ASMTP White Paper

6 September 2010

ESCOM® Corporation

Table of Contents

ASMTP White Paper

ASMTP (Active SMTP) is an advanced mail filtering solution developed by ESCOM® Corporation, a Virginia internet security company founded in 1988. The name **ASMTP** (TM) stands for "Active SMTP" and refers to the active filtering methods used to test remote mail servers and e-mail addresses using the Internet standard Simple Mail Transfer Protocol (SMTP).

ASMTP is primarily an anomaly detection engine that uses ESCOM's own patented technology in conjunction with traditional mechanisms for detecting fraudulent e-mail. These traditional mechanism include:

- Local and remote (RBL) blacklists, but ASMTP is not primarily a blacklisting system;
- Sender Policy Framework (SPF) used by Microsoft and other vendors, but ASMTP is much more than SPF;
- Content filtering, but ASMTP will work almost as well without content filtering;
- And ASMTP includes mechanisms to reject mail with malicious content (e.g., viruses, worms, phishing), but is not primarily an anti-virus or anti-phishing system.

What distinguishes ASMTP from other products is the **risk-based active filtering approach** ESCOM pioneered during the late 1990s. Our patented technology identifies desktop clients pretending to be servers, open SMTP relays that can be abused from anywhere in the world, and the use of forged user addresses that are not configured to receive return mail. ASMTP does these tests during the SMTP handshake and without transferring any data.

If you are evaluating spam-filtering solutions, ESCOM's edge is that ASMTP can detect almost all client-based mail and most forged addresses during the SMTP handshake and without transferring any data or attachments. For example, ASMTP's patented **client filter** identifies almost all SMTP Direct connections such as those used by infected Microsoft desktop clients, or **zombies**. Desktop clients were never intended to send unauthenticated SMTP mail direct to servers, and now there's more reasons than ever to block them. ASMTP 4 stops client zombies because it can dynamically distinguish clients from actual mail servers, and block direct client connections. According to David Brittenham at Mo-Net, Inc., a Missouri ISP:

> "Our beta testing with ASMTP 4 showed the client filter to be extremely effective with almost no administration. During a two-month test period, with ASMTP configured to do client filtering for all our users, I did not see any mail accepted from client zombies or any evidence of legitimate mail being rejected by the client filter."

ESCOM has continuously refined ASMTP over the last five years so that a new customer can install ASMTP with no blacklists, no blocked domains, no content filtering, and still reject most spam and other undesirable messages without losing legitimate messages. This pays off in reduced network bandwidth and computer resource requirements, and significantly less administrative involvement. False positive rates are somewhat subjective and vary from site to site, but are usually competitive with false positives from content filtering and static blacklisting.

Large ISPs such as AOL and Yahoo have made huge investments in their own proprietary spam filtering solutions, but smaller regional ISPs cannot afford such investments. Centralized spam-filtering bureaus are good but usually charge on a per-seat or per-message basis. Now ESCOM permits small/medium enterprises (SMEs) and local/regional ISPs to lease ASMTP at a flat annual fee, regardless of the number of users, and get results on a par with the big ISPs and expensive filtering bureaus.

ESCOM's ASMTP technology is available in the following forms, as described at ESCOM's web site:

- **ASMTP Software Distribution CD** that you can install on your own Red Hat Linux, Red Hat Enterprise Linux, Fedora, or CentOS platform. The ASMTP distribution includes three PDF documents and HOWTO files on selecting hardware and loading your selected operating systems. Installation typically takes less than an hour for the Red Hat Linux install and less than an hour for the ASMTP install.
- **ASMTP Appliance**. ESCOM can build hardware-based appliances to order or install the software on your own hardware, but we no longer have a standard hardware-based appliance as we once did. It doesn't make any sense for ESCOM to try to sell outdated hardware at a huge markup, when ASMTP will run on almost any computer that runs Linux.

Overview

ASMTP is a proxy server that protects your mail server from client SMTP direct, open relays, forged addresses, malicious attachments, banned content, and other problems. As shown in Figure 1, ASMTP is usually installed on a separate appliance on a LAN between the Internet and an organization's mail server (MTA). It is also possible to run ASMTP and a Linux-based mail server (e.g., sendmail) on the same computer.

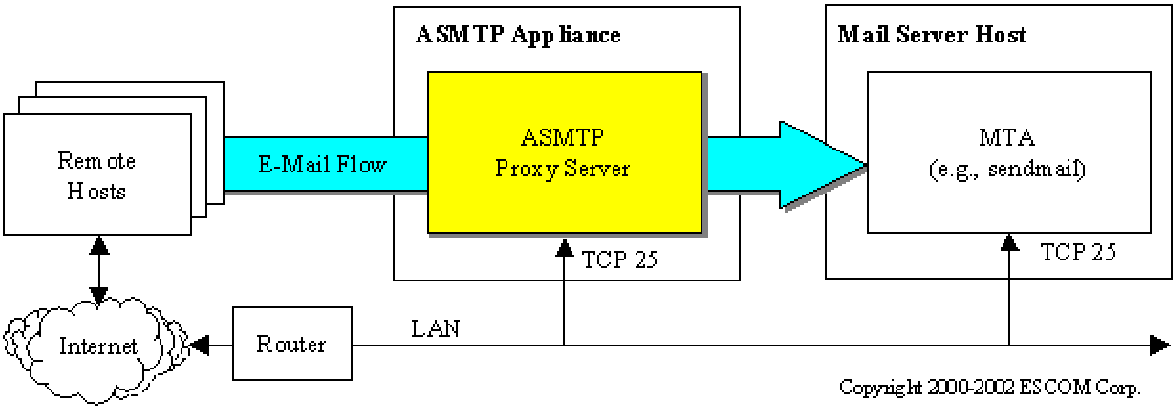

Figure 1. ASMTP Architecture.

ASMTP handles only incoming Internet mail; outbound mail is sent directly from the MTA to the Internet. Incoming mail is directed to ASMTP by defining the ASMTP box as the Mail Exchanger (MX) for one or more local domains. (Similarly, in the event of a hardware failure, you can change the MX record to send mail directly to your MTA.)

ASMTP handles both SMTP (Simple Mail Transfer Protocol, RFC 821) and Extended SMTP (ESMTP, RFC 1425) messages. The remote host selects the mode by sending a HELO message for SMTP or an EHLO message for ESMTP. ASMTP transparently passes all ESMTP protocol data sent with the MAIL From transaction (e.g., SIZE=, BODY=8BITMIME, ENVID=) or during the RCPT To: transactions (NOTIFY=, ORCPT=). It also provides an access point for SMTP authentication (e.g., AUTH LOGIN or AUTH CRAM-MD5).

Because ASMTP uses SMTP to forward filtered mail to the MTA, it is compatible with any SMTP or ESMTP server. Our customers run various versions of Exchange, sendmail, qmail, Domino, Groupwise, MMDF, and other servers. ASMTP provides an internal interface to optional Clam AntiVirus and Bogofilter plugins running on the same platform. ClamAV and Bogofilter are open-source software designed for e-mail scanning on mail gateways. ASMTP can also be chained to various other downstream antivirus or content filters, including content filtering on MTA.

ESCOM configures ASMTP (both appliances and software distributions) so that customers can safely run the ASMTP appliance on the open Internet without a separate firewall. ASMTP uses Linux **iptables** packet filtering to permit access to certain necessary TCP ports (e.g., TCP port 25 must be open to permit incoming mail) and to block access to all unnecessary ports. Sites with firewalls may also install ASMTP behind their firewall (perhaps using translated addresses) or in the firewall's DMZ.

ASMTP is extremely lightweight as compared to handling spam within a mail server. Part of this is the result of a well-engineered inline proxy design, and part of it is because the active filters (client, relay, dns, helo, SPF, etc.) can discard most junk mail (including viruses) without having to do content filtering, virus scanning, or even opening a connection to your MTA. For higher cumulative throughput or improved availability, customers can install multiple appliances in parallel behind a TCP (layer 4) switch or configure MX records for multiple appliance to have the same preference value.

Because ASMTP intercepts (rejects, quarantines, or automatically junks) incoming spam, it keeps almost all spam off your organization's mail server and out of your user mailboxes. This architecture has the following benefits: First, it reduces the processing load on your mail servers because ASMTP is much faster than handling spam on your mail server. Second, it prevents unauthorized relaying via your mail servers, independent of whether your servers block relaying. Third, ASMTP protects mail servers by keeping dangerous messages (e.g., buffer overruns, etc.) and forged addresses off your mail servers. Fourth, ASMTP protects your Microsoft servers and clients by intercepting viruses and other malicious content. And, finally, this design ensures that when your users do reply to messages, these replies will usually be delivered instead of bouncing back to your server and creating even more problems.

Patented Technology

ESCOM holds US and international patents on the following three filters:

- **Client filter**. This filter dynamically identifies SMTP Direct connections sent directly from personal computers (desktops, laptops) pretending to be servers. This includes spam (often the most objectionable spam), viruses, denial-of-service, and phishing messages from compromised Windows zombies.
- **User Address Verification filter**. This filter dynamically identifies nonexistent sender addresses by querying an authorized server (e.g., MX host) for the sender domain whether it will accept email for the sender address. If the servers for the sender's domain will not accept mail for that user, then the sender address is almost certainly forged.
- **Relay filter**. This filter dynamically identifies high-risk open relays using traditional SMTP relaying. It is not that significant any more since Microsoft distributes Exchange in a safe configuration, so it has been extended to detect other anomalies indicative of Microsoft server zombies.

These three patented filters are included as part of every ASMTP software distribution. ESCOM's patents and source code are also available for licensing to integrators, mail-filtering companies, large ISPs, or other businesses.

Functional Overview

Figure 2 shows the key elements of the ASMTP Appliance. ASMTP runs as a proxy server daemon on Linux and FreeBSD, with the operating system providing the networking environment for the ASMTP software. ASMTP runs on any Linux compatible hardware platform with one or more Ethernet devices, including multiprocessor rackmount servers, low-cost tower servers, or even surplus workstations. The ASMTP Appliance also includes the Web-Based Quarantine Server (WebQS), which runs as an extension to an Apache **httpd** server.

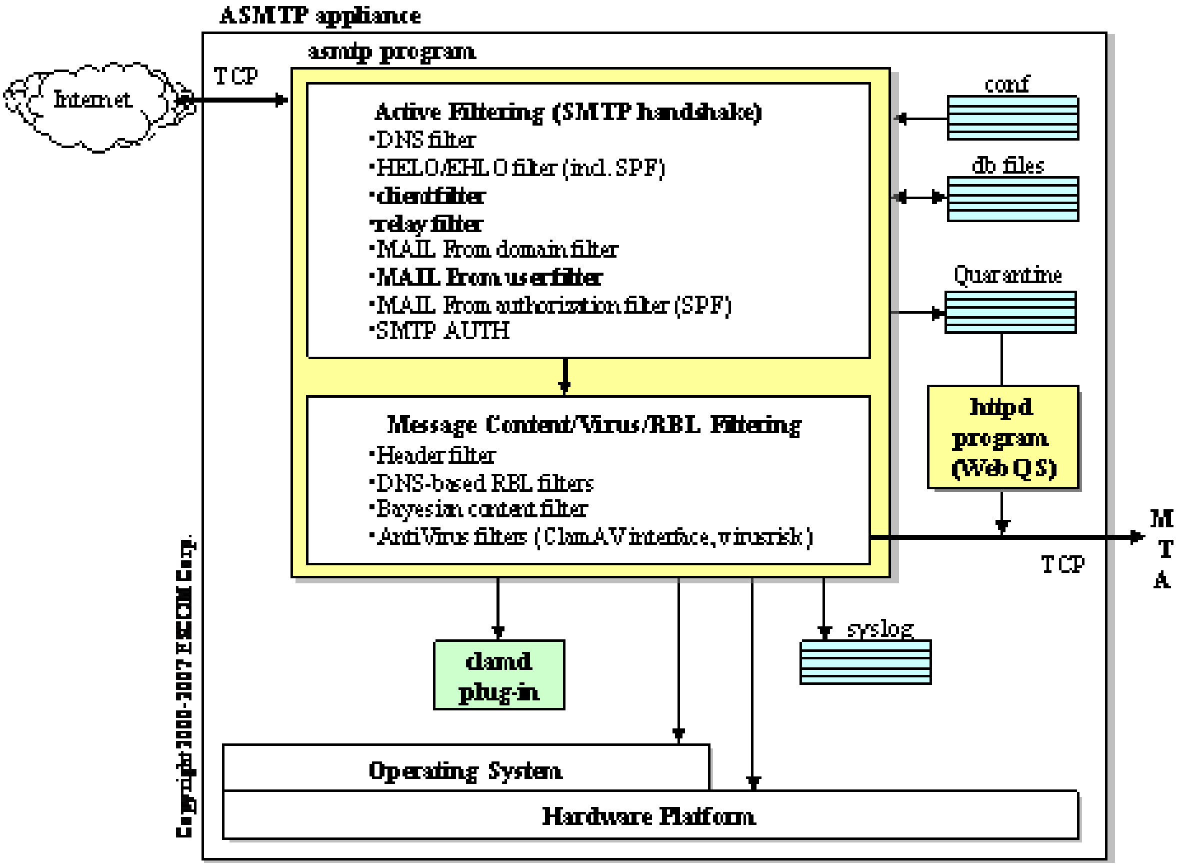

Figure 2. ASMTP Design

ASMTP includes seven Active Filters that operate during the SMTP handshake with the remote host. These active filters dispose of client (zombie) spam, forged HELOs, and forged MAIL addresses without receiving the message header, text, or attachments.

The remaining mail (from servers and with legitimate addresses) is received and filtered by ASMTP's Post-Processing Filters. These include message content filtering, virus filtering, and real-time blacklist (RBL) lookups. ASMTP includes its own native content and virus filters, but also provide plugin interfaces to other products, including the open source Clam AntiVirus and Bogofilter programs. ESCOM builds binary distributions of these programs on separate media for ASMTP customers, and provides the source code for these programs on request.

ASMTP includes about a dozen text and hashed Database Files that local administrators can use, if necessary, to block or enable access. However, ASMTP does not usually require significant database modifications beyond automatic actions performed by WebQS while junking or sending quarantined messages. Support Functions include mechanisms such as SPF, ESMTP processing, resource limits, and SMTP Authentication.

Active Filtering

ESCOM uses the term "active filtering" to refer to ASMTP's use of public information (e.g., DNS records, protocol responses, etc) to identify high risks for spam or other e-mail abuse. These techniques permit SME networks and ISPs to block most spam, viruses, and phishing based on devious behavior, without having to open a connection to the MTA. The remaining well-behaved bulkmail spam (now legal in the US as a result of the Can-Spam Act) can be straightforwardly handled by virus filtering, RBLs, content filtering, and local blacklisting if necessary.

ASMTP has seven configurable filters that operate during the SMTP handshake (connect, HELO, MAIL, RCPT) and one filter that operates during transfer of the message header. These filters are specified in a text configuration file and may be independently enabled/disabled, with exceptions configured for quarantine or rejection (e.g., SMTP 550 response).

A filter is enabled if its specification contains the keyword "filter". Exceptions to this filter are quarantined in a text file on the ASMTP appliance if the filter is enabled and the specification contains the word "quarantine". Otherwise, exceptions are rejected for each filtered recipient at RCPT time. Following is ASMTP's default filtering configuration, but any customer can disable filters or enable/disable quarantine by editing the following text configuration:

```
remote_dns      filter quarantine
remote_helo     filter
remote_relay    filter
remote_client   filter
mfrom_user      filter
mfrom_domain    filter
mfrom_match     filter
msg_header      filter quarantine
```

Remote Filters

The first four filters detect risky configurations at the remote host.

- The **remote_dns** filter does a comprehensive check of the remote host's pointer (PTR) and address (A) records, similar to Wietse Venema's tcp-wrappers software. All internet servers should have complete and consistent DNS information, but sadly they don't, so you should usually disable this filter or set the quarantine flag.
- The **remote_helo** filter checks DNS to determine whether the HELO/EHLO name exists and whether the remote host is authorized to use the name.
- The **remote_relay** filter implements ESCOM's patented Relay Filter. It is instrumental in helping identify hijacked Microsoft servers (zombies).
- The **remote_client** filter is ESCOM's patented Client Filter. This is probably the most important active filter, since it singlehandedly blocks mail from Microsoft zombie clients pretending to be servers. Estimates vary, but probably half of all spam has been sent this way for the last few years. Although classification as a "client" does not mean that a message is necessarily undesirable (after all, that is extremely subjective), but client-based SMTP Direct mail is a significant risk factor. Almost all mail from desktop clients is junk, and there are no acceptable reasons why anyone must of necessity send unauthenticated e-mail from client IP addresses. Comcast, Verizon, and foreign networks such as numericable.fr have mail servers, so users on those networks can forward their mail via those authorized mail servers. ASMTP's client filter has very few false positives, and customers can cut down significantly on zombie spam (and viruses) by enabling this filter and turning off its quarantine flag.

MAIL From Filters

These filters identify anomalies with the SMTP MAIL From (envelope) address. As mentioned in ESCOM's presentation at the February 2004 NIST Spam Workshop (http://csrc.nist.gov/spam), these correspond to the three ways in which a sender address may be forged:

- **Nonexistent domain name in sender address**. For example, if you receive MAIL From: <bob@gov.porn>, then it must be forged because (as of this writing) there is no gov.porn domain in DNS.
- **Unauthorized use of a sender domain name**. If you receive MAIL From: <bob@escom.com> via a server in Argentina, it is forged because ESCOM.COM does not have any servers in Argentina. ESCOM.COM publishes its authorized servers in a SPF (currently TXT) record in DNS so that SPF-aware servers around the world can reject mail with forged @escom.com addresses. As we mentioned above, ASMTP includes SPF as one part of a broader domain authorization filter. This includes additional DNS heuristics and a local db file to cover cases where the sender domain is either not listed in DNS or the SPF record does not specify -all. Customers may add, delete, or modify records in this db file, but most customers never change it.
- **Nonexistent username in sender address**. For example, if you receive MAIL From: <mabelle.wilton@astral.ro>, the patented user filter queries an authorized server (e.g., MX host) for the astral.ro sender domain to determine whether that server will accept email for the user mabelle.wilton. ASMTP performs these tests while the remote host is still connected and without sending a return message, so this detects provably-forged sender addresses without any apparent latency. This filter returns an indeterminate result for domains such as aol.com and yahoo.com that always return 250 responses for all properly formatted RCPT addresses.

Header Filter

Finally, the **msg_header** filter addresses anomalies in the message header, such as, sender address mismatch (envelope vs. Header), absence of a From: address, absence of a To: or Cc: address, absence of external Received: lines, and other problems. This filter occurs during the reception of the message header, but is listed because it uses the same type of filter/quarantine specification as the active filters that operate at SMTP time.

Advantages of Active Filtering

ASMTP's patented active filtering mechanisms are extremely effective in identifying the worst of spam, viruses, phishing, and other SMTP mail where the actual sender does not wish to be identified. There are several reasons for this success:

- Active Filtering is **dynamic**, so it can identify potential spam from IP addresses, domains, and sender e-mail addresses it has never seen before. It uses public information about the remote host and its network instead of relying on a history of prior abuse as with various blacklisting approaches. ASMTP can usually detect the very first relayed, forged, or STMP direct message sent from a completely new mail server. Consequently, as an administrator, you do not have to spend a lot of time adding IP addresses or e-mail addresses to blacklists.
- Active Filtering is **language independent**. It does not require separate databases for Spanish, Korean, French, or Chinese spam. That is because the tricks spammers use are universal.
- By itself, Active Filtering is **content independent**, so it easily handles the cases that have traditionally been a problem for content filtering systems. It does not require a dictionary of alternative spellings, capitalizations, or punctuation. It does not matter if the message is in regular text or HTML, if it is included as an attachment, if HTML text is broken up by embedded tags or comments, or even if the text is presented as a GIF or JPEG image. It handles messages that consist of nothing more than a single URL and it handles messages that contains lengthy quotations or random words that were included to bias probability-based (Bayesian) content filtering techniques.

Active filtering is not a solution to everything but it effectively and efficiently screens client SMTP Direct mail, forged addresses, and other anomalies typically used by those who send spam, viruses, phishing, and other problem messages.

Post-Processing Filters

Active filtering removes the client (zombie) spam, forged HELOs, forged MAIL addresses, and other anomalies from the data stream during the SMTP handshake. What remains is e-mail from servers with plausible HELO names and MAIL From addresses. This smaller subset of messages can be efficiently processed by the following filters: AntiVirus filters, DNS-based remote blacklists, Content filtering, and Backscatter filtering. ASMTP runs these post-processing filters after the remote host sends the end-of-message (i.e., dot) notification.

AntiVirus Filters

ASMTP scans all messages, even trusted, for malicious content (worms, viruses) if one of the following mechanisms is configured.

- **virusrisk file extension filtering**. This filter is part of ASMTP. It rejects, quarantines, or junks messages with dangerous file extensions such as .pif or .scr. About 20 such file extensions and the corresponding action are defined in the virusrisk.db file, but administrators can modify the list as required at their respective sites. The main problem with virusrisk is that it cannot tell whether the contents of a zipped attachment are malicious based on the .zip file extension.
- **Interface to Clam AntiVirus Plugin**. The Clam AntiVirus (ClamAV, http://www.clamav.com) distribution is open-source (GPL) software that includes the **clamd** server, various administrative programs, and related files. ESCOM provides customers with a separate CDROM that contains the ClamAV binaries, an installation script, configuration data, and the unmodified ClamAV source distribution. When ClamAV is installed and configured, ASMTP passes quarantine files to **clamd** and processes the message in accordance with the result returned by the **clamd** plugin.

DNS-based RBLs

ASMTP permits separate IP-based (rblblacklist) and name-based (rblblacklistdom) RBL filters, each of which may reference an arbitrary number of DNS zones (servers). The two types of RBLs are shown in the following records in the ASMTP conf file:

```
rblblacklist sbl-xbl.spamhaus.org bl.spamcop.net
rblblacklistdom postmaster.rfc-ignorant.org abuse.rfc-ignorant.org
```

ASMTP does RBL processing for non-trusted senders after the message is received, which reduces the load on the remote RBL servers and the load on the local DNS server. But more important, this allows ASMTP to get the maximum benefit from RBL servers such as the Spamhaus Register of Known Spam Operations (ROKSO, http://www.spamhaus.org) and Spamcop (http://www.spamcop.net), which handle much of the remaining server-based spam.

Most customers disable the rblblacklistdom filter, but the two rfc-ignorant.org (http://www.rfc-ignorant.org) zones provide effective filtering for domains that refuse to provide postmaster@ and abuse@ addresses. ASMTP contains proprietary mechanisms to quarantine, rather than reject, mail from well-known servers such as Hotmail, Yahoo, and Earthlink which are sometimes listed by rfc-ignorant.

The ASMTP RBL design junks the rejected message instead of discarding it. Thus, if a RBL server blocks mail from one of your customers, you can retrieve the mail later from the junk folder.

ASMTP also includes an rbltrusted interface that enables mail authorized by the Habeas User List (HUL) and by Bonded Sender. These appear to be mostly commercial bulk mail, but presumably they are commercial bulk mail from opt-in senders.

Content Filtering

ASMTP does content filtering for (a) all quarantined messages and (b) all untrusted messages that are being passed to the MTA, using one or both of the following content filters. Both content filters check the message header, body, and text attachments.

- **Native content.db filtering**. The native content.db filter (part of ASMTP) is a two-state (pass, fail) content filter that rejects a message when it finds a single keyword and associated context pattern in the message. It uses database records that are manually created by an administrator entering a keyword and one or more context pattern(s) into the WebQS Databases page. ASMTP tokenizes the data and checks content.db for each token. If ASMTP finds a token in content.db, it checks each context pattern to see if it exists in the message data and junks the message if it contains the token and context pattern. The main advantage of this filter are that it is deterministic and cannot be poisoned by spam that contains random tokens or excerpts from textbooks or newspapers). It also does not require training and the content.db database is relatively sparse compared to Bayesian filtering.
- **Bogofilter Bayesian filtering**. The Bogofilter (http://bogofilter.sourceforge.net) distribution is open-source (GPL) software that includes the **bogofilter** program, related utilities, and other files. The **bogofilter** program is

usually configured to provide a three-state result (Spam, Unsure, or Nonspam) based on a calculated spam probability in the interval 0.0 to 1.0. ESCOM provides customers with a separate CDROM that contains the Bogofilter binaries, an installation script, configuration data, and the unmodified Bogofilter source distribution. When Bogofilter is installed and configured, ASMTP executes the **bogofilter** program as a plugin to scan the specified quarantine file and process the file in accordance with the result. The main advantage of Bogofilter is that it is automatic once it is trained. It is possible to quarantine all Unsures, so that WebQS will train on each message that is Junked or Sent from quarantine.

Bayesian spam filters such as Bogofilter are excellent for filtering mail from major ISPs such as Hotmail, Yahoo, and Gmail that may send a mixture of legitimate mail and spam. It also works well with spam from commercial bulkmail servers, and thus partially overlaps the RBL mechanism. But Bayesian filtering has trouble with (a) spams that contain only a URL and (b) spams that contain additional unrelated data (e.g., excerpts from newspapers) that are intended to poison the wordlist cache. However, ASMTP's active filtering usually strips these problem messages out of the data stream before Bogofilter has to make a decision.

Backscatter Filtering

The term "backscatter" refers to false delivery status notifications (DSNs), out-of-office autoreplies, and other automatic responses bounced from unprotected servers when a spammer forges an address in your domain. ASMTP performs backscatter filtering on non-trusted messages for the null <> MAIL From address and other administrative addresses.

Databases

ASMTP uses about a dozen hashed database files that define the local policy and configuration data. The Berkeley 1.85 database access software can locate any record with only a few disk accesses, regardless of the size of the file. An administrator can manage these files from his or her web browser at the WebQS Databases page, directly with a shell program, or from various scripts. In addition, ASMTP and WebQS make some automatic changes to these db files. These db files provide the following capabilities.

Local Blacklists

ASMTP provides efficient connect-time blacklisting by IP address/block or remote host name/domain. It searches a blacklist database for an exact IP match or class C/B/A subnet match of the remote host IP address. ASMTP also checks a domain database for the remote host name or parent domain match. This permits efficient blocking of entire domain trees, e.g., **`ad.jp`** or even top-level domains such as **`cn`** with a single database record. In its normal configuration, a match by either the IP or domain blacklist will cause ASMTP to display an error response, record a log record, and disconnect from the remote host.

In addition to the normal web-based management functions for all db files, WebQS provides one-click blacklisting of remote hosts (by IP or class C block) on the WebQS Home Page when an administrator junks a message.

Trusted Hosts

ASMTP permits virtually unlimited numbers of trusted domains and IP addresses. If a domain (e.g., escom.com) is configured as trusted, then all hosts in that domain (e.g.,x25.escom.com) are trusted unless overridden by a more specific record. Mail from trusted hosts is unfiltered except for antivirus scanning.

Sender Addresses

ASMTP checks sender addresses following the MAIL From: command. Processing depends on whether the MAIL From address (or MAIL From @domain) exists in the sender database. If so, ASMTP blocks, quarantines, or whitelists the message as directed by the database. However, most addresses are not known to the database, and for these ASMTP performs Active Filtering verification of the MAIL From address.

Recipient Addresses

The recipient database defines the filtering policy for individual recipient addresses and recipient domains. A network with a single domain (e.g., escom.com) and all users configured for filtering might have just a single record:

```
  @escom.com    =filt
```

ASMTP permits multiple recipient domains with potentially different policies. The following example shows how ASMTP handles mail for three recipient domains (@blue.net, @green.com, and @red.org), each with a different default policy. In addition, two users have different policies than their respective domain defaults:

```
@blue.net     =filt
@green.com    =pass
@red.org      =nak
alice@red.org =filt
bob@blue.net  =pass
```

When ASMTP receives a RCPT address (e.g., bob@blue.net, it checks first for the complete address, and if that does not exist, then checks for the recipient domain (@blue.net). When ASMTP matches a recipient address or domain, it uses the filtering policy defined in that record. (If neither exists, ASMTP rejects the message as an attempt to relay through the local network to another domain. Consequently, this mechanism enforces the site anti-relay policy, even if your MTA does not prevent relaying.)

So even though mail is filtered by default for blue.net, if bob@blue.net has a passthrough record, then bob's mail will not be filtered except for connect-time blacklisting or MAIL-time blocking. Further, any message may have multiple recipients, and each may be configured differently. To continue with the above example, carol@blue.net will be filtered (by the default @blue.net record), the nonexistent user ted@red.org will be rejected (by the default @red.org record), and alice@red.org will be filtered.

Again, the recipient database may have only a single record (e.g., "@escom.com =filt") that defines the recipient filtering policy and lists the recipient domains handled by ASMTP. All other recipient domains, e.g., RCPT To: <postmaster@aol.com>, are treated as relay attempts and rejected. It is not necessary to explicitly list all local recipient addresses and so it is not necessary to manually keep the recipient database in sync with the addresses on your mail servers. ASMTP dynamically learns the existence of a recipient address by sending the recipient address to your MTA and observing the response or, if an OpenLDAP (http://www.openldap.org) plugin is enabled, by querying a local directory server to determine whether the recipient address exists within your organization.

Per-Recipient Access Lists

ASMTP permits individual (filtered) users to manage their respective access lists via the WebQS Access List interface. This interface permits users to block remote host IP addresses and domains (essentially, per-recipient blacklisting) and also to block or enable e-mail addresses and domains. These databases supercede all other filtering decisions for a recipient except for connect-time and MAIL-time blacklisting.

Other Databases

Other db files provide support for content filtering, virusrisk attachment filtering, and SMTP authentication. Other databases are continually modified as the result of ASMTP processing.

Support Functions

Resource Limits

ASMTP includes system resource limits and message resource limits. System resource limits (e.g., maximum load average, maximum ASMTP processes) are checked by each new child process, and ASMTP exits with a 4xx retry response to the remote host if the system currently exceeds any configured resource limit.

ASMTP checks message message resource limits (maximum message size, maximum recipients, and maximum number of SMTP messages on a single connection) and gives a retry response to the remote host.

Sender Policy Framework (SPF)

ASMTP includes ESCOM's SPF (http://spf.pobox.com) implementation for HELO, MAIL From, and header filtering. It permits five layers of includes and redirects and includes proprietary extensions to handle domains that do not specify mismatch rejection (-all).

HELO/EHLO Processing

ASMTP supports standard SMTP and ESMTP extensions such as AUTH, SIZE, 8BITMIME, and other transparent extensions passed via MAIL or RCPT commands. The processing at HELO/EHLO time is part of the remote_helo filter and includes SPF, domain existence, and other proprietary checks to determine if the remote host is authorized to issue the HELO/EHLO name.

SMTP Authentication

ASMTP supports AUTH LOGIN, CRAM-MD5, and PLAIN authentication methods. A particular site may configure all of these methods, or any subset. An authenticated sender becomes trusted even if from a DHCP client on a foreign network and is permitted to send outbound mail to domains other than those listed in the recipient database.

WebQS and Quarantine

Figure 3 shows how ASMTP sends some messages directly to the MTA, rejects some messages, and quarantines others.

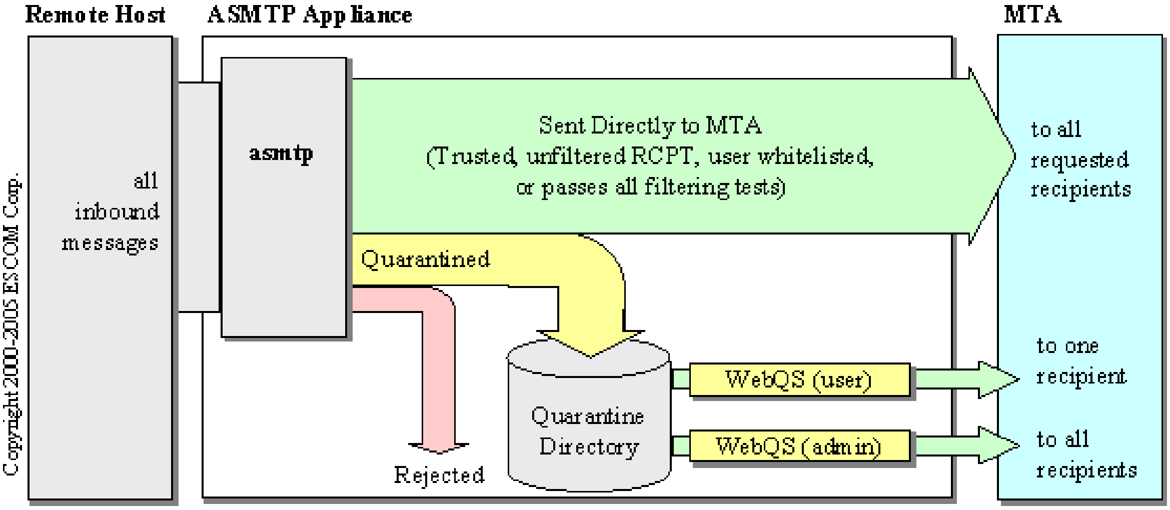

Figure 3. Quarantine Message Flow

Quarantined messages are saved in text files in the asmtp spool directory. Each file contains the remote host name and IP address, SMTP transactions (MAIL, RCPT, DATA), and the message itself (header, body, attachments).

A message sent to multiple recipients may be quarantined for some recipients and delivered to the MTA for others, depending on the per-recipient filtering configuration and per-recipient access lists. A message quarantined for multiple recipients is stored as a single file with multiple RCPT addresses.

ASMTP's quarantine mechanisms ensure that filtering is fail-safe. For example, if a message is quarantined because the sending host has a bad DNS configuration, that message is available for review and can be forwarded by an administrator or by any of its recipients. Mail that is forwarded from quarantine storage is temporarily delayed but is otherwise indistinguishable from mail sent directly to the mail server.

ESCOM's Web-based Quarantine Server (WebQS) is the preferred tool for reviewing, and junking or sending quarantined messages. WebQS is a password-protected service that is available to administrators and to individual recipients with a web browser. The WebQS functionality is an extension to the Apache **httpd** server so WebQS has the look and feel of any other web page, however, WebQS generates dynamic HTML to provide the following information:

- **List all unresolved quarantine files**. The home page is presented as a table with one message per row. An administrator sees all quarantine files, while an individual recipient only sees his or her own messages. The user display shows the subject and sender's address for each message, and provides links to junk or send the message. An administrator's display includes the remote host name as a blacklist link and recipients. The home page provides links to sort by date/time (default), subject, sender address, or first recipient and radio buttons to provide other administrative options.

- **View the contents of a quarantine file**. When an administrator or user clicks on the Subject of a message, WebQS displays the quarantine file itself. HTML within the header or body of a message is disabled to prevent downloading malicious content and "web bug" tracing of legitimate addresses.
- **Junking and Sending messages**. WebQS provides multiple selection via Junk and Send radio buttons for each message. A single Submit junks all messages selected as Junk and sends all messages selected as Send to the MTA. This clears all selected messages from the home page listing. When an administrator junks or sends a message, it is junked/sent for all recipients, while a user action pertains only to that one recipient.
- Other functions. WebQS provides interfaces to change one's password (administrator and user), enable/disable filtering (user only), display statistics and log files (administrator only), blacklist the host or Class C that sent a particular message (administrator only), display and edit access lists (administrator and user), manage the hashed database files (administrator only), execute OS commands (administrator only), and send spam complains (administrator only). It also provides a means for new users to sign up for access to WebQS.

Installing ASMTP

The ASMTP software is provided as a CDROM distribution for customers to install on a Red Hat Linux, Enterprise Linux, or Fedora system. ASMTP has an Installation Guide (PDF) that covers all installation issues, and various HOWTO files (text) that describe how to install the underlying Red Hat system. Installing the Red Hat OS according to one of the HOWTO files takes on the order of an hour if you haven't done it before. The ASMTP installation takes about two minutes and ASMTP configuration may take from 2-10 minutes depending on how closely you review its progress.

ESCOM also provides binary distributions on separate CDROMs for recent Clam AntiVirus and Bogofilter distributions. These typically take a minute or two each to install, but you should also read the COPYING file if you are unfamiliar with open source software licensed under the GPL.

Using ASMTP

We do not believe there is any enterprise spam filter that works perfectly out of the box and runs on autopilot with no administrative involvement. However, ASMTP comes pretty close. ESCOM has been installing and testing "bare bones" installations for almost two years, configured as follows:

- Change recipient database to filter for all recipients (e.g., @escom.com =filt).
- No initial IP, domain, or sender address blacklisting.
- Default trusted domains.
- All Active Filters enabled, with remote_dns and msg_header quarantined.
- Typically two or three RBL servers, including spamcop.net and spamhaus.org.
- ClamAV and Bogofilter installed, with Bogofilter configured to quarantine all Unsures for training.

We typically see ASMTP active filtering blocking over 95 percent of all spam on these minimally-configured systems, with content filtering (e.g., ClamAV and Bogofilter) and RBLs cumulatively blocking or quarantining almost all of the remainder. Thus, active filtering blocks the junk that sometimes causes problems for content filtering, and content filtering and RBLs block mail from well-configured bulk mailers.

Some spam (mostly commercial bulk mail) and some legitimate mail is quarantined, but the volume decreases as you train Bogofilter and blacklist some senders. If you have Bogofilter configured, WebQS incrementally trains Bogofilter to recognize all Junked messages as spam and all Sent messages as nonspam (Ham). Just check the appropriate radio buttons on the WebQS home page and click Submit.

Administrators may blacklist remote hosts that send quarantined spam by clicking the remote host IP or Class C links on the home page. Blacklisting is desirable (and sometimes even necessary) for some sources, e.g., foreign domains you've never heard of or spew-only bulk mailers, but it is not necessary to "blacklist the world" to control spam. We recommend blacklisting the following:

- Undesirable mail that makes it through ASMTP to your mail server and is reported by your users.
- Network abuse, e.g., denial of service attacks or address probing.
- Quarantined spam, viruses, phishing, etc. Blacklisting these remote hosts saves you time by stopping them from quarantining more of the same.
- To optimize resources (bandwidth, memory, etc), you may want to blacklist the remote hosts that are blocked by RBLs, ClamAV, or Bogofilter. Static blacklisting is much more efficient that receiving and scanning entire messages.

Summary

ASMTP combines several "best of breed" technologies, such as ESCOM's patented client and user address verification filters, non-proprietary domain authorization based on SPF (plus our own extensions), and open source software such as ClamAV and Bogofilter.

ASMTP leases are now available for an unlimited number of users for under $1000 per year. Call ESCOM at 703-620-4823 for a no-obligation trial of ASMTP 4, or to inquire about licensing patents or software for use in your own products.