# Building the Lab on a Windows 10 Host

To build the lab gather the following:

* Oracle Virtual Box installed on the host computer with enough RAM and disk to support three (3) Virtual Ubuntu machines running concurrently
* The Ubuntu server install media in ISO format

The following are the names for the three VMs to be created:

1. northclient – the host above the firewall
2. firewall – the firewall
3. southclient – the host below the firewall

## Initial Setup

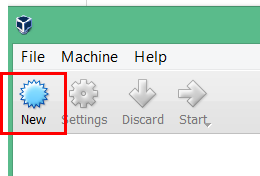
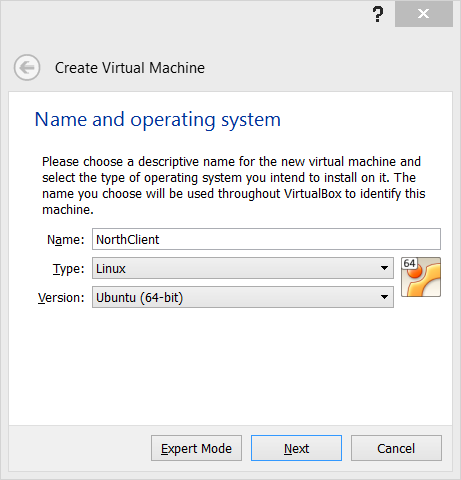
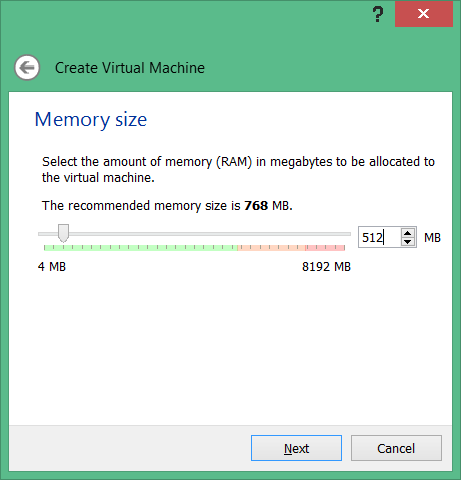
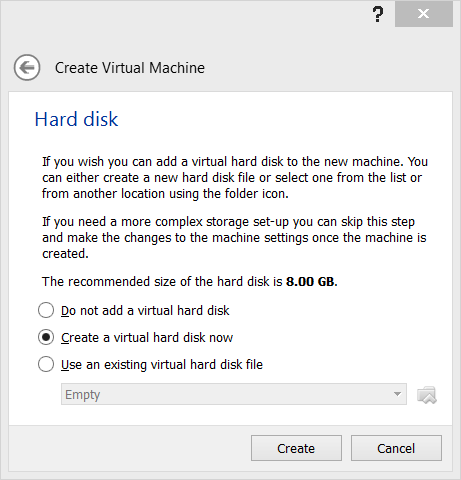
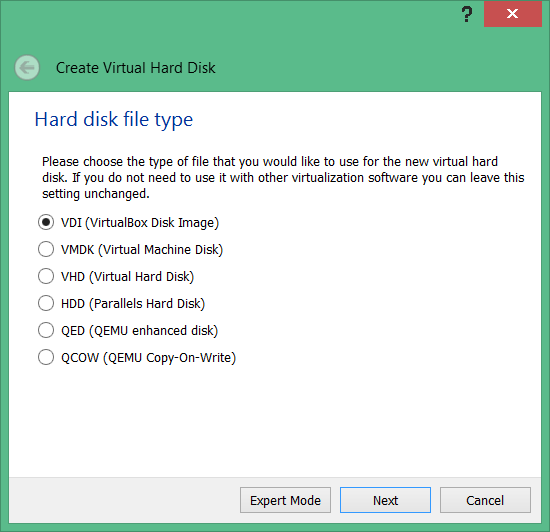
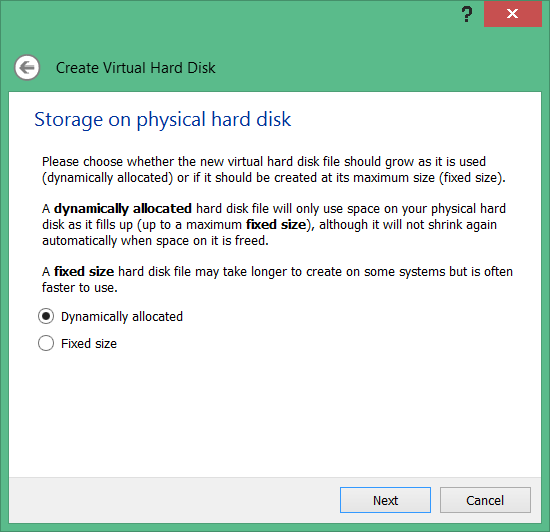
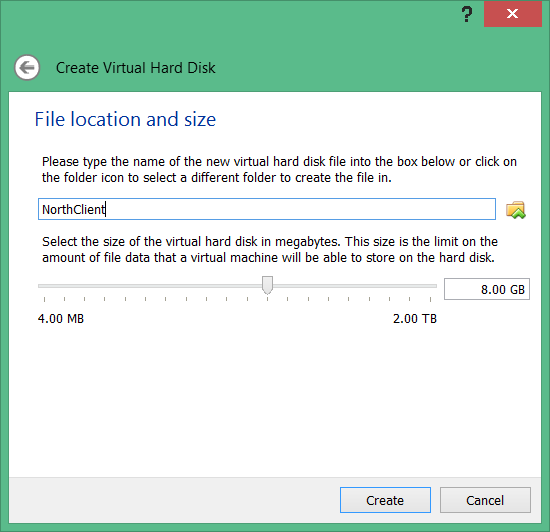
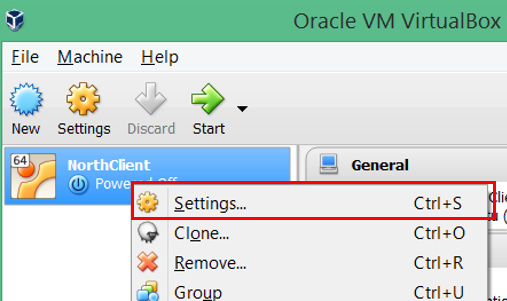
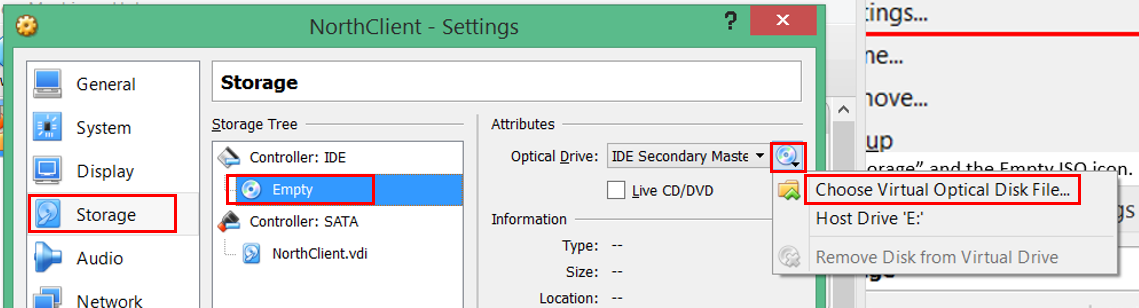
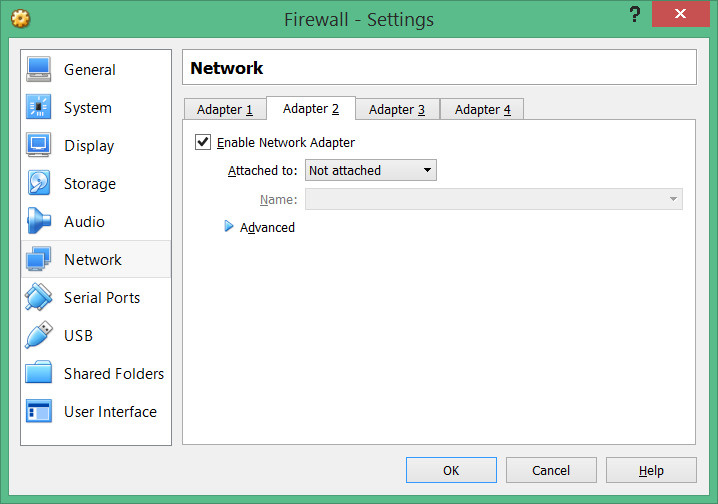
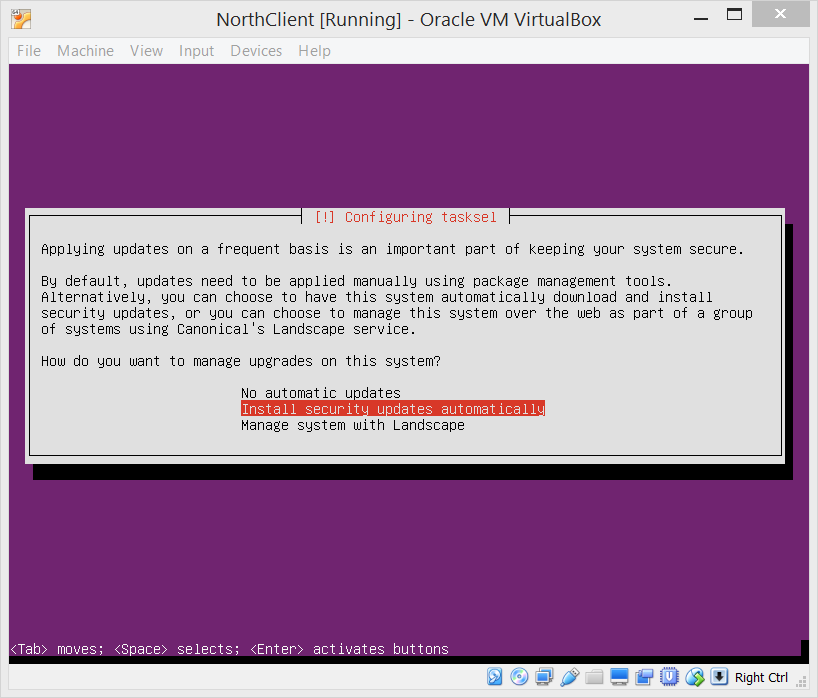
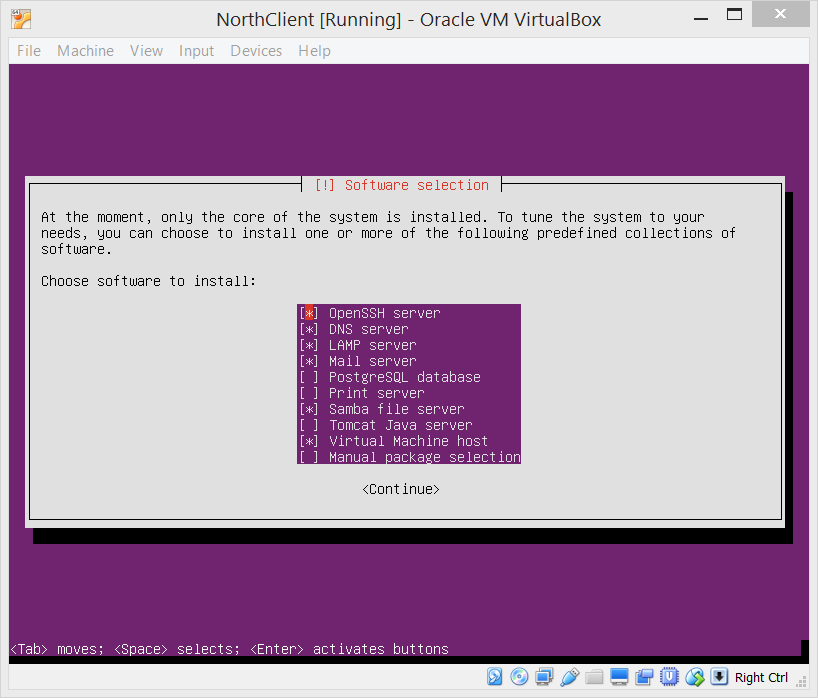
Take the following steps to prepare your computer for building the lab.

1. Download and install Virtual Box from <https://www.virtualbox.org/wiki/Downloads>
2. Download the current LTS Ubuntu ISO from <http://www.ubuntu.com/download/server>
3. Install Virtual Box on your host computer, choosing the default options.

## Creating the Virtual Machines

Create a VM and clone it 2x times. Name the three machines to be created, firewall, northclient, and southclient. If importing from an \*.ova file, skip to the configuration steps; otherwise, proceed below with the manual installation.

Follow the following process to create the 3 Ubuntu Servers needed for this lab:

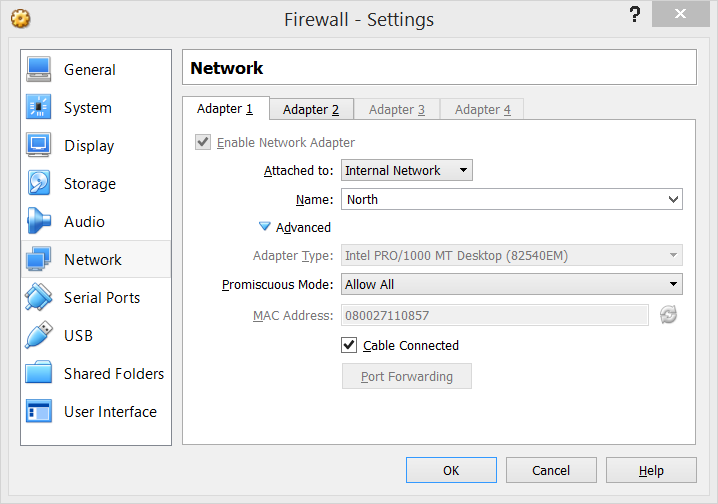
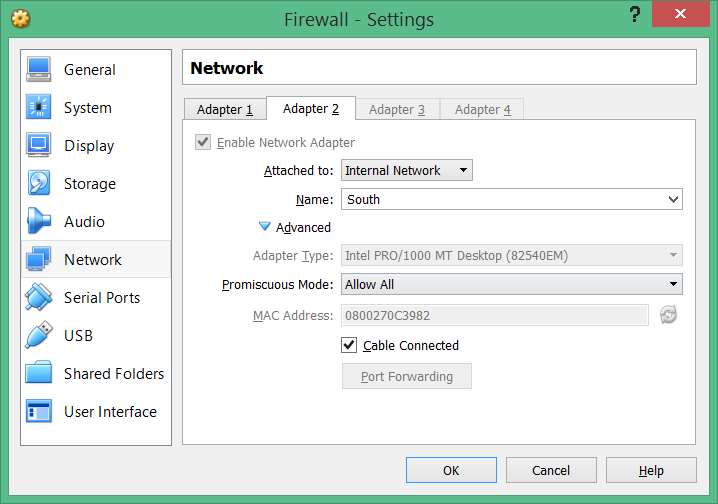
1. Click on the “New” icon:  
   
2. Choose a name for the VM, depending upon which host you are creating (the Initial Setup section above). Choose “Linux” for “Type” and “Ubuntu” for “Version”. Be sure to pick 64 or 32 bit as appropriate. If possible, use 64 bit (this will depend upon your host computer).  
   
3. Choose the amount of RAM to be used. 512MB should be enough for this lab for all 3 VMs.  
   
4. Choose to create a virtual disk now.  
   
5. Choose VDI.  
   
6. Choose Dynamically Allocated.  
   
7. Choose 8GB of disk space to be used.  
   
8. Once the host is created, right click on it and select “Settings”.  
   
9. In the resulting window, select “Storage” and select “Empty”. Click on the CD icon and select “Choose Virtual Optical Disk File…”. 
10. In the resulting dialog box, select the Ubuntu Server image that was downloaded in the Initial Setup section (see above). Click “Open” to close the File Dialog
11. If the host being created is the **North or South client**, choose “Okay” to close the Settings window.
12. If the host being created is the **Firewall**, choose “Network” and click on the “Adapter 2” tab. Select “Enable Network Adapter”. Choose “Okay” to close the Settings window.  
    
13. Click Start to power on the VM. Follow all of the default Ubuntu installation options, but choose the following options at the following screens:
    1. **Hostname:** When prompted, use the same name as selected for the VM in VirtualBox.
    2. **Security Updates**: Select Install security updates automatically:  
       
    3. For Software selection, choose the following
       1. for the **North and South Clients**:  
          
          1. OpenSSH server
          2. DNS server
          3. LAMP server
          4. Mail server
          5. Samba file server
          6. Virtual Machine Host
       2. For the **Firewall**:
          1. OpenSSH server
          2. Virtual Machine Host

## 

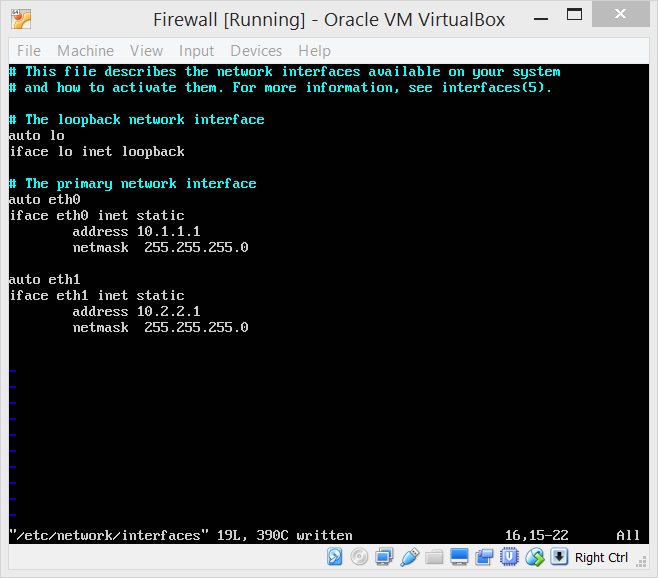
## Configure the Network

After all three VMs have been installed, follow these steps to configure the network setup.

### Configure VirtualBox

1. Open the Settings window for the Firewall VM. Choose Network, and select “Internal Network” for “Attached To”. Type in the name “North”. Set “Promiscuous Mode” to “Allow All”:
2. Choose the “Adapter 2” tab and select “Internal Network” for “Attached To”. Type in the name “South”. Set “Promiscuous Mode” to “Allow All”:  
   
3. Click “Okay” to close the window and save the settings.
4. On the northclient VM, set its interface to the same as “Adapter 1” of the Firewall.
5. On southclient VM, set its interface to the same as “Adapter 2” of the Firewall.

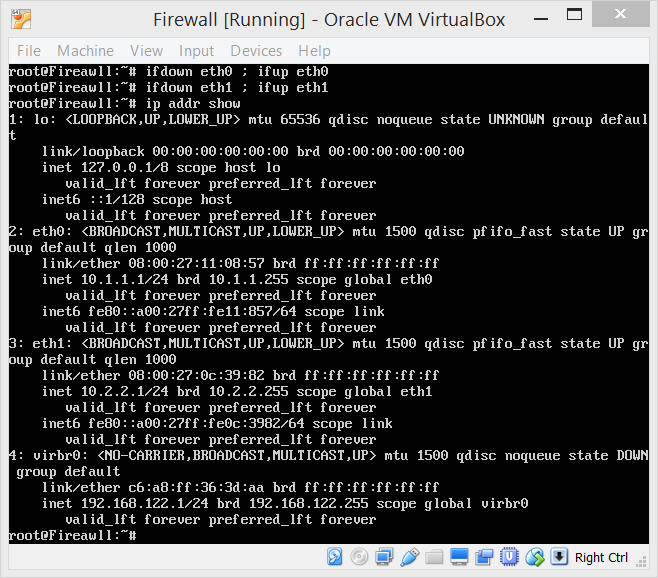
### Configure the Virtual Machines

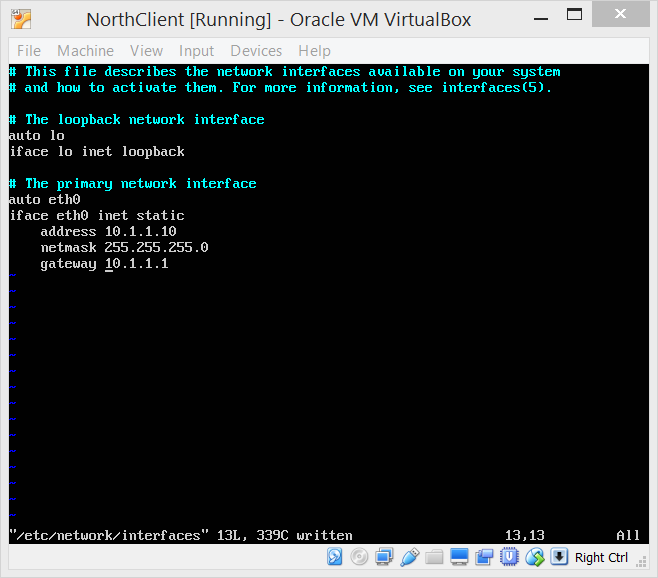
1. On the Firewall, change the /etc/network/interfaces file to configure the network interfaces:  
   
   1. eth0

|  |  |
| --- | --- |
| Type | Static |
| Address | 10.1.1.1 |
| Netmask | 255.255.255.0 |

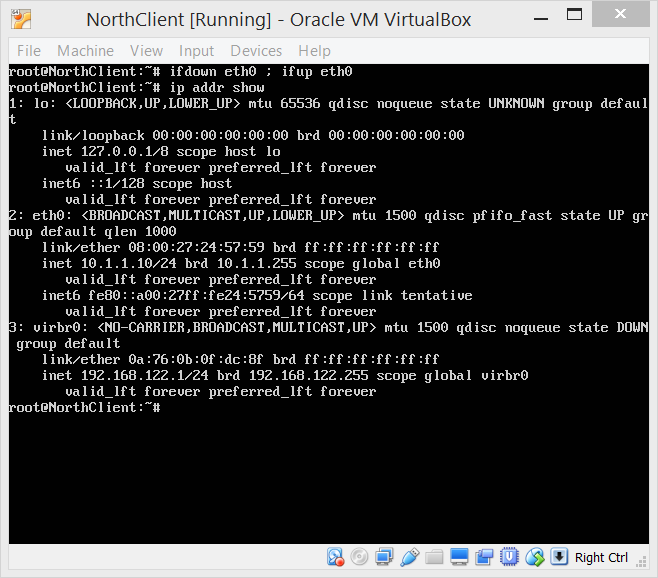
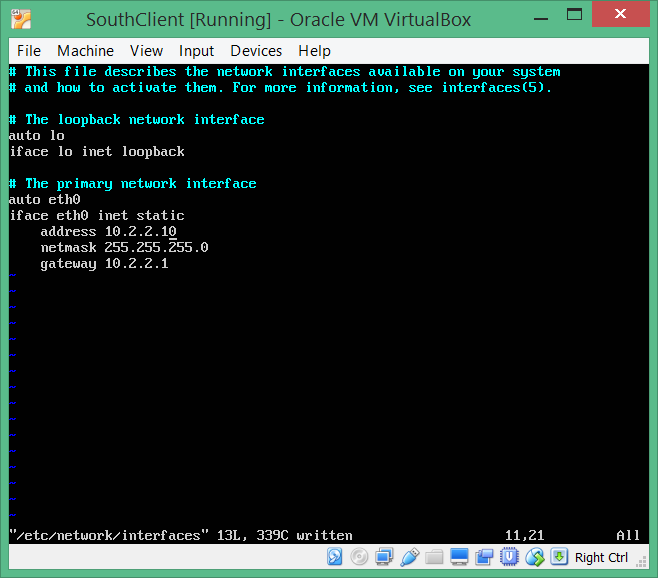
* 1. eth1

|  |  |
| --- | --- |
| Type | Static |
| Address | 10.2.2.1 |
| Netmask | 255.255.255.0 |

* 1. Restart the network interfaces by executing:
     1. ifdown eth0; ifup eth0
     2. ifdown eth1; ifup eth1
  2. Check the network status with ‘ip addr show’  
     

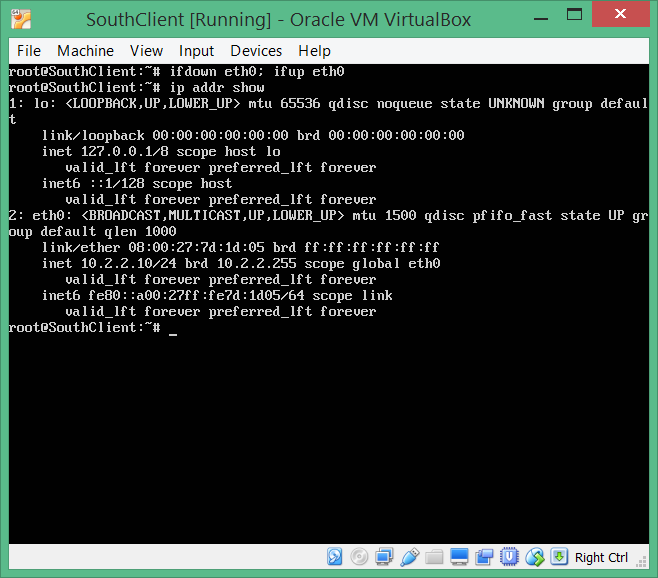
1. On the northclient, change /etc/network/interfaces file to configure the eth0 network interface:   
   

|  |  |
| --- | --- |
| Type | Static |
| Address | 10.1.1.10 |
| Netmask | 255.255.255.0 |
| Gateway | 10.1.1.1 |

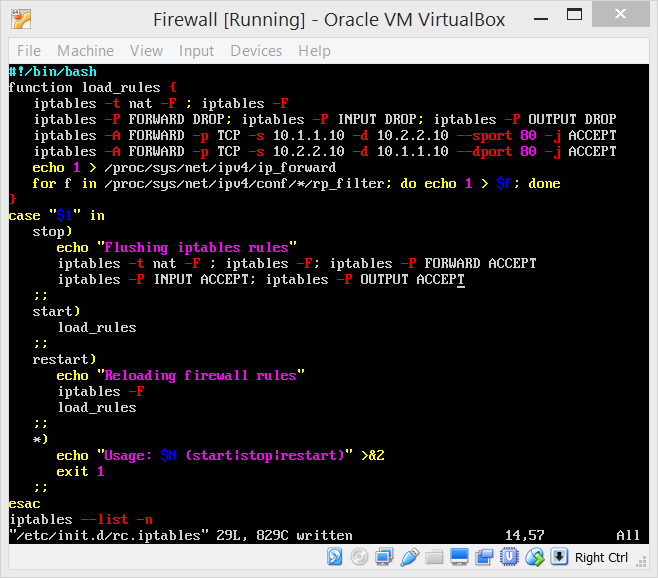
1. Restart the network interfaces by executing: ifdown eth0; ifup eth0
2. Check the network status with ‘ip addr show’  
   
3. On the northclient, edit /etc/network/interfaces file to configure the eth0 network interface:   
   

|  |  |
| --- | --- |
| Type | Static |
| Address | 10.1.1.10 |
| Netmask | 255.255.255.0 |
| Gateway | 10.1.1.1 |

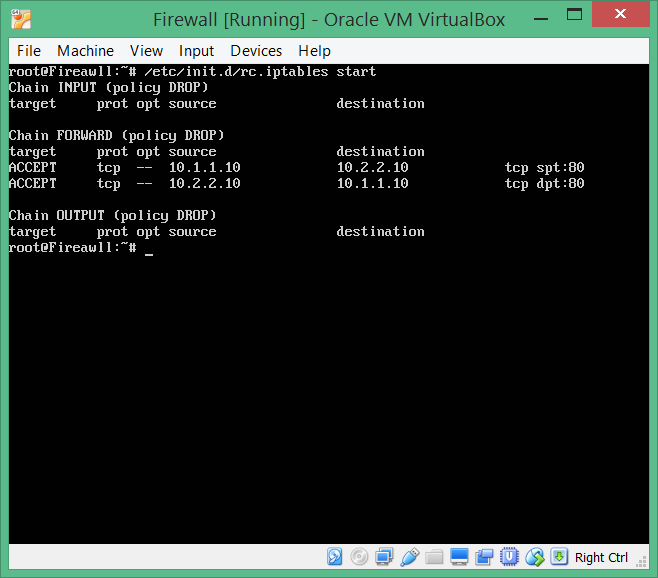
1. Restart the network interfaces by executing: ifdown eth0; ifup eth0

1. Check the network status with ‘ip addr show’  
   

### Configure the firewall host init script for iptables

1. As root, create the /etc/init.d/rc.iptables file and add the following content:  
   

A copy of this script is provided in the configuration files (rc.iptables.sh).

1. Save the file and set the permissions to 755.
2. Execute the file, passing the ‘start’ argument:  
   

# You have completed the initial VM build and configuration steps. Continue to the lab exercises.