

Sun and Clearswift

Secure messaging with assured network separation



In an attempt to protect sensitive information, government, military, intelligence, and commercial organizations physically separate networks, resulting in disconnected networks that make it difficult to share sensitive information of differing classifications. Secure information sharing must be protected against the risk of release of sensitive information and in accordance with policies and regulatory requirements. Clearswift DeepSecure technology on an appropriate Sun platform helps secure an organization's email whether inbound, outbound, or internal to help ensure traffic complies with policies and regulations.

Maintaining network separation for controlled information sharing

Transferring secure information between trusted but disparate environments is critical to the speed and agility of operations for fast moving environments. This can be extremely important for organizations such as the military or central government during a crisis or heightened levels of operations. For environments that would otherwise prohibit the sharing of information, DeepSecure enables a controlled and accountable flow of messaging traffic between networks of differing security levels or policies.

Clearswift DeepSecure technology is based on the Bastion messaging firewall. Deployed in military implementations around the world and approved to Common Criteria Evaluation Assurance Level 4 (CC EAL4), the messaging firewall overcomes the network isolation of disparate environments and enables the exchange of emails between networks of differing sensitivity. By allowing only messaging to flow through trusted processes, Bastion enables the control and accountability of messaging traffic between networks that would otherwise preclude a direct connection with each other.

Maintaining the desired network separation of channels between networks, DeepSecure forwards messages through an intermediary rather than through a straight data stream — preventing messaging protocols from being subverted and used for external network attacks or unauthorized transfer of confidential information. Information transmission is often bi-directional and requires stringent monitoring in both directions. Bastion maintains separate channels for message flow between networks allowing DeepSecure to apply different security policies in each direction — producing exceptional boundary protection and network integrity that is capable of meeting the most stringent security requirements. Fingerprinting, word searching, and filtering for viruses, malware, media, and content is accomplished by the DeepSecure policy server, which helps enforce an end-to-end comprehensive management and security solution across multiple protocols, locations, and servers. Policies can be managed across multiple and dispersed servers with an intuitive Windows graphical interface — enabling organizations to build a hierarchical definition of message policy for bi-directional messaging at the individual, departmental, or organizational level.

Highlights

- Improve information sharing between networks of differing security classifications to increase the effectiveness of decision making and operations
- Deliver Secure/Multipurpose Internet Mail Extensions (S/MIME) or encrypted messages safely in a military or central government environment
- Help prevent accidental or intentional release of sensitive information through secure message flow and audit trail
- Reduce total cost of operational or military messaging costs, through improved efficiency and secure automation of information exchange processes
- Increase levels of privacy and accountability while reducing risk with Sun's Trusted Solaris™ Operating System

Sun and Clearswift — decreasing risk with a certified solution

Running on the Trusted Solaris™ 8 Operating System (Solaris OS), DeepSecure is a high-assurance border guard (EAL4) for both X.400 and Internet email. Designed to provide protection in some of the most rigorous security-minded environments, DeepSecure offers a rich selection of message content policy options, content inspection, military message labelling, and cross domain connectivity. Recursively decomposing each message into its constituent elements including decryption, signature verification, and attachment decomposition, DeepSecure validates protocol conformance, identifies originator and recipients, locates an appropriate policy relationship, applies the specified policy rules and actions, and then re-assembles the message according to the required policy. As part of maintaining networking resources, DeepSecure can use X.500 or Lightweight Directory Access Protocol (LDAP) Directories to obtain X.509 Certificates and Certificate Revocation Lists (CRLs), X.841 Security (Label) Policy Information Files (SPIFs), DeepSecure policies, or virus and spam definition updates.

A field certified solution, by a recognized certification body in the field of IT, offers credence for an application. The core components of DeepSecure are evaluated to CC EAL4 and its evaluated architecture allows for the use of a selection of non-evaluated, but approved plug-ins without compromising the overall evaluation.

This can easily be constructed to support a range of third-party applications including virus checkers that are required to meet the needs of an enterprise. In order to maintain the CC EAL4 status for the complete solution, DeepSecure currently runs on the Trusted Solaris 8 Operating System on SPARC technology-based platforms. A future version is planned to be evaluated on the Solaris 10 11/06 Trusted Extensions Operating System. Both of these have also passed certification and received the Common Criteria Certificate. DeepSecure conforms to X.400 (1999) and all previous versions, to Military Messaging specified in Standardization Agreement (STANAG) 4406 Ed.2, Allied Communications Publication (ACP) 123 and ACP 145, to S/MIME v3.1, and to current versions of MIME and Simple Mail Transfer Protocol (SMTP) Internet email.

Sun Trusted Solaris

The Trusted Solaris Operating System offers built-in security for high levels of privacy, increased accountability, and reduced risk of security violations. Utilizing the underlying Trusted Solaris subsystems helps keep data of different security levels and categories in separate compartments to safely inspect encrypted messages and prevent attacks while messages are checked for content. An audit subsystem helps to collect and track user actions and create accountability for users of the system. Trusted administrative tools, windowing, and startup utilities help create an environment for each user that can be tailored for specific needs and maintain control and validity of the environment.

Learn More

For more information, visit sun.com, clearswift.com, or contact your local Sun sales representative.

Additional security capabilities can be provided by Solaris Trusted Extensions. For instance, the Solaris 10 11/06 implementation of System V Inter Process Communication (SVIPC) utilizes mechanisms to synchronize, execute, and share data and memory spaces between mutually exclusive yet cooperating processes, helping to enable secure information sharing.

Creating a controlled and accountable environment

Clearswift helps enable messaging traffic to comply with internal policy and external regulations — creating an easy to deploy, manage, and maintain email security solution for both inbound and outbound traffic. DeepSecure uses Clearswift Bastion to provide a trusted environment to help prevent eavesdropping attacks while messages are temporarily decrypted for content checking. As a complete and accredited to EAL4 solution, the Clearswift DeepSecure solution on an appropriate Sun platform secures highly sensitive information through content security separation, and compliance with policies and regulations — helping companies meet stringent security requirements.



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

© 2008 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Solaris, and Trusted Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the US and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Information subject to change without notice. Printed in USA SunWIN #535700 06/08

