FORTRA

DATASHEET *(Clearswift)*

Secure ICAP Gateway

BlueFinch ESBD

Optimized Data Security for Web Proxy Infrastructures and MFT

As part of an all-encompassing data security strategy, organizations need to secure and protect content that is uploaded or downloaded from the web or shared via managed file transfer (MFT) solutions.

The Secure ICAP Gateway complements existing web proxy infrastructures and MFT software to provide an added layer of data security. A deep content inspection engine detects sensitive or critical data, active and malicious threats and then applies the appropriate remedial action, allowing safe content to flow through and reducing business disruption.

The Secure ICAP Gateway is deployed by organizations in defense, financial, government and healthcare industries who need to ensure their data security policies are consistent over all channels. This fully automated solution keeps internet data safe and secure, underpinning compliance requirements and avoiding unwanted data breaches.

ICAP Integration

The SECUREICAP Gateway has been developed using the industry standard ICAP protocol interface, bringing enhanced data loss prevention (DLP) and threat protection capabilities to existing web proxy gateways supporting ICAP, such as F5, Blue Coat, Cisco, and Squid. The product is integrated very easily, with no disruption to the current infrastructure.

MFT Integration

Minimize the data security risk of content flowing through managed file transfer solutions by integrating the Secure ICAP Gateway with GoAnywhere MFT. The combined solution provides a secure document sharing platform that monitors, blocks, redacts or sanitizes content depending on organizational policy, ensuring the content is appropriate for the recipient and free from cyber-threats.

PRODUCT SUMMARY

KEY FEATURES

- Integrates with existing ICAP-supporting infrastructures
- Forward and reverse proxy modes protects users and web servers
- Threat protection and sanitization to combat malware and phishing
- Bi-directional data redaction in document and images ensures compliance
- Granular policies control access to websites and cloud apps
- Monitor mode enables policies to be fine-tuned before enforcement

SYSTEM MANAGEMENT

- Flexible and granular policy control
- Active directory or LDAP integration
- Easy to use web-based management interface with role-based access control
- Comprehensive workflow options
- SNMP and SMTP management alerts

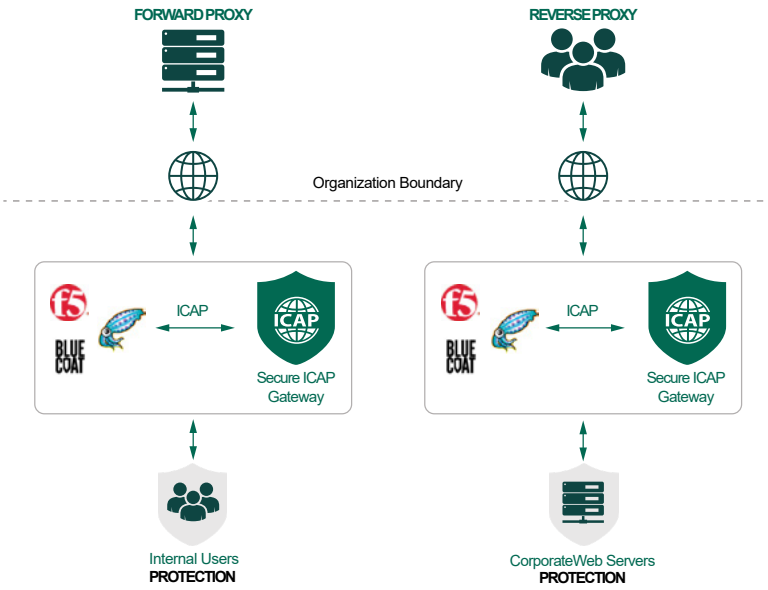
DEPLOYMENT OPTIONS

- Public cloud deployment on Microsoft Azure or Amazon Web Services
- Virtual VMware environment
- Software image on own or packaged hardware

BlueFinch ESBD Netherlands: +31 (0)8 82 58 33 46 France: +33 (0)9 70 75 61 13 www.bluefinch-esbd.com sales@bluefinch-esbd.com

Real-World Deployment

Some DLP tools are complex to manage and deploy, resulting in a high number of inaccurate policy violations. The Secure ICAP Gateway manages these operational concerns with advanced, bi-directional features that restrict the sharing of unauthorized data, while minimizing the false positives that can restrict business productivity. Connection to external data sources and lexical expression qualifiers allow the Secure ICAP Gateway to accurately identify real data loss possibilities before breaches occur.



Flexible and granular policies permit different workflows to be triggered depending on the violation. Content can be dynamically modified in real time allowing for continuous and compliant collaboration. Built in compliance dictionaries and over 200 pre-defined PCI and PII tokens help to simplify policy definition and maintain compliance.

The Secure ICAP Gateway operates in both forward and reverse proxy mode providing comprehensive protection for both inbound and outbound activity.

Deep Content Inspection

A deep content inspection (DCI) engine fully disassembles the communication flow in real time and applies the appropriate policy depending the content, context and required regulation policy. A context-aware scanning capability helps detect and prevent scenarios where users try to upload documents containing Intellectual Property for example to Shadow IT websites or cloud file sharing apps such as Dropbox.

The DCI engine also offers true-file type detection and file structure verification to prevent executable files from being downloaded.

Adaptive Redaction

Rather than block content flowing through the Secure ICAP Gateway, unique Adaptive Redaction features sanitize sensitive or critical data in Microsoft Office, Open Office, PDF and image files in real time, keeping them safe and secure.

Data Redaction – sensitive data or critical information is automatically removed from documents and images. Text in images is identified using Optical Character Recognition (OCR).

Document and Image Sanitization – metadata, change history and properties are removed from files.

Structural Sanitization – Active code (macros, scripts and Active/X) is removed from common document formats.

Advanced Threat Protection

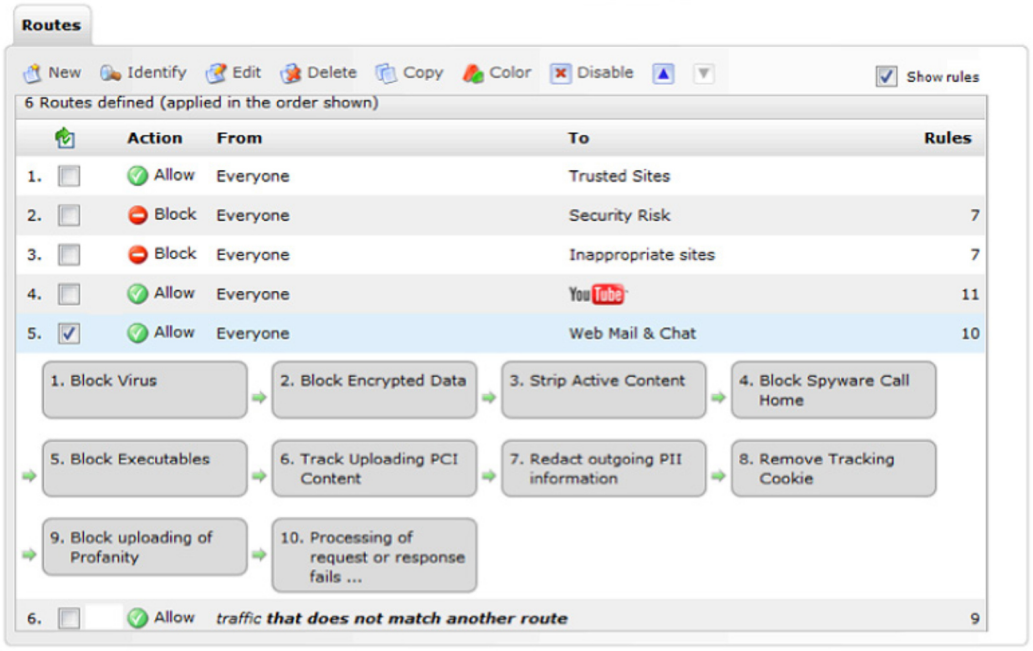
The Secure ICAP Gateway is available with choice of Avira or Sophos anti-malware protection anti-malware protection, that update automatically to provide the latest coverage. These technologies are supplemented by the Structural Sanitization feature that removes active content from documents and websites in real time without any delays.

BlueFinch ESBD Netherlands: +31 (0)8 82 58 33 46 France: +33 (0)9 70 75 61 13 www.bluefinch-esbd.com sales@bluefinch-esbd.com

Users are prevented from accessing websites contained in a URL database, covering millions of websites and billions of webpages. The database details security risk categories, including malicious malware and phishing categories, and is continuously updated to provide additional security protection. Although 50 million new websites are added every year, some sites may remain uncategorized. In this case, a real time categorization engine recognizes the characteristics of inappropriate websites and prevents access.

Controlling Access to Web 2.0

Defining policies for access to popular social media websites is easy. Different access rules can be set at an individual or departmental level and each route comes with pre-populated content rules. For example, you may want to allow access to YouTube, but restrict inappropriate content.



Let's Get Started

See the Secure ICAP Gateway in action. Request a demo at sales@bluefinch-esbd;.com or directly online https://tinyurl.com/SIG-demo