SecurityGateway for Email Servers

Layered Defenses and Flexible Configuration Improve Server Performance and Security

SecurityGateway for Email Servers combines over two decades of email security expertise with proven security technologies to protect businesses from the latest email-borne threats. Using multiple security methods, SecurityGateway assures the accurate delivery of legitimate email while blocking out spam, malware and other unwanted junk.

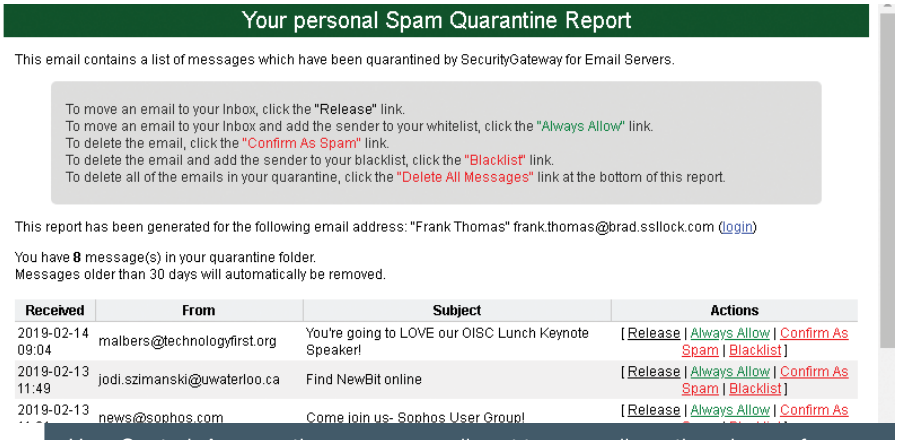
SecurityGateway incorporates multiple AV engines and proactive Outbreak Protection technology combined with additional signature recognition and heuristic analysis to detect viruses, spam, phishing, ransomware and other types of unwanted and harmful email.

Data Leak Prevention rules allow administrators to easily filter messages containing sensitive information such as credit card numbers, Social Security numbers, and other types of sensitive data.

Message encryption, e-sign, and track & prove services powered by RPost provide additional privacy, collaboration, and verifiable proof of delivery, time, and exact message content.

For companies that do not have legitimate business in certain geographical locations, Location Screening allows administrators to block connections from specific countries.

SecurityGateway's email archiving features provide a fully indexed and searchable repository of all messages sent and received - for both administrators and end users, with advanced search and options for downloading archived messages or restoring them to the mailbox, plus retention policies and legal hold for regulatory compliance.


Your personal Spam Quarantine Report

This email contains a list of messages which have been quarantined by SecurityGateway for Email Servers.

To move an email to your Inbox, click the "Release" link.
To move an email to your Inbox and add the sender to your whitelist, click the "Always Allow" link.
To delete the email, click the "Confirm As Spam" link.
To delete the email and add the sender to your blacklist, click the "Blacklist" link.
To delete all of the emails in your quarantine, click the "Delete All Messages" link at the bottom of this report.

This report has been generated for the following email address: "Frank Thomas" frank.thomas@brad.sslock.com (login)

You have **8** message(s) in your quarantine folder.
Messages older than 30 days will automatically be removed.

Received	From	Subject	Actions
2019-02-14 09:04	malbers@technologyfirst.org	You're going to LOVE our OISC Lunch Keynote Speaker!	[Release | Always Allow | Confirm As Spam | Blacklist]
2019-02-13 11:49	jodi.szimanski@uwaterloo.ca	Find NewBit online	[Release | Always Allow | Confirm As Spam | Blacklist]
2019-02-13	news@sophos.com	Come join us- Sophos User Group!	[Release | Always Allow | Confirm As

User Control: A quarantine summry email sent to users allows the release of messages or whitelisting of email without the need to burden the IT Administrator.

Key Features

- **Accurate Threat Detection**
  Multiple analysis tools for blocking the latest threats
  - AntiSpam
  - AntiVirus
  - AntiPhishing
  - AntiSpoofing
- **Data Leak Prevention**
  An easy-to-use interface allows policies to be created which detect and prevent the unauthorized transmission of sensitive information outside of your network.
- **Expanded Security Services**
  Email encryption, e-sign, and email track & prove deliverability powered by RPost.
- **Defense Layer Customization**
  Administrators can improve server performance by prioritizing the order in which specific security rules will execute when analyzing incoming or outgoing email traffic.
- **Comprehensive Reporting**
  Identify email traffic patterns and potential problems with comprehensive reporting. All reports support point-and-click drill-down targeting for easy analysis of trends and issues.
- **Integrated Archiving**
  All inbound and outbound email messages can be archived for added protection against disasters. Retention policies and Legal Hold help businesses meet regulatory compliance requirements and litigation needs.

Key Benefits

- **Easy Administration.**
  Intuitive, task oriented, responsive interface allows already overworked administrators to perform common actions with minimal effort. Administrative responsibilities can be delegated to a domain administrator. End users are empowered to determine the fate of a message without the need to contact the administrator.
- **Proven Threat Detection.**
  Multiple security tests, including multiple antivirus plug-ins, deliver enterprise-class protection against hidden threats in both inbound and outbound email.
- **On-Premise or Hosted Deployment.**
  Per-user options for both commercial hosting and on-premise subscriptions available.
- **Investment Protection.**
  Receive free upgrades to the latest product versions for the duration of the subscription term.

System Requirements

- Microsoft Windows 10|2016|8|2012|7|2008|Vista|2019 (including 64-bit versions)
- CPU 800MHz or higher (dual core CPU 2.4GHz or higher recommended)
- 512 MB RAM (2 GB recommended)
- Network Interface Card
- TCP/IP network protocol installed
- NTFS volume with minimum of 500MB free space
- Any modern web browser

SecurityGateway Configuration and Features

External Threat Protection

AntiSpam
- Heuristic and Bayesian
- DNS and URI Blacklists
- Message Certification
- Greylisting
- Backscatter Protection
- Message Scoring

AntiVirus
- Multiple AV engines
- Threat Signature Updates
- Recurrent Pattern Detection (RPD)
- Zero-Hour Outbreak Protection

AntiSpoofing
- Reverse Lookups
- Callback Verification

Email Authentication
- DomainKeys Identified Mail
- Sender Policy Framework (SPF)
- DMARC

AntiAbuse
- Relay Control
- SMTP Authentication
- IP Shielding
- Dynamic Screening and DDoS
- Location Screening
- Tarpitting

Filtering
- Multiple Search Strings
- Message Content Filter
- Preset File Types
- Attachment Filtering

Blacklists
- Blacklist Addresses
- Blacklist Hosts
- Blacklist IPs
- Blacklist Actions

Whitelists
- Whitelist Addresses
- Whitelist Hosts
- Whitelist IPs

Internal Threat Protection

Data Leak Prevention

Policy Enforcement via Sieve Filtering Language

Encryption: SSL & TLS

Redirect HTTP to HTTPS

Administrator Options

Multiple Languages

Flexible User Interface

Domains and Users
- Per User Options
- Automatic Domain & User Creation
- User Verification Source Options
- Global & Domain Admin Settings
- Unlimited Account Aliases

Multiple Domain Mail Handling

Per-Domain IP Addresses

Message Quarantine Options
- Domain Level Access
- User Level Access

Database Maintenance
- Data Retention Settings
- External Database Support

Disclaimer in Headers/ Footers

Terms of Use

Archiving

Private Account Options
- Individual Whitelist & Blacklists
- Individual Message Logs
- Quarantine Management

Performance Features

Defense Layer Customization

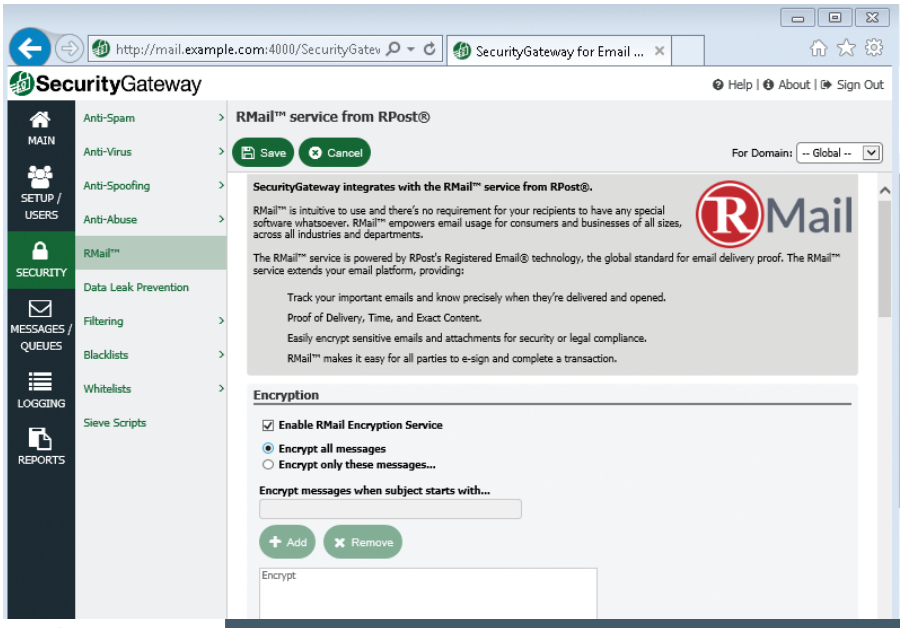
Bandwidth Throttling

Logs & Reports

Detailed Logs
- Message Logs
- Message Log Filtering
- Historical Logs

Real-Time Charting Reports
- Summary Report
- Inbound/Outbound Email Reports
- AntiSpam/AntiVirus Reports Local User Reports
- Scheduled Statistics Report

Expanded Security Services
- Message Encryption
- E-Sign
- Track & Prove Services



RMail encryption, e-sign, and track & prove services.

MDaemon® technologies