CP 1

Document

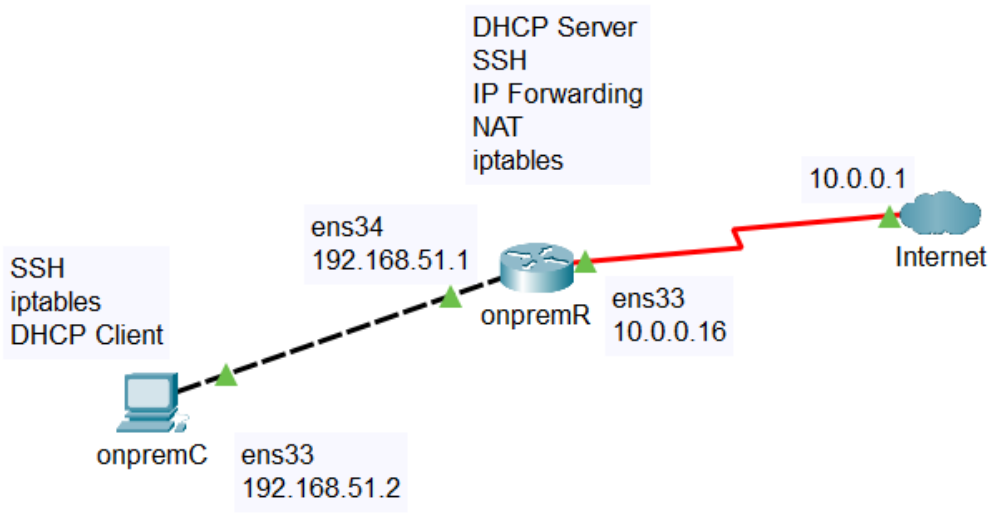
31 JAN 2021
NDD430B

Student: FATJON DAUTI
Instructor: SCOTT APTED

Table of Contents

Network Diagram displaying the topology of on premises (Vmware) network including:

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



Creating the SSH key pair

SSH allows for secure remote connections on servers or other devices which we want to configure, monitor or administer. It uses port 22 by default. The use of an SSH key-pair infrastructure make it easy to login on devices remotely without entering a password. Since we need to connect to onpremR from onpremC, we can create the SSH key-pair on our onpremC and copy the created public key to the onpremR. The keys will be created under the userid (fdauti) account.

We can verify that the ssh client is install on onpreC by running: dpkg -l | grep ssh

```
root@onpremC-51:~# dpkg -l | grep ssh
ii  libssh-4:amd64                      0.9.3-2ubuntu2.1                amd64        tiny C SSH library (OpenSSL flavor)
ii  openssh-client                      1:8.2p1-4ubuntu0.1              amd64        secure shell (SSH) client, for secure access to remote machines
ii  python3-paramiko                    2.6.0-2                         all          Make ssh v2 connections (Python 3)
```

The openssh-client package is installed by default, so we are good to go. On onpremR, which is a CentOs distribution, the ***openssh-server*** package is installed by default:

```
[fdauti@onpremR-51 ~]$ rpm -qa | grep ssh
openssh-clients-7.4p1-21.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
```

This package installs a service called sshd, which is listening by default for connections on port 22:

```
[root@onpremR-51 ~]# netstat -natp | grep sshd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      968/sshd
tcp        0      0 10.0.0.16:22            192.168.51.2:49180      ESTABLISHED 1545/sshd: fdauti [
```

The configuration file for the sshd service is **/etc/ssh/sshd_config**
To disable connections to onpremR with the root account we need to edit sshd_config using an editor like vi, and make sure the line “PermitRootLogin no” is uncommented. Also, since we will use a key-pair infrastructure, after creating it, we should return back to this file and disable SSH login with a password by using the line: “PasswordAuthentication no”. Whenever we edit sshd_config, we have to reload sshd service by using: service sshd reload

The generate the SSH public/private keys on onpremC as a user run: **ssh-keygen -t rsa**
(-t for specifying the rsa encryption). We will not use a pass-phrase, do avoid the downside of typing it every-time. The files that will be created are:
~/.ssh/id_rsa - the private key
~/.ssh/id_rsa.pub - the public key
The easy way to copy the public key to the machine we want to connect to, the onpremR is:
ssh-copy-id -i ~/.ssh/id_rsa.pub userid@onpremR_IP
Providing correct paths and permissions exist, there is always the option to copy the key manually by using, cat ~/.ssh/id_rsa.pub | ssh root@Server_IP_Address "cat >> ~/.ssh/authorized_keys"
.ssh/authorized_keys - under the userid(fdauti) account holds the SSH keys that can be used for logging into onpremR with the fdauti account

We can login to onpremR from onpremC as a user (not with the root account) by:
ssh fdauti@10.0.0.16

Step by Step creation process for onpremR

As shown in the diagram on the first section, the onpremR is the router that will allow the client to connect to the Internet or other services that reside outside the onprem network. onpremR is a virtual machine running Centos 7 minimal Linux distribution. The minimal installation of Centos allows only CLI configuration, uses less resources and is more secure having a smaller attack footprint. We will add 2 network interfaces to this virtual machine, one configured on VMware Workstation as a Lan Segment, which will enable connection with the onpremC and the other interface configured as NAT or Bridge, which will enable connection with the Internet. The difference is, by selecting Bridge this interface will be in the same IP range as the physical network of our host machine.

To create this virtual machine we can use the CentOS-7-x86_64-DVD-2009.iso file download from CentOS website or any other mirror website that hold this version. During the installation, we need to specify a password for the root account and then create another user account with our userid and a password.

To change the hostname machine we can use: hostnamectl set-hostname onpremR-51
To make sure that selinux is enabled and enforcing: sestatus /etc/selinux/config

We can login with our userid, and su to root to run commands that require privileged access, like yum update , to update all packages on our machine.

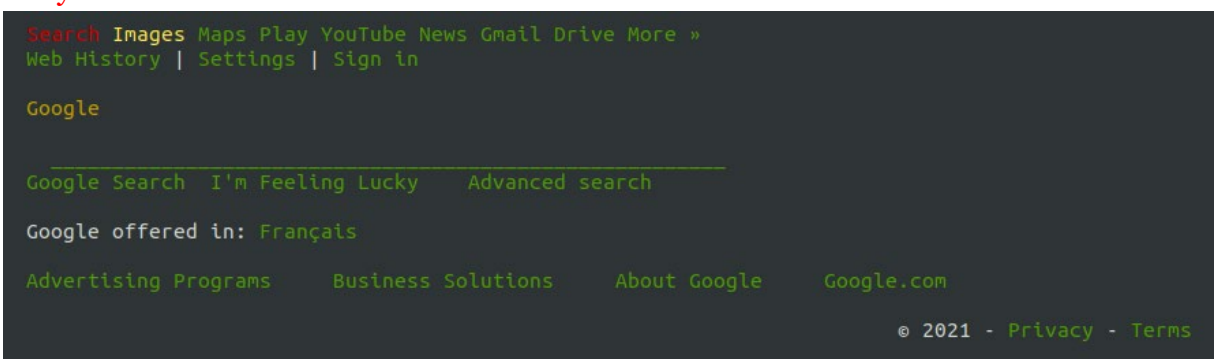
To disable the default firewall that comes with Centos, firewalled:

- systemctl stop firewalld
- systemctl disable firewalld

To install iptables firewall: yum install iptables-services
To start iptables and autostart it on boot:

- systemctl start iptables
- systemctl enalbe iptables

On onpremR we installed 2 additional packages using yum install, Lynx and dos2unix.
Lynx is a web browsers for command-line interfaces. We can check and address by running command: lynx <url>



dos2unix is used to convert plain text files in DOS/MAC format to UNIX format

```
[root@onpremR-51 fdauti]# dos2unix test.txt
dos2unix: converting file test.txt to Unix format ...
```

Since onpremR will be our DHCP server, we need to create a persistent Network Connection for its Lan segment interface, by configuring a static IP for it, for the network 192.168.51.0/24
Since this machine is going to be our router, we can use the first IP in this range. The file that needs to be edited is : /etc/sysconfig/network-scripts/ifcfg-ens34 with a similar configuration as below:

```
[root@onpremR-51 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens34
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
NMCONTROLLED=no
HWADDR=00:0c:29:50:60:e1
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens34
UUID=4e66c010-5056-4886-8ac0-8b3f11ef4ad3
DEVICE=ens34
ONBOOT=yes
IPADDR=192.168.51.1
PREFIX=24
IPV6_PRIVACY=no
```

The important parameters are:
-HWADDR
-Bootproto set to static
-Onboot set to yes
-IPADDR and Prefix

HWADDR needs to be set to the Mac address of the ens34 interface

Configure a DHCP Server on onpremR

First, we check if DHCP is installed, by running the command below as root:

```
[root@onpremR-51 ~]# rpm -qa | grep dhcp
dhcp-4.2.5-82.el7.centos.x86_64
```

If DHCP was not present, we can always install it by running: *yum install dhcp*
We should make sure this service is started and enabled by running: systemctl start dhcpd and systemctl enable dhcpd

/etc/dhcp/dhcpd.conf is the configuration file for DHCP server. On this file we should have the following options configured:

```
#Global options that apply to all networks:
option domain-name-servers 10.0.0.1;
default-lease-time 600;
max-lease-time 7200;

#Subnet Declarations that apply to a specific subnet
subnet 192.168.51.0 netmask 255.255.255.0 {
        range 192.168.51.2 192.168.51.9;
        option routers 192.168.51.1;
}
```

In the above declarations, we have defined the dns server to be 10.0.0.1, the router of the physical network, and a default leas time for IPs of 600 seconds, with a maximum of 2 hours, after which the client will try to renew its IP. This parameter can be shorter for networks with lots of mobile clients and longer for networks with few clients and less movement.
Clients machines on the same lan segment as onpremR ens33 interface will be assigned an IP from the range defined in the subnet declaration above. The default-gateway for these clients will be the IP of ens33 interface of onpremR. Usually, onpremC will be assigned the first IP of this range, 192.168.51.2

To make changes on dhcpd.conf effective, we have to restart the dhcp service: systemctl restart dhcpd

IP Forwarding and NAT

On onpremR we need to configure IP Forwarding and NAT. By default IP Forwarding is disabled by since we are setting up a Linux Router we need it enabled. To enable IP Forwarding permanently, we can edit the file /etc/sysctl.conf and set “net.ipv4.ip_forward = 1” , then run the command sysctl -p /etc/sysctl.conf to make the change effective.

Since our network is a private one and we want to connect it with the “outside” networks, like the internet, we need a NAT service to map IP address from the private Lan network with IP address from the NAT or Briged network (10.0.0.0/24). Packets arriving from the local net with a recipient's IP address somewhere in the internet have to be modified such that the sender's address is equal to the router's address. In the onpremR case, Interface 'ens34' is connected to the local net and the device itself is connected to the internet via a second interface 'ens33'. To connect the local network 192.168.51.0 /24 to the Internet we use the command:
iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
The options can be explained as:
-t nat select table "nat" for configuration of NAT rules
-A POSTROUTING append a rule to the POSTROUTING chain of iptables
-o ens33 rules applied for packets that leave the ens33 network interface (-o for "output")
-j MASQUERADE action that should take place is to 'masquerade' packets, or replace sender's address by the router's address.

To save changes run service iptables save, and to view the rule: iptables -t nat -L -vn

```
Chain POSTROUTING (policy ACCEPT 41 packets, 12924 bytes)
 pkts bytes target     prot opt in     out     source               destination
 9002 2876K MASQUERADE  all  --  *      ens33   0.0.0.0/0            0.0.0.0/0
```

Summary information for the onpremR VM created on VMware Workstation

onpremR-51

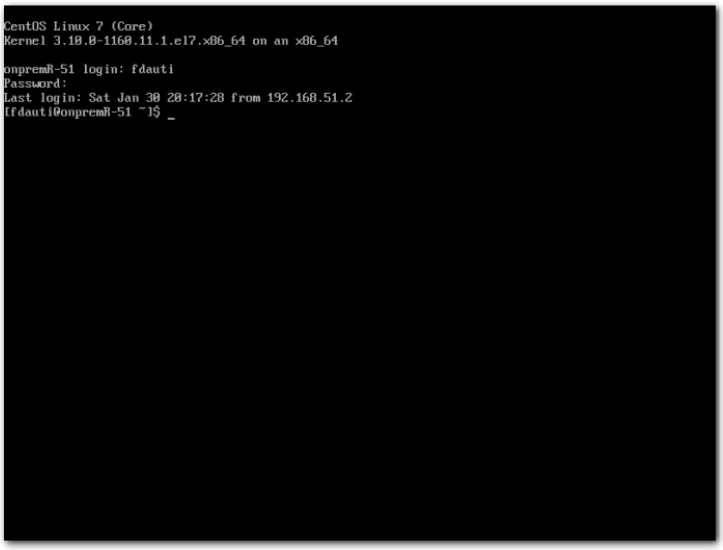
Resume this virtual machine
Edit virtual machine settings

Devices

Memory	1 GB
Processors	1
Hard Disk (SCSI)	10 GB
CD/DVD (IDE)	Using file C:\ISO...
Network Adapter	Bridged (Autom...
Network Adapter 2	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.



Virtual Machine Settings

Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	10 GB
CD/DVD (IDE)	Using file C:\ISO\CentOS-7-x...
Network Adapter	Bridged (Automatic)
Network Adapter 2	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status
- [x] Connected
- [x] Connect at power on

Network connection
- ( ) Bridged: Connected directly to the physical network
  - [ ] Replicate physical network connection state
- ( ) NAT: Used to share the host's IP address
- ( ) Host-only: A private network shared with the host
- ( ) Custom: Specific virtual network
  - VMnet0
- (•) LAN segment:
  - local-LAN-51

LAN Segments... Advanced...

IP address scheme and iptables on onpremR

```
[fdauti@onpremR-51 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:50:60:d7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.16/24 brd 10.0.0.255 scope global noprefixroute dynamic ens33
       valid_lft 80920sec preferred_lft 80920sec
    inet6 fe80::4cc3:c906:ea64:f7c2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:50:60:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.1/24 brd 192.168.51.255 scope global noprefixroute ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe50:60e1/64 scope link
       valid_lft forever preferred_lft forever
[fdauti@onpremR-51 ~]$
```

```
[fdauti@onpremR-51 ~]$ sudo iptables -nL
[sudo] password for fdauti:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0            reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[fdauti@onpremR-51 ~]$
```

Step by Step creation process for onpremC

onpremC is a virtual machine running an Ubuntu desktop linux distro, *ubuntu-20.04.1-desktop-amd64.iso*. The installation process is similar to the installing other VMs on VMWare Wrokstation. On this VM, we will use only one network interface configured on the same Lan Segment as onpremR. By default Ubuntu does not set up a root password and therefore we don't get the ability to log in as root. But we can perform tasks with superuser privileges using sudo <command>, or switch to root by using: sudo -i

To set the hostname: hostnamectl set-hostname onpremC-51

To perform an update use: sudo apt-get update and sudo apt-get upgrade , which updates respectively the repositories and packages. We can then proceed to remove the ufw firewall that comes with Ubuntu on top of iptables, which is already installed by default, sudo apt-get remove ufw

By default, the ens33 Lan segment interface on Ubuntu will be configured to get the ip by dhcp. To force a release an renew of an IP we can run with root privileges: dhclient -rv and dhclient ens33

Here is the log message when DHCP Server assigns an IP to the onpremC client, we can see how it goes by the DORA process:

```
Jan 24 19:55:19 onpremR-51 dhcpd: DHCPDISCOVER from 00:0c:29:66:33:31 via ens34
Jan 24 19:55:20 onpremR-51 dhcpd: DHCPOFFER on 192.168.51.2 to 00:0c:29:66:33:31 (onpremC-51) via ens34
Jan 24 19:55:20 onpremR-51 dhcpd: DHCPREQUEST for 192.168.51.2 (192.168.51.1) from 00:0c:29:66:33:31 (onpremC-51) via ens34
Jan 24 19:55:20 onpremR-51 dhcpd: DHCPACK on 192.168.51.2 to 00:0c:29:66:33:31 (onpremC-51) via ens34
```

Summary information for the onpremC VM created on VMware Workstation

onpremC-51

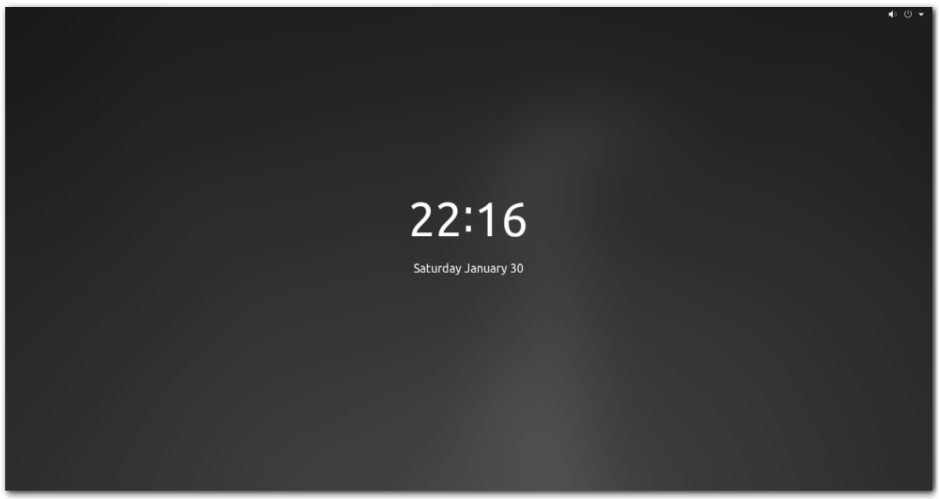
Resume this virtual machine
Edit virtual machine settings

Devices

Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file autoin...
CD/DVD 2 (SATA)	Using file C:\ISO...
Floppy	Using file autoin...
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file autoinst.iso
CD/DVD 2 (SATA)	Using file C:\ISO\ubuntu-20....
Floppy	Using file autoinst.flp
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

- [x] Connected
- [x] Connect at power on

Network connection

- ( ) Bridged: Connected directly to the physical network
  - [ ] Replicate physical network connection state
- ( ) NAT: Used to share the host's IP address
- ( ) Host-only: A private network shared with the host
- ( ) Custom: Specific virtual network
  - VMnet0
- (•) LAN segment:
  - local-LAN-51

LAN Segments... | Advanced...

IP address scheme and iptables on onpremC

```
fdauti@onpremC-51:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:66:33:31 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.51.2/24 brd 192.168.51.255 scope global dynamic noprefixroute ens33
       valid_lft 355sec preferred_lft 355sec
    inet6 fe80::6987:f037:145:71a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
fdauti@onpremC-51:~$
```

```
fdauti@onpremC-51:~$ sudo iptables -nL
[sudo] password for fdauti:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
fdauti@onpremC-51:~$
```

References

- https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-2
- https://linux.die.net/man/5/dhcpd.conf
- https://docs.mysirena.xyz/centos-7/prefilight-configuration/how-to-enable-ip-forwarding
- https://www.karlrupp.net/en/computer/nat_tutorial
- https://www.poftut.com/how-to-start-stop-and-enable-disable-iptables-or-ufw-in-ubuntu-debian-kali-mint/
- https://kb.iu.edu/d/afik (Lynx)
- https://www.tutorialspoint.com/unix_commands/dos2unix.htm