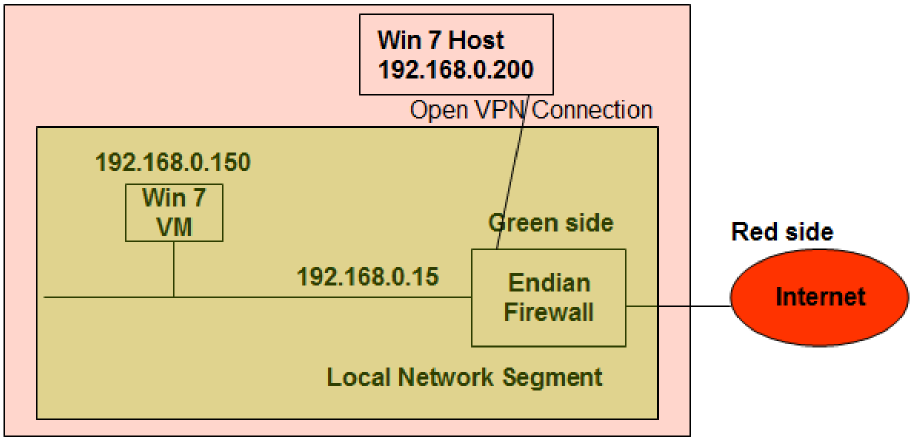
CSC 435 Computer Networks, Spring 2014
Instructor: Dr. Natarajan Meghanathan

Lab Project # 5: Endian Firewall: Creating a Virtual Network and Configuring VPN Connection to the Network

Due: April 16, 2014 **Max. Points:** 100

The objective of this project is to setup a local virtual network of a Windows 7 virtual machine obtaining its IP address (from an assigned range, using DHCP - Dynamic Host Configuration Protocol) from an Endian Firewall. We will then configure the Endian Firewall to allow VPN connections to this network from outside and assign IP addresses to those machines from a different range. We will VPN-in from the Windows 7 or any host machine on which you will do this project. We will test the successful establishment of the VPN connection through different ways that also include running simple datagram receiver and sender Java programs on the Win 7 VM and Win 7 host machines respectively.

The Endian Firewall has two interfaces: one interface on the green side wherein the above local virtual network comprising of the Win 7 VM exists and the other interface on the red side that is connected to the Internet through a wide area network connection. The Endian Firewall and the Win 7 VM run on a physical host that may also run Windows 7 or any other operating system, depending on the host you are working on. The whole setup is as shown below.



VM IP Address Range for DHCP

Name of Student	IP Address Range for DHCP (Machines in the Local Network)	IP Address Range for VPN Connected Machines
Aaron Barker	192.168.0.170 - 192.168.0.220	192.168.0.235 - 192.168.0.244
Tiffani Gardner	192.168.0.20 - 192.168.0.70	192.168.0.85 - 192.168.0.94
Gregory Luckett	192.168.0.30 - 192.168.0.80	192.168.0.95 - 192.168.0.104
Cameron Taylor	192.168.0.40 - 192.168.0.90	192.168.0.105 - 192.168.0.109
Carlos Ware	192.168.0.50 - 192.168.0.100	192.168.0.115 - 192.168.0.119
Karrington Lewis	192.168.0.60 - 192.168.0.110	192.168.0.125 - 192.168.0.129
Rashad Evans	192.168.0.70 - 192.168.0.120	192.168.0.135 - 192.168.0.139
Deja Knight	192.168.0.80 - 192.168.0.130	192.168.0.145 - 192.168.0.149
Sarah Price	192.168.0.90 - 192.168.0.140	192.168.0.155 - 192.168.0.159
Alain-Daniel Wa-Baguma	192.168.0.110 - 192.168.0.160	192.168.0.175 - 192.168.0.179
Deandrea Whinsenton	192.168.0.120 - 192.168.0.170	192.168.0.135 - 192.168.0.139
Allison Gray	192.168.0.130 - 192.168.0.180	192.168.0.145 - 192.168.0.149

Installing VMWare Player

Download the latest version (v.5 or v.6) of VMware Player for your Operating System from https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/5_0

Installing Endian Firewall

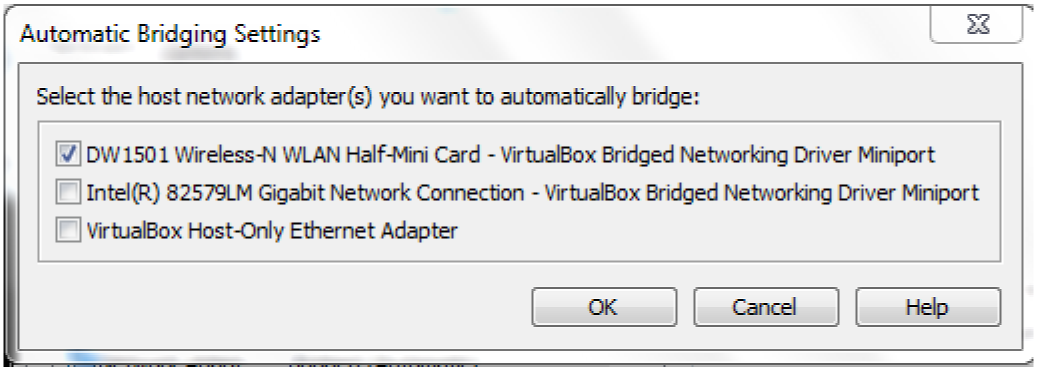
Download the Endian firewall iso file from http://www.endian.com/en/community/download/ and select the Download Now button to download Endian community firewall. The latest version is 3.0.

Open the VMware Player. Select "Create a New Virtual Machine". Select Installer disc image file (iso): browse for your Endian firewall .iso file and click **Next**

Choose Linux and other 2.6 Kernel. Give it a name Endian firewall. Set the hard disk size to 4 GB. Store the virtual disk as a single file.

Customize Hardware
Use 512 MB for memory.
We need two network adapters. For the network adapter that is already there, select the LAN segment --> create a LAN by clicking Add and then enter a name of your choice. In my case, I enter **meg-net**. Make sure the LAN segment you created is selected for the first network adapter.

Select the network adapter option, click Add and create a second network -adapter by selecting the bridged option. Make sure the Configure Adapters button is selected and the network card that you would use on the local host to connect to the Internet is selected. In my case I am using a laptop on wireless connection. So, I am selecting the wireless card for the Automatic Bridging settings.



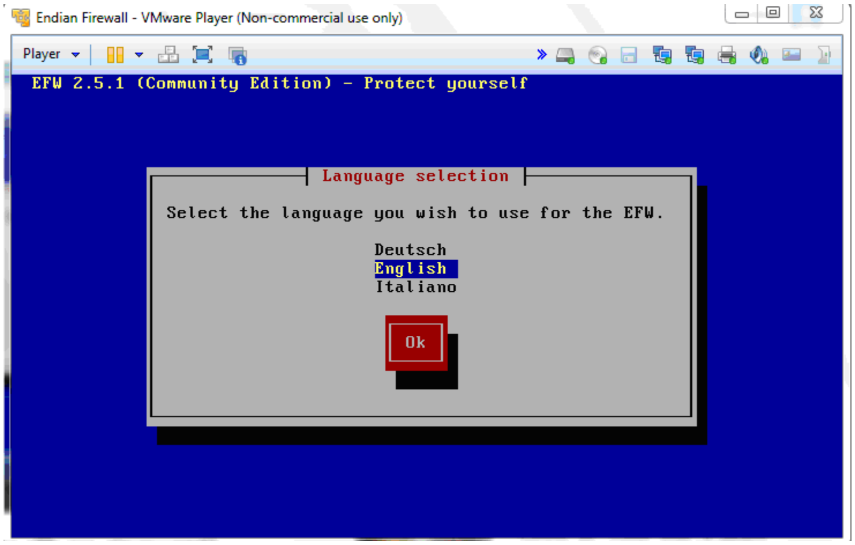
Automatic Bridging Settings

Select the host network adapter(s) you want to automatically bridge:

☑ DW1501 Wireless-N WLAN Half-Mini Card - VirtualBox Bridged Networking Driver Miniport
□ Intel(R) 82579LM Gigabit Network Connection - VirtualBox Bridged Networking Driver Miniport
□ VirtualBox Host-Only Ethernet Adapter

Complete the configuration of the Endian Firewall.

Next, on the VMPlayer main menu, select the Endian Firewall and Open the Virtual machine to play it. The installation of the Endian firewall will start. A blue screen with some text will appear as shown below.



EFW 2.5.1 (Community Edition) - Protect yourself

Language selection

Select the language you wish to use for the EFW.

Deutsch
English
Italiano

To navigate in the blue screen, you have to take your mouse pointer/ cursor inside the screen and click somewhere on the blue screen to make the mouse pointer get lost so that the control could be moved to select the options using the arrow keys and/or tab space.

Wait for a while for the **Install packages** and **Install pre-installed signatures** to complete

Do not worry about some messages appearing on the screen during the installation

Lets go ahead and accept the IP address and Network Mask that will display by selecting OK. In my case, it is 192.168.0.15 (IP address) and 255.255.255.0 (subnet mask)

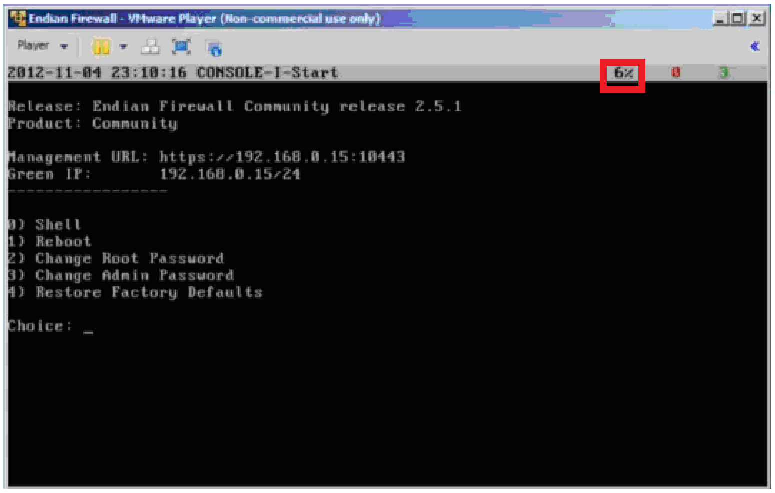
Wait for the post installation procedures to complete.

Do not worry about the error regarding CD ROM. Just select OK and proceed.

An **EFW is successfully installed** message will appear. Just remove if you have any floppy/CD ROM/ UDB drive inserted to the computer.

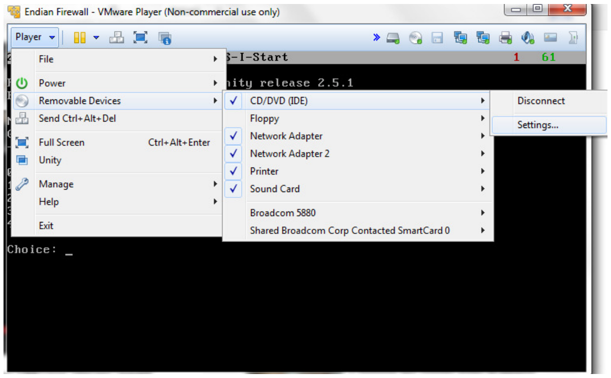
The firewall will shutdown and reboot. The firewall will reboot to a command shell. Wait for the first number on the top to increase from 1% to 100%.

The Firewall can be managed through a web interface that can be accessed through another machine (VM) on the local network (Green IP). As of now, the installation should look like this:

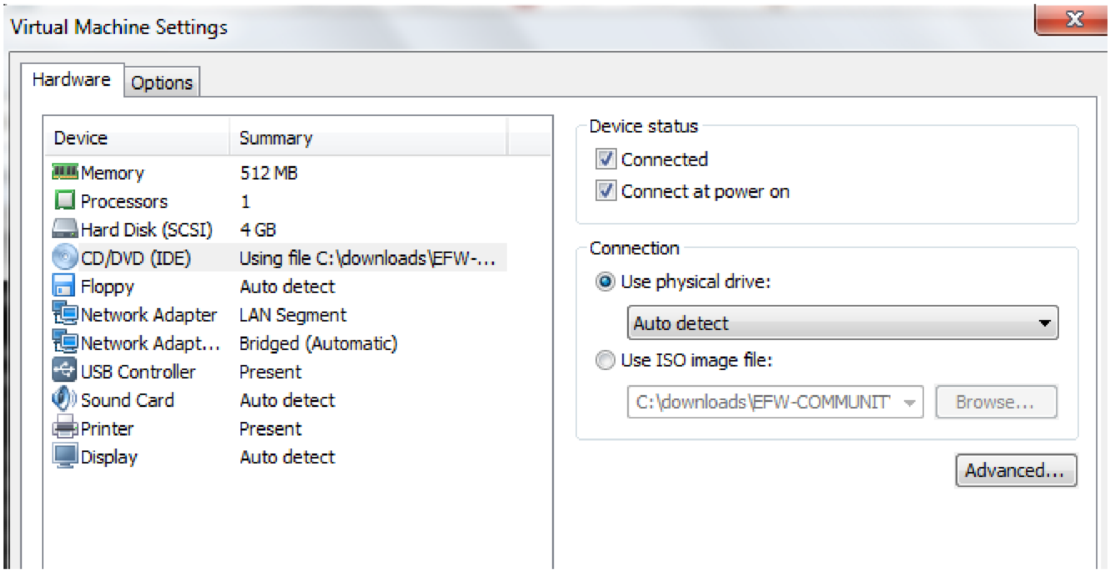


```
2012-11-04 23:10:16 CONSOLE-I-Start                              6%     0     3

Release: Endian Firewall Community release 2.5.1
Product: Community

Management URL: https://192.168.0.15:10443
Green IP:       192.168.0.15/24
-----------------

0) Shell
1) Reboot
2) Change Root Password
3) Change Admin Password
4) Restore Factory Defaults

Choice: _
```

Lets go to the VM Player settings for the Firewall. We no longer need to boot from the iso file and boot from the installation. For this, go to the Player menu on the top of the VMPlayer screen, select Removable Devices --> CD/DVD (IDE) --> Settings and then select Physical Drive (instead of Use ISO Image file)



```
S-I-Start                                   1     61
nity release 2.5.1
Choice: _
```



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	4 GB
CD/DVD (IDE)	Using file C:\downloads\EFW-...
Floppy	Auto detect
Network Adapter	LAN Segment
Network Adapt...	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Connection

● Use physical drive:

Auto detect

○ Use ISO image file:

C:\downloads\EFW-COMMUNIT

Installing Windows 7 Virtual Machine (Win 7 VM)

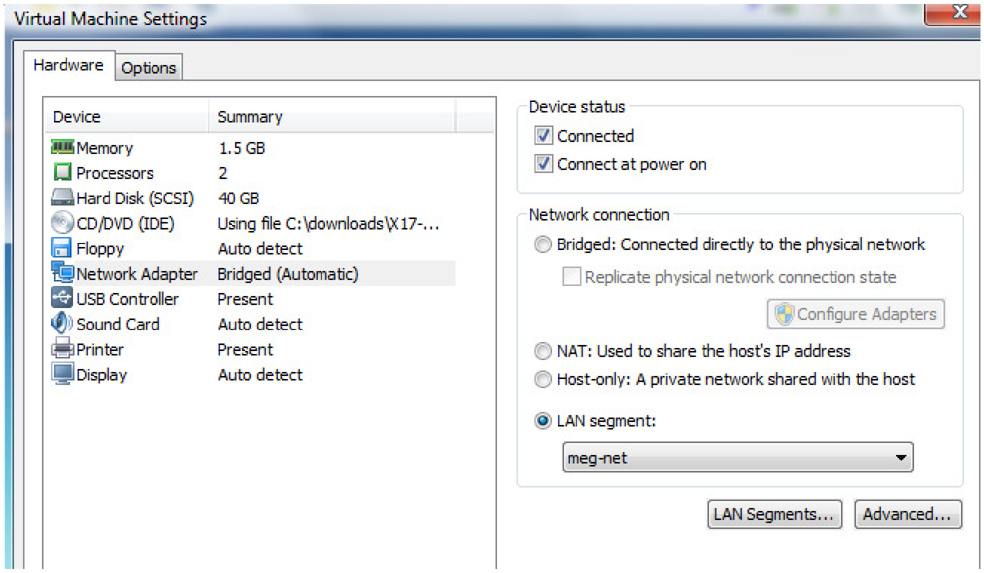
Use the ISO file for Windows 7 (x86) that can be downloaded from http://msft.digitalrivercontent.net/win/X17-59183.iso

Create a Win 7 VM running on VM Player. Follow the instructions below.

Use 40 GB to 60 GB for the disk size, depending on the space available.

Select Customize Hardware.
Use two processors (instead of default 1). Select Memory 1 GB or more, as you can afford.

Set the network adapter to the LAN segment option and Select --> Add the LAN segment name that you gave during the installation of the Endian firewall (in my case, it is meg-net).



Device	Summary
Memory	1.5 GB
Processors	2
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Using file C:\downloads\X17-...
Floppy	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status
☑ Connected
☑ 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
● LAN segment:
meg-net

Select the name of your Windows 7 machine from the VMPlayer main menu and start the Windows 7 machine by selecting the Play Machine option in the VM Player screen. Go through the installation process for Windows 7. You can skip the product key screen that may appear during the installation.

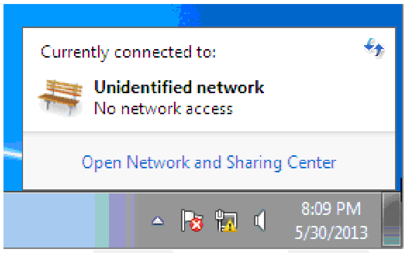
Give the Win 7 VM a name that represents your J# along with Win 7. For example, if your J# is J1234567, the name of the machine should be **J123456-Win7-PC**

Let the Windows 7 system restart. Setup a username, password and name for the VM.

Select the **work network** option.

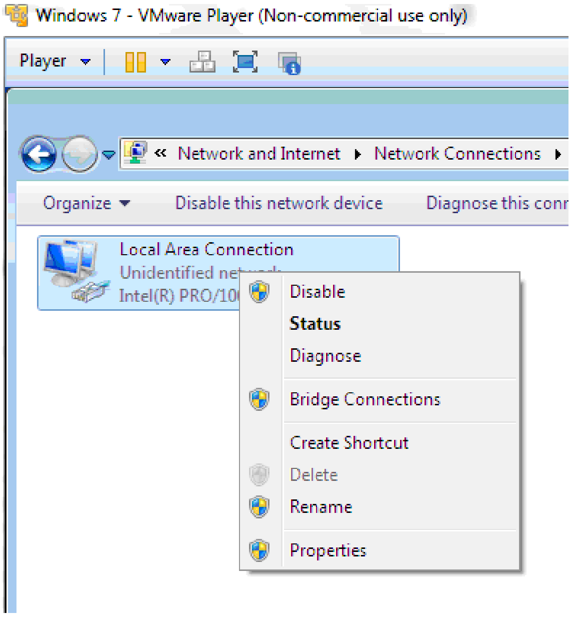
Make sure the LAN segment option is selected for the Network Adapter. You could do this by going to the Player menu on the top and select Settings.

Go to the Network and Sharing center and change the adapter settings. Right click on the Adapter. Select properties..



Currently connected to:

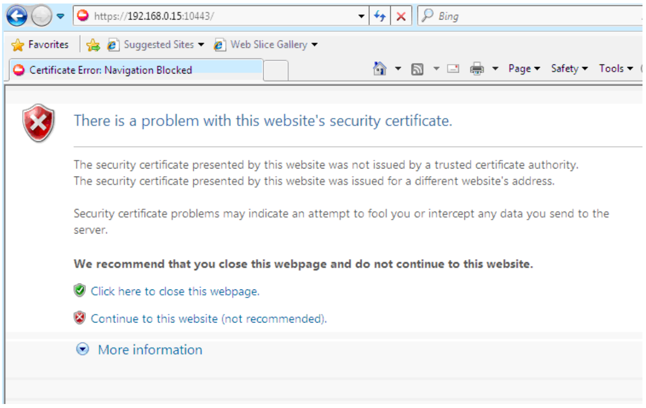
Unidentified network
No network access



Select IPv4 and select the Properties button.

We will statically set the IP address now. Give an IP address of 192.168.0.50. Set the gateway and DNS server address to the local network IP address of the Endian Firewall. The Subnet mask will be 255.255.255.0.

Open a web browser and enter the IP address and port number that appears on your Endian firewall command shell screen. In my case, I would use **https://192.168.0.15:10443**



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Click Continue to this website.

Welcome to Endian firewall screen will appear. Click the >>> button to proceed. Select English and Timezone (America/Chicago). Accept license. Leave it as **No** for backup and proceed. Create a password for admin and root. The admin account is to access the firewall through the web and the root account is to access the firewall through the command line option by logging using SSH. To keep it simple, just set the same password for both the accounts.

Let the Firewall pick the IP address for the WAN side (the Internet side) using DHCP to the DHCP server that the local host also contacts to pickup an IP address. So, select Ethernet (DHCP) option.

The Red interface is the interface facing the Internet and the Green interface is the interface facing the local network segment (in my case, meg-net) to which the Windows 7 VM is also connected to.

Do not worry about Step 2/8 about choosing network zones. Just have the None option selected and move on.

Step 3/8: For the Green side, just have everything as it is:

The IP address on the local network segment in my case is 192.168.0.15, same thing as it appears on the command screen for the firewall. The port 1 should be selected. Click >>> and move on.

Step 4/8: For the Red side, select port 2 and leave both the MTU, Spoof MAC address empty.

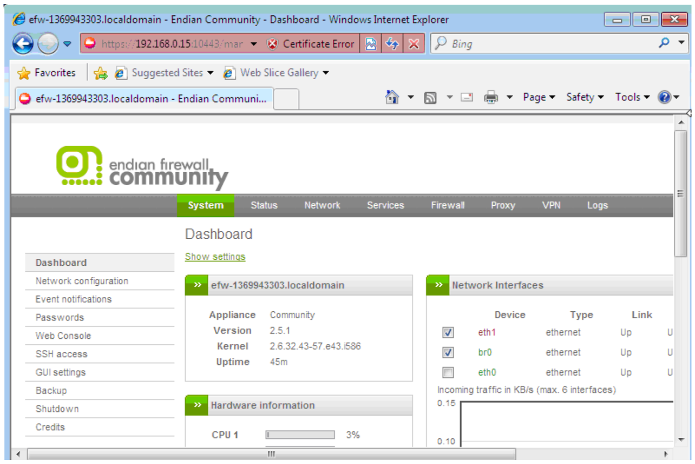
Have DNS be automatic as it is and move on.

Step 5/8 Configure DNS resolver. Just move on.
Step 6/8: Do not need to set any email addresses.

Step 7/8 : Apply configuration. Click OK, Apply configuration.

Step 8/8: End. Now, the firewall will reboot. You could see in the command shell that the firewall is booting up.

Login to the admin account using **admin** as username and the password that you setup during the configuration stage. You should get the welcome screen.



Dashboard

efw-1369943303.localdomain

Appliance Community
Version 2.5.1
Kernel 2.6.32.43-57.e43.i586
Uptime 45m

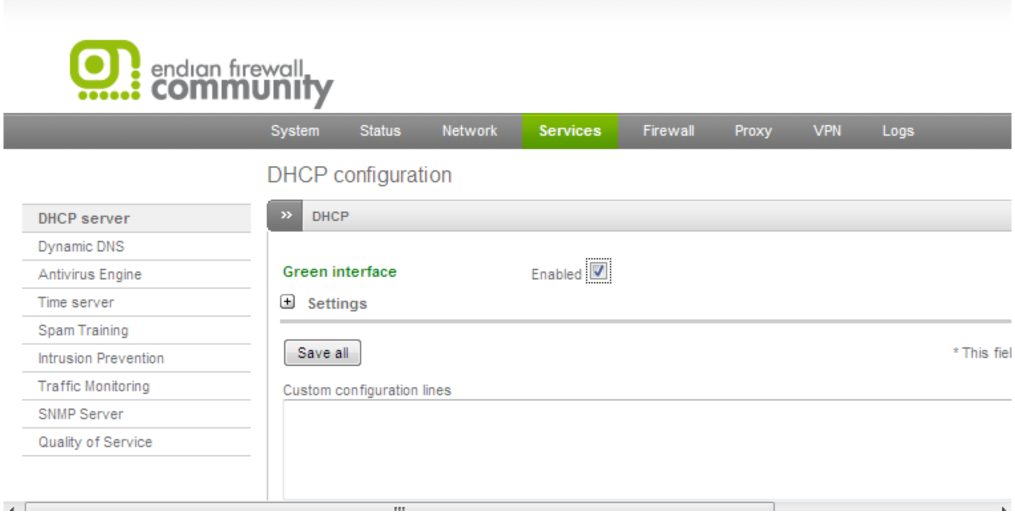
Hardware information

CPU 1 3%

Network Interfaces

	Device	Type	Link	
☑	eth1	ethernet	Up	U
☑	br0	ethernet	Up	U
□	eth0	ethernet	Up	U

Go to the Services menu on the top and select Enable DHCP. Open the Green side + option.



DHCP configuration

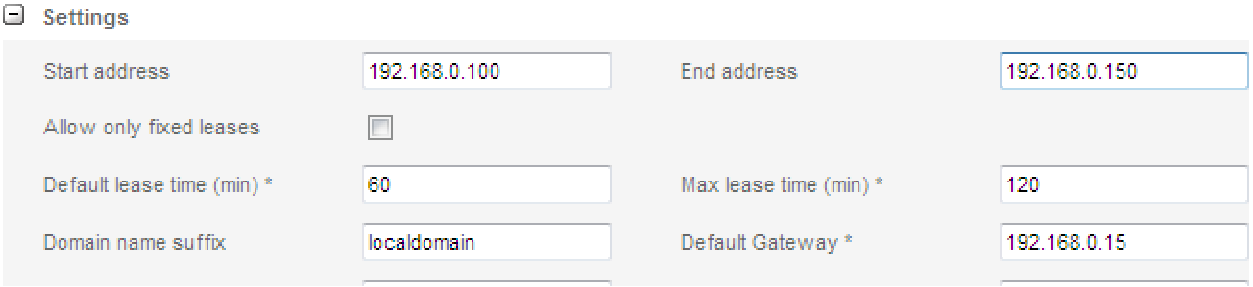
Green interface Enabled ☑

⊞ Settings

* This fiel

Custom configuration lines

Set the start and end addresses (the range of IP addresses that you want for any machine to have when it attempts to lease an IP address from the firewall) to be something that is assigned to each of you. In my case, I have set 192.168.0.100 and 192.168.0.150 as the starting and ending addresses respectively throughout this project description. **Each of you should use the range that is assigned individually to you (given at the end of the project description).**

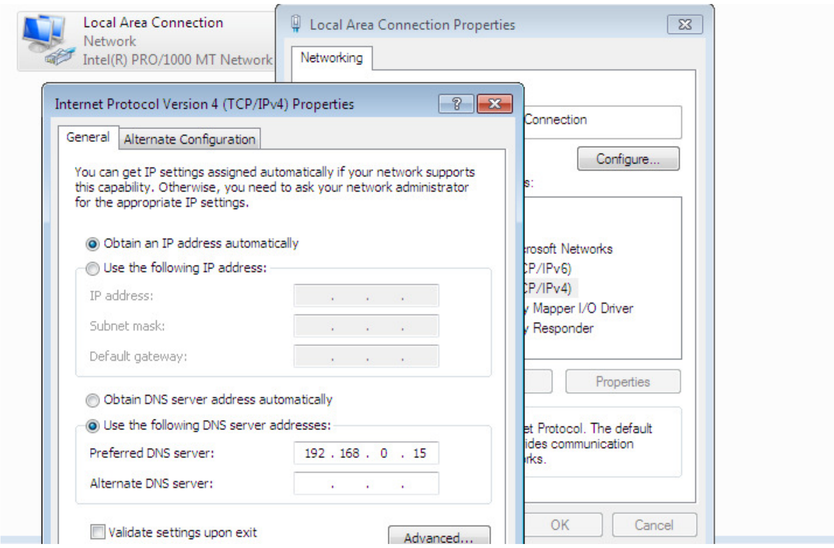


⊟ Settings

Start address	192.168.0.100	End address	192.168.0.150
Allow only fixed leases	□		
Default lease time (min) *	60	Max lease time (min) *	120
Domain name suffix	localdomain	Default Gateway *	192.168.0.15

Make sure the default gateway and DNS server IP addresses both are the IP address of your Endian firewall on the local network segment. In my case, it is 192.168.0.15. Make sure to click the **Save all** button.

Now, go the network adapter settings on your Windows 7 VM and change its properties in such a way that it automatically obtains an IP address from the Endian firewall using DHCP rather than using a static IP address.



Local Area Connection
Network
Intel(R) PRO/1000 MT Network

Local Area Connection Properties

Networking

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 15
Alternate DNS server: . . .

□ Validate settings upon exit

You can leave the preferred DNS server to be the IP address of the Endian firewall on the local network side (in my case, 192.168.0.15).

Now, trying to open a web browser and visit a website of your choice. If you are able to visit the website, then it means everything is working fine and you are able to go to the Internet from your local network through the Endian firewall.

Open a DOS window on your Windows 7 VM and type ipconfig to find the IP address of the interface that attaches the VM to the local network segment. Make sure the IP address that you see falls within the range of the leased IP addresses that you had setup for the firewall.

Also, go to the Services menu on the firewall, and you can see that the IP address of your Windows 7 VM is listed among the currently leased dynamic IP addresses.

Creating an OpenVPN Connection to the Local Network through the Endian Firewall

Go the Web Configuration interface of the Endian Firewall that you have opened on the Win 7 VM. Click on the Open VPN tab (On the left side you can see that we are in the OpenVPN Server screen - we will first do some settings on this screen). We will setup VPN tunnel to our local network through the EFW. Lets say when someone does a VPN to our local network, they will get 192.168.0.200 - 192.168.0.220. Set these values to be the values for the dynamic IP pool start and end addresses. Also select the **Open VPN Server enabled** checkbox. (Just Check: Go to the Services Tab and make sure the VPN IP address range does not overlap with the pool of DHCP addresses we are handing out to machines directly attached to the local network).

Go back to VPN. We will now enable the VPN Server - Save and restart.

Now, we need to create an account. Go to Accounts tab --> Add Account --> Username: testJ4567 where J4567 should correspond in your case to the last 4 digits for your J#. Password: of your choice (more than 5 characters).
We do not need to have setup anything else. This should be fine. We will go and Save the current settings.

For the settings to take effect, restart the VPN server.

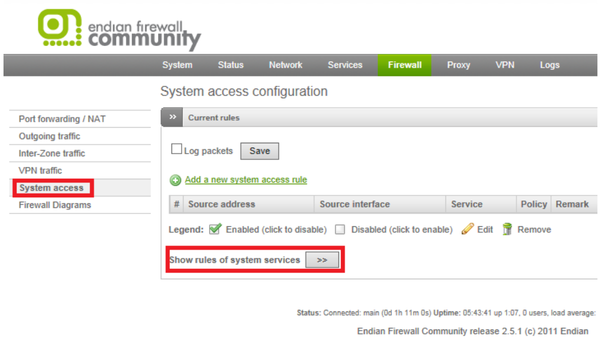
For a user to connect to the local network, they need the CA certificate. Download the certificate and save to the desktop.

Go to the Advanced tab. We will note the port (1194) and the protocol (UDP) that we will be connecting on. Everything else in the Advance tab can stay as it is.

We will need to test the VPN access from a machine that has OpenVPNClient. We will test the connection by trying to VPN tunnel from our Win 7 host machine (you could also try from the Internet if you are operating on a public network) to our internal network through the EFW and see if we can obtain an IP address from the VPN range that we have configured for (in my case, 192.168.0.200 to 192.168.0.220).

Go to Firewall tab in the Web configuration interface for the EFW in the Win 7 VM.

Click on the System access menu on the left-side menu options for the firewall. Now, on the screen that appears, click the Show rules of system services >> button, you can see the rules for all the services that are running on the firewall.



System access configuration

□ Log packets

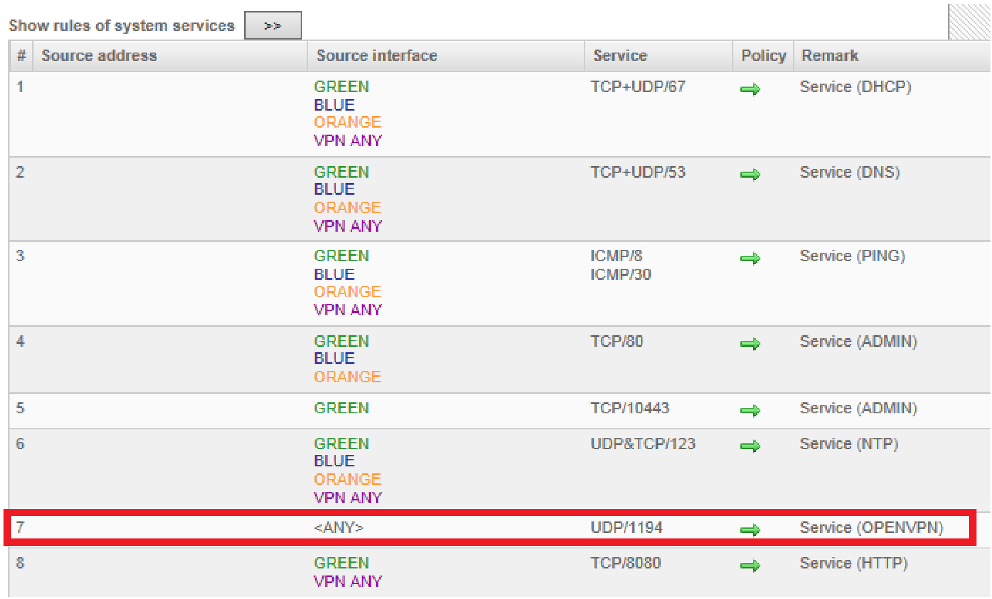
#	Source address	Source interface	Service	Policy	Remark

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) Edit Remove

Status: Connected: main (0d 1h 11m 0s) Uptime: 05:43:41 up 1:07, 0 users, load average:

Endian Firewall Community release 2.5.1 (c) 2011 Endian

You can see one of the services should be OpenVPN on port 1194.



#	Source address	Source interface	Service	Policy	Remark
1		GREEN BLUE ORANGE VPN ANY	TCP+UDP/67	⇨	Service (DHCP)
2		GREEN BLUE ORANGE VPN ANY	TCP+UDP/53	⇨	Service (DNS)
3		GREEN BLUE ORANGE VPN ANY	ICMP/8 ICMP/30	⇨	Service (PING)
4		GREEN BLUE ORANGE	TCP/80	⇨	Service (ADMIN)
5		GREEN	TCP/10443	⇨	Service (ADMIN)
6		GREEN BLUE ORANGE VPN ANY	UDP&TCP/123	⇨	Service (NTP)
7		<ANY>	UDP/1194	⇨	Service (OPENVPN)
8		GREEN VPN ANY	TCP/8080	⇨	Service (HTTP)

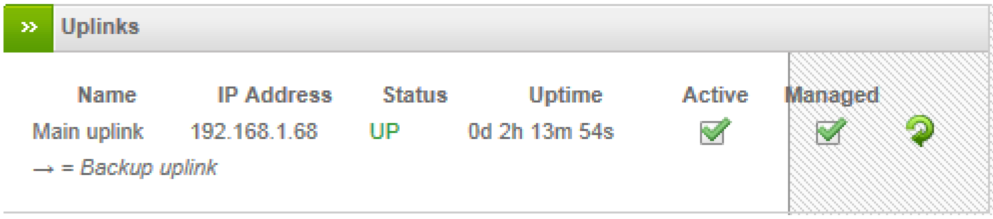
on the Win 7 host machine, go www.openvpn.net. Click on VPN Solution. Go to Downloads --> Community Downloads --> Download the Windows installer OpenVPN 2.2.2 (this is a better one and is a stable release, even though there may be more recent versions in their website). Go through the installation process. Once installed, it will run in the System tray or you can initiate it from the Start menu on the host machine.

We need to configure the OpenVPN client to connect to the OpenVPN Server. Go to the folder where OpenVPN is installed. In my Win 7 host machine, it is located at C:\Program Files (x86)\OpenVPN. Here, there is a sample-config folder, inside which you can find a sample.ovpn file, which you can open with a text editor (like notepad) and see its contents. In this sample.ovpn file, wherever there is a # sign, it is a new line. We can break into a different line at each of these #s.

Type the following contents to a text file (create the text file) and save it locally to a location in your Win 7 host machine and give it a name Virtual-EFW.ovpn (make sure the All Files option is opened for the file type, when you save this file name).

```
client
dev tap
proto udp
remote 192.168.1.68
resolv-retry infinite
nobind
persist-key
persist-tun
ca efw-1369943303.cer
auth-user-pass
comp-lzo
```

where 192.168.1.68 is the WAN-side IP address of the Endian Firewall - Red zone, facing to the Internet. To find this IP address, go to the Win 7 VM where you have opened the web configuration site for the Endian Firewall. Click the System tab on Web Configuration screen, and scroll all the way down. In the bottom right, you will see an **Uplink** section and there you can notice the IP address of the main uplink, which is the one facing the Internet. In my case, it is 192.168.1.68.



Uplinks

Name	IP Address	Status	Uptime	Active	Managed	
Main uplink	192.168.1.68	UP	0d 2h 13m 54s	✓	✓	↻

→ = *Backup uplink*

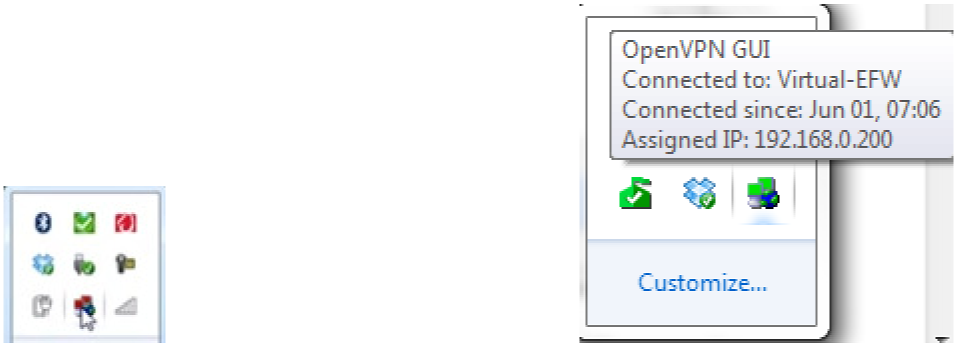
where efw-1369943303.cer is the name of the certificate file that you downloaded from the web configuration site of the Endian Firewall to your Win 7 VM. You need to email this file from the Win 7 VM to an email account that you can now login from your Win 7 host machine; download to a folder where you can locally save this certificate file on your Win 7 host machine. Then, on the Win 7 host machine, open My Computer and go to the folder C:\Program Files (x86)\OpenVPN\Config. Copy the above certificate file from the location where you previously saved it to the above Config folder. A confirmation message asking you whether you want to continue and save it with administrator privileges may show up; you click Continue and save the file.

You use the same approach to transfer the Virtual-EFW.ovpn file from wherever you saved it on the local computer to the C:\Program Files (x86)\OpenVPN\Config folder.

We will test if we can connect.

<u>Start Recording from now on and record all the steps:</u>

Right click on the OpenVPNClient icon from the System tray and click on Connect (if the Virtual-EFW.ovpn name shows up and select it). A **Connect** screen will appear and enter the username and password information to connect to the Endian firewall. If everything goes fine, you should be connected to the Endian firewall. Go back to the System tray and you will see the OpenVPNClient icon would have turned green. When you place your mouse cursor on the icon, you will see the IP address obtained as well as the date/time since the connection exists.



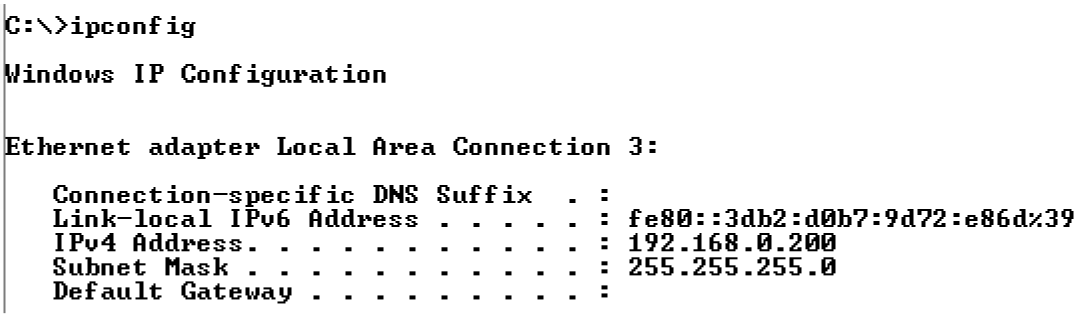
OpenVPN GUI
Connected to: Virtual-EFW
Connected since: Jun 01, 07:06
Assigned IP: 192.168.0.200

Before the VPN connection
(it will be red colored icon)

After the VPN connection is obtained
(it will be green colored, if connection is successful)

<u>Figure 1</u>

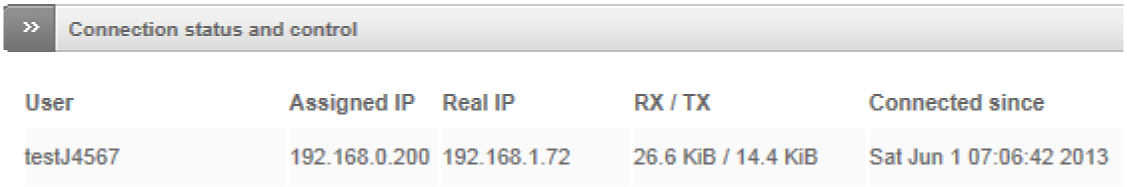
You can further confirm by opening a DOS command prompt on the Win 7 host machine and type ipconfig. You will see the IP address 192.168.0.200 (as in my case).



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3db2:d0b7:9d72:e86d%39
   IPv4 Address. . . . . . . . . . . : 192.168.0.200
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

<u>Figure 2</u>

You can also go the VPN tab in the Web Configuration interface of the Endian Firewall that you have opened on your Win 7 VM, and scroll all the way to the bottom to see that the testuser testJ4567 has connected through the firewall to the local network.



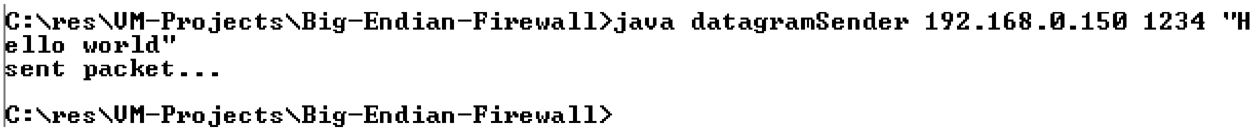
Connection status and control

User	Assigned IP	Real IP	RX / TX	Connected since
testJ4567	192.168.0.200	192.168.1.72	26.6 KiB / 14.4 KiB	Sat Jun 1 07:06:42 2013

Figure 3

Testing VPN Connection using Socket Program

As further testing of the connection, you can run the datagramReceiver in your Win 7 VM (provided Java is installed in it (if not installed; download and install Java SDK in the Win 7 VM and set the Java path) and the datagramSender in your Win 7 host machine that has now VPNed to the local network where the Win 7 VM exists. Make sure you allow access for the Win 7 VM to open a socket when you run the datagramReceiver program. You need to find out the IP address of the Win 7 VM using the ipconfig command (in my case, it is 192.168.0.150) and enter it as one of the parameters of the datagramSender program to connect to the former as shown below.



```
C:\res\VM-Projects\Big-Endian-Firewall>java datagramSender 192.168.0.150 1234 "H
ello world"
sent packet...

C:\res\VM-Projects\Big-Endian-Firewall>
```

Receiver Java Program (start it first, run it on the destination - Win 7 VM)

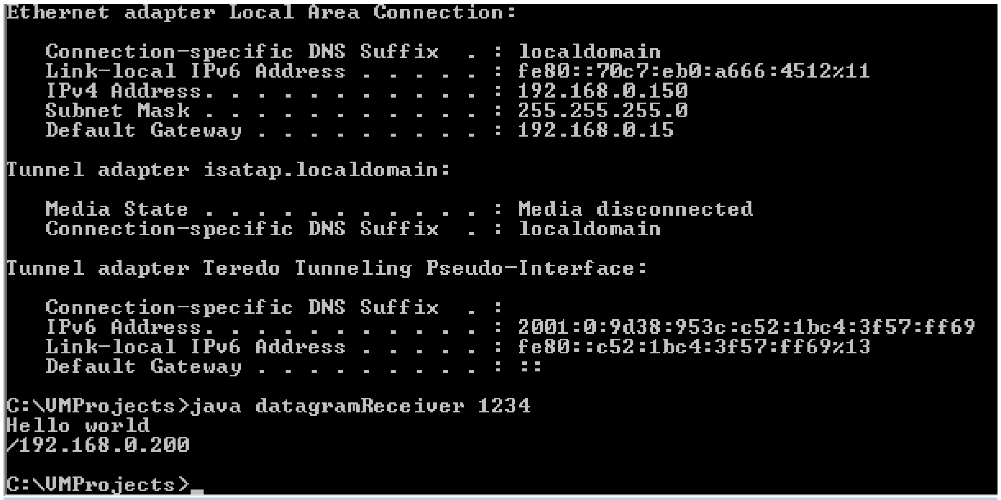
```
import java.net.*;
import java.io.*;

class datagramReceiver{
public static void main(String[] args){
 try{
  int MAX_LEN = 40;
  DatagramSocket mySocket = new DatagramSocket(Integer.parseInt(args[0]));
  byte[] buffer = new byte[MAX_LEN];
  DatagramPacket packet = new DatagramPacket(buffer, MAX_LEN);
  mySocket.receive(packet); // receiver is blocked here until it gets the message
  String message = new String(buffer);
  System.out.println(message);
  System.out.println(packet.getAddress( ));
  mySocket.close( );
 }
catch(Exception e){e.printStackTrace( );}
 }
}
```

Sender Java Program (start it later, run it on the source - Win 7 host)

```
import java.net.*;
import java.io.*;

class datagramSender{
 public static void main(String[] args){

  try{
    InetAddress receiverHost = InetAddress.getByName(args[0]);
```

```
   int receiverPort = Integer.parseInt(args[1]);
   String message = args[2];
   DatagramSocket mySocket = new DatagramSocket();
   byte[] buffer = message.getBytes();
   DatagramPacket packet = new DatagramPacket(buffer, buffer.length, receiverHost, receiverPort);
   mySocket.send(packet);
   mySocket.close();
   System.out.println("sent packet...");
  }
 catch(Exception e){e.printStackTrace();}
  }
 }
```

Collect a comprehensive screenshot that shows the IP address of the Win 7 VM along with the Hello World message received from the datagramSender program and the IP address of the sender machine (the Win 7 host machine) from which the message was received.



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::70c7:eb0:a666:4512%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.15

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:953c:c52:1bc4:3f57:ff69
   Link-local IPv6 Address . . . . . : fe80::c52:1bc4:3f57:ff69%13
   Default Gateway . . . . . . . . . : ::

C:\VMProjects>java datagramReceiver 1234
Hello world
/192.168.0.200

C:\VMProjects>_
```

Figure 4

Note: Shut down the firewall and the virtual machines after you have completed the project.

What to Submit:

Hardcopy

(1) A 250-words (or more) summary of what you did and understood from this project
(2) A network connection diagram (similar to the one in the first page), showing the connectivity and the IP addresses of the VMs and the VPN connection depending on the results you obtain.
(3) Screenshots of Figures 1 through 4 as indicated in bold and underlined in the previous pages of the project description.

Video Recording

Record the video (starting from Page 12) and show all the steps involved in testing the VPN connection and the execution results of the Socket programs.
Upload the video to Google Drive and share the link to natarajan.meghanathan@jsums.edu