



NETWORK SECURITY LAB SERIES

Lab 2: Configuring a Linux Based Firewall to Allow Incoming and Outgoing Traffic

Document Version: **2015-09-28**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction	3
Lab Topology.....	4
Lab Settings	5
1 Installing the Linux Firewall	6
1.1 Testing the Current Firewall and Installing the Linux Firewall	6
1.2 Conclusion	17
1.3 Discussion Questions.....	17
2 Configuring and Testing the Linux Based Firewall	18
2.1 Configuring the Firewall	18
2.2 Conclusion	29
2.3 Discussion Questions.....	29
3 Using Internal Services from an External Machine.....	30
3.1 Testing the Firewall	30
3.2 Conclusion	35
3.3 Discussion Questions.....	35
References	36



Introduction

This lab is a part of a series of lab exercises intended to support courseware for Network Security training. This lab includes the following tasks:

1. Testing the Current Firewall and Installing the Linux Firewall
2. Configuring and Testing the Linux Based Firewall
3. Using Internal Services from an External Machine

Key terms for this lab:

FTP –File Transfer Protocol, which uses port 20 and 21 and can be used to upload or download files from the command line or a browser, like Firefox.

HTTP - Hyper Text Transfer Protocol, which uses port 80 and is commonly used to download files from a website using browsers like Internet Explorer.

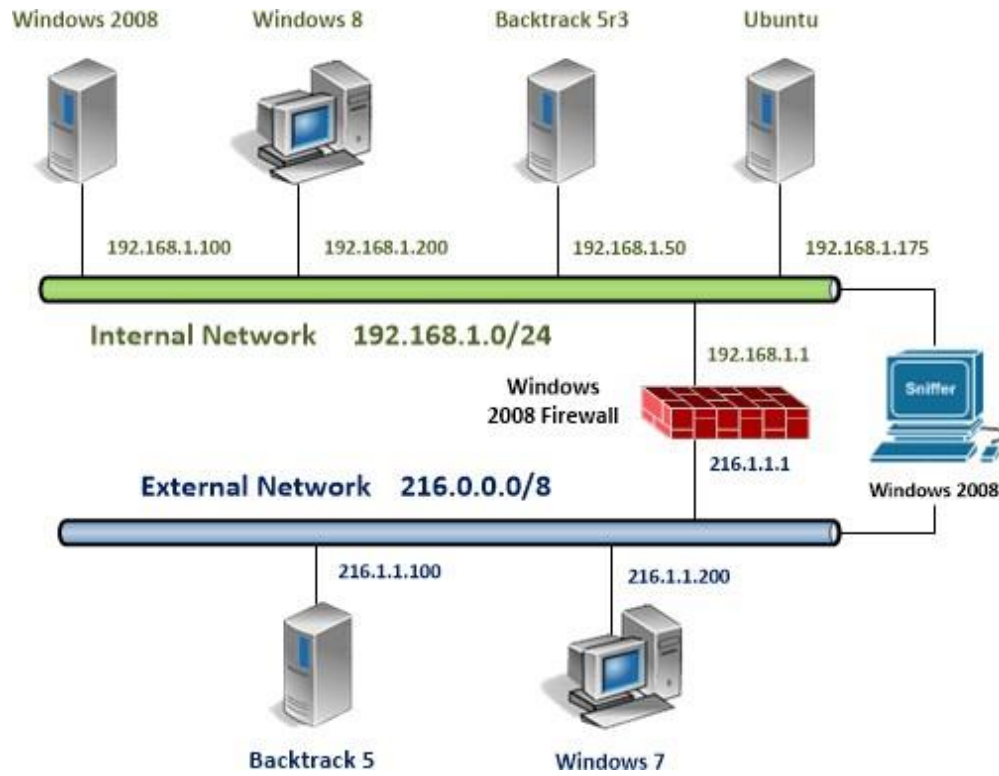
nmap – Nmap can be used in Linux, Mac, or Microsoft Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Nmap was used in the movie the Matrix.

PORT – There are 65,536 ports, numbered from 0-65,535. The first 1024 ports, ports 0-1023 are said to be well-known. They include ports like HTTP (Port 80) and FTP (Port 21).

SSH – Secure Shell uses port 22. SSH provides a much better option than TELNET for remote administration because traffic is encrypted. SSH is native to most Linux systems.



Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows 2008 Internal Machine	192.168.1.100	Administrator	P@ssw0rd
Windows 8 Internal Machine	192.168.1.200	Student	password
BackTrack 5 R3 Internal Machine	192.168.1.50	root	toor
Windows 7 External Machine	216.1.1.200	student	password
Windows 2008 Firewall	216.1.1.1 192.168.1.1	administrator	firewall

For all the tasks in this lab, you will be asked to open and return to various machines and applications within each machine. For some steps, this can get confusing.

To minimize confusion and the need to reopen machines and applications, it is suggested that you minimize, rather than close a machine before opening another.

At the end of the lab, remember to close all open windows and close the PC viewers.



1 Installing the Linux Firewall

In this section we, will examine the current Firewall configuration. Then, we will install a Linux firewall, which will be configured to match the settings of the Windows firewalls. We will be installing the Linux based firewall distribution called Endian Firewall, which is a Red Hat based distribution based on Red Hat Linux Enterprise.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Testing the Current Firewall and Installing the Linux Firewall

In order to configure, and set up the services required, perform the following steps on the **BackTrack 5 R3 Internal Machine**.

1. Click the **Backtrack 5r3** icon to open the **BackTrack 5 R3 Internal Machine**. Type **root** for the login and **toor** (*root spelled backwards*) for the password.

Click in the window and press Enter if BackTrack is displaying a black screen.

The password of toor will not be displayed when you type it, for security purposes.

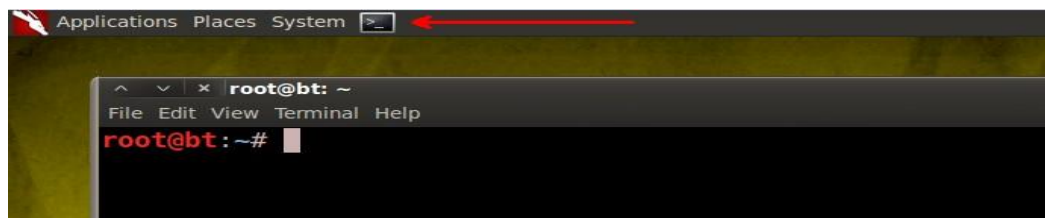
```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information disabled due to load higher than 1.0
root@bt:~# _
```

2. Type the following command to start the Graphical User Interface (GUI).
root@bt:~# **startx**

```
root@bt:~# startx _
```

3. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.



4. Type the following command to test for outbound connectivity.

```
root@bt:~# ping 216.1.1.200 -c 4
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ping 216.1.1.200 -c 4
PING 216.1.1.200 (216.1.1.200) 56(84) bytes of data.
64 bytes from 216.1.1.200: icmp_seq=1 ttl=128 time=0.854 ms
64 bytes from 216.1.1.200: icmp_seq=2 ttl=128 time=0.416 ms
64 bytes from 216.1.1.200: icmp_seq=3 ttl=128 time=0.404 ms
64 bytes from 216.1.1.200: icmp_seq=4 ttl=128 time=0.385 ms

--- 216.1.1.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.385/0.514/0.854/0.198 ms
root@bt:~#
```

The Windows based firewall is allowing outbound traffic. Network Address Translation (NAT) is set up, allowing this internal Linux machine with the IP address of 192.168.1.50 to communicate with the Windows 7 External Machine on the public network.

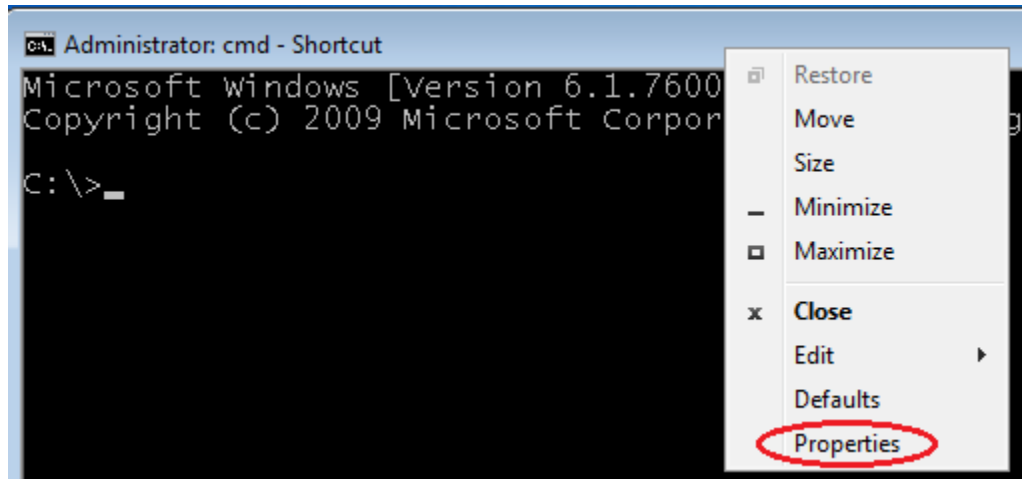
5. Log into the **Windows 7 External Machine** by clicking on the **Windows 7** icon on the topology. If required, enter the username, **student**. Type in the password, **password**, and press **Enter** to log in.



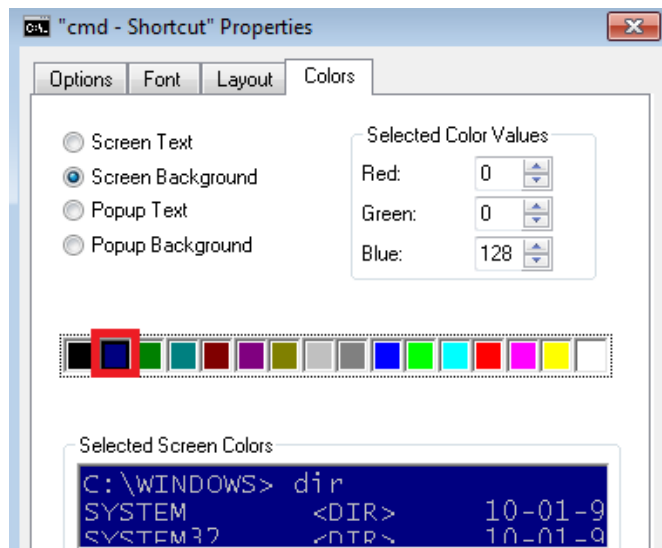
6. Open a command prompt by clicking on the **cmd-Shortcut** on the desktop.



7. Right-click on the blue bar at the top of command prompt and go to **Properties**.



8. Click the Colors tab. Select blue (2nd from the left) and click OK.



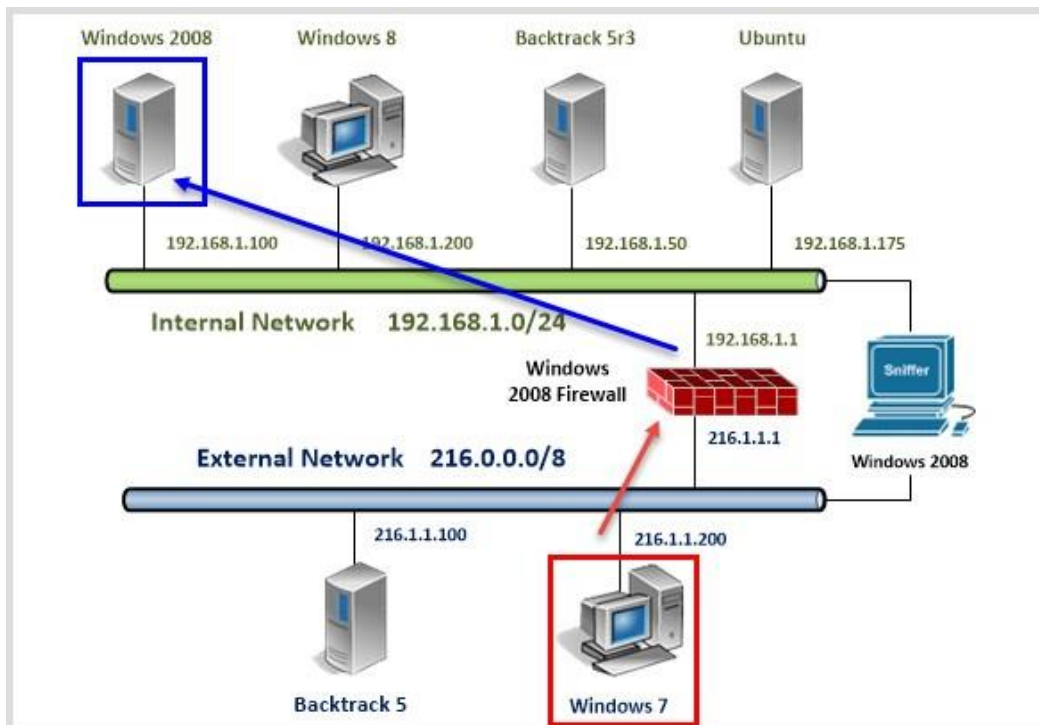
9. Type the following command to scan the internal Windows Server 2008 machine for open ports:

C:\>nmap 192.168.1.100

```
C:\>nmap 192.168.1.100
Starting Nmap 5.51 ( http://nmap.org
mass_dns: warning: Unable to determine
Try using --system-dns or specify va
Nmap scan report for 192.168.1.100
Host is up (0.00s latency).
Not shown: 974 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps1
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPs1
```

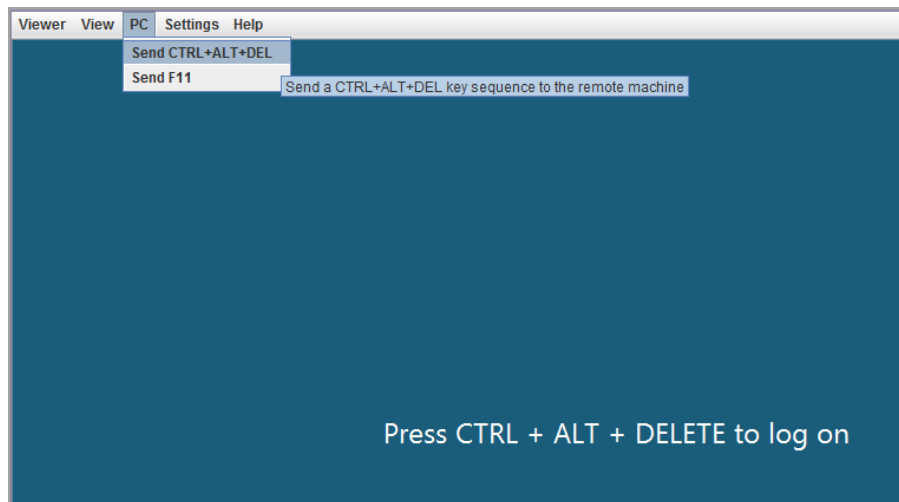
You may ignore the DNS warning message.

Currently, the firewall is configured to allow incoming requests to the Windows 2008 machine on the Internal Network.



We will now install and configure a Linux based firewall. We will configure it to allow all traffic outbound. We will also allow incoming traffic for FTP, Telnet, SMTP, HTTP and POP3, redirect to the Windows 2008 server located on the Internal Network (IP address of 192.168.1.100)

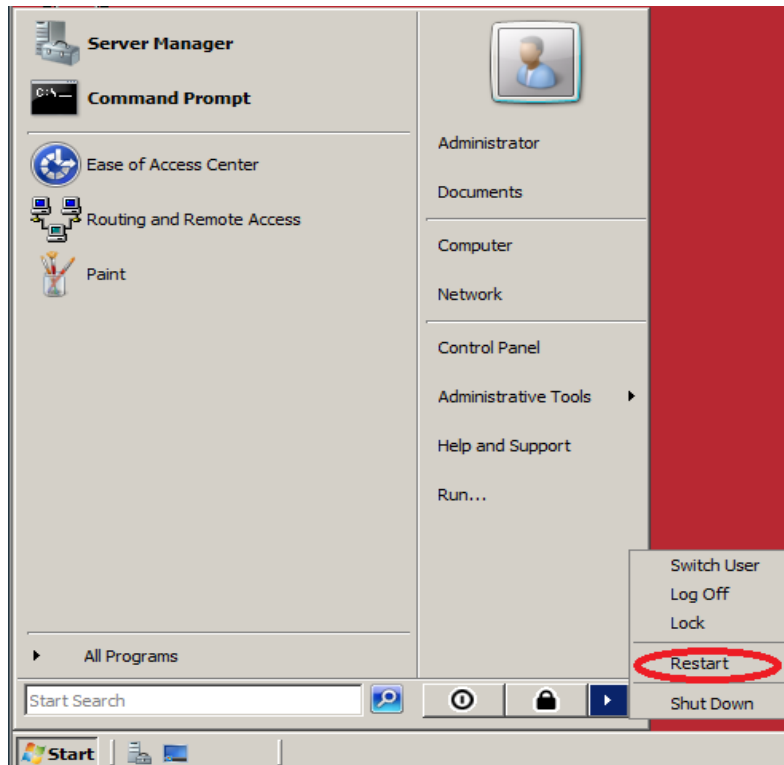
10. From the topology, click on the **Windows 2008 Firewall**. Click **PC**, and then **Send Ctrl+Alt+Del** in the top-left corner of the screen in order to log on to the Windows 2008 server.



11. Enter **firewall** for the Administrator password to the Windows 2008 Server.



12. Click on the Start button. Click the arrow to the far-right and select **Restart**.



13. Select the **Hardware: Maintenance (Planned)** option in the list from the drop-down box and click OK.



14. At the Linux boot prompt, type **install** and press **Enter**.

```
ISOLINUX 3.31 2006-09-25 Copyright (C) 1994-2005 H. Peter Anvin
In 30 seconds, this machine will boot to Windows 2008

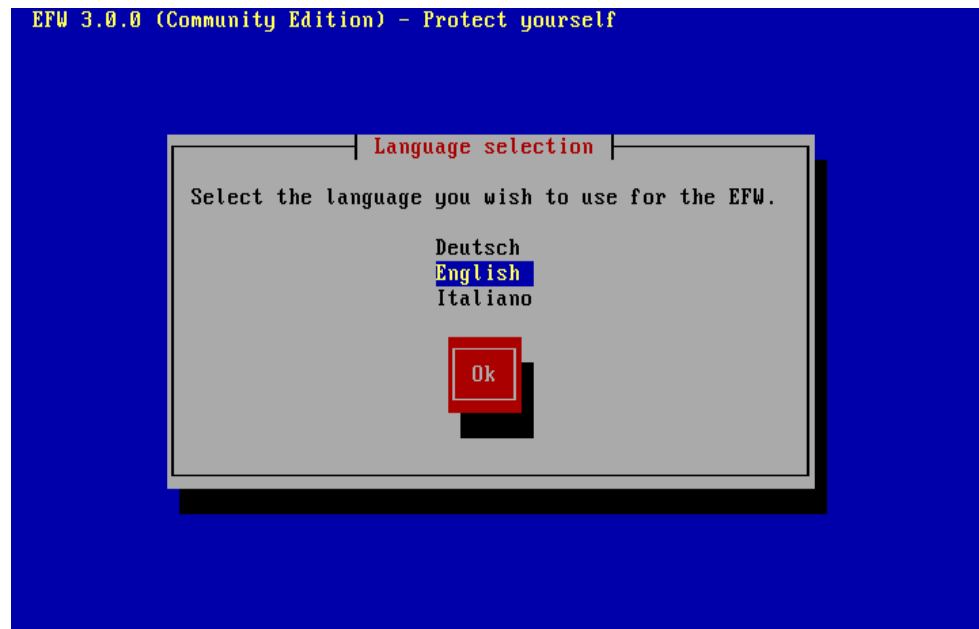
Welcome to Endian Firewall, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware of this before
continuing this installation.

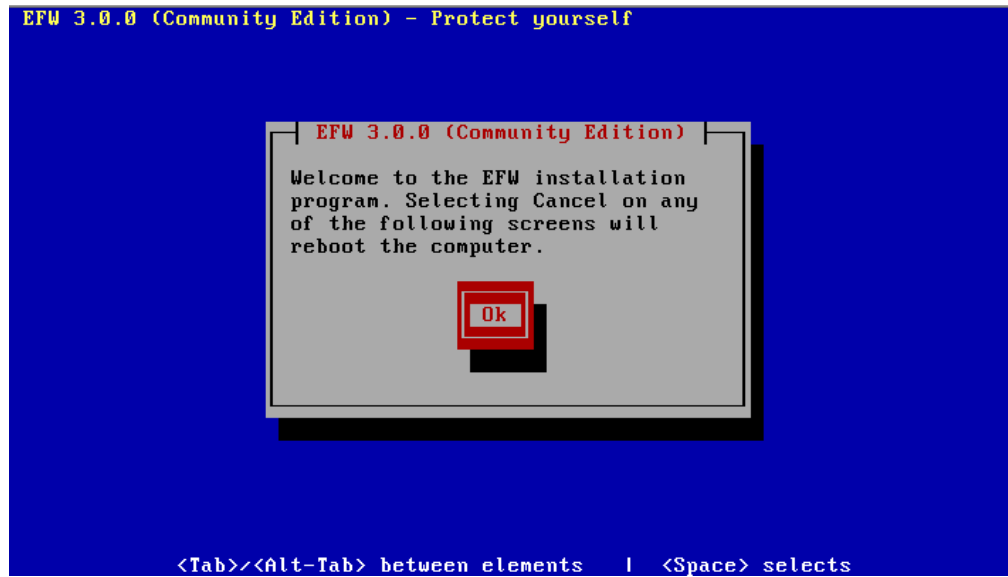
-----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
-----

Type: install to install
boot: install_
```

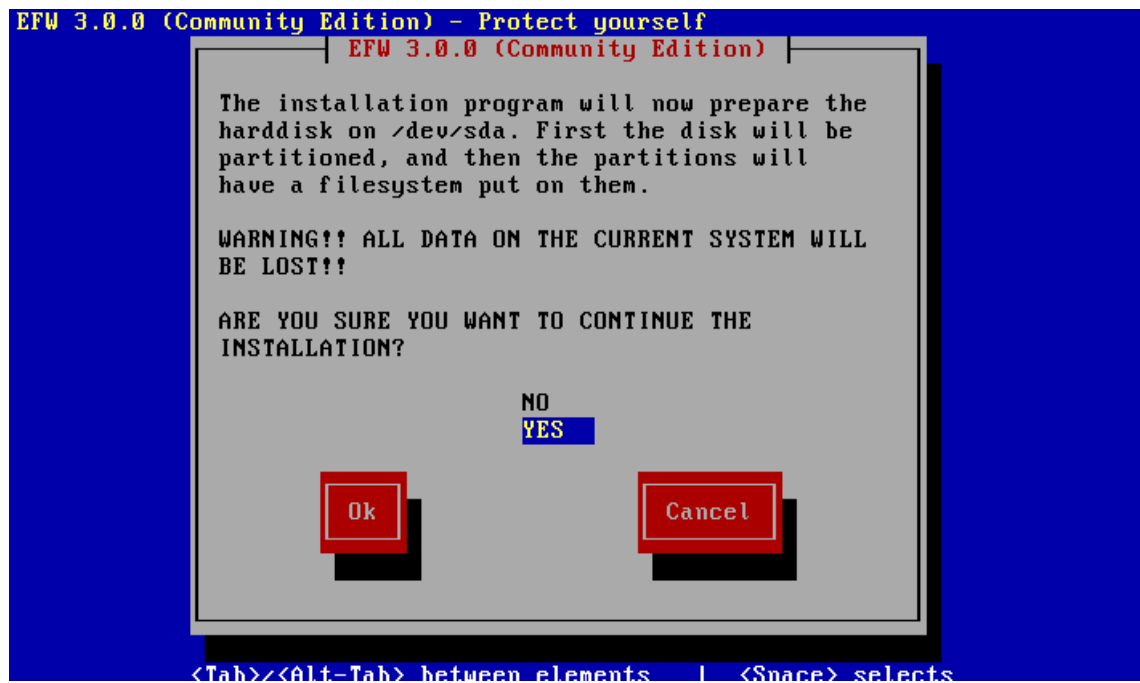
15. Press the Enter button to select **English** at the Language selection screen.



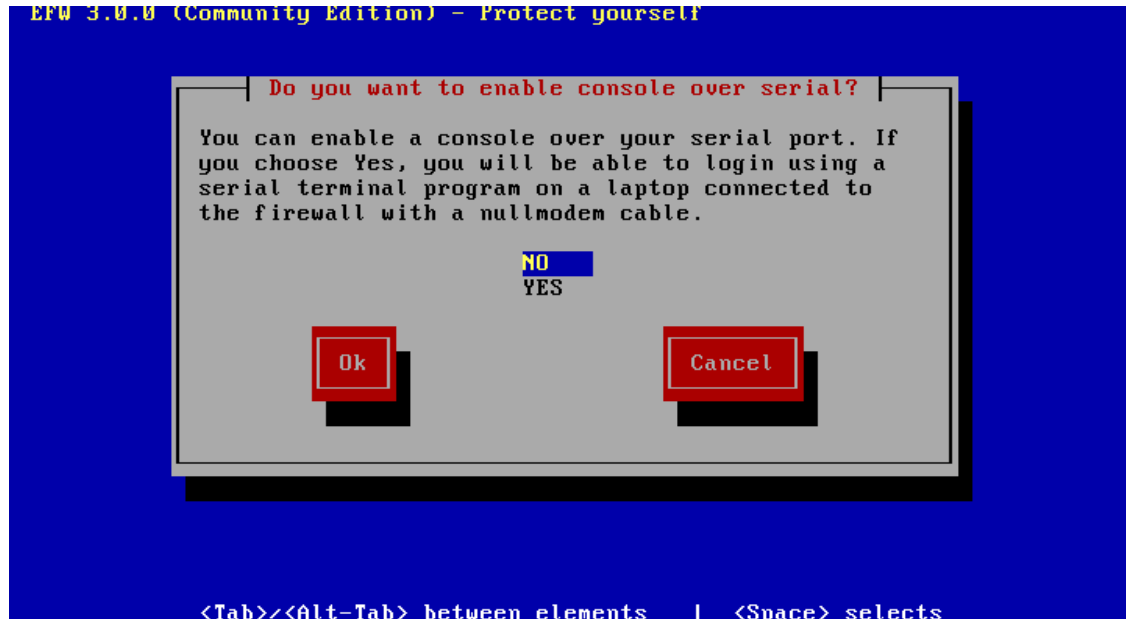
16. Press **Enter** at the Welcome to the EFW Installation program screen.



17. At the **Prepare the Hard Disk** screen, select **Yes** using the down arrow and then press the **Enter** button.

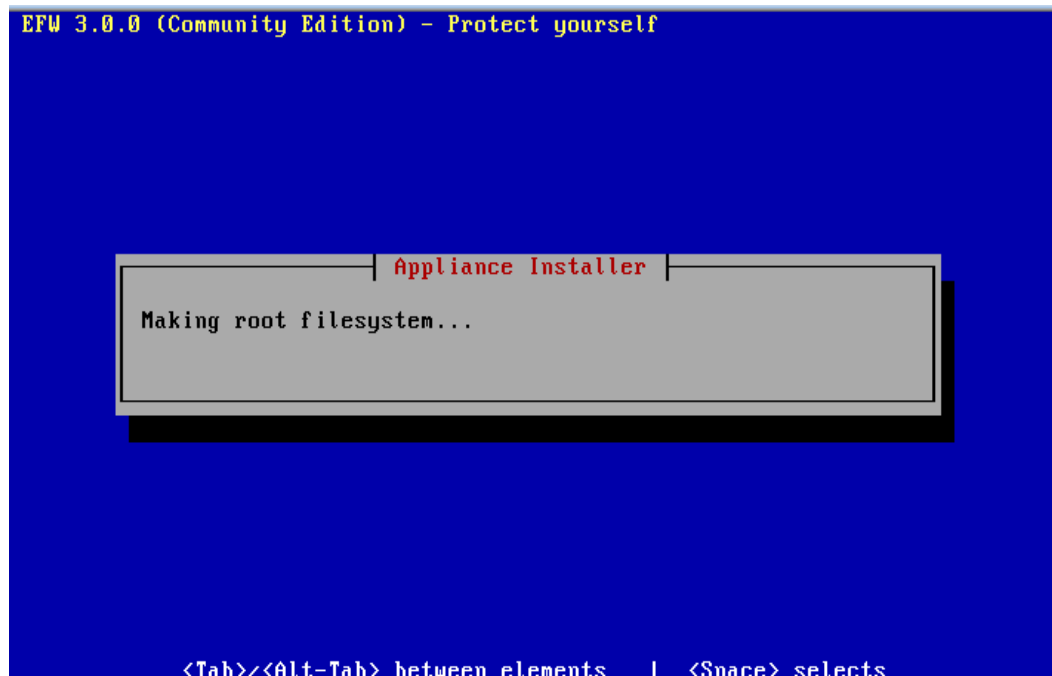


18. Press **Enter** to No Console Access over a serial port.

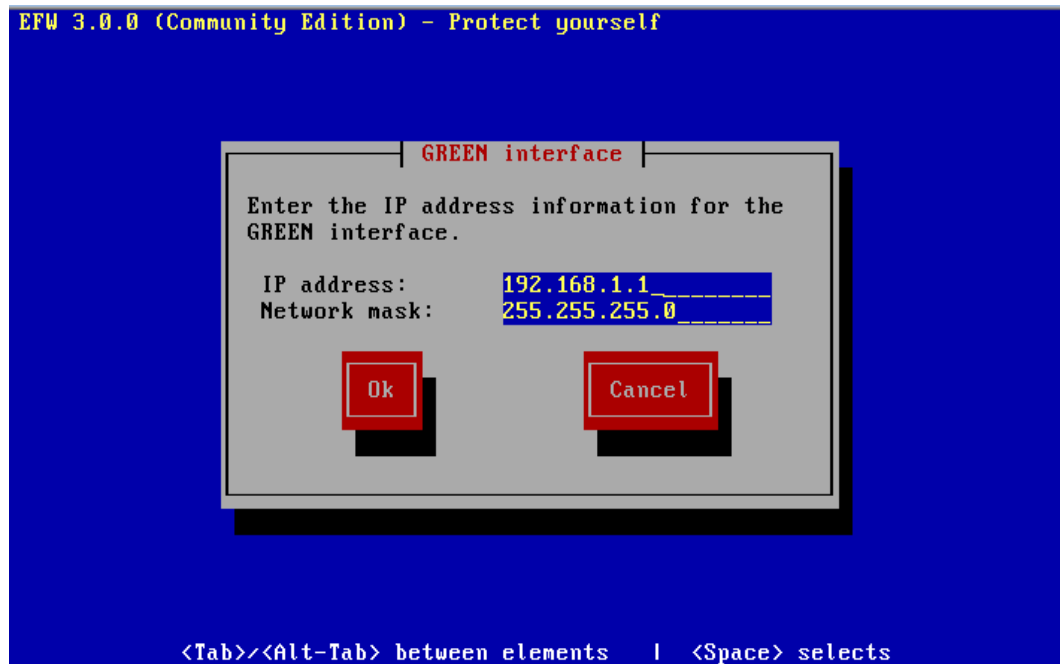


19. EFW will make the root file system and then will indicate that it is installing packages.

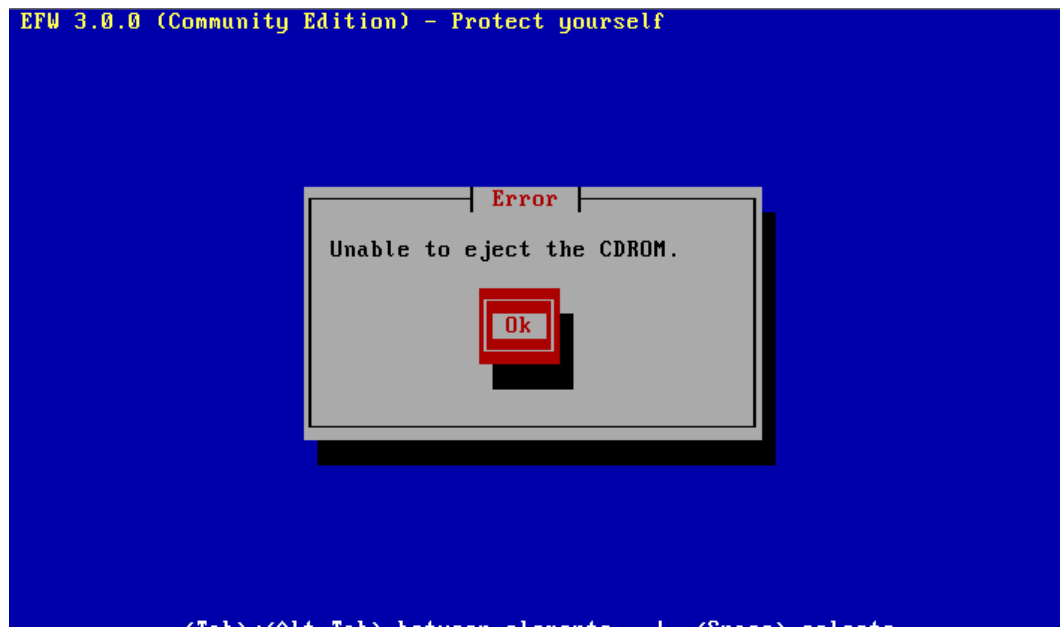
The entire process may take up to 15 minutes to complete.



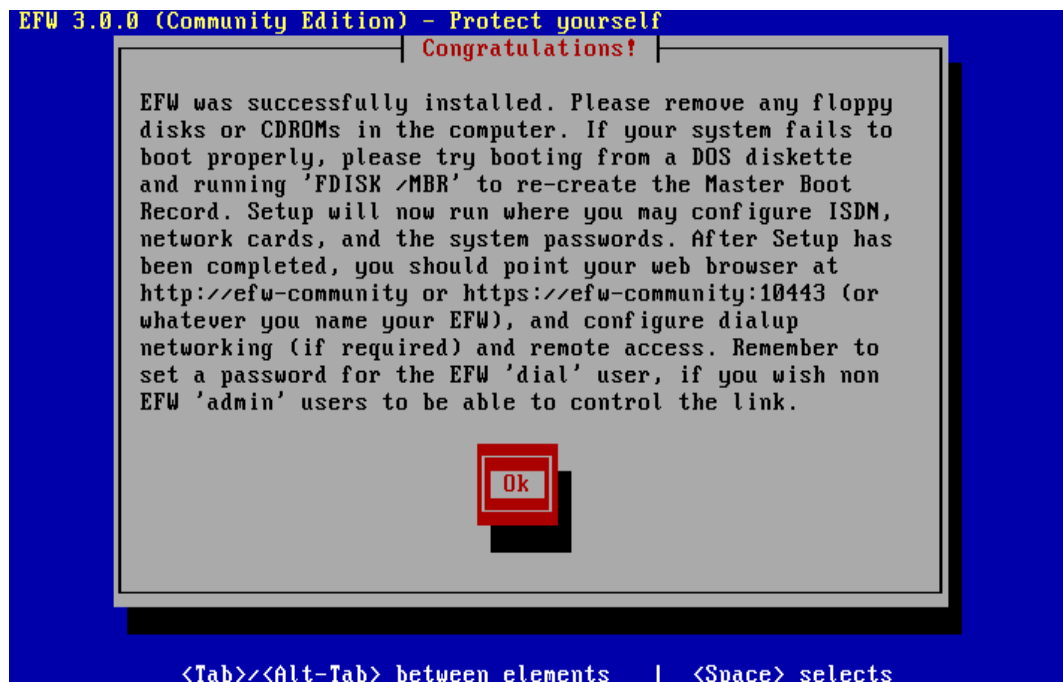
20. For the GREEN Interface, type 192.168.1.1 as the IP address, press **Enter** twice and then once for OK.



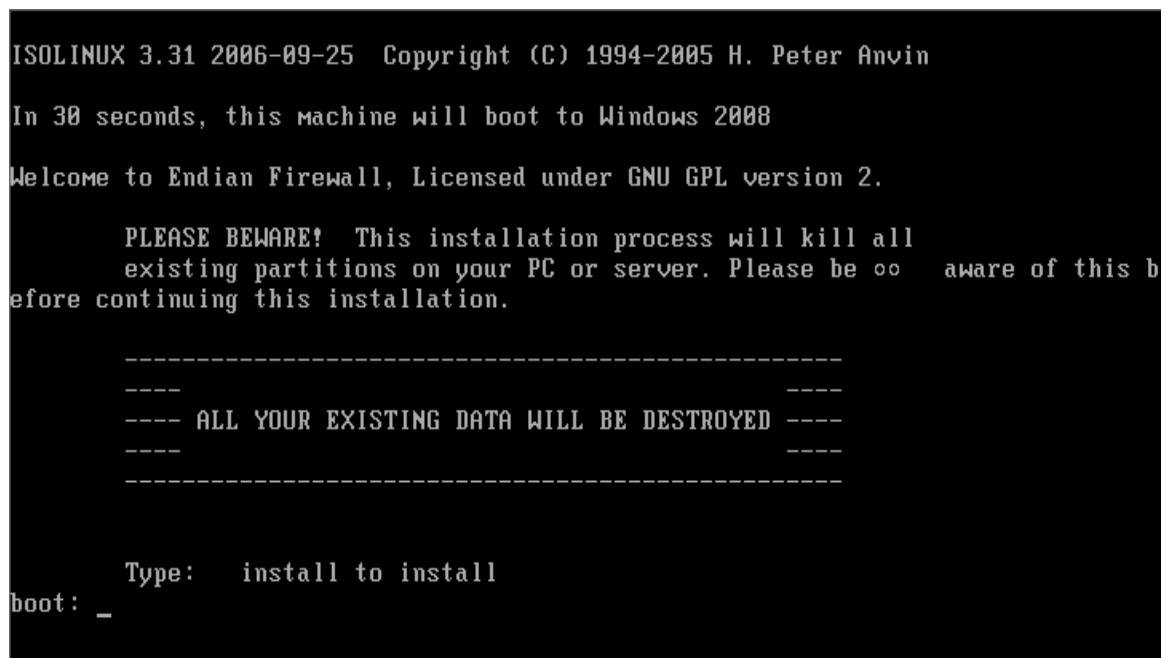
21. Press **Enter** for **Ok** at the unable to eject the CD-ROM error.



22. You will receive a message indicating EFW was successfully installed. Press Enter for **Ok** to reboot.



23. You can press **Enter** at this screen or wait 30 seconds and EFW will load.



After the firewall loads up to the following screen, it will be ready to be configured.

```
Release: Endian Firewall Community release 3.0.devel
Product: Community

Management URL: https://192.168.1.1:10443
Green IP:      192.168.1.1/24
-----

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

Choice: _
```

1.2 Conclusion

The Windows based firewall was allowing all outbound traffic. Network Address Translation (NAT), is set up allowing the internal machines (such as the Windows 8 Internal Machine) to communicate with the machines on the public network (such as the Windows 7 External Machine). In addition, the Windows firewall was configured to redirect incoming requests for the FTP, TELNET, SMTP, HTTP, and POP3 to the Windows 2008 machine on the Internal Network. Linux based firewalls like Untangle, Smoothwall, MOnowall, Endian Community Firewall, and pfSense are commonly used in the industry. In the next section, we will configure the Linux based Endian firewall to replicate the setting of the Windows based firewall.

1.3 Discussion Questions

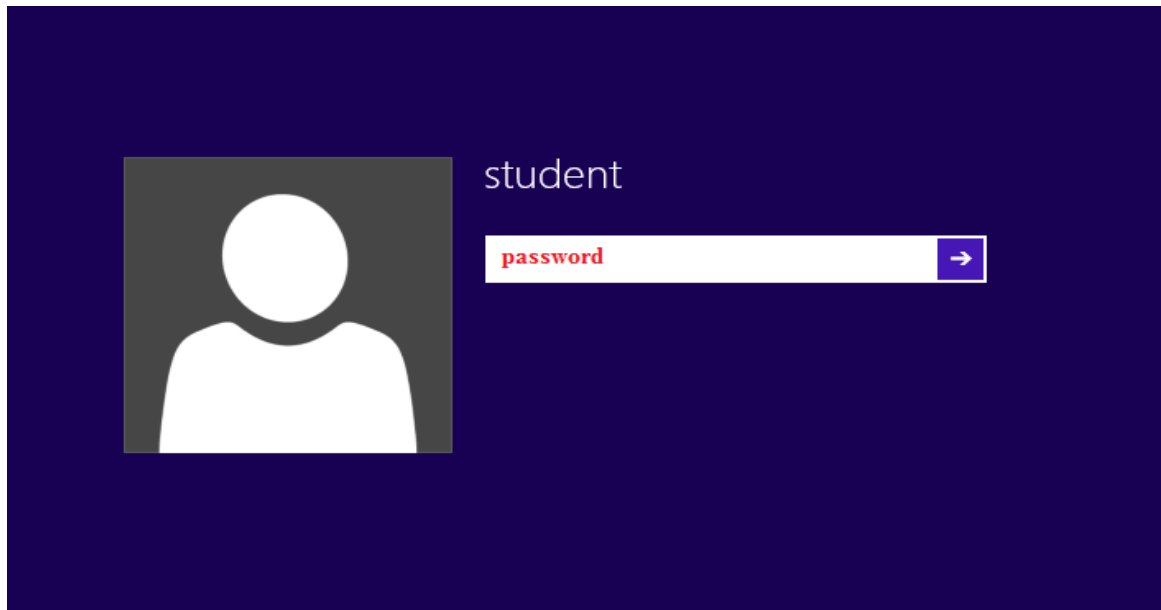
1. What is NAT, and how can you check to ensure that outbound traffic is allowed?
Ans: A technique which allow multiple device on a private network to share a single public IP address NAT is Network Address Translation. Over here to check we will use command ping 216.1.1200-c 4
2. What machine on this network is running FTP, TELNET, SMTP, HTTP, and POP3?
Ans: On Win2008Firewall this network is running
3. What tool can be used to check for open ports on a system?
Ans: We used over here Nmap tool to check the ports. Nmap(IP address)
4. Which ports do FTP, TELNET, SMTP, HTTP, and POP3 utilize?
Ans:The ports utilities are FTP-21,TELNET -23 ,SMTP-25,HTTP-80 and POP#-110

2 Configuring and Testing the Linux Based Firewall

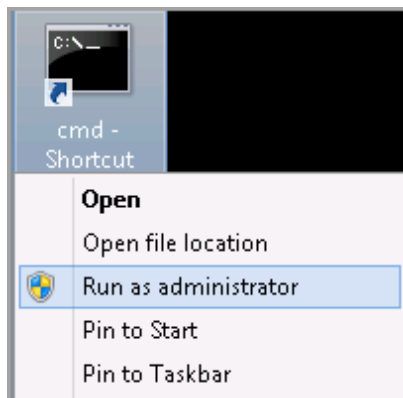
The Windows firewall was currently set up to allow all outbound traffic. In this objective, we will allow all outbound traffic and configure incoming requests for FTP, Telnet, SMTP, HTTP and POP3 to be redirected to the internal Windows Server 2008 VM with the Linux Community Edition Endian Firewall.

2.1 Configuring the Firewall

1. Click on the **Windows 8** icon on the lab topology to bring up the login screen. For the student password, type **password**, and then press **Enter**.



2. Right-click the cmd-Shortcut on the desktop and select **Run as administrator**.



3. Type the following command to ping the firewall on its internal interface.
C:\>ping 192.168.1.1

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

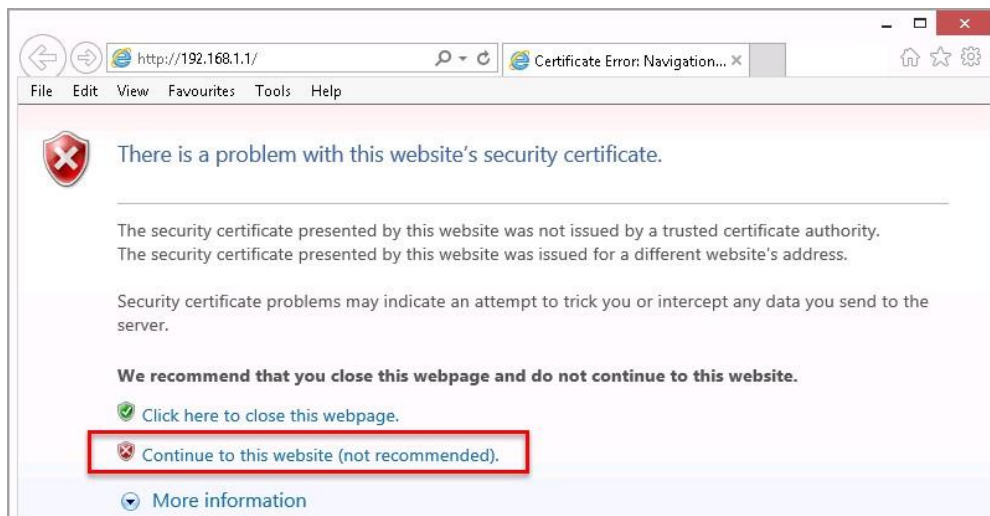
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

4. Click on the shortcut to Internet Explorer on the Windows 8 Internal Machine desktop.



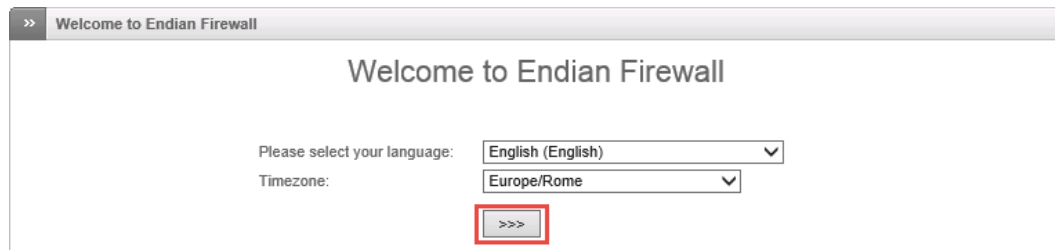
5. Go to the following URL: <http://192.168.1.1/>. Click **Continue to this website**.



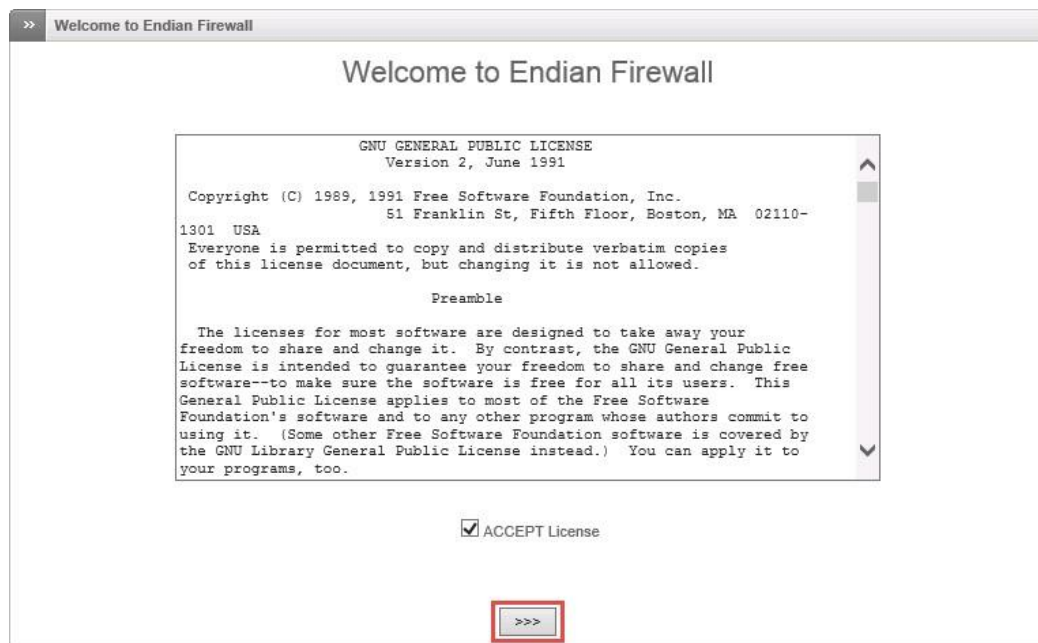
- Click the >>> (**Next**) button at the Welcome to Endian Firewall.



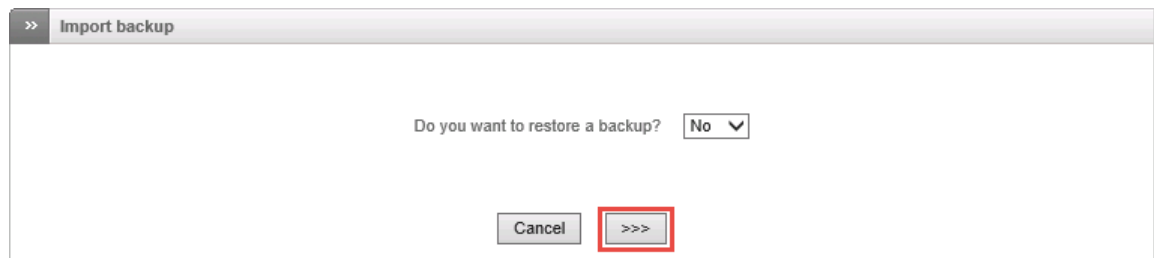
- Click >>> at the select your language and time zone screen.



- Click the **Accept License** check-box and click the >>> button below.



9. Click >>> at the Restore Backup screen.



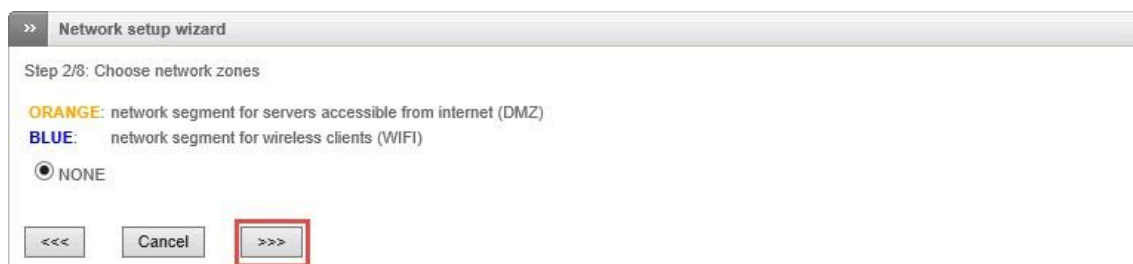
10. For the Web Frontend and the SSH Password, type **password** and click >>>.



11. Select **ETHERNET STATIC** and click the >>> button.



12. Click >>> at the Network Zones screen.



13. Click >>> at the GREEN Interface Screen (Local Area Network-192.168.1.1).

Network setup wizard

Step 3/8: Network preferences

GREEN (trusted, internal network (LAN)):

IP address: network mask:

Add additional addresses (one IP/Netmask or IP/CIDR per line):

Interfaces:

Port	Link	Description	MAC	Device
<input checked="" type="checkbox"/> 1	✓	Intel ?	00:50:56:9c:a9:97	eth0
<input type="checkbox"/> 2	✓	Intel ?	00:50:56:9c:8a:94	eth1

Hostname:

Domainname:

<<< Cancel >>>

14. For the Red Interface, type **216.1.1.1**. For the network mask, select **255.0.0.0** from the dropdown. Select the **Port 2** radio button for the internal card and type **216.1.1.1** for the gateway. Click >>>.

Network setup wizard

Step 4/8: Internet access preferences

RED (untrusted, internet connection (WAN)):

IP address: network mask:

Add additional addresses (one IP/Netmask or IP/CIDR per line):

Interfaces:

Port	Link	Description	MAC	Device
<input type="radio"/> 1	✓	Intel ?	00:50:56:9c:a9:97	eth0
<input checked="" type="radio"/> 2	✓	Intel ?	00:50:56:9c:8a:94	eth1

Default gateway:

MTU:

Spoof MAC address with:

☒ This field may be blank.

<<< Cancel >>>

15. Put **8.8.8.8** for both DNS Servers (Google). This system is not on the Internet.



Network setup wizard

Step 5/8: configure DNS resolver

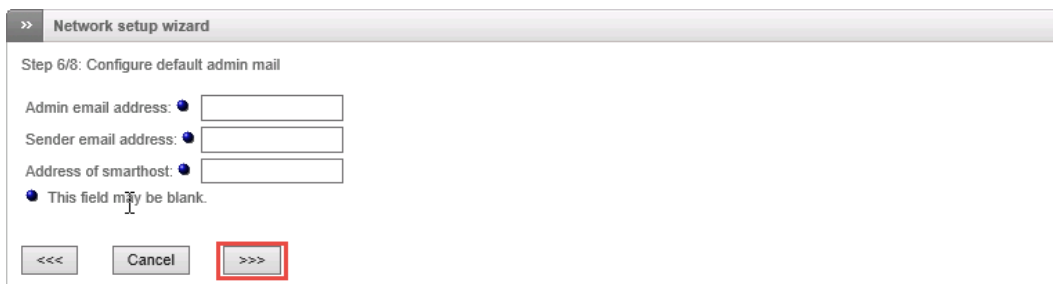
manual DNS configuration:

DNS 1:

DNS 2:

<<< Cancel >>>

16. Click >>> at the Admin Email Address screen.



Network setup wizard

Step 6/8: Configure default admin mail

Admin email address:

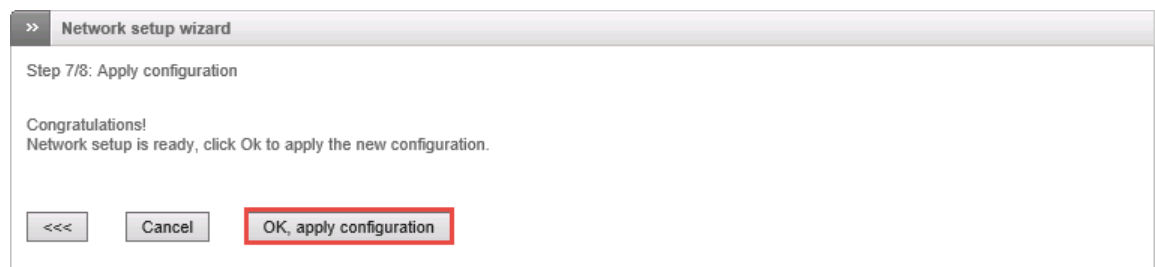
Sender email address:

Address of smarthost:

☒ This field may be blank.

<<< Cancel >>>

17. Click **Ok, apply configuration** to apply settings.




Network setup wizard

Step 7/8: Apply configuration

Congratulations!
Network setup is ready, click Ok to apply the new configuration.

<<< Cancel OK, apply configuration

18. Wait for the Network Setup page to reload.



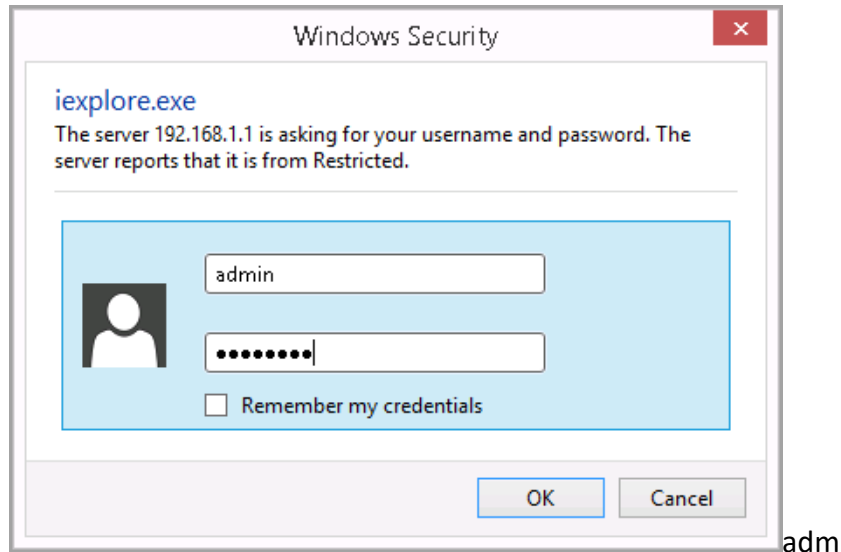
Network setup wizard

Step 8/8: End

Your configuration has been saved. Please wait until the dependent services have been reloaded. This may take up to 20 seconds. Enjoy!

Remember to check if IP address blocks of services are still configured as you wish. Mainly check the configuration of "Network based access control" of the HTTP Proxy.

19. For the username, type **admin**. For the password, type **password**. Click OK.



20. From the **Windows 8 Internal Machine** command prompt, type the following command to see if outbound ping is allowed:

C:\>ping 216.1.1.200

```
C:\>ping 216.1.1.200
Pinging 216.1.1.200 with 32 bytes of data:
Reply from 216.1.1.200: bytes=32 time<1ms TTL=127
Reply from 216.1.1.200: bytes=32 time<1ms TTL=127
Reply from 216.1.1.200: bytes=32 time<1ms TTL=127
Reply from 216.1.1.200: bytes=32 time<1ms TTL=127
```

21. Type the following commands to see if outbound FTP traffic is allowed:

[ftp 216.1.1.200](#)

user: **ftp**

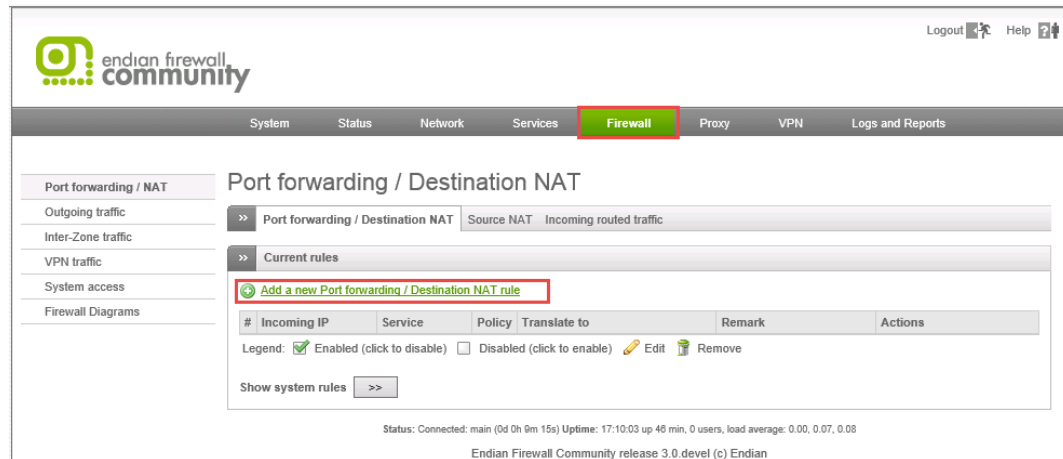
Password: **password**

ftp> **bye**

```
C:\>ftp 216.1.1.200
Connected to 216.1.1.200.
220 Microsoft FTP Service
User (216.1.1.200:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name)
Password:
230 User logged in.
ftp> bye
221 Goodbye.
```


For outbound traffic, no Firewall configuration was needed. We will now configure the inbound traffic.

22. Click the Firewall tab in the middle of the web page. Click the green link that states **Add a new Port forwarding / Destination NAT rule**.



23. Highlight **Uplink main 216.1.1.1** and select/enter the values below:

Service	FTP
Incoming port	21
Insert IP	192.168.1.100
Port Range	21

24. Click **Create Rule**.

25. Click **Add a new Port forwarding / Destination NAT rule.**

26. Highlight **Uplink main 216.1.1.1** and select/enter the values below:

Service	Telnet
Incoming port	23
Insert IP	192.168.1.100
Port Range	23

27. Click **Create Rule.**

Port forwarding / Destination NAT Rule Editor

Simple Mode | [Advanced Mode](#)

Incoming IP
Type * **Zone/VPN/Uplink**
Select interfaces (hold CTRL for multiselect)
<ANY Uplink>
Uplink main - IP:216.1.1.1
Zone GREEN - IP:All known
Zone GREEN - IP:192.168.1.1

Incoming Service/Port
Service * **Telnet**
Protocol * **TCP**
Incoming port/range (one per line, e.g. 80, 80:88)
23

Translate to *
Insert IP **192.168.1.100**
Port/Range (e.g. 80, 80:88) **23**
NAT **NAT**

☒ Enabled ☐ Log Remark Position * **Last**

Create Rule or [Cancel](#) * This Field is required.

28. Click **Add a new Port forwarding / Destination NAT rule.**

29. Highlight **Uplink main 216.1.1.1** and select/enter the values below:

Service	HTTP
Incoming port	80
Insert IP	192.168.1.100
Port Range	80

30. Click **Create Rule.**

Port forwarding / Destination NAT Rule Editor

Simple Mode | [Advanced Mode](#)

Incoming IP
Type * **Zone/VPN/Uplink**
Select interfaces (hold CTRL for multiselect)
<ANY Uplink>
Uplink main - IP:216.1.1.1
Zone GREEN - IP:All known
Zone GREEN - IP:192.168.1.1

Incoming Service/Port
Service * **HTTP**
Protocol * **TCP**
Incoming port/range (one per line, e.g. 80, 80:88)
80

Translate to *
Insert IP **192.168.1.100**
Port/Range (e.g. 80, 80:88) **80**
NAT **NAT**

☒ Enabled ☐ Log Remark Position * **Last**

Create Rule or [Cancel](#) * This Field is required.

31. Click **Add a new Port forwarding / Destination NAT rule.**
32. Highlight **Uplink main 216.1.1.1** and select/enter the values below:

Service	SMTP
Incoming port	25
Insert IP	192.168.1.100
Port Range	25

33. Click **Create Rule.**

Port forwarding / Destination NAT Rule Editor

Simple Mode | [Advanced Mode](#)

Incoming IP
Type * **Zone/VPN/Uplink**
Select interfaces (hold CTRL for multiselect)
<ANY Uplink>
Uplink main - IP: 216.1.1.1
Zone GREEN - IP: All known
Zone GREEN - IP: 192.168.1.1

Incoming Service/Port
Service * SMTP
Incoming port/range (one per line, e.g. 80, 80:88) 25
Protocol * TCP

Translate to *
Insert IP 192.168.1.100
Port/Range (e.g. 80, 80:88) 25
NAT NAT

☒ Enabled ☐ Log Remark Position * Last

[Create Rule](#) or [Cancel](#) * This Field is required.

34. Click **Add a new Port forwarding / Destination NAT rule.**
35. Highlight **Uplink main 216.1.1.1** and select/enter the values below:

Service	POP3
Incoming port	110
Insert IP	192.168.1.100
Port Range	110

36. Click **Create Rule.**

Port forwarding / Destination NAT Rule Editor

Simple Mode | [Advanced Mode](#)

Incoming IP
Type * **Zone/VPN/Uplink**
Select interfaces (hold CTRL for multiselect)
<ANY Uplink>
Uplink main - IP: 216.1.1.1
Zone GREEN - IP: All known
Zone GREEN - IP: 192.168.1.1

Incoming Service/Port
Service * POP3
Incoming port/range (one per line, e.g. 80, 80:88) 110
Protocol * TCP

Translate to *
Insert IP 192.168.1.100
Port/Range (e.g. 80, 80:88) 110
NAT NAT

☒ Enabled ☐ Log Remark Position * Last

[Create Rule](#) or [Cancel](#) * This Field is required.

37. Review all 5 of the listed rules and then click the **Apply** button.



>> Current rules						
+ Add a new Port forwarding / Destination NAT rule						
#	Incoming IP	Service	Policy	Translate to	Remark	Actions
1	216.1.1.1 (Uplink main)	TCP/21		192.168.1.100		
	ALLOW with IPS from:		<ANY>			
2	216.1.1.1 (Uplink main)	TCP/23		192.168.1.100 : 23		
	ALLOW with IPS from:		<ANY>			
3	216.1.1.1 (Uplink main)	TCP/80		192.168.1.100 : 80		
	ALLOW with IPS from:		<ANY>			
4	216.1.1.1 (Uplink main)	TCP/25		192.168.1.100 : 25		
	ALLOW with IPS from:		<ANY>			
5	216.1.1.1 (Uplink main)	TCP/110		192.168.1.100 : 110		
	ALLOW with IPS from:		<ANY>			

You will see an orange box appear stating NAT rules applied successfully.



38. From the Windows 7 External machine, type the following command to scan the firewall for open ports:

C:\>nmap 216.1.1.1

```
C:\>nmap 216.1.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2015-08-31 16:10 Eastern Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS lookups will be disabled.
Try using --system-dns or specify valid servers with --dns-servers=
Nmap scan report for server.XYZcompany.com (216.1.1.1)
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
MAC Address: 00:50:56:9C:8A:94 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
```

You may ignore the DNS warning message.

2.2 Conclusion

In order for external users on the WAN (Internet) to use services on a machine on the Internal Network, the firewall must be configured to allow requests to be re-directed to an internal machine. Ports can be opened and closed by using the Port forwarding / Destination NAT rule within the Linux-based Endian Community Firewall.

2.3 Discussion Questions

1. Within the Endian Community Firewall, where is redirection configured?
Ans: In the Endian Community Firewall, redirection is configured in firewall. Specifically, it is under the "Port forwarding" or "Destination NAT" sections, where we can add new port and create file.
2. What ports do SMTP and POP3 utilize?
Ans: Over here SMTP used 25 and POP3-110
3. What tool can be utilized by an external user to determine if ports are open?
Ans: Tool such as Nmap or an online port scanner to determine if ports are open on a target system. Over here I have used Nmap tool to where I have send the packets and check which port are open and accepting the connections
4. Do any outbound rules need to be configured on the Endian Community Firewall?
Ans : YES, need to configured the outbound rules to avoid unwanted traffic from some

websites

3 Using Internal Services from an External Machine

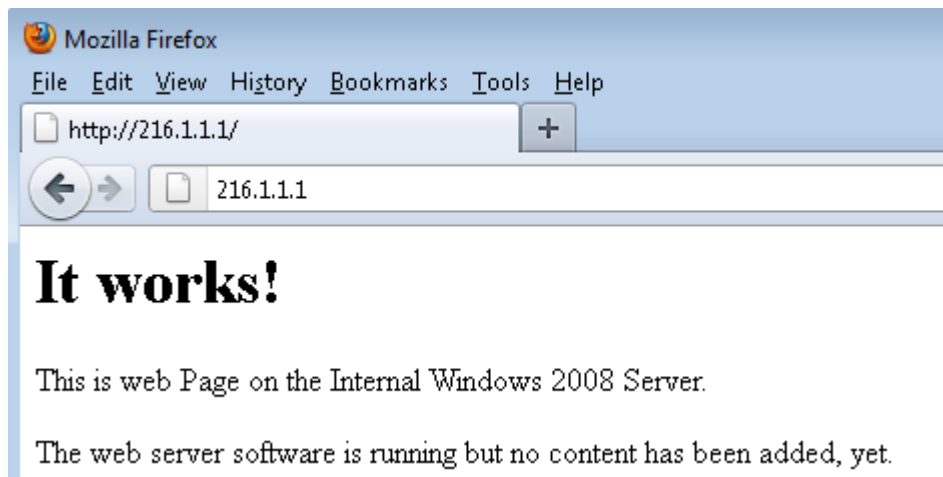
Even though we have used nmap to verify that the correct ports are open, a good network administrator will also test each of the services to verify that they are working correctly. In this scenario, we will test the FTP, TELNET, SMTP, HTTP and POP3 services of the Linux-based Endian Community Firewall.

3.1 Testing the Firewall

1. On the Windows 7 External Machine, click on the shortcut to Firefox on the desktop.



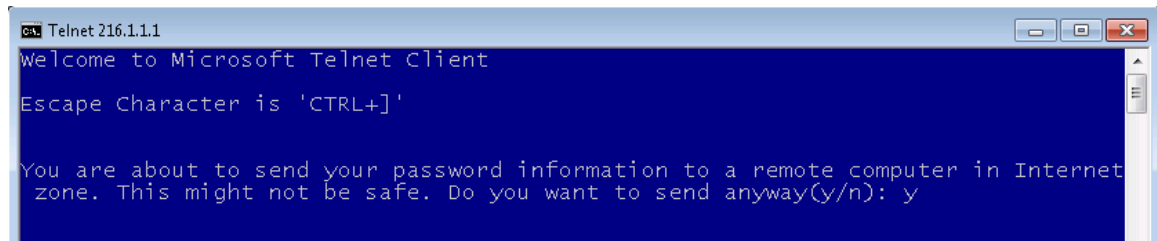
2. Navigate to <http://216.1.1.1>. If you receive the message **It works!**, then you know the redirection of HTTP through the Linux-based Endian Community Firewall is working correctly.



3. From the Windows command prompt, type the following command:
C:\>telnet 216.1.1.1

```
C:\>telnet 216.1.1.1
```

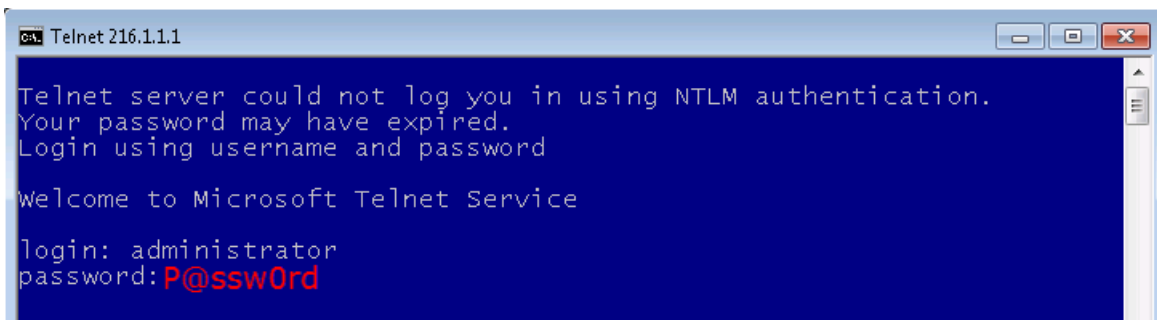
4. Type **y** to continue connecting.



```
Telnet 216.1.1.1
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'

You are about to send your password information to a remote computer in Internet
zone. This might not be safe. Do you want to send anyway(y/n): y
```

5. Type **administrator** for the username and **P@ssw0rd** for the password. (The “0” in P@ssw0rd is a zero.)

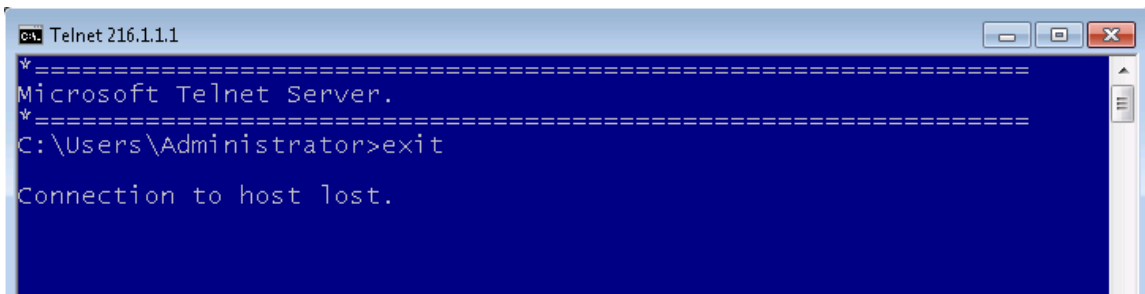


```
Telnet 216.1.1.1
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

Welcome to Microsoft Telnet Service

login: administrator
password: P@ssw0rd
```

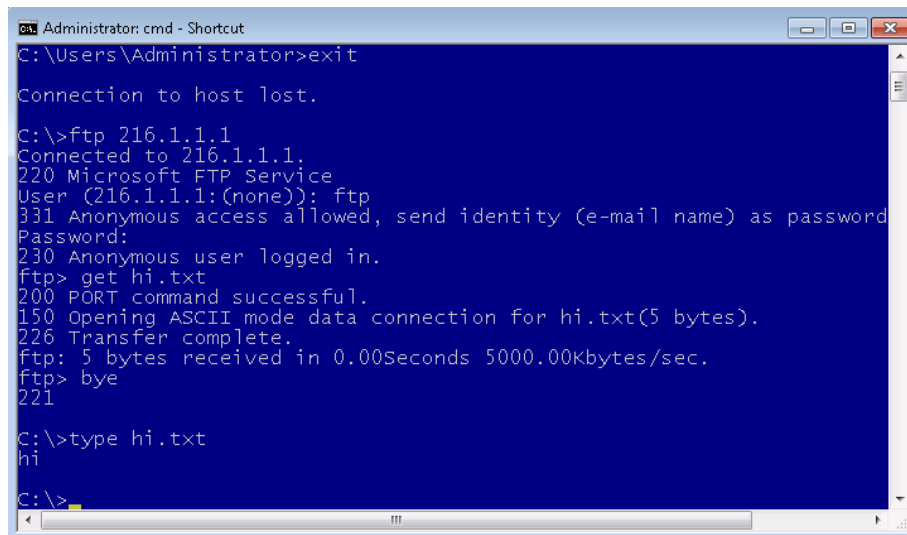
6. To leave the TELNET session, type **exit**. You now know the redirection of TELNET through the Linux-based Endian Community Firewall is working correctly.



```
Telnet 216.1.1.1
Microsoft Telnet Server.
C:\Users\Administrator>exit
Connection to host lost.
```

7. Type the following commands to connect to the FTP site and download the file.

```
C:\>ftp 216.1.1.1
user: ftp
Password: password
ftp> get hi.txt
ftp> bye
C:\>type hi.txt
```



The screenshot shows a Windows command prompt window titled "Administrator: cmd - Shortcut". The user has entered the command "exit", which resulted in "Connection to host lost." The user then enters "ftp 216.1.1.1", connecting to the host. The session shows the user logging in as an anonymous user, downloading "hi.txt" successfully, and then typing "hi" in the command prompt after the FTP session ends.

```
Administrator: cmd - Shortcut
C:\Users\Administrator>exit
Connection to host lost.

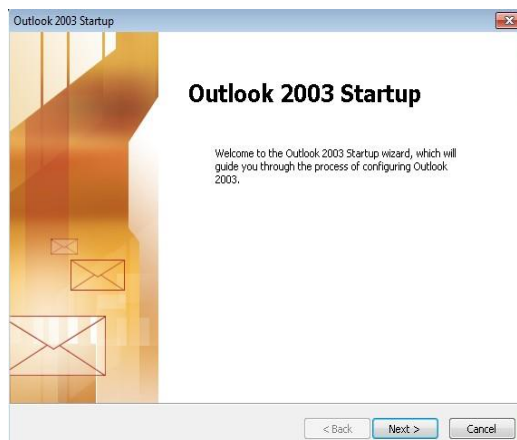
C:\>ftp 216.1.1.1
Connected to 216.1.1.1.
220 Microsoft FTP Service
User (216.1.1.1:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password
Password:
230 Anonymous user logged in.
ftp> get hi.txt
200 PORT command successful.
150 Opening ASCII mode data connection for hi.txt(5 bytes).
226 Transfer complete.
ftp: 5 bytes received in 0.00Seconds 5000.00kbytes/sec.
ftp> bye
221

C:\>type hi.txt
hi
C:\>
```

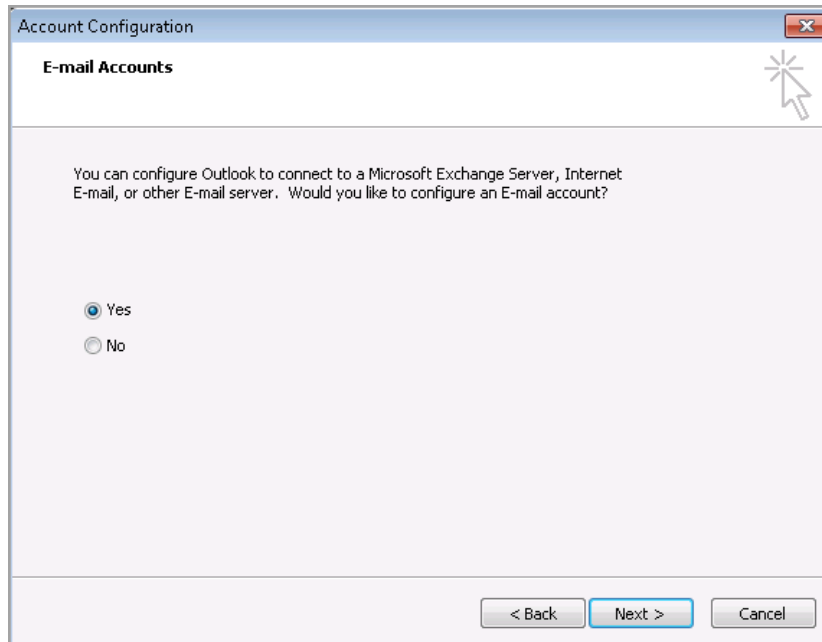
8. On the Windows 7 External Machine, click on the shortcut to **Microsoft Office Outlook**.



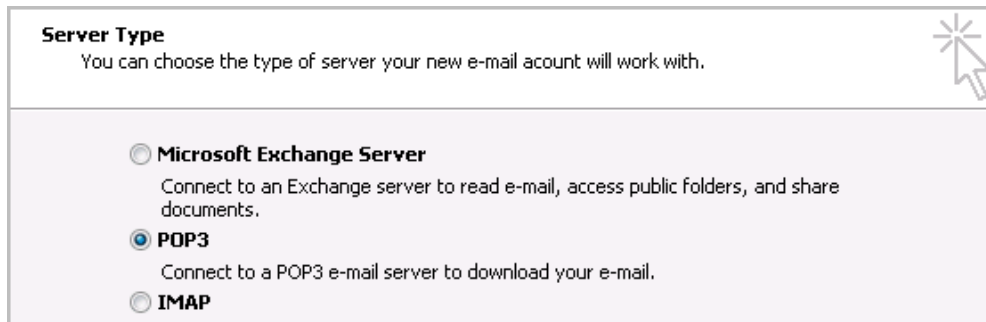
9. Click **Next** on the Outlook Startup screen.



10. Click **Next** on the Account Configuration screen.



11. Select **POP3** (Post Office Protocol) as the server type. Click the **Next** button.



12. Fill out the following fields:

Your Name	administrator
E-mail Address	administrator@XYZcompany.com
User Name	administrator
Password	P@ssw0rd
Incoming Mail Server	216.1.1.1 (Firewall IP)
Outgoing Mail Server	216.1.1.1 (Firewall IP)

13. Click the button labeled **More Settings**.

E-mail Accounts

Internet E-mail Settings (POP3)
Each of these settings are required to get your e-mail account working.

User Information

Your Name:
E-mail Address:

Server Information

Incoming mail server (POP3):
Outgoing mail server (SMTP):

Login Information

User Name:
Password:
☒ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

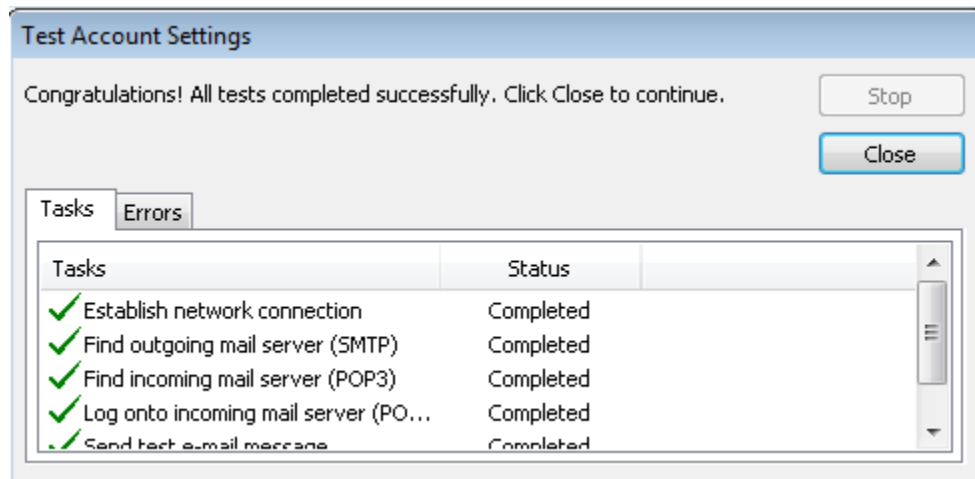
14. Click on the **Outgoing Server** tab and check the box that states, "**My outgoing server (SMTP) requires authentication**", click OK.

Internet E-mail Settings

General **Outgoing Server** Connection Advanced

☒ My outgoing server (SMTP) requires authentication

15. Click the **Test Account Settings** button. You should receive 4 green checks.



16. Close all open windows and PC viewers. End the reservation.

3.2 Conclusion

While using nmap is an effective way to verify ports are open, it will not be as effective as testing each service. In this section of the lab, we tested the SMTP, POP3, HTTP, FTP, and HTTP services that were being allowed through the Linux based firewall. The successful logins and file transfers proved that the services were operating properly. These quality assurance checks are essential for production environments.

3.3 Discussion Questions

1. What is the command to download a file in FTP?
Ans: Command for FTP is Get<name of file>
2. What does SMTP stand for and what port does it use?
Ans: SMTP used port 23 and SMTP is Simple mail transfer protocol
3. What is the purpose of TELNET and what port does it use?
Ans: TELNET is to allow remote access to a server or device over a network. It uses port 23 to establish a connection between the local and remote devices
4. How do you terminate an FTP session?
Ans: By entering EXIT we can terminated the FTP session.

References

1. pfSense Firewall:
<https://www.pfsense.org>
2. Smoothwall Firewall:
<http://www.smoothwall.org/>
3. Untangle Firewall:
<https://www.untangle.com/store/firewall.html>
4. Endian Firewall:
<http://www.endian.com/us/#.U5P47WzD8dU>
5. M0n0wall:
<http://m0n0.ch/wall/>

