



# SecurityGateway

For Exchange/SMTP Servers

## Layered Defenses and Flexible Configuration Improve Server Performance and Security

SecurityGateway for Exchange/SMTP combines over a decade of email security expertise with proven security technologies to protect message traffic from malicious attacks, message tampering and email address identity theft for organizations using Microsoft Exchange® and other SMTP email servers.

Using multiple security methods, SecurityGateway for Exchange/SMTP assures the accurate delivery of legitimate email while minimizing the potential of false positives.

SecurityGateway for Exchange/SMTP offers flexible protection with simple, easy-to-use settings for trouble-free administration. Its layered security design, protects businesses against incoming and outgoing email abuse by denying spammers, thieves and hackers a single point-of-failure to exploit.

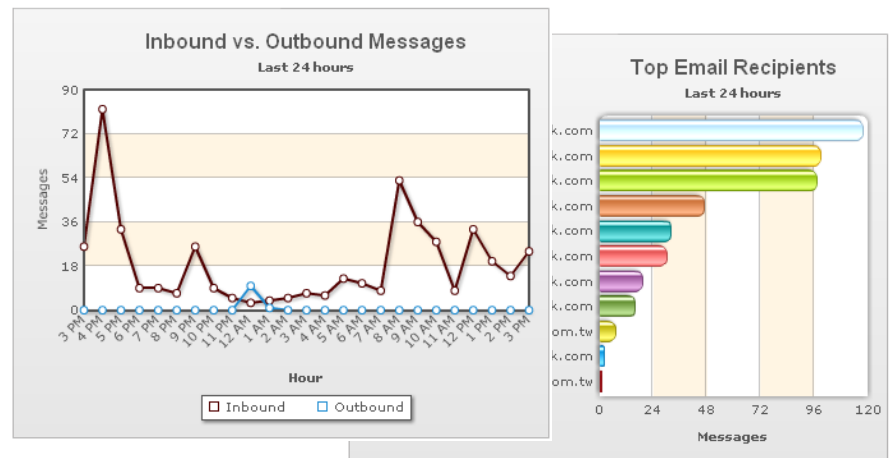
### Key Features

- **False Positive Protection**—Because no one benefits when an email is wrongly identified as spam or unsafe, protections assure the ultimate delivery of legitimate messages.
- **Hidden Threat Detection**—Multiple security tests, including multiple anti-virus plug-ins, deliver enterprise-class protection against hidden threats, incoming and outgoing.
- **Flexible Design**—Because security measures of the future will be different from those of today, design flexibility protects your software investment for years to come.
- **Web Access**—The gateway is easily accessible through a web browser interface for both administrators and users.
- **Blacklists and Whitelists**—Messages from senders on blacklists are always rejected. Messages from senders on whitelists can optionally bypass some tests.
- **User-Specific Lists**—Users can specify their own blacklists and whitelists.
- **Message Logs**—Logs for administrators and users show the disposition of each email—delivered, quarantined, rejected—and why.
- **Graphical Reports**—Realtime graphical reports reveal email trends. Each report contains clickable points linked to the message logs.
- **Fine-Tuning Tests**—Adjustments can be made to the aggressiveness of each test, either globally or for individual domains.

Customers wanting multiple AV engines and proactive Outbreak Protection features can add the ProtectionPlus plug-in. ProtectionPlus extends and



compliments the built-in features of SecurityGateway by combining additional signature recognition and heuristic analysis to detect viruses, spam, phishing, spyware and other types of unwanted and harmful email.



The SecurityGateway for Exchange/SMTP provides multiple graphical reports

# SecurityGateway Configuration and Features

## Security Options

### Anti-Spam

- Heuristic and Bayesian
- DNS Blocklists
- URI Blocklists
- Greylisting
- Message Certification
- Backscatter Protection
- Message Scoring
- Outbreak Protection via **ProtectionPlus**

### Anti-Virus

- Automatic Pattern Updates
- Multiple engines via **ProtectionPlus**

### Anti-Spoofing

- Reverse Lookups
- DKIM Signing and Verification
- SPF
- SenderID
- Call Back Verify

### Anti-Abuse

- Relay Control
- SMTP Authentication
- IP Shielding
- Dynamic Screening
- Tarpitping
- Bandwidth Throttling

### Filtering

- Message Content Filter
- Preset File Types

### Blacklists

- Addresses
- Hosts
- IPs
- Blacklist Actions

## Whitelists

- Addresses
- Hosts
- IPs

## Policy Enforcement

- Sieve Rules

## Optional - ProtectionPlus

- Kaspersky AV Engine
- Outbreak Protection via real-time pattern analysis

## Configuration Options

### Domains and Users

- Automatic Domain and User Creation/Maintenance
- Multiple Email Domains
- Domain Administrators
- Per-User Options

### Mail Handling

- Multi-Domains Per Mail Server
- Custom Mail Delivery Options

### Quarantine Options

- Domain Level for Admins
- User-Level Access

### Database Maintenance

- Backup & Restore

## System Logs

### Message Logging

- Global Message Log
- Domain Message Log
- Quarantined Messages

## Historical Logs

- Configurable Log Retention
- Snapshot System Log
- Snapshot Inbound Log
- Snapshot Outbound Log
- Snapshot HTTP Log

## Reports

### Summary

- Extensive Filter Options
- Real-Time Charting
- Junk Email Breakdown
- Bandwidth Utilization

### Inbound Email

- Messages Processed
- Top Recipients
- Top Recipients by Size

### Outbound Email

- Messages Processed
- Top Senders
- Top Senders by Size

### Anti-Spam

- Top Senders by Domain
- Top Recipients

### Anti-Virus

- Inbound Caught
- Inbound by Name
- Outbound Caught
- Outbound by Name

## Private Account Options

- Processing Settings
- Whitelists and Blacklists
- Message Logs
- Quarantine Management

## Key Benefits

**Simple Administration.** Intuitive, task oriented interface allows already overworked administrators to perform common actions with minimal effort. Administrative responsibilities may be delegated to a domain administrator. End users are empowered to determine the fate of a message without the need to contact the administrator.

**Powerful Filtering.** SecurityGateway for Exchange/SMTP's powerful filtering engine is based upon the industry standard SIEVE mail filtering language. An administrator may extend the functionality of SecurityGateway for Exchange/SMTP with their own SIEVE scripts.

**Accurate Detection.** With multiple analysis tools for separating threats from legitimate email, SecurityGateway stops virtually all problem email, while enabling more efficient business communications.

**Data Loss Prevention.** An easy-to-use interface allows policies to be created to support outbound content inspection. Filter settings can help detect and prevent unauthorized transmission of sensitive information outside of your network.

**Investment Protection.** Includes one year of renewable Upgrade Protection, providing free upgrades to the latest product versions for the duration of the Upgrade Protection term.

## System Requirements

- Computer with Pentium 4 processor (Multiple core processor recommended).
- 512 MB of memory (2 GB recommended)
- Microsoft Windows Vista/XP/2000/2003 operating system.
- Network Interface Card.
- TCP/IP network protocol installed.
- NTFS volume with minimum of 500MB free space.
- Firefox 1.5, Internet Explorer 6.0, Opera 8.5, or Safari 3.0 web browser. Adobe Flash Player 8.0 or above for graphical report viewing.

© 2008 Alt-N Technologies, Ltd.  
2550 SW Grapevine Parkway,  
Suite 150 Grapevine, Texas 76051  
Phone: (817) 601-3222  
Fax: (817) 601-3223  
MDaemon is a registered trademark of Alt-N Technologies.  
Microsoft Exchange is a registered trademark of the Microsoft Corporation.  
[www.altn.com](http://www.altn.com)

The top screenshot shows the 'Message Log - user0' interface. It features a table with columns: Date, From, Recipient, Subject, and Action. The table lists several messages, including one from 'ISP-Planet Weekly HTML Newsletter' and another from 'WebWeekly: Disabling the Submit'. The bottom screenshot shows a 'WorldClient - Mozilla Firefox' window displaying a quarantine log email. The email content includes a table with columns: Received, From, Subject, and Actions. The table lists several messages, including 'SpaceDaily Express - Dec...' and 'Space War Express - Dec...'. The email also includes a 'Click here to view your quarantine folder or manage your preferences.' link.

Top: Individual users can access their messages logs and perform tasks, such as marking as spam.

Bottom: A quarantine log email sent to users allows the release of messages or whitelisting of senders.