Please use a Screen or Video Capture software to save your works!

OBJECTIVE & PREPARATION

Warning: Your Lab 4 must be completed with a functional DNS server for your domain before this lab will work.

You may not be aware of it as a user, but email is a very complex system to administer. In fact, the more modern email systems (e.g. web-based mail applications…etc.) are more technically involved than the other archaic, hard-to-configure, and sometimes inter-operable mail systems.

We are going to spread the remaining email labs over a few weeks, so that by the end of this topic, you will have a sufficient understanding of what services are involved in sending, filtering, and reading email. You will also have the skills to configure a basic mail setup using the default services provided for your Centos7 Linux distribution.

Believe it or not, this is a SIMPLE diagram of you sending an email to someone else:

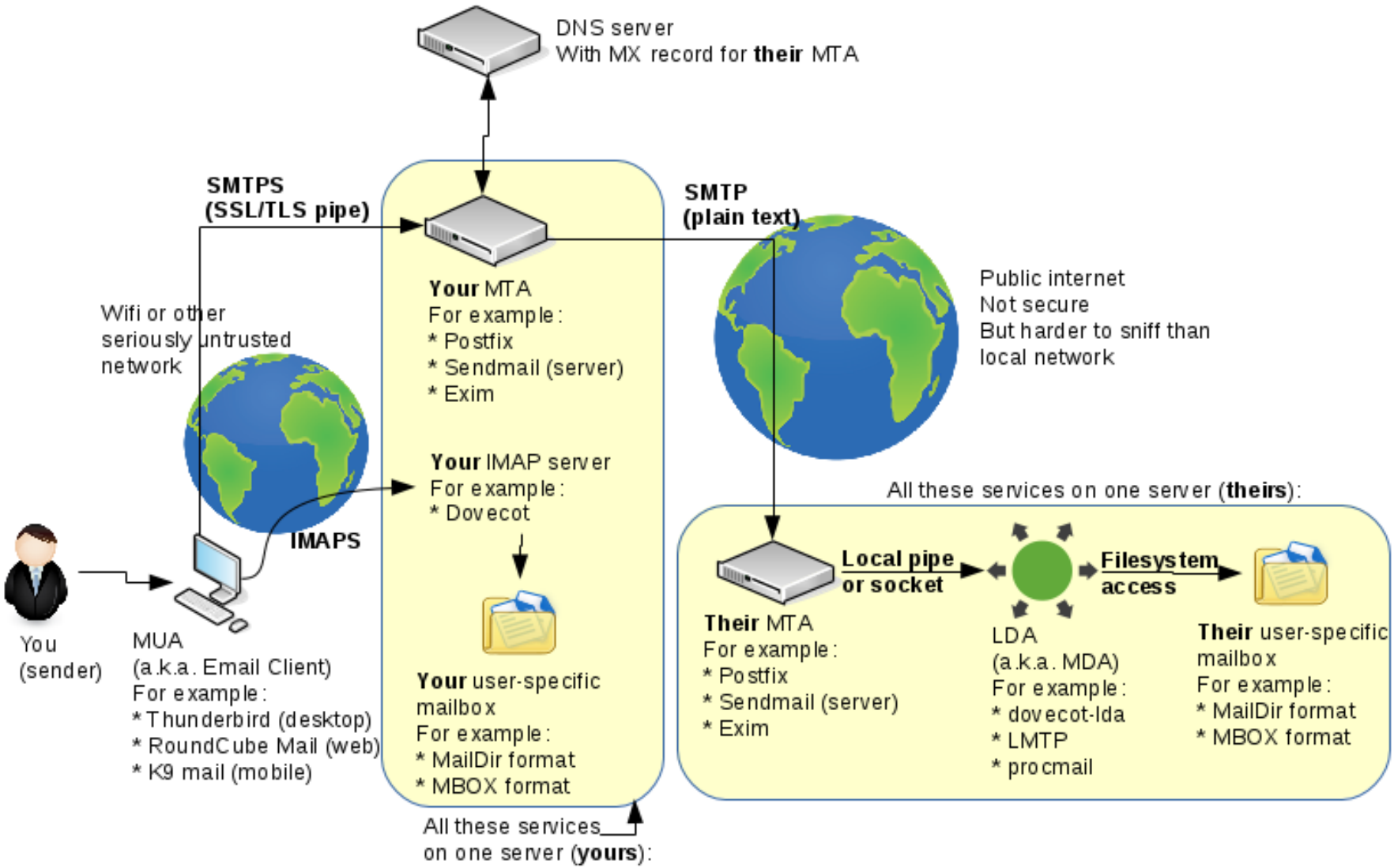
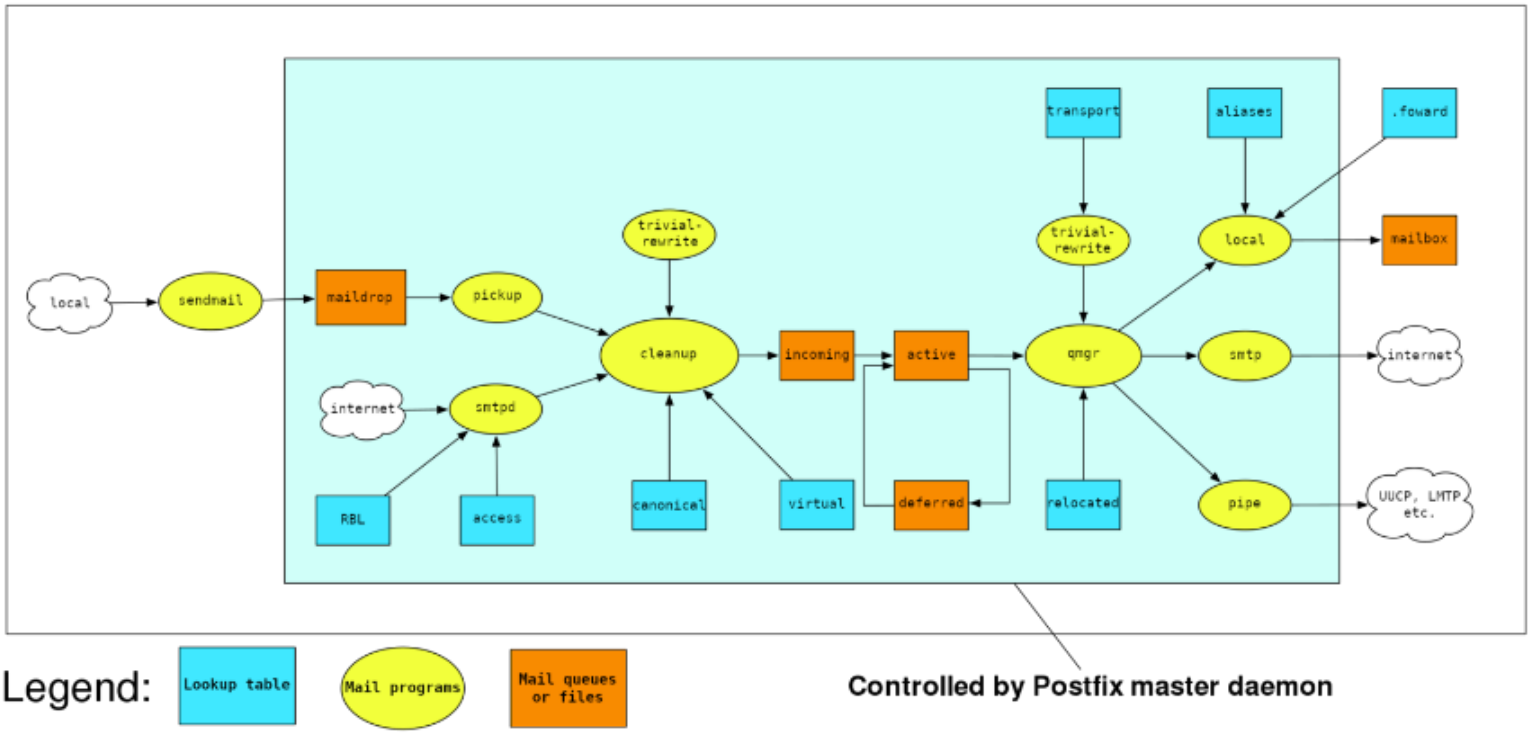


Diagram of **you** sending email to **them**

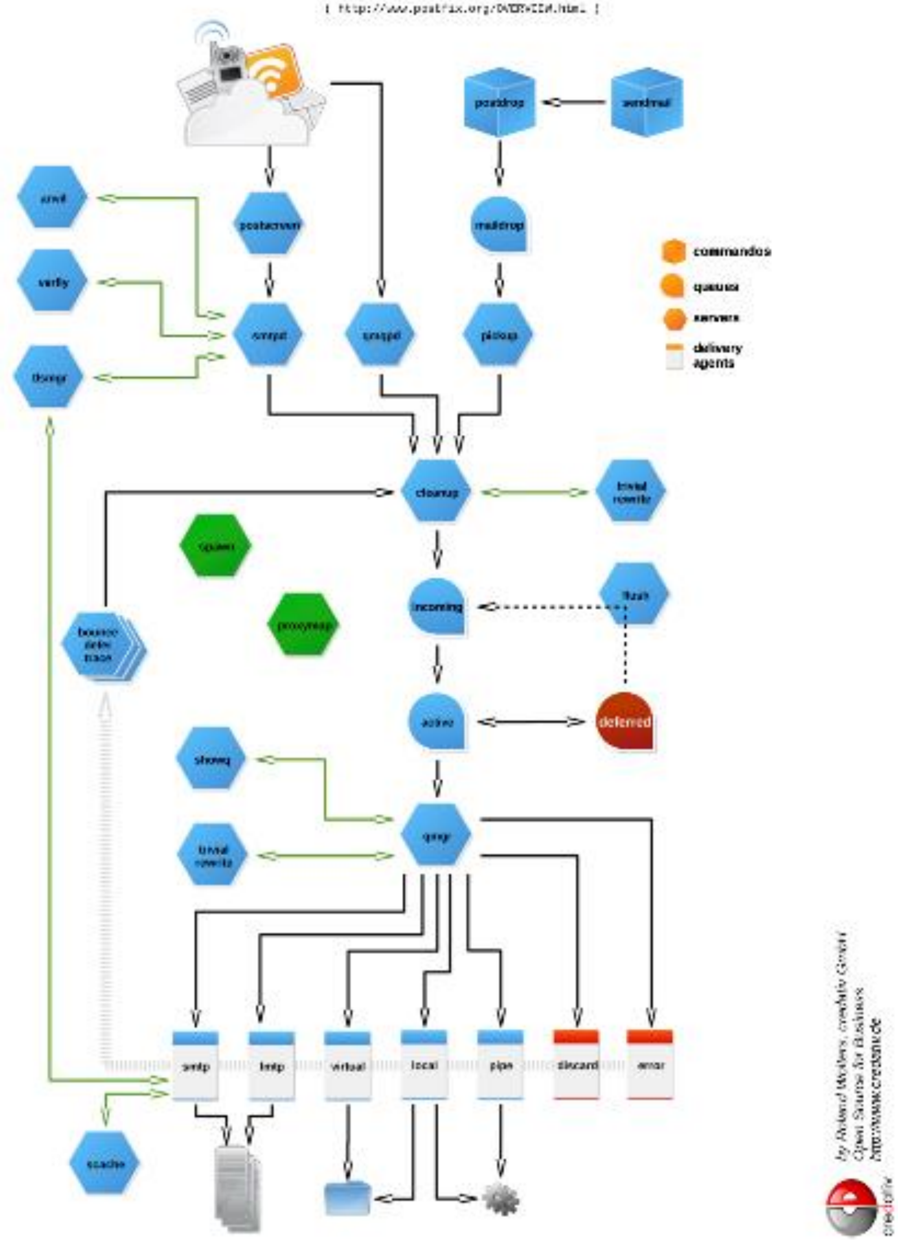
This lab will show you how to set up a **Mail User Agent (MUA),** using the **mailx** package on your Server VM to send and receive emails on your local VM. *(Practically, you should use separate VM for your DNS server and mail server. However, due to the constrains of Azure free credit and with the complexity of configuring firewall rules between extra VM(s), you will lose focus on what you should learn, therefore, we will host the DNS and Mail server in the same VM.)* In this case, the Postfix package which represents your MTA is most likely already installed and running on your local VM. In addition to sending and receiving emails on your Local VM, you will, **in theory**, also be able to send a text-based email from your Server VM to a personal account (e.g. Gmail). **However, Cloud Hosted Platforms usually block outbound port 25. Therefore, you will not be able to send email out.** You will also learn how to make multiple MTAs in the same network collaborate in sending emails. In addition, you will learn where the message store (MS) is located that stores mail messages until they are viewed and either deleted or transferred to other folders.

Although, you will not be able to receive mail messages from outside sources at this point. (Such as receiving email from your personal Gmail account), this lab acts as a starting point in order to run a basic email server. You are NOT required to go into tremendous depth (just the minimum requirements). For example, we will not go over every aspect of the Postfix MTA service, but you should know what it represents and what is its main purpose, as opposed to the following complex diagram 1 & 2.

Postfix architecture



Postfix Architecture Overview



Online References:

Mail Send Command (examples how to send email using mail command)

View and Manage Received email Messages (Common commands to view and manage received email messages)

Reading Full Email Headers (Explanation of message header information)

Here's an overview (common mail server terms)

Case 1: Install, Set-Up, And Use the Mail User Agent (MUA)

We will use a simple text-based **Mail User Agent (MUA)** called **mailx** in this lab to **both send and receive** mail messages within your **Server VM (vm1)** and to **only send** mail messages from your Server VM to Client VM.

NOTE: Because you're using private IP addresses and no external DNS servers are pointing to your network, you **cannot** send email messages from outside your environment to your **Server VM**.

Installing the Mail User Agent (MUA)

Perform the following Steps:

- Make sure you are in your Server VM.
- Install the mailx application (MUA) using yum

  yum install mailx

NOTE: You can refer to the link below to acquaint yourself on how to send email messages using mailx application: Mail Send Command Examples

Sending a Mail Message from your Server VM to a Gmail Account: ops345v1a@gmail.com

Note: Send email externally is blocked by Microsoft and the blocking cannot be removed with Free subscription. For the purpose of the lab submission, you can skip the steps when you see the issue.

https://learn.microsoft.com/en-us/azure/virtual-network/troubleshoot-outbound-smtp-connectivity

We will now test to see if your MTA for your Server VM is correctly running by sending email messages from your Server VM to the ops345v1a@gmail.com or your personal email. (Though the outbound port 25 is blocked by Microsoft, you still can see the error.) **Do not test Seneca email, your account may get locked.**

Perform the following steps:

1. Make sure you are still in your Server VM (vm1).
2. Test email from your machine by sending an email to ops345v1a@gmail.com using the following command: (use your own email in the following command)
   mail -s "Lab5 - test1" ops345v1a@gmail.com
   NOTE: after you type in the body of the mail message, move to an empty line, and then press the key combination <ctrl><d> to send the message.
3. **Only works if outbound port 25 unblocked. Instructor will demo in class with on-prem VMs.** Check your email account (Inbox / Junk email Folder) to see if you got the email (note that it may take a few minutes to arrive, so you may also wish to try an alternate email account if you have one from another vendor other than Gmail). When you do receive that email, make a note of the return address.
4. If you did not receive the mail, check the mail logs on your Server VM to determine any errors messages that would indicate a mail server setup problem. If you receive a similar log as the following screenshot, that would mean smtp is blocked. There is not much you can do, you can skip the step 5 and step 6.
   tail /var/log/maillog

```
Oct 23 23:50:11 server postfix/smtp[4635]: connect to alt1.gmail-smtp-in.l.google.com[2607:f8b0:4003
:c15::1a]:25: Network is unreachable
Oct 23 23:50:11 server postfix/smtp[4635]: connect to alt2.gmail-smtp-in.l.google.com[2607:f8b0:4001
:c56::1a]:25: Network is unreachable
Oct 23 23:50:11 server postfix/smtp[4635]: 5A272243852: to=<ops345v1a@gmail.com>, relay=none, delay=
34067, delays=34007/0.02/60/0, dsn=4.4.1, status=deferred (connect to alt2.gmail-smtp-in.l.google.co
m[2607:f8b0:4001:c56::1a]:25: Network is unreachable)
Oct 24 00:34:11 server postfix/qmgr[2112]: 7750B98AE: from=<root@server.localdomain>, size=483, nrcp
t=1 (queue active)
Oct 24 00:34:11 server postfix/smtp[5139]: connect to gmail-smtp-in.l.google.com[2607:f8b0:4023:c0d:
:1a]:25: Network is unreachable
Oct 24 00:34:41 server postfix/smtp[5139]: connect to gmail-smtp-in.l.google.com[142.251.2.26]:25: C
onnection timed out
Oct 24 00:34:41 server postfix/smtp[5139]: connect to alt1.gmail-smtp-in.l.google.com[2607:f8b0:4003
:c15::1a]:25: Network is unreachable
Oct 24 00:35:11 server postfix/smtp[5139]: connect to alt1.gmail-smtp-in.l.google.com[64.233.171.27]
:25: Connection timed out
Oct 24 00:35:11 server postfix/smtp[5139]: connect to alt2.gmail-smtp-in.l.google.com[2607:f8b0:4001
:c56::1b]:25: Network is unreachable
Oct 24 00:35:11 server postfix/smtp[5139]: 7750B98AE: to=<ops345v1a@gmail.com>, relay=none, delay=49
110, delays=49050/0.02/60/0, dsn=4.4.1, status=deferred (connect to alt2.gmail-smtp-in.l.google.com[
2607:f8b0:4001:c56::1b]:25: Network is unreachable)
```

5. Once you have succeeded in sending the first email, send a second email to the same destination using the following command:
   mail -r "someone@hacker.com (Canadian Revenue Agency)" -s "Lab5 - test2" ops345v1a@gmail.com
6. Check your email to see if you got the email. If you did, make a note of the return address. How would you think that including the **-r** option could be used by penetration hackers to gain access to a computer system? What sort of steps do you think should be taken to help prevent this type of attack from happening?

Sending a Mail Message within your Server VM

We will now test both your MUA (mailx) and MTA (postfix) by sending and receiving email messages on the local Server VM only.

Perform the following Steps:

1. Send an email message locally (i.e. only within your Server VM) by issuing the command:
   mail -s "Lab5 - Local - Test1" ops345
2. After you type in the body of the mail message, move to an empty line, type period "." and press the ENTER key to send the message.
3. Login with your regular user and issue the following command to read the mail message you send to yourself:
   mail
   NOTE: You can refer to the link below to view a reference chart on how to read and delete received email messages at the mail command prompt: Commands to View and Manage email Messages
4. Issue the following command: cat /var/spool/mail/ops345
   What do you see? What does this show you in terms of where mail is stored on your email server?
5. If you received an email message, the message and subject line should appear as a listing in your mail command.
   NOTE: If you did not receive a mail message, check your mail server settings, check to see if your mail server is running and also check /var/log/maillog and /var/log/messages (this step requires **root** privilege).
6. Once you have received the message, type the mail message number that is displayed in your email message list in the prompt and press ENTER. You should be able to confirm the message body that you sent.

7. Exit the mail program by typing the letter q and press ENTER.
8. Re-issue the mail command. What happened? Issue the command: cat /var/spool/mail/ops345
   What do you notice?
9. Exit the mail command.

Case 2: Setup MTA To Send Mail Messages (No Encryption)

Please verify you have a functional DNS server (at least forward resolution) and necessary iptables rules to allow DNS query.

```
iptables -I INPUT -p tcp --dport=53 -j ACCEPT

iptables -I INPUT -p udp --dport=53 -j ACCEPT
```

1. Add your local DNS server on top of the Internet facing DNS server in /etc/resolv.conf file on both VMs.

```
# Generated by NetworkManager
nameserver 192.168.0.10
search trsbzaaxruwepnasx1xvozqdaf.phxx.internal.cloudapp.net
nameserver 168.63.129.16
```

   This will make sure the mail server checks the local DNS first.

We will use the postfix application as the MTA, and we will set it up on your Server VM and Client VM. They will act as the "sending" email servers for your internal network. You will be able to send email out of your network, and receive email from within your network, but you will not receive email from outside of your network due to the following reasons:

- Individuals outside of your domain will never find the MX records because there are no other DNS servers pointing to your DNS server (i.e. you haven't registered your own domain name and paid for it).

- Even if the individuals could read your MX records, your local network is using IP addresses on a private subnet, which is not routable on the Internet, so it cannot be reached from outside of your system. (unless you configured port forwarding of port 25 in your router properly.)

Verify the Postfix Service Status

Perform the following steps:

1. The postfix application should be installed by default. If it isn't, install it.
2. Postfix is capable of sending email with the default configuration, so start and enable this service, and verify that the postfix service is running.
3. Look for the running postfix service in the list of listening ports by issuing the following command:
   ss -atnp
4. Which service is postfix running? Locate the port used by SMTP, and look for connections with the state LISTEN (i.e. currently listening).

Testing the connection to the Postfix Service

We will demonstrate the use of the **nc** application to test that the postfix service is running and listening.

Perform the following steps:

1. If the **nc** command is not installed on your VMs, install it on both VMs.
2. Connect from your Server VM to itself using the nc command by issuing the following command:
   nc localhost 25
3. You should see a response:

```
[root@server ops345]# nc localhost 25
220 server.jasonpang.ops ESMTP Postfix
```

4. You could theoretically use SMTP commands to send an email here, but this would be a very unusual use of your mail server. You have an MUA for a reason.
5. Enter the command QUIT to close the connection to the server, then <ctrl>-c to terminate the nc command.
   NOTE: If it worked, this indicates that the postfix service is running, listening, and responding to connections.
6. Let's see if it works from other machines. Use nc to connect to Server VM from Client VM and see if it works. If your firewall is set up properly, the nc command should not permit a connection (i.e. no route to host).
   nc server.jasonpang.ops 25
   ```
   [root@client ops335]# nc server.jasonpang.ops 25
   Ncat: No route to host.
   ```
7. Create an iptables rule to allow incoming connections to your SMTP server on your Server VM.
   iptables -I INPUT -p tcp --dport=25 -j ACCEPT
8. Once you open the port in the firewall, retry the nc command. You should get a different error this time (e.g. connection refused).
   ```
   [root@client ops335]# nc server.jasonpang.ops 25
   Ncat: Connection refused.
   ```
   This time the problem is that your service isn't listening on the outside interface, it's currently configured to listen only on the loopback (lo) interface.
9. Make sure the new iptables rule gets saved so that it will be loaded automatically from startup.
   iptables-save > /etc/sysconfig/iptables

Listening on all interfaces

We need to configure the MTA not only to listen to connections from other (separate) MTAs, but to set the domain name and server name in order to allow the user to issue emails in the "standard way", and allow mail messages to provide a correct email address for replies.

Perform the following steps:

1. In your **Server VM** machine, edit the postfix configuration file called: /etc/postfix/main.cf
2. Our first editing change to the postfix configuration will be to make the service "listen" for incoming connections on the external interface (i.e eth0 from the VMs point of view). And internal interface (eth1) Change the value of the following parameter to what is displayed below:
   inet_interfaces = all
3. We should also set the string that will end up in the **From:** header in messages sent by this server. Change the **mydomain** option to YOUR domain name (shown below):
   mydomain = yoursenecaid.ops
4. Also, you must set the **hostname** for this server so that will correctly specify the hostname in the **From:** header in a sent mail message. Make sure the following parameter only appears once (shown below):
   myorigin = $myhostname
5. Ensure that your hostname and DOMAIN name is properly set on your machine, otherwise you will need to set the myhostname parameter.

Warning: Make sure there are no other un-commented copies of those above-mentioned parameters in the Postfix configuration file.

6. Restart the postfix service (systemctl restart postfix), then use the ss -atnp command to confirm that your MTA is now listening on all interfaces (not just loopback)

7. Test by connecting to it (using the nc command) from your Client VM machine.

```
[root@client ops335]# nc server.jasonpang.ops 25
220 server.ops ESMTP Postfix
```

Case 3: Sending Email Between MTAs For Server VM and Client VM (No Encryption)

Your Server VM should now be capable of sending and receiving email, but we can't be sure until we test it. This also would not help the users on the other machines in the network, which are still not capable of receiving email.

Perform the following steps:

1. Repeat the configuration from Case 2 on Client VM (swap Server VM and Client VM when issuing command so that you are configuring Client VM, and using your Server VM server to test the connections).
2. Once that is complete, send an email from ops345 on Server VM to ops345 on Client VM, and then reply from Client VM to Server VM.
3. If both messages arrive, both MTAs are working. If not, use the troubleshooting tools and techniques you have already learned to diagnose and fix the problem.

Case 4: (Optional) Get a DDNS domain name for your public IP and receive email from external vendor.

Optional: To be demonstrated by the instructor in class.

Save the captured file(s) as OPS345_Lab05_yourusername and upload to Blackboard.

If it is video recordings, upload to OneDrive and share with jason.pang@senecacollege.ca

Troubleshooting items if not working.

Iptables:

iptables -I INPUT -p tcp --dport=53 -j ACCEPT

iptables -I INPUT -p udp --dport=53 -j ACCEPT

iptables -I INPUT -p tcp --dport=25 -j ACCEPT

Hostname of VM:

vi /etc/hostname

systemctl restart systemd-hostnamed

DNS server:

Are you able to do: nslookup server.yoursenecaid.ops 192.168.0.10

Is the first DNS as 192.168.0.10? vi /etc/resolv.conf

Are all the required elements installed?

yum install bind*

yum install nc

yum install mailx