Clearswift and Blue Coat Integration

The need to protect critical information is beyond any discussion. Advanced threats are commonly found striking enterprises and generating important information losses that are hard to quantify. At the same time, regulations are becoming stricter and imply larger fines in case of breaches. Most of these leaks happen through the Internet gateways, hidden as common data types or standard browsing traffic. Unfortunately, many companies take the approach of only using basic web browsing filters and antimalware engines. Whilst this might cover simple security needs, there is a necessity to take control and act to remediate critical information losses. Clearswift and Blue Coat have partnered together to provide a highly scalable web security platform able to not only detect information security issues, but also to transparently solve them before the loss happens.

The CISO Paradox

During the last years there has been a great evolution on how companies deal with information. The explosion of new communication means - like Web2.0 and mobile devices - and the push to collaboration with partners or customers have increased by orders of magnitude the amount of information being communicated. There has been an important shift from information being a cost to being a valuable asset for business to grow.

At the same time, regulations have been focused on protecting information with increasing impact in case of losses.

However, the security teams have hardly been increased in size and struggle to implement the appropriate information security measures. Migrating platforms is painful, but the existing ones could not be covering all the needs.

The Clearswift and Blue Coat integration

Having the need to widen the advanced threat protection strategy to be able to also accurately identify critical information, Blue Coat and Clearswift have worked together to provide a combined solution that deals with this issues.

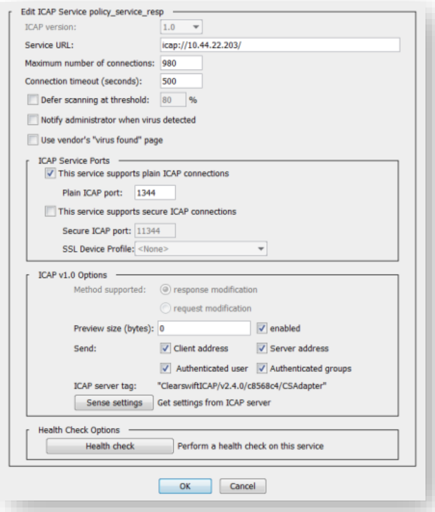
The resulting platform takes advantage of the perfect match between both technologies to provide some key unique features:

- Complete protection and control, as even SSL connections are decrypted and inspected
- Layered defenses for a complete protection
- Deep content inspection to identify even the smallest piece of information
- Adaptive Redaction to modify the requests and responses to prevent data losses and targeted attacks from hitting the company

The deployment is greatly simplified by using ICAP, which allows deciding by policy which content, from/to which user and to/from which site, needs to be inspected.

This is a well-known integration method for Blue Coat administrators and requires just three simple steps:

- Configure the ICAP service groups in Blue Coat ProxySG:



Edit ICAP Service policy_service_resp

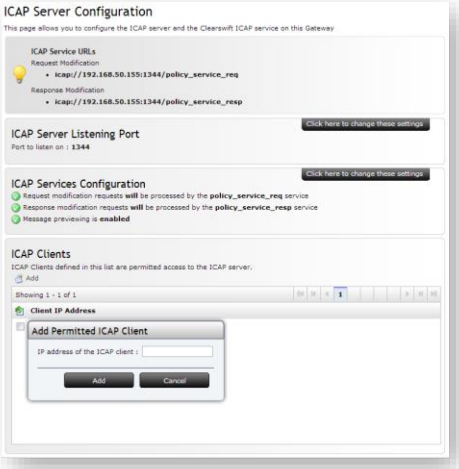
ICAP version: 1.0
Service URL: icap://10.44.22.203/
Maximum number of connections: 980
Connection timeout (seconds): 500
□ Defer scanning at threshold: 80 %
□ Notify administrator when virus detected
□ Use vendor's "virus found" page

ICAP Service Ports
☑ This service supports plain ICAP connections
Plain ICAP port: 1344
□ This service supports secure ICAP connections
Secure ICAP port: 11344
SSL Device Profile: <None>

ICAP v1.0 Options
Method supported: ● response modification ○ request modification
Preview size (bytes): 0 ☑ enabled
Send: ☑ Client address ☑ Server address ☑ Authenticated user ☑ Authenticated groups
ICAP server tag: "ClearswiftICAP/v2.4.0/c8568c4/CSAdapter"

Sense settings
Get settings from ICAP server
Health Check Options
Health check
Perform a health check on this service
OK
Cancel

- Set the policy to redirect specific traffic to the Clearswift ICAP Gateway for inspection
- Configure the Clearswift ICAP Gateway to accept connections from the Blue Coat ProxySG:



ICAP Server Configuration

This page allows you to configure the ICAP server and the Clearswift ICAP service on this Gateway

ICAP Service URLs
Request Modification
- icap://192.168.50.155:1344/policy_service_req

Response Modification
- icap://192.168.50.155:1344/policy_service_resp

ICAP Server Listening Port
Port to listen on : 1344

ICAP Services Configuration
Request modification requests **will** be processed by the **policy_service_req** service
Response modification requests **will** be processed by the **policy_service_resp** service
Message previewing is **enabled**

ICAP Clients
ICAP Clients defined in this list are permitted access to the ICAP server.
Showing 1 - 1 of 1
Client IP Address

Add Permitted ICAP Client
IP address of the ICAP client :

Click here to change these settings
Click here to change these settings
Add
1
Add
Cancel

Once the integration is done, the inspection policy can be configured in the SECURE ICAP Gateway.

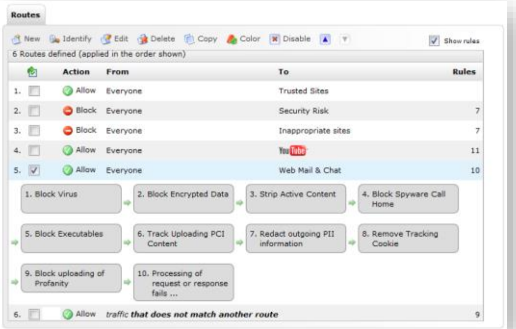
Clearswift Technology Overview

Clearswift's award winning deep content inspection technology can recursively decompose the communication flows to granularly apply information security policies.

The SECURE ICAP Gateway can perform true data type detection even with embedded objects. Once identified, the information in them is extracted and analyzed to detect potential o verified data losses.

In order to simplify the definition of the content security policy, predefined templates with common dictionaries are provided. The ability to detect tokens, like credit card numbers, and to get content from structured data sources – such as databases – makes it even simpler to determine the nature of the information and to drastically reduce the number of false positives.

Blocking violations is the first approach that companies tend to think of when talking about data losses. Even though this might be valid in some cases, Clearswift introduces technology to modify the content to remove the offending content while allowing the rest of the communication to happen. Even hidden meta-data which might contain revision history or quick save data is stripped off. Business processes are not stopped and the critical information is protected.



Routes

6 Routes defined (applied in the order shown)

		Action	From	To	Rules
1.	□	Allow	Everyone	Trusted Sites	
2.	□	Block	Everyone	Security Risk	7
3.	□	Block	Everyone	Inappropriate sites	7
4.	□	Allow	Everyone	YouTube	11
5.	☑	Allow	Everyone	Web Mail & Chat	10
6.	□	Allow	*traffic* ***that does not match another route***		9

1. Block Virus
2. Block Encrypted Data
3. Strip Active Content
4. Block Spyware Call Home
5. Block Executables
6. Track Uploading PCI Content
7. Redact outgoing PII information
8. Remove Tracking Cookie
9. Block uploading of Profanity
10. Processing of request or response fails ...

The ability to make changes on the fly is applicable for both incoming and outgoing content and is not limited to removing data. Advanced and persistent threats can also be removed from their common infection vectors with the active content removal feature.

Blue Coat Technology Overview

The Blue Coat ProxySG is the worldwide leader web security platform. Its modular architecture allows achieving great scalability and a suited solution in many different environments.

Its unique combination of bandwidth optimization and layered and extensible security permits it to be complemented with specialized companies to achieve the best available security platform.

About Blue Coat

Blue Coat empowers enterprises to safely and securely choose the best applications, services, devices, data sources, and content the world has to offer, so they can create, communicate, collaborate, innovate, execute, compete and win in their markets. Blue Coat has a long history of protecting organizations, their data and their employees and is the trusted brand to 15,000 customers worldwide, including 86 percent of the FORTUNE Global 500. With a robust portfolio of intellectual property anchored by more than 200 patents and patents pending, the company continues to drive innovations that assure business continuity, agility and governance.

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.