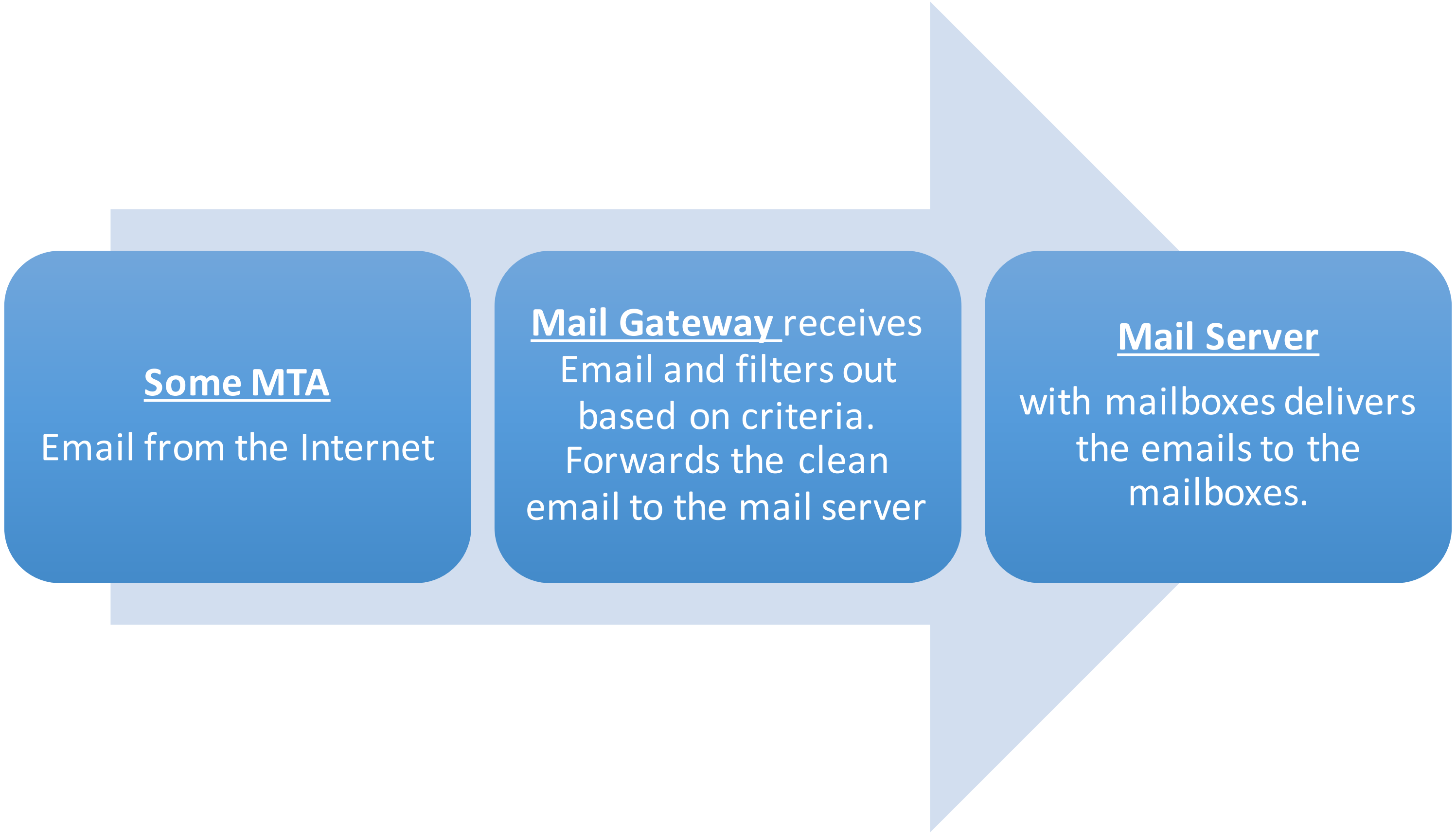
Email Gateways

Kevin Chege

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

How it flows



Some MTA

Email from the Internet

Mail Gateway receives Email and filters out based on criteria. Forwards the clean email to the mail server

Mail Server

with mailboxes delivers the emails to the mailboxes.

Advantages

- Remove harmful email before it reaches mail boxes
  - Phishing emails, malware, viruses etc
- 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)

Disadvantages

- 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

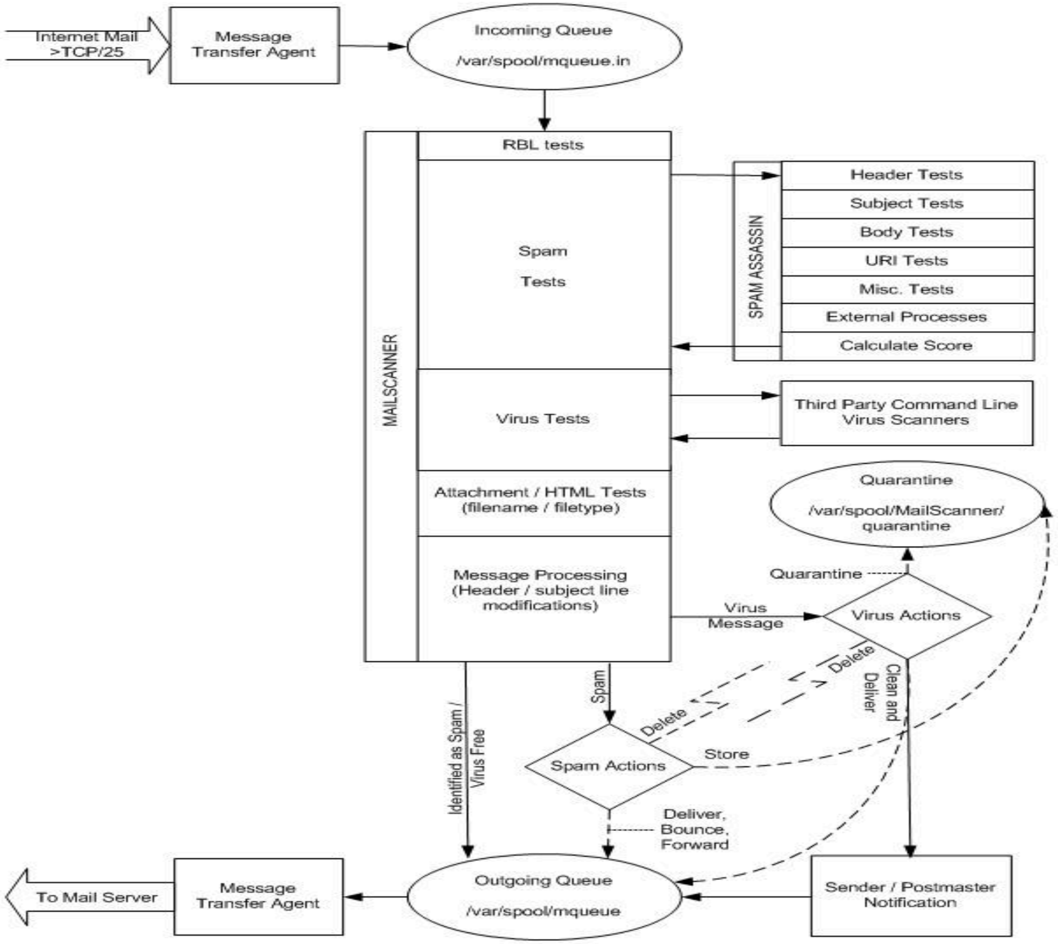
- Software:
  - Anti Spam SMTP Proxy - http://en.wikipedia.org/wiki/Anti-Spam_SMTP_Proxy
  - Mail Border - http://www.mailborder.com/
  - ScrolloutF1 - http://www.scrolloutf1.com/
  - Xeams - http://www.xeams.com/
- Hardware (Blackbox):
  - Barracuda - https://www.barracuda.com/products/emailsecuritygateway

MailScanner

- MailScanner is a highly respected open source email security system design for Linux-based email gateways.
    - It is used at over 30,000 sites around the world
    - Has fast become the standard email solution at many ISP sites for virus protection and spam filtering.
- MailScanner scans email for viruses, spam, phishing, malware, and other attacks against security vulnerabilities and plays a major part in the security of a network.
- MailScanner supports a wide range of MTAs and virus scanners to include the popular open source Clam AV. Spam detection is accomplished via Spamassassin, which is by far the most popular and standardized spam detection engine.
- Written and Founded by: Julian Field

MailScanner Process Overview

September 25, 2003



Internet Mail >TCP/25

Message Transfer Agent

Incoming Queue /var/spool/mqueue.in

MAILSCANNER

RBL tests

Spam Tests

SPAM ASSASSIN

Header Tests

Subject Tests

Body Tests

URI Tests

Misc. Tests

External Processes

Calculate Score

Virus Tests

Third Party Command Line Virus Scanners

Attachment / HTML Tests (filename / filetype)

Message Processing (Header / subject line modifications)

Quarantine /var/spool/MailScanner/ quarantine

Quarantine

Virus Message

Virus Actions

Delete

Clean and Deliver

Spam

Identified as Spam / Virus Free

Delete

Spam Actions

Store

Deliver, Bounce, Forward

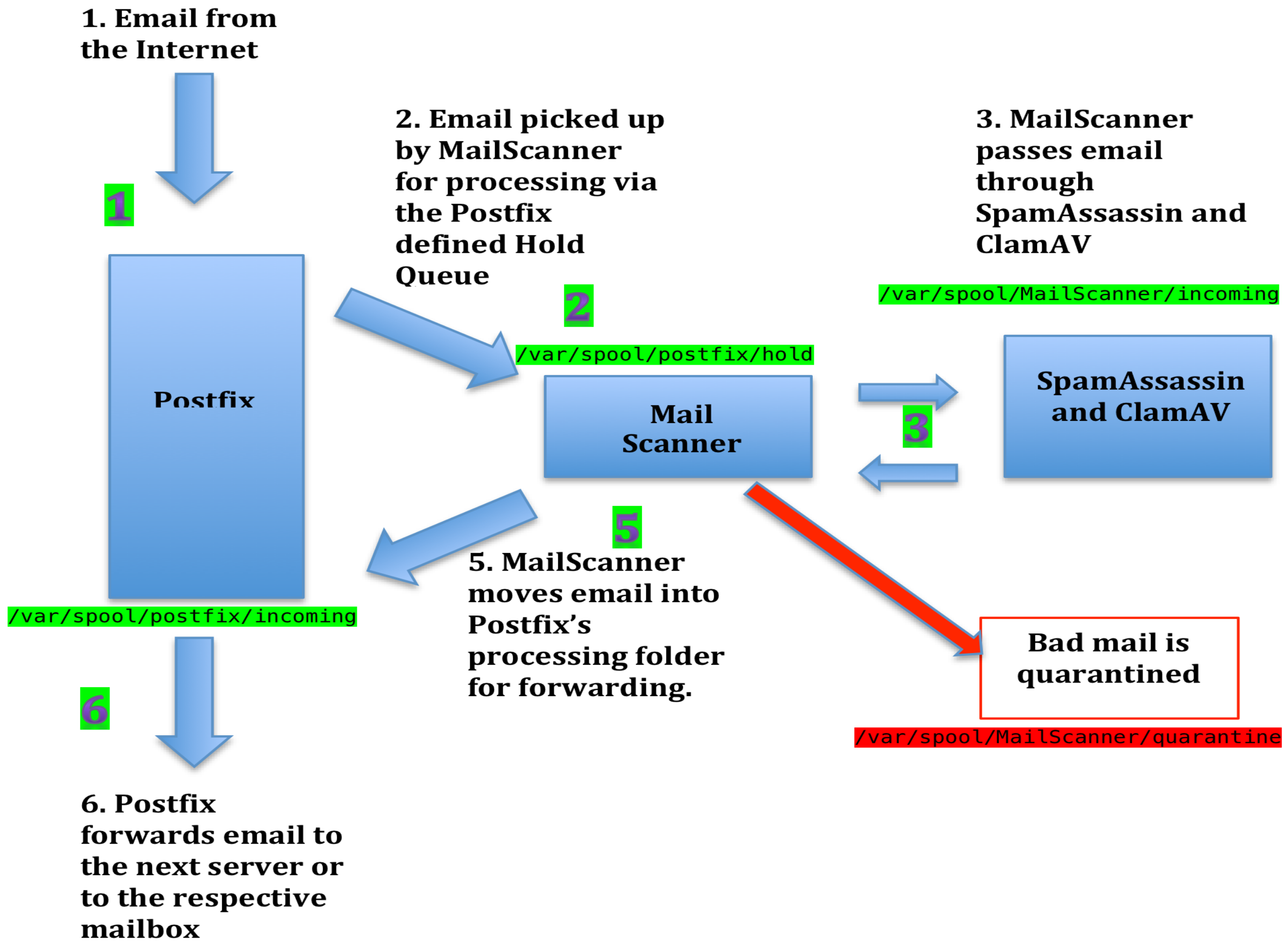
Outgoing Queue /var/spool/mqueue

Sender / Postmaster Notification

Message Transfer Agent

To Mail Server

A bit simpler…



1. Email from the Internet

2. Email picked up by MailScanner for processing via the Postfix defined Hold Queue

3. MailScanner passes email through SpamAssassin and ClamAV

5. MailScanner moves email into Postfix's processing folder for forwarding.

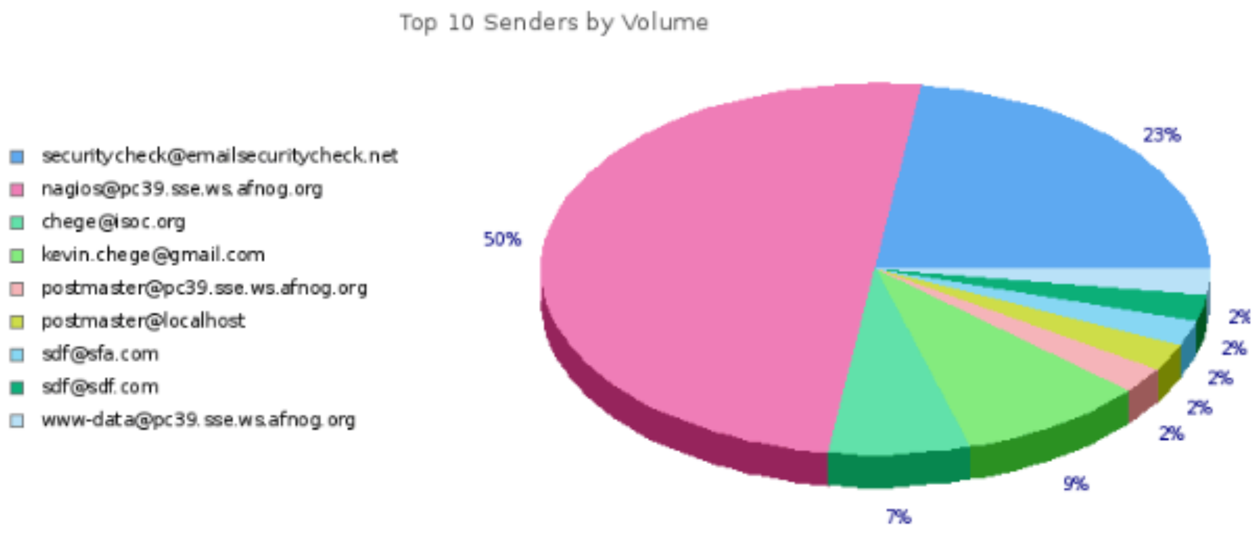
6. Postfix forwards email to the next server or to the respective mailbox

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 powerful mail gateway

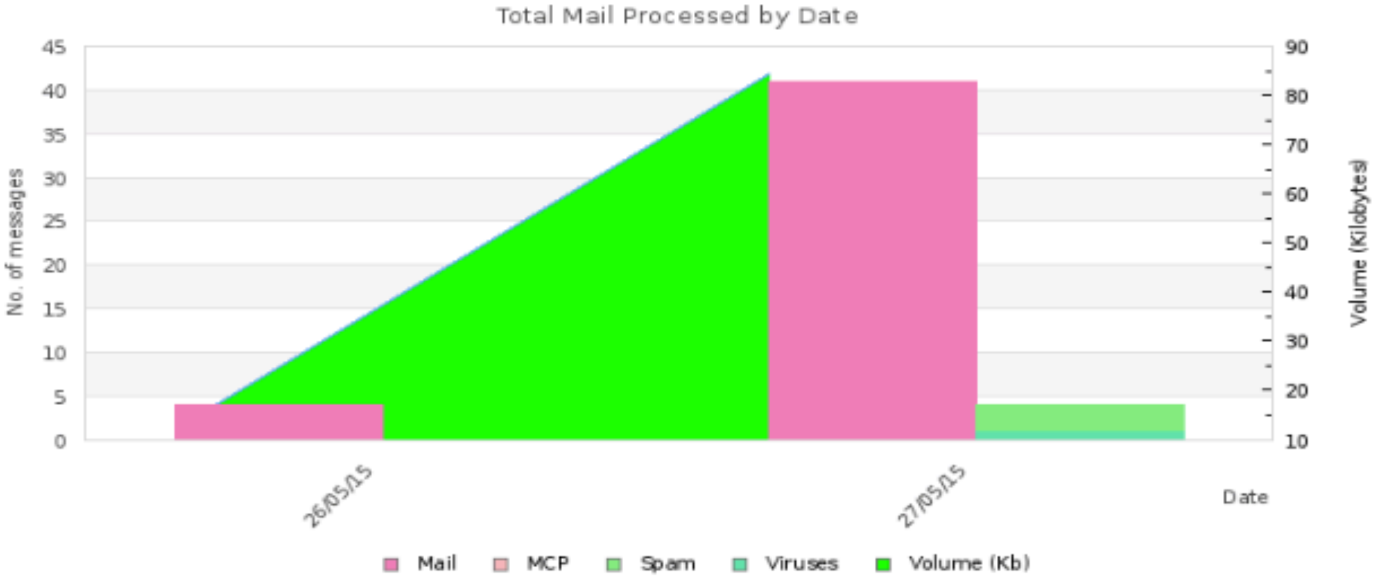
MailScanner has hundreds of Knobs

- https://www.mailscanner.info/MailScanner.conf.index.html
- The defaults mostly work but for a production environment, please read the manual!
- We will install with basic features of
  - Process email and check for SPAM and viruses
  - Log all emails to MySQL (SPAM and Not SPAM)
  - Store all emails in the quarantine



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

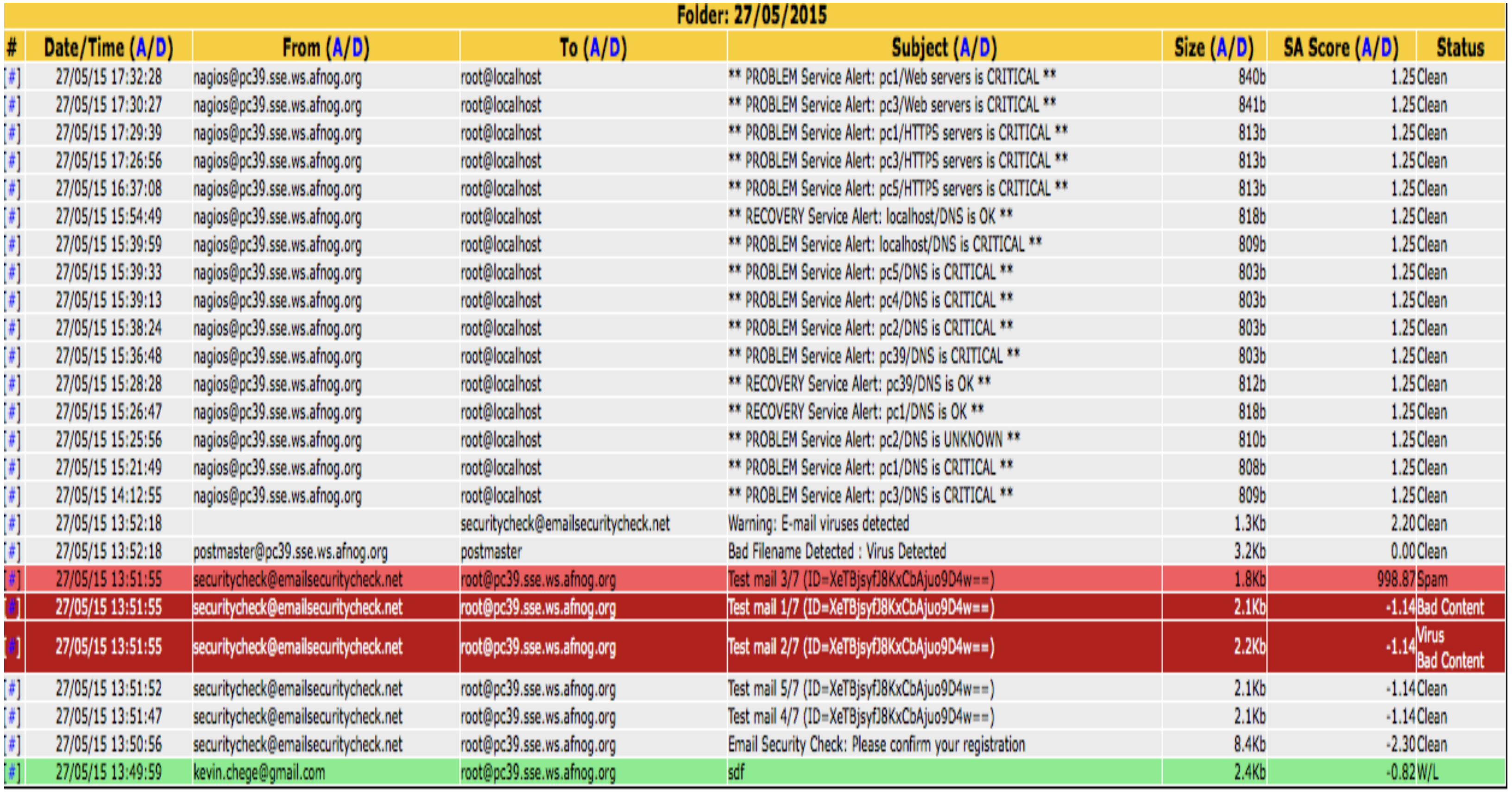
www.mailscanner.info
MailScanner



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

MailScanner Reports



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

References

- https://www.mailscanner.info
- https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail
- http://postfix.org
- https://www.safaribooksonline.com/library/view/postfix-the-definitive/0596002122/ch04s05.html