CIA Lab Assignment:
Mail Transfer Agents (MTA)
*cloud infrastructure edition

Prerequisites:
This assignment must be performed in groups of two where each person installs different MTA, namely *Postfix* or *Exim. Remember to keep an exact log of your actions, highlighting the problems you've encountered and how you solved them.*

Task 1 - Install

There are many different MTAs available, both open source and proprietary. In this assignment we will be looking at two well known open source MTAs. *Exim* was originally based on the Smail MTA, but has since diverged. Exim is also the default MTA for Debian, and is currently the most used. *Postfix* is one of the most secure MTAs. Postfix is somewhat different from other MTAs in that it consists of many small programs. This setup agrees with the UNIX philosophy, but it also complicates an integration into the UNIX daemon configuration.

1. Install from source code

a) First make sure that your system does not contain a pre-installed version of the MTA of your choice, if so, remove it before you continue.

b) Make sure the source code is retrieved from a secure location. Use the official website for the MTA of your choice.

c) Because it is important that an MTA be correct and secure it is often signed using a digital PGP signature. If your MTA is signed then make sure you have downloaded the correct sources by checking the validity of the key and the signature.

d) There are a number of options that you will have to enter before compilation, so that the functionality can be compiled into the program. Make sure the basic install holds all the necessary functionality. Show the options you configured.

2. Most of the options for an MTA can be found in a configuration file that will be loaded when the MTA starts. It is recommended to start with an example configuration that looks a lot like what you need for now. Show how you adapt it to your needs.

3. Configure:

a) Add a local account on your experimental machine and make sure that the MTA can deliver mail to it. Show the required configuration.

b) Add to your log an email received by this account. *Do not forget the full headers!*

c) Also make sure that any email intended for `postmaster@st<X>.sne21.ru` is delivered to this account. Show the full email as delivered to the new account and the required configuration.

Task 2 - Sending mail - email validation - SPF & DKIM

For many people unsolicited commercial email, or rather SPAM, is a big problem. There are many ways to filter SPAM, each one having advantages and disadvantages. Examples include domain keys, SPF records, DNS block lists, greylisting, reverse checks, tarpitting, Bayesian filters, whitelists, etc. A lot of viruses and malware are transported over email (as well as the World Wide Web). Because viruses can cause a lot of trouble, discarding viral messages is a nice service to offer to your users.

Due to this reason cloud providers block standard SMTP port (25) for all outbound connections on their cloud instances to protect their IP address pools from having bad reputation.

Since your setup is deployed in the cloud, you are going to face that issue. To overcome this situation there are relay email servers that can accept your outgoing mail on other ports (587, 465, 2525) and forward it to the original destination server (that only works on port 25).

To provide such functionality this servers

- Provide you with credentials that should be used to submit your mail
- Require you to placing SPF/DKIM records that

- serves as a form of verification that you the domain owner
- used by original mail destination server to verify that relay server is eligible to send mail from your domain

4. Write a small paragraph that highlights the advantages and disadvantages of SPF and DomainKeys Identified Mail (DKIM). What would you choose at a first glance and why?

5. Set up your mail server to use a relay server to be able to send outgoing mail for different domains (contact your TA to obtain address/credentials to the relay server and SPF/DKIM records).

6. Test how your mail is delivered to commonly known mail servers (f.e. gmail). Provide full email/MTA headers to see how SPF/DKIM were delivered.

Task 3 - Mail backup

You should now have a working MTA for your domain. If your server is not reachable for whatever reason, you would not want email sent to you to be returned to the sender immediately. To remedy this we will configure backup MTAs on other servers. One of these backup MTAs will receive email intended for your domain when your own MTA is offline. Note that a backup MTA should not be confused with a server that makes backups of your mail, they have different functions.

In a group of two, you should have one backup MTA that will be the backup for the domain of your partner.

7. You have backup:

a) Adapt the DNS information for your domain, so that the backup MTA on your partner's server can be found.

   (…your partner configures its MTA as a backup MTA…)

b) Validate by shutting your service down and sending a message to your domain

   (…your partner sees its logs and where the message is temporarily stored…)

c) Bring your service back up and wait.

8. You provide backup:

a) Make your MTA act as a backup for your partner's domain.
b) Show the logs while doing your mate's acceptance test and show where the message is temporarily stored.
c) Once your partner's MTA is back online, eventually force an immediate delivery and show your mail logs.

Task 4 - Mailing loops

9. Create an email loop with your partner from domain to domain using email aliases.

10. Send an email to the loop using your own email address and see what happens on your MTA.

11. Can you change the behaviour of your MTA in response to this loop?

Task 5 - Virtual Domains

12. Create a new subdomain within your domain and add an MX entry to it.

13. Then extend your MTA configuration to handle virtual domains, and have it handle the email for the newly created domain.

14. Validate that you are now receiving emails for both domains.

Task 6 - Transport Encryption

15. *Questions*

a) Which one is better, SSL/TLS or STARTTLS, why?
b) Which one is actually in use for SMTP?

16. *Task*

a) Add transport encryption to your MTA.
b) Eventually force the transport to be encrypted only (refuse non encrypted transport).
c) Proceed with validation (proof or acceptance testing), as usual.

BONUS (2 points) - Task 7 - Anti-spam filters

17. Investigate what generic anti-spam open source software packages are out there, choose one, download it (compile it if necessary) and configure your MTA to use it. Make sure that in your MTA group there are 2 different anti-spam solutions implemented!