



Deep Secure

www.clearswift.com



Trusted 'store and forward' messaging intermediary...

Clearswift® Deep Secure provides an organisation with the ability to:

- Connect two networks of different security classifications with assured security.
- Implement two discrete security policies - one for incoming traffic and one for outgoing traffic.
- Protect against threats including network attacks and the disclosure of classified material
- Perform security checks on signed and encrypted messages at the Gateway

What is Deep Secure?:

- **Combined Software & Hardware solution**
- **Boundary Security for email**
- **Analysis of email entering or leaving an Organisation**
- **Content Security (virus scanning, textual analysis, encryption & digital signatures)**
- **Firewall architecture capable of meeting the most stringent security requirements**

THE CHALLENGE

As organisations move to a "paperless office", the need for email is increasing. This increase in email usage is causing sleepless nights for IT departments in many organisations. How do we allow the usage of email for transferring secure information and maintain the integrity of the network and thus the office. A solution is required that allows secure (encrypted) and standard emails to be audited at the gateway to the organisation.

THE PRODUCT

The key features of Clearswift® Deep Secure are:

- Firewall level protection for your organisation's messaging environment, including classified (secure) and non-classified email.
- Internal structure consists of two completely isolated DMZ areas with sets of discrete compartments where specific applications vet messages in accordance with the network security policy.
- Messages pass through a fixed sequence of these compartments.
- No form of communication, other than messaging, is permitted.
- Enforcement of an organisation's Security Policy.

Enabling Technology

Clearswift® Deep Secure uses a number of industry known enabling technologies and infrastructural components:

- X.500 directory services.
- SMTP and/or X.400 Messaging protocols.
- A full PKI (Public Key Infrastructure) supporting a separate Certificate Authority to issue and authenticate security certificates.

Assured Network Separation

Messages are stored; then forwarded through an intermediary, rather than through a data stream. This prevents messaging protocols being subverted and being used for external network attacks or unauthorised transfer of confidential data.

Clearswift® Deep Secure maintains separate channels for message flow between networks, allowing different security policies to be applied in each direction. Communication is restricted to two (2) fixed IP addresses.

Label Based Message Release

Clearswift® Deep Secure will:

- Categorise messages based on sensitivity or classification labels.
- Define a label threshold, representing the maximum sensitivity level of information that can be exchanged.
- Police communication and restrict the flow of information between any sender/recipient pair.

More than messaging security

Clearswift® Deep Secure uses external routing MTAs (Messaging Transfer Agents) to prevent direct subversion. In addition, secondary screening routers can provide filtering at packet (firewall) level.

Clearswift® Deep Secure allows reduced visibility of the boundary device (port number filter) and protection against flood denial of service attack (Robustness).

CHARACTERISTICS

So how does Clearswift® Deep Secure provide the ability to audit secure and non-classified emails, while still maintaining the network integrity?

Clearswift® Deep Secure provides an organisation with the ability to deploy a secure messaging gateway, which will ensure that their security policy is met for all unsecured and secure messages. This solution provides the organisation with the option of providing network integrity, while still allowing secure information to be distributed using email.

Clearswift® Deep Secure provides an intuitive graphical policy editor and a visual map that reflects the structure and needs of your organisation.

Clearswift® Deep Secure has been developed for SUN's Trusted Solaris operating system. This operating system has been certified for use in highly secure environments.

Clearswift® Deep Secure complements Trusted Solaris manageability and availability and hardware platforms that support pluggable components, mirrored disks and dual processors, which provides **Clearswift® Deep Secure** with a high level of reliability and availability.

The **Clearswift® Deep Secure** Policy Engine provides the ability to implement policy, including message deconstruction, content analysis, message signature and message encryption. This engine runs inside each compartment and processes network traffic that that area is responsible for. Complying messages are allowed to pass and non-complying messages are dealt with according to the security policy.

The Policy Engine deconstructs each message, applies the policy and re-constructs the message. The messages are routed after processing – either forward for delivery, or backward to the originator.

The Policy Engine communicates with the ClearPoint Management Console.

Key Benefits:

- **Easy implementation of company-wide security policy**
- **Ease of use**
- **Ensures Network Integrity**
- **Ensures Message Integrity**
- **High level of Manageability**
- **High level of Reliability and extremely high Availability**
- **Uses industry known enabling technologies and infrastructure**



Clearswift® Deep Secure supports and provides the level of security provided by SUN's Trusted Solaris Operating System.

Contact eB2Bcom

Melbourne: +61-3 - 9896-7800
Sydney: +61-2 - 9779-1597
email: sales@eb2bcom.com
Web: www.eb2bcom.com