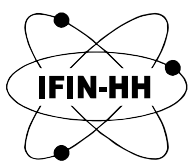
Network Services Introduction

E-Mail Servers, Spam and Postfix

Dr. Horia V. Corcalciuc
Horia Hulubei National Institute for R&D in Physics and Nuclear Engineering (IFIN-HH)

February 11, 2017



Introduction

- **Simple Mail Transfer Protocol** (**SMTP**) is the standard Internet protocol for transmitting E-Mail defined in **RFC 821** and **RFC 5321**.
- SMTP uses TCP port 25 for **server to server** mail transmission although it can be used for **client to server** communication as well. SMTPs uses TCP port 465 for SSL encrypted communication as legacy but has deprecated in favour of **STARTTLS** (although a lot of ISPs are still using this port). TCP port 587 is called **message submission** and is described in RFC 6409.
- The term SSL usually refers to an encryption wrapper for port 465 whilst TLS refers to the the server using the STARTTLS mechanism for encryption. Mail can be encrypted between the **client and the server** as well as **between server to server** transmissions.

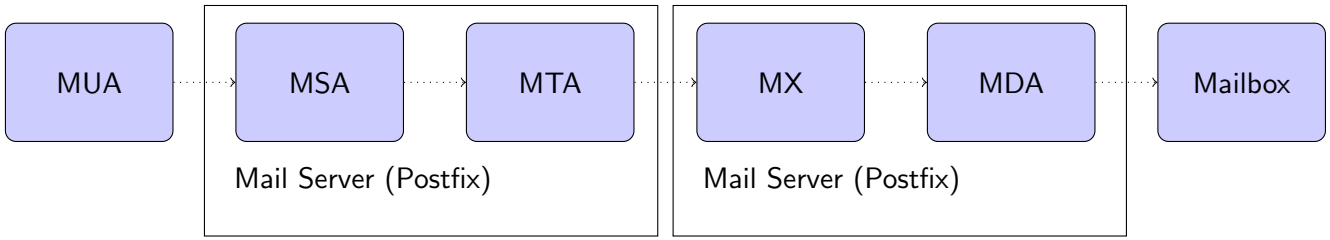
Port Configuration

Most Common Ports Used by E-Mail

Port	Description
25	Server to server or client to server connections.
465	SMTPs deprecated but still largely in use.
587	Client to server submission.
110	Post Office Protocol (unsecured).
995	Secure Post Office Protocol (POPs).
143	Internet Message Access Protocol (IMAP).
993	Secure Internet Message Access Protocol (IMAPs).

- Internet Service Providers have taken the decision (cca. y2k) to filter outbound connections to port 25 in order to reduce spam. Unfortunately, the decision is mostly economical and just used as leverage for ISPs to pitch costly packages to home owners in order to remove the limitation.
- The list of ports is not complete and rather pertains to a minimal infrastructures assembled using OpenSource software. For instance, **groupware** such as Microsoft Exchange **uses a lot more ports** that should not be blocked or the software will not function correctly.

Diagram



- The **Mail User Agent** (**MUA**) submits the E-Mail to the **Mail Submission Agent** (**MSA**) on TCP port 587 (or 25).
- If accepted, the **MSA** delivers the E-Mail to the **Mail Transfer Agent** (**MTA**).
- The **MTA** then retrieves the **Mail Exchange** records of the destination server (**MX**) Lecture: ISC BIND Domain Name System. If successful, the **MTA** connects to the destination mail exchange server (**MX**) and transfers the E-Mail.
- The **MX** server will then hand the E-Mail to the **Mail Delivery Agent** (**MDA**).
- The **MDA** can then deliver the E-Mail to a mailbox that a **MUA** can poll - usually via the **Post Office Protocol** (**POP**) or via the **Internet Message Access Protocol** (**IMAP**).

IFIN-HH

Submitting an E-Mail

Submitting an E-Mail for Transfer

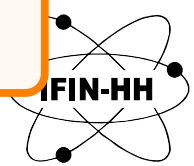
```
220 mail.server.ro ESMTP Postfix
EHLO mail.server.ro
250-mail.server.ro
250-PIPELINING
250-SIZE 31000000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: zzz.zzzz@yy.yyyy.ro
250 2.1.0 Ok
RCPT TO: xxx.xxxx@yy.yyyy.ro
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
You're fired!
.
250 2.0.0 Ok: queued as BBFFD7B60
```

- `HELO` is used by the client to identify to the server - as an extension, `EHLO` is used instead to query the features of the server.
- The `MAIL FROM` is issued by the client to state from where the E-Mail originates.
- `RCPT TO` is issued by the client stating what the destination mailbox should be.
- `DATA` is then issued by the client to signal the start of the message. After that, the client can post additional headers as well as the message followed by a full stop.

SMTP Restrictions

Annotated Postfix Restrictions

```
220 mail.server.ro ESMTP Postfix                    # smtpd_client_restrictions
EHLO mail.server.ro                                 # smtpd_helo_restrictions
250-mail.server.ro
250-PIPELINING
250-SIZE 31000000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: zzz.zzzz@yy.yyyy.ro                      # smtpd_sender_restrictions
250 2.1.0 Ok
RCPT TO: xxx.xxxx@yy.yyyy.ro                        # smtpd_recipient_restrictions
250 2.1.5 Ok
DATA                                                # smtpd_data_restrictions
354 End data with <CR><LF>.<CR><LF>
To: xxx.xxxx@yy.yyyy.ro                             # header_checks
From: zzz.zzzz@yy.yyyy.ro
Subject: Job
You're fired!                                       # body_checks
.
250 2.0.0 Ok: queued as BBFFD7B60
```



Configuring SMTP Restrictions

Example Postfix Client Restrictions

```
smtpd_client_restrictions = permit_mynetworks,
        permit_sasl_authenticated,
        reject_unknown_client_hostname,          # dangerous for unauthenticated clients
        sleep 3,
        reject_unauth_pipelining

smtpd_sender_restrictions = ...
smtpd_recipient_restrictions = ...
smtpd_helo_restrictions = ...
smtpd_data_restrictions = ...
```

- **The order of the applied restrictions matters** - for instance, you would want to accept local networks first (or authenticated clients first) because you know they are legitimate senders, before performing any other checks.
- It is important to **apply the restrictions sparingly** because too many restrictions may make your server incompatible with other servers and even clients - for instance, clients rarely have a valid DNS such that DNS checks for clients will mostly fail thereby not letting your legitimate users send E-Mail.

IFIN-HH

Forward-Confirmed Reverse DNS (FCrDNS)

Forward DNS Mapping

```
                                MX      1 mail.server.ro.
mail.server.ro          A       194.102.59.5
```

Reverse DNS Mapping

```
5       PTR     mail.server.ro.
```

- **Forward-Confirmed Reverse DNS** (**FCrDNS**) specifies that a hostname should map to an IP address and that IP address should map back to the same hostname.
- **FCrDNS** checks can be used to prevent a lot of spam due to spammers not being able to bypass this verification since they are rarely in control of both the DNS configuration and the mail server.

IFIN-HH

Implementing FCrDNS with Postfix

Postfix Configuration for FCrDNS

```
smtpd_client_restrictions = permit_mynetworks,
        permit_sasl_authenticated,
        reject_unknown_client_hostname,        ; FCrDNS
        sleep 3,
        reject_unauth_pipelining
```

The `reject_unknown_client_hostname` rule will be triggered when:

- The client IP address to hostname mapping fails, or
- The client hostname to IP address mapping fails, or
- The client hostname to IP address mapping does not match the client IP address.

This restriction is very strong and should be applied carefully - or use the `reject_unknown_reverse_client_hostname` restriction that triggers when the client IP address does not have an address to hostname mapping.

IFIN-HH

Real-Time Blackhole List (RBL)

RBL

```
smtpd_client_restrictions = ...
        reject_rbl_client sbl.spamhaus.org
        reject_rbl_client zen.spamhaus.org,
        reject_rbl_client cbl.abuseat.org,
        reject_rbl_client bl.spamcop.net,
        ...
```

- **Blacklisting is the worst form possible of access control** but unfortunately **whitelisting** is not a possibility given that mail may array from any source on the Internet.
- Postfix allows you to subscribe to blacklists on the internet via the configuration keys `reject_rbl_client`, `reject_rhsbl_helo`, `reject_rhsbl_sender`, etc...
- Bear in mind that **by using blacklists you are delegating your security** to a source that you do not control - blacklists have been abused in the past through social engineering such that legitimate clients were blocked illictily.

Censorship

Header and Body Checks Postfix Configuration

```
header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
```

Using Regular Expression to Censor Words

```
/^Subject:.*viagra/ DISCARD
```

- **Censorship is no security** and content (body and header) censorship **should be avoided** at all costs due to the overwhelming amount of **false positives** as well as the weakness of regular expressions to overcome obfuscation.
- Even though the rule matches all case-insensitive variations of the name `Viagra`, such a check will fail in case the sender formats the word as `Viagrá`.
- Once the header and body checks have been declared in `main.cf`, the map should be generated using the `postmap` command.

IFIN-HH

Sender Policy Framework

SPF Checks

```
mail.server.ro.          SPF          "v=spf1 a mx -all"
```

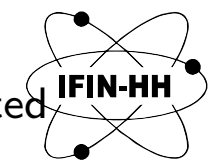
Postfix `main.cf`

```
smtpd_relay_restrictions = ...
        check_policy_service unix:private/policy,
        ...
```

Postfix `master.cf`

```
policy  unix  -       n       n       -       -       spawn
  user=nobody argv=/usr/bin/perl /usr/sbin/postfix-policyd-spf-perl
```

- **The Sender Policy Framework** (**SPF**) can be used to declare which domains are allowed to send mail through your server and from what IP addresses or hostnames your mails are allowed to originate from.
- SPF can also be used to check that E-Mail correctly originates from designated mail-servers such that spoofed E-Mails can be rejected.



Domain Keys Identified Mail

DKIM Postfix Setup

```
milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:localhost:4765
non_smtpd_milters = inet:localhost:4765
```

DNS DKIM Configuration Example

```
mail._domainkey   TXT  "v=DKIM1; k=rsa; g=*; p=z2ucTITz1/PKL..."
_adsp._domainkey  TXT  "dkim=discardable"
```

- Similar to SPF checks, **Domain Keys Identified Mail** (**DKIM**) allows the receiver of the E-Mail to verify that the E-Mail came from the origin server thereby offering a solid spoofing protection.

IFIN-HH

Greylisting

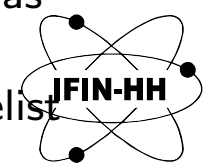
Greylisting Specified in RFC6647

SMTP servers can reject E-Mail with a temporary failure (4xx) error code such that correctly implemented and configured SMTP servers are supposed to retry the connection after a given timespan ranging from minutes to hours instead of failing immediately. Greylisting exploits this feature of the specification such that the server will temporary reject any incoming mail and accept it after a configurable timespan since most spam software will not retry the connection again.

Postfix `main.cf`

```
smtpd_recipient_restrictions = ...
        check_policy_service inet:127.0.0.1:10023,
        ...
```

- Greylisting solutions such as `postgrey` are designed to implement greylisting as well as allow whitelisting and auto-whitelisting of addresses.
- When implemented, **E-Mail will be delayed slightly** until the automatic whitelist fills up with most frequently used addresses.



End Notes

A good reference for this seminar series, as well as a recommended book is Andrew Tannenbaum's "Modern Operating Systems". Andrew Tannenbaum created Minix (a free UNIX alternative) and Linus Torvalds was his student:

- Modern Operating Systems, Tanenbaum, A.S. and Bos, H., ISBN 9780133591620, LCCN 2013444331, 2014, Prentice Hall

The slides will be posted at:

- Personal Website

IFIN-HH