



## NETWORK SECURITY LAB SERIES

### Lab 4: Configuring a Linux Based Firewall to Allow 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 Setting up and Testing External Services .....	6
1.1 Testing the Current Firewall and Installing the Linux Firewall .....	6
1.2 Conclusion .....	18
1.3 Discussion Questions.....	18
2 Installing the Linux Based Firewall .....	19
2.1 Configuring the Firewall .....	19
2.2 Conclusion .....	37
2.3 Discussion Questions.....	37
3 Testing External Services on the Linux Based Firewall .....	38
3.1 Testing the Firewall .....	38
3.2 Conclusion .....	41
3.3 Discussion Questions.....	41
References .....	42



## 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. Setting up and Testing External Services
2. Installing the Linux Based Firewall
3. Testing External Services on the Linux Based Firewall

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.

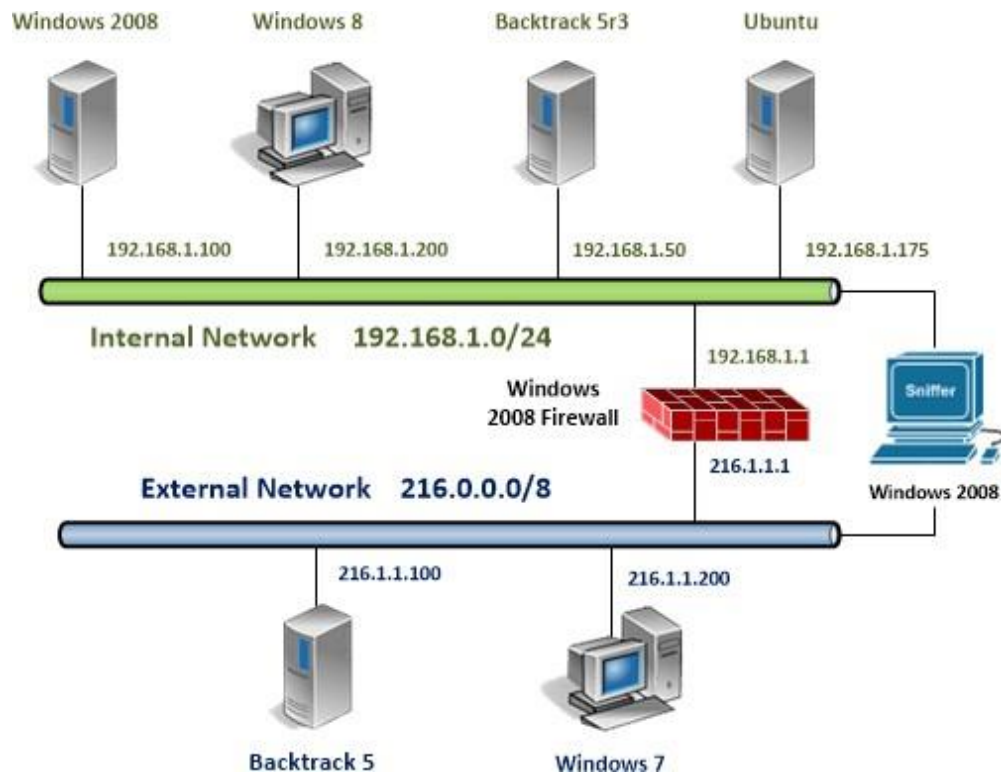
**nmap** – Nmap can be used in Linux, Mac, or Microsoft Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap 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 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
Backtrack 5 External Machine	216.1.1.100	root	toor
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 Setting up and Testing External Services

In this section we, will examine the current Firewall configuration. Currently, all outbound TCP/IP traffic is allowed. While this is convenient, it may not be the best policy for networks. Blocking certain outbound traffic can increase a network's security.

### 1.1 Testing the Current Firewall and Installing the Linux Firewall

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.

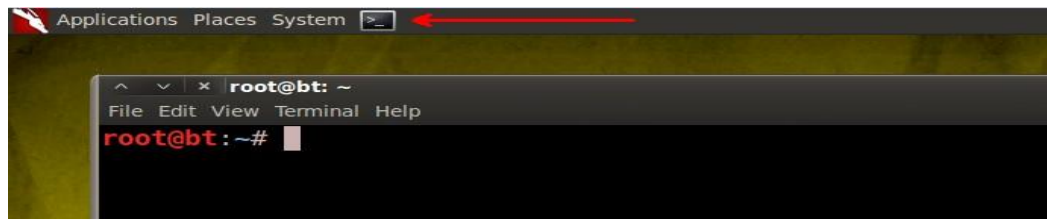
```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

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**

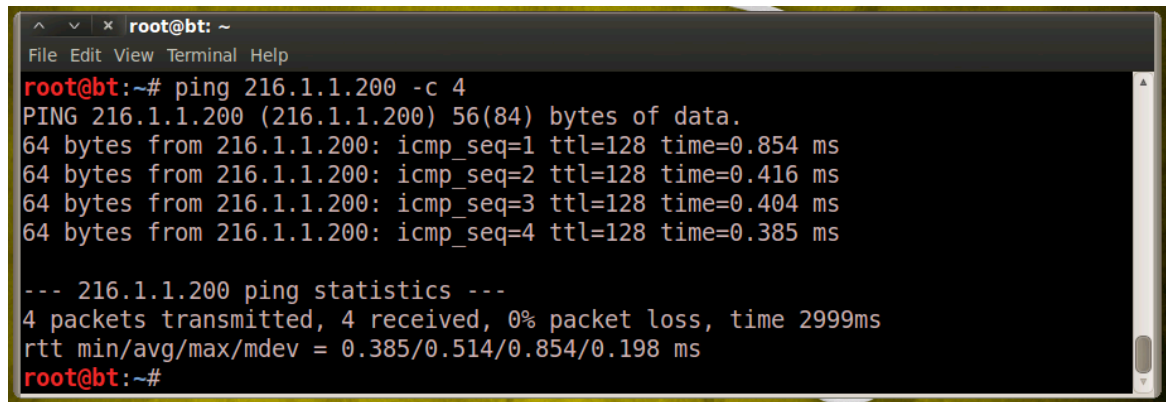
```
root@bt:~# startx_
```

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
```

A screenshot of a terminal window titled 'root@bt: ~'. The terminal shows the command 'ping 216.1.1.200 -c 4' being executed. The output displays four successful ping requests with varying times (0.854 ms, 0.416 ms, 0.404 ms, 0.385 ms). Below this, it shows 'ping statistics' for 216.1.1.200: 4 packets transmitted, 4 received, 0% packet loss, and a total time of 2999ms. The round-trip times are listed as 0.385/0.514/0.854/0.198 ms. The prompt returns to 'root@bt:~#'.

```
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 Linux based Firewall is allowing all outbound traffic including ICMP.

5. There are FTP Servers set up on the Windows 7 External Machine and the Backtrack 5 External Machine. To test outbound FTP connectivity, type:

```
root@bt:~# ftp 216.1.1.200
```

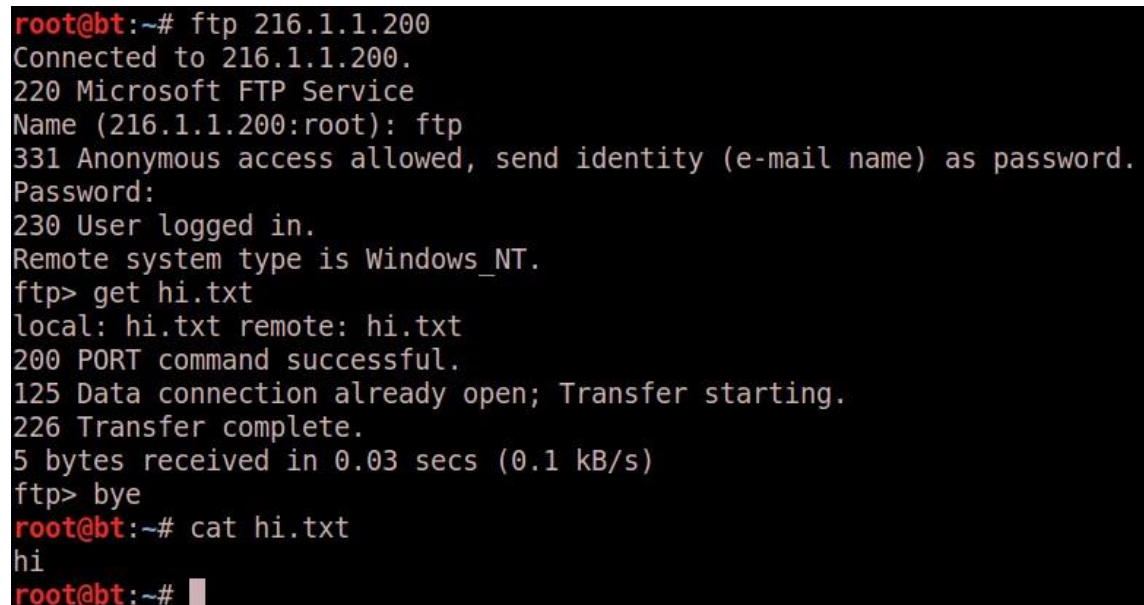
```
user: ftp
```

```
Password: password
```

```
ftp> get hi.txt
```

```
ftp> bye
```

```
root@bt:~# cat hi.txt
```

A screenshot of a terminal window showing the output of the 'ftp 216.1.1.200' command. It shows a successful connection to the FTP service on 216.1.1.200. The user 'ftp' is logged in, and the system type is identified as 'Windows\_NT'. The command 'get hi.txt' is executed, showing the file is transferred successfully. The output includes details like '5 bytes received in 0.03 secs (0.1 kB/s)'. Finally, the user types 'bye' and returns to the shell prompt. The 'cat hi.txt' command is then used to verify the file content, which is 'hi'.

```
root@bt:~# ftp 216.1.1.200
Connected to 216.1.1.200.
220 Microsoft FTP Service
Name (216.1.1.200:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> get hi.txt
local: hi.txt remote: hi.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5 bytes received in 0.03 secs (0.1 kB/s)
ftp> bye
root@bt:~# cat hi.txt
hi
root@bt:~#
```

Perform the following steps on the **Backtrack 5 External Machine** to set up HTTP services:

- Click the **Backtrack 5** icon to open the **BackTrack 5 External 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
```

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

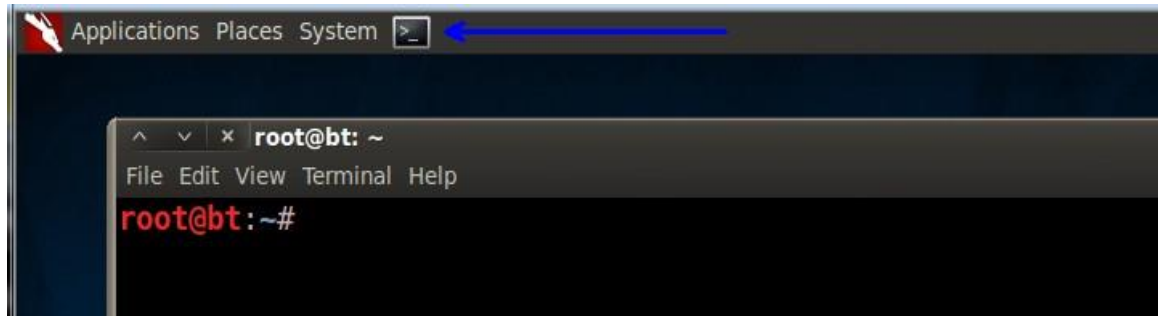
```
root@bt:~# startx_
```

- To start Apache, select **BackTrack > Services > HTTPD > apache start**. A window will appear and then close.





Open a terminal on by clicking on the picture to the right of the word **System** in the task bar in the top of the screen of the Backtrack 5 External Machine.

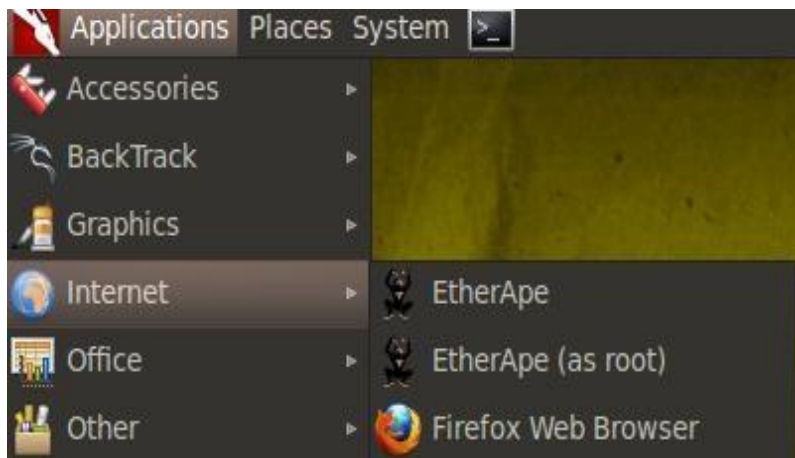


9. To view the current running services, type the following command:

```
root@bt:~# netstat -tan
```

```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:7337          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp6       0      0 :::1:7337               :::*                    LISTEN
```

10. Go back to the **BackTrack 5 R3 Internal Machine**, click on **Applications > Internet > Firefox Web Browser**.



11. Type `http://216.1.1.100` in the URL bar and press Enter to connect to the external web site.



Next, we will set up a TFTP server on the **BackTrack 5 External Machine**. Go back to the Backtrack 5 External Machine.

12. Make a directory named **tftpboot** by typing the following command:

```
root@bt:~# mkdir /tftpboot
```

```
root@bt:~# mkdir /tftpboot
```

13. Start the tftp server by typing the following command:

```
root@bt:~# atftpd --daemon /tftpboot
```

```
root@bt:~# atftpd --daemon /tftpboot
```

14. Type the following command to verify that TFTP is listening on UDP port 69:

```
root@bt:~# nmap -sU 127.0.0.1
```

```
root@bt:~# nmap -sU 127.0.0.1

Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-25 19:38 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
69/udp    open|filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
```

15. Create a file in the tftpboot directory of the BackTrack 5 External Machine by typing the following:

```
root@bt:~# echo tftp uses UDP and port 69 > /tftpboot/tftp.txt
```

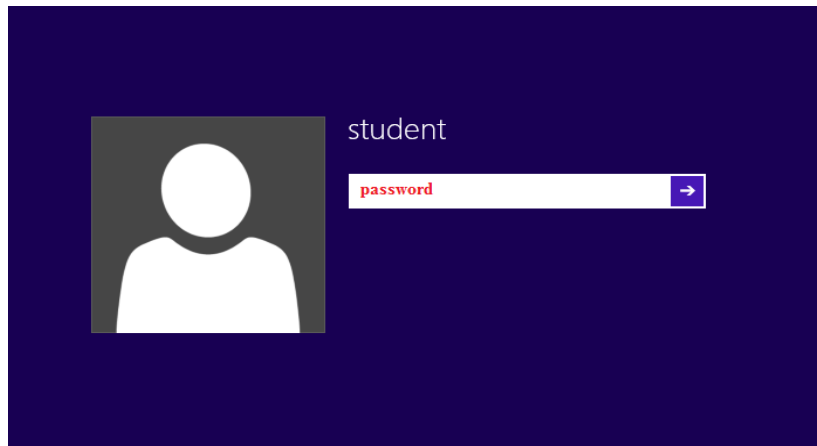
```
root@bt:~# echo tftp uses UDP and port 69 > /tftpboot/tftp.txt
```

16. Verify that the text file is present in the tftpboot directory by typing:

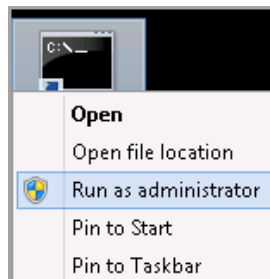
```
root@bt:~# cat /tftpboot/tftp.txt
```

```
root@bt:~# cat /tftpboot/tftp.txt
tftp uses UDP and port 69
```

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

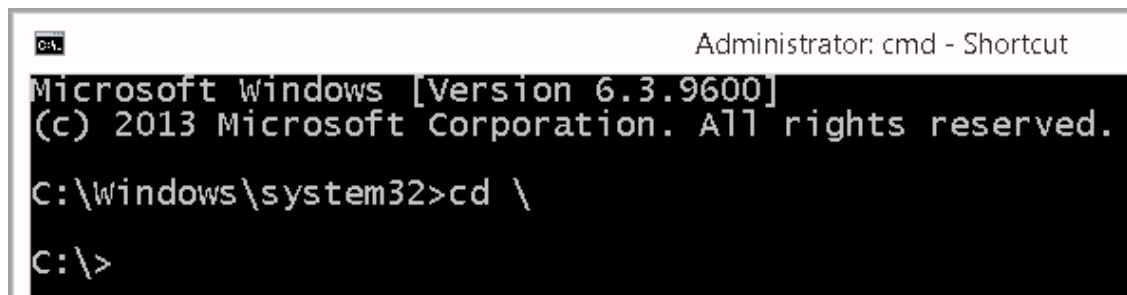


18. Right-click on the cmd-Shortcut on the desktop and select **Run as administrator**.



19. Type the command **cd \** to go to the root of the C: Drive:

```
C:\Windows\system32>cd \
```



20. To download the file, type the following:

C:\>tftp 216.1.1.100 get tftp.txt

```
C:\>tftp 216.1.1.100 get tftp.txt
Transfer successful: 27 bytes in 1 second(s), 27 bytes/s
```

21. View the contents of the file by typing the following command:

C:\>type tftp.txt

```
C:\>type tftp.txt
tftp uses UDP and port 69
```

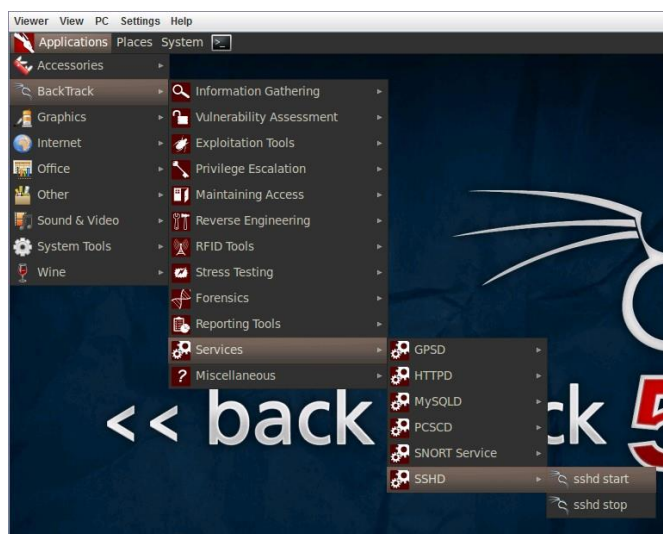
Next, we will set up SSH on the BackTrack 5 External Machine. Go back to the **Backtrack 5 External machine**.

22. Type the following command to generate the keys for SSH:

root@bt:~#sshd-generate

```
root@bt:~# sshd-generate
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
71:49:a3:79:9a:0a:a5:88:8a:e9:e6:04:34:9f:ae:88 root@bt
The key's randomart image is:
+--[RSA1 2048]----+
```

23. Start SSH by selecting **Applications > BackTrack > Services > SSHD > sshd start**. A window will appear and then close.



24. To view the current running services, type the following command:

```
root@bt:~# netstat -tan
```

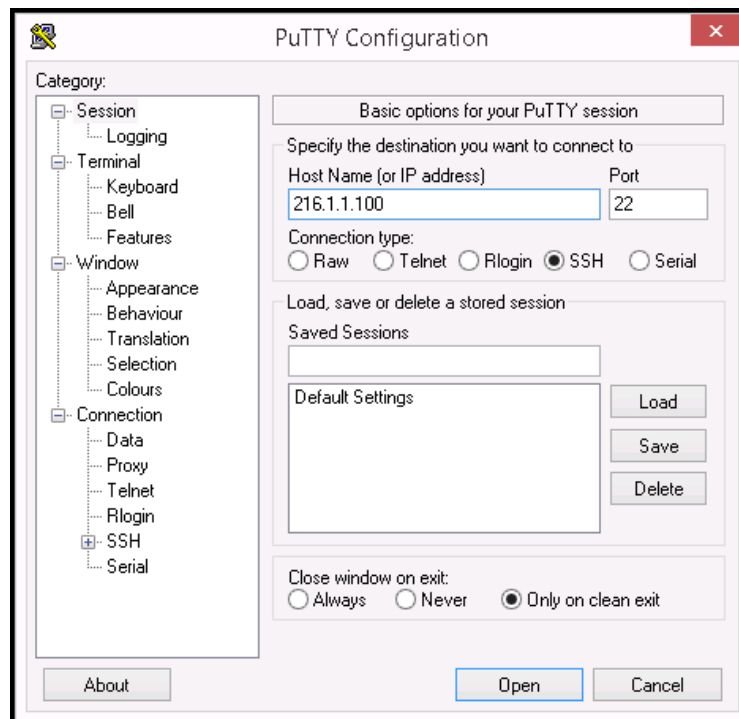
```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 127.0.0.1:7337          0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:21             0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp6     0      0 :::7337                :::*                    LISTEN
tcp6     0      0 :::22                  :::*                    LISTEN
```

After starting SSHD, the BackTrack system is now also listening on port 22.

25. Go back to the **Windows 8 Internal Machine** desktop and double-click on the putty.exe application.



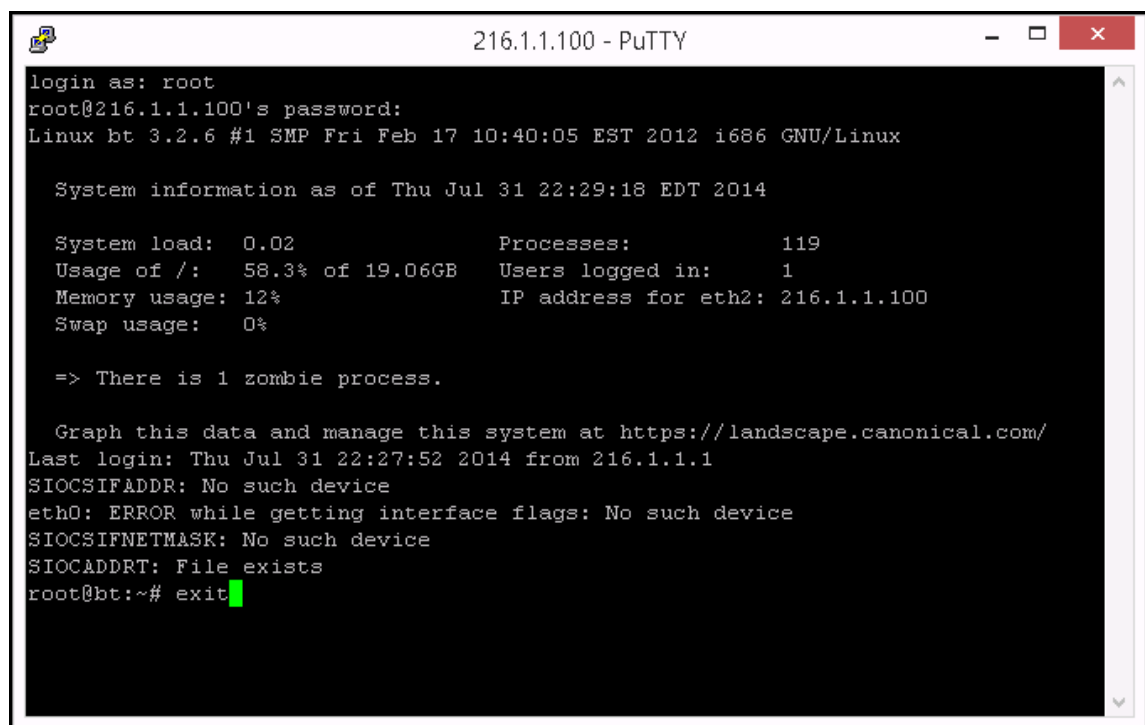
26. Enter **216.1.1.100** for the Host Name and click the Open button.



27. Click Yes to the PuTTY Security Alert message box.



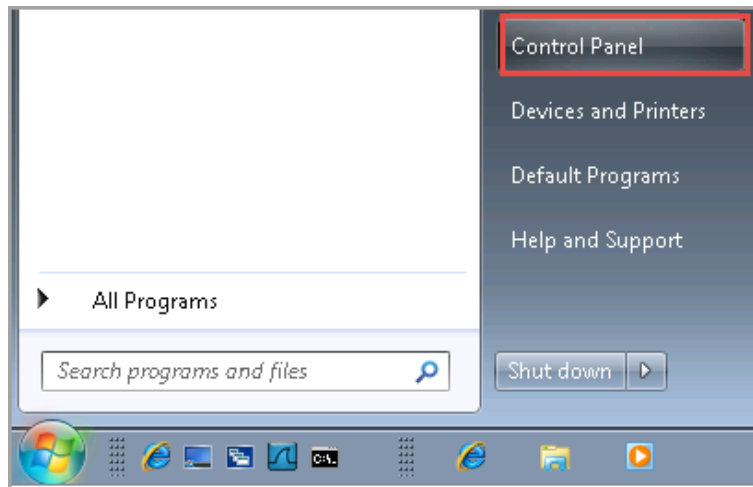
28. For the username type **root**, and for the password type **toor**. After you login, type **exit** and press Enter.



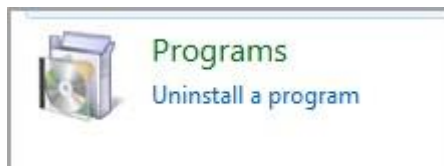
29. Log into the **Windows 7 External Machine** by clicking on the **Windows 7** icon on the topology. If required, enter the username, **student**. Type in the password, **password**, and press **Enter** to log in.



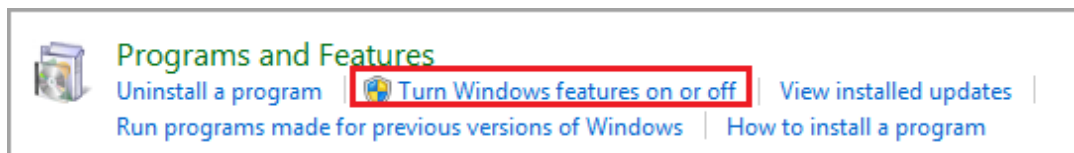
30. Click on the Start button and go to the link for the **Control Panel**.



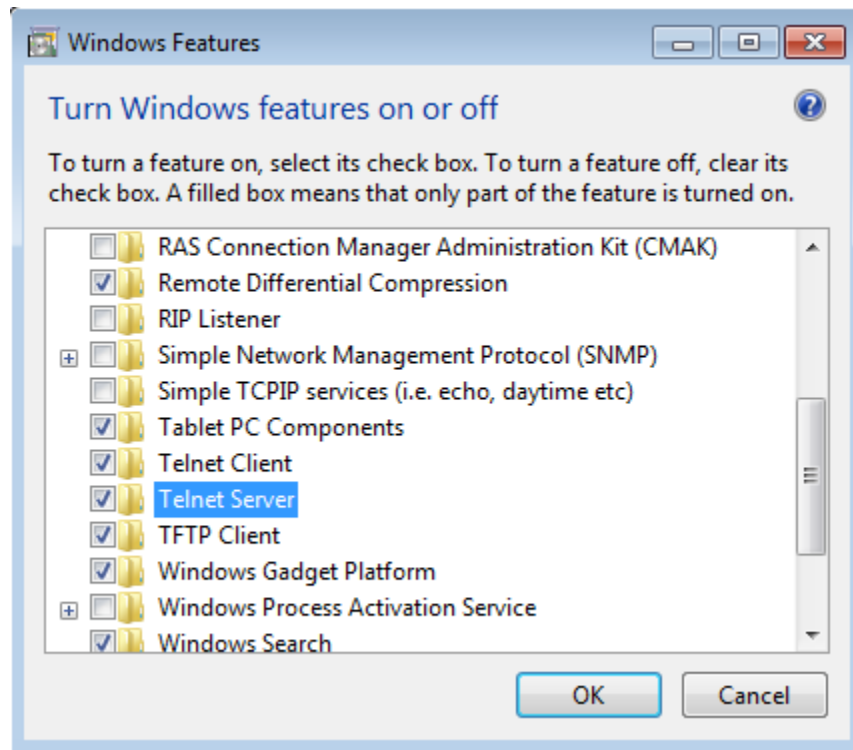
31. Click on the Programs link within the Control Panel.



32. Click on the link to **Turn Windows features on or off**.



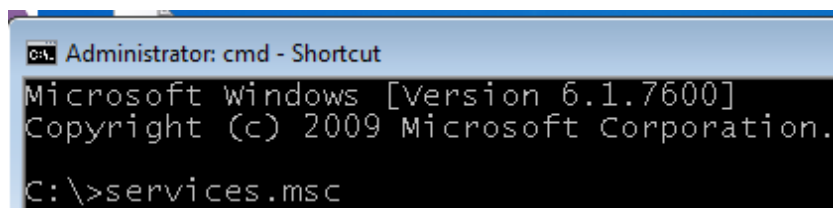
33. Find **Telnet Server** in the list (alphabetical) Check the box and click OK.



34. After the Telnet Server feature completes, open a command prompt by clicking on the shortcut on the desktop.

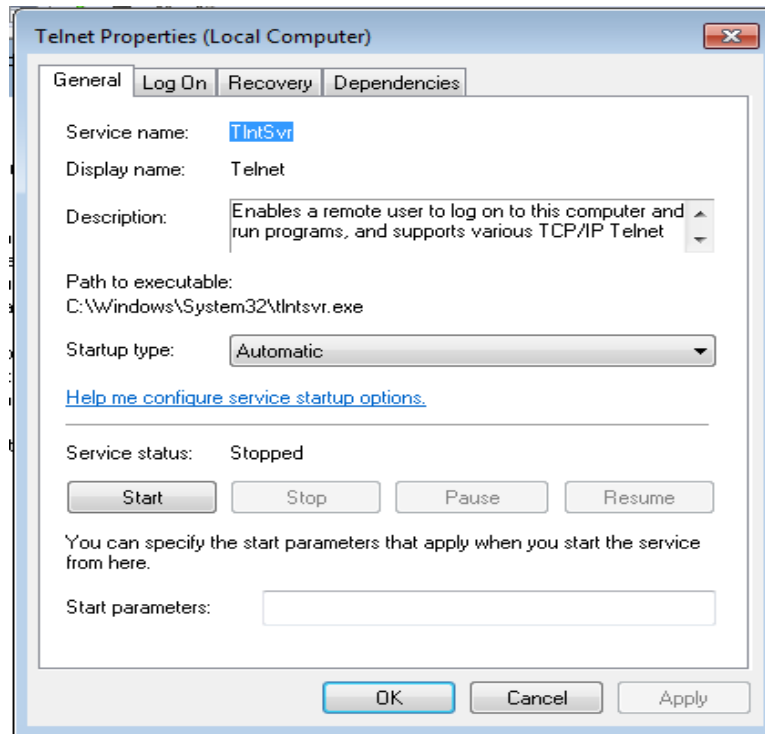


35. Type the following command to launch the services console:  
C:\>**services.msc**





36. Scroll down and find Telnet in the list. Right-click Telnet and then click Properties. Change the Startup type to **Automatic**. Click the **Apply** button and then click the **Start** button. Close Telnet properties and Services.



37. Type the following command to determine if telnet is listening:

C:\>netstat -an | find "23" | find "TCP"

```
C:\>netstat -an | find "23" | find "TCP"
TCP    0.0.0.0:23          0.0.0.0:0          LISTENING
TCP    [::]:23           [::]:0             LISTENING
```

38. Go back to the **Windows 8 Internal Machine** command prompt and type the following to telnet to the Windows 7 External Machine.

C:\>telnet 216.1.1.200

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

C:\>telnet 216.1.1.200_
```

39. Click **y** to the security warning message from the TELNET server.

```
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):
```

You are automatically logged in, because both the Windows 7 External Machine and the Windows 8 Internal Machine have the same user name: student, with the same password: **password**.

```
*=====
Microsoft Telnet Server.
*=====
C:\Users\student>_
```

## 1.2 Conclusion

The Linux based firewall is allowing all outbound traffic. We tested outbound PING, FTP, HTTP, TELNET, TFTP, and SSH, and in each case, the outbound traffic was allowed.

## 1.3 Discussion Questions

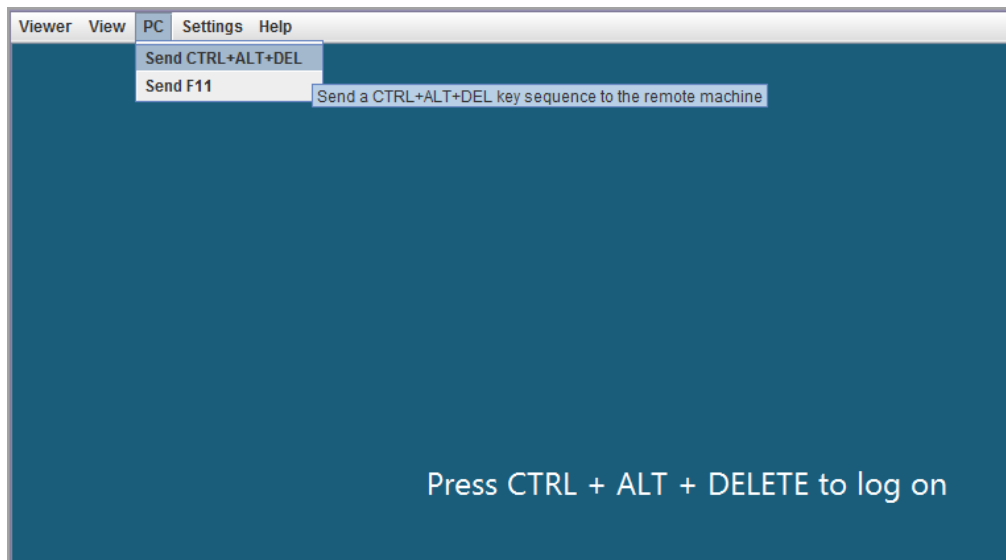
1. What needs to be done to configure a TELNET server on Windows 7?  
**Ans: Configure TELNET server on windows 7 from services.msc and change type to automatically.**
2. What needs to be done so that SSHD can be configured on BackTrack?  
**Ans: To configure SSHD services Start SSHD service and enter sshd-generate**
3. What protocol covered in this section uses UDP instead of TCP?  
**Ans: Protocol covered in this section is TFTP**
4. Which ports do FTP, TELNET, SSH, HTTP, and TFTP utilize?  
**Ans: The port used are:**  
**FTP: Port 25**  
**Telnet: Port 23**  
**SSH: Port 22**  
**HTTP: Port 80**  
**TFTP: Port 69**

## 2 Installing the Linux Based Firewall

In this step, we will install the Linux Community Edition Endian Firewall. This firewall will restrict some of the outbound access so users do not use any clear-text protocols (Except HTTP).

### 2.1 Configuring the Firewall

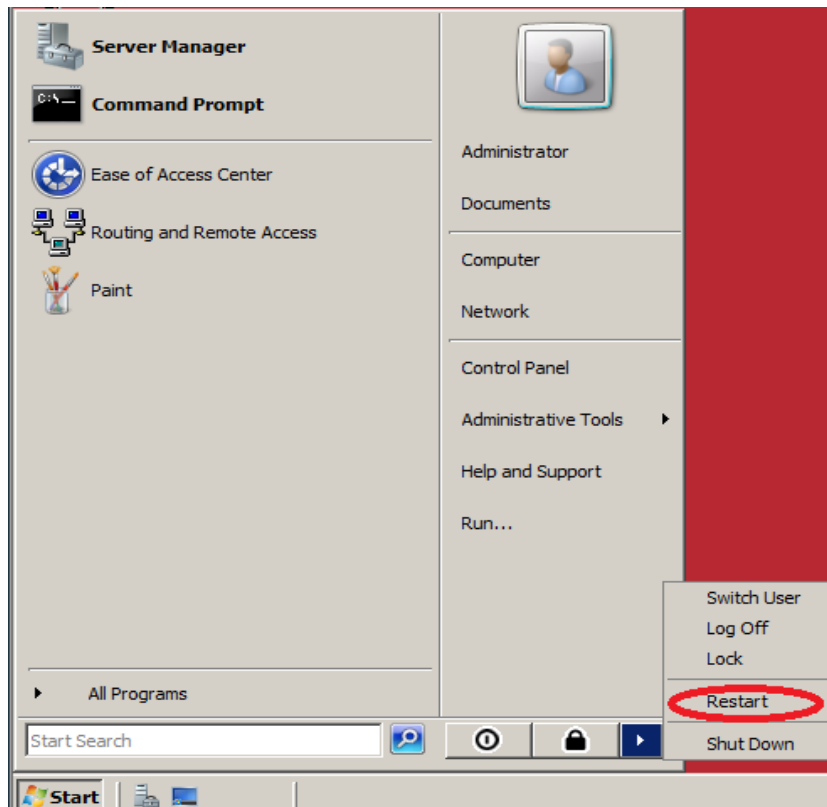
1. Log into the **Windows 2008 Server Firewall** by clicking on the **Windows 2008 Firewall** icon on the topology. Click PC, then **Send Ctrl+Alt+Del** in the top- left corner of the screen in order to log on to the Windows 2008 server.



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



3. Click on the start button. Click the arrow to the far right and select **Restart**.



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



5. At the Linux boot prompt, type the word **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

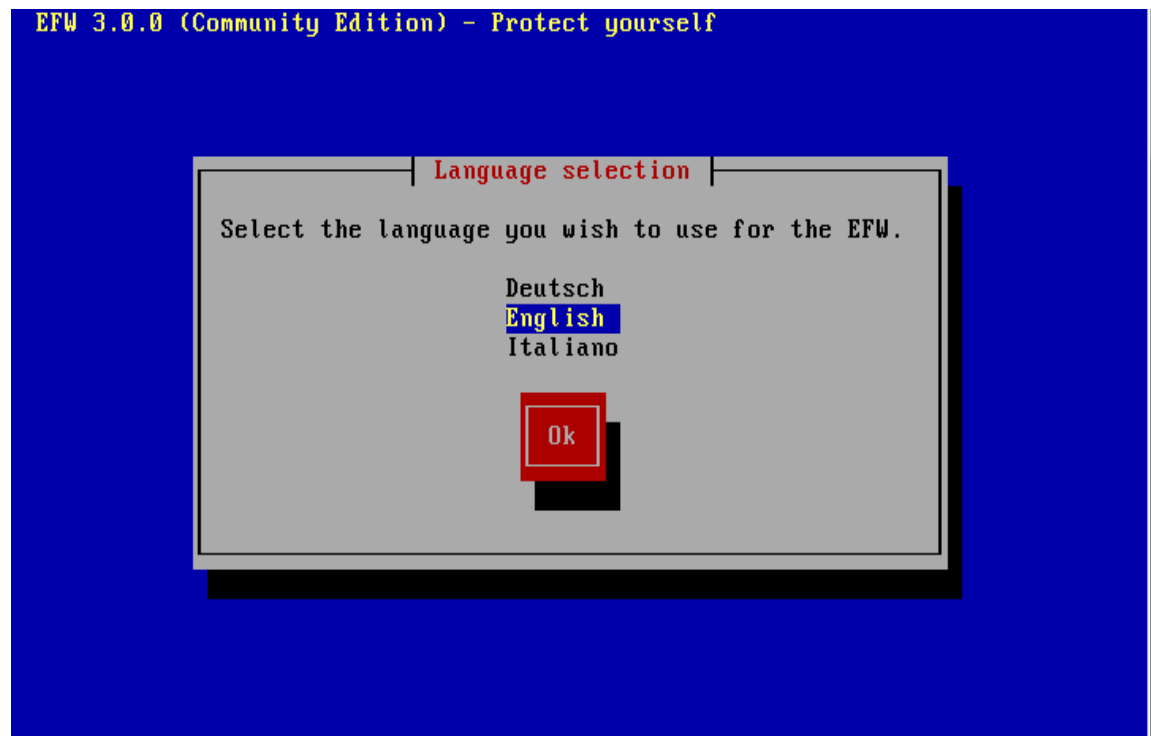
Welcome to Endian Firewall, Licensed under GNU GPL version 2.

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

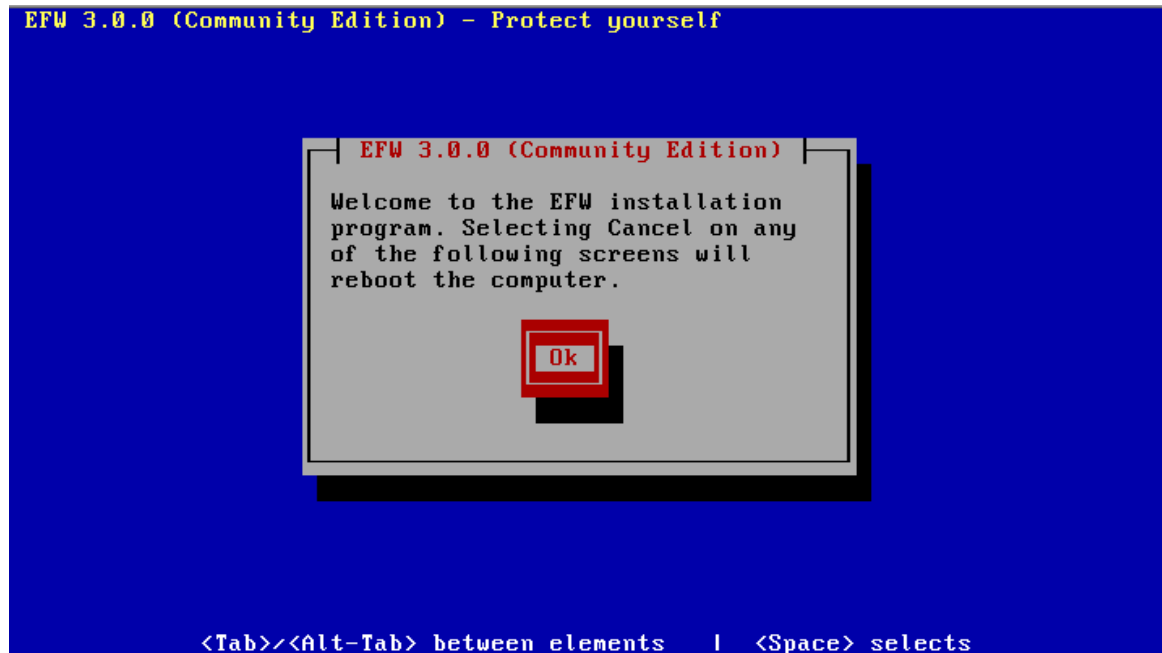
-----
----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
----
-----

Type: install to install
boot: install_
```

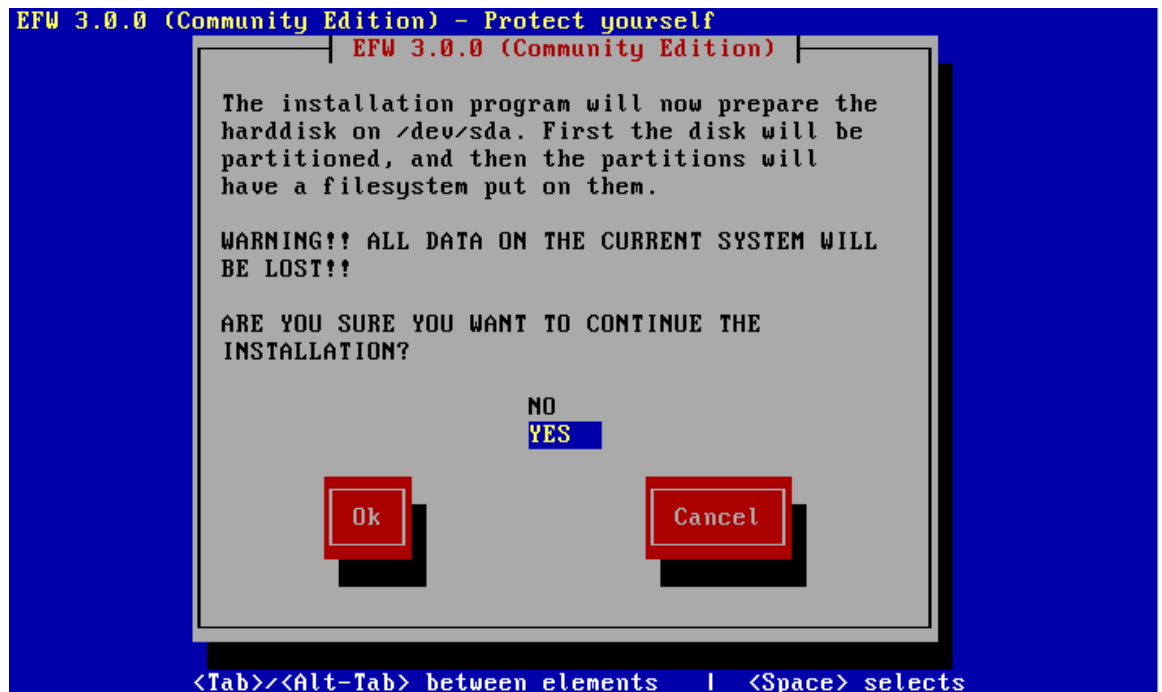
6. Press the Enter button to select **English** at the Language selection screen.



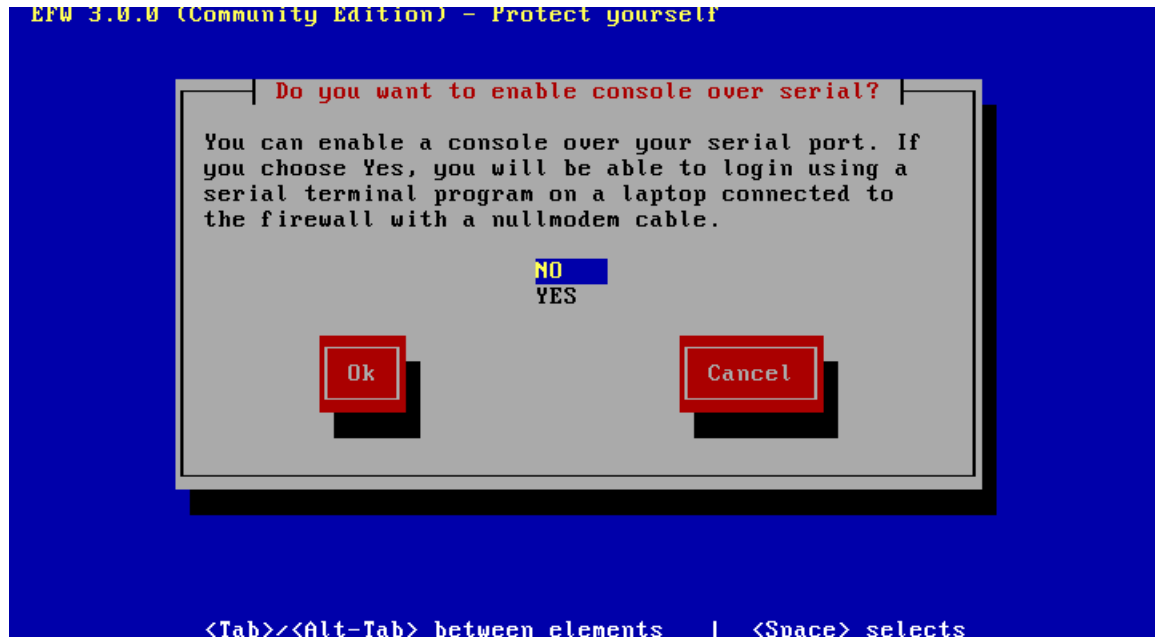
7. Press Enter at the Welcome to the EFW Installation program screen.



8. At the **Prepare the Hard Disk** screen, select **Yes** and then press the **Enter** button.

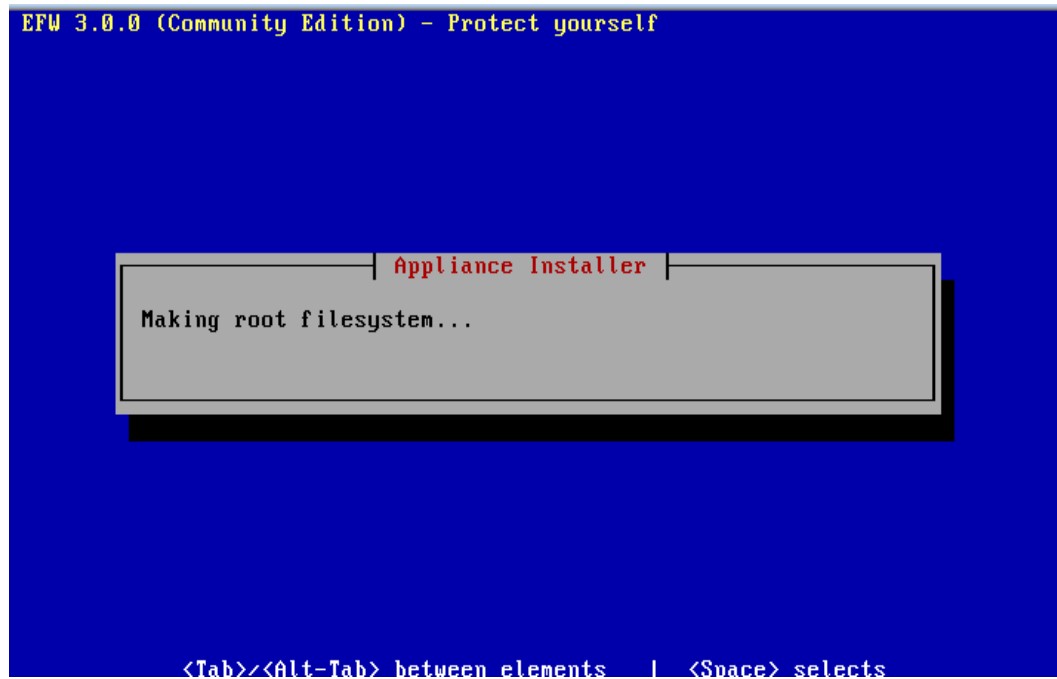


9. Press Enter to No Console Access over a serial port.

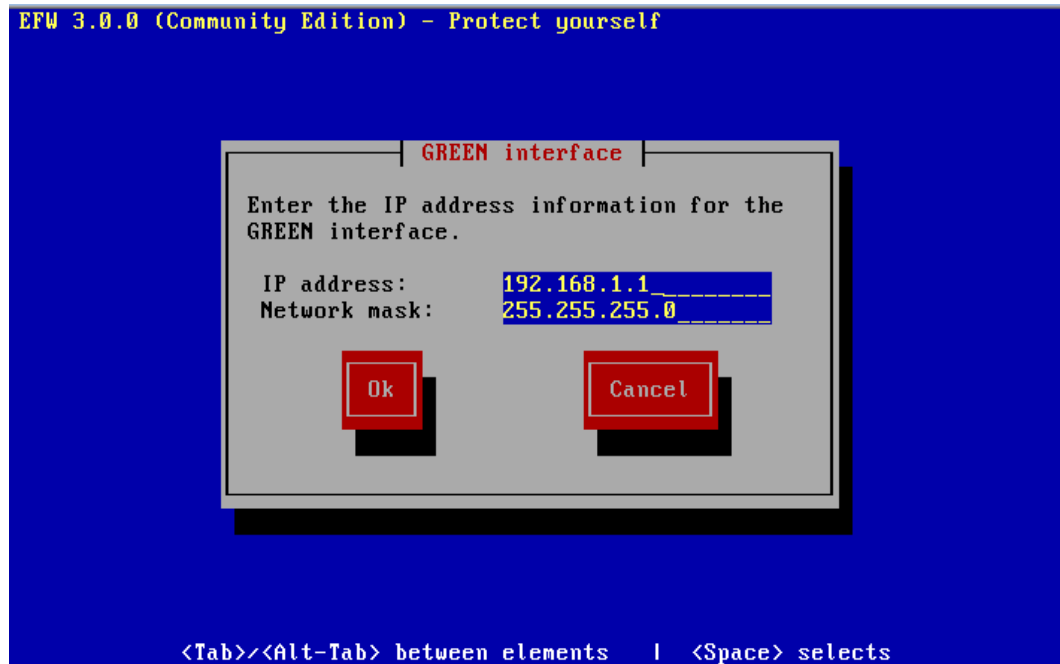


10. EFW will make the root file system and then will indicate that it is installing packages.

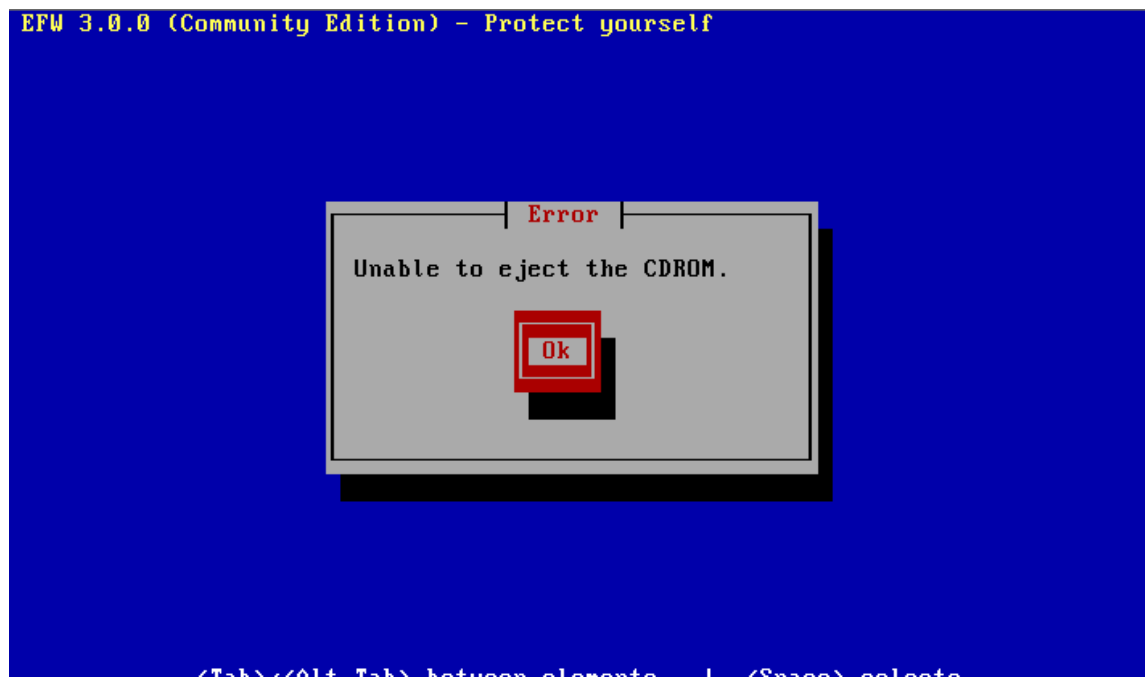
The entire process may take up to 15 minutes to complete.



11. For the GREEN Interface, type 192.168.1.1 as the IP address, press Enter twice and then once for OK. This installation may take a few minutes to complete.

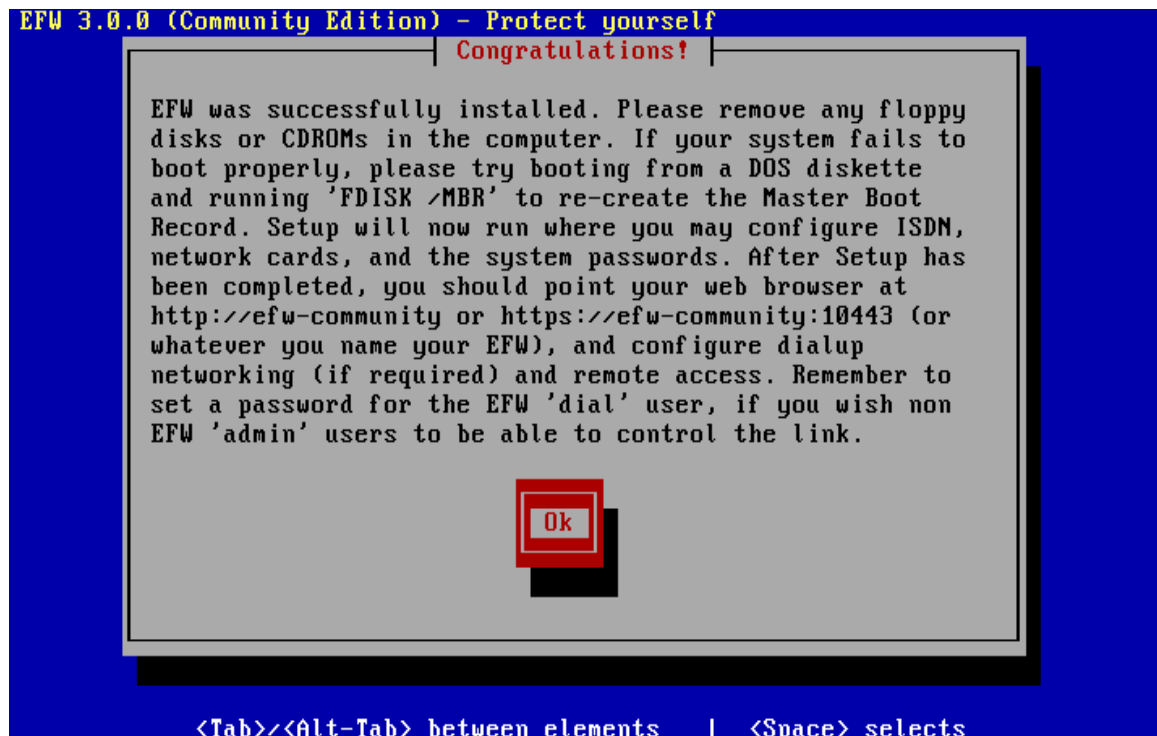


12. Press Enter for OK at the unable to eject the CD-ROM error.

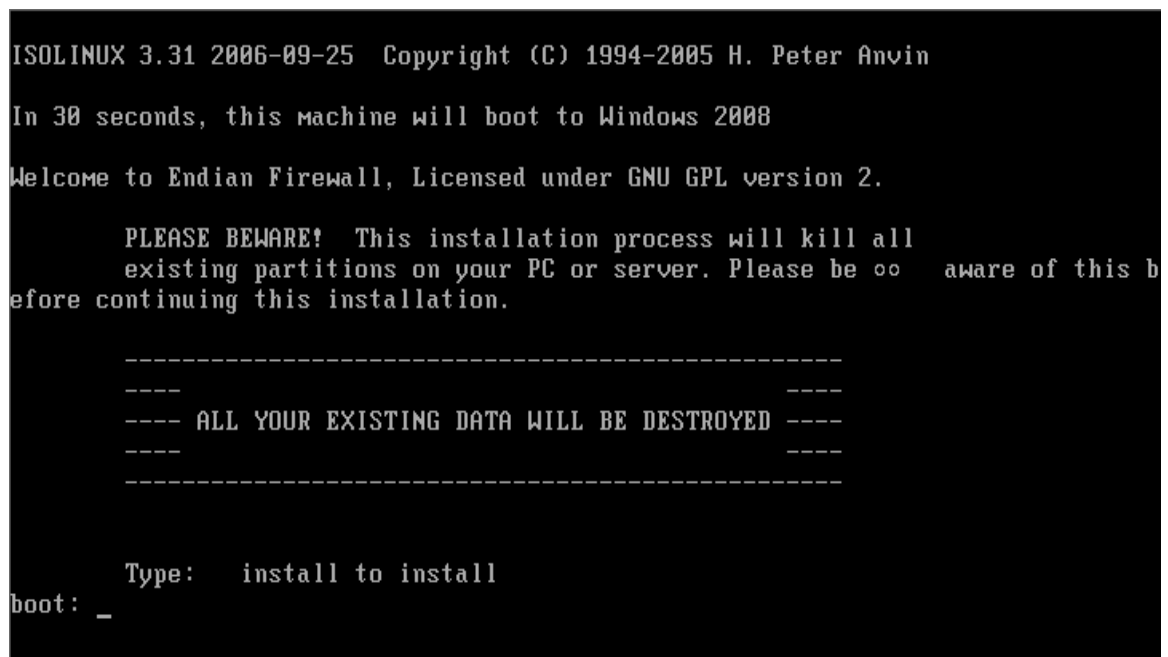




13. You will receive a message indicating EFW was successfully installed. Press Enter for Ok to reboot.



14. 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
-----

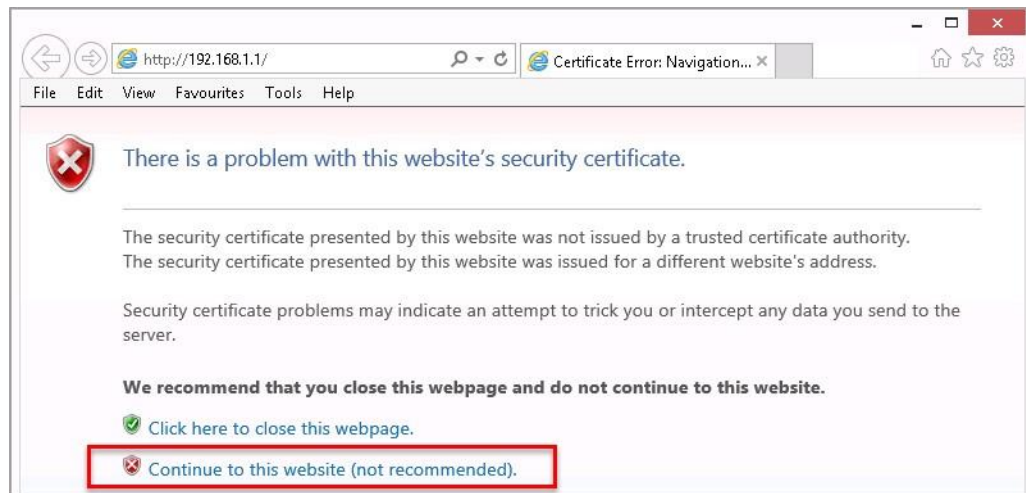
0) Shell
1) Reboot
2) Change Root Password
3) Change Admin Password
4) Restore Factory Defaults

Choice: _
```

15. Go back to the **Windows 8 Internal Machine** and click on the shortcut to Internet Explorer on the desktop.



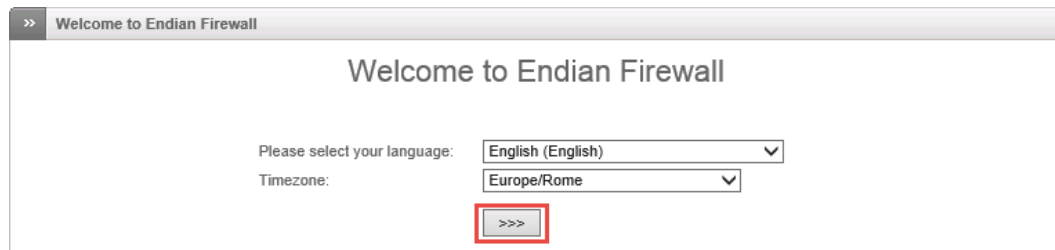
16. Go to the following URL: <http://192.168.1.1/>. Click **Continue to this Website**.



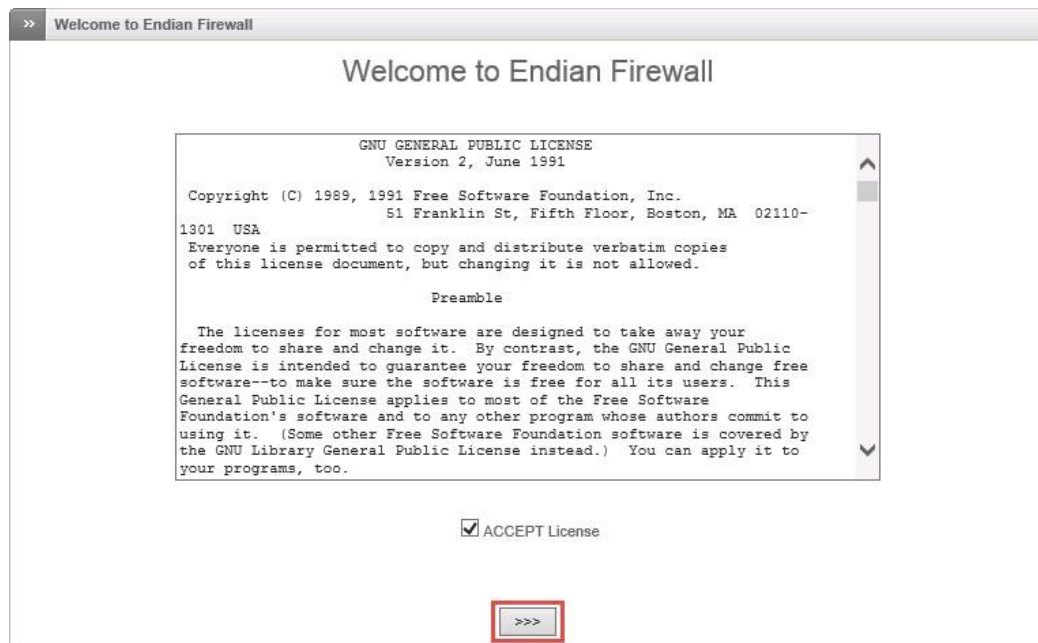
17. Click the >>> (Next) button at the Welcome to Endian Firewall.



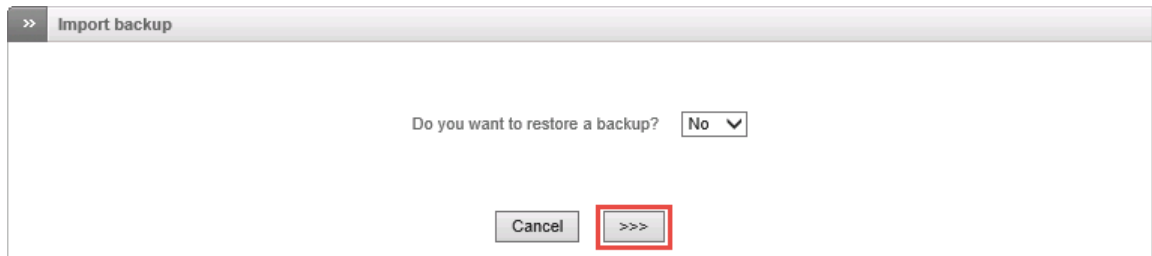
18. Click >>> at the select your language and select your time zone screen.



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



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




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



22. Select ETHERNET STATIC and click the >>> button.



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



24. 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 >>>

25. For the Red Interface, type **216.1.1.1**. For the network mask, select **255.0.0.0**. 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="checkbox"/> 1	✓	Intel ?	00:50:56:9c:a9:97	eth0
<input checked="" type="checkbox"/> 2	✓	Intel ?	00:50:56:9c:8a:94	eth1

Default gateway:

MTU:

Spoof MAC address with:

☒ This field may be blank.

<<< Cancel >>>

26. 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: 8.8.8.8

DNS 2: 8.8.8.8

<<< Cancel >>>

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



Network setup wizard

Step 6/8: Configure default admin mail

Admin email address:

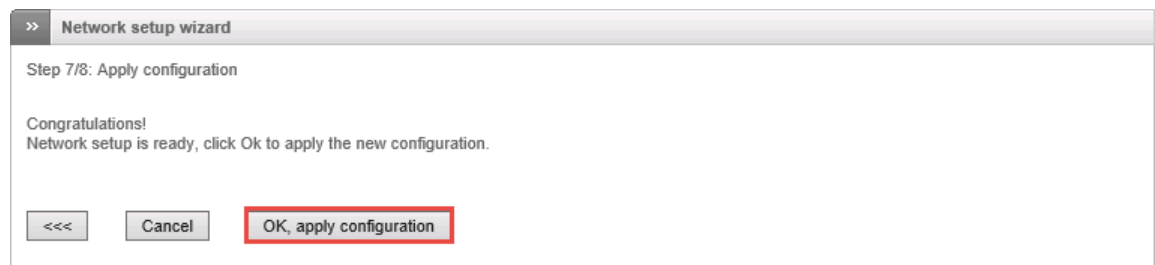
Sender email address:

Address of smarthost:

☒ This field may be blank.

<<< Cancel >>>

28. 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

29. Wait for the Network Setup page to reload.



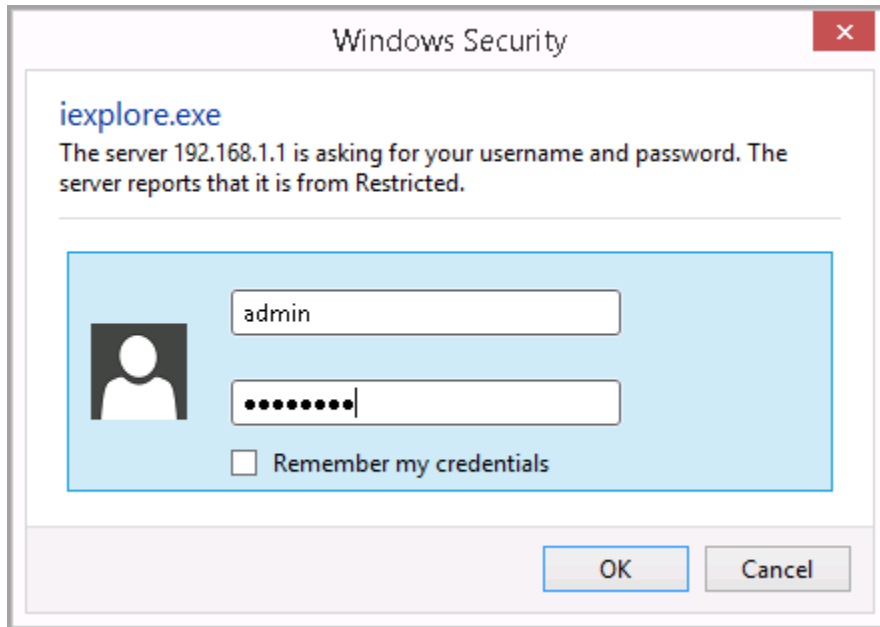
Network setup wizard

Step 8/8: End

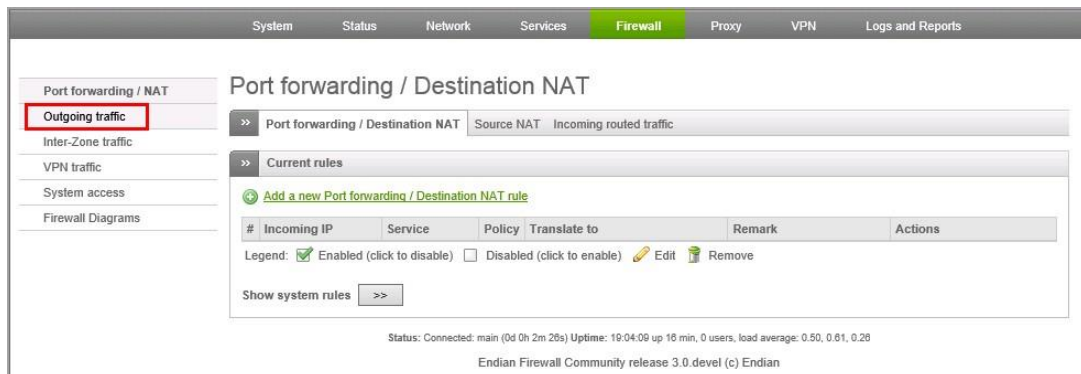
Your configuration has been saved. Please wait until the dependent services have been reloaded. This may take up to 20 seconds. Enjoy!

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.

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



31. Click the Firewall tab, then click on the **Outgoing traffic** link to the far left.



32. Examine the Outgoing Traffic Rules. The following protocols are allowed outbound:

Protocol	Port
HTTP	80
HTTPS	443
FTP	21
SMTP	25
POP3	110
IMAP	143
IMAPs	993
POP3s	995
DNS	53
PING	N/A

Outgoing firewall configuration

Current rules

[Add a new firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN BLUE	RED	TCP/80		allow HTTP	
2	GREEN BLUE	RED	TCP/443		allow HTTPS	
3	GREEN	RED	TCP/21		allow FTP	
4	GREEN	RED	TCP/25		allow SMTP	
5	GREEN	RED	TCP/110		allow POP	
6	GREEN	RED	TCP/143		allow IMAP	
7	GREEN	RED	TCP/995		allow POP3s	
8	GREEN	RED	TCP/993		allow IMAPs	
9	GREEN ORANGE BLUE	RED	TCP+UDP/53		allow DNS	
10	GREEN ORANGE BLUE	RED	ICMP/8 ICMP/30		allow PING	

33. Open the command prompt and type the following command on the Windows 8 Internal Machine 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
```



34. To verify the configuration, type the following command on the Windows 8 Internal Machine:
- C:\>nmap 216.1.1.200

```
C:\>nmap 216.1.1.200

Starting Nmap 5.51 ( http://nmap.org ) at 2014-08-01 19:16 Eastern Summer Time
Nmap scan report for 216.1.1.200
Host is up (0.00s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    open  http
110/tcp   closed pop3
143/tcp   closed imap
443/tcp   closed https
993/tcp   closed imaps
995/tcp   closed pop3s

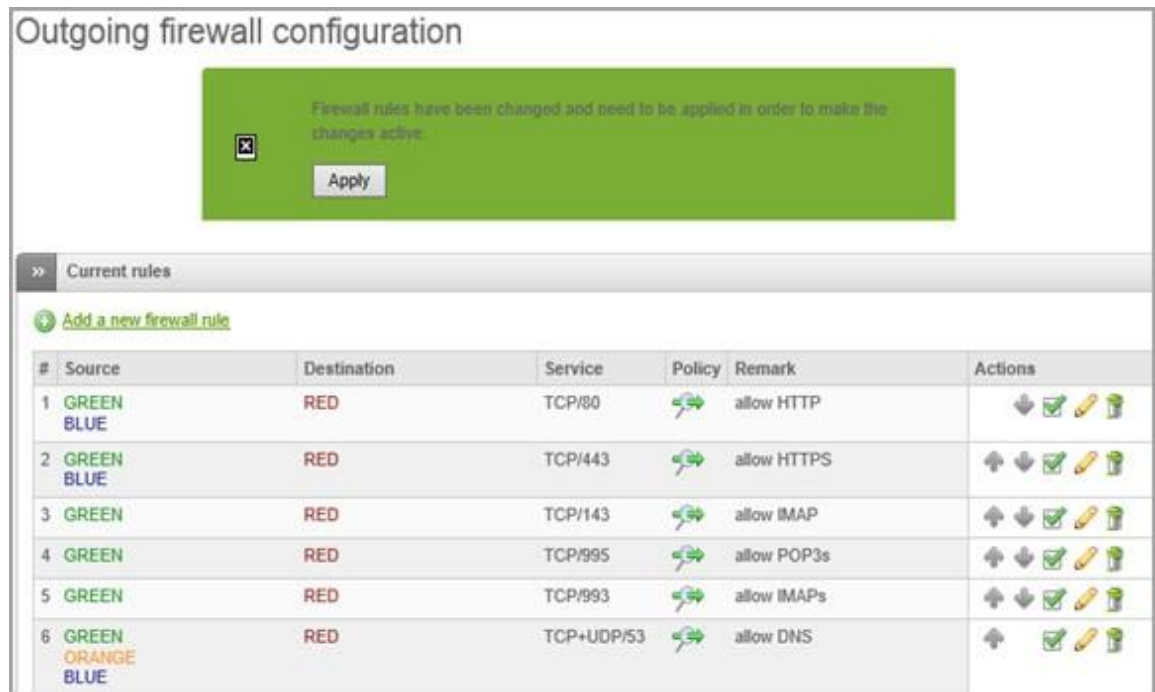
Nmap done: 1 IP address (1 host up) scanned in 18.00 seconds
```

Notice, only the ports listed appear in the list. Ports that are not open on BackTrack are showing as closed and ports that are open, like SSH, are not even showing up on the list.

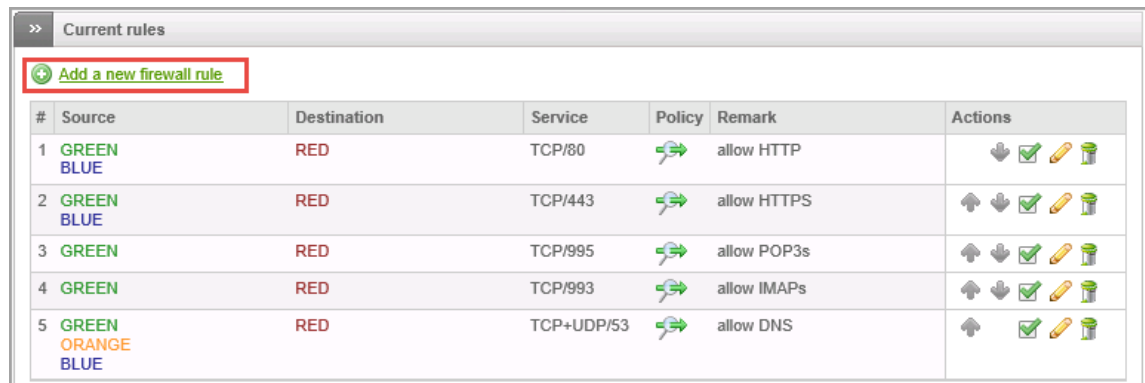
35. Return to the browser on the Windows 8 Internal Machine. Click the trash can to delete the rules allowing FTP, SMTP, POP, IMAP, and PING.

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN BLUE	RED	TCP/80		allow HTTP	
2	GREEN BLUE	RED	TCP/443		allow HTTPS	
3	GREEN	RED	TCP/21		allow FTP	
4	GREEN	RED	TCP/25		allow SMTP	
5	GREEN	RED	TCP/110		allow POP	
6	GREEN	RED	TCP/143		allow IMAP	
7	GREEN	RED	TCP/995		allow POP3s	
8	GREEN	RED	TCP/993		allow IMAPs	
9	GREEN ORANGE BLUE	RED	TCP+UDP/53		allow DNS	
10	GREEN ORANGE BLUE	RED	ICMP/8 ICMP/30		allow PING	

36. Click **Apply** to Apply the configuration.



37. Click Add a new Firewall rule.



38. Under Source Type, select **Zone/Interface**, and select **GREEN**. Under Service, select **SSH** from the drop down menu list. Click the create rule button.

Outgoing firewall rule editor

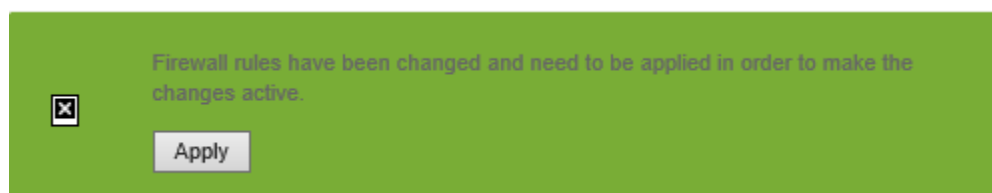
Source Type \* **Zone/Interface**   
 Select interfaces (hold CTRL for multiselect)   
**GREEN**   
 Interface 1 (Zone: GREEN)

Destination Type \* **<RED>**   
 This rule will match the entire RED

Service/Port   
 Service \* **SSH** Protocol \* **TCP** Destination port (one per line)   
 22

Policy \*   
 Action **ALLOW with IPS** Remark   
 Position \* **Last**   
☒ Enabled ☐ Log all accepted packets   
 Create rule or Cancel \* This Field is required.

39. Click **Apply** to Apply the New Firewall Rule.



40. Click Add a new Firewall rule.

>> Current rules

**Add a new firewall rule**

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN BLUE	RED	TCP/80		allow HTTP	
2	GREEN BLUE	RED	TCP/443		allow HTTPS	
3	GREEN	RED	TCP/995		allow POP3s	
4	GREEN	RED	TCP/993		allow IMAPs	
5	GREEN ORANGE BLUE	RED	TCP+UDP/53		allow DNS	

41. Under Source Type, select **Zone/Interface**, and select **GREEN**. Under Protocol, select **ICMP** from the drop-down menu list. Under Policy, select **DENY**. Click Create rule.

Outgoing firewall rule editor

Source Type \* **Zone/Interface**  
Select interfaces (hold CTRL for multiselect)  
**GREEN**  
interface 1 (Zone: GREEN)

Destination Type \* **<RED>**  
This rule will match the entire RED

Service/Port  
Service \* **User defined** Protocol \* **ICMP** Destination port (one per line)

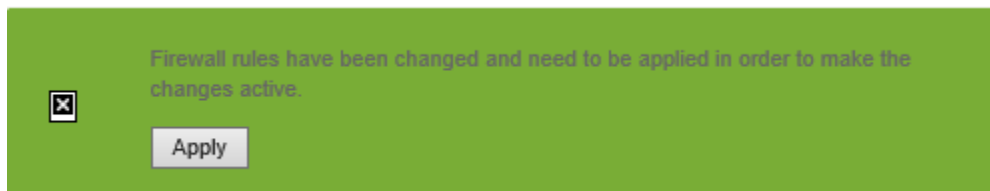
Policy \*  
Action **DENY** Remark  Position \* **Last**

☒ Enabled ☐ Log all accepted packets

or

\* This Field is required.

42. Click **Apply** to Apply the New Firewall Rule.



## 2.2 Conclusion

The Linux based firewall was allowing all outbound traffic. Endian Community Firewall has much tighter outbound restrictions that can be adjusted as needed.

## 2.3 Discussion Questions

1. What is the difference between the GREEN and the RED Interface?  
**Ans: Green interface connects only to the computer that IPCOP is protecting while RED interface connects to Green, Blue, Orange networks and there computers from traffic originating on the network.**
2. Does Domain Name System (DNS) use TCP, UDP, or both?  
**Ans: Uses TCP and UDP.**
3. Does the Endian Community Firewall allow SSH out by default?  
**Ans: It will be disabled by default. By clicking the checkmark in the box you will activate remote SSH access.**
4. Which ports do IMAPs and POPs utilize?  
**Ans: POP uses port 110 and 995 , IMAP uses port 143 and 993.**

### 3 Testing External Services on the Linux Based Firewall

The Windows firewall was currently set up to allow all outbound traffic. The Linux Community Edition Endian Firewall has more restrictive outbound filters, and the filters can be altered further to add or delete additional protocols from the outbound list.

#### 3.1 Testing the Firewall

Blocking certain outbound traffic can increase a network's security.

1. Type the following from the Windows 8 Internal Machine to test outbound ping:

C:\>**ping 216.1.1.200**

```
C:\>ping 216.1.1.200
Pinging 216.1.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

The Linux Endian Firewall is denying ICMP traffic.

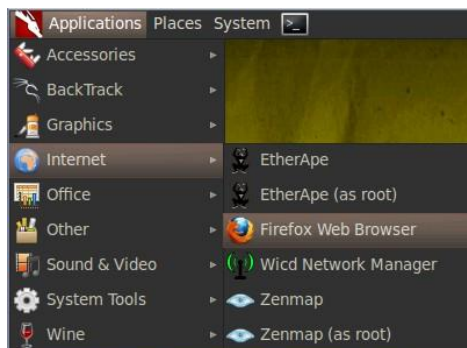
2. To test outbound FTP connectivity from the Windows 8 Internal Machine, type:

C:\>[ftp 216.1.1.100](#)

Type **bye** to exit the FTP session

```
C:\>ftp 216.1.1.200
> ftp: connect :Connection timed out
ftp>
```

3. On the BackTrack 5r3 Internal Machine, navigate back to the Firefox Web Browser. If not already opened, click **Applications > Internet > Firefox Web Browser**.



4. Type **http://216.1.1.200** in the URL bar to connect to the external web site.



5. On the Windows 8 Internal Machine, type the following command to attempt the TFTP transfer:

C:\> **tftp 216.1.1.200 get tftp.txt**

```
C:\>tftp 216.1.1.200 get tftp.txt
Timeout occurred
Connect request failed
```

6. Type the following command to attempt to TELNET:

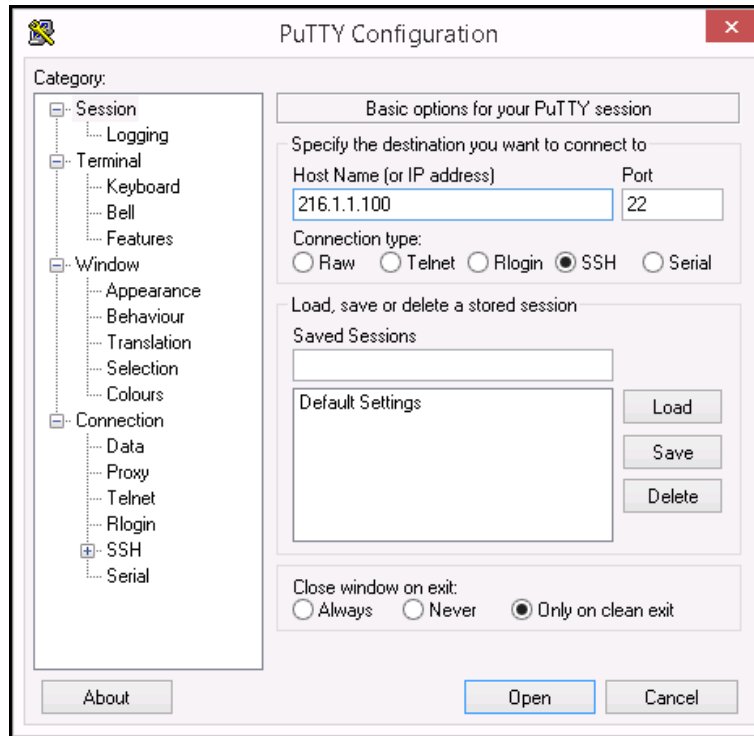
C:\>**telnet 216.1.1.200**

```
C:\>telnet 216.1.1.200
Connecting To 216.1.1.200...Could not open connection to the host, on port 23: C
onnect failed
```

7. On the desktop, double-click on the putty.exe application.



8. Enter 216.1.1.100 for the Host Name and click the Open button.



9. For the username, type **root** and for the password, type **toor**. Type **exit**.



10. Close all open windows and PC viewers, then end the reservation.



## 3.2 Conclusion

The Linux based firewall is allowing users to connect to HTTP and SSH servers, but not TFTP, FTP, or TELNET servers. Outbound ping is also not allowed out of the network.

## 3.3 Discussion Questions

1. Why might it be a good idea to block PING?  
**Ans: PING is a utility of command line it is available in every operating system. It sends the request to network to connect virtually. This might cause in damaging the system. Disabling is easy.**
2. Why might it be a good idea to block TELNET?  
**Ans: It is sending a Plain text through the local network. So, it's not secure .**
3. Why might it be a good idea to block TFTP?  
**Ans: Security and Visibility are the major disadvantage of TFTP. So, it's a good idea to block TFTP.**
4. Why might it be a good idea to block FTP?  
**Ans: It is the reason for unauthorized access as it doesn't encrypt username and password.**

## 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/>

