PineApp
Our Innovation - Your SeCurity

Mail-SeCure™ 5000 Series

PineApp Mail-SeCure appliance offers a comprehensive email security solution

The war against spammers is not a simple one and requires spam fighters to be dynamic, sophisticated and creative.

Mail-SeCure 5000 series is a leading email security appliance that protects large scale organizations from both targeted and non-targeted email-related threats. Mail-SeCure provides a buffer between the Internet and the organization's email systems, using a full pack of perimeter security layers.

Virus Protection

Mail-SeCure inspects all email traffic and protects the organization's network from known and emerging threats, such as Viruses & new-age Virus outbreaks, Worms and Trojan-horses. This is done by using a five layer Anti-Virus system, composed of PineApp's proprietary Email-Worm detector, a triple F-SeCure Anti-Virus engine and a Zero-Hour™ Outbreak detection engine.

Spam and Phishing Prevention

Fighting spammers has become a challenge as spammers are constantly improving their technologies to bypass Anti-Spam systems. Mail-SeCure has an advanced eleven-layer Anti-Spam engine, enhanced by proven technology that prevents all known Spam, including Image-based Spam. All incoming mail undergoes an in-depth analysis by the different Anti-Spam layers. Mail-SeCure identifies 98.5% of incoming Spam and immediately blocks or tags it as Spam, in accordance with the organization's policy. By combining Anti-Spam technologies with advanced policy management, PineApp has reduced the false positive ratio to almost zero.

Advanced Management

Mail-SeCure's innovative Three-tier policy management mechanism enables administrators to define rules for users, groups, or the entire organization. This flexibility enables the system administrators to enforce the organization's policy for both incoming and outgoing mail flow. Mail-SeCure smoothly interconnects with existing directory services using the LDAP protocol. Users can manage their own quarantine and Black & White lists. Furthermore, users receive daily reports from which they can manage their mail flow and release quarantined mail.

Easy installation

With no need for software installation, Mail-SeCure integrates into any network topology as an SMTP relay. In most cases, Mail-SeCure's default settings are sufficient for most organizations, thus making the installation and configuration easy and simple.

Benefits

- Complete email protection suite
- One-stop-shop, no additional licensing costs
- Real-time technology implementation against new emerging threats
- Reduces bandwidth using perimeter-level protection layers
- Reputation filters keep potential threats away from your network
- Outbreak detection engine keeps your network clean from new-age email Viruses
- Proven technology against Image-based Spam
- Anti-Phishing prevention, protects users from fraudulent mail
- Auto-updated - self-maintained system
- Integrated load balancing
- Scalability; allows businesses to grow by stacking two or more Mail-SeCure appliances
- Significantly fast ROI

Specification and Features

Model Comparison	5040	5050	5080
Number of mail users (recommended)	2,500	5,000	10,000
Domains	Unlimited		
Hardware Platform	Sun Microsystems Fire X4100		
Ethernet	4xGbE		
CPU Cores	2	2	4
Storage Size	2x72GB SAS (RAID1)	2x144GB SAS (RAID1)	
Power Supplies	1	1	2
Input Power	100~240VAC 50/60Hz		
Dimensions (WxDxH)	43.2x61x4.4 cm (17x24x1.7 inch) 1U rack mount		
Advanced Management	IPMI, KVM over IP		
Warranty	1 year limited warranty		
Licensing	Revolutionary unlimited user licensing program		
Certifications	CE, CB, FCC, LUV, UL, RoHS		

Anti-Spam Engines

Perimeter Engines

- Zombie detection & IP Reputation system
- External and Internal RBL lookups
- NextGen Greylisting

Recurrent Pattern Detection (RPD™)

Deep Inspection Engines

- Image Analysis engine
- Bayesian statistical engine
- Heuristic engine with over 2,500 rules
- URL, Telephone & Email Database
- Domain to IP conversion (SURBL)
- Honey pots with real-time database update
- SPF and DomainKeys support

Anti-Virus Engines

- PineApp Propriety heuristic Worm detection engine
- F-Secure® Orion - heuristic-based
- F-Secure® Libra - signature-based
- Kaspersky® AVP - heuristic and signature based
- Zero-Hour™ outbreak detection

Anti-Phishing Engines

- Internal updated databases
- External databases

Advanced Policy Management

- Support LDAP: Pre-defined & Open LDAP Management credentials
- Policy Per global/group/user
- Separate rules for Incoming and Outgoing mail
- Spam thresholds (global/group/user)
- Spam quarantine and/or tagging (global/group/user)
- Footnote rules (global/group/user)
- Notification rules (global/group/user)
- Attachment rules (global/group/user)
- Black and White lists (global/group/user/personal)

End-user interface

- Personal Black and White lists
- Personal quarantine management
- HTTP and/or email-based interface

Perimeter-level protection package

- DoES (Denial of Email Service) resilience
- Mail-bombing protection
- Syntax verifications
- Zombie detection & IP Reputation system
- Harvest prevention
- IP Rate limit
- Spoofing prevention for incoming mail
- Spoofing prevention for outbound mail (Anti-Zombie)
- Validation of sender's domain
- SMTP Authentication:
  - Local/LDAP/Forward
  - Brute-force prevention

High Availability

- Integrated Load Balancing
- Centralized cluster management

Reporting

- Mail traffic management
- Administrative daily report
- Detailed statistics and reports
- SNMP Active monitoring
- End-user mail traffic reports

Mail-Server (optional)

- POP3/S and IMAP/S
- Virtual domains support
- Disk quota management
- Automatic mailbox backup
- Secure Web-Access

More Features

- Backscatter prevention
- Masquerading - static and LDAP based
- Mail-routing - static and LDAP based
- Queue management
- POP3 Retriever
- POP3 Transparent proxy

F-SECURE

PineApp Ltd., Tel: +972 4 8212 321, Fax: +972 4 8203 676, Email: info@PineApp.com
PineApp USA, Tel: +1 877 300 3422, Fax: +1 850 219 5728, Email: infoUSA@PineApp.com