Global Information Assurance Certification Paper

How to stop Spam and Viruses at the Mail Gateway

By Francois Yang

GSEC CERTIFICATION
Case Study Version 1.4b Option 1
August 10, 2003
30 Day Retake

Table of Content

Summary

Due to the increasing amount of viruses found each year and new methods of spamming. Users are forced to waste many hours just going thru spam each year and IT personnel to spend hours recovering data from computers that have been infected by viruses. E-mail is one of the fastest ways for businesses to communicate with others, but it is also one of the fastest ways to bring down a whole network. Viruses such as Klez, Bugbear and Sircam could have been prevented from reaching user workstations by implementing a mail gateway setup. A mail gateway is a server that sits in front of the actual E-mails server and filters all incoming and outgoing E-mails for unwanted content and viruses.
Once the E-mail is scanned and spam or virus free, the gateway passes it on to the actual E-mail server for processing.
This document will discuss how to minimize the amount of spam and viruses from getting inside the corporate network, by implementing a mail gateway with Postfix and RAV Antivirus.

Spam

- What is it and how can we stop them?

According to mail-abuse the definition for spam is.
"An electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender." (http://www.mail-abuse.org/standard.html)
Spam can be any E-mail that you didn't request and that may contain some type of advertisement for products and services. Spam does not only waste time and money, but it can also trick users into clicking on links that can infect their workstations or be a way to collect valid E-mail addresses and install programs. There is not one solution to block spam from getting into a network, but there are ways to minimize them.
Postfix and RAV Antivirus both have many rules that you can setup to fit your need to reduce the amount of spam you receive.

Viruses

- What are they and how can we stop them?

According to McAfee "a virus is a man made program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised as games or images with clever marketing titles such as "Your order is ready" or "Hi"". (http://www.mcafee.com/anti-virus/default.asp)
Putting filters and anti-virus software at the mail gateways can minimize the spread of viruses in a corporate environment. It will prevent the viruses from reaching the servers, workstations and the risk of someone launching them. In addition to having filters at the mail gateways, all workstations and servers should have an anti-virus program running in case the gateway doesn't stop the virus.
Also all anti-virus programs should be updated at least weekly, either manually or automatically. If the anti-virus is not updated, it will only detect old viruses and not any knew ones.

Postfix

- What is it?

Postfix is a Mail Transport Agent (MTA) that was created by Wietse Venema to replace Sendmail. (http://www.postfix.org/)
According to Wietse "Postfix attempts to be fast, easy to administer, and secure, while at the same time being sendmail compatible enough to not upset existing users."
(http://www.postfix.org/motivation.html)
Postfix is one of the most secure MTA by default. It separates all it's process, so that one process cannot be use to control another one. It is also very easy to configure and manage.

- How to use Postfix to fight spam and viruses.

Postfix has the unsolicited commercial email or UCE control rules that you can setup to limit the amount of spam you receive. It also has the option to add real-time blackhole lists or RBL servers to the main.cf file to block well-known spammer domains and addresses. It can be set to check if an address is spoofed or valid and has the ability to create White and Black lists. An address is spoofed when someone is making itself appear as a different address. White lists are a list of IP's or Domains that you want to accept mail from. Black lists are a list of IP's or Domains that you want to reject any E-mails from. Postfix has many options and the way you will configure them will depend on your network and what you attempt to achieve. To give an idea of what postfix UCE settings will be covered, here is part of what a main.cf file may look like. All the files that it refers to, will have to be created before adding them in the config. If the files are not created prior to adding them to the main.cf file, it won't work. Postfix will pop up with a lot of error messages and may not route any mail. It is important to know that Postfix processes the configuration file from top down. If a rule is causing a lot of false positive, you can move it down.

```
transport_maps = hash:/etc/postfix/transport.map
relay_domains = $mynetworks, hash:/etc/postfix/transport.map
smtpd_recipient_restrictions =
 reject_unauth_pipelining,
```

```
 reject_non_fqdn_recipient,
 reject_unknown_recipient_domain
 permit_mynetworks,
 reject_unauth_destination,
 check_client_access hash:/etc/postfix/mta_clients_bw.map,
 check_sender_access hash:/etc/postfix/from_senders_bw.map,
 check_sender_access regexp:/etc/postfix/from_senders_bw.regexp,
 check_client_access regexp:/etc/postfix/mta_clients_dul.regexp,
 reject_non_fqdn_sender,
 reject_unknown_sender_domain,
 check_sender_access hash:/etc/postfix/from_senders_mybogus.map,
 reject_rbl_client blackholes.wirehub.net,
 reject_rbl_client dynablock.wirehub.net,
 permit
header_checks = pcre:/etc/postfix/header_checks.regexp
smtpd_helo_required = yes
smtp_always_send_ehlo = yes
strict_rfc821_envelopes = yes
strict_7bit_headers = yes
# Modify the banner as desired from "Attn:" onwards
smtpd_banner = $myhostname - ESMTP - $mail_name - Attn: Authorized Personnel
Only
message_size_limit = 5120000
header_size_limit = 512
```

UCE DESCRIPTIONS

- reject_unauth_pipelining

Pipelining is when a Mail Transport Agent or MTA sends several SMTP commands at the same time without waiting for a response for each command. Spammers use this technique to send spam quickly thru misconfigured servers. They also use this to run dictionary attacks in attempts to gain access to your network.
Turning on reject_unauth_pipelining will make sure that each command gets a response before going to the next one.

- reject_non_fqdn_recipient

When this option is turned on, Postfix will makes sure that all E-mail addresses in the "rcpt to" field are fully qualified domain names (fqdn). An example of a fully qualified domain name is "yourdomain.com".
yourdomaincom or yourdomain.h are not fqdn.
Postfix will reject anything that is not an fqdn. It will not waste any resources trying to resolve a non existent domain.
reject_non_fqdn_senders
When turned on, makes sure that all E-mail addresses in the "From" field are fully qualified domain names. All E-mails with a non fqdn will be rejected right away.
This will prevent Postfix from trying to send bounce messages to non existent domains.

- reject_unknown_recipient_domain

This option will reject all E-mails going to unknown domains or domains without an A or MX record. Postfix will not attempt to deliver an E-mail if it can't resolve it.

- permit_mynetworks

This parameter determines what network you want to allow Postfix to relay mail for.
In order to properly use this option, you will have to add your network and only the subnets that you want Postfix to relay mail for.
Example:
mynetworks = xxx.xxx.xxx.xxx/x
It will only accept connections from itself, xxx.xxx.xxx.xxx/x and drop everything else.

- reject_unauth_destination

This option tells Postfix to reject all E-mails unless the destination domain or sub domain matches the one you specify in "relay domains "in your main.cf file.

- check_client_access

This is where you would specify who you want to accept or reject SMTP connections from. You will need to create a database for it to search.
The database can be in dbm, db or regexp format depending of the type you want to use. To build a database for a dbm or db format, you would issue the command " postmap /etc/postfix/database " then " postfix reload " to reload the configurations. These procedure needs to be done every time you make a change to the file. For regexp database, you don't need to do anything. Once you update the file, it will work.
Here are examples of how the file should look like.
db:
xxx.xxx.xxx.xxx OK
yyy.yyy.yyy.yyy ACL mta_clients_bw
This will allow all connections from xxx.xxx.xxx.xxx drop all connections from yyy.yyy.yyy.yyy.
It will send an error message back to the sender telling them that it was rejected by "mta_clients_bw". This will help you troubleshoot why an E-mail was rejected.
regexp:
/(docsis|dsl|client|dhcp|pool|cpe|host|cust|dial|access|in\-addr|arpa|cable|nombres|upc\-[a-z]|user|bri\-).*\..*\.[a-z][a-z]/ 554 ACL mta_clients_dul
This will reject any E-mail from any MTA whose names contains any of the expressions.
To find out what the MTA's name is, you can type this command.
"host domain"
You will get something like;
"domain has address xxx.xxx.xxx.xxx"
"domain mail is handled (pri=1) by mail.domain.com"
If the name mail.domain.com contains any of the expressions above, Postfix will reject the E-mail.
This will cause some false positive if you're not careful. It is more geared toward a corporate environment; it will drop a lot of connections from some dialups, cable and DSL ISPs.

- check_senders_access

It allows you specify whom you want to accept or reject mail from based on their E-mail address or domain.
This parameter looks at the sender field of the E-mail and not the MTA connection.

You will also need a database for this option. As mentioned above the database can be in db or regexp format and you must run the postmap and reload commands for the changes to take affect.

db:

someone@theirdomain.com	OK
spamer@hisdomain.com	554 ACL from_senders_bw
@spam.com	554 ACL from_senders_bw

This will allow your server to accept mail from someone@theirdomain.com even if it was hosted on a DSL line or the MTA had the word DSL in its name.

It will also reject all mail coming from the E-mail address spamer@hisdomain.com and the domain spam.com, but still accept mail from all other addresses from hisdomain.com.

regexp:

/@b\./ 554 ACL from_senders_bw

This will reject all mail coming from any domain that contains @b.*.

- reject_unknown_sender_domain

Postfix does a reverse lookup of the domain to verify that it is a valid domain.

It rejects all connections from the senders when the sender's domain doesn't have a valid DNS A or MX record. This will reject all the fake domains that spammers are trying to use or spoof. It can also reject good E-mails when there's a DNS problem or when the remote server does not have their reverse lookup setup properly. It doesn't matter whether the problem is on your server or the remote server. If Postfix cannot resolve the address it will drop it.

- real-time blackhole lists

It is a list of known mass mailing MTAs or spammers E-mail addresses and domains. They are updated by different organizations and people who choose to help by reporting mass mailers. Most of them are free, but some require a small fee. Setting up multiple RBLs in you postfix config will help you stop more unwanted E-mails, but you will have to watch your resources.

The way they work is every time you receive an E-mail, the client is run against the RBL list to see if it finds a match. When a match is found, Postfix rejects the E-mail and logs which RBL found a match. If no matches are found, Postfix moves to the next rule.

You can enter as many RBL list as you want, just remember that it will run the client against all of them, and could potentially become a bottleneck if the bandwidth or server can't handle the traffic. If a legitimate domain is being listed by one or multiple RBL as being a potential spammer or mass mailer, you can white list it. White listing, means that when Postfix, sees that IP address or domain, it will automatically send the E-mail without going thru the other rules.

RBLs are enter in the main.cf file this way.

reject_rbl_client rbl_site

- header_checks

By default the header_checks allows anything in the E-mail header.

You can specify what to reject in the header by creating filters and having Postfix run checks against them.

If a match is found, Postfix will function as specified in the file.

The functions are to reject, ignore, warn, hold, discard or filter.

I use only the "reject" to reject all the matches, and "warn" for testing new rules.

The warn option will deliver the E-mail, but log it as matching a rule.
This will help determine how much false positive can be cause by a rule and if it's worth implementing it.
Some simple rules look like this.
/^Subject:.*(phentermine|viagra|xenical|valtrex|propecia|zyban|claritin|meridia|retin\-a|hgh)/ REJECT
Will reject any E-mails that the subject match any of the words in the string.

/^.*name\=\".*\.(pif|shs|shb|ini|cmd|do|hta|reg|net|com|vbs|scr|dll|lnk|hta|vbe|js|jse|bat|vxd|shm)\"$/ REJECT
Will reject any E-mail with the matching double extensions.

- smtpd_helo_required and smtp_always_send_ehlo

smtpd_helo_required will require that all SMTP sessions start with a HELO.
This will stop a lot of bulk mailing programs, because they don't send any HELO commands. They only try to send mail thru as quickly as they can.
smtp_always_send_ehlo tells Postfix to always send a HELO when it wants to initiate an SMTP session. This will prevent other servers with similar configurations to reject your E-mails.

- Strict_rfc821_envelopes

This option will allow you to decide what is allowed in the MAIL FROM and RCPT TO fields of any E-mail. When turned on, it will only allow E-mails with E-mail addresses in the two fields. Anything else will be rejected. This will stop spammers that try to add extra codes and miss configured servers. To turn on this option, add the following line to the main.cf file.
strict_rfc821_envelopes = yes

- Strict_7bit_headers

Only allows E-mails with 7-bit into the header. Some E-mail servers still send 8-bit headers and will be block.
To turn on the field add this line to the main.cf file.
strict_7bit_headers = yes

- Banner

Always modify the banner to state that no UCE is allowed.
That may discourage some people from using you as a relay point for their spams.
To change the banner, add the following line to the main.cf file.
smtpd_banner = $myhostname - ESMTP - $mail_name - Attn: banner
Your banner will be after the "Attn:"

- message_size_limit

Lets you specify the maximum size of all E-mails being routed thru the server.
E-mails that are too big can cause a denial of service or crash the system.
When setting up the size, remember to use 1024000 Bytes for 1 MB to calculate the appropriate size.
The message size is set by adding this line.
message_size_limit = 5120000
This will limit the size of acceptable E-mails to 5 MB. 5 x 1024000 Bytes = 5120000 KB

- header_size_limit

Setting a limit to the header size will limit the amount of addresses in the RCPT to field.

Most E-mails will fit in a 256 byte header, but you can make it 512 if you're felling nervous about making that small.
This will reject E-mails from bulk E-mail systems, who sends an E-mail with hundreds of E-mail addresses in the to field. To setup the header size, you need to add this line to your main.cf file.
header_size_limit = 512

Setting Postfix with these settings will reject most of the spam and some viruses trying to come into your network, but it is not enough. A lot of viruses now days, will use Your E-mail address or someone in your address book to send itself to others. Postfix will pick most of them up when doing a reverse lookup and determining that the IP address doesn't match the domain, but some will match up and they will be let thru. Spammers are also using miss configured and compromised servers to send their junk mail. In those cases, the reverse lookup will pass, and Postfix move on to other filters. If an infected E-mail passes all the filters, Postfix won't know that it is infected and will send the bad E-mail. For this reason you will still need an Antivirus to scan all E-mails who makes it past Postfix for viruses. RAV antivirus is very easy to setup and has daily updates to protect against new viruses.

RAV Antivirus

RAV is a multiplatform antivirus that has the ability to do virus scanning, spam filtering, content filtering and message stamping. The following parts of RAV is what makes it a good anti virus for your gateway. The Multi Layer Embedded Scanning Technology or MLES gives the ability to scan within embedded attachments for viruses. The Heuristic Method Technology or HMETH gives the ability to scan E-mails for virus behaviors and possibly detect unknown viruses. The Bulk Mail Stop or BMS gives the ability to scan all E-mails headers and body heuristically for spam characteristics. The Content Filtering Technology gives the ability to scan by subject, filename and body of any E-mails for any specified rules.

- How to use RAV to stop spam and viruses

When E-mail arrives at your server, the RAV daemon intercepts the E-mail and scans it for viruses, content and integrity. If the message passes all the filters, it then passes the message back to the MTA, in this case Postfix who then runs its own rules and filters before it delivers the E-mail. You can customize RAV to take different actions for different occasions. All network are not the same, so RAV will only be configured to suit your network. This is how a general setup would look like.

- Stopping Spam with RAV

When an E-mail is received, RAV proceed by first running the mail client against a White/Black list. If the client is listed in the White list, it will be sent directly to the scanning engine to scan for viruses. If the client is not in the White list, if will then be run against a list of RBLs before being sent to the scanning engine. After the E-mail is scanned and virus free, it will be run against RAV's anti-spam engine. The engine looks for known spam characteristics in the header and body of the E-mail. There are four

level of accuracy, low, medium, high and very high. Unfortunately RAV will not disclose specifically what the engine is looking for.
The White/Black list is a list of IP addresses and E-mail addresses that you either want to accept or reject mail from.
The White/Black list and spam accuracy can be setup in the "global" file located in "/usr/local/etc/rav/".
White list wbl_accept yourdomain.com
Black list wbl_reject spammerdomain.com
antispam_configuration = bulk_very_high_precision
The RBL list is setup in "/usr/local/etc/rav/rbl_settings".
rbl_site = rblsite.com
After every changes you make you must run "killall –HUP ravmd" to restart RAV and apply the changes.
You don't have to use the RBL option of RAV if you're already using Postfix.
It's pointless to run an E-mail against multiple RBL sites twice. It will only slow down mail delivery. To disable the RBL option, simply comment out the line by putting a # in front of it.

- Stopping Viruses with RAV Antivirus

RAV's virus definitions are updated everyday to help fight against new viruses.
The virus update is a small script that you can schedule to run at anytime for your convenience, by setting up a cron job.
RAV can be configured to clean, move, copy, delete, rename, ignore, reject and discard any infected E-mails.
To configure RAV's actions, edit the file "/usr/local/etc/rav/actions"
RAV can also be setup to perform multiple actions when a virus is found.
One way of setting up multiple actions would look like this;
act_for_infected_files = clean, delete, discard
This would tell RAV to clean the infected E-mail before sending it to the recipient. If the file can't be clean, it will delete it then discard it.

- clean

The clean action will tell RAV to attempt to clean the infected file before sending the E-mail. If the E-mail can not be cleaned, RAV will perform other actions that you've setup in the configuration file. If no other actions are specified, RAV will reject the E-mail.

- move

The move action will move the infected E-mail to a folder for later reviewing.

- delete

The delete options will send the body of the E-mail to the recipient, but will replace the infected attachments with a "warn.txt" file. The "warn.txt" will be the same size as the original attachment. So if the infected attachment is 250kb then "warn.txt" file will 250kb. If the infected is 5mb then the "warn.txt" will be 5mb.
The size of the attachment has to be the same size or some E-mail programs and protocols may not like it and reject it. RAV will patch the "warn.txt" file with spaces to match the size. If the attachment is really small, only part of the "warn.txt" file will be sent.

- reject

The reject option will reject the E-mail and send a bounce back to the sender.

- discard

The discard option will silently discard the E-mail and not send any notification to the sender. This will prevent spammers from finding good E-mail accounts.

You can set RAV to automatically notify the sender, client and administrator when an infected E-mail or attachment is found. You can setup who will receive the notification in the "global" file, usually located in "/usr/local/etc/rav/groups".
The notification can be customize in the "/usr/local/etc/rav/languages/english" file.
infected_m_english = "
The file ATTACH_NAME attached to mail (with subject: SUBJECT) sent by FROM_USER to TO_USER (S)
is infected with virus: VIRUS_NAME."

ATTACH_NAME is the name of the attachment that was sent.
SUBJECT is the subject of the E-mail.
FROM_USER is the E-mail address of the sender.
TO_USER(S) is the E-mail address of the recipient.
VIRUS_NAME is the name of the virus that RAV found.

Setting up RAV at the mail gateway with these configurations and with Postfix will stop most viruses and spam attempting to enter your network. Again the configurations will depend on your network and the amount of false positive will depend on who send E-mails to your work place.

- Helpful Tools

There are numerous tools out there to help administer E-mail servers, but two of them really stand out for what they do. Pflogsumm.pl and spam-stats.pl, are good tools to have because they give a good overview of a server's workload. Pflogsumm.pl (http://jimsun.linxnet.com/postfix_contrib.html) will generate a custom report of your E-mail traffic. It can display the total number of sent and received E-mails for the day, the top senders and recipients E-mail addresses and the top sending and receiving domains. It will also give details about bounced, deferred or reject E-mails and some SMTP errors and warnings. It also lists all the E-mail addresses that were rejected and what rules rejected it. It will help you determine how many false positive you have. This will also show all the stmp warnings that are generated by experimental rules.
Spamstat.pl (http://taz.net.au/postfix/scripts/) will generate a report about how much spam was rejected by looking thru your mail logs.
The report will show which RBL or postfix setting rejected the E-mail, how many they rejected and the total count. Because the rejecting RBL is listed, you can notify the remote client of their status and have them contact the RBL site to have the removed.

Conclusion

Spammers are always finding new ways to bypass our defenses against spam.
Users are forced to spend many hours on company time reading and deleting spam.
Virus authors are writing more and more complex viruses everyday.
Trojans, backdoors, Denial Of Services and mass mailing worms are just examples of viruses that can easily spread thru E-mail and take down a network.

There is no single solution to stop all spam and viruses from entering your network, but by implementing Postfix and RAV together at a mail gateway, you can minimize the amount of threat that enters your network. Postfix has the ability to reject E-mails based on their Header, size, subject, body content and attachments. RAV Antivirus will scan all E-mails for viruses before passing it on to Postfix for processing. If a virus is found it has the ability to clean, quarantine, delete and discard the E-mail and also automatically notify the sender, recipient and administrator of the event.
Having just one will not due. You need something like Postfix to do all the filtering and integrity checking, and RAV for all the virus scanning.

Resources

1. RAV Antivirus User Guide
ftp://rav.raeinternet.com/pub/rav/mailservers/documentation/pdf/ravmailservers842-usersguide.pdf

2. RAV Antivirus Configuration Guide
ftp://rav.raeinternet.com/pub/rav/mailservers/documentation/pdf/ravmd.conf.pdf

3. Craig Sanders spam-stats.pl website
http://taz.net.au/postfix/scripts/spam-stats.pl

4. Jimsun's pflogsumm.pl website
http://jimsun.linxnet.com/postfix_contrib.html

5. Hoang Q. Tran "Configuring Mail Gateway Using Postfix"
http://www.muine.org/~hoang/postfix.html

6. Mail abuse website
http://www.mail-abuse.org/standard.html

7. Mcafee's website
http://www.mcafee.com/anti-virus/default.asp

8. Len Conrad's IMGATE
http://imgate.meiway.com/

9. Postfix UCE settings and descriptions
http://www.postfix.org/uce.html

10. Postfix's resource settings and descriptions
http://www.postfix.org/resource.html