



Security Management

Put to the test: PineApp Mail-Secure 3.60

Mail abuse prevented by Origin-based Anti Spam measures

15.08.2008 | Author: Ulrich Roderer

With Mail-Secure, PineApp has delivered a security appliance with the ability to monitor mail traffic, filter out unwelcome content, block viruses and stop spam mails. Searchdatacenter.de took a look at the product's performance in practical application.

PineApp Mail-Secure is a 19" appliance; a single rack space in height, equipped with a total of four network interfaces. They may be used within the LAN, to connect to the DMZ, and for WAN connections. The product was geared to serve as an enterprise mail relay. For test purposes, we set up the solution for use as a sort of mail proxy in our network; that is, we integrated it into the LAN and configured our firewall's external port 25 so it would forward incoming mail to the appliance. Then we instructed the appliance to forward checked and filtered mail to a specific mail server in the network. On our test client we selected the appliance as the SMTP server so it would also monitor outgoing mail. We were then able to send and receive mail both locally and via the Internet, all of which were checked by the solution.

Getting started

After connecting the appliance to the network and launching the solution, the administrators must move a configuration client into the C-class subnet 192.168.24.0. Then they can use browsers to access the solution's management interface, available at this URL <https://192.168.24.24:7443>. The administrator account "pineapp" and the password "password" serve for login purposes. The appliance does not compel the IT staff member to change the default password after the first login, but a tip in the quick installation guide notes that this would be the sensible thing to do.

All IT staff members have to do for the initial configuration is go to "Networking/Interfaces", adapt the network configuration comprising the IP address, network mask and gateway to their environment, and reconnect to the product using the solution's new LAN IP address. Next up are the DNS server specifications (under "Networking/General") and the postmaster mail address (in "Mail System/General"). Then it's time to set up the first mail domain (via "Mail System/Local Domains"). For test purposes, we decided to create an SMTP domain and use the mail server as the delivery server in our LAN. Another alternative is to generate POP domains, whereby in this case the IT people enter another mailbox and a login name. After the domain is set up, the user must access "Mail System/Relay Networks" to tell the appliance which network addresses may send mail in the local area network and what the local mail server's IP address is. A manual update of the antivirus patterns in the "Antivirus" menu concludes the mail configuration. By default, the solution works with two mail rules that prevent transmission of executable files via mail and blocks spam mail with a score of six (more on spam ratings later). As far as anti-spam settings go, the vendor recommends activating not only the content-based anti-spam modules, but also Commtouch RPD technology. It uses recurrent pattern detection (RPD) to compare incoming mail with a

database kept up to date by the Commtouch Detection Center's real-time Internet traffic monitoring. RPD works independently of the language in the mail. Also recommended are Zero-Hour Virus Protection, the heuristic engine and PineApp's ZDS. The heuristic engine also uses a Bayes filter and the ZDS (Zombie Detection System) checks sender addresses in real time to determine if they are known zombie addresses with a reputation for slinging spam. To this end, it compares sender info with a database maintained by the vendor.

For the appliance to work properly, the following ports must be open in the firewall: 25 (SMTP) incoming and outgoing, 53 (DNS) and 80 (HTTP) outgoing, and optionally for manufacturer service access, incoming 7022 (via SSH) and 7443 (via SSL). This concludes the initial configuration and the product can go to work.

Configuration

When an administrator logs into the online configuration interface, he ends up looking at an administrative tool that at first glance seems a bit unfamiliar. Nowadays such tools generally work with a menu system on the left that uses a tree structure similar to Explorer or branches out into submenus. The PineApp appliance also features a menu bar, but the submenu items are found at the upper edge of the window. It would appear that this will take some time getting used to, but one soon grows accustomed to it. Beyond this, there are at the top edge outside the menu another two configuration options that should not be overlooked. These serve to select the language - Chinese, English, French, Portuguese, Russian, or Spanish - and determine how many entries the tool shows on one page (for example - for log lists).

The product's default view after logging in is an overview page showing info about the license, software version, serial number, version number of the antivirus database, etc. It also provides details on the network load (with data received and sent in MB), data on uptime and system load, as well as the host names, current CPU temperature, disk utilization, length of the mail queues, and status of mail and/or anti-spam services.

The next panels are relatively straightforward: "Licensing" indicates when the current license expires and allows a new license to be entered. The user management panel not only serves to change the password of the administrative account, but also to add new users authorized to access the appliance (more on this later). Administrators can even have a daily e-mail report sent to users and synchronize user accounts with a LDAP server. The latter was not a problem during the test. The LDAP connectors work with Communigate 5, Exchange 5.5, Iplanet, Lotus Notes, Novell, Openldap, Windows 2000, and Windows server 2003.

Apart from that, system configuration includes another option for generating an SSL certificate, configuring time zones with NTP servers, and a dialog for updating software (here the administrators are also able to view the log; at the time of the test, software version 3.60 was current). Then there are configuration management commands (with backup, restore, download, and upload), a function for saving the configuration and mailboxes using a scheduler (which works via SMB/CIFS and FTP), and a monitoring page that also contains alerts. This page allows personnel to monitor the processor fan, CPU temperature, system temperature, and the temperature of the board. In addition, they can activate SNMP, load the appliance's MIB to their client, and set up a syslog to a central server. Rounding out the system configuration are settings for administering authorized management IP addresses via remote access across SSH or an external modem, as well as a syslog view and commands for rebooting and shutting down.

In the network panel, the personnel not only configure the four interfaces' network settings, but also define the ports for HTTP, HTTPS and SSH services, as well as an HTTP proxy. If necessary, they can define static routes and enter the parameters for static NAT, port forwarding and masquerading. This can be useful, for example, if the product is used in a gateway configuration. An overview page always shows the routing and ARP tables as well as the current status of the individual network interfaces. A ping function is available for testing the connection to certain sites. Because mail relay may also be used in high-availability configurations, the network settings include a cluster management dialog that also allows users to define load balancing settings. Mail-Secure is OPSEC certified, so it also communicates with Checkpoint Firewall-1 and is able to provide IP reputation services to it.

The mail system's configuration is of greater interest. First of all, it offers the option of activating SMTP authentication and SMTP via TLS as well as blocking incoming messages when more than 1000 messages are lined up in the scanning mail queue. Beyond this, the general mail system settings comprise the following options: messaging settings (for the sender or the receiver of suspicious mail and/or the administrator), options for handling bounces, the postmaster's mail address, service banners, a forwarding host and size restrictions for messages.

Domain to host and/or address-to-host conversion affords the administrators the option of configuring the system so that it forwards different e-mails to different servers depending on their domains or addresses. In addition, there is also the possibility of setting up mail retrievers to fetch mail from POP servers at certain intervals and forward mail to defined destination addresses. Administrators employ so-called POP scanning if they wish to use the appliance as a transparent POP proxy. This feature is available only when the solution operates in gateway mode. Backscatter protection serves to counter illicit bounce-back messages, whereby IT personnel are able to enter trusted SMTP IP addresses. Finally, the POP3 access list restricts access to the product's POP service.

The rest of the mail configuration panels are quickly described: A queue info panel with a search function (according to time, mails, size, and the like) keeps administrators posted on the system's actions. Various logs afford insight into mail deliveries as well as SMTP, POP, and IMAP traffic. Conversely, a masquerading function available on demand ensures a user's mail address appears other than it actually is. Mail addressed to {testuser@firma.com} can be rendered as if they were addressed to testuser@firma.de, among other things. Finally, administrators can access additional settings to define the maximum number of simultaneous connections, timeout, messages' lifespan, the number of permissible SMTP authentication attempts per user, and the like.

Rules

Rules determine how the appliance handles mail, which is why policy configuration is the heart of the solution. By default, the product works according to the two aforementioned rules that suppress executable files in mail and spam with scores of six and higher on the rating scale. However, IT personnel can set out many other rules, including content rules serving to check mail for undesirable content.

Various general settings in this panel may be configured so the appliance immediately deletes viruses rather than quarantining the infected mail. Here administrators can determine how the solution handles mail directed to nonexistent user accounts - auto quarantine, auto delete, and so on. "Default Permissions" determine new users' rights to the system - personal spam manager, network managers, read only and so forth. This affords IT personnel the option of adapting permissions for the individual accounts precisely to their given requirements. Of particular interest in this context is a function called "Maximum non-existing recipients allowed within a message before blocking it entirely." It blocks all messages addressed to several receiver accounts nonexistent (for example, 50 percent) within the enterprise. This is how the appliance combats spammers searching blindly for any mail account in the enterprise domain. It is highly likely that more than 50 percent of receivers indicated by these spammers do not exist, while legitimate senders are highly unlikely to ever make this many mistakes.

Policies are defined by means of direction (remote to local, local to local, or local to remote, whereby only incoming spam is checked); the source address or mask; for spam rules the maximum and minimum spam score (that is, the appliance's assessment of the probability that this information is spam - it determines this value for every mail); the categories to be blocked (categories such as drugs, gambling, and violence are available for content rules); forwarding (if desired); and the notifications the system sends to the sender, receiver, or administrator when the rule is acted on. Then there are the response choices - delete, block, park, or allow. All rules may be defined globally, on a group basis, or for specific users. This puts a very powerful tool into the administrator's hands, with which he can influence granularly all mail transactions in his environment, from forwarding to attachment rules and anti-spamming. This functionality was totally convincing in the test.

Mail traffic management offers IT personnel the option of viewing mail sorted by direction, sender, etc. and viewing details on source IP addresses, found viruses, spam score, and the like. In contrast, zone management serves to define park zones and quarantines. Here the administrators can do things like determine for how many days a mail is to be quarantined.

In order to use file types to establish rules - for example, to filter out certain mail attachments - individual file types may be grouped in categories such as "Graphic", "Music and Sound", "Executables," and so forth. This makes it much easier to keep track of what's going on. File types may also be defined here.

Content filtering, which we had mentioned earlier, may be also configured flexibly. Administrators have the option of assigning certain words to categories, adding new rules, and so forth. All categories must be activated within the content filter definition; otherwise they will not be available for rule definition. In the test, we noted that there are indeed categories such as bad words for Dutch, French, and Italian as well as an entry for Russian pornography, but unfortunately the manufacturer has stunted on German content.

Further policy definition options help personnel to create footnotes the system automatically adds to incoming and outgoing messages; view the scanning queue; and define the templates for sender, receiver, and administrator notifications. The people tasked to define templates also have key words such as `_REASON_` and `_ACTION_` available, which they can use in exactly the same way as variables. Thus a definition could look like this:

The reason why your mail was blocked is: `_REASON_`

The PineApp appliance relies on antivirus systems from F-Secure and Kaspersky to combat viruses. The default update frequency is 30 minutes, which may be changed using the configuration tool; the same goes for the scan time limit for a file.

Various methods serve to configure the anti-spam functions. Alongside the spam scoring feature discussed in the section on policy definition and the procedures described in the section on initial configuration, these include spoofing protection, a sender domain check, Treat Commtouch RPD Bulk Classification (which classifies mail addressed to many receivers as spam), and PineApp Nextgen Greylisting. The latter rejects mail from an unknown IP address, sending a "try again" message. Spammers will hardly try to resend their information, but most "normal" mail servers will. On top of all this is the IP Commtouch Reputation System set up as a first-line defense to block spam from zombies - which according to the manufacturer accounts for about 90 percent of all spam - at the SMTP level. Another interesting anti-spam measure is Anti-Zombie Fake SMTP Banner Delay. This feature takes advantage of the fact that most spammers set up connections to mail hosts only if these answer within the shortest time. The SMTP Banner Delay holds up host answers so that most spam senders bail out while normal mail transmissions hold the line.

Optionally, it is even possible to check trusted IP addresses, automatically add all external receivers to the respective sender's white list, forward identified spam as attachments (only in POP proxy mode), and route incoming mail through spam filters even when the transparent POP3 proxy is in use. In addition, administrators can go to the anti-spam configuration panel to define the tagging string by which the system identifies suspected spam messages in the reference line, and if necessary, trigger a report for every spam mail.

What's more, the appliance can work with real-time black hole lists (RBLs) and black as well as white lists on demand. bl.spamcop.net and sbl-xbl.spamhaus.org were activated as the defaults for the RBLs. Finally, a daily report can let users know which actions the appliance has taken, view traffic, and release mail from quarantine. The report is available in Chinese, English, French, Hebrew, Italian, Portuguese, Russian, and Spanish. It is even possible to load one's own logo to the appliance and integrate it into the report.

The last functional area we have to cover comprises statistics and reports. It offers various charts providing views of all mail traffic (including blocked and forwarded mails), SMTP connections, for content analysis, and for outgoing and incoming data. Specific reports may be generated for forwarded, rejected and other similar mail, for SMTP connections, and for mail in general (clean, virus, spam, etc.). Beyond that, the product offers user and domain reports with info on clean and infected mail, as well as spam and the like, at the user and domain levels. These reports may be exported in CSV format so personnel can use them in other applications whenever they wish. The appliance's functional scope also comprises statistics formatted in lists. They provide numeric data on outgoing and incoming connections, blocked mail, identified viruses, and so forth. The statistics feature also supplies average values for traffic per minute, hour, or day. A top list showing the top senders and receivers of viruses, spam and the like at the user and domain levels rounds out the appliance's feature set.

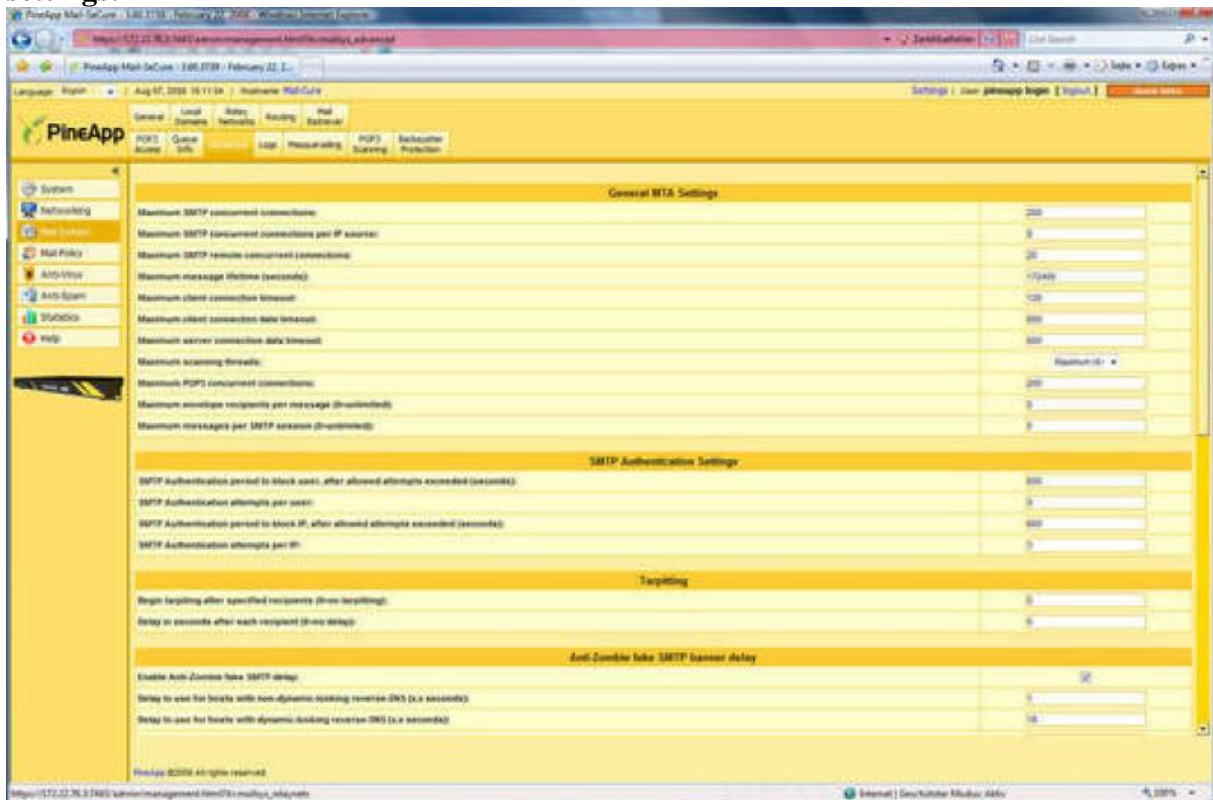
User access

If a user with default rights logs in to the appliance, he can also work with the Web interface. In this case, he has the opportunity to modify his user-specific rules and administer black and white lists of his own.

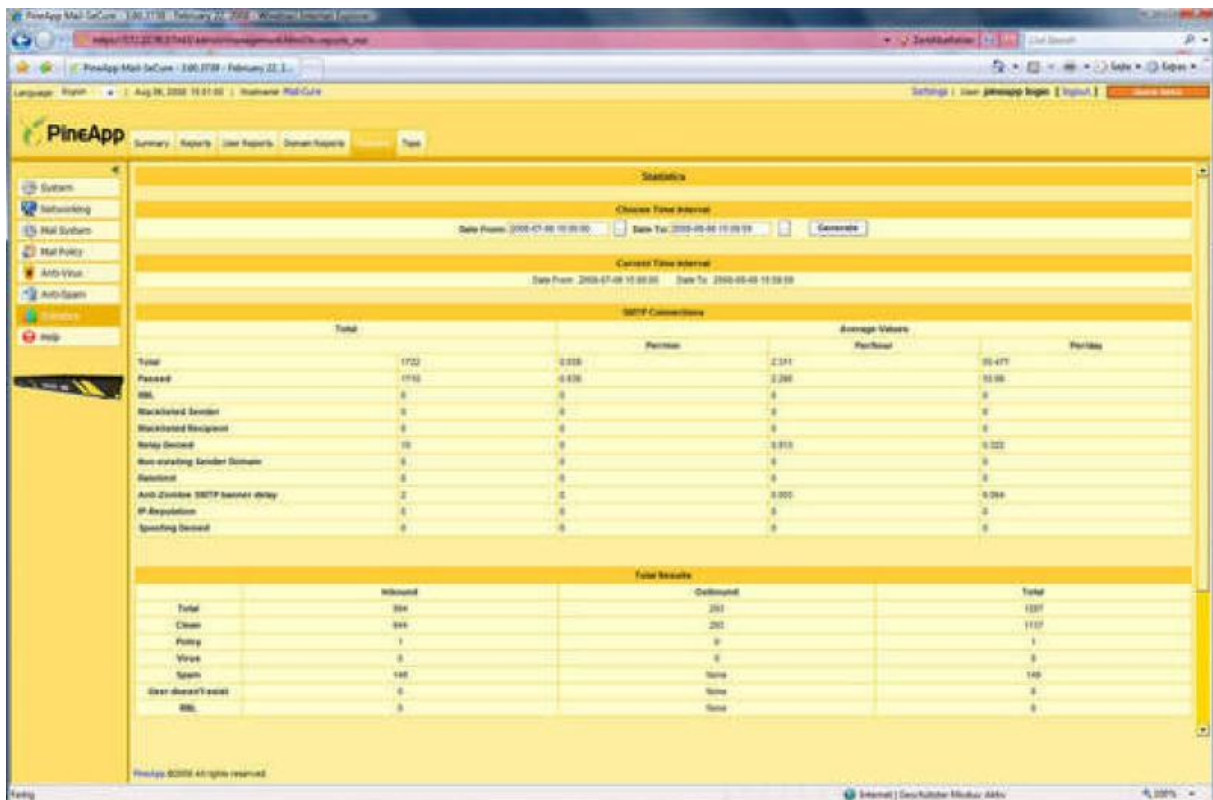
The test

According to the manufacturer, Mail-Secure does 80 to 90 percent of its spam filtering by analyzing source addresses; that is, content scans only account for part of the filtering. Consequently, a test that sends a predetermined amount of ham and spam messages through the appliance in the test lab will not yield an objective result. In this case, all mail stems from the same sender, so the PineApp solution's most important anti-spam measure is ignored in a lab environment. We achieved a recognition rate of just 60 percent in such a scenario. This is why it makes sense to deploy the solution in surroundings where spam mail - like in the real world - comes from different senders. We did this and found the following results: During the test period, our test account received slightly more than 3000 mails, 2500 of which were spam messages. The appliance recognized more than 98 percent of this spam mail, with zero false positives, which jibes with the manufacturer's advertised claim of a 98 to 99 percent recognition rate. This confirms that origin-based anti-spam measures deliver useful results in practice. The product's other functions, content filtering rules, anti-virus engine (which found all viruses in the test), and reports were absolutely convincing in the test. The same goes for the online help. Thus PineApp's Mail-Secure is definitely a recommendable solution with good performance benchmarks. So, let no one be deterred by the initially unfamiliar look of the administrative tool.

IT personnel can influence SMTP traffic precisely using the mail system's additional settings:



Comprehensive statistics provide information about traffic routed through the appliance:



Clear graphics afford insight into the system's actions:

