Lab 1: Creating a Virtual Infrastructure

A Setting up the network

Figure 1 outlines the setup of the lab for routing, where we will assign three network addresses. Interfaces which are connected to the Vyatta firewall will be able to route, but we have to use NAT to allow the DMZ and private networks to connect to the public network.

Our first task is to route through the Vyatta firewall to connect two networks. In the lab you will be assigned two networks in the form:

172.16.*x*.0/24 172.16.*y*.0/24 Demo: http://youtu.be/4X2ulNeixto

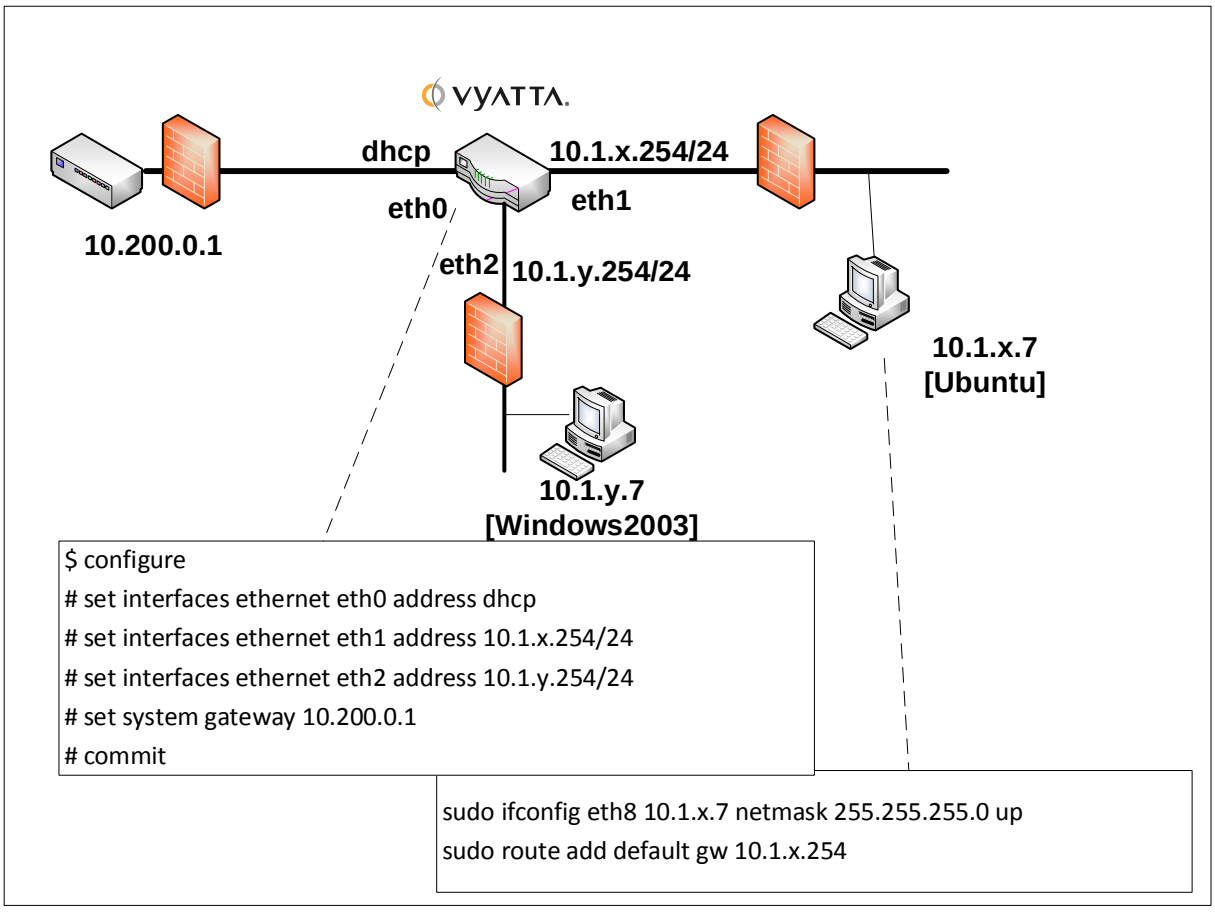

Figure 1: Lab setup (eth0 – Public, eth1 – Private, eth2 – DMZ)

Log into vSphere and locate **csn11123**, and then select one of the following allocated folders:

Allocated	Ubuntu	Windows	Eth0	Eth1	Eth2
Group_001	172.16.1.7/24	172.16.2.7/24	DHCP	172.16.1.254/24	172.16.2.254/24
Group_002	172.16.3.7/24	172.16.4.7/24	DHCP	172.16.3.254/24	172.16.4.254/24
Group_003	172.16.5.7/24	172.16.6.7/24	DHCP	172.16.5.254/24	172.16.6.254/24
Group_004	172.16.7.7/24	172.16.8.7/24	DHCP	172.16.7.254/24	172.16.8.254/24
Group_005	172.16.9.7/24	172.16.10.7/24	DHCP	172.16.9.254/24	172.16.10.254/24
Group_006	172.16.11.7/24	172.16.12.7/24	DHCP	172.16.11.254/24	172.16.12.254/24

Group_007	172.16.13.7/24	172.16.14.7/24	DHCP	172.16.13.254/24	172.16.14.254/24
Group_008	172.16.15.7/24	172.16.16.7/24	DHCP	172.16.15.254/24	172.16.16.254/24
Group_009	172.16.17.7/24	172.16.18.7/24	DHCP	172.16.17.254/24	172.16.18.254/24
Group_010	172.16.19.7/24	172.16.20.7/24	DHCP	172.16.19.254/24	172.16.20.254/24
Group_011	172.16.21.7/24	172.16.22.7/24	DHCP	172.16.21.254/24	172.16.22.254/24
Group_012	172.16.23.7/24	172.16.24.7/24	DHCP	172.16.23.254/24	172.16.24.254/24
Group_013	172.16.25.7/24	172.16.26.7/24	DHCP	172.16.25.254/24	172.16.26.254/24
Group_014	172.16.27.7/24	172.16.28.7/24	DHCP	172.16.27.254/24	172.16.28.254/24
Group_015	172.16.29.7/24	172.16.30.7/24	DHCP	172.16.29.254/24	172.16.30.254/24
Group_016	172.16.31.7/24	172.16.32.7/24	DHCP	172.16.31.254/24	172.16.32.254/24
Group_017	172.16.33.7/24	172.16.34.7/24	DHCP	172.16.33.254/24	172.16.34.254/24
Group_018	172.16.35.7/24	172.16.36.7/24	DHCP	172.16.35.254/24	172.16.36.254/24
Group_019	172.16.37.7/24	172.16.38.7/24	DHCP	172.16.37.254/24	172.16.38.254/24
Group_020	172.16.39.7/24	172.16.40.7/24	DHCP	172.16.39.254/24	172.16.40.254/24
Group_021	172.16.41.7/24	172.16.42.7/24	DHCP	172.16.41.254/24	172.16.42.254/24
Group_022	172.16.43.7/24	172.16.44.7/24	DHCP	172.16.43.254/24	172.16.44.254/24
Group_023	172.16.45.7/24	172.16.46.7/24	DHCP	172.16.45.254/24	172.16.46.254/24
Group_024	172.16.47.7/24	172.16.48.7/24	DHCP	172.16.47.254/24	172.16.48.254/24
Group_025	172.16.49.7/24	172.16.50.7/24	DHCP	172.16.49.254/24	172.16.50.254/24
Group_026	172.16.51.7/24	172.16.52.7/24	DHCP	172.16.51.254/24	172.16.52.254/24
Group_027	172.16.53.7/24	172.16.54.7/24	DHCP	172.16.53.254/24	172.16.54.254/24
Group_028	172.16.55.7/24	172.16.56.7/24	DHCP	172.16.55.254/24	172.16.56.254/24
Group_029	172.16.57.7/24	172.16.58.7/24	DHCP	172.16.57.254/24	172.16.58.254/24
Group_030	172.16.59.7/24	172.16.60.7/24	DHCP	172.16.59.254/24	172.16.60.254/24
Group_031	172.16.61.7/24	172.16.62.7/24	DHCP	172.16.61.254/24	172.16.62.254/24
Group_032	172.16.63.7/24	172.16.64.7/24	DHCP	172.16.63.254/24	172.16.64.254/24
Group_033	172.16.65.7/24	172.16.66.7/24	DHCP	172.16.65.254/24	172.16.66.254/24
Group_034	172.16.67.7/24	172.16.68.7/24	DHCP	172.16.67.254/24	172.16.68.254/24
Group_035	172.16.69.7/24	172.16.70.7/24	DHCP	172.16.69.254/24	172.16.70.254/24
Group_036	172.16.71.7/24	172.16.72.7/24	DHCP	172.16.71.254/24	172.16.72.254/24
Group_037	172.16.73.7/24	172.16.74.7/24	DHCP	172.16.73.254/24	172.16.74.254/24
Group_038	172.16.75.7/24	172.16.75.7/24	DHCP	172.16.75.254/24	172.16.76.254/24

User logins: Ubuntu (User: napier, Password: napier123), Windows: (User: Administrator, Password: napier), Vyatta (User: vyatta, Password: vyatta).
Note: Sometimes the network names are different, such as Eth3, Eth4 and Eth5. Assume that the first network name is Public, the second is the Private network, and the third is the DMZ.

Draw your own network diagram here, by filling-in the blank boxes, with the allocated networks, subnets, and IP addresses:

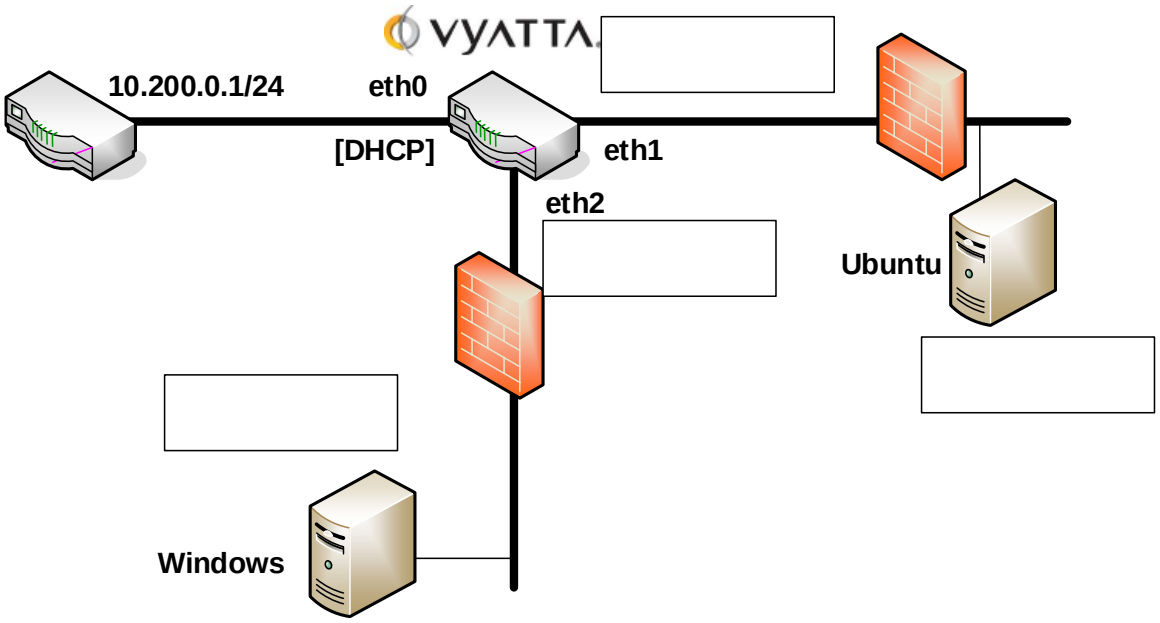

Figure 2: Your network setup

☞ Select your Ubuntu host (User: napier, Password: napier123) and configure and add it at 172.16.*x*.7 with a default gateway of 172.16.*x*.254 and a subnet mask of 255.255.255.0.

Can you ping the 172.16.*x*.7 port from the host selected? Yes/No

☞ Select your Windows server (User: Administrator, Password: napier) and configure and add it at 172.16.*y*.7 with a default gateway of 172.16.*y*.254 and a subnet mask of 255.255.255.0.

Can you ping the 172.16.*y*.7 port from the host selected? Yes/No

☞ From each of your hosts, can you ping the other host? Yes/No

Why can't you ping the other host?

Note. For Linux uses the commands:

```
sudo ifconfig eth8 172.16.x.7 netmask 255.255.255.0 up
sudo route add default gw 172.16.x.254
```

B Routing between connected networks

Start up your Vyatta firewall. Initially erase the config in the firewall, and reboot it, with:

```
cp /opt/vyatta/etc/config.boot.default /opt/vyatta/etc/config/config.boot
reboot
```

Next perform the following:

☞ Setup a few simple things, such as the hostname, a username and password, and so on:

```
$ configure
# set system host-name yourname
# set system login user yourname authentication plaintext-password yourpass
```

☞ Configure the firewall using the following commands (changing the *x* and *y* for your net):

```
$ configure
# set interfaces ethernet eth0 address dhcp
# set interfaces ethernet eth1 address 172.16.x.254/24
# set interfaces ethernet eth2 address 172.16.y.254/24
# set system gateway 10.200.0.1
```

Before you commit the configuration, can you ping the 172.16.*y*.7 port from the host on at 172.16.*x*.7? Yes/No

Now go ahead and commit the configuration with:

```
# commit
# exit
```

Can you ping the 172.16.*y*.7 port from the host on 172.16.*x*.7? Yes/No

Can you ping the 172.16.*x*.7 port from the host on 172.16.*y*.7? Yes/No

Now run Wireshark on your hosts, and repeat. Examine you network trace, and determine the successful ping request, and ping reply. Which ICMP type codes are used for the request and the successful reply:

What do the following commands do:

`show configuration`:

`show interface`:

Now delete the IP address on the eth1 interface on the firewall, and reassess:

Can you ping the 172.16.*y*.7 port from the host on the 172.16.*x*.7? Yes/No

Can you ping the 172.16.*x*.7 port from the host on the 172.16.*y*.7? Yes/No

Now run Wireshark on your hosts, and repeat. Examine you network trace, and determine the unsuccessful ping request, and ping reply. Which ICMP type codes are used for the request and the unsuccessful reply:

Note:

```
$ configure
# delete interfaces ethernet eth1 address 172.16.x.254/24
# commit
```

Now, reapply the IP address, and using the arp –a command, determine the MAC addresses of the gateway adapter, and check this against the configuration of the firewall.

What are the MAC addresses of the firewall:

Now with a browser on each host, access the Web server on the other network.

Can you access the Web server on the 172.16.*y*.7 from 172.16.*x*.7? Yes/No

Can you access the Web server on the 172.16.*x*.7 from 172.16.*y*.7? Yes/No

As before, disable the IP address on the eth1 port, and reapply (make sure you refresh the cache on the browser):

Can you access the Web server on the 172.16.*y*.7 from 172.16.*x*.7? Yes/No

Can you access the Web server on the 172.16.*x*.7 from 172.16.*y*.7? Yes/No

Reapply everything as before, and test that it still works.

Startup Wireshark on each of your hosts, and capture traffic.

☞ Run an nmap scan from the Windows host to the Linux one. What ports are open on the Linux host:

☞ Run an nmap scan from the Linux host to the Windows one. What ports are open on the Windows host:

Commands:
```
nmap –sS 172.16.1.0/24
```

C Setting up NAT

Now we need to setup NAT to map the addresses on the DMZ and the private network to an address taken from the public network. We are using NAT overloading (or NAT masquerade) which will map the private addresses to a public address (taken from eth0).

To map the addresses from the private to the public network:

```
# set nat source rule 1 outbound-interface eth0
```

```
# set nat source rule 1 source address 172.16.x.0/24
# set nat source rule 1 translation address masquerade
# commit
# save
```

To map the addresses from the DMZ to the public network:

```
# set nat source rule 2 outbound-interface eth0
# set nat source rule 2 source address 172.16.y.0/24
# set nat source rule 2 translation address masquerade
# commit
# save
```

You should now have network connection from the private and DMZ networks to the public network. On your Ubuntu host change name server to 10.200.0.1 with:

```
sudo nano /etc/resolv.config
```

And change the nameserver to:

```
nameserver 10.200.0.1
```

Now can you ping 10.200.0.1 from Ubuntu? Yes/No
Now can you ping 10.200.0.1 from Windows2003? Yes/No

Now can you ping 8.8.8.8 from Ubuntu? Yes/No
Now can you ping 8.8.8.8 from Windows2003? Yes/No

Now can you access Google.com from Ubuntu? Yes/No
Now can you access Google.com from Windows2003? Yes/No

D Setting up services on firewall

Now save your configuration in edit mode with:

```
# save
# exit
$ reboot
```

You can now reboot the firewall (use the command **reboot**), and login with your new username and password.

Now restart Wireshark on the Linux install. Next enable the Telnet server on the Vyatta firewall with:

```
# set service telnet
# commit
```

Now telnet into the Vyatta firewall.

Was the login successful? Yes/No

Using the TCP Stream trace on the Wireshark trace. What can you observe from the stream? Can you see the password for the login?

Note:
`sudo wireshark`

Now restart Wireshark on the Linux install. Next enable the SSH server on the Vyatta firewall with:

```
# set service ssh
# commit
```

Now ssh into the Vyatta firewall from the Linux host using:

`ssh 172.16.`*y*`.254 -l` *username*

Was the login successful? Yes/No

Using the TCP Stream trace on the Wireshark trace. What can you observe from the stream? Can you see the password for the login?

E Identifying Services

Within a network infrastructure we have services which run on hosts. These services provide a given functionality, such as for sending/receiving email, file storage, and so on.

From → To	Command	Observation
DMZ	On your Windows host, run the command: `netstat –a` and outline some of the services which are running on your host (define the port number and the name of the service and only pick off the LISTENING status on the port).	Outline some of the services which are running on your host (define the port number and the name of the service):
LAN	For the Ubuntu Virtual Machine, and run the command: `netstat –l`.	Outline some of the services which are running on your host (define the port number and the name of the service):
DMZ	Next we will determine if these services are working. There should be a Web server working on each of the virtual machines (Ubuntu and Windows 2003), so from the Windows host and using a Web browser, access the home page: `http://172.16.x.7`	Is the service working: [Yes] [No]

LAN	From Ubuntu, access the Web server at: `http://172.16.y.7`	Is the service working: [Yes] [No]
LAN	Next we will determine if these services are working using a command line. From your UBUNTU host, undertake the following: `telnet 172.16.y.7 80` then enter: `GET /`	Outline the message that is returned:
DMZ	Repeat the previous example from the WINDOWS host: `telnet 172.16.x.7 80`	

DMZ	There should be an FTP server working on Ubuntu and Windows 2003. From WINDOWS, access the FTP server on the UBUNTU server:
	`telnet 172.16.x.7 21`
	
	then enter:
	
	`USER napier`
	`PASS napier123`
	`QUIT`
		Outline the messages that you received:
		
		What happens to each of these when you try with an incorrect username and password:

LAN	From UBUNTU access the WINDOWS host with `telnet 172.16.x.7 21` then enter:	Outline the messages that you received: What happens to each of these when you try with an incorrect username and password:

	USER Administrator PASS napier QUIT	
DMZ	On the UBUNTU instance you will see that the **VNC** service is running, which is the remote access service. From your WINDOWS host, access the VNC service using a VNC client, and see what happens.	What does this service do:
DMZ	Next we will assess the SMTP service running on the WINDOWS virtual machine. From your UBUNTU machine console run a service to access SMTP: `telnet 172.16.y.7 25` Table 1 outlines the commands to use.	On the WINDOWS virtual machine, go into the C:\inetpub\mailroot\queue folder, and view the queued email message. Was the mail successfully queued? If not, which mail folder has the file in? Outline the format of the EML file?

Table 1: SMTP commands

```
220 napier Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959 ready at  Sun, 2 Dec 2009 21:56:01 +0000
help
214-This server supports the following commands:
214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY
helo me
250 napier Hello [172.16.75.1]
mail from: email@domain.com
250 2.1.0 email@domain.com....Sender OK
rcpt to: fred@mydomain.com
250 2.1.5 fred@mydomain.com
Data
354 Start mail input; end with <CRLF>.<CRLF>
From: Bob <bob@test.org>
To: Alice <alice@test.org >
```

```
Date: Sun, 20 Dec 2013
Subject: Test message
Hello Alice.
This is an email to say hello
.
250 2.6.0 <NAPIERMp7lzvxrMVHFb00000001@napier> Queued mail for delivery
```

F Enumeration – Host scan

Nmap is one of the most popular network scanning tools. It is widely available, for Windows and Linux/Unix platforms, and has both a Command Line Interface (CLI) and a Graphical User Interface (GUI).

From → To	Command	Observation
LAN to WAN	**`sudo nmap –sP –r 10.200.0.0/24`**	Which hosts are on-line:
LAN to DMZ	**`sudo nmap –sP –r 172.16.y.0/24`**	Which hosts are on-line:
DMZ to LAN	**`nmap –sP –r 172.16.x.0/24`**	Which hosts are on-line:
LAN to DMZ	Run Wireshark on host in LAN, and run: **`sudo nmap –sP –r 172.16.y.0/24`**	Which transport layer protocol does NMAP use to discover the host: [ICMP] or [ARP]
LAN to LAN	Run Wireshark on host in LAN, and run: **`sudo nmap –sP –r 172.16.x.0/24`**	Which transport layer protocol does NMAP use to discover the host: [ICMP] or [ARP]