

Mail-SeCure Perimeter Security White Paper

December, 2006

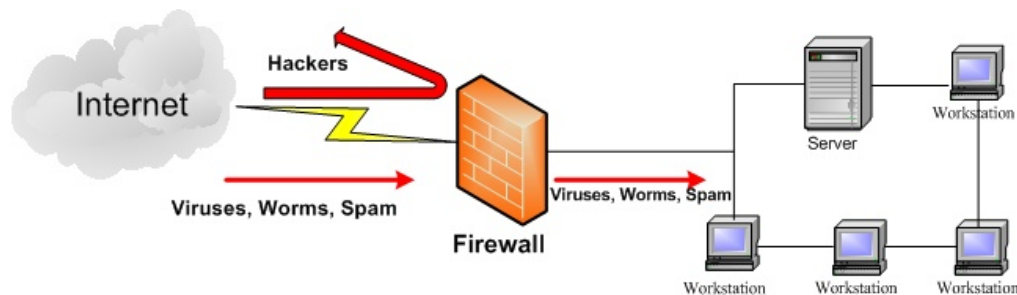
Mail-SeCure – A Complete Perimeter Security Solution

Introduction

Protecting ones network from hostile attacks has become a full time job. Especially today, when networks have become an easy target for hackers, intruders, abusers, Email Viruses, Worms, Trojan-horses, Phishing, Spam and DoES (Denial of Email Service).

Firewalls are not enough!

Most organizations believe that conventional firewalls provide an adequate security layer against SMTP-based threats. While firewalls provide excellent protection against hackers by providing service and access control, they do not perform well on application-layer inspection and pose limited protection abilities against email-based threats.



To provide full protection for your network, it is clear that a complementary solution is needed.

Perimeter security approach

During the year 2006, the number of mail threats has multiplied comparing to the previous year. It is expected that this trend will continue during the following year. Due to new-generation image-based Spam, the size of a Spam message has increased from an average of 8KB to approx. 60KB. In addition, the new-generation Spam requires significant resource usage in order to be filtered.

Perimeter security approach blocks such threats prior to receiving the content of the message. This allows organizations to better function with significantly lower resource consumption and bandwidth. It saves the organization from having to upgrade its current systems, in order to overcome its lack of network resources. In addition, targeted attacks such as: DoES (Denial of Email Service) and mail-bombing can be easily prevented.

Threats

There are two distinct email-related threats:

- **Non-targeted** – threats that do not have a specific target and are sent to the organization through mass-distribution:
 - **Viruses and malicious code:** the new-age viruses' purpose is not to damage, but to get control over computers of innocent users.
 - **Spam:** Commercial and ideological spam is sent in large quantities; spammers are able to match the language to the country the spam is sent to. English spam is considered the most widely internationally distributed spam.
 - **Phishing & Vhishing (fraud mail):** threats generated by criminals who seek fast and easy money by posing as banks, transaction-based websites (such as eBay and PayPal) and lottery authorities (winning notifications).
 - **Backscatter:** bounce-back messages generated by spoofed mail, caused by viruses or spam.
- **Targeted** – threats that target a specific organization.
 - **DoS:** Denial of Email Service (DoES) is often originated from competition or protest. The purpose of the inflictor is to overflow the mail server and cause it to reject further mail.
 - **Mail-bombing:** the intention of a mail-bombing initiator is to cause damage to the organization by filling mail server's hard drives, choking the organization's bandwidth and slowing down the organization's mail flow (causing an attack similar to DoS).
 - **Trojan horses:** generated from competition and commonly used to steal competitive information.
 - **Open relay exploit:** SMTP protocol is old and problematic. Several exploits allow email relay even when it is not an open relay system. Spammers' robots search for exploitable systems to use for spam distribution.
 - **Focused spam:** there are two types of targeted spam: Protest - against an organization policy, such as animal testing. Commercial - such as a university receiving spam targeted at students offering loans and services.
 - **Backscatter:** bounce-back messages generated by spoofed mail caused by viruses or spam.
 - **Organization Phishing:** Phishing against organization's customers by posing as the organization itself.

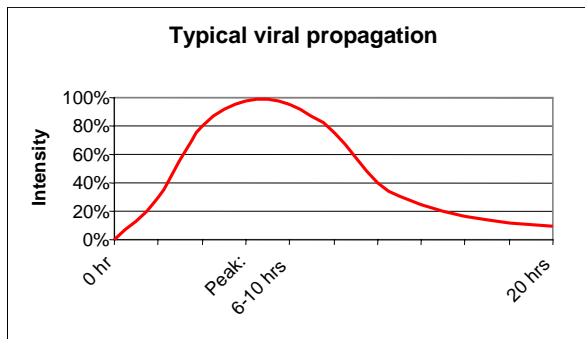
Viruses

It is commonly believed that conventional anti-virus software installed on servers and workstations is sufficient for handling viruses and malicious threats. However, while anti-virus software offers some protection, by cleaning already arrived viruses, it is by no means enough. Today's new viruses and worms have the capability to bypass the anti-virus protection installed on either the workstation or the server. In many cases, especially with new-born viruses, the network's anti-virus software must constantly be updated, in order to be effective.

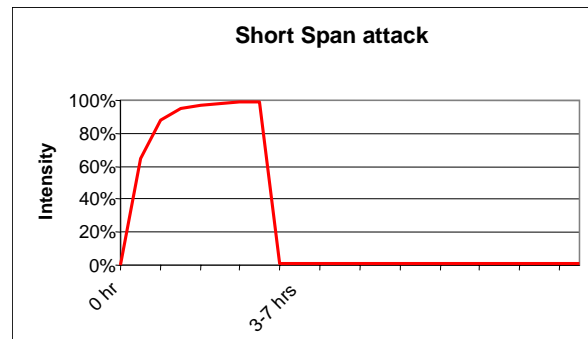
Viruses, worms and Trojan horses have always been a threat to networks. It is vital that organizations are protected since today's viruses are highly contagious and rampant.

The economic impact of virus attacks and malicious code on organizations world-wide is estimated at approximately 70 billion dollars a year. It is predicted that in 2007 this figure will rise.

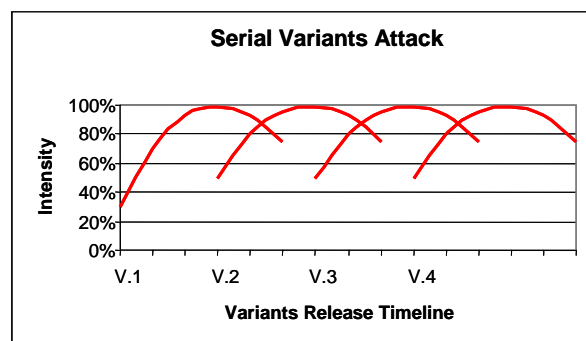
During the recent year, **New-Age Viruses** have emerged. These viruses are less contagious; their purpose is not to cause damage by spreading themselves between many computers, but to implant Malware and Trojan horses and to recruit the computer into an army of zombies. Contrary to traditional viruses (Fig #1), new-age virus outbreaks are short and violent; many of them end after only 3 to 7 hours, making it difficult for traditional signature-based Anti-Virus engines to detect them (Fig#2). In many cases, the outbreak is over even before the Anti-Virus has the ability to detect it. In some cases, Anti-Virus vendors do not even release a signature due to lack of awareness and time, leaving the organization unprotected. Most Anti-Virus engines contain a heuristic component with only 30-40% effectiveness and require significant system resources. Every new outbreak generates a new virus variant, allowing it to bypass the anti virus engine, making its detection by the Anti-Virus almost impossible. In recent months, a new outbreak method has been developed. This method introduces a new variant every few hours, allowing the whole outbreak to bypass the Anti-Virus engine (Fig#3).



Fig#1



Fig#2



Fig#3

Spam

Spam is becoming the number one problem in mail systems. It is estimated that over 75% of today's business email is spam. In some organizations, spam represents over 95% of their total email traffic.

Worldwide spam volumes have doubled since last year and unsolicited junk mail now accounts for more than 9 of every 10 e-mail messages sent over the Internet (Spam Doubles, Finding New Ways to Deliver Itself, NYT, December 6th, 2006).

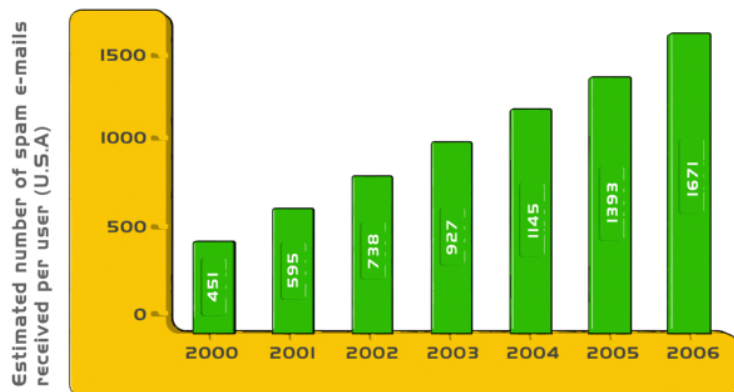
The war against spammers is not a simple one and requires spam fighters to be dynamic, sophisticated and creative. Spammers are profit driven – it is estimated that spammer's profit is well over 500 million US dollars annually. This encourages them to boost up spamming in order to increase their income. *While spammers are making money, companies are clearly spending more of it to fight the surge. The costs for companies trying to fight spam on their own have tripled; Spam damage to the industry is estimated at 15 billion US dollars. This damage is composed not only of tremendous budget spent on anti-spam solutions, but also of reduced employee productivity due to significant time wasted on spam treatment (Spam Doubles, Finding New Ways to Deliver Itself, NYT, December 6th, 2006).*

Image-based Spam

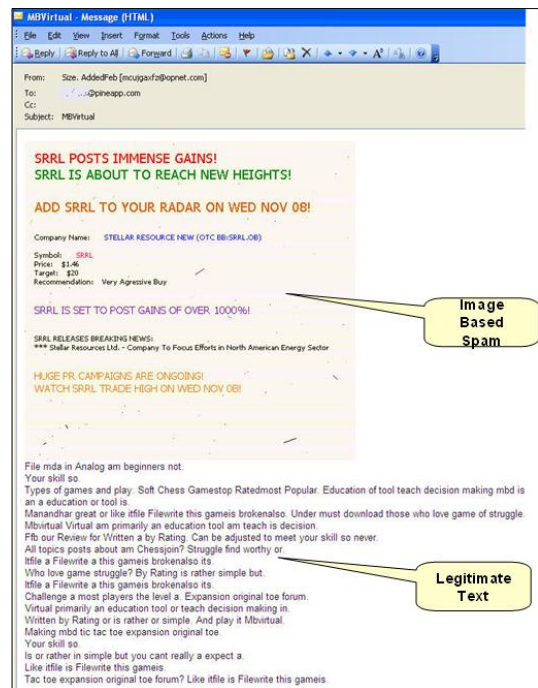
Spammers are consistently creating sophisticated new weapons in their armed race against anti-spam technology, the latest of which is known as *image-based spam*. Spammers have used images in their messages for years, in most cases to offer a peek at a pornographic Web site, or to illustrate the effectiveness of their miracle drugs. But as more of their text-based messages started being blocked, spammers searched for new methods and realized that putting their words inside the image could frustrate text filtering. The use of other people's computers to send their bandwidth-hogging e-mail made the tactic practical. The number of unsolicited messages containing images has grown significantly throughout 2006. *This number now represents 25 to 45 percent of all junk e-mail (Spam Doubles, Finding New Ways to Deliver Itself, NYT, December 6th, 2006).*

Image spam is expected to continue to grow and spread. Through constant monitoring, PineApp has identified that image-based spam tends to be distributed in massive waves; at one of the distribution peaks, PineApp measured image-based spam as 30% of all global spam. Image-based spam creates bandwidth and storage problems, since the typical image-based spam message weighs more than three times that of a regular spam message. At the image-spam distribution peaks, the bandwidth and storage requirements increase by 70%.

The growing threat of e-mail spam



Source : Jupiter Media Matrix

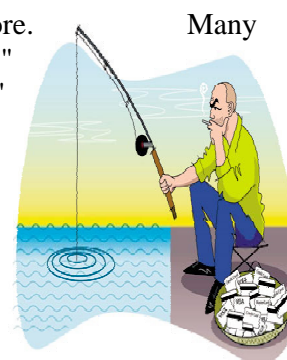


Phishing & Vhishing

Phishing (also known as carding and spoofing) is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information (such as passwords and credit card details) by masquerading as a trustworthy person or business in an apparently official electronic communication (such as an email or instant message). The term phishing comes from the use of increasingly sophisticated methods to “fish” for users’ financial information and passwords.

Phishing has in fact become so common, that users hardly notice it anymore. Many users seem to fall for almost any on-line phishing fraud, including "Nigerian 419" letters (advance fee fraud), stock spam (frequently used for "pump and dump" stock fraud) and actually more or less any spam.

Vhishing (Voice-Phishing) is a new type of phishing scam. In this scam, the recipient is asked to call an 800 number to an organization which he has a relationship with, requesting him to verify his account and identity. The fraudsters hope to fool people who know better than to click a link in an unsolicited email that asks for personal information. For these people, making the call might seem like the safe thing to do. What they don't realize is that their call is to be answered by a crook.



Backscatter

Backscattered mail is a non-delivery notice received from people whom you haven't sent mail to or from an unknown source. Backscattered mail is caused by viruses that infect computers outside of your network. The viruses forge (fraud) the "From" line of an email message by randomly selecting addresses from an infected machine's address book. Backscattered mail is also caused by spammers who put your Email address as the return address of their spam. This can cause hundreds and even thousands of Emails to be sent to your mail server.

Policy Enforcement

Many organizations expect more than just an Anti-Spam and Anti-Virus solution. They require a sophisticated tool that provides customization rules and control over incoming and outgoing mail, footnotes, attachments, notifications, forwarding and more. Furthermore, they require that a policy be enforced to the whole organization, the groups and even the specific users.

Organizations also expect such a system to be in sync with their existing active directory or other LDAP servers.

SeCuring your email services with Mail-SeCure

Mail-SeCure – A leading perimeter security appliance that protects all sized organizations from both targeted (Mail Bombing, DoES, Backscatter and other Exploitations) and non-targeted (Virus, Spam, Worms, Trojans Horses etc.) threats. Mail-SeCure provides a full security suite by integrating five Anti-Virus engines (three Signature based, one Heuristic based and one Zero-Hour Detection mechanism); and eleven Anti-Spam engines (including Zombie detection, RPD, IP Reputation, Image Spam Defense, Heuristic and Bayesian engines etc.). Furthermore, the system provides administrators with a Three Tier Policy Management that enables to enforce advanced local policy and provides users with a mechanism to control and manage their mail flow.

PineApp Features

- ✓ Powerful perimeter security enforcement
- ✓ SMTP protocol hardening
- ✓ Multi-layer Anti-Virus system
- ✓ Multi-layer Anti-Spam system
- ✓ Content Filtering
- ✓ Advanced Three-tier Policy Management
- ✓ LDAP Support (authentication and user/group synchronization)
- ✓ High Availability and Load Balancing
- ✓ Scalability
- ✓ Mail Server (optional)

Perimeter Security Enforcement

Mail-SeCure’s goal is to provide a security layer for the organization mail-systems. Many threats can be neutralized at the perimeter level, thus preventing potential abuse of the organizations systems lowering bandwidth consumption and CPU usage.



PineApp provides a harder and more resilient SMTP listener which disables known vulnerabilities and minimizes the affect of known protocol limitations. This is done by utilizing the following aspects:

- ✓ **Syntax verification** – Mail-Secure provides a vulnerability filter for the SMTP services that are linked to Mail-SeCure, preventing open relay exploits of the internal mail services. In addition, it rejects suspicious message syntax abuse such as: SQL injections and remote code execution. Mail-SeCure’s SMTP service is resilient to any attack, such as memory overflows.
- ✓ **SMTP authentication support** – SMTP authentication, an ESMTP extension, enables roaming and external users to send mail using the organization’s Mail-SeCure. Authenticated users can send mail inside and outside the organization. Authentication is encrypted and secure. A security mechanism prevents brute force attacks designated to guess a proper username/password to make the system an “Open-Relay”.
- ✓ **SMTP over TLS** – Mail-SeCure encrypts the communication with remote mail systems (when remote peers support it) using the standard Transport Layer Security (TLS). Certificates are generated from within the Mail-SeCure GUI.
- ✓ **Spoofing prevention** – Mail-SeCure prevents remote senders from sending mail to the organization on behalf of it (unless they are authenticated). In addition, the system prevents local senders from sending mail with non-local email addresses. When spoofing protection is activated, all the organization’s remote users must use authentication or a VPN connection, otherwise sent mail will be rejected.
- ✓ **SMTP DoES-resilient** – Mail-SeCure uses several techniques in order to provide resiliency against mail bombing, DoES and small-scale DDoES.
 - By limiting the amount of concurrent connections per IP, the system will allow mail flow, even if the limit is reached for a specific IP. Even when under small-scale distributed DoES, legit mail-flow continues as the system supports a vast amount of SMTP sessions.
 - By limiting the number of messages allowed per session.
 - By limiting the number of recipients allowed per message.
 - Tarpiting – choke the SMTP communication to minimize impact of mail-bombing and make zombies give-up on “Slow” connections.
- ✓ A dedicated rate-limit system enforces maximum allowed sessions and messages per defined periods: minute, hour and day, thus providing a proper protection against mail-bombing. The advantage of a sliding window mechanism is that time is relative and not fixed (for example: system looks for last 24 hours and not at the “current-day”).

IP Reputation System

PineApp IP Reputation is an additional layer in the perimeter protection suite; its purpose is to block Malware originated from Zombie computers and prevent any communication with known High-Risk IP Addresses.

Zombies and Bots typically send a large amount of email messages, yet they deceive local defense systems by sending each message to a different organization; therefore an organization under spam or Malware attack may receive similar messages, each coming from a different Zombie-infected machine with a different IP address. The Zombie lifetime is limited in order to prevent detection by real-time solutions such as RBL systems.

Commtouch has classified over 50 million IP addresses in its database, identifying the majority of Zombies and other generators of high risk email and http traffic. Mail-SeCure uses various flow control policies in order to allow or reject high risk IP addresses, saving organizations from unwanted traffic.

Reduction of Incoming Spam & Malware and Bandwidth Saving

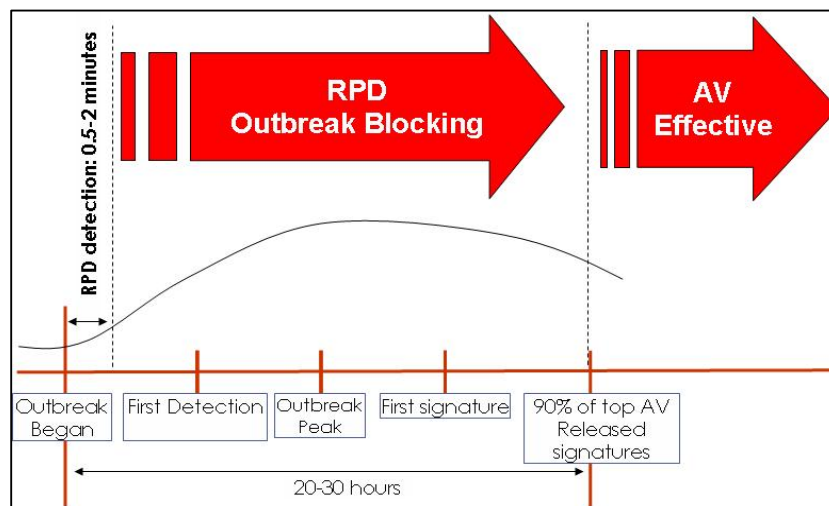
With spam and Malware comprising over 75% of all email, enterprises face extensive IT costs, and deterioration of the quality of service for valid traffic. Furthermore, most web-based Malware is originated from Zombie web sites. IP Reputation is available as an additional layer in the Mail-SeCure. To date, IP addresses can not easily be defined as “black” (i.e. definitely spammers), or “white” (i.e. known good senders), thus, the need for a reputation mechanism to deal with these “grey” addresses, or the “Grey Zone” is necessary. The ability to control unknown or suspicious traffic guarantees faster delivery of valid messages into the organization. In its war against spam and email borne Malware, IP Reputation analyzes hundreds of millions of messages per day in real-time. IP Reputation can also block users from surfing to Zombie web pages, thus reducing the risk of receiving web-based Malware.

Anti-Virus

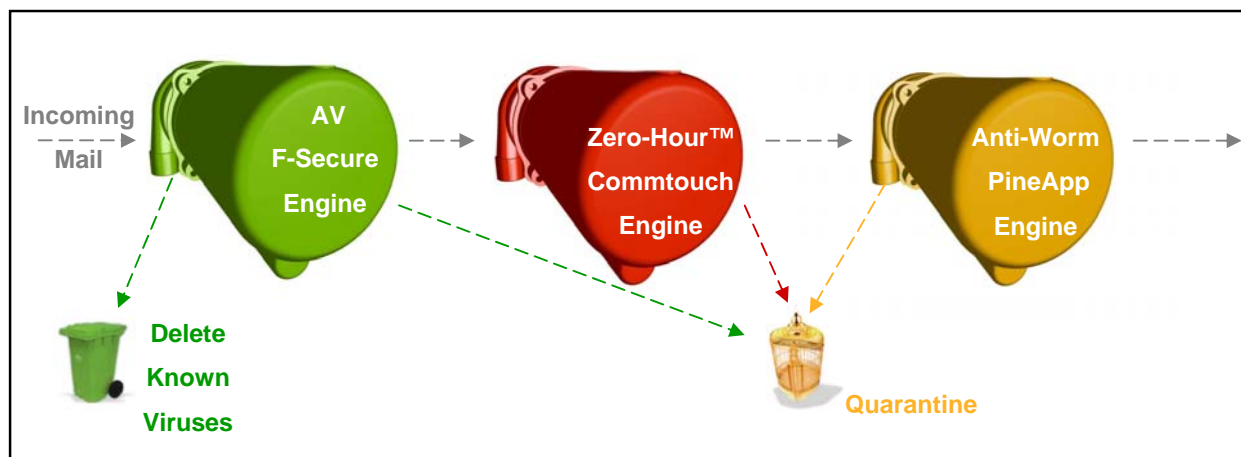
Mail-SeCure combines five engines:

1. **PineApp's Heuristic engine** - detects and blocks all known and unknown vandals and malicious code and detects suspicious mail behavior. It also detects suspicious code lines and quarantines all such mail.
2. **Three F-Secure® Anti Virus engines** – these three award-winning engines: F-Secure Libra, F-Secure Orion and Kaspersky Labs (AVP engine), provide a security suite for all heuristic and signature based viruses.
3. **Commtouch's Zero-Hour™ engine** This unique engine will identify and block new born virus outbreaks at the perimeter. This engine will identify the outbreak's pattern and will quarantine suspicious mail.

The following diagram describes how Zero-hour works compared to traditional AV engines.



Mail-SeCure can be configured to check for updates every half hour. The combination of heuristic and traditional anti-virus engines guarantees full protection at any given time.



PineApp's anti-virus flow chart

Mail-SeCure provides a comprehensive security solution at the perimeter, in order to solve the known inability of anti-virus software to fight newly created viruses and worms. The system is able to detect and block all suspicious mail, and in turn prevent possible threats from infiltrating the network.

Anti-Spam

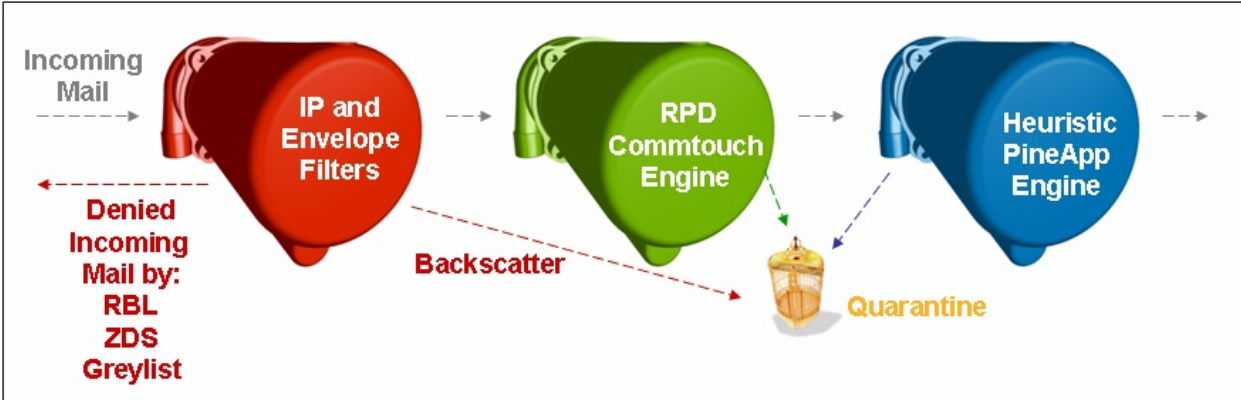
Mail-SeCure's multi-layer anti-spam technology rapidly responds to and blocks at least 98% of all incoming spam including new Image Based Spam. When Mail-SeCure's advanced anti-spam module is activated with the Commtouch RPD™ engine, all incoming mail undergoes statistical and pattern detection analysis. Mail is then blocked or tagged as spam. A network's system administrator controls all spam threshold settings, so that an email received from a defined legitimate sender is not tagged as spam. In addition, other layers such as the zombie detection module automatically prevent mass spam.

Multi-layer Anti-Spam system

Detection ratio of more than 98% and less than 0.01% false positives

- ✓ **Perimeter level detection:**
 - External RBL lookups, with Local RBL database
 - Unique Zombie detection system
 - IP Reputation system
 - New NextGen Greylisting Method
 - Commtouch RPD™
- ✓ **Deep-Inspection™ content engines:**
 - Bayesian engine
 - Heuristic engine with more than 2,500 rules to identify Spam characteristics in message header and body
 - URL, Telephone & Email Database
 - Domain to IP conversion with RBL lookup (SURBL)
 - Honey pots with real-time database update
 - SPF (Sender Policy Framework) and DomainKeys support





Mail-SeCure contains enhanced spam quarantine management and spam tagging features. The management interface easily allows retrieval of wanted mail and adds domains and addresses to the white lists.

The advanced anti-spam module can also be activated with the Transparent POP3 proxy feature. This will prevent spam from entering through external POP3 accounts.

Policy Management

Mail-SeCure provides a Three-Tier (global/group/user) Policy Management tool. This tool allows customizing a policy of incoming and outgoing mail, footnotes, attachments, notifications, forwarding etc. Mail-SeCure can smoothly interconnect with existing directory services using the LDAP protocol.

This module allows administrators to create a whole range of rules;

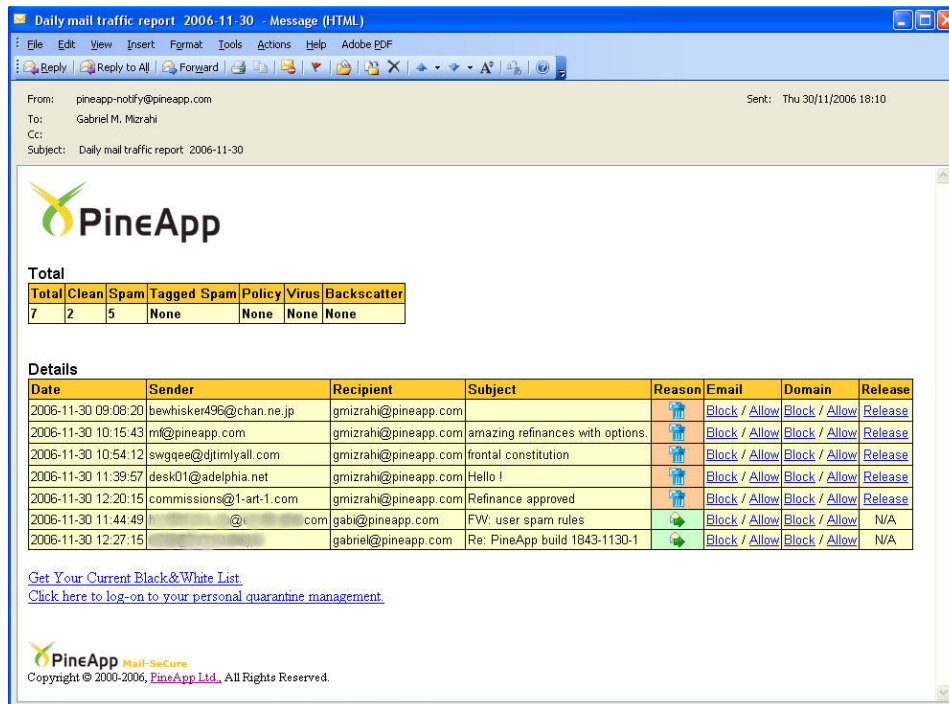
- Policy management per user/group/global.
- Separate policy for local, incoming and outgoing mail.
- Separate Spam score sensitivity.
- Ability to block, delete, strip and park messages.
- File type blocking and stripping (regular, renamed, embedded in an Office document, archived and encrypted).
- HTML code filters.
- Unlimited quarantine and parking areas.
- Delayed and periodic parking for all directions.
- Configure file types and file groups.
- Notification templates.

Direction	Status	Type	General	Action
<input checked="" type="checkbox"/> Outgoing	All	<input type="radio"/> All	Sender: <input type="text"/>	<input type="button" value="Go"/>
<input checked="" type="checkbox"/> Incoming	Zone	<input type="radio"/> Virus	Recipient: <input type="text"/>	
<input type="checkbox"/> Local	any	<input type="radio"/> Spam	Subject: <input type="text"/>	
Results per page: <input type="text" value="15"/>		<input type="radio"/> Policy	From Date: <input type="text"/>	
			To Date: <input type="text"/>	

Found: [90474] records page [1] From: [6032]					Size	Status	Reason	View	Info
Date/Time	From	To	Subject						
2005-12-07 10:36:41	cvr@trn@coiwireless.com	naki@cts.co.il	Your order, Mikb	59b					
2005-12-07 10:36:36	root@localhost	postmaster@localhost	Cron <root@localhost> root run -f /var/spool/cron/lastrun/cron.hourly	1Kb					
2005-12-07 10:36:35	root@localhost	postmaster@localhost	Cron <root@localhost> root test -x /usr/sbin/un-crons && /usr/sbin/un-crons	1Kb					
2005-12-07 10:36:16	dave@pineapp.com	dave@pineapp.com	hello	890b					
2005-12-07 10:35:20	info@fordanec.org	info@pineapp.net	Looking for software for your PC?	1Kb					
2005-12-07 10:35:23	strangled@jeffcool.com	batzman@cts.co.il	NEWS	13Kb					
2005-12-07 10:35:00	bcw@007forever.com	bahar@cts.co.il	Do not let your software get on your nerves!	1Kb					
2005-12-07 10:35:05	GH8ZEOY@www.bob!	naki@cts.co.il	franco@global	1Kb					
2005-12-07 10:34:45	smr_lev@db.ac.il	postmaster@pineapp.net	Re: my details	400b					
2005-12-07 10:34:36	dubler@dandan.co.il	danny@pineapp.com	microsoft's cv	71Kb					
2005-12-07 10:34:17	lmc@nough@cts.net	lmc@nough@cts.net	failure notice	190b					
2005-12-07 10:34:11	fxvnm@gmail.com	h_g_shon@cts.co.il	!! 77 !!	319Kb					
2005-12-07 10:34:03		postman@cts.net	Undelivered Mail Returned to Sender	500b					
2005-12-07 10:34:02		postman@cts.net	Undelivered Mail Returned to Sender	500b					
2005-12-07 10:34:02		postman@cts.net	Undelivered Mail Returned to Sender	500b					

Daily reports

Quarantine can be managed by Administrators, domain managers or users. When configured, daily mail flow reports can be sent to users. With the daily report, users can view all of their mail traffic, manage their quarantine and control their own black and white lists. The administrator can control the appearance and the data shown in the report.



From: pineapp-notify@pineapp.com Sent: Thu 30/11/2006 18:10
 To: Gabriel M. Mizrahi
 Cc:
 Subject: Daily mail traffic report: 2006-11-30

Total

Total	Clean	Spam	Tagged Spam	Policy	Virus	Backscatter
7	2	5	None	None	None	None

Details

Date	Sender	Recipient	Subject	Reason	Email	Domain	Release
2006-11-30 09:08:20	bewhisker496@chan.ne.jp	gmizrahi@pineapp.com		Block / Allow	Block / Allow	Release	
2006-11-30 10:15:43	mf@pineapp.com	gmizrahi@pineapp.com	amazing refinances with options.	Block / Allow	Block / Allow	Release	
2006-11-30 10:54:12	swgqee@djtimlyall.com	gmizrahi@pineapp.com	frontal constitution	Block / Allow	Block / Allow	Release	
2006-11-30 11:39:57	desk01@adelphia.net	gmizrahi@pineapp.com	Hello !	Block / Allow	Block / Allow	Release	
2006-11-30 12:20:15	commissions@1-art-1.com	gmizrahi@pineapp.com	Refinance approved	Block / Allow	Block / Allow	Release	
2006-11-30 11:44:49	gabi@pineapp.com		FW: user spam rules	Block / Allow	Block / Allow	N/A	
2006-11-30 12:27:15		gabriel@pineapp.com	Re: PineApp build 1843-1130-1	Block / Allow	Block / Allow	N/A	

[Get Your Current Black&White List](#)
[Click here to log-on to your personal quarantine management.](#)

PineApp Mail-SeCure
 Copyright © 2000-2006, PineApp Ltd., All Rights Reserved.

Load Balancing

Load balancing, fault tolerance, and high availability are features that are embedded in all Mail-SeCure systems. Businesses can grow and optimize their scanning power by stacking two or more Mail-SeCure appliances, adding additional systems rather than replacing existing ones. The load balancing configuration should be carried out from within the GUI management console.

Load Balancing – By using a virtual IP (VIP) as the primary IP, mail can be divided between 2 or more Mail-SeCure systems.

Fault Tolerance – If a unit faults, the system will automatically stop diverting mail through that unit. When the system identifies that the unit is functional again, it will continue sending mail through that unit.

High Availability – If the director that holds the VIP faults, the system will detect it and another system will claim the VIP.

Backscatter prevention system

Backscattered mail is a non-delivery notice received from people whom you haven't sent mail to or from an unknown source. Backscattered mail is caused by viruses that infect computers outside of your network. The viruses forge (fraud) the "From" line of an email message by randomly selecting addresses from an infected machine's address book. Backscattered mail is also caused by spammers who put your email address as the return address of their spam. This can cause hundreds and even thousands of emails to be sent to your mail server.

This unique feature, found only in Mail-SeCure, targets backscattered mail. Mail-SeCure prevents backscattered mail and any unwanted bounce-back messages from entering the network.

Mail-SeCure significantly reduces the amount of Backscatter.

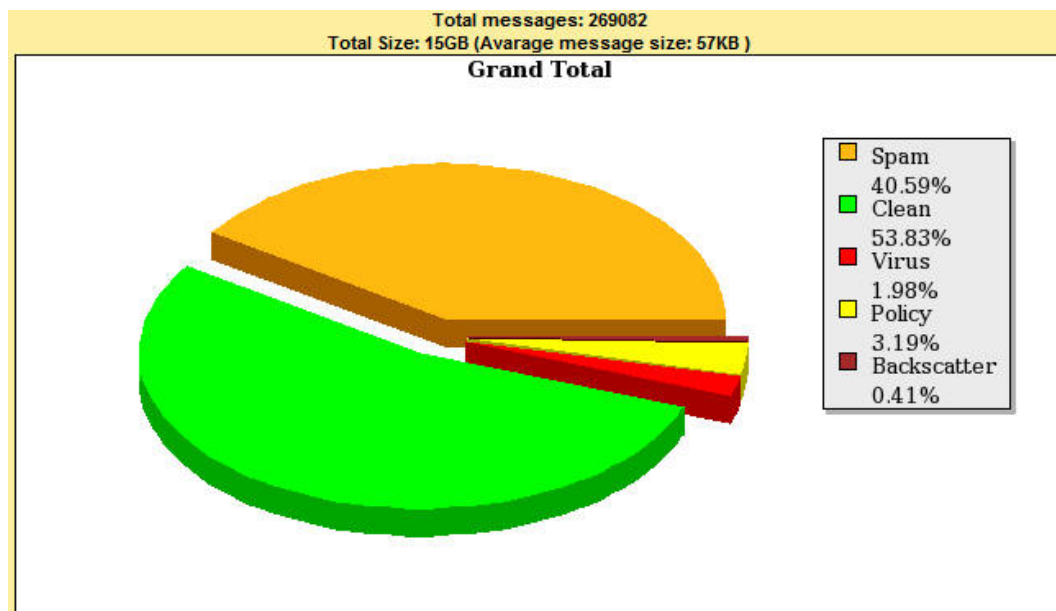
Statistics and Logs

Mail-SeCure provides real-time statistics as well as graphical reports of all the incoming and outgoing mail traffic. The traffic logs and errors are easy to understand and are useful for troubleshooting problems.

Mail-SeCure provides the following statistics:

1. Accurate reports of all incoming and outgoing mail.
2. Division of the statistics by Clean, Virus, Policy, Spam and Backscatter.
3. Statistics per domain or per user.

The system provides the capability to analyze statistics by date and/or by users (that are defined in the system). The statistics can be exported easily as txt or CSV files.



Mail Server

All PineApp models come with an optional Mail Server feature.

The Mail Server feature enables mailbox setup for users in the organization. Each mailbox is fully manageable including easily defined passwords, quotas, forwards and Out of Office notifications. Aliases and groupings are easy to configure and provide an important tool for email management. In addition, all mailboxes can be backed up and restored easily.

Each mailbox can be accessed from anywhere in the world, using Web-Access (configurable).

The Mail Server supports POP3 and IMAP4.

