

Connecting the unconnectable.

■ The ultimate in firewall protection.

As organisations move to a paperless office, the need for email is. Bastion is a unique EAL4-certified messaging firewall preferred in environments handling very sensitive information and requiring total protection from the rest of the organisation.

Bastion 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.

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

■ Certified Assured Protection.

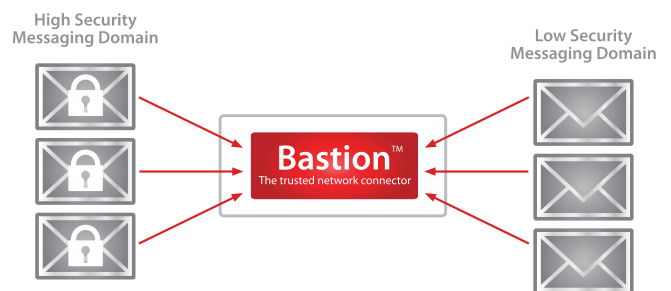
Bastion is aimed at markets that require Common Criteria EAL4 level of security assurance. The solution is based upon specifically created evaluated software, combined with a portfolio of Deep-Secure Ltd.'s messaging products operating within the Trusted Solaris operating system. Trusted Solaris is itself approved to CC EAL4 common criteria (CAPP, LSPP and RBACPP). Unlike many other firewall products, Bastion 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.

■ Building up defences.

Bastion 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 Bastion is such that these modules need not be subject to evaluation. Bastion 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 and audit and alarms.



■ The solution in action.

Bastion 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 Bastion 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 Bastion 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 Bastion will act as a trusted 'store and forward' messaging intermediary. Bastion can thus prevent messaging protocols from being subverted and used for external network attacks or transfer of confidential data.

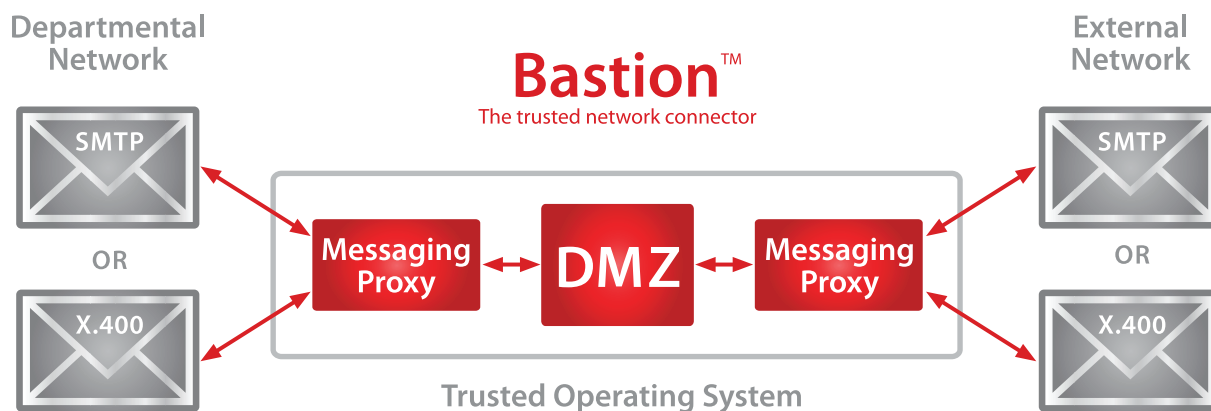
Bastion maintains separate channels for message flow between networks, allowing different policies to be applied in each direction. If required, all message traffic can be blocked in one direction. An audit trail of all message traffic is maintained.

■ Key features.

- 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
- Supports SNMP protocol commands for use within remotely monitored environments
- Allows isolated networks to be connected to DMZ compartments

Overview

Typically, Bastion will be installed in tandem with components of the advanced content security solution for which Deep-Secure Ltd. is renowned. 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 Bastion DMZ. For further information please refer to the DeepSecure™ 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.

Bastion opens the possibility for controlled and accountable communication to take place between these sensitive networks. Bastion meets the need for information exchange whilst satisfying security concerns.

The assured protection provided by Bastion 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 organisations with high security requirements, as are to be found in the global financial community, insurance arena, healthcare and high technology industries.

System Requirements.

Bastion 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 appropriate evaluated version of Trusted Solaris. Please contact Deep-Secure Ltd. for further details on network requirements.

A complete package.

Bastion 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 Bastion meets the certified CC EAL4 security target.

About Deep-Secure Ltd.

Deep-Secure Ltd, a company backed by the Venture Capital Firm, YFM, acquired the Specialist Products Division of Clearswift, the information security company, in December 2009.

Since 2001, the Specialist Products Division of Clearswift has built up a reputation as the premier provider of high assurance Email content inspection and network separation products for defence and government security around the world.

These customers require the hardware platform, application firewall and mail guard are evaluated to Common Criteria EAL 4, requiring very special levels of security knowledge and development

Deep-Secure Ltd. uniquely provides all the evaluated components within a highly configurable solution set.

© 2010 Deep-Secure Ltd. All rights reserved. The Deep-Secure Logo and Deep-Secure product names including ClearPoint™, DeepSecure™, Bastion™ II, X.400 Filter™ and FlashPoint are trademarks of Deep-Secure Ltd. All other trademarks are the property of their respective owners. Deep-Secure Ltd. (registered number 7005288) is registered in Britain with registered offices at 400 Thames Valley Park Drive, Thames Valley Park, Reading RG6 1PT, England.

Contact DeepSecure.

400 Thames Valley Park Drive,
Thames Valley Park,
Reading, RG6 1PT,
United Kingdom

T. +44 (0) 1189 637972
F. +44 (0) 1189 637971
E. info@deep-secure.com
W. www.deep-secure.com

**DEEP
SECURE** 
Assured messaging and application security solutions