

www.securecomputing.com

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years, and is uniquely qualified to be the global security solutions provider to organizations of all sizes.

“IronMail has helped us secure our patient information and transmit critical messages without worrying about whether we are violating a policy or regulation.”

– Jim Donaldson, Baptist Health Care Corporation

Encryption-Push benefits

- Enables secure email communication in any environment, regardless of the recipients' encryption capabilities
- Policy-driven encryption ensures that sensitive information is protected without requiring end-user action
- Easy to install and compatible with any type of messaging server, including Exchange, Notes and Domino
- Robust reporting and analysis tools provide instant insight into email traffic crossing the enterprise gateway
- Multiple encryption options for business-to-business or business-to-user communication assures compatibility with any intended recipient

Secure Computing Encryption-Push

Send policy-based encrypted messages to any recipient

While there is little debate about the need to encrypt messages that contain sensitive information, many security officers have resisted installing an encryption solution on their enterprise email network due to difficulties in deployment and administration of existing solutions. Traditionally, these solutions have required bypassing corporate messaging security infrastructure such as anti-virus and content filtering controls. Now, there's a new solution that doesn't compromise any aspect of your messaging security. The Encryption-Push™ module, available as a component of the IronMail® appliance by Secure Computing, sends recipients a secure message as an attachment to an otherwise standard email. The recipient can view and respond to the message in a standard Web browser.

- **Key escrow** – allows escrow of recipient encryption keys to a configured email address. The keys are packed into an encrypted file with a password and emailed to an escrow email address, ensuring that your encryption solution is fault-tolerant in case of a disaster or other event that renders the encryption server unavailable.
- **Key synchronization** – simplifies synchronization of usernames and passwords, challenge response information, and encryption keys between encryption servers.
- **Flexible authentication** – allows the Encryption-Push module to use username/password authentication or no authentication. This is configurable by the administrator according to corporate security policies.
- **Desktop message retention** – gives message recipients the ability to access encrypted messages at any time, from any machine with a Web browser. Enterprises no longer must manage the encrypted messages or message store.

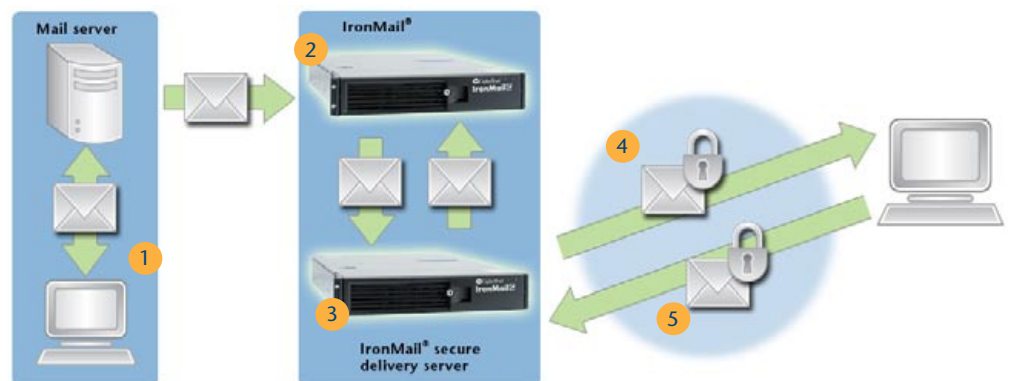


Figure 1: How Secure Computing Encryption-Push works at the gateway.

1. Users send email as usual
2. IronMail examines message content and, based on policy, determines that encryption is required.
3. Message is routed to the IronMail Secure Delivery Server
4. Secure message is generated and sent to the recipient, who then opens the secure attachment to view the message
5. Recipient replies securely to the message via a standard Web browser.

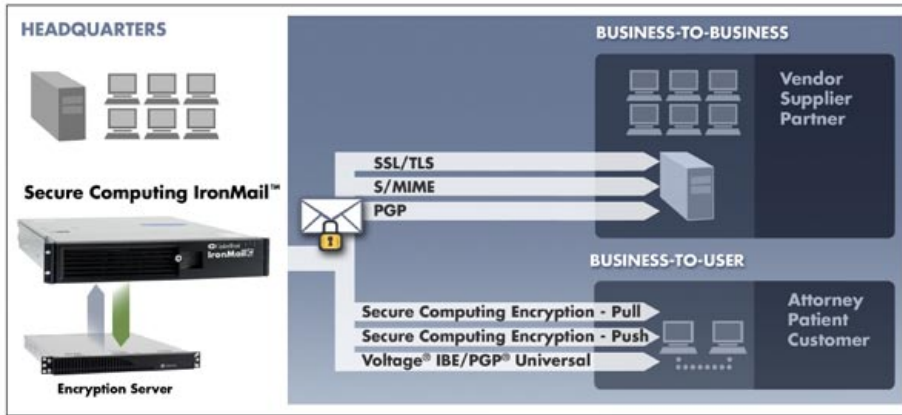


Figure 2: Secure Computing Encryption: multiple options for secure communications with any recipient

Business-to-business encryption

IronMail supports multiple encryption protocols for secure email communications between businesses:

SSL/TLS: Secure Sockets Layer (SSL) is a protocol for encryption and authentication of Internet connections. Transport Layer Security (TLS) is the standardized version of SSL. IronMail uses SSL/TLS to create a secure “tunnel” for messages to travel through to the recipient server or client. This option is shipped native with each IronMail providing policy-driven encryption.

S/MIME: IronMail offers support for S/MIME (Secure Multipurpose Internet Mail Extensions) to encrypt messages and send them securely. S/MIME requires key exchange between the sender and recipient servers that is managed by IronMail.

PGP: IronMail customers can also select PGP (Pretty Good Privacy) technology to send encrypted messages. This solution combines IronMail’s market-leading message scanning and policy enforcement technology with PGP Universal’s world-class centrally managed encryption capabilities.

Business-to-user encryption

Often, organizations need to communicate with recipients who do not have encryption capabilities. For these situations, Secure Computing offers several methods of encrypting messages that are effective regardless of the recipient’s encryption capabilities:

Encryption–Push: The Push encryption module sends recipients a secure message as an attachment to an otherwise standard email. The recipient can view and respond to the message using any Web browser.

Encryption–Pull: IronMail offers a secure staging server as a “pull” encryption option. With this method, an email notifies the recipient that a message is waiting in a secure Web-based mailbox. The recipient logs into a secure Web page to retrieve, view and reply to any encrypted messages.

Voltage® IBE server: By using well-known identities as public keys, IronMail’s Voltage IBE server eliminates the complexity of managing certificates, Certificate Revocation Lists (CRL), and other costly infrastructure.

PGP® universal automatic encryption and key management: Customers who select the IronMail/PGP Universal solution benefit from proven integration and joint policy configuration as well as single point of purchase, deployment and support.

SECURE
COMPUTING

www.securecomputing.com



For more information

Contact your local reseller,
or Secure Computing at:
1-800-379-4944 (inside U.S.)
1-408-979-6100 (worldwide)
sales@securecomputing.com
www.securecomputing.com

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100
Fax: +1.408.979.6501

European Headquarters

No 1 The Arena
Downshire Way
Bracknell
Berkshire, RG12 1PU UK
Tel: +44.0.870.460.4766
Fax: +44.0.870.460.4767

Asia/Pacific Headquarters

Hong Kong
1604-5 MLC Tower
248 Queen’s Road East
Wan Chai Hong Kong
Tel: +852.2520.2422
Fax: +852.2587.1333

Japan Headquarters

Shinjuku Mitsui Bldg. 2, 7F
Nishi-Shinjuku 3-2-11
Shinjuku-ku, Tokyo, 160-0023
Japan
Tel: +81.3.5339.6310
Fax: +81.3.4496.4537

For a complete listing of all our global offices,
see www.securecomputing.com/goto/globaloffices