BLOOMBASE®

BROCHURE

Bloombase Spitfire Message

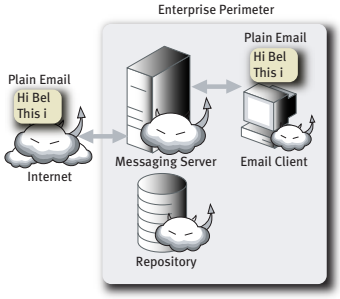
Enterprise Email Security Server / Virtual Appliance

Enterprise Email Confidentiality

Today's enterprises rely heavily on email systems for their day-to-day business and operations. Statistics show email volume grows at an annual rate of 30% [IDC quoted in Storage Magazine]

Despite efforts and investment spent on email protection such as content detection, content filtering, anti-virus and anti-spamming, email theft and contents tampering remain unsolved.

Imagine a secret email from top management is disclosed or confidential data files sent as attachments in emails are altered to achieve evil purposes. Email theft or unauthorized data alteration are technically possible while emails are in transit, adding potential risks to email transporting in the networked environment. When emails are permanently persisted in backend messaging servers where company operators and administrators can easily access, it opens another high risk area where confidential data can easily get exposed. Corporate confidential information are unwantedly made known to outsiders, harming corporate image and in most cases, causing immediate financial loss.



A typical scenario in messaging infrastructures of most enterprises - email messages are unencrypted. Unauthorized parties can get access to the secret information along the whole path of message delivery.

The Technical Solution and The Downside

Email encryption based on Secured Multipurpose Internet Mail Extension (SMIME) and digital signature technologies based on public key infrastructure (PKI) as well as strong encryption protect plain contents from prying eyes and provide evidence to possible unauthorized content alterations.

However, adoption of these technologies in corporations lag far behind than anyone could have imagined. A major obstacle is the need to change end-user daily workflow that keeps users away.

Revolutionary Email Protection Approach

Spitfire Messaging Server is the ultimate solution to successful secure corporate email deployment.

Spitfire Messaging is a standalone high-performance e-mail cryptographic engine that encrypts emails on-the-fly in corporate messaging systems.

It supports all commercial messaging servers on the market and deployment is hassle-free. With Spitfire Messaging, users enjoy security of messaging with absolutely no sacrifice in usability.

How Does It Work

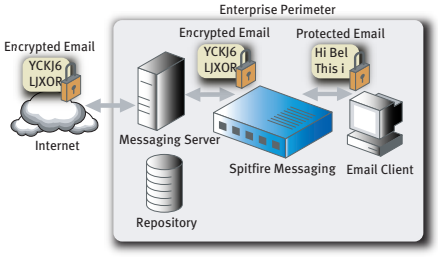
Spitfire Messaging server detects the network path between corporate messaging server and messaging clients for plain email messages.

Once a valid message is trapped, Spitfire Messaging encrypts plain emails and adds digital signature to ciphered messages before delivered by messaging server.

Message recipients uncover true contents with their email clients they used to work with without changing their daily workflow. As recipients are the only ones possessing the decryption keys, Internet hackers or corporate operators have no way of snooping confidential contents.

Spitfire Messaging Server is a network attached appliance requiring no change on enterprise messaging infrastructure. Deployment and implementation are easy. No programming is required.

Spitfire Messaging Server can run as a cluster of servers to fulfill demanding and mission-critical messaging processing requirements for carrier and large enterprise use.



Spitfire Message sits between email client and enterprise messaging gateway to encrypt outgoing email network packets on-the-fly without requiring user attention

Enterprise Email Integrity and Authority

Phishing and email fraud remain a serious Internet security problem despite presence of information security products including email anti-spammer and content filter. Unlike spamming, email fraud can cause tremendous loss of user properties and corporate assets.

In attempt to solve email fraud problem, "responsible" businesses choose NOT sending marketing emails. But this does not solve the actual problem. Customer service and sales/marketing tasks once again become laborous human workload, immediately raises operating costs.

Spitfire Messaging is created to solve identity security problem of corporate emails - from e-marketing advertisments to electronic statements. Spitfire Messaging adds evidence to from whom an email is sent, whether or not the contents are altered and protects sensitive contents from prying eyes.

Spitfire Messaging can integrate easily with corporate messaging systems to transparently sign user outgoing emails and verify incoming emails to ensure integrity and source authority assuring confidence and trust in all emails processed by a corporate user.

Spitfire Messaging Server operates on a trimmed-down bundled version of Spitfire KeyCastle which is a carrier-proven key server for secure X.509 certificate and key storage. Management is a breeze via standard web-browsers.

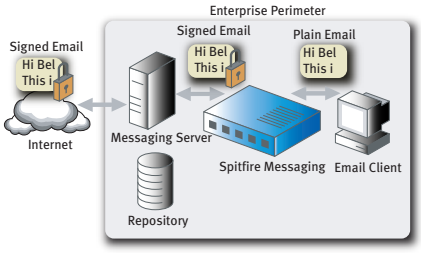
Business Benefits and Applications

Email repository storage protection
- Incoming and out-going plain emails are encrypted before reaching corporate groupware. Emails get persisted in storage in their encrypted form

Secure mobile email
- Deploy Spitfire Messaging in mobile corporate messaging environment to enjoy true end-to-end secure mobile messaging

Electronic bill encryption
- Protect electronic bills in emails by strong encryption for consumers' most private and confidential billing information

E-marketing source authenticity assurance
- Add digital signatures to e-marketing messages to assure customers obtaining the most accurate and trustworthy promotion resources



Spitfire Messaging Server acts as an email digital signature generator to add authority information to out-going emails assuring source authority - identity and data integrity. On the reverse, Spitfire Messaging Server scans for incoming digitally signed messages and ensure incoming messages are from valid parties and contents unaltered before presenting to user clients.

Functions and Features Highlights

Secured Simple Mail Transfer Protocol (SMTP)
- Standard based and work virtually with all messaging servers in the market

User independence and transparent processing
- No user training required. Outgoing emails are encrypted immediately under the covers requiring no user workflow change

Secured Multipurpose Internet Mail Extension (SMIME) encryption support
- International standard on email encryption ensuring compliance and risk-free implementation

Transparent Encryption and Decryption
- High performance and intelligent cryptographic engine to detect network traffic for email contents and carry out cryptographic operations based on user-predefined rules

Transparent Signature Generation and Verification
- Add digital signature to emails to assure source and accuracy of electronic messages. Digital signature provides evidence that an instruction or information of a signed email has been authorized.

Technical Specifications Highlights

Security
- NIST FIPS 140-2 validated cryptographic module
- Industry-proven cryptographic processing engine
- AES-128/192/256, 3DES, CAST5, RC2 encryption
- 512/1024/2048-bit long X.509 asymmetric key

Messaging
- S/MIME encryption, decryption, signing and verification

Certificate Management
- Multiple certificate authority (CA) support
- Built-in certificate request and revocation check (CRL/OCSP)

Network Management
- SNMP (v1, v2c, v3), syslog, log rotation and auto-archive

System Administration
- Secured web-based and serial console

Bloombase - Transparent Data Security **email** info@bloombase.com **web** www.bloombase.com

BLOOMBASE®