Some Email Best Practices

Kevin Chege

SPF

- SPF – Sender Policy Framework
  - SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record (or TXT record) in the Domain Name System (DNS).
- *@ IN TXT “v=spf1 include:gmail.com ip4:1.2.3.4 mx -all”*
- The above will only allow mail from IP 1.2.3.4 and any server in the domain with an MX record
- If not sure use a generation tool online
  - http://www.mtgsy.net/dns/spfwizard.php

Domain Keys Identified Mail (DKIM)

- is an email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is authorized by that domain's administrators and that the email (including attachments) has not been modified during transport. A digital signature included with the message can be validated by the recipient using the signer's public key published in the DNS.
- DKIM requires cryptographic checksums to be generated for each message sent through a mail server
- Modern MTA can both sign and verify DKIM
- Information about DKIM for a domain is stored in DNS via TXT records
- Generating keys for emails results in computational overhead not otherwise required for e-mail delivery.

DKIM Part 2

- DKIM allows the signer to distinguish its legitimate mail stream. It does not directly prevent or disclose abusive behavior.
- This ability to distinguish legitimate mail from potentially forged mail has benefits for recipients of e-mail as well as senders, and "DKIM awareness" is programmed into some e-mail software.

Reverse Records

- Have reverse records (PTR) for your mail server so that it is resolveable from the IP
- Mandatory by most servers these days
- Used to verify authenticity of the sending mail server
- The IP Address must resolve back to the mail server name
- You can have multiple reverse records
- You can have an SPF record that states that any IP that has a reverse record can send email from your domain
- *IN TXT "v=spf1 ptr:domain.co.tz ip4:1.2.3.4 mx -all"*

Use Anti Spam and Anti Virus software

- Will reduce overall spam and email received
- You can also have a mail “firewall” or gateway aka Mail Filter to stop spam before it reaches your server
- Some softwares are:
  - Spamassassin (AntiSpam)
  - ClamAV (AntiVirus)
  - MailScanner and Amavisd (use the above)
  - Maia Mail Guard
- When setup try a penetration testing site to see how well your server can protect you from SPAM and Viruses

GreyListing

- Valid mail servers will have no problem if the receiving gives a soft error (4xx)
- They will attempt to send the mail again after some time
- Greylisting configured on a receiving mail server will give a soft error (4xx) to the sending server and store the IP/Hostname of the sending server in a file
- If the sending server returns again after some time (can be specified usually 5min) the email is accepted
- Used as a measure to deny mail from bots that are compromised to send mass mail. They often do not try again if the server did not accept the mail

Accept only well formatted messages

- Sender must be a valid name not an IP ie not user@192.14.5.6
- Mail server HELO name must be resolvable ie FQDN
- Server identification must resolve ie HELO/EHLO name must be resolveable
- Email should be from a valid email address format eg: from tom@example.com and not from tom@example

Security

- Run secure pages from the mail server and secure SMTP to clients
  - Secure Webmail – port 443
  - Secure SMTP – port 465/587
- Force clients to use secure IMAP or Secure POP
  - Secure POP – port 995
  - Secure IMAP – port 993
- Require authentication on your mail server before a mail enters the queue from a sending client aka SMTP AUTH

Use Blacklist databases

- Use DNSBL – DNS Based Blackhole Lists or RBL (Real Time Blackhole lists) to deny mail from well known spamming machines
- Some well known good ones are
  - SORBS – http://sorbs.net
  - SPAMHAUS – http://spamhaus.org
  - SPAMCOP – http://spamcop.net
  - MANITU – http://manitu.net

Require strong Passwords

- Advise users to use strong passwords or passphrases for their email
- Alphanumeric passwords are better than normal passwords ie combine letters with numbers
- Passphrases are even better, more difficult to break
- Use your mother tongue ☺

Backup and Redundancy

- Have multiple MX records so that your server is not the only one able to receive mail for you
- Backup your mail, use tools like Rsync to copy mail to another server as often as you can
- Ensure your DNS records (MX, NS etc) are correct and test them when you complete you setup
- Use online tests like
  - http://intodns.net

References

- Wikipedia and Google
- http://www.linuxmagic.com/best_practices
- http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

Postfix Mail Server

Kevin Chege

ISOC

What is Postfix?

- **Postfix** is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail, intended as an alternative to the widely used Sendmail MTA.
- Postfix is released under the IBM Public License 1.0 which is a free software licence.
- Originally written in 1997 by Wietse Venema at the IBM Thomas J. Watson Research Center and first released in December 1998, Postfix continues as of 2014 to be actively developed by its creator and other contributors. The software is also known by its former names **VMailer** and **IBM Secure Mailer**.
- In January 2013 in a study performed by E-Soft, Inc. found that approximately 25% of the publicly reachable mail-servers on the Internet ran Postfix.

Postfix

- Works on UNIX-like systems including AIX, BSD, HP-UX, Linux, MacOS X, Solaris, and more.
- It is the default MTA for the OS X, NetBSD[3] and Ubuntu operating systems
- Used by: AOL, Apple Server, Stanford University, United States Navy, NASA, Rackspace, many ISPs

Some Key Features

- SASL authentication
- Mail forwarding or delivery
- "Virtual" domains with distinct address-namespaces
- A large number of database lookup mechanisms including Berkeley DB, CDB, OpenLDAP LMDB, Memcached, LDAP and multiple SQL database implementations
- Extended
  - Deep content inspection before or after a message is accepted into the mail queue;
  - Mail authentication with DKIM, SPF, or other protocols;
  - SMTP-level access policies such as greylisting or rate control.

Postfix on Debian

- Installed via: **$sudo apt-get install postfix**
- Directories:
  /etc/postfix
- Configuration files
  - main.cf - stores site specific Postfix configuration parameters while
  - master.cf – defines daemon processes

main.cf

- specifies a very small subset of all the parameters that control the operation of the Postfix mail system
- you will have to set up a minimal number of configuration parameters.
- Postfix configuration parameters resemble shell variables
  - parameter = value
  - other_parameter = $parameter
- Postfix uses database files for access control, address rewriting and other purposes

main.cf Key Settings

- myorigin = $myhostname
  - specifies the domain that appears in mail that is posted on this machine. Defaults to the value of the machine's hostname
- mydestination = $myhostname, localhost
  - specifies what domains this machine will deliver locally
  - if your machine is a mail server for its entire domain, you must list $mydomain as well in this setting
- The mydomain parameter specifies the parent domain of $myhostname. By default, it is derived from $myhostname by stripping off the first part (unless if the result would be a top-level domain)

Relaying Mail – From

- Postfix will forward mail from clients in authorized network blocks to any destination
- Authorized networks are defined with the mynetworks configuration parameter
- The default is to authorize all clients in the IP subnetworks that the local machine is attached to.
- By default, Postfix will NOT be an open relay ie it will not forward from IPs outside your network to the Internet
  - mynetworks_style = subnet
  - mynetworks = 127.0.0.0/8 168.100.189.2/32

Relaying mail - to

- By default, Postfix will forward mail from strangers (clients outside authorized networks) to authorized remote destinations only.
- Authorized remote destinations are defined with the relay_domains configuration parameter.
- The default is to authorize all domains (and subdomains) of the domains listed with the mydestination parameter.
- This means that by default, your Postfix mail server will accept mail from anyone to recipients to the local Postfix server

Outbound emails

- By default, Postfix tries to deliver mail directly to the Internet.
- Depending on your local conditions this may not be possible or desirable
- For example, your system may be behind a firewall, or it may be connected via a provider who does not allow direct mail to the Internet.
- In those cases you need to configure Postfix to deliver mail indirectly via a relay host.
  - relayhost = [mail.isp.tld]
  - Note that the [] disables MX lookups so is necessary

Reporting problems

- You should set up a postmaster alias in the aliases table that directs mail to a real person
- The postmaster address is required to exist, so that people can report mail delivery problems.
- While you're updating the aliases(5) table, be sure to direct mail for the super-user to a human person too.
  /etc/aliases:

  ```
  postmaster: afnog
  root: afnog
  ```
- After editing the aliases file, run the command *$sudo newaliases*

Default reports

- bounce
  - Inform the postmaster of undeliverable mail. Either send the postmaster a copy of undeliverable mail that is returned to the sender, or send a transcript of the SMTP
- 2bounce
  - When Postfix is unable to return undeliverable mail to the sender,
- delay
  - Inform the postmaster of delayed mail. In this case, the postmaster receives message headers only.
- policy
  - Inform the postmaster of client requests that were rejected because of (UCE) policy restrictions. The postmaster receives a transcript of the SMTP session.
- protocol
  - Inform the postmaster of protocol errors (client or server side) or attempts by a client to execute unimplemented commands.
- resource
  - Inform the postmaster of mail not delivered due to resource problems (for example, queue file write errors)
- software
  - Inform the postmaster of mail not delivered due to software problems.

Logging

- Postfix will log all messages to /var/log/mail.log
- Done using the syslogd daemon
- All transactions of messages coming in being sent out of the server will be logged
- Logs will contain details like hostnames, recipients, time and date, and whether the email was queued or dropped

Postfix Daemon process chrooted

- Postfix daemon processes can be configured (via the master.cf file) to run in a chroot jail
- The processes run at a fixed low privilege and with file system access limited to the Postfix queue directories (/var/spool/postfix).
- This provides a significant barrier against intrusion.
- The barrier is not impenetrable (chroot limits file system access only)

Interfaces and Protocol

- The inet_interfaces parameter specifies all network interface addresses that the Postfix system should listen on
  - inet_interfaces = all
- inet_protocols parameter specifies which protocols Postfix will attempt to use
  - inet_protocols = ipv4, ipv6

Starting, stopping and logs

- Starting/Stopping

  ```
  $sudo service postfix start
  $sudo service postfix stop
  ```

- Reloading rules

  ```
  $sudo postfix reload
  ```

- Checking logs

  ```
  $sudo tail –f /var/log/mail.log
  ```

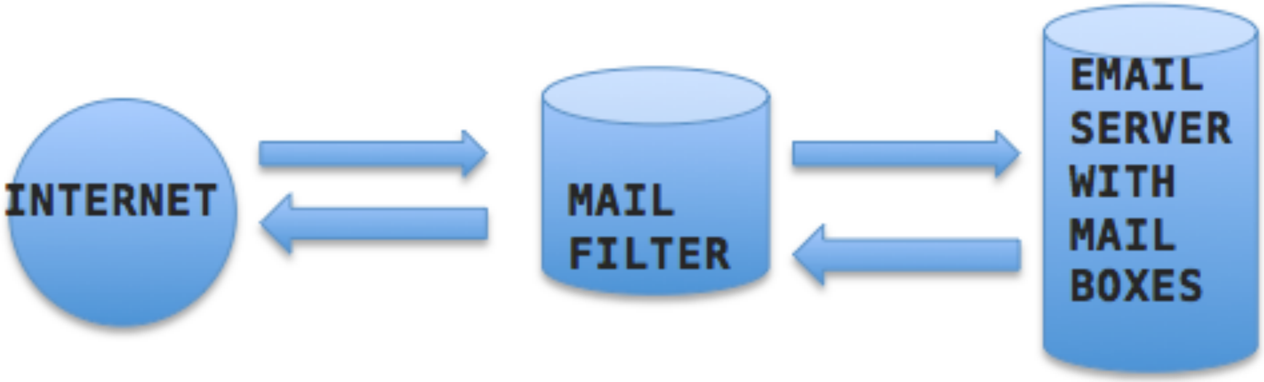
Building a Mail Gateway

aka Mail Firewall or Mail Filter appliance

What is a Mail Gateway?

- A software/service/appliance that is able to receive and filter emails before they reach the email boxes
- Typically, a mail gateway will not contain mail box accounts and will only receive emails, filter them based on configured parameters, and then forward them to the mail server that contains the mailboxes
- The purpose is to remove dangerous or harmful content (like spam and viruses) on email before they reach user boxes
- A mail filter can process incoming emails and or outgoing emails

Typical Setup



Advantages

- Remove harmful email before it reaches mail boxes
- Remove the work of filtering email from the server that is handling email boxes
- Highly configurable and can block emails based on a number of criteria including content that is in the body of the email
- If hosted outside the network, can reduce load on the network connection/link (also known as far side scrubbing)

Disadvantage

- Mistakes in configuration may mean mail is not delivered. They are highly customisable with hundreds of options and parameters which you must be careful with
- Increase the number of email servers to be managed

Common tools used in Mail Gateways

- Spamassassin – No. 1 Open Source anti-spam platform giving system administrators a filter to classify email and block spam (unsolicited bulk email)
- ClamAV – Virus scanning software. Can be used for email scanning and web scanning
- Amavisd – interface between the MTA and the above tools. A common mail filtering installation with *Amavis* consists of an MTA, ClamAV and Spamassassin
- MailScanner - open source email security system design for Linux-based email gateways

Mail Gateway Appliances

These are solutions that can be installed on servers and provide Mail Gateway services

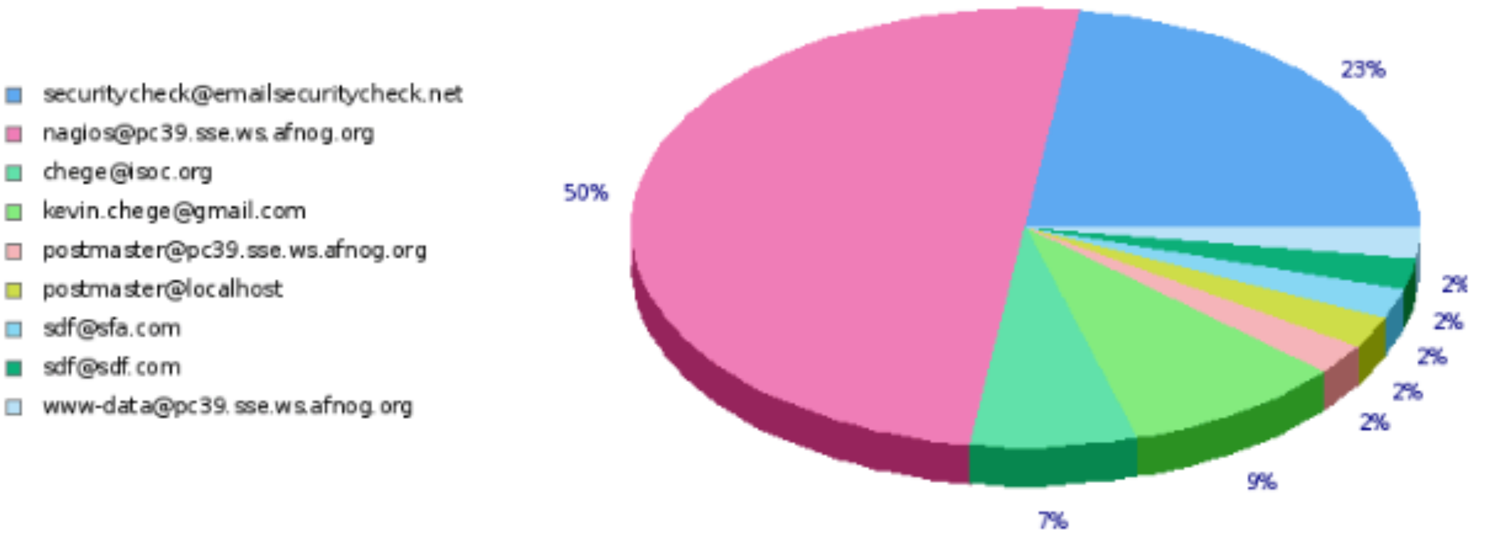
- Anti Spam SMTP Proxy - http://en.wikipedia.org/wiki/Anti-Spam_SMTP_Proxy
- Mail Border - http://www.mailborder.com/
- ScrolloutF1 - http://www.scrolloutf1.com/
- Xeams - http://www.xeams.com/

MailScanner as an Appliance

- MailScanner can be combined with a frontend to become a Mail Gateway appliance
- Two frontends are available:
  - Baruwa – http://baruwa.org
  - Mailwatch - http://mailwatch.org/
- When properly managed and configured with Postfix or Exim as the MTA, one can build a industrial strength mail gateway

www.mailscanner.info MailScanner

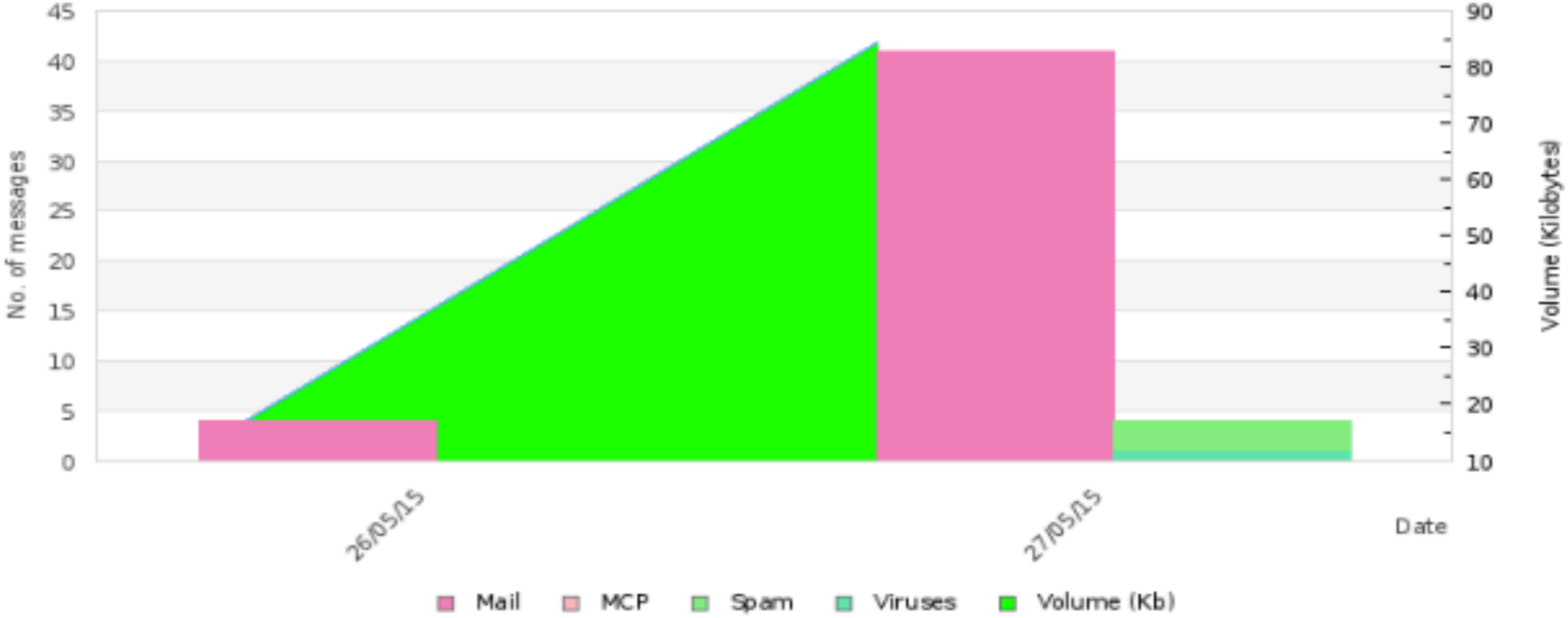
Top 10 Senders by Volume



E-Mail Address	Count	Size
securitycheck@emailsecuritycheck.net	10	45.9Kb
nagios@pc39.sse.ws.afnog.org	22	17.5Kb
chege@isoc.org	3	13.2Kb
kevin.chege@gmail.com	4	9.6Kb
postmaster@pc39.sse.ws.afnog.org	1	3.2Kb
postmaster@localhost	1	2.7Kb
sdf@sfa.com	1	1.2Kb
sdf@sdf.com	1	833b
www-data@pc39.sse.ws.afnog.org	1	794b

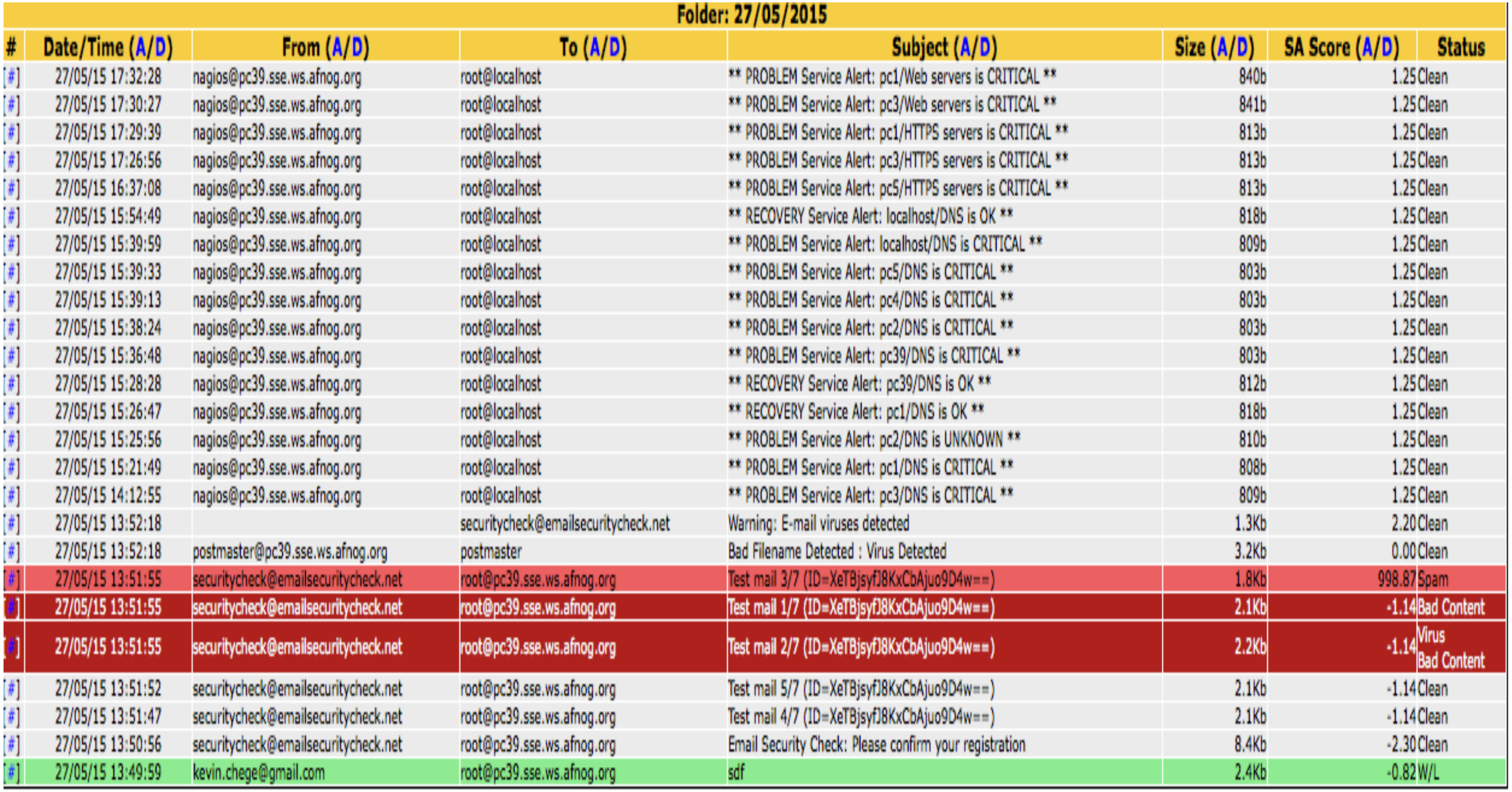
MailScanner www.mailscanner.info

Total Mail Processed by Date



Date	Mail	Virus	%	Spam	%	MCP	%	Volume		Unknown Users	Can't Resolve	RBL
26/05/15	4	0	0.0	0	0.0	0	0.0	12Kb		0	0	0
27/05/15	41	1	2.4	3	7.3	0	0.0	84.2Kb		0	0	0
Totals	**45**	**1**	**2.2**	**3**	**6.7**	**0**	**0.0**	**96.2Kb**		**0**	**0**	**0**

Page generated in 0.485303 seconds



Folder: 27/05/2015

#	Date/Time (A/D)	From (A/D)	To (A/D)	Subject (A/D)	Size (A/D)	SA Score (A/D)	Status
[#]	27/05/15 17:32:28	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc1/Web servers is CRITICAL **	840b	1.25	Clean
[#]	27/05/15 17:30:27	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc3/Web servers is CRITICAL **	841b	1.25	Clean
[#]	27/05/15 17:29:39	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc1/HTTPS servers is CRITICAL **	813b	1.25	Clean
[#]	27/05/15 17:26:56	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc3/HTTPS servers is CRITICAL **	813b	1.25	Clean
[#]	27/05/15 16:37:08	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc5/HTTPS servers is CRITICAL **	813b	1.25	Clean
[#]	27/05/15 15:54:49	nagios@pc39.sse.ws.afnog.org	root@localhost	** RECOVERY Service Alert: localhost/DNS is OK **	818b	1.25	Clean
[#]	27/05/15 15:39:59	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: localhost/DNS is CRITICAL **	809b	1.25	Clean
[#]	27/05/15 15:39:33	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc5/DNS is CRITICAL **	803b	1.25	Clean
[#]	27/05/15 15:39:13	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc4/DNS is CRITICAL **	803b	1.25	Clean
[#]	27/05/15 15:38:24	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc2/DNS is CRITICAL **	803b	1.25	Clean
[#]	27/05/15 15:36:48	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc39/DNS is CRITICAL **	803b	1.25	Clean
[#]	27/05/15 15:28:28	nagios@pc39.sse.ws.afnog.org	root@localhost	** RECOVERY Service Alert: pc39/DNS is OK **	812b	1.25	Clean
[#]	27/05/15 15:26:47	nagios@pc39.sse.ws.afnog.org	root@localhost	** RECOVERY Service Alert: pc1/DNS is OK **	818b	1.25	Clean
[#]	27/05/15 15:25:56	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc2/DNS is UNKNOWN **	810b	1.25	Clean
[#]	27/05/15 15:21:49	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc1/DNS is CRITICAL **	808b	1.25	Clean
[#]	27/05/15 14:12:55	nagios@pc39.sse.ws.afnog.org	root@localhost	** PROBLEM Service Alert: pc3/DNS is CRITICAL **	809b	1.25	Clean
[#]	27/05/15 13:52:18		securitycheck@emailsecuritycheck.net	Warning: E-mail viruses detected	1.3Kb	2.20	Clean
[#]	27/05/15 13:52:18	postmaster@pc39.sse.ws.afnog.org	postmaster	Bad Filename Detected : Virus Detected	3.2Kb	0.00	Clean
[#]	27/05/15 13:51:55	securitycheck@emailsecuritycheck.net	root@pc39.sse.ws.afnog.org	Test mail 3/7 (ID=XeTBjsyfJ8KxCbAjuo9D4w==)	1.8Kb	998.87	Spam
[#]	27/05/15 13:51:55	securitycheck@emailsecuritycheck.net	root@pc39.sse.ws.afnog.org	Test mail 1/7 (ID=XeTBjsyfJ8KxCbAjuo9D4w==)	2.1Kb	-1.14	Bad Content
[#]	27/05/15 13:51:55	securitycheck@emailsecuritycheck.net	root@pc39.sse.ws.afnog.org	Test mail 2/7 (ID=XeTBjsyfJ8KxCbAjuo9D4w==)	2.2Kb	-1.14	Virus Bad Content
[#]	27/05/15 13:51:52	securitycheck@emailsecuritycheck.net	root@pc39.sse.ws.afnog.org	Test mail 5/7 (ID=XeTBjsyfJ8KxCbAjuo9D4w==)	2.1Kb	-1.14	Clean
[#]	27/05/15 13:51:47	securitycheck@emailsecuritycheck.net	root@pc39.sse.ws.afnog.org	Test mail 4/7 (ID=XeTBjsyfJ8KxCbAjuo9D4w==)	2.1Kb	-1.14	Clean
[#]	27/05/15 13:50:56	securitycheck@emailsecuritycheck.net	root@pc39.sse.ws.afnog.org	Email Security Check: Please confirm your registration	8.4Kb	-2.30	Clean
[#]	27/05/15 13:49:59	kevin.chege@gmail.com	root@pc39.sse.ws.afnog.org	sdf	2.4Kb	-0.82	W/L

Let us build our Mail Gateway

- We will now setup a mail gateway
- Configuring a mail filter is not easy. You must be aware of what you are enabling or disabling. Preconfigured files will be provided due to time limitation
- Setting the correct DNS entries is key
- You will filter email for your neighbor and he will filter your email
- At the end, you should have a fairly strong and working mail filter