Email Intro

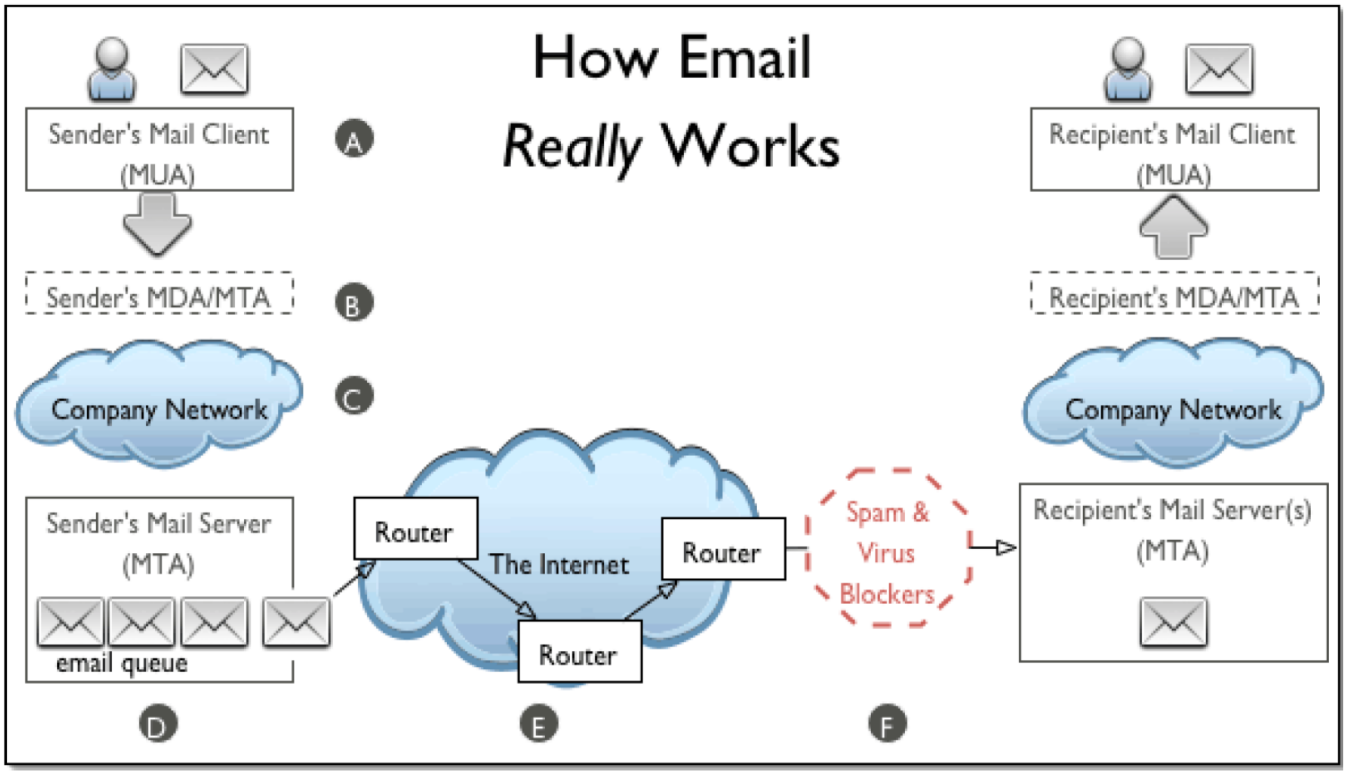
SS-E AFNOG 2019

Kevin Chege

Goals

- Install a Mail Server (Debian)
- Put a web interface to access our emails
- Go through email best practices
- Build a mail filter to clean emails on other system (FreeBSD)

How Email Really Works



Message Format

- **Envelope**
  - Routing information for the "postman"
- **Message Header**
  - Sender
  - Recipients (simple, lists, copies, blind copies)
  - Other fields of control (date, subject)
- **Message Body**
  - Free text
  - Structured document (i.e.: MIME)

SMTP: response codes

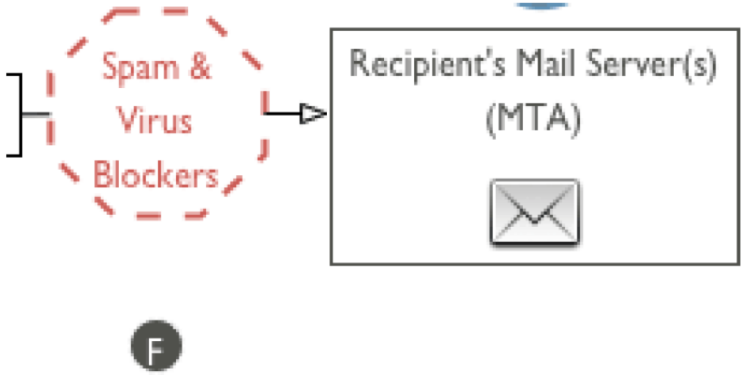
- 1xx:positive preliminary answer (action to be continued in subsequent command)
- 2xx:positive response indicating that processing has been carried out as requested
- 3xx:positive partial response: the client must give more data for processing to continue
- 4xx:negative answer, processing is refused, but the command can be tried again later
- 5xx:negative answer, processing cannot be carried out

DNS resolution and transfer process

- **To find the recipient's IP address and mailbox**, the MTA must **drill down through the DNS system**, which consists of a set of servers distributed across the Internet beginning with the root nameservers
  - root servers refer requests for a given domain to the root nameservers that handle requests for that tld
    - ***MTA can bypass this step because it has already knows which domain nameservers handle requests for these .tlds e.g. telecom.ma***
  - asks the appropriate DNS server which Mail Exchange (MX) servers have knowledge of the subdomain or local host in the email address
  - DNS server responds with an MX record: a prioritized list of MX servers for this domain
  - To the DNS server, the server that accepts messages is an MX server. When is transferring messages, it is called an MTA.
  - MTA contacts the MX servers on the MX record in order of priority until it finds the designated host for that address domain
  - **sending MTA asks if the host accepts messages for the recipient's username at that domain (i.e., username@domain.tld) and transfers the message**

Firewalls, spam, and virus filters

- An email encountering a firewall may be **tested by spam and virus filters** before it is allowed to pass inside the firewall
- filters test to see **if the message qualifies as spam or malware**
- If the message contains **malware, the file is usually quarantined and the sender is notified**
- If the message is identified as spam, **it will probably be deleted without notifying the sender**.



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
- Able to process thousands

Some Key Features

- SASL authentication Simple Auth Security Layer
- 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 and FreeBSD

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

master.cf

- defines how a client program connects to a service, and what daemon program runs when a service is requested.
- The Postfix master daemon launches all of the other Postfix services as they are needed. The various services, and how they are run, are specified in the master.cf file.
- The SMTP service is defined in this file as well as third party apps like an SPF program or a DKIM Program

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

- **Checking non-default running config**
  $sudo postconf –n

- **Reloading rules**
  $sudo postfix reload

- **Checking logs**
  Debian**:** $sudo tail –f /var/log/mail.log
  FreeBSD: $sudo tail –f /var/log/maillog

Further Postfix Reading

- Queue manipulation
  - http://www.tech-g.com/2012/07/15/inspecting-postfixs-email-queue/
- Postfix on Debian
  - https://wiki.debian.org/Postfix