Lab 3: Creating Secure Architectures

A Challenge

Our challenge is to setup **MyBank Incorp**, where each of you will be allocated a network and hosts to configure and get on-line (Figure 1). For this you will be allocated your own network (NET01, NET02, and so on) which you can access from the vSoC Cloud infrastructure (vsoc.napier.ac.uk). Table 1 outlines your challenges and how you might achieve them. You have a pfSense firewall, a Linux host, and a Windows host to achieve your objectives.

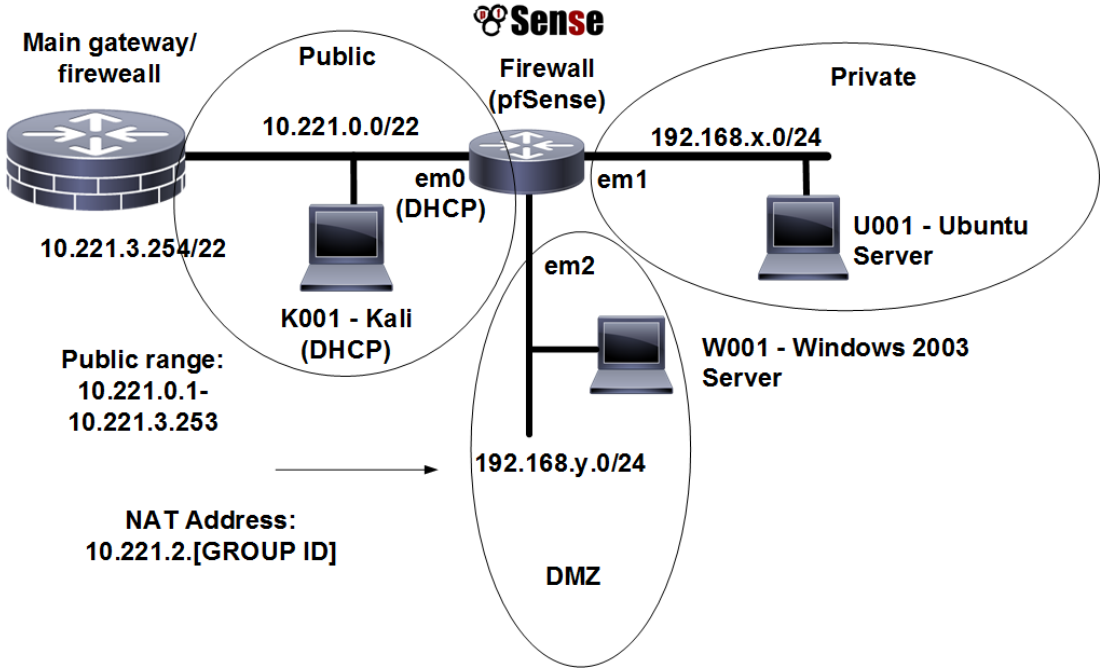

Figure 1: My Bank architecture

Table 1: Your challenges

Challenge	Description	How will I do this?	Completed
1	The hosts on your network can connect to each other. **Test:** Ping from the host in the Private network to the DMZ, and vice-versa.	Setup the IP addresses on the hosts to be on the same network as the gateway. The firewall address that the host connects to must be on the same network.	
2	You are able to connect to the Internet from a host in the Private network. **Test:** Open up Google.com from a browser from the host in the Private network	Get your network working, and make sure the domain name service is pointing to 10.221.3.254, and it should work. You may need to debug this. If you can connect to 8.8.8.8, but not the domain name, you have a DNS problem.	
3	A host on the DMZ is contactable from outside your network. **Test:** You either ask someone from another network to ping your host, or you ping from the Public port of the firewall, or you use the TEST network to ping.	You setup 1:1 NAT on the host in your DMZ, and map it to an address on the 10.221.0.0/24 network.	
4	You are able to discover the range of other firewalls which connect to the network. **Test:** You use NMAP to scan the 10.221.0.0/24 network, and discover the gateways.	You should run NMAP from one of the hosts in your network for the 10.221.0.0 network, and that it shows the nodes that are connected (host scan).	
5	You are able to perform a scan of the services on a host from another network from your private network. **Test:** You run NMAP on a server address on another network.	You should run NMAP to discover the services which are being run on the server in the DMZ on another network.	

A Setting up the network

In this lab we will connect multiple firewalls to the main gateway, and be able to complete the challenges in Table 1. You will be given two things:

Group Number: Your networks will be: 192.168.*x*.0/24 192.168.*y*.0/24 Demo: http://www.youtube.com/watch?v=d4a0bDhlyvI

First log into vSoC (vsoc.napier.ac.uk), and then select your network infrastructure. In this lab we will use **Allocation A**:

http://asecuritysite.com/csn09112/prep

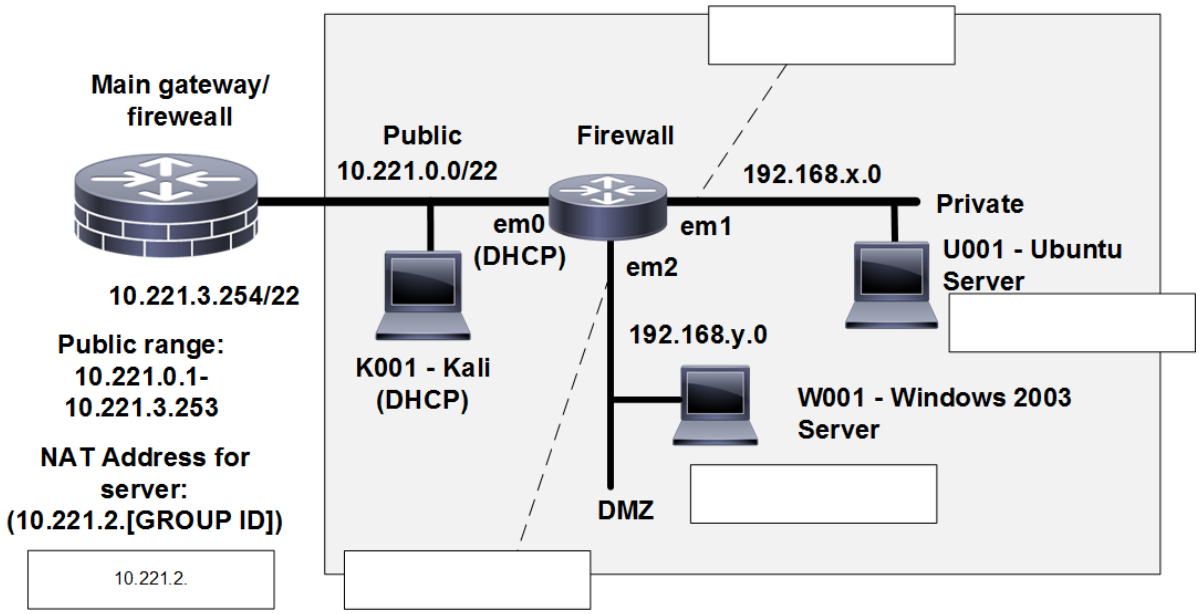

Figure 2: Lab setup

B Initial Firewall Creation

Now go to the **g** folder, and select the firewall for your network. Next configure the Linux server in the **Private zone**, and the Windows server in the **DMZ**.

☞ Boot your firewall, and say no to setting up VLANs. Now setup the first three networks adapters with em0 (WAN), em1 (LAN) and em2 (OPT1). ☞ Check that you have been granted an IP address on the WAN (em0) port. What address is it:

Can you ping the main gateway from the firewall (10.221.3.254) and your own WAN port?

Yes/No

Now we want to setup your private network gateway.

☞ Select the (2) option to change the IP addresses on the interfaces. Setup the IP address for the em1 interface to 192.168.*x*.254/24.

☞ Note the URL that you can configure your firewall. What is the URL:

That's it! You are all finished in doing the initial configuration on the firewall. We will now go ahead and configure the hosts and gain access to the firewall from a Web browser.

C Host setup

Now we will configure the hosts to sit on the Private and DMZ zones.

☞ Setup the Linux host to connect to 192.168.*x*.7/24 with a default gateway of your firewall port (192.168.*x*.254/24).

```
sudo ifconfig ethx 192.168.x.7 netmask 255.255.255.0 up
sudo route add default gw 192.168.x.254
```

☞ Next setup the nameserver on the Linux host by editing the /etc/resolv.config and adding a nameserver:

```
sudo nano /etc/resolv.conf
```

then add:

```
nameserver 10.221.3.254
nameserver 8.8.8.8
```

On the Windows server modify the static address on the interface with:

IP: 192.168.*y*.7
Subnet mask: 255.255.255.0
Gateway: 192.168.*y*.254
DNS: 10.221.3.254

Now we will finalise the configuration of the firewall:

Log into the firewall from the Linux host on the Private zone with:

http://192.168.*x*.254

Username: admin, Password: pfsense

Setup the required IP on the DMZ (192.168.*y*.254) and subnet mask.

On the firewall, from Diagnostics, view the ARP cache. Which addresses are in the cache:

On the firewall, from Diagnostics, ping each of the 192.168.*x*.254 and 192.168.x.7 interfaces from the LAN network. Can you ping them? Yes/No

On the Windows host, ping 192.168.*y*.254 and 192.168.*y*.7 interfaces. Can you ping them? Yes/No Why can't you ping the 192.168.y.254 interface?

On the firewall, create a rule which allows a host on the DMZ to use ICMP to any destination.

On the Windows host, ping 192.168.*y*.254 and 192.168.*y*.7 interfaces. You should now be able to ping them.

On the Windows host, ping 192.168.*x*.254 and 192.168.*x*.7 interfaces. You should now be able to ping them.

On the firewall, create a rule which allows the Public network to ping both the DMZ and Private network. From the firewall, can you ping the hosts in the DMZ and Private network from the WAN port.

Now from the Windows host and the Linux host, ping all the key addresses, including the gateway 10.221.3.254 and 10.200.0.2.

Now we will investigate NAT on the device.

Run packet capture on the firewall, and then ping from both the Windows host and the Linux host. Stop the trace.

Which IP address appears in the pings?

Why is it just a single address?

Now we will investigate the routing table on the firewall.

On the firewall, investigate the firewall, and identify how the device makes decisions on the routing of data packets. What is the default gateway?

D Device Audit

Now we will make sure everything is in order with our infrastructure, such as for testing for network traffic, MAC addresses and so on. Audit list:

On the firewall, capture traffic on the DMZ port, and generate some traffic from the LAN to the DMZ (such as accessing the Web server in the DMZ).
Does the traffic have the IP address of the gateway on the LAN port? Tick [ ]

On the firewall, capture traffic on the WAN port, and generate some traffic from the LAN and DMZ (such as accessing Google.com).
Does the traffic have the IP address of the WAN port? Tick [ ]

On the firewall, examine the ARP table. Also on the hosts in the DMZ and the LAN, run arp –a, and determine all your MAC addresses.
Do all the MAC addresses tie-up? Tick [ ]

E NMAP

Run Wireshark on both hosts. Now run NMAP from the Linux host to the Windows host, and from the Windows host to the Linux host.

What IP addresses are used in the source addresses of the scan?

Which services have been identified from the Linux host to the Windows host?

Which services have been identified from the Windows host to the Linux host?

Why are these different in their scope? Where is the blocking happening?

Now enable http, https, and ftp from the Private network to the DMZ.

Now enable https, https, and ftp from the DMZ to the Private network.

Re-do NMAP. How are the scans different?

Can you now access the Web server from the Linux host to the Windows host?

Can you now access the Web server from the Windows host to the Linux host?

Access Google.com from the Linux host.

Can you access it? If not, on the firewall, enable UDP/TCP DNS (Port 53) from DMZ and also from the Private network. Add logging on the rule.

Can you now access Google.com from the Linux host and the Windows host?

On the firewall, examine the log and view the accesses for a DNS lookup on Google.com. Which addresses are present?

F 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://192.168.x.7`	Is the service working: [Yes] [No]

LAN	From Ubuntu, access the Web server at: `http://192.168.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 192.168.y.7 80` then enter: `GET /`	Outline the message that is returned:
DMZ	Repeat the previous example from the WINDOWS host: `telnet 192.168.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 192.168.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 192.168.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 192.168.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 [192.168.75.1]
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
```

G 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 10.221.0.0/24`**	Which hosts are on-line:
LAN to DMZ	**`sudo nmap –sP –r 192.168.y.0/24`**	Which hosts are on-line:
DMZ to LAN	**`nmap –sP –r 192.168.x.0/24`**	Which hosts are on-line:
LAN to DMZ	Run Wireshark on host in LAN, and run: **`sudo nmap –sP –r 192.168.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 192.168.x.0/24`**	Which transport layer protocol does NMAP use to discover the host: [ICMP] or [ARP]

At the end of Part 1. You should have completed Challenge 1 and 2.

NAT and 1:1 mappings

No other group can access any of your hosts, as you are behind NAT. Now we need to setup a 1:1 mapping and a virtual IP address (with Proxy ARP) to map an internal address to an external one. First we need to find an IP address from the 10.221.0.0/22 network **which is not being used**, and then we will use this to allow other group's access to the hosts in the DMZ (Figure 3).

Demo: https://youtu.be/1wn2io8EWvs

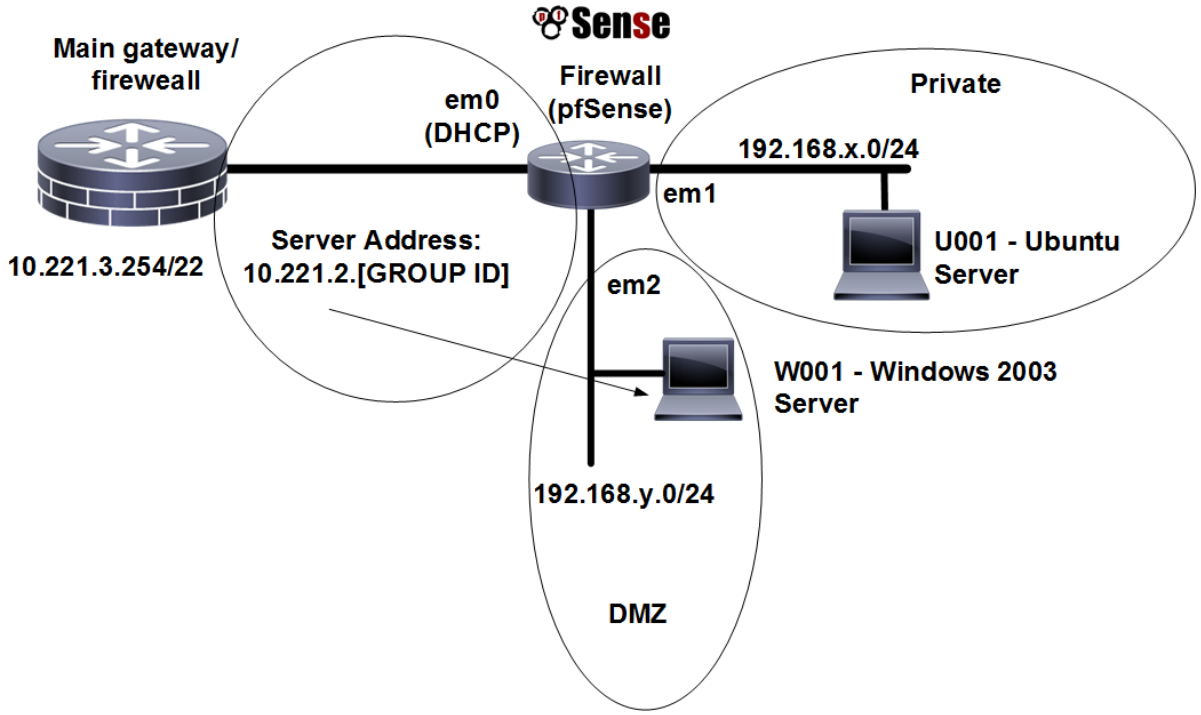

Figure 3: Setup 1:1 NAT for mapping of servers

Run NMAP from the Private network with:

Run NMAP from the Private network with: **nmap –sP 10.221.0.0/24**

Which hosts are on-line?

Now pick an address which is (where GROUP ID is your ID number):

10.221.2.[GROUP ID]

Now, on the firewall, setup a 1:1 mapping of the External IP address that you have selected and the Internal IP address on the DMZ (Figure 4).

Next, setup a Virtual IP address (with Proxy ARP) for the external address you have selected, which will advertise the IP address (Figure 5).

Now from the WAN interface, ping the host in the DMZ. Can you ping it?

Finally ask, someone in another group to ping your host in the DMZ. Can they ping it?

Now get them to access the Web server on your host.

Finally get them to NMAP your host? What can you observe from the NMAP?

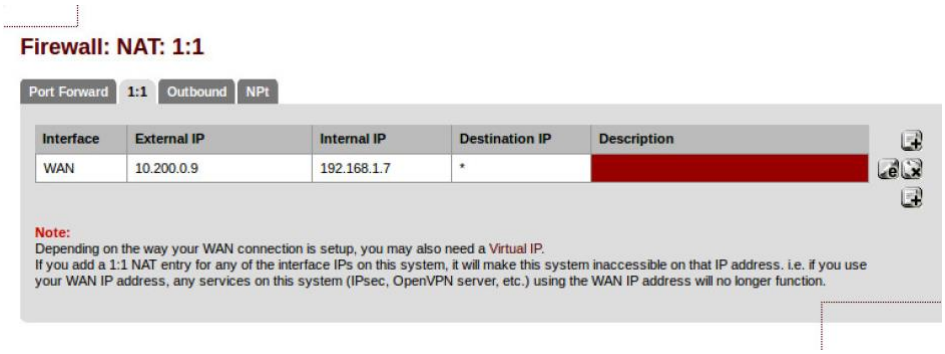

Figure 4: 1:1 NAT settings

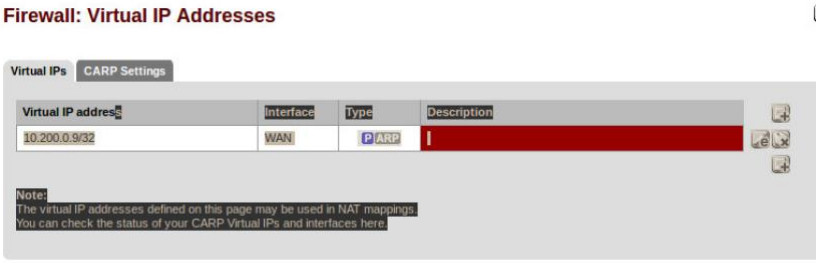

Figure 5: Virtual IP addresses

Connecting to another network

Now, wait for other teams to finish (or use the Test setup). You should have ready:

- A forward-facing Web and FTP site ready to connect from outside your network.

NMAP their server, and then make sure you can connect to the service. Now get them to block your specific source (just one address), and recheck that you cannot connect. Finally change your IP address, and re-do the NMAP, and make sure you can connect.

Please note some of the information related to their server. What information can you determine? Can you determine the MAC address of their server?

You should now have achieved challenges 3, 4 and 5.

Software Tutorial

Complete the software tutorial at:

`http://asecuritysite.com/csn09112/software02`

Appendix

User logins:

Ubuntu	User: napier, Password: napier123
Windows:	User: Administrator, Password: napier
Vyatta	User: vyatta, Password: vyatta
pfsense	User: admin, Password: pfsense