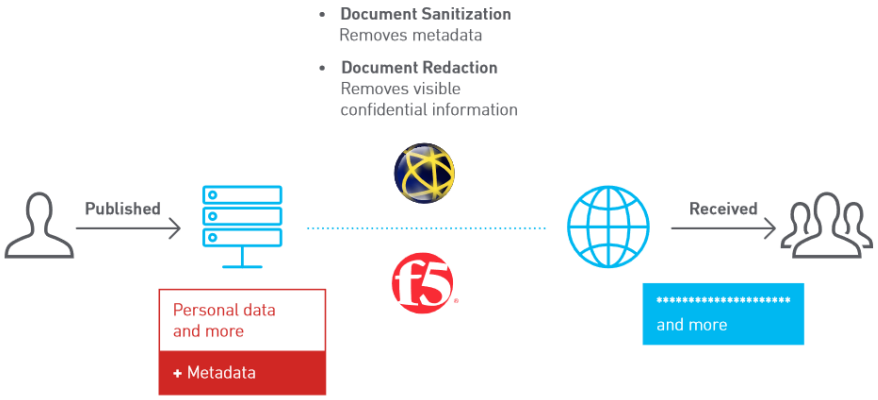
Advanced URL filtering that controls access to sites according to their categorization. URL categories include security risks covering malicious malware and phishing categories, which are continuously updated to provide additional security protection.

Protecting published content

Any piece of information that is published on a website, regardless of whether it is done in a password protected area only for certain partners or as publicly available content, is a potential egress point. This means that information should be analyzed and the corporate security policy applied. Human errors, like publishing the wrong file, can easily lead to data losses.

Also hidden information in the form of metadata is hardly ever removed before content is published which means that usernames, internal servers and even allegedly removed information can be accessed by externals.

BIG-IP LTM optimizes the delivery of applications. When deployed together with the Clearswift SECURE ICAP Gateway and its Adaptive Redaction technology, it can modify the content as it is delivered to remove confidential information and hidden metadata.



About Inter Engineering

Inter Engineering is a value added distributor dedicated to the provision of Data Security solutions and services internationally.
With a track record of over 20 years and focus on technical expertise the company is one of Clearswift's most competent partners. Focused cooperation with a channel of well educated reselling partners guarantees local competence over the whole territory.

Contact Details

+30-2410-670-030
sales@inter-datasecurity.com
www.inter-datasecurity.com

About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Its unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at www.clearswift.com