CP3 Document

23 FEB 2021
NDD430B

Student: FATJON DAUTI
Instructor: SCOTT APTED

Table of Contents

Create a network diagram that displays the topology and includes: 3
- IP addressing information for all interfaces 3
- A list of services being hosted by each device 3

APACHE (step-by-step) 3
MariaDB Install (step-by-step) 4
Mail Setup (step-by-step) 6
Appendix A – DNS Settings 10
- Expand this table to include all FQDNs and IPs configured in your DNS 10

Appendix B – Linux VM Configurations 11
- The text output from running *hostnamectl* on ALL Linux machines (4) 11

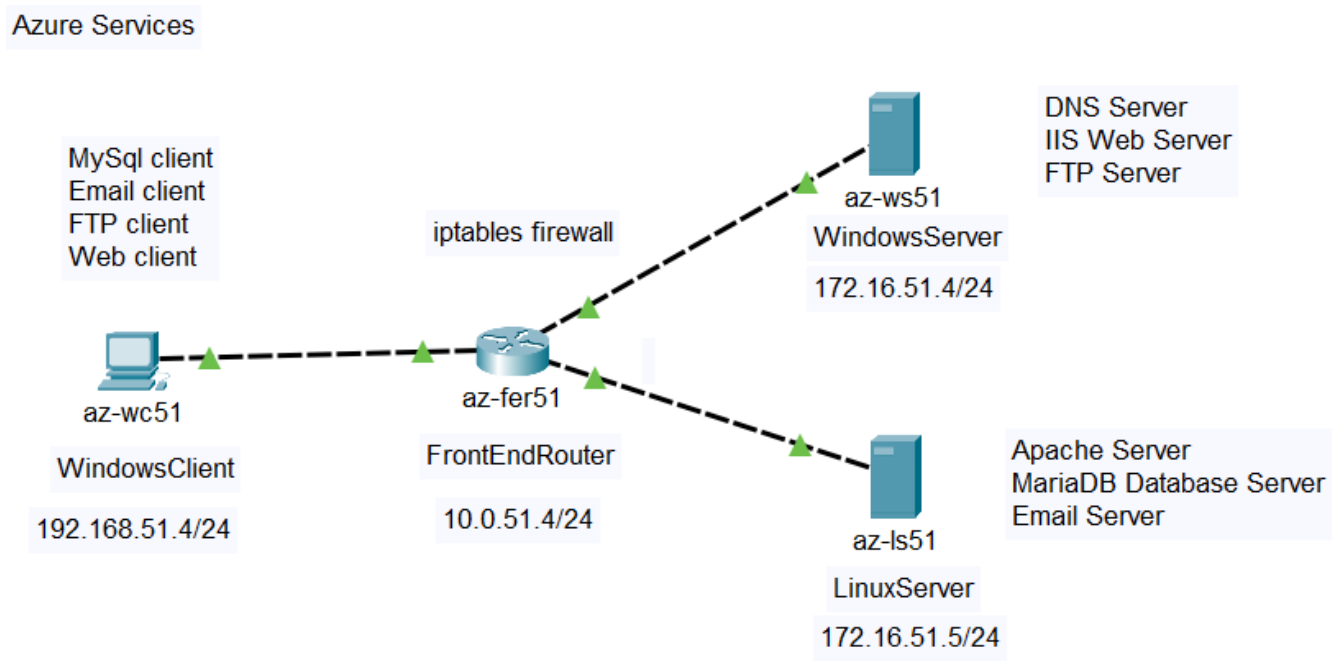
Appendix C – Firewall Configurations 12
- iptables Configurations for ALL Linux machines (4) 12
- Firewall Configuration for Windows Server 13

Appendix D – Routing Configurations 14
- Routing tables for az-fer and onpremR (output of *ip route*) 14

Appendix E – Break-In Attempts - az-fer 14

Create a network diagram that displays the topology and includes:

- **IP addressing information for all interfaces**
- **A list of services being hosted by each device**



APACHE (step-by-step)

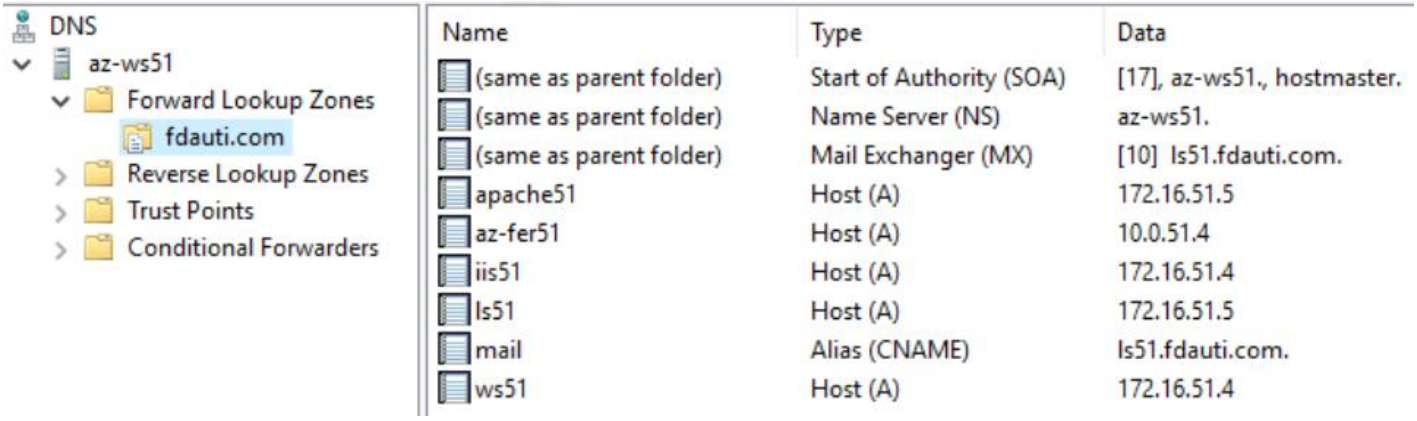
Apache is a popular open-source web-server used to store and deliver web pages (html + images, scripts, style sheets). We will install the Apache service on the az-ls51 VM, running CentOS 7.9. The web-server uses http protocol and listen for connections on tcp port 80 by default. Apache can be installed on CentOS by running the command: yum install httpd -y

Next, we start and enable the apache httpd service, systemctl start httpd; systemctl enable httpd
We can install and use a text based web client like lynx, to test proper installation by running: lynx 127.0.0.1 , the default page of apache server will show up.

If we flush iptables rules on ls51 VM, and add forwarding rules on az-fer51 VM to allow connections on port 80 for ls51 VM, we can access Apache from our az-wc51 VM. Configuring iptables on ls51, we should make sure to allow incoming connections on tcp port 80.

To configure az-ls51 to use DNS, we follow the same steps of CheckPoint 2, when configuring az-fer51 to use DNS. Basically, we edit the eth0 network interface to use az-ws51 as the DNS server.

Also, the appropriate A record pointing to 172.16.51.5 IP (ls51) need to be added on az-ws51 DNS manager for the fdauti.com forward lookup zone.



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[17], az-ws51., hostmaster.
(same as parent folder)	Name Server (NS)	az-ws51.
(same as parent folder)	Mail Exchanger (MX)	[10] ls51.fdauti.com.
apache51	Host (A)	172.16.51.5
az-fer51	Host (A)	10.0.51.4
iis51	Host (A)	172.16.51.4
ls51	Host (A)	172.16.51.5
mail	Alias (CNAME)	ls51.fdauti.com.
ws51	Host (A)	172.16.51.4

After these steps, we can reach Apache with the FQDN ls51.fdauti.com or apache51.fdauti.com from az-wc51, our client VM.

To let Apache display the name, unique ID number, and FQDN name of server, create an index.html file in the DocumentRoot directory of apache, with that information inside. As specified on the apache configuration file ***/etc/httpd/conf/httpd.conf*** - the default DocumentRoot directory is "***/var/www/html***"

```
[root@az-ls51 ~]# ll -h /var/www/html/
total 4.0K
-rw-r--r--. 1 root root 38 Feb 19 05:18 index.html
```

MariaDB Install (step-by-step)

MariaDB is an open-source database server used to manage databases. Using MySQL commands we can administer databases hosted on a database server like mariadb. First, install mariadb on ls51 using yum install mariadb-server

We can confirm installation as follow, by default mariadb will listen on tcp port 3306 on all interfaces

```
[root@az-ls51 ~]# netstat -nautp | grep 3306
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      1926/mysqld
```

If MariaDB doesn't listen to this address by default, we can change the setting on ***/etc/my.cnf*** file, by specifying "bind-address 0.0.0.0" under [mysqld]

We should also configure iptables on ls51 and az-fer51, to allow connections on port 3306

Next thing, is running command: mysql_secure_installation This will configure some basic but important security settings, such as creating a password for the root account, disabling anonymous users etc. With the configured password, we logon to mysql server, mysql -u root -p
Next, we can create another user as shown below,

```
[root@az-ls51 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 14
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'fdauti'@'localhost' IDENTIFIED BY 'fdauti';
Query OK, 0 rows affected (0.00 sec)
```

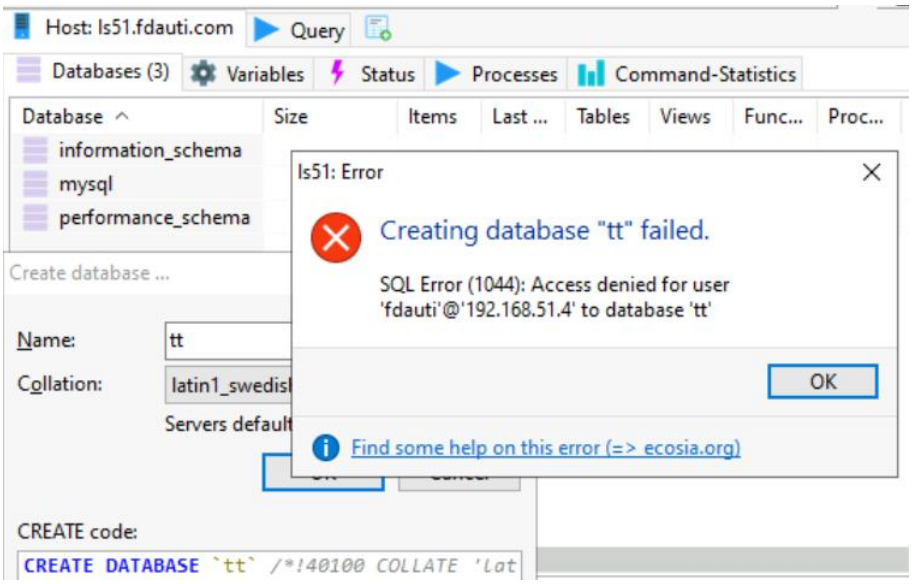
Accessing the database as the newly created user, fdauti:

```
[root@az-ls51 ~]# mysql -u fdauti -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 16
Server version: 5.5.68-MariaDB MariaDB Server
```

We can allow the newly created user fdauti, to access the database remotely by granting the user this permission, running this command while login as root: GRANT SELECT ON *.* TO 'fdauti'@'192.168.51.4' IDENTIFIED BY 'fdauti' WITH GRANT OPTION; The SELECT permission will enable this user to only read through databases, not create or modify them.

The user will not be able to create a database locally or remotely if using a client to connect:

```
MariaDB [(none)]> create database test;
ERROR 1044 (42000): Access denied for user 'fdauti'@'localhost' to database 'test'
```



This is how user and host columns would look like on mysql database. Notice, remote access is only allowed for fdauti user from the az-wc51 client VM.

Host: ls51.fdauti.com Query*

```
1 select user, host from mysql.user;
```

user (5r × 2c)

user	host
root	127.0.0.1
fdauti	192.168.51.4
root	::1
fdauti	localhost
root	localhost

Mail Setup (step-by-step)

Postfix is the default mail server application running on our ls51 linux server. We can test postfix is up and running by issuing the command: ss -natp | grep 25

By default postfix is listing on the loopback interface on tcp port 25. We need to make sure it is listening to all interfaces, by editing the postfix configuration file ***etc/postfix/main.cf***
On this file, we also specify our domain and hostname to correctly identify the mail sent
- *inet_interfaces = all*
- *mydomain = fdauti.com*
- *myorigin = $mydomain*
- *mydestination = $mydomain, $myhostname, localhost.$mydomain, localhost*

As always, we need to make sure port 25 is opened in ls51 iptables firewall, and az-fer51 firewall is correctly forwarding mail to ls51 on smtp port 25. The rules for the Input chain on ls51 and forwarding chain on az-fer51 are specified in the iptables section of this document.

To apply the configurations issue: systemctl restart postfix

After these initial changes, we can test that the postfix server is listing on port 25 and accepting connection from other machines by running from az-fer51: nc ls51.fdauti.com 25

```
[root@az-fer51 ~]# nc ls51.fdauti.com 25
220 az-ls51.fdauti.com ESMTP Postfix
quit
221 2.0.0 Bye
```

Next, we need to add a MX DNS record on our DNS Server (ws51) that will point mail sent to the fdauti.com domain towards the mail server ls51 configured to accept it. Incoming mail addressed to

fdauti.com should be sent to ls51. Adding a CNAME record, we can refer to ws51.fdauti.com mail server as mail.fdauti.com. We can confirm that MX records are correctly setup for the fdauti.com domain, by running: host -t MX fdauti.com or even dig -MX fdauti.com

```
[root@az-ls51 ~]# host -t MX fdauti.com
fdauti.com mail is handled by 10 ls51.fdauti.com.
```

Postfix is working as the MTA (Mail Transfer Agent) our SMTP Server - responsible for sending emails, but there are more component to a Mail Server, such as the MDA (Mail Delivery Agent), responsible for delivering mail to a user inbox. Although Postfix can fulfill this role too, it is recommended to use a more robust solution, by installing another package such as Dovecot, that will store messages to disk on specific subfolders (massage store).

Dovecot will function as an IMAP (or POP3) server, answering MUA (Mail User Agent) requests by storing or retrieving messages from the Message Store. IMAP works with many clients (MUAs) and is preferred to POP3 because messages stored on server after delivered, so a user can always access them on any device the user is login from to check email.

Install Dovecot on ls51, yum install dovecot and start/enable the service. Then configure postfix to use dovecot for delivering and storing email by editing ***/etc/postfix/main.cf*** to add the following line under mailbox_command:

mailbox_command=/usr/libexec/dovecot/dovecot-lda -f "$SENDER" -a "$RECIPIENT"
and apply changes with postfix reload

There are 2 popular message store options to choose from, mbox and maildir. Maildir is preferred because it uses one directory for each user and one file for each message. To configure maildir on dovecot edit file ***/etc/dovecot/conf.d/10-mail.conf*** on the line
mail_location=maildir:~/Maildir
New mail will be placed under the user home directory.

Configure **/etc/dovecot/dovecot.conf** to make sure Dovecot is working only as our IMAP server by editing the protocols line to allow imap only. Also ,on this configuration file it is recommended to add this line also, which is useful when the hostname of the machine does not include the domain part.
postmaster_address = fdauti.com

Since imap works on port 143, we need to make appropriate firewall changes to allow connections on port 143 on ls51 (Input) and az-fer51(Forward) for iptables.

Testing correct setup to see if the imap server is listening for connections on port 143:

```
[root@az-ls51 ~]# ss -natp | grep 143
LISTEN     0      100          *:143                    *:*                  users:(("dovecot"
LISTEN     0      100       [::]:143                 [::]:*                  users:(("dovecot"
```

```
[root@az-fer51 ~]# nc ls51.fdauti.com 143
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot ready.
```

For demonstration purposes, we need to allow connections to Dovecot IMAP server over an unencrypted connection, by editing 2 Dovecot configuration files as follow:

/etc/dovecot/conf.d/10-auth.conf

- *disable_plaintext_auth*=no (to enable plain text logins when not using a secure protocol)

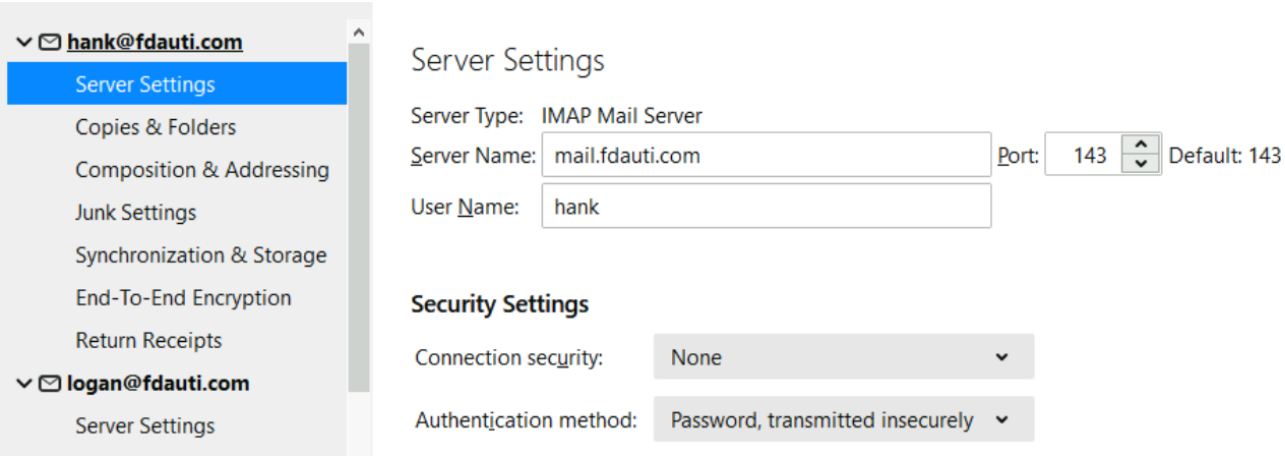
/etc/dovecot/conf.d/10-ssl.conf

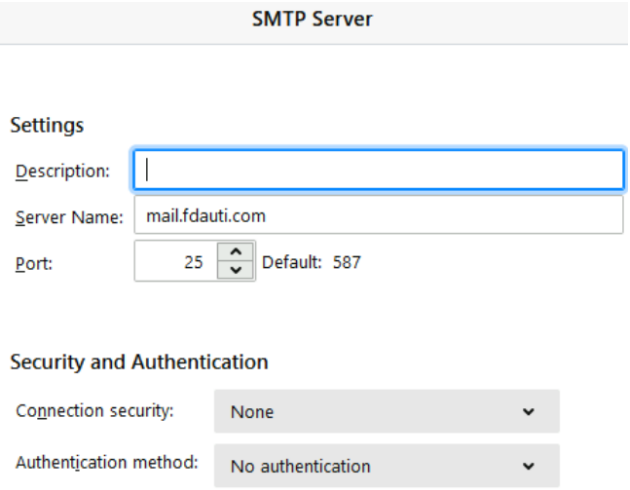
- *ssl=yes*

Finally, using dovecot -n, we can check if dovecot configuration is correct.

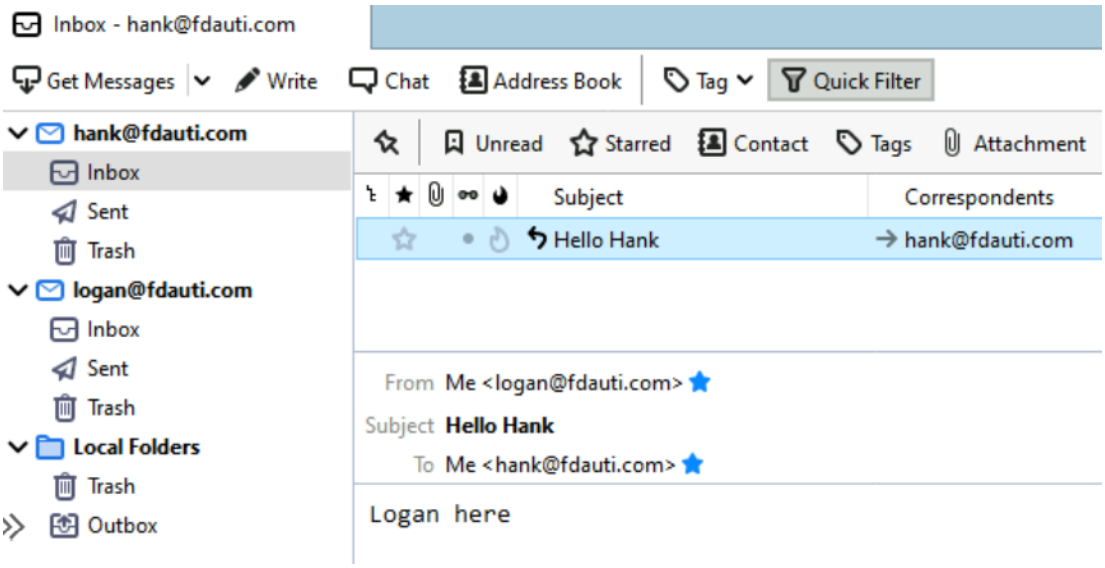
To demonstrate the Mail Server functionality, we add to local user to ls51, hank and logan. useradd -m hank ; useradd -m logan and add a password for them with passwd

For each of them, we will setup a user-account on a mail-client (MUA) like Thunderbird on az-wc51 VM. We will use mail.fdauti.com (CNAME for ls51 mail server) as the incoming/outgoing mail server, since both our IMAP and SMTP server are running on the same machine.





Sending and receiving email between the 2 users accounts on Thunderbird



The Maildir message store directory for user hank on the mail server VM

```
[root@az-ls51 ~]# ll -rh /home/hank/Maildir/
total 24K
drwx------. 2 hank hank    6 Feb 19 16:40 tmp
-rw-------. 1 hank hank   11 Feb 19 16:42 subscriptions
drwx------. 2 hank hank    6 Feb 19 16:40 new
-r--r--r--. 1 hank hank    0 Feb 19 16:38 dovecot-uidvalidity.60302fef
-rw-------. 1 hank hank    8 Feb 19 16:42 dovecot-uidvalidity
-rw-------. 1 hank hank   98 Feb 19 16:40 dovecot-uidlist
-rw-------. 1 hank hank   48 Feb 19 16:42 dovecot.mailbox.log
-rw-------. 1 hank hank 1.4K Feb 19 16:43 dovecot.index.log
-rw-------. 1 hank hank 2.3K Feb 19 16:40 dovecot.index.cache
drwx------. 2 hank hank   62 Feb 19 16:42 cur
```

Appendix A – DNS Settings

DNS Table

- **Expand this table to include all FQDNs and IPs configured in your DNS**

FQDN	IP Address
ls51.fdauti.com	172.16.51.5
iis51.fdauti.com	172.16.51.4
az-fer51.fdauti.com	10.0.51.4
ws51.fdauti.com	172.16.51.4
mail.fdauti.com	172.16.51.5
apache51.fdauti.com	172.16.51.5

Appendix B – Linux VM Configurations

- **The text output from running *hostnamectl* on ALL Linux machines (4)**

```
 Static hostname: az-fer51
       Icon name: computer-vm
         Chassis: vm
      Machine ID: f8b9cbb48fa844c68755eb040009d83b
         Boot ID: 278597ff457b45d0bb9853b1456c9850
  Virtualization: microsoft
Operating System: CentOS Linux 7 (Core)
     CPE OS Name: cpe:/o:centos:centos:7
          Kernel: Linux 3.10.0-1160.15.2.el7.x86_64
    Architecture: x86-64

 Static hostname: az-ls51
       Icon name: computer-vm
         Chassis: vm
      Machine ID: b210cf36d2b54793bd0d8d5c3f8cc892
         Boot ID: 59488cf8fe5c4b7dbee920dc784cd86b
  Virtualization: microsoft
Operating System: CentOS Linux 7 (Core)
     CPE OS Name: cpe:/o:centos:centos:7
          Kernel: Linux 3.10.0-1160.15.2.el7.x86_64
    Architecture: x86-64

 Static hostname: onpremR-51
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 0339622267e24d289010edee94cdb012
         Boot ID: 744b06b672c34843b9492273d93dae7b
  Virtualization: vmware
Operating System: CentOS Linux 7 (Core)
     CPE OS Name: cpe:/o:centos:centos:7
          Kernel: Linux 3.10.0-1160.15.2.el7.x86_64
    Architecture: x86-64

 Static hostname: onpremC-51
       Icon name: computer-vm
         Chassis: vm
      Machine ID: c485aff6f4ae492fb04a3e8df6c9e560
         Boot ID: 8f2bc41e93e74ffb804fdc47f5edbcfc
  Virtualization: vmware
Operating System: Ubuntu 20.04.2 LTS
          Kernel: Linux 5.8.0-41-generic
    Architecture: x86-64
```

Appendix C – Firewall Configurations

- **iptables Configurations for ALL Linux machines (4)**

Linux Server iptables

```
[root@az-ls51 ~]# iptables -L -vn
Chain INPUT (policy DROP 159 packets, 11428 bytes)
 pkts bytes target     prot opt in     out     source               destination
70187   54M ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  *      *       168.63.129.16        0.0.0.0/0
  226 17176 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:123
 2747 1462K ACCEPT     udp  --  *      *       172.16.51.4          0.0.0.0/0            udp spt:53
    3   156 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    1    52 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3306
    3   164 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:25
   13   684 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:143

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 46358 packets, 6847K bytes)
 pkts bytes target     prot opt in     out     source               destination
62116   20M ACCEPT     all  --  *      *       0.0.0.0/0            168.63.129.16
[root@az-ls51 ~]#
```

Front-end-Router iptables

```
[fdauti@az-fer51 ~]$ sudo iptables -L -vn
Chain INPUT (policy DROP 33 packets, 2376 bytes)
 pkts bytes target     prot opt in     out     source               destination
28074   24M ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  *      *       168.63.129.16        0.0.0.0/0
  140 10640 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:123
    3   156 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2151
 3359  632K ACCEPT     udp  --  *      *       172.16.51.4          0.0.0.0/0            udp spt:53
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          tcp dpt:3389
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            tcp spt:3389
  359 27423 ACCEPT     udp  --  *      *       0.0.0.0/0            172.16.51.4          udp dpt:53
  333 54199 ACCEPT     udp  --  *      *       172.16.51.4          0.0.0.0/0            udp spt:53
   18  1589 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          tcp dpt:80
   15   899 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            tcp spt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            tcp spt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          multiport dports 9990:9999
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            multiport sports 9990:9999
 5428  348K ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.5          tcp dpt:22
 3118  362K ACCEPT     tcp  --  *      *       172.16.51.5          0.0.0.0/0            tcp spt:22
   23  3208 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.5          tcp dpt:80
   18  2631 ACCEPT     tcp  --  *      *       172.16.51.5          0.0.0.0/0            tcp spt:80
   21  2114 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.5          tcp dpt:25
   23  1510 ACCEPT     tcp  --  *      *       172.16.51.5          0.0.0.0/0            tcp spt:25
  934 48092 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.5          tcp dpt:143
 1000 82702 ACCEPT     tcp  --  *      *       172.16.51.5          0.0.0.0/0            tcp spt:143
  978 53340 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.5          tcp dpt:3306
  771  596K ACCEPT     tcp  --  *      *       172.16.51.5          0.0.0.0/0            tcp spt:3306

Chain OUTPUT (policy ACCEPT 12368 packets, 1935K bytes)
 pkts bytes target     prot opt in     out     source               destination
27071 8718K ACCEPT     all  --  *      *       0.0.0.0/0            168.63.129.16
[fdauti@az-fer51 ~]$
```

Onprem Router iptables

```
Chain INPUT (policy DROP 11 packets, 924 bytes)
 pkts bytes target     prot opt in     out     source               destination
  847 83427 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    4   240 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    8  2528 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
    9   756 ACCEPT     icmp --  *      *       192.168.51.0/24      0.0.0.0/0
    6   504 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
   14  1830 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 8839  793K ACCEPT     all  --  *      *       192.168.51.0/24      0.0.0.0/0
10756   19M ACCEPT     all  --  *      *       0.0.0.0/0            192.168.51.0/24

Chain OUTPUT (policy ACCEPT 177 packets, 18392 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@onpremR-51 ~]#
```

Ubuntu Client iptables

To make rules persistent on Ubuntu we can install the *iptables-persistent* package.

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1     1288 1165K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
2        6   504 ACCEPT     icmp --  *      *       192.168.51.0/24      0.0.0.0/0
3        4  1312 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:68
4      694 68765 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
5       76 12763 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
root@onpremC-51:~#
```

- **Firewall Configuration for Windows Server**

Firewall configuration on ws51, to allow FTP data transfer on specific port range:

Appendix D – Routing Configurations

- **Routing tables for az-fer and onpremR (output of *ip route*)**

az-fer routing table

```
[root@az-fer51 ~]# ip route
default via 10.0.51.1 dev eth0 proto dhcp metric 100
10.0.51.0/24 dev eth0 proto kernel scope link src 10.0.51.4 metric 100
168.63.129.16 via 10.0.51.1 dev eth0 proto dhcp metric 100
169.254.169.254 via 10.0.51.1 dev eth0 proto dhcp metric 100
```

onpremR routing table

```
[fdauti@onpremR-51 ~]$ ip route
default via 172.17.128.1 dev ens33 proto dhcp metric 100
172.17.128.0/20 dev ens33 proto kernel scope link src 172.17.141.212 metric 100
192.168.51.0/24 dev ens34 proto kernel scope link src 192.168.51.1 metric 101
[fdauti@onpremR-51 ~]$
```

Appendix E – Break-In Attempts - az-fer

- **Examine /var/log/secure and show possible break in attempts for three different dates**

Break-In attempt by 10.0.80.4

```
[root@az-fer51 ~]# tail -f /var/log/secure
Feb 19 21:01:39 az-fer51 sshd[4296]: Connection closed by 10.0.80.4 port 42114 [preauth]
Feb 19 21:01:39 az-fer51 sshd[4298]: Connection closed by 10.0.80.4 port 42116 [preauth]
Feb 19 21:06:49 az-fer51 sshd[4336]: Connection closed by 10.0.80.4 port 42910 [preauth]
Feb 19 21:06:49 az-fer51 sshd[4338]: Connection closed by 10.0.80.4 port 42912 [preauth]
Feb 19 21:11:58 az-fer51 sshd[4383]: Connection closed by 10.0.80.4 port 43698 [preauth]
Feb 19 21:11:58 az-fer51 sshd[4385]: Connection closed by 10.0.80.4 port 43700 [preauth]
Feb 19 21:17:08 az-fer51 sshd[4425]: Connection closed by 10.0.80.4 port 44486 [preauth]
Feb 19 21:17:08 az-fer51 sshd[4427]: Connection closed by 10.0.80.4 port 44488 [preauth]
Feb 19 21:22:18 az-fer51 sshd[4473]: Connection closed by 10.0.80.4 port 45276 [preauth]
Feb 19 21:22:18 az-fer51 sshd[4475]: Connection closed by 10.0.80.4 port 45278 [preauth]
```