



CLEARSWIFT™

Managing and securing
electronic communications

CS Bastion II™

Connecting the Unconnectable

Trust CS Bastion II™ to take your high security network from isolation to communication while maintaining total protection.

CS Bastion II™ is a unique high security messaging firewall preferred in environments handling very sensitive information and requiring total protection from the rest of the organization. CS Bastion II™ allows the controlled and accountable flow of messaging traffic between networks of differing security levels or policies, in environments that would otherwise preclude the direct connection of such networks.

CS Bastion II™ comprises of software and hardware and operates as a stand-alone system. It provides a two-way firewall for X.400 or SMTP/MIME messaging traffic or for X.525 Directory synchronization traffic between sensitive private networks or between public and private networks, maintaining an assured separation between the networks it connects. CS Bastion II™ prevents any other form of communication between these networks.



Certified Assured Protection

CS Bastion II™ is aimed at markets that require Common Criteria EAL4 level of security assurance. The solution is based upon specifically created evaluated software, combined with a portfolio of Clearswift ENTERPRISEsuite™ messaging products operating within the Trusted Solaris operating system. Trusted Solaris is itself approved to CC EAL4 common criteria (CAPP, LSPP and RBACPP). Unlike many other firewall products, CS Bastion II™ does not just rely upon the assurance of its underlying operating system, but actually contains key functions implemented as trusted code, also assured to CC EAL4. The solution was developed in association with QinetiQ, formerly the UK Defence Evaluation and Research Agency (DERA).

The Solution in Action

CS Bastion II™ acts as a trusted intermediary for all messaging traffic between internal and external networks or networks that do not share a common level of trust. The internal structure of CS Bastion II™ comprises a sequence of completely isolated compartments. The evaluated code ensures that a message passes through a fixed sequence of compartments. No other forms of communication are permitted by the CS Bastion II™ to flow between the networks, thus providing the required assured network separation.

A network or packet firewall allows an end-to-end data stream, whereas CS Bastion II™ will act as a trusted 'store and forward' messaging intermediary. CS Bastion II™ can thus prevent messaging protocols from being subverted and used for external network attacks or transfer of confidential data.

CS Bastion II™ maintains separate channels for message flow between networks, allowing different policies to be applied in each direction. If required, all message traffic can be blocked in one direction. An audit trail of all message traffic is maintained.

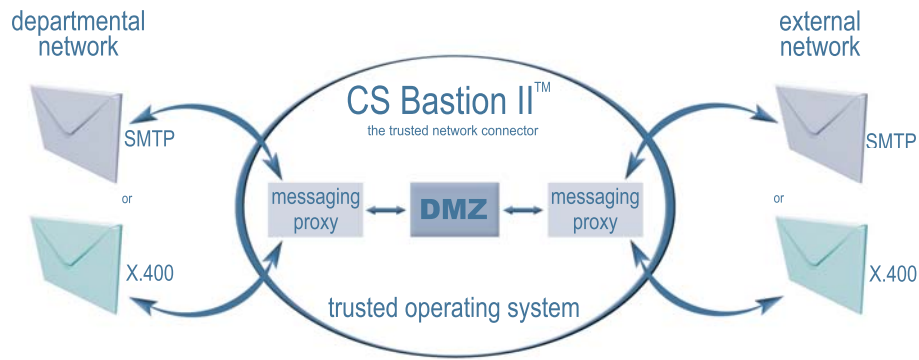
Why choose Clearswift?

Clearswift is the world's number one provider of software for managing and securing electronic communications. With a growing user-base of more than 12,000 customers, 11 million users around the world depend on Clearswift for protection and peace-of-mind.

Why choose CS Bastion II™?

- Certified CC EAL4 security solution
- Overcomes network isolation
- Meets stringent security policy requirements
- Allows messaging between networks of differing sensitivity
- Flexible architecture allowing plug-in filter modules
- Supports X.400 or SMTP/MIME messaging protocols
- Turnkey package simplicity
- Supports X.525 DISP for synchronisation of Directory servers
- Allows isolated networks to be connected to DMZ compartments

CLEARSWIFT™



BUILDING UP DEFENCES

CS Bastion II™ offers a protected environment (De-Militarized Zone) in which additional message screening can be applied. The DMZ consists of compartments that are isolated from each other and from the internal and the external networks. There can be a maximum of four compartments in each direction. Each compartment can have access to its own private network.

The architecture of CS Bastion II™ is such that these modules need not be subject to evaluation. CS Bastion II™ will operate on messages with military content (P772, STANAG 4406) and PCT signature format (Protecting Content Type). Other modules can be introduced to perform specific inspection and filtering of the email traffic: Security label filtering & Audit and alarms.

Typically, CS Bastion II™ will be installed in tandem with components of the Clearswift ENTERPRISEsuite™. Such components may include: Virus scanning, Macro screening, Content filtering & Document Blocking. These components can be applied to S/MIME digitally signed and encrypted messages within the securely protected environment of the CS Bastion II™ DMZ. For further information please refer to the CS Deep Secure Factsheet.

MEETING REAL NEEDS

The ability to interconnect networks conveying information of differing levels of sensitivity is often subject to stringent security policies. In the past these security policies may have even prevented such interconnection, despite the very real need for information interchange. CS Bastion II™ opens the possibility for controlled and accountable communication to take place between these sensitive networks. CS Bastion II™ meets the need for information exchange whilst satisfying security concerns.

The assured protection provided by CS Bastion II™ permits this solution to act as a key component in connecting sensitive Governmental networks to threat-laden public networks, such as the Internet. This assured protection can equally be applied to organizations with high security requirements, as are to be found in the global financial community, insurance arena, healthcare and high technology industries.

A COMPLETE PACKAGE

CS Bastion II™ is generally supplied as a complete turnkey system, comprising software and Sun SPARC hardware, configured and working to requirements. The provision of a turnkey system contributes towards ensuring that CS Bastion II™ meets the certified CC EAL4 security target.

System Requirement

CS Bastion II is normally provided as a complete turnkey solution based on SUN SPARC hardware, utilising the Trusted Solaris operating system. Minimum Requirements: the networks to be connected must be TCP/IP networks, email protocol supported must be either X.400 or SMTP/MIME, any hardware supported by the evaluated Trusted Solaris 8. Please contact Clearswift for further details on network requirements.



CLEARSWIFT™

Managing and securing
electronic communications

AUSTRALIA

Canberra - eB2Bcom
8-10 Jardine St
KINGSTON
ACT, 2604
Tel: +61-2-6234-8043

Sydney - eB2Bcom
Level 66, MLC Centre
19-29 Martin Place
SYDNEY, NSW, 2000
Tel: +61-2-9238-2009

Melbourne - eB2Bcom
Suite 3, 935 Station Street
BOX HILL NORTH
VICTORIA, 3129
Tel: +61-3-9896-7800

email: sales@eb2bcom.com

www.eb2bcom.com

JAPAN

North Sydney - Clearswift
Ground Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel: +61 2 9424 1200
Fax: +61 2 9424 1201

Japan - Clearswift
Eisho Takanawadai Bldg 6F
2-11-8,
Minato-ku Shiroganedai
Tokyo-to, 108-0071
JAPAN
Tel: +81 (3) 5423 8171
Fax: +81 (3) 5423 1274

www.clearswift.com