FORTRA™

SOLUTION BRIEF (CYBERSECURITY)

Cross Domain Gateway Filters

Today there is a growing requirement for Cross Domain Solutions (CDS) across internal defence realms, between nations and across the defence information supply chain. While custom hardware is frequently used in the form of a data diode to execute the actual transfer, there is a need to verify and validate the content prior to the transfer.

Business Problem

The need to share information is growing at an almost exponential rate, with requirements for intra- and inter-department sharing, as well as across national boundaries and throughout the defence information supply chain. As the quantity of traffic increases, so too does the requirement that only the correct information be shared with the correct organisations and individuals. Content needs to be inspected, validated, and verified before it is either sent or received into or between the networks. The complexities of validation and verification are best handled with a content filter on the traffic flow which is able to handle the sophisticated policies required, but remains simple to deploy, configure, and administer. While bespoke software was used in the past, cost, and scale have become limiting factors meaning that a commercially viable but functionally capable solution is now the preferred option.

Clearswift's Approach to Cross Domain Filtering

Clearswift has spent more than 20 years securing critical information flowing through digital collaboration channels. The Clearswift family of Secure Gateway products are deployed in some of the largest defence organizations across the globe in some of the most testing environments. The success of these solutions lies in the specialist architecture of the product, the flexibility of the underpinning policy engine and the advanced and extensive Deep Content Inspection engine, which is used to create filtering for Cross Domain Solutions.

Deep Content Inspection (DCI) from Clearswift goes beyond the levels of what is traditionally offered in the market. It is not limited by zip/encryption, file size, analysis timing delays, virtual environment evasion techniques, or multiple embedded document layers. It is designed to offer high detection rates and low impact to minimise false positive rates, a key challenge within information critical environments.

The key advances that the Clearswift approach offers include:

- **DCI,** coupled with document rewrite, can remove both visible and invisible information, as well as active content based on policy. 'Invisible' information, including that hidden in comments, document properties, and revision history creates risk of unauthorised information sharing. While embedded active content in innocuous-looking files can create risk from ransomware and other malware which is activated when the document is opened.
- **Adaptive Data Loss Prevention (A-DLP)** is the non-disruptive removal or transformation of data according to policy (rules), to ensure that information shared complies with prevailing security policies before it is sent to or received by the recipient (person, application, or system).

PRODUCT SUMMARY

Products

- Clearswift Secure ICAP Gateway (SIG)
- Clearswift Secure Web Gateway (SWG)

Professional Services

Consultancy options are available to help with the deployment and configuration of this solution:

- Architecture Design
- Policy Design
- Solution Implementation

Support

Clearswift provides 24x7 global support as standard, with additional options for premium support.

- **Intelligent policy enforcement** is applied to only the information that breaks policy and compliance regulations, while allowing the rest of the document to continue without disruptive false positives. Adaptive DLP also sanitises documents by stripping out hidden metadata (author, username, server names, etc.) and sensitive information that can be harvested and used for targeted attacks. Adaptive DLP modifies the information in real-time according to policies rather than a simple masking, so as to ensure only the acceptable level of information is shared and received, and that sensitive information remains safe at all times.
- **Advanced Threat Protection** is used to detect and automatically strip out active content in the form of embedded malware triggered executables, scripts, or macros in weaponised documents which is then used to extract or hold sensitive data hostage. Clearswift's Advanced Threat Protection sanitises without delay in delivery, as only the active content is removed, allowing the file transfer with full content to continue unhindered.
- **Intuitive interface and comprehensive workflow features** help to eliminate the need for bespoke programs / scripts, single-function tools, and manual processes that were traditionally required.

How does Clearswift Gateway Filtering work?

The diagram below shows one configuration of a web gateway-based filter solution.

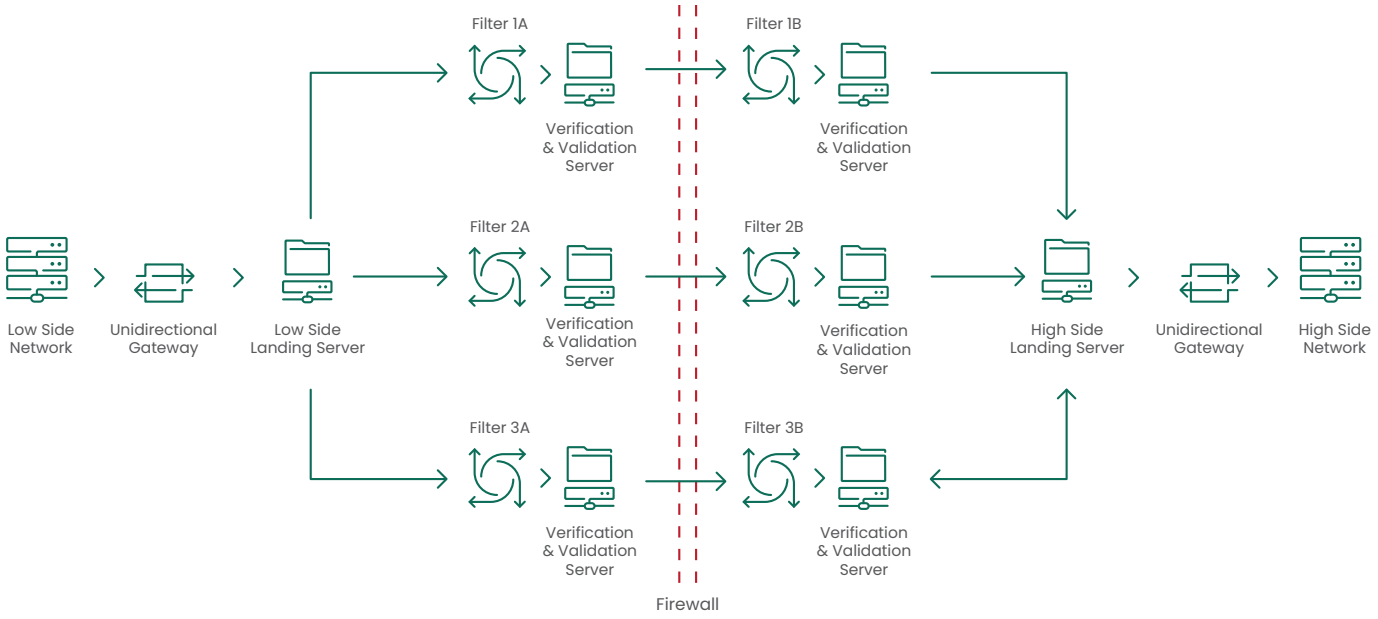


Diagram 1:
Example configuration of Clearswift Gateway Filter.

A "filtering module" within the system is considered to be a dataflow-specific filter, combined with its independent Verification and Validation service.

Data is passed from the low-side network through a unidirectional gateway to the low-side landing server. From the low-side landing server, data as it passes through a specific filtering module. The filtering module performs various checks to inspect and sanitise data as it is passes through and the results are then passed through to its independent Verification and Validation service, which is then passed through a firewall.

Data is then passed from the firewall through a second filtering module which performs various final checks to verify and validate the data. The results are then passed through to the independent verification and validation server, which is then passed through to the high side landing service, and on through another unidirectional gateway to the high-side network.

The Cross Domain Solution has been designed in a modular fashion to allow for scalability, resiliency, and redundancy.

Multiple Network Card Support

The Clearswift Secure Web Gateway (SWG) can be set up and configured with multiple network cards with each network card performing a specific role to ensure dataflow segregation.

This is achieved on the SWG by assigning the gateway 3 separate network cards within the console:

- Inbound traffic is assigned to one NIC, and will only accept traffic from a defined IP Address or IP Range (depending on design requirements)
- Outgoing traffic on another NIC is tied to a defined IP Address specified in the Clearswift Web Route Policy
- The third NIC is configured with a specific IP Address to allow access to the management console and is explicitly defined in the management console

Each network card must be placed in a different subnet to ensure traffic is isolated.

Features

Designed to scale to enterprise deployments, the system provides:

- **Business-level information asset protection:** focused on the asset value, risk profile, and the associated impact of the data associated with it;
- **Secure handling and management:** according to the systems that support the communication of clearly identified sensitive information and granular control to meet policy requirements;
- **Optical Character Recognition:** enables advanced features for dealing with scanned documents;
- **Sophisticated anti-steganography features:** prevent malicious exfiltration of data hidden in images;
- **Coherent and consistent:** ensures appropriate sharing of information within and across teams both internally and externally to the organisations that are holding or creating the data;
- **Data flow visibility:** necessary controls and visibility of the files flowing to support both audit and compliance under the specific collaboration policy requirements; for example, DCPP;
- **Support for operational requirements:** for cybersecurity monitoring and incident response, including SIEM integration via Syslog with standard W3C format logs;
- **Able to flexibly meet policies and procedures:** that lay down how information is to be managed and secured within and across the defence community;
- **Support to the cross domain implementation requirements:** defined within the architectural design patterns defined by national technical authorities

Benefits

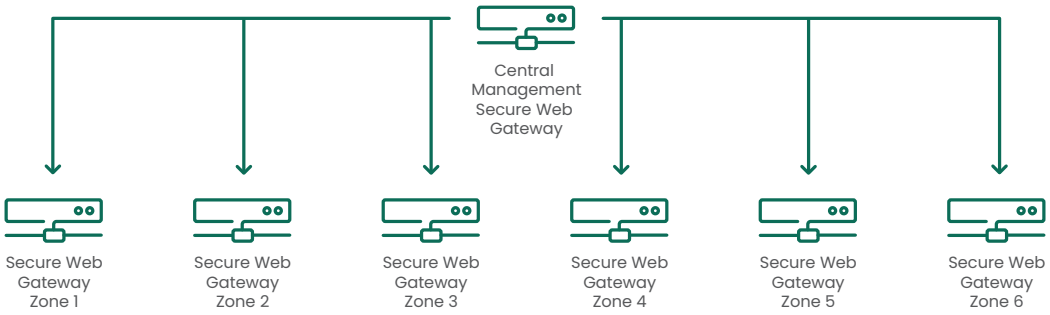
Designed for organisations of all sizes, the system provides:

- **Low friction:** simple and frictionless deployment using an established, proven and assured security technology platform to minimise cost and maximise time to value;
- **Deep content validation:** proven capability to meet the specific demands of the UK Defence community especially in the ability to implement controls requiring deep data checks, validation of content sensitivity and meeting the adaptive requirements for content modification for DLP policy;
- **Multiple domain support:** support for architectures that will protect multiple operating domains and information exchange protocols to enable the benefits afforded by defence platform transformation in capability provision through industry-enabled services – cost, time, flexibility and diversity of supply;
- **User experience:** innovation-led improvement to end user experience for secure sharing of information that reduces risk and the impacts of data loss or security breach;
- **Assurance:** enhancing the baseline levels of cyber protection in the face of increasing state-level threat;
- **Reduced operational cost:** specific features to deal with workflow, including policy violations to minimise operational costs;
- **Support:** underpinned by a defence-aware organisational culture that is creative, passionate and built around a customer focused 'one-team' approach, aligned with the essence of the Team Defence community, to ensure the low-risk delivery of enhanced protection

Deployment

The Clearswift SWG allows for configuration to be centrally managed to ensure that configuration and policies are the same across each CDS module. This is achieved by peering all the web gateways with a central management gateway and administrators can manage the entire fleet by the single management user interface. Communication between the management gateway and the Secure Web Gateways in each zone is over https (443). Changes can be made centrally and pushed out to all gateways or to specific gateways as required.

Policy enables information flow separation and creates a flexible environment based on both content and destination:



The Clearswift SWG is designed to be deployed stand-alone, or in conjunction with other Clearswift Secure Gateway products. When deployed with other products, a consistent Deep Content Inspection and policy engine ensures consistent discovery of critical information, DLP policy and Adaptive Redaction functionality for information flow control. Clearswift products include:

Clearswift Information Governance Server (IGS): Track, trace and control information (not just files) passing across the organisation boundary, including information provenance reporting

Clearswift Secure Email Gateway (SEG): Track, trace and control information contained in email and attachments across the organisation boundary with advanced DLP features including Adaptive Redaction

Clearswift Secure Exchange Gateway (SXG): Track, trace and control information as it travels in internal email providing internal DLP and email segregation functionality without the need for separate infrastructures

Clearswift Secure ICAP Gateway (SIG): Track, trace and control information when used with a 3rd party proxy or managed file transfer (MFT) solution which offers an ICAP integration point

Cost

Flexible pricing options are available to suit differing implementation requirements across the varying scale of organisations that constitute the defence community. This ensures the solutions are commercially appropriate, affordable, and sustainable whilst offering the ability for customers to consolidate their existing security solutions into an integrated platform.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organisations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

