DEEP SECURE

Assured messaging and application security solutions

Deep-Secure Mail Guard Feature Guide

The Deep-Secure Mail Guard provides a rich selection of message security functionality and content policy options to Simple Message Transfer Protocol (SMTP) and/or X.400 email messages. It ensures that controls are applied to the flow of mail messages using a sophisticated Policy Enforcement and Content Checking service.

The Deep-Secure Mail Guard is deployed on the boundary of the internal network and all inbound and outbound messages are routed through it.

The Deep-Secure Mail Guard checks the messaging traffic, allowing it to pass, blocking it or putting it on hold as policy dictates.

The Deep-Secure Mail Guard is available on a number of platforms. Where firewall protection is provided at the network security layer, or within environments having low impact levels, a mainstream operating system platform can be used. Alternatively, where assured network

Key Features

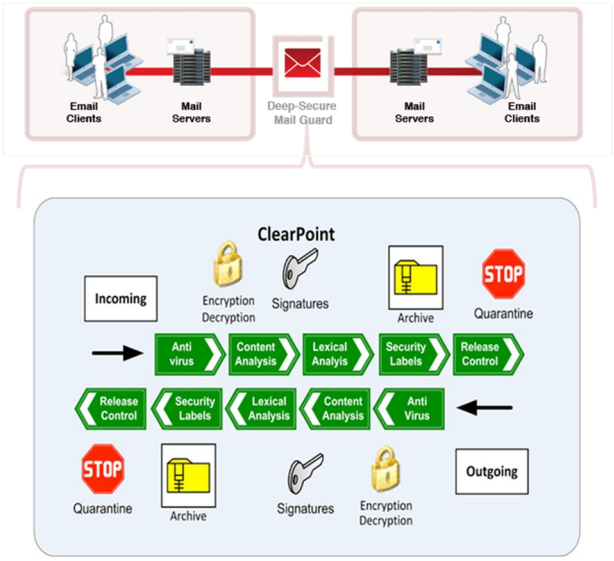
- Powerful policy engine
- Policy based on sender and recipient
- Content policy for signed and encrypted messages
- Intuitive graphical administration interface
- Conformant to a wide range of Government and military standards
- Offers anti-virus integration
- Data type checking
- Textual analysis
- Accounting and audit
- Security labelling support for multiple label types

DEEP SECURE

Assured messaging and application security solutions

How Does it Work?

The Deep-Secure Mail Guard receives messages from external mail servers and validates protocol conformance. Messages are then passed to the Policy Engine which is at the heart of the Deep-Secure Mail Guard. This is responsible for checking messages and applying policy.



The Policy Engine recursively decomposes each received message into its constituent message parts, attachments, signatures and message meta-data. Encrypted content may be decrypted and the signatures of signed content validated.

The Policy Engine then identifies originator and recipients and finds the appropriate policy to apply the specified rules and actions. This can include any conditional policy rules that may be applicable dependent on message content.

Policy rules may be set to modify certain messages before they are delivered. Content may be removed, notifications added, encrypted or signed.

Depending on the outcome of the policy checks, the messages are either delivered to the Outbound MTA to continue to their destination or disposed of according to the Policy Rules.

Policy Rules

The policy rules can include:

- Discarding or non-delivering the message;
- Holding the message for manual inspection or repair;
- Sanitising or removing an element of the message;
- Triggering notification messages to the originator, recipients, configured groups and administrators;
- Causing the message to be archived;
- Adding an entry to the audit log.

Nesting Policy Rules

Sophisticated policies can be created by defining whole sets of rules to be triggered depending on the outcome of any other rule's condition. The dependency may be positive or negative and may nest to any depth. This mechanism has a wide variety of applications, such as:

- Selecting the textual analysis rules to be applied based on the language detected within a message, e.g. to apply a language specific blacklist of disallowed words, or to use a textual analysis Plug-In specific to the identified language;
- Enforcing relationships between textual security labels in attachments and the security label of a message;
- Allowing the precedence of a message to affect the data types allowed within it and the maximum message size permitted;
- Adding a security label or a Subject Indicator Code (SIC) to a message, depending on the result of analysis of the message content.

Content Checking

The Policy Engine's Content Checking capability is provided by a number of Plug-Ins, including:

- Cryptographic software module;
- Virus scanners using third party engines;
- Heuristic data-type recognition;
- Textual analysis and "dirty word" checking.
- Adding an entry to the audit log.

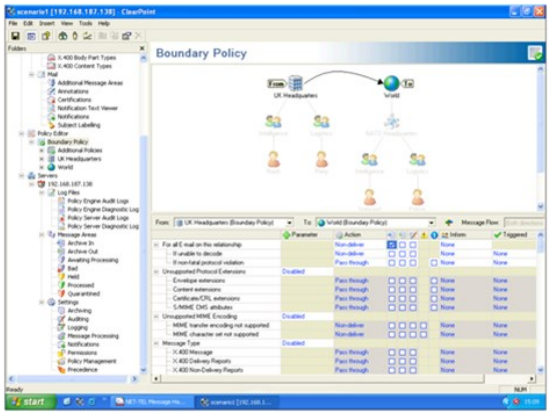
The Plug-In approach allows for flexible integration of industry leading components into Deep-Secure Guards. Additional modules can be added at any time providing they are conformant to the open API used within Deep-Secure.

DEEP SECURE

Assured messaging and application security solutions

Management

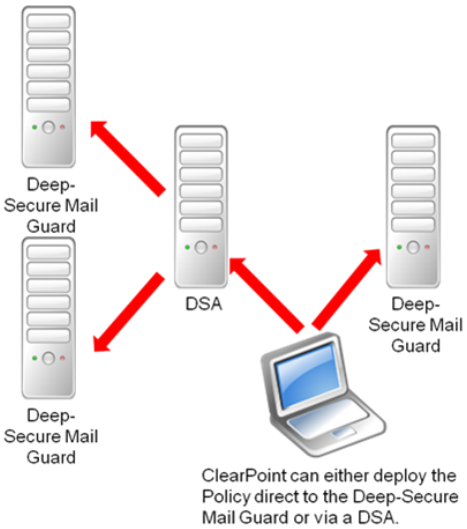
The policy enforced by the Deep-Secure Mail Guard is configured using a powerful graphical policy management interface, ClearPoint, which is common to the Deep-Secure Guards.



This simplifies policy management by presenting a hierarchical view capable of describing rules that apply broadly to whole "departments" or to individual senders and recipients. The concept of rule inheritance enables the administrator to more easily understand complex policies.

The management interface clearly displays all policy applicable to a message sent by any originator to any recipient. It shows both the policy rules defined specifically for that relationship and those inherited from higher up in the policy hierarchy.

The management interface can manage a Deep-Secure Guard by connecting directly to it, but where a Guard farm needs to be managed it is more convenient to use a Directory Server to deploy policies. In this case the policy is stored in the Directory and the Guards synchronise with the Directory to receive updates. Digital signatures are used to ensure the integrity of the policies.



When connected to a Policy Server, the management interface also displays and manages server configuration, archives, audit logs, diagnostic logs, and messages for administrator review.

Individual administrators are authenticated using digital signatures. Privileges control the capabilities made available to each administrator, thus supporting separation of duties, and administrator actions are audited.

DEEP SECURE

Assured messaging and application security solutions

Security Labelling

The Deep-Secure Mail Guard has comprehensive support for environments where messages are marked with security labels. It can check for security labels in messages and compare them against clearances specified in its policy. Labels can be stored in a variety of places including:

- Text labels in the first line of the message;
- Text labels in the message's subject;
- S/MIME ESS Security Labels, Military messaging (P772) content security labels, X.411 security labels and ASN.1 encoded labels, using X.841 security policies.

X.841 security policies are created by a graphical management tool, the SPIF Editor. The SPIF Editor defines the mapping of security label values into equivalent values based on security policies. The Deep-Secure Mail Guard uses the message label to check and validate labels with the policy and work with security level clearances as part of the process of mapping labels in messages. SPIF Editor supports security category syntaxes defined in STANAG 4406 Ed.1, ACP 145, X.841, STANAG 4406 Ed.2 and SDN.801 (US DMS).

Content Inspection of Signed and Encrypted Messages

The Deep-Secure Mail Guard can apply content policy to cryptographically signed and encrypted messages, including capabilities to add, remove or replace digital signatures and the encryption of messages. To check encrypted content, the Guard must be a (blind) recipient of the message.

All cryptographic functions are contained in a pluggable module accessed through an industry standard S/MIME cryptographic API. This approach offers the flexibility to choose from commercially available options for crypto algorithms.

The library typically provided by DeepSecure is the Cryptomathic PrimeInk Premium option offering support for most popular algorithms including X.509 certificates, S/MIME, PKCs, AES, DES, 3DES, HMAC- SHA-1, RSA, DSA,SHA-1,SHA-256, SHA-384, SHA-512, MD5, MDC2, RIPEMD -160 and Diffie-Hellman.

Directory Server Software Integration

Deep-Secure Mail Guard can integrate with Directories to obtain the following information:

- Certificates for signature verification, where these are not contained in each signed message;
- CRLs and ARLs;
- Certificates needed to encrypt a message;
- Certificates needed to authenticate Deep-Secure administrators;
- Policy, where deployed via a Directory;
- X.841 SPIFs, with the X.841 Security Label option;
- Virus/spam definition updates.

The Deep-Secure Mail Guard can use either X.500 or LDAP Directories and can use multiple Directory servers if needed.

BCC Injection

A BCC injection rule can be defined to make a blind copy of any message sent to a user be sent to an additional mailbox for that user in another domain. For example, some users may have a second mailbox which they access by a mobile device and a copy of every message sent to their main mailbox is to be copied there.

Message ID Regeneration

A Message ID Regeneration rule can be defined to sanitise the MIME Message ID header of a message. This is particularly useful for outgoing email where information about the internal domain needs to be hidden.

MIME Boundary Regeneration

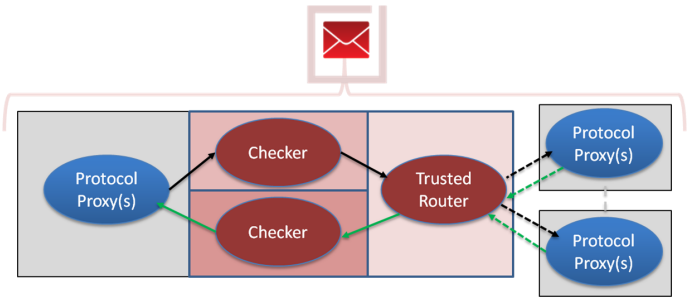
A MIME Boundary Regeneration rule can be defined to sanitise the separator string used to delineate parts of a multi-part MIME message. This is particularly useful for outgoing email where information about the internal domain needs to be hidden. The rule is configured as a boolean option. If enabled, any existing MIME boundary strings in a message are replaced by a newly generated random value.

DEEP SECURE

Assured messaging and application security solutions

Trusted Routing

The optional Trusted Router component can be used with a Deep-Secure SMTP Mail Guard to route messages to multiple external networks using an internal email address domain routing table or using the value of an X-Header carried in the outgoing messages.



Where X-Headers are used for routing, additional policy configurations may be required to allow originator/recipient notifications to be routed.

X-Headers can be added to, or removed from, SMTP email message by policy rules, so in combination it is possible to have policy rules affect the routing of messages by the Trusted Router. However the policy rules only affect messages passing through the guard, not those generated by the guard such as notifications.

Standards Support

Deep-Secure Mail Guard conforms to the following standards:

- X.400 ISO/IEC 10021 (1999) and all previous versions;
- X.500 ISO/IEC 9594;
- Military Messaging specified in STANAG 4406 Ed.2, ACP 123 and ACP 145;
- S/MIMEv3.1 RFC 3851, 3852, 3370, 3850, 2634,2631, 3447, 3565, 3854, 3855;
- SMTP/MIME RFC 2821, 2822, 2045, 2046, 2047,2048, 2049, 1847, 2156, 2157, 2164, 2231, 2387,2480, 3461, 3462, 3463, 3464, 3798;
- X.481 ISO/IEC 15816.

Operating System Requirements

The Deep-Secure Mail Guard runs on:

- Solaris 10
- Deep-Secure Assured Platform (Solaris 10 TX)
- Microsoft Windows (is scheduled)
- The management interface, ClearPoint, runs on Microsoft Windows
- The SPIF Editor runs on Microsoft Windows

DEEP SECURE

Assured messaging and application security solutions

Policy Definition Summary

Policy can be defined in terms of the following factors:

- Protocol conformance
- Unsupported protocol extensions
- Unsupported MIME encoding
- Message type
- Returned content
- X.400 precedence
- X.400 content types
- X.400 body part types
- SMTP headers
- MIME media types
- Size restriction
- Size restriction per precedence
- Security labelling
- First line labelling
- BCC injection
- Message ID regeneration
- Message Boundary regeneration
- Subject labelling
- Message modification
- Security label modification
- Mandate signature/encryption
- Signature/encryption modification
- Data type filtering
- Macro filtering
- Textual analysis
- Virus scanning

DEEP SECURE

Assured messaging and application security solutions

Deep-Secure Product Suite

Deep-Secure Mail Guard

Controls the flow of SMTP and/or X.400 email messages across network boundaries.

Deep-Secure Web Guard

Controls the flow of data carried by HTTP (S) between applications for browsing, publishing or web services.

Deep-Secure Network Management Guard

Controls the flow of network management traffic between networks.

Deep-Secure XML Guard

Enforces the constraints necessary to check and control XML application traffic between networks.

Deep-Secure TransGap

Enables data to be imported / exported between systems without compromising security.

Deep-Secure Control Systems Guard

Controls the flow of MODBUS and OPC data across zonal boundaries.

Deep-Secure File Transfer Guard

Controls the flow of documents by FTP(S) and/or SFTP between networks.

Deep-Secure Digital Identity Guard

Checks digital identities across security boundaries over LDAP, HTTP and OCSP.

Deep-Secure Chat Guard

Controls XMPP/SIP sessions and the flow of documents and data during those sessions.

Deep-Secure X.400 MTA

Provides native support for the rapid transfer of X.400 messages.

About Deep-Secure Ltd.

UK owned and headquartered in Malvern, Deep-Secure is a software specialist with a 30 year technology track record helping organisations in defence, security, private and public sectors to securely share information.

Our products simultaneously guard our customers network boundaries and secure the data they need to share. They're proven and trusted by the most security-conscious organisations in the world.

1 Nimrod House

Sandy's Road

Malvern

Worcester WR14 1JJ

+44 (0) 1684 217070

Email: info@deep-secure.com

www.deep-secure.com