NETWORK SECURITY LAB SERIES

Lab 7: Configuring a Virtual Private Network with OpenVPN

Document Version: 2015-09-28

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

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. Installing the Firewall and Configuring the VPN Server
2. Configuring the VPN Server and Clients
3. Using Internal Services from an External Machine

Key terms for this lab:

PPTP – Point to Point tunneling protocol is an older VPN technology that allows remote users to connect to a company's VPN server and access internal resources.

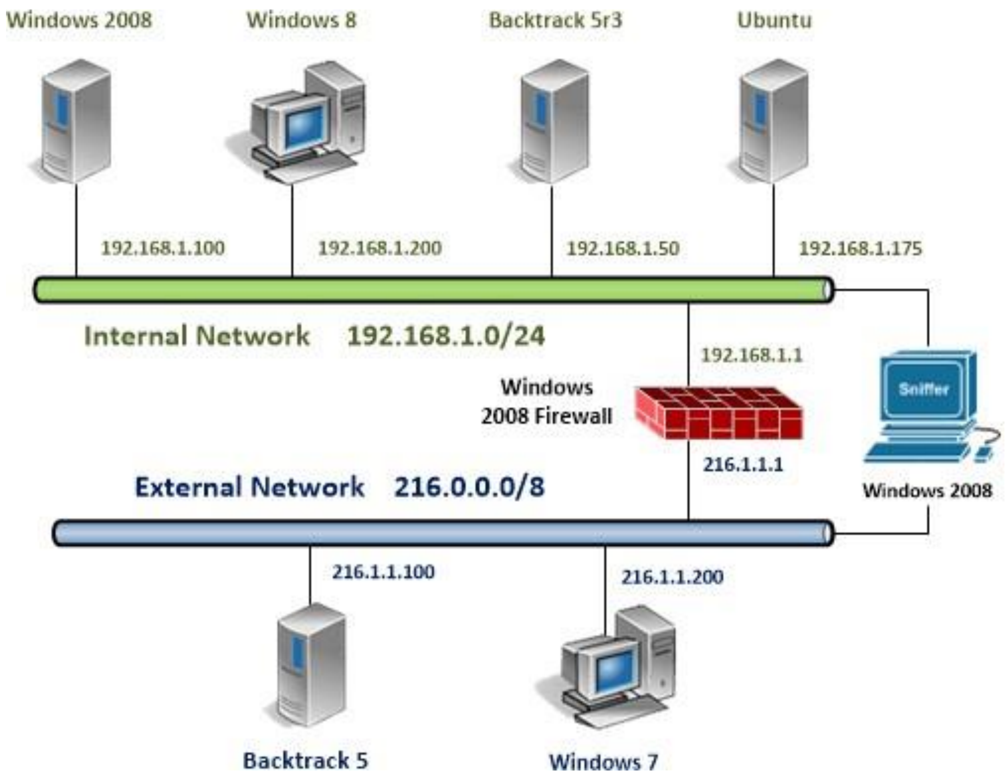
L2TP – Layer 2 tunneling protocol is a VPN technology that uses IPsec and allows remote users to connect to a company's VPN server and access internal resources.

VPN – Most firewalls can be configured to allow incoming traffic on their external interfaces to be redirected to internal hosts.

NAT – Network Address Translation will allow internal hosts to reach the external network through a single IP address. Most firewalls can be configured to perform NAT.

IPsec – IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

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 External Machine	216.1.1.100	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
Windows 2008 Sniffer	n/a	administrator	sniffer

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.

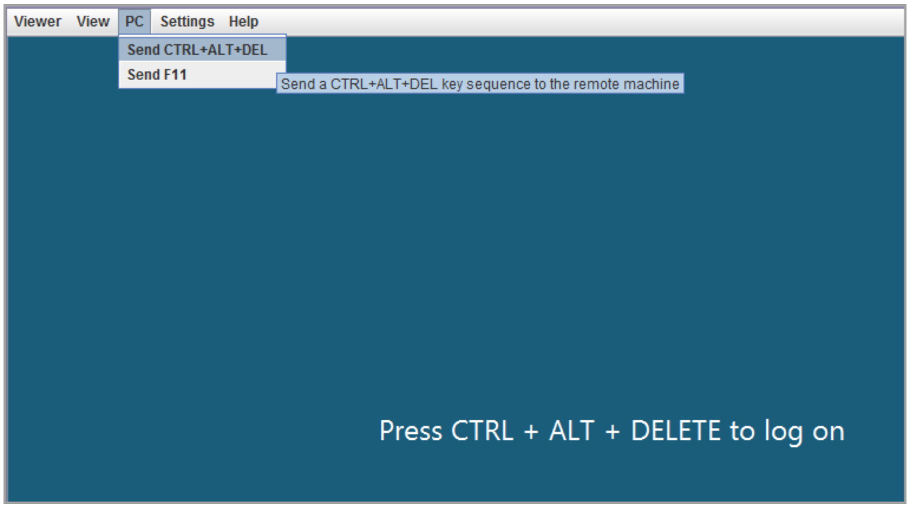
At the end of the lab, remember to close all open windows and close the PC viewers.

1 Installing the Linux Firewall

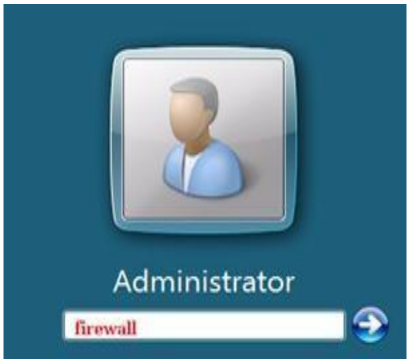
In this section, we install the Linux Endian Community Firewall. Then we will configure it as a VPN server. After the VPN server is configured, the clients will also need configuring. After connecting, authorized external users can access internal resources.

1.1 Testing the Current Firewall and Setting up the VPN Server

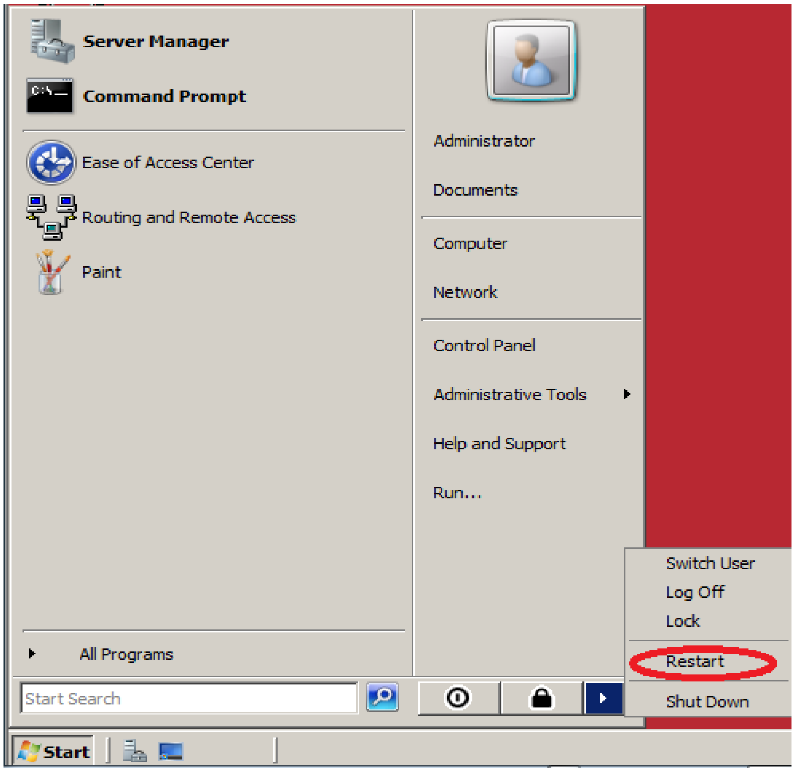
1. Log on to the **Windows 2008 Firewall** by clicking on the Windows 2008 Firewall icon on the topology. Click **PC,** and then **Send Ctrl+Alt+Del** in the top-left corner of the screen in order to log on to the Windows 2008 server.


Viewer
View
PC
Settings
Help
Send CTRL+ALT+DEL
Send F11
Send a CTRL+ALT+DEL key sequence to the remote machine
Press CTRL + ALT + DELETE to log on

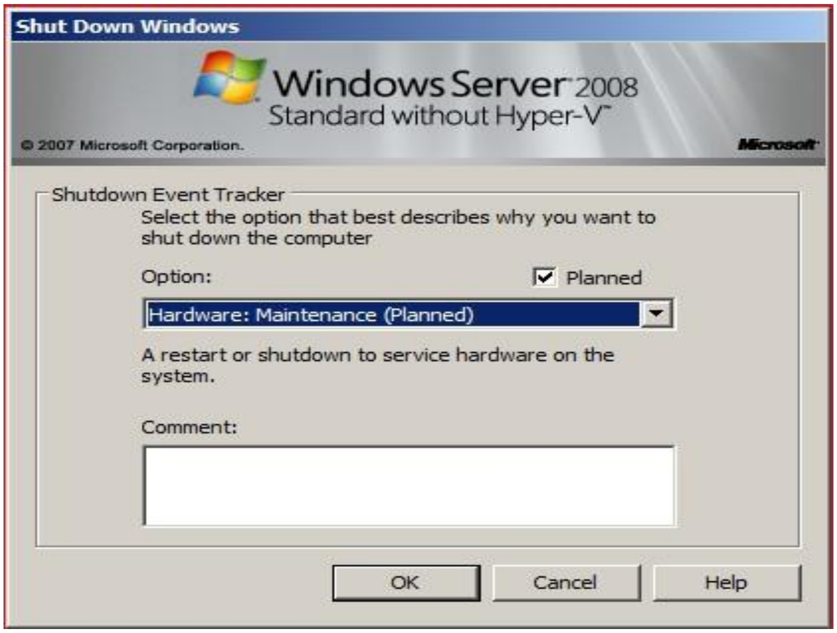
2. Enter **firewall** for the Administrator password to the Windows 2008 Server.



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.



Shutdown Event Tracker

Select the option that best describes why you want to shut down the computer

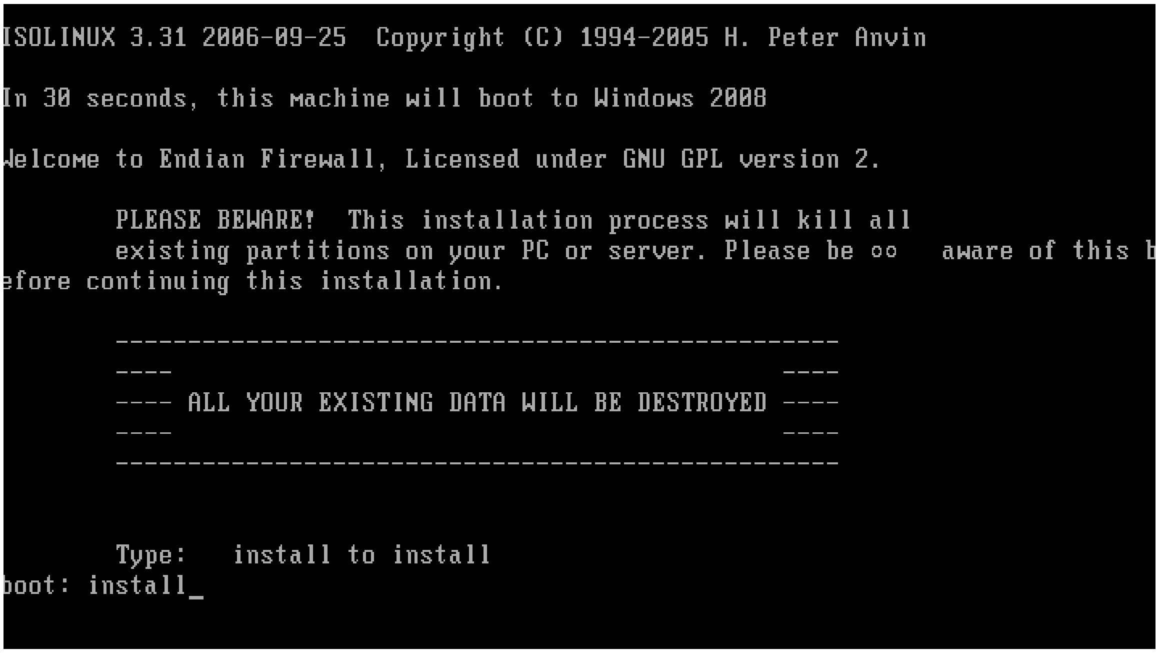
Option: ☑ Planned

Hardware: Maintenance (Planned)

A restart or shutdown to service hardware on the system.

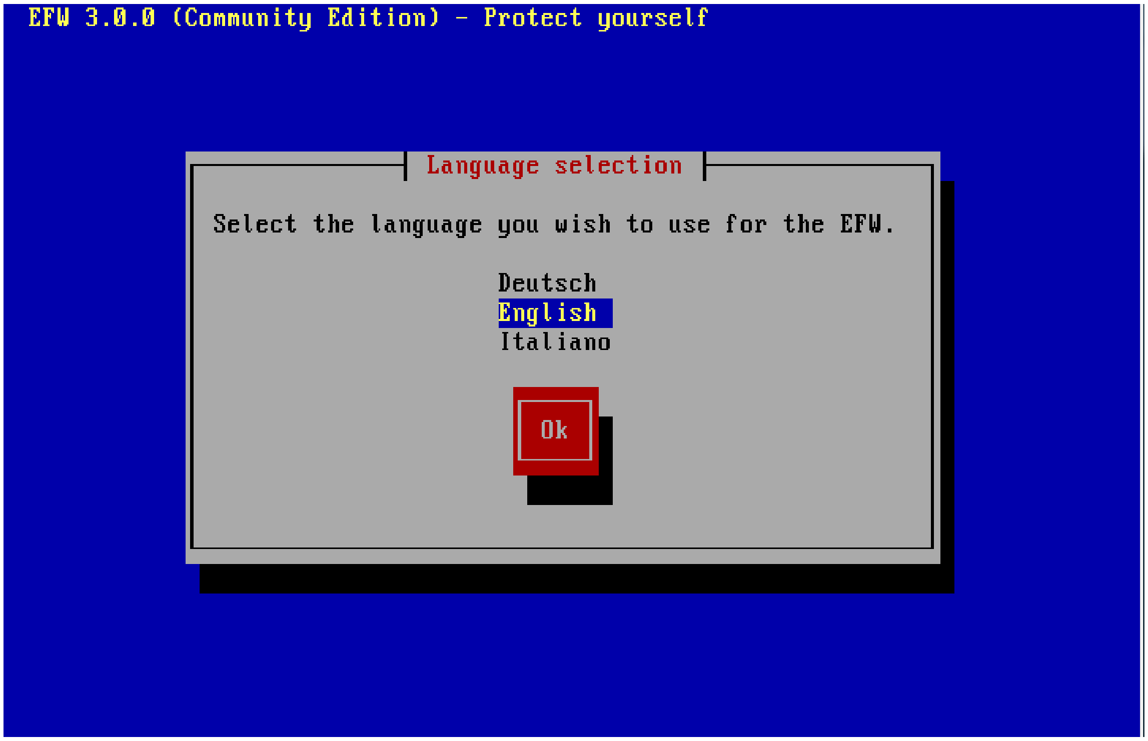
Comment:

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 oo   aware of this b
efore continuing this installation.

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


        Type:   install to install
boot: install_
```

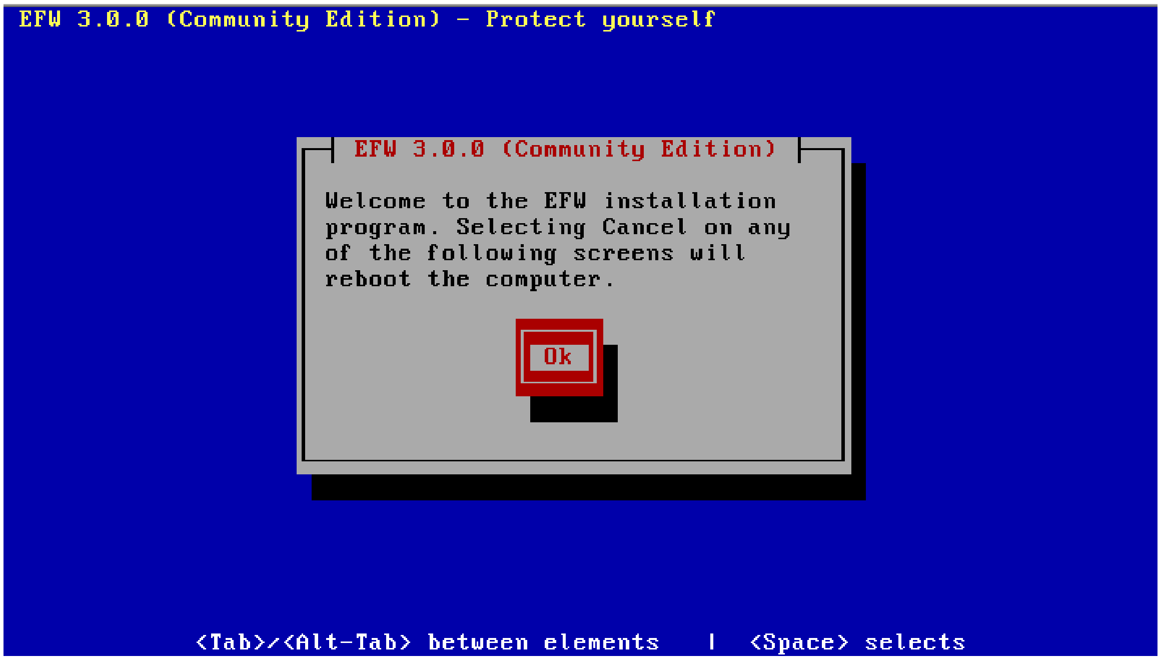
6. Press the Enter button for **English** at the Language selection screen.



EFW 3.0.0 (Community Edition) - Protect yourself

Select the language you wish to use for the EFW.

7. Press Enter for Ok at the **Welcome to the EFW Installation** screen.

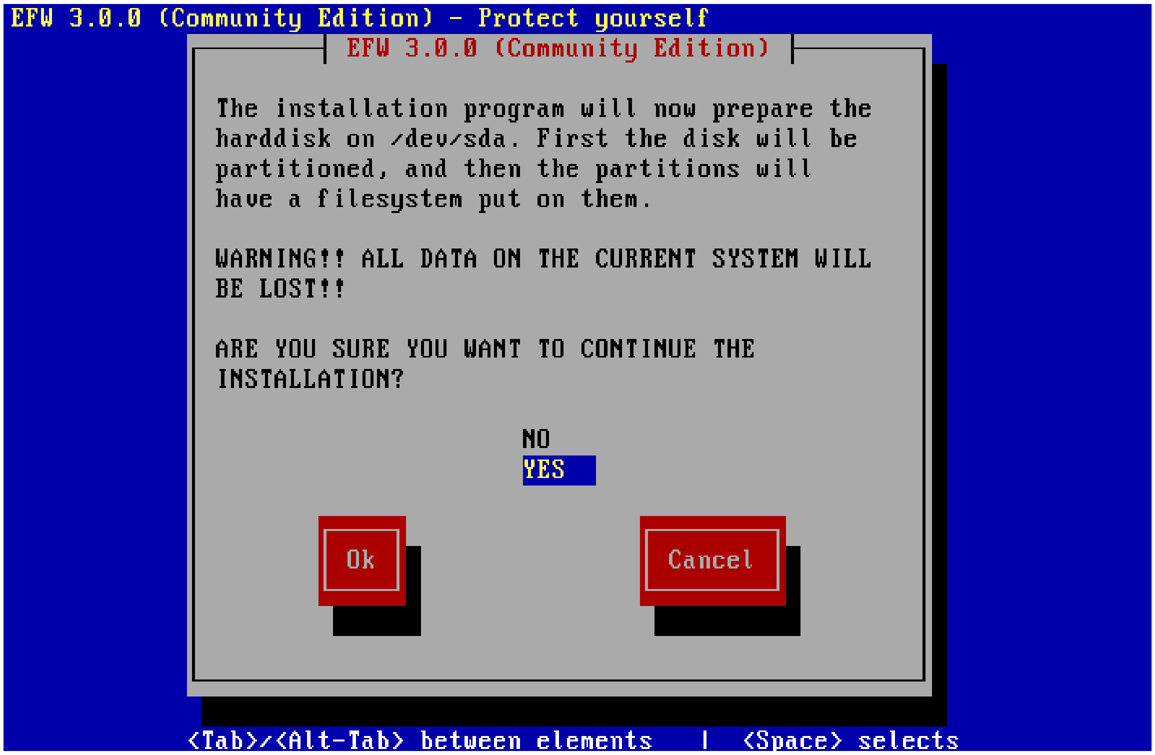


EFW 3.0.0 (Community Edition) - Protect yourself

EFW 3.0.0 (Community Edition)

Welcome to the EFW installation program. Selecting Cancel on any of the following screens will reboot the computer.

8. At the **prepare the hard disk** screen, select Yes and then press the OK button.



EFW 3.0.0 (Community Edition) - Protect yourself

EFW 3.0.0 (Community Edition)

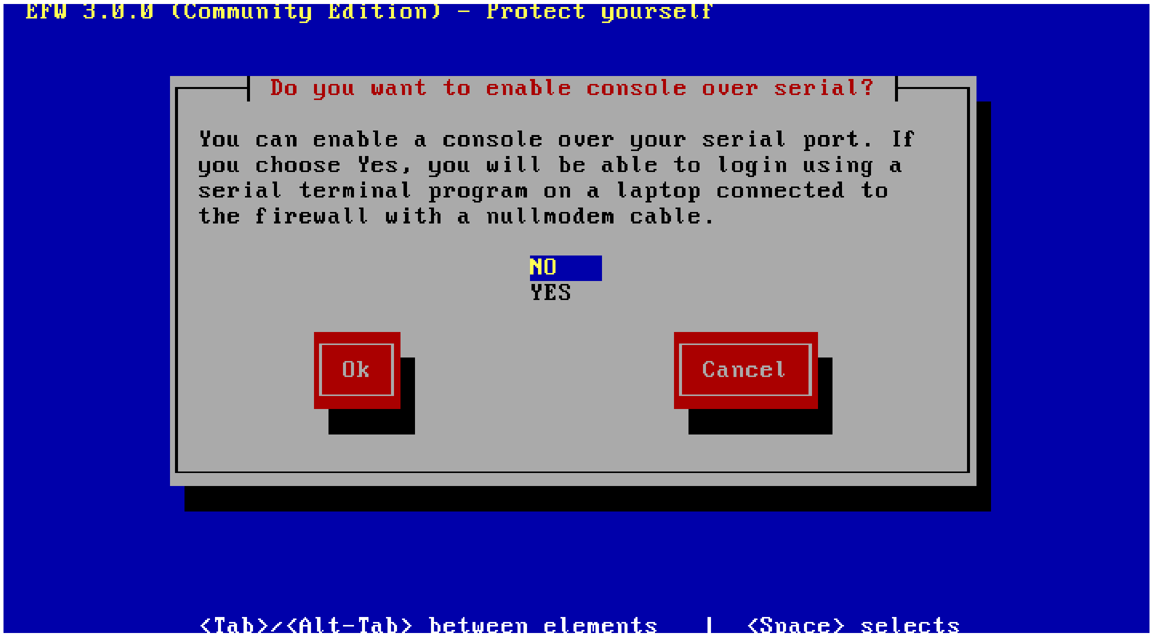
The installation program will now prepare the harddisk on /dev/sda. First the disk will be partitioned, and then the partitions will have a filesystem put on them.

WARNING!! ALL DATA ON THE CURRENT SYSTEM WILL BE LOST!!

ARE YOU SURE YOU WANT TO CONTINUE THE INSTALLATION?

NO
YES

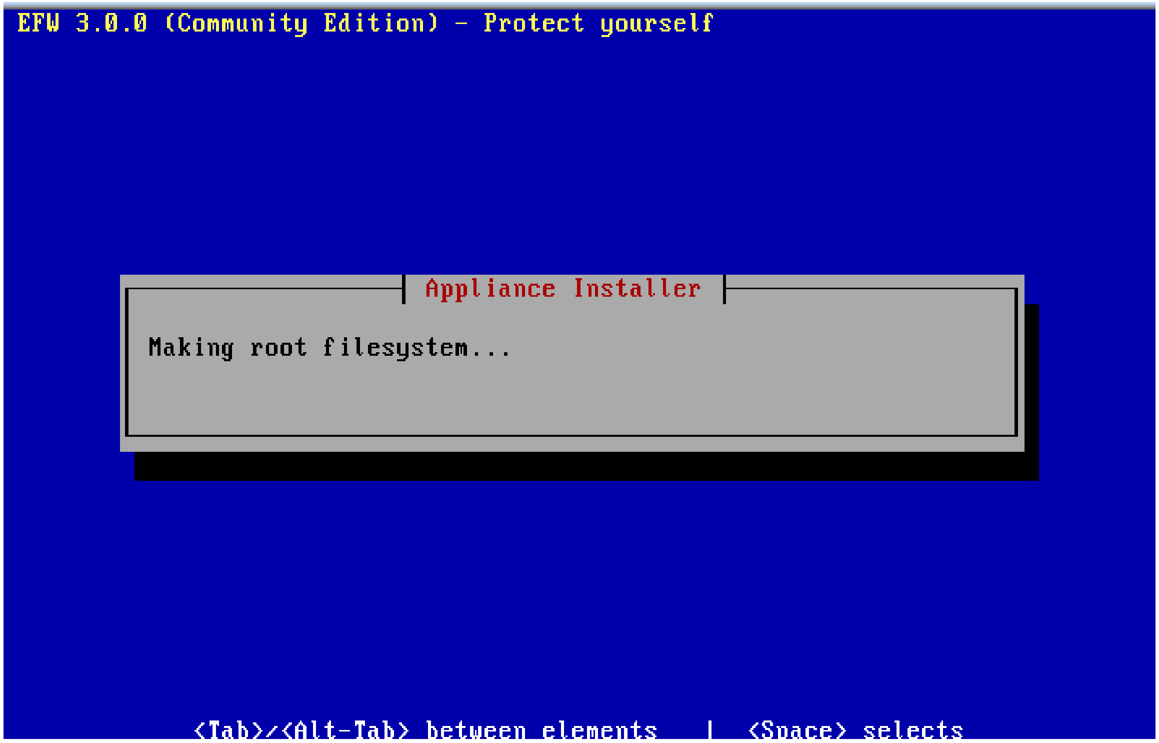
9. Press OK for **No** Console Access over a serial port.



```
EFW 3.0.0 (Community Edition) - Protect yourself

Do you want to enable console over serial?

You can enable a console over your serial port. If
you choose Yes, you will be able to login using a
serial terminal program on a laptop connected to
the firewall with a nullmodem cable.

NO
YES

<Tab>/<Alt-Tab> between elements   |  <Space> selects
```

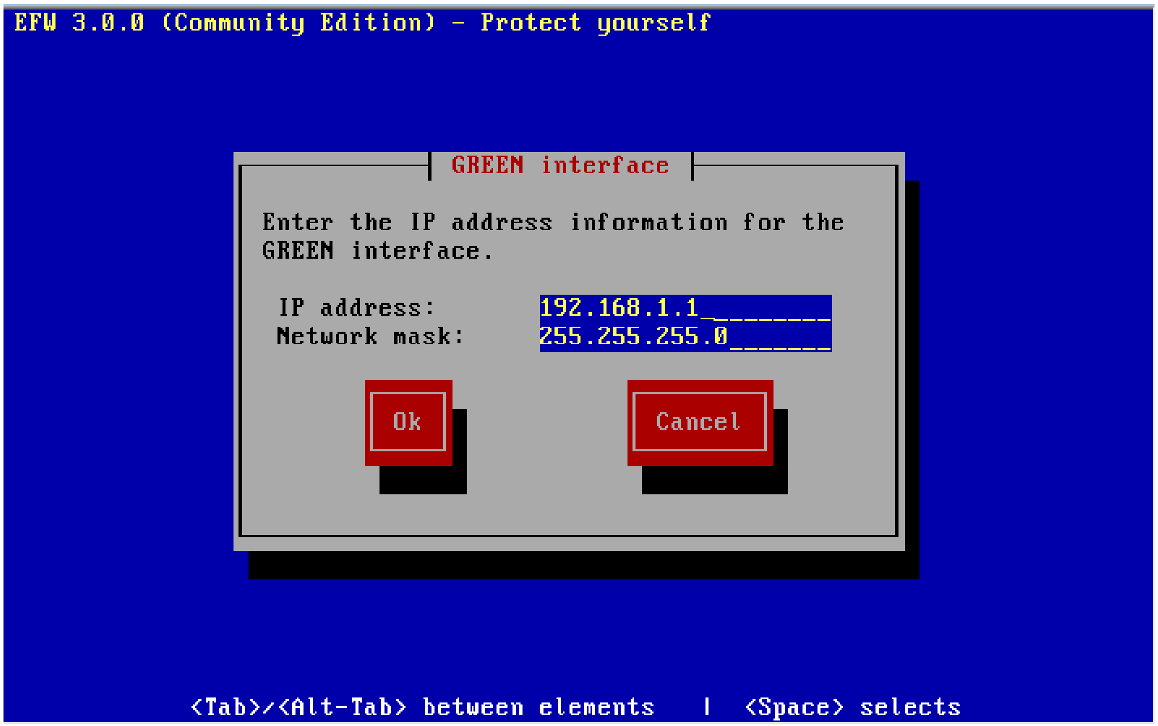
10. EFW will make the root file system and then it will indicate that it is installing packages.

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



```
EFW 3.0.0 (Community Edition) - Protect yourself

Appliance Installer

Making root filesystem...

<Tab>/<Alt-Tab> between elements   |  <Space> selects
```

11. For the GREEN Interface, type **192.168.1.1** at the IP address, press Enter twice and once more for OK.



EFW 3.0.0 (Community Edition) - Protect yourself

GREEN interface

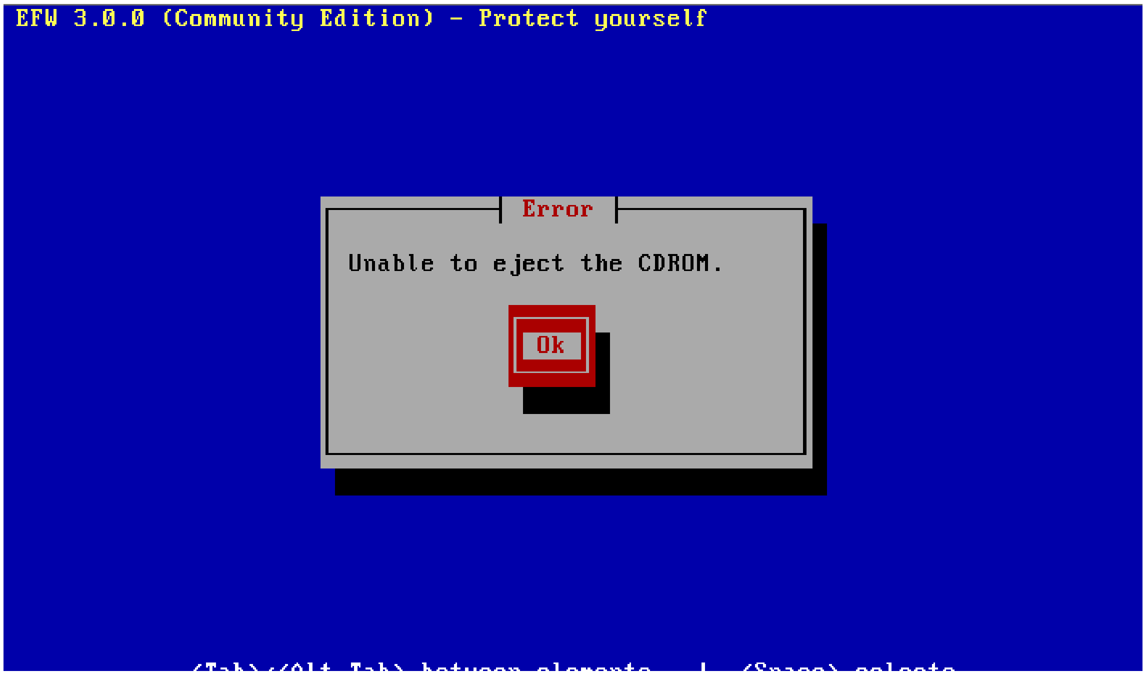
Enter the IP address information for the GREEN interface.

IP address: 192.168.1.1

Network mask: 255.255.255.0

<Tab>/<Alt-Tab> between elements | <Space> selects

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



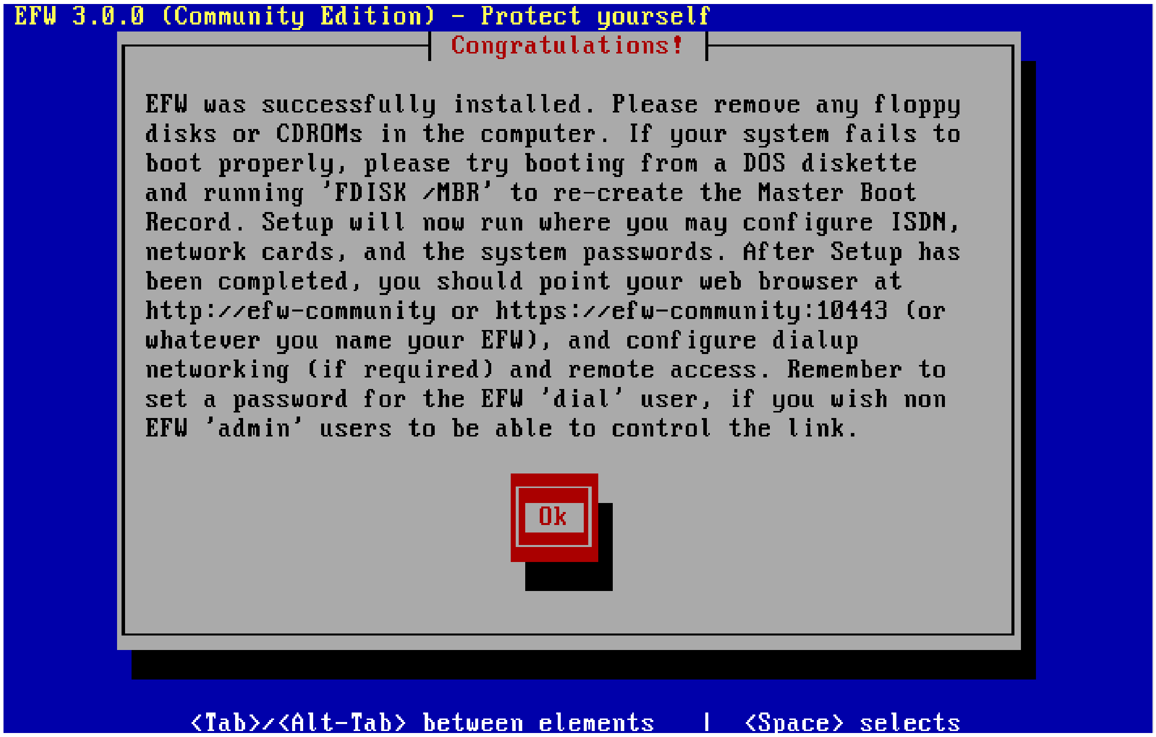
EFW 3.0.0 (Community Edition) - Protect yourself

Error

Unable to eject the CDROM.

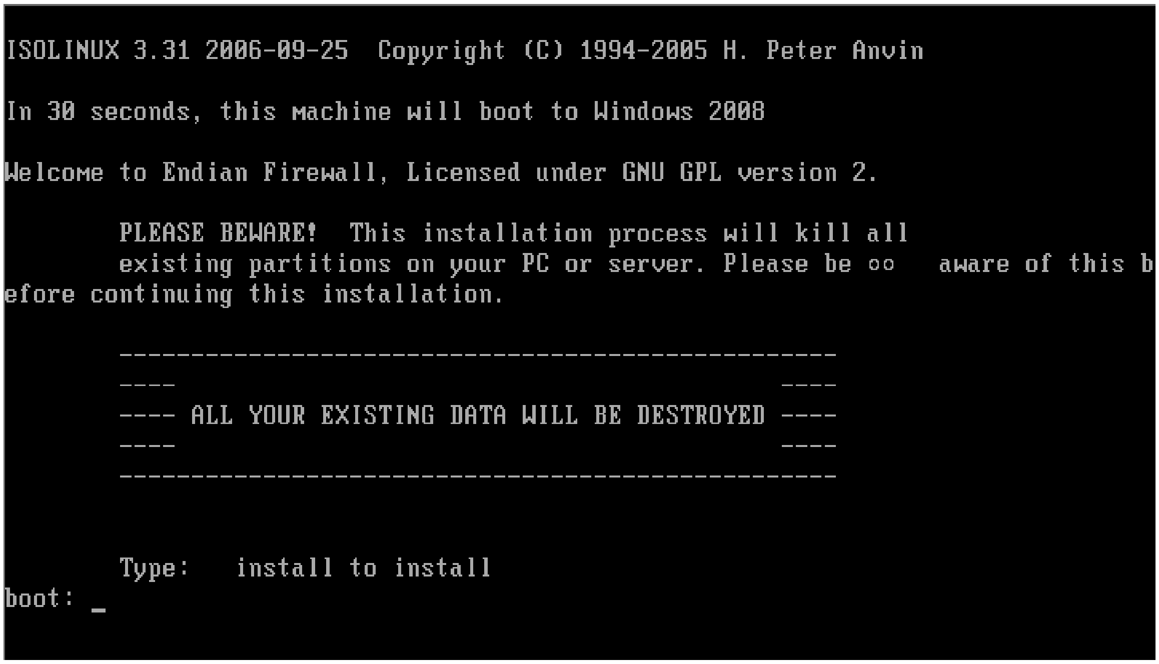
<Tab>/<Alt-Tab> between elements | <Space> selects

13. You will receive the successful installation message. Press Enter to reboot.



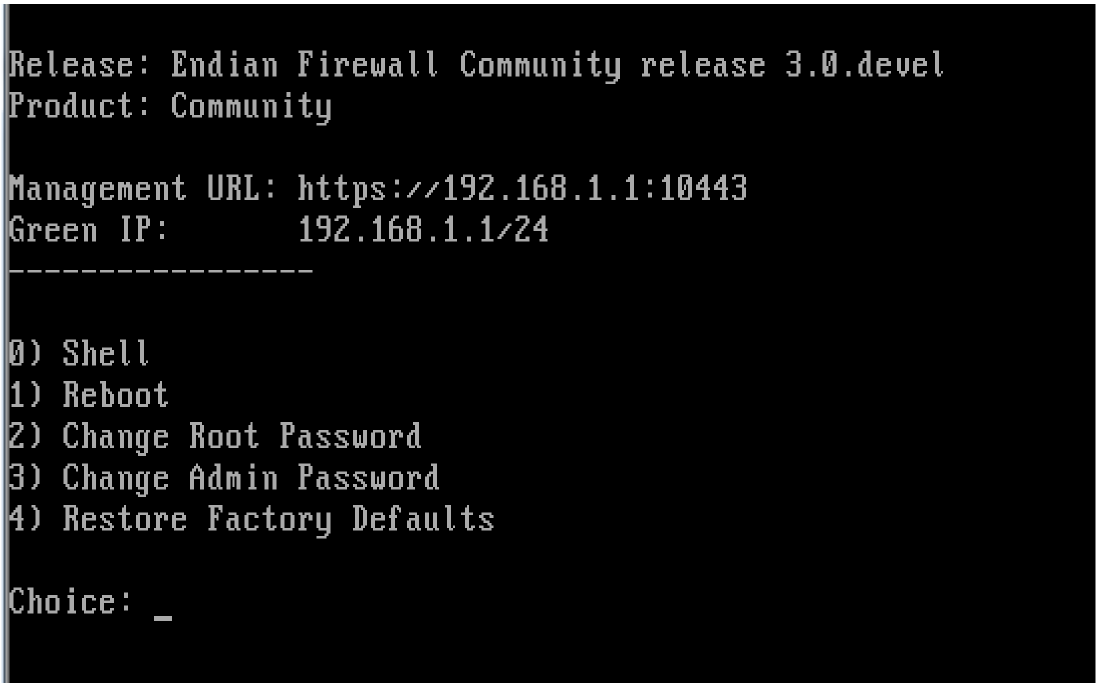
```
EFW 3.0.0 (Community Edition) - Protect yourself
                     Congratulations!

  EFW was successfully installed. Please remove any floppy
  disks or CDROMs in the computer. If your system fails to
  boot properly, please try booting from a DOS diskette
  and running 'FDISK /MBR' to re-create the Master Boot
  Record. Setup will now run where you may configure ISDN,
  network cards, and the system passwords. After Setup has
  been completed, you should point your web browser at
  http://efw-community or https://efw-community:10443 (or
  whatever you name your EFW), and configure dialup
  networking (if required) and remote access. Remember to
  set a password for the EFW 'dial' user, if you wish non
  EFW 'admin' users to be able to control the link.
```

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



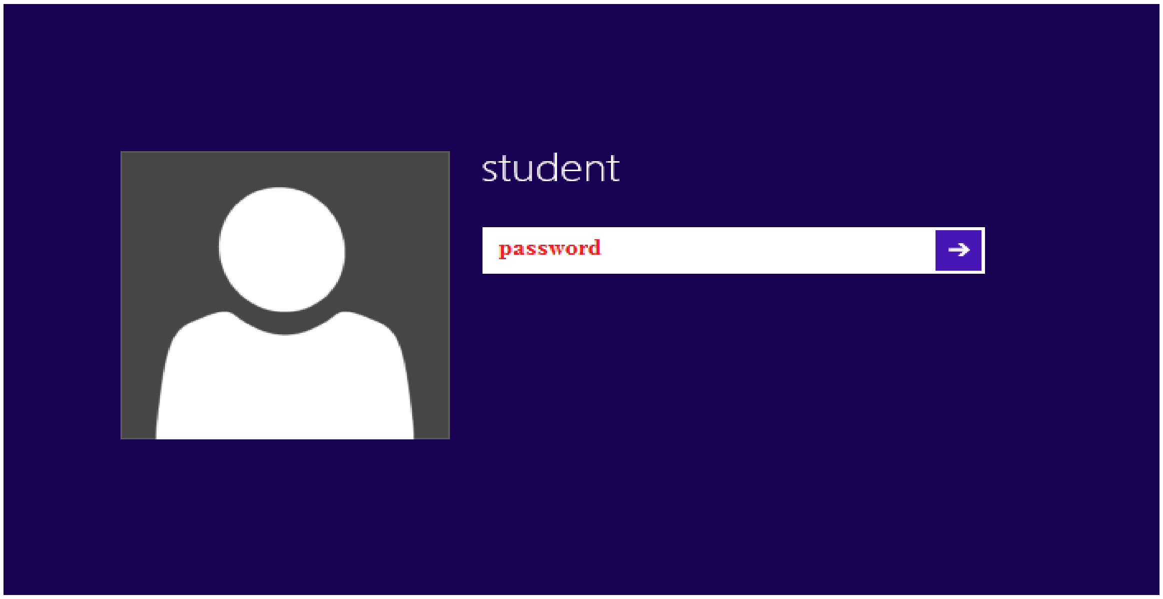
```
ISOLINUX 3.31 2006-09-25  Copyright (C) 1994-2005 H. Peter Anvin

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 oo   aware of this b
efore continuing this installation.

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


        Type:   install to install
boot: _
```

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



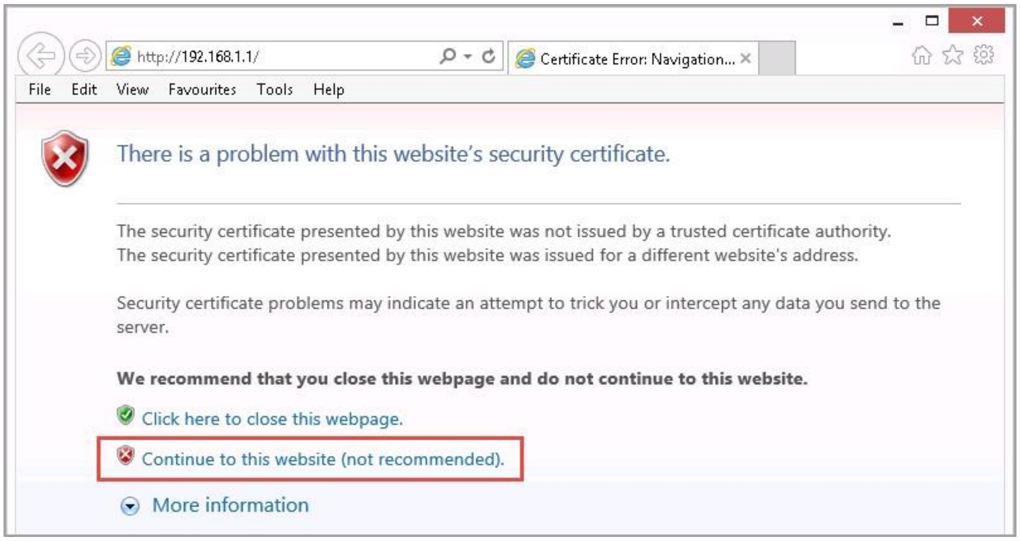
```
Release: Endian Firewall Community release 3.0.devel
Product: Community

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. 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.



16. Click on the shortcut to **Internet Explorer** on the Windows 8 desktop.

17. Go to the following URL: http://192.168.1.1/. Click **Continue to this website**.



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 trick you or intercept any data you send to the server.

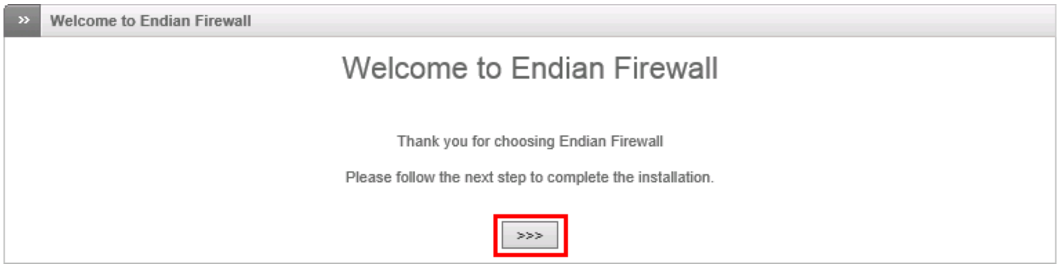
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

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

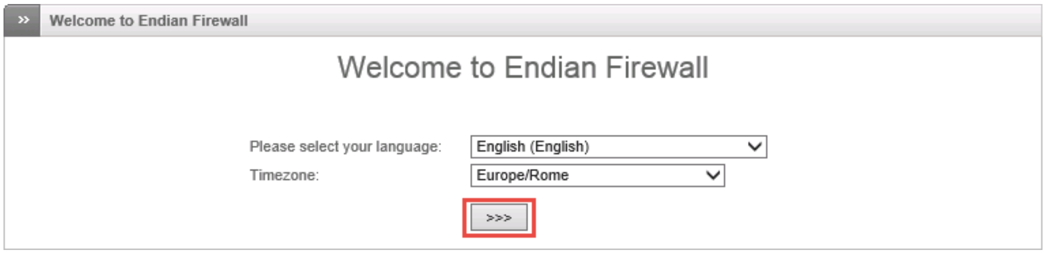


Welcome to Endian Firewall

Thank you for choosing Endian Firewall

Please follow the next step to complete the installation.

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

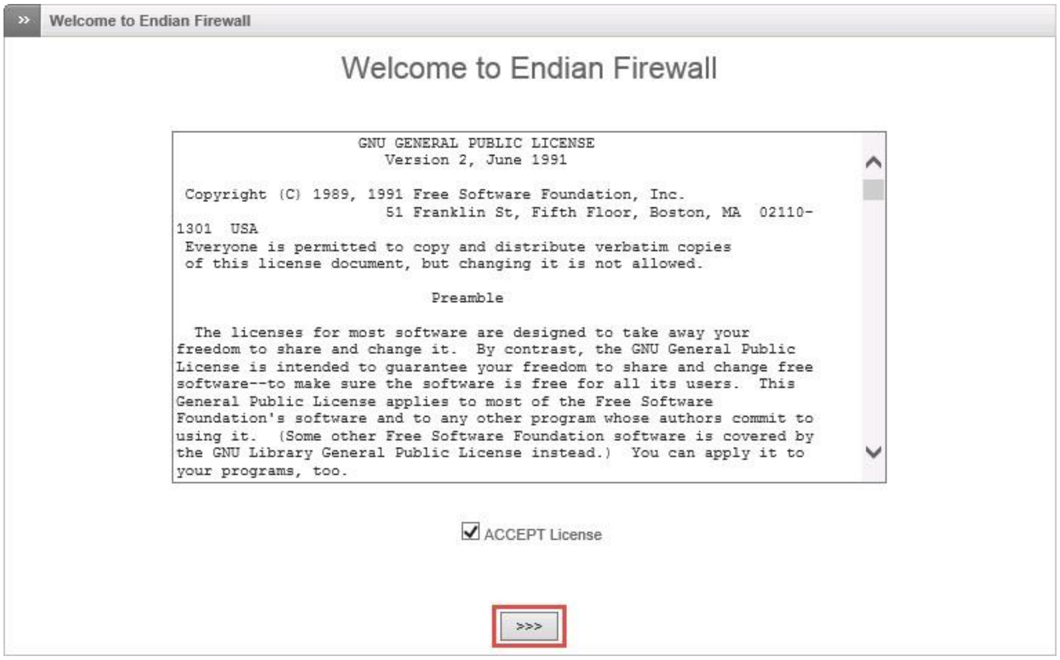


Welcome to Endian Firewall

Please select your language: English (English)

Timezone: Europe/Rome

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

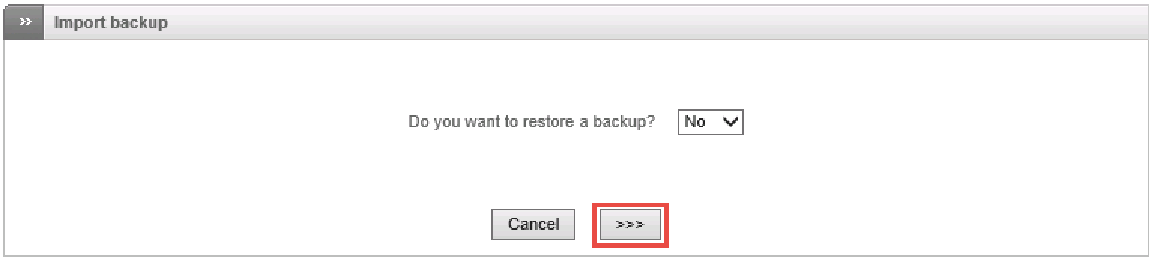


Welcome to Endian Firewall

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA  02110-
1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.)  You can apply it to
your programs, too.
```

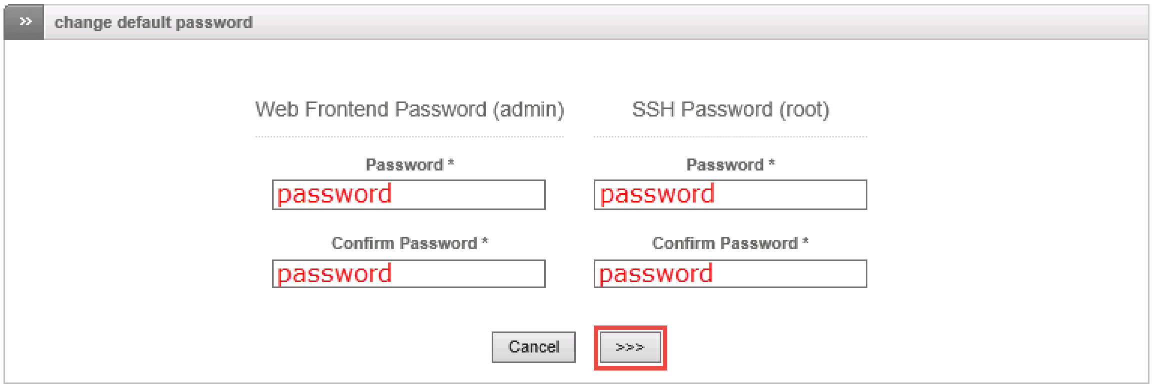
☑ ACCEPT License

21. Click **>>>** at the Restore Backup screen.



Do you want to restore a backup? No

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



Web Frontend Password (admin)

Password * password

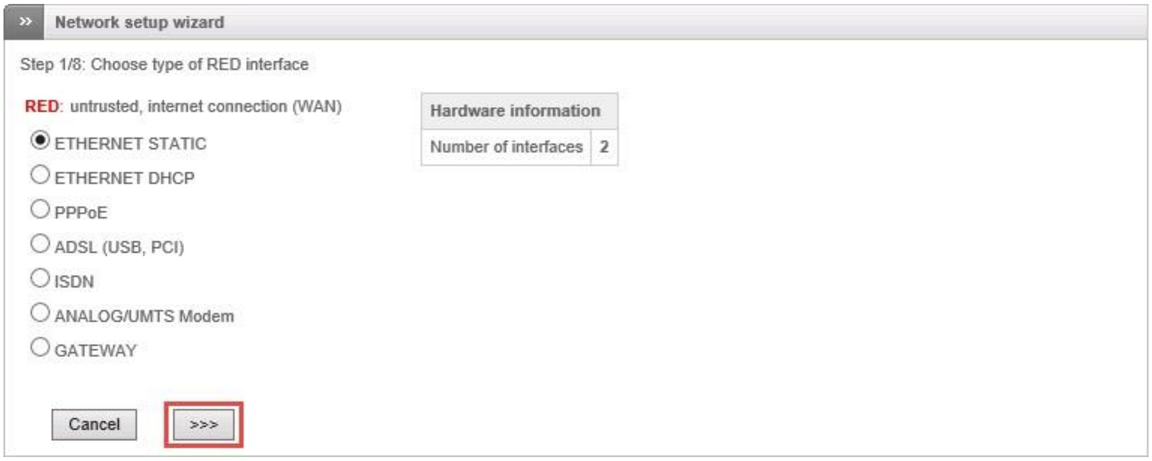
Confirm Password * password

SSH Password (root)

Password * password

Confirm Password * password

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



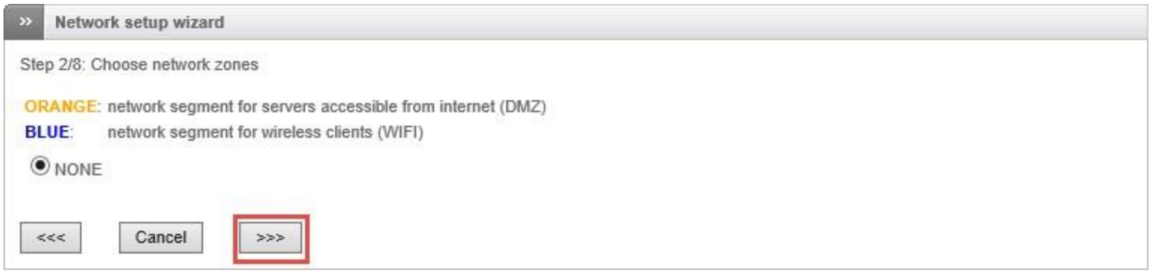
Step 1/8: Choose type of RED interface

RED: untrusted, internet connection (WAN)

● ETHERNET STATIC
○ ETHERNET DHCP
○ PPPoE
○ ADSL (USB, PCI)
○ ISDN
○ ANALOG/UMTS Modem
○ GATEWAY

Hardware information	
Number of interfaces	2

24. Click **>>>** at the Network Zones screen.

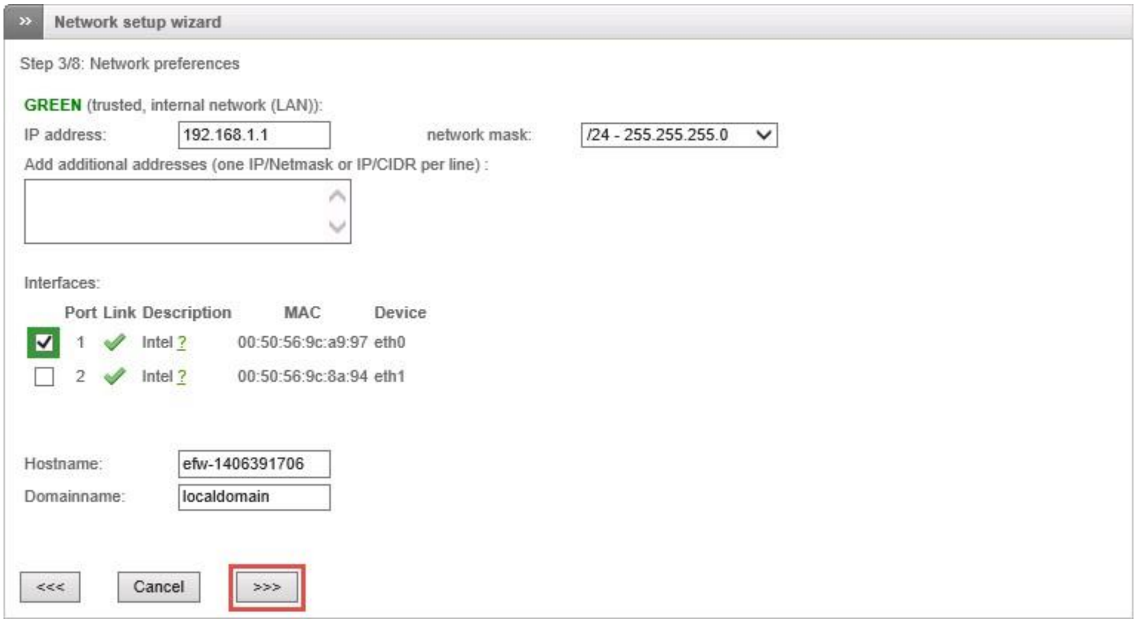


Step 2/8: Choose network zones

ORANGE: network segment for servers accessible from internet (DMZ)
BLUE: network segment for wireless clients (WIFI)

● NONE

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



Step 3/8: Network preferences

GREEN (trusted, internal network (LAN)):

IP address: 192.168.1.1 network mask: /24 - 255.255.255.0

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

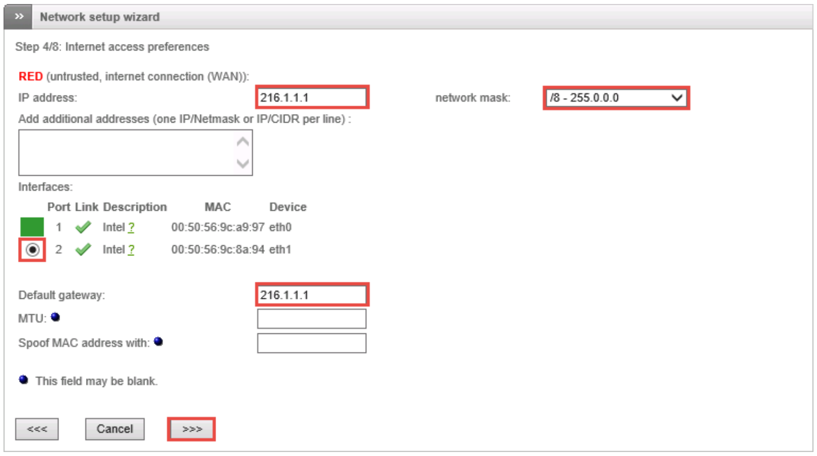
Interfaces:

	Port	Link	Description	MAC	Device
☑	1	✓	Intel ?	00:50:56:9c:a9:97	eth0
□	2	✓	Intel ?	00:50:56:9c:8a:94	eth1

Hostname: efw-1406391706

Domainname: localdomain

26. 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 Default gateway. Click **>>>**.



Step 4/8: Internet access preferences

RED (untrusted, internet connection (WAN)):
IP address: 216.1.1.1 network mask: /8 - 255.0.0.0
Add additional addresses (one IP/Netmask or IP/CIDR per line) :

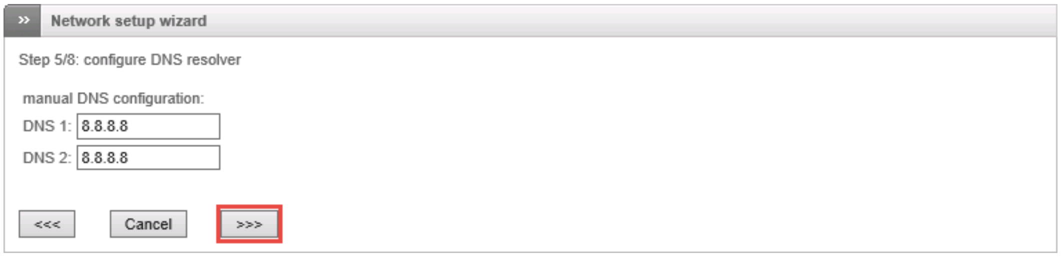
Interfaces:

	Port	Link	Description	MAC	Device
🟩	1	✓	Intel ?	00:50:56:9c:a9:97	eth0
●	2	✓	Intel ?	00:50:56:9c:8a:94	eth1

Default gateway: 216.1.1.1
MTU: ●
Spoof MAC address with: ●

● This field may be blank.

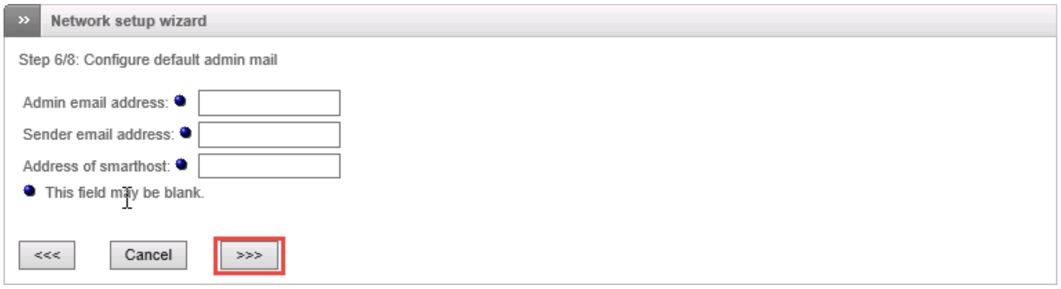
27. Put 8.8.8.8 for both DNS Servers (Google). This system is not on the Internet.



Step 5/8: configure DNS resolver

manual DNS configuration:
DNS 1: 8.8.8.8
DNS 2: 8.8.8.8

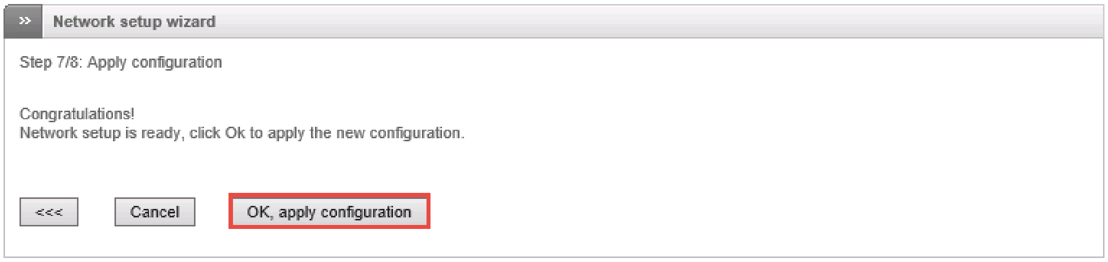
28. Click **>>>** at the Admin Email Address screen.



Step 6/8: Configure default admin mail

Admin email address: ●
Sender email address: ●
Address of smarthost: ●
● This field may be blank.

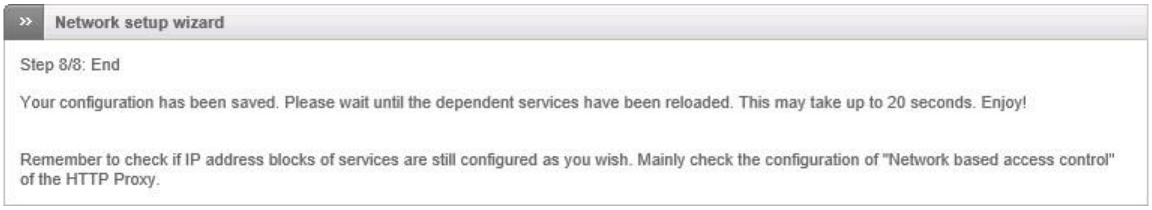
29. Click **Ok, apply configuration** to apply settings.



Step 7/8: Apply configuration

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

30. Wait for the Network Setup page to reload.

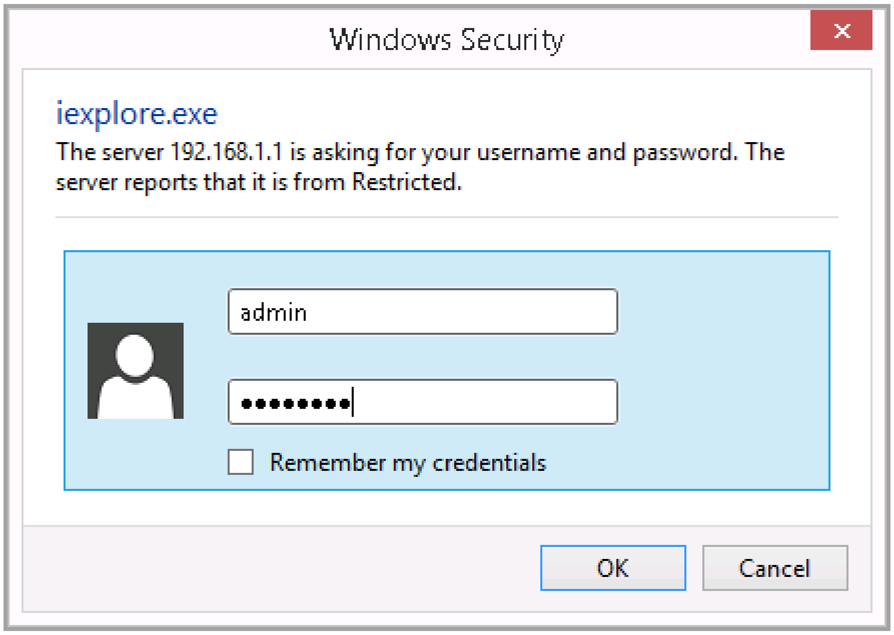


Step 8/8: End

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.

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



iexplore.exe

The server 192.168.1.1 is asking for your username and password. The server reports that it is from Restricted.

admin

••••••••

□ Remember my credentials

1.2 Conclusion

Some firewalls include VPN capabilities. A Virtual Private Network can be set up so that external users from the Internet can connect in and access internal network resources. VPNs encrypt traffic so that the communication between the VPN server and client is safe.

1.3 Discussion Questions

1. What internal IP address does the Firewall use?
   Ans: The internal IP address the Firewall use is 192.168.1.1 2 .

2. What is the difference between the Red and Green interfaces?
   Ans: The Red interface is the Public Internet, it is used for filtering the incoming signal from the network. Green interface is the Private Internet, it is used for filtering the outgoing traffic from the private network.

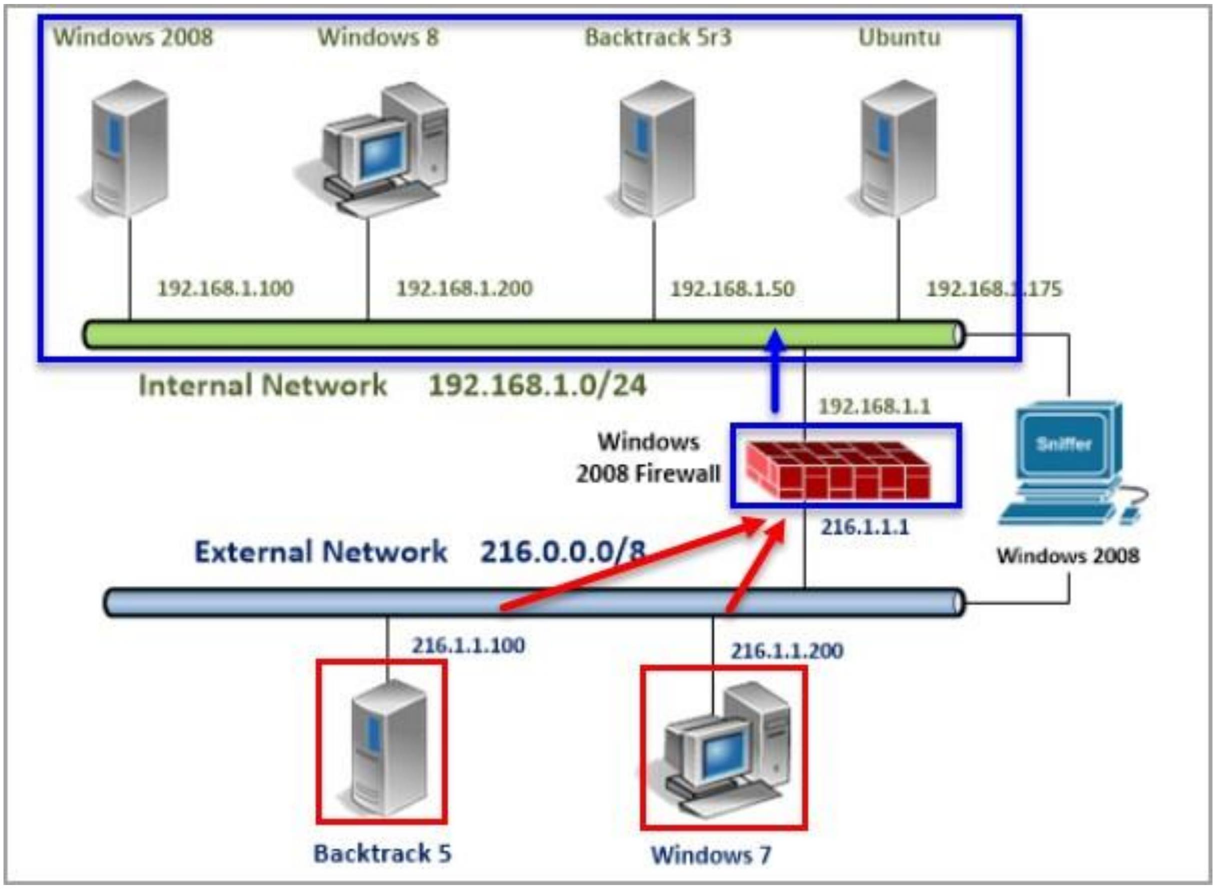
3. What is the Public IP address of the firewall?
   Ans: The Public IP address of the firewall is 216.1.1.1 4.

4. What is the benefit of using a Linux firewall over a Windows one?
   Ans: The are several advantages of using a Linux firewall over a window the Linux is known for its stability and reliability, Linux is generally considered to be more secure than Windows, due to its framework and design principles.

2 Configuring the VPN Server and Client

Virtual Private Network (VPN) allows clients from an external network to connect to and utilize the resources of an internal network. Virtual Private Networks, which are encrypted, allow individuals to work from remote locations. The encryption of a Virtual Private Network allows external users to access internal resources in a secure manner.

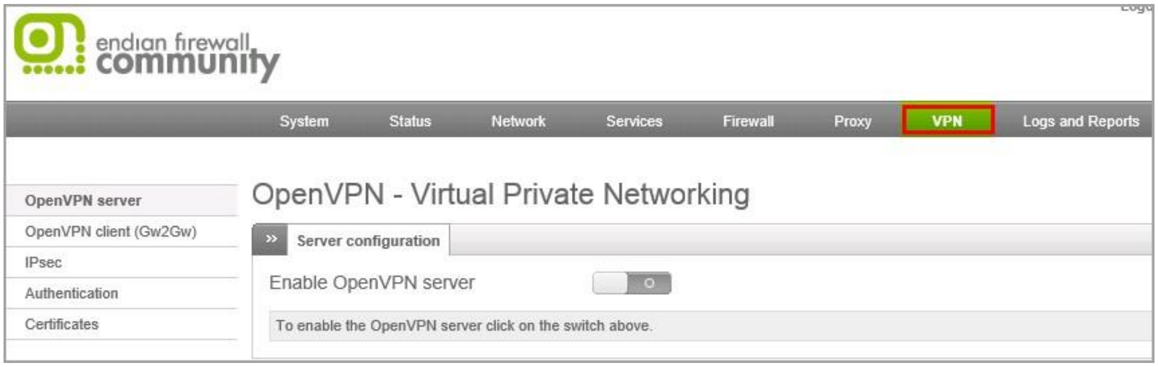
The VPN that we will configure on the Linux based Endian Firewall will allow users to access internal resources on the network. After connecting to the firewall, the external user will be assigned an internal IP address on the internal 192.168.1.0/24 network.



Next, we will need to configure the VPN on the Linux based Endian Community Firewall. We will continue using the browser on the Windows 8 Internal machine to complete the setup.

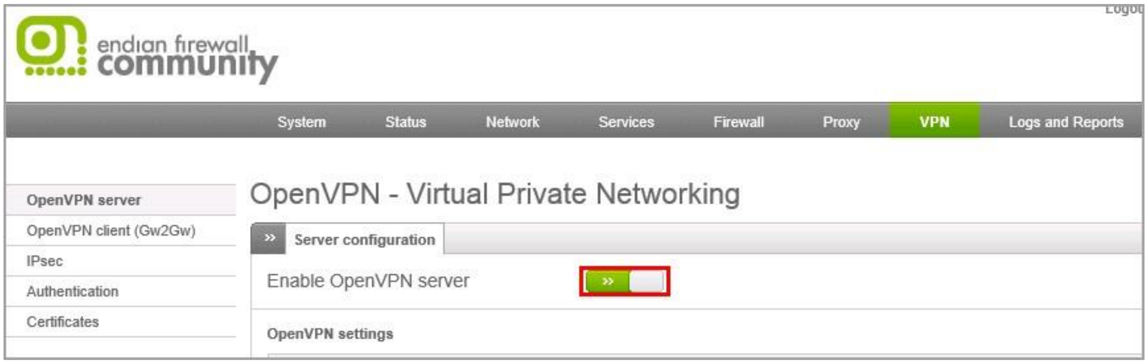
2.1 Configure the VPN

1. In the browser of the Windows 8 Internal Machine connected to the Linux based Endian Community Firewall, click the VPN tab to configure the OpenVPN server.



To enable the OpenVPN server click on the switch above.

2. By default, the OpenVPN server is not running and it needs to be turned on. Click the Open VPNserver slider in the middle of the screen. The slider will turn green to indicate it is on.

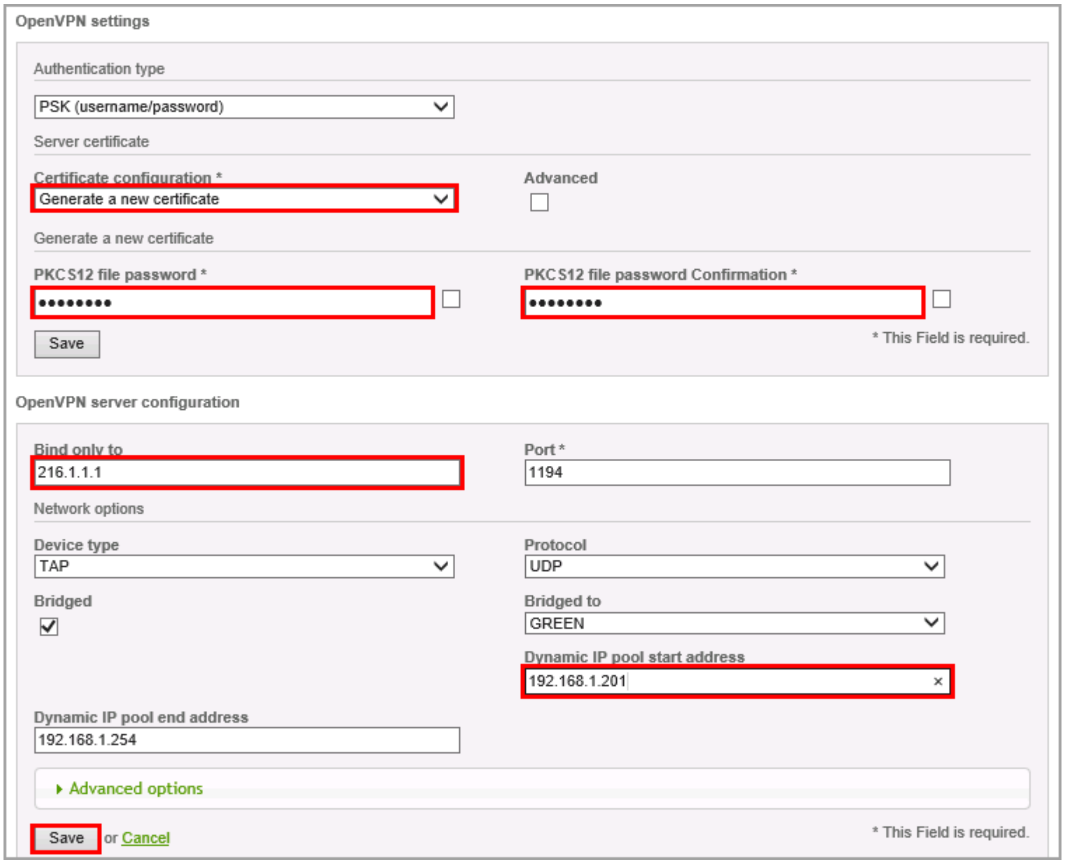


3. Select/enter the values below:

Authentication type	PSK (username/password).
Certificate configuration	Generate a New Certificate.
PKCS12 file password	password
PKCS12 file password confirmation	password
Bind only to IP address	216.1.1.1
Dynamic IP pool start address	192.168.1.201.

- Leave the Port, Device type, bridged, and protocol fields to their default settings.
- Leave the default for the Dynamic IP pool end address (192.168.1.254)

4. Click the **Save** button to Save the OpenVPN configuration.



OpenVPN settings

Authentication type

PSK (username/password)

Server certificate

Certificate configuration *: Generate a new certificate

Advanced ☐

Generate a new certificate

PKCS12 file password *: •••••••• ☐

PKCS12 file password Confirmation *: •••••••• ☐

Save

* This Field is required.

OpenVPN server configuration

Bind only to: 216.1.1.1

Port *: 1194

Network options

Device type: TAP

Protocol: UDP

Bridged: ☑

Bridged to: GREEN

Dynamic IP pool start address: 192.168.1.201

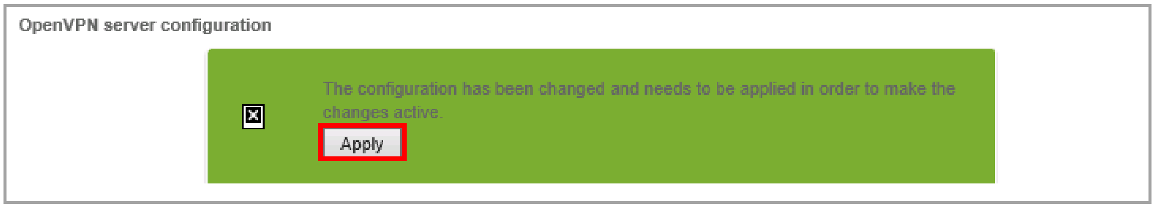
Dynamic IP pool end address: 192.168.1.254

▸ Advanced options

Save or Cancel

* This Field is required.

5. Click the apply button to apply the OpenVPN settings that we have configured.

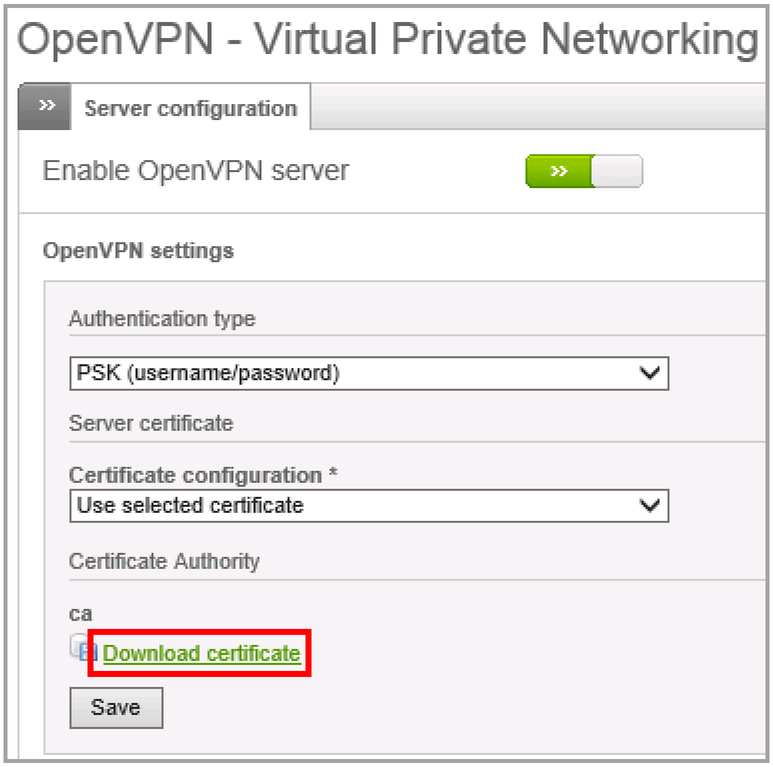


OpenVPN server configuration

☒ The configuration has been changed and needs to be applied in order to make the changes active.

Apply

6. Click the **Download certificate** button to download the cacert.pem file.



OpenVPN - Virtual Private Networking

Server configuration

Enable OpenVPN server

OpenVPN settings

Authentication type: PSK (username/password)

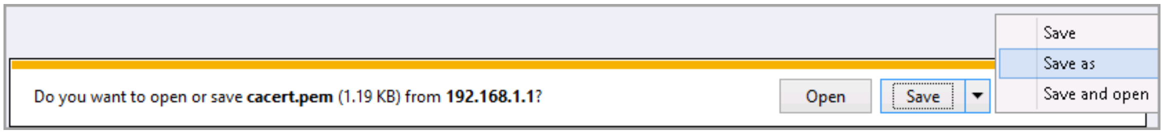
Server certificate

Certificate configuration *: Use selected certificate

Certificate Authority

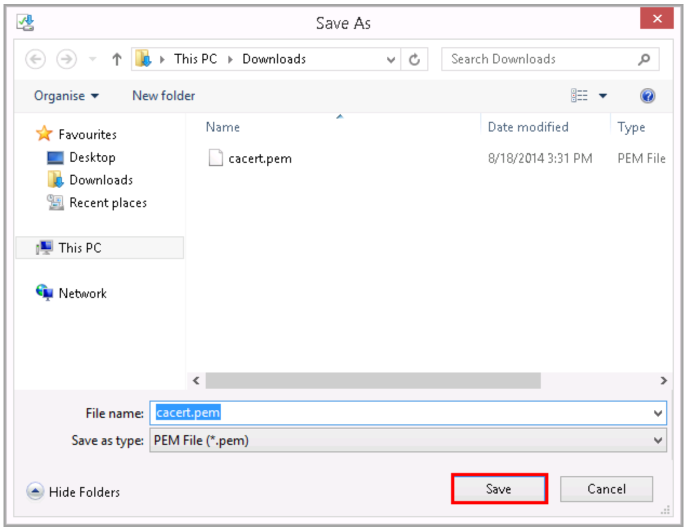
ca

7. Click **Save** and **Save as** to save the file.



Do you want to open or save **cacert.pem** (1.19 KB) from **192.168.1.1**?

8. Click **Save** to save the cacert.pem file to the default directory of Downloads.



Save As

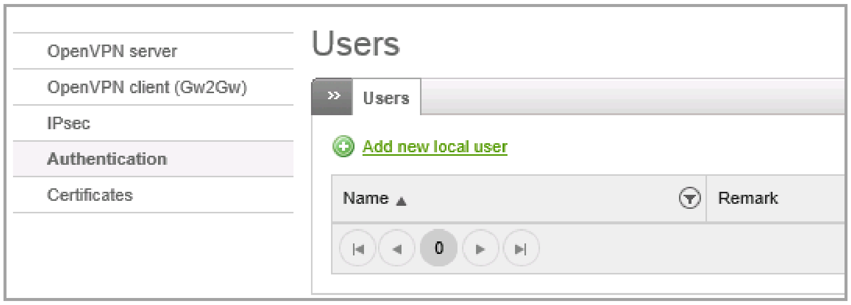
This PC › Downloads

Name	Date modified	Type
cacert.pem	8/18/2014 3:31 PM	PEM File

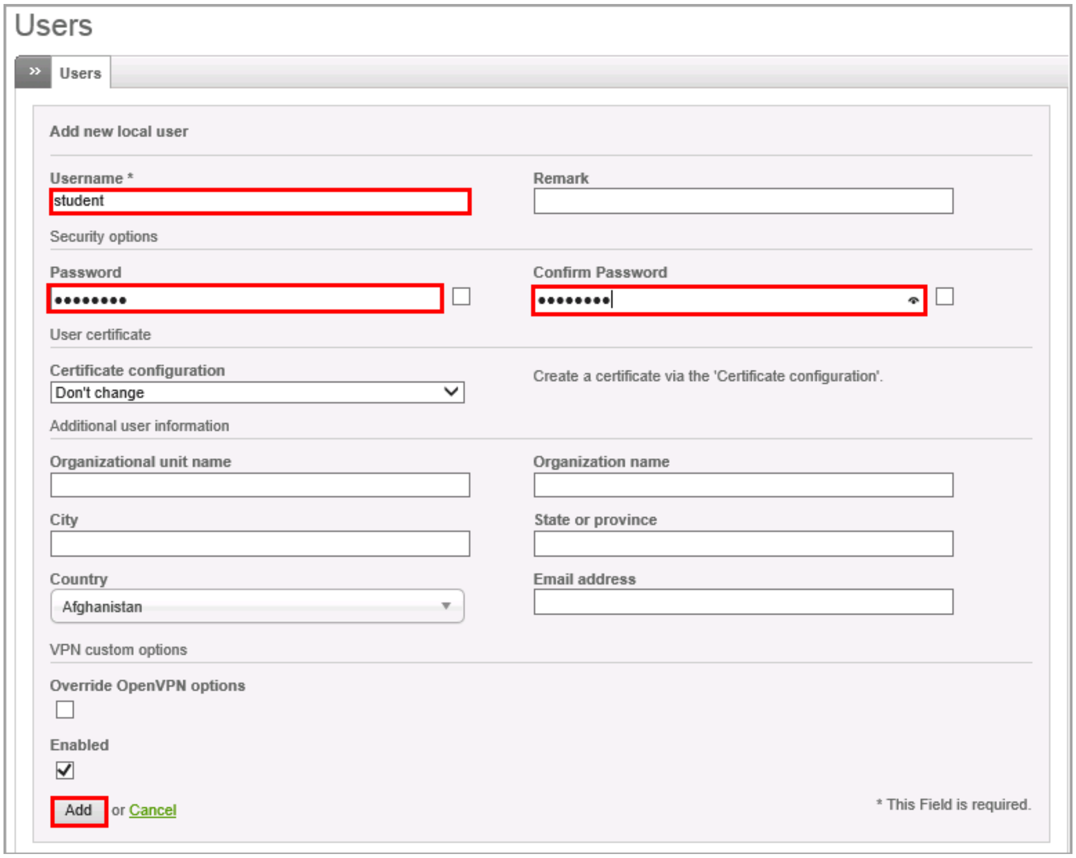
File name: cacert.pem

Save as type: PEM File (*.pem)

9. Return to the OpenVPN GUI interface and click the Authentication tab under OpenVPN Server in the left menu and click **Add a new local user**.



10. Add **student** for the username. Type **password** for the password and confirmation **password**. Then click the **Add** button to add student as a VPN user.



Add new local user

Username * student

Remark

Security options

Password •••••••• □

Confirm Password •••••••• □

User certificate

Certificate configuration: Don't change

Create a certificate via the 'Certificate configuration'.

Additional user information

Organizational unit name

Organization name

City

State or province

Country: Afghanistan

Email address

VPN custom options

Override OpenVPN options □

Enabled ☑

Add or Cancel

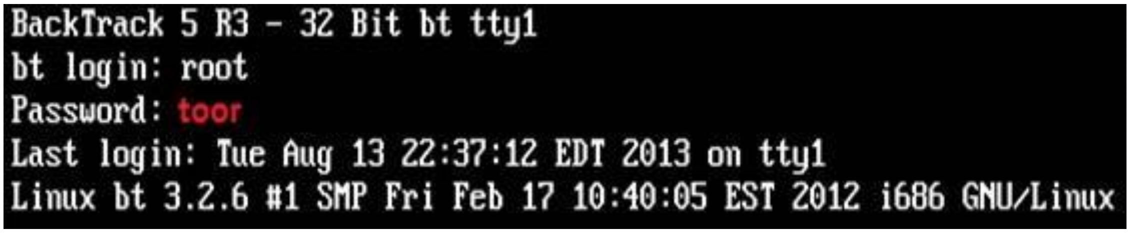
* This Field is required.

Perform the following steps on the **Backtrack 5 External Machine.**

11. Click the **Backtrack 5** icon on the topology to open the **BackTrack 5 External Machine**. Type **root** for the login and **toor** *(root spelled backwards)* for the password.

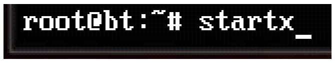
Click in the window and press Enter if BackTrack is displaying a black screen.

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



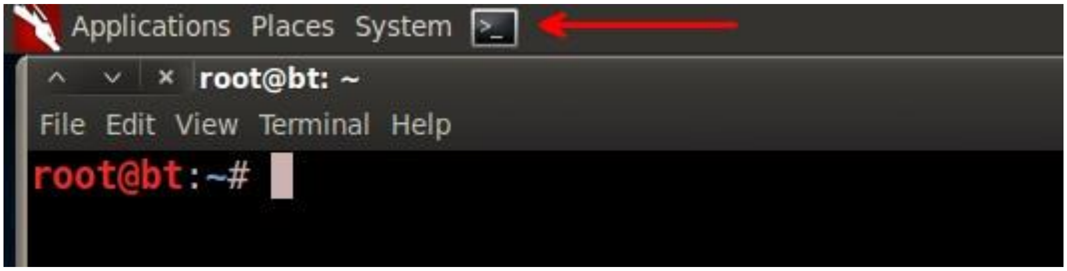
```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
```

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



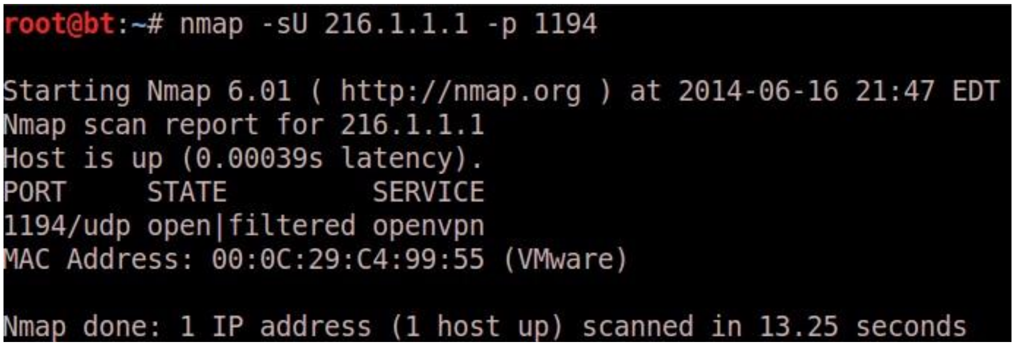
```
root@bt:~# startx_
```

13. 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 in BackTrack version 5 R3.



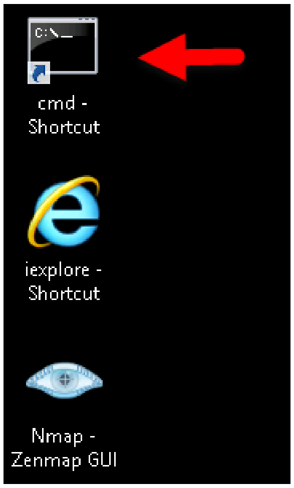
```
root@bt:~#
```

14. Type the following command to look for the open UDP port:
root@bt:~# **nmap -sU 216.1.1.1 -p 1194**

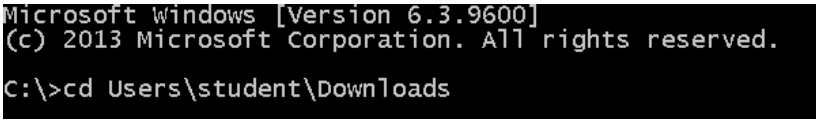


```
root@bt:~# nmap -sU 216.1.1.1 -p 1194

Starting Nmap 6.01 ( http://nmap.org ) at 2014-06-16 21:47 EDT
Nmap scan report for 216.1.1.1
Host is up (0.00039s latency).
PORT     STATE         SERVICE
1194/udp open|filtered openvpn
MAC Address: 00:0C:29:C4:99:55 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

15. On the **Windows 8 Internal Machine**, minimize the web browser and double-click on the **cmd-Shortcut** on the desktop.

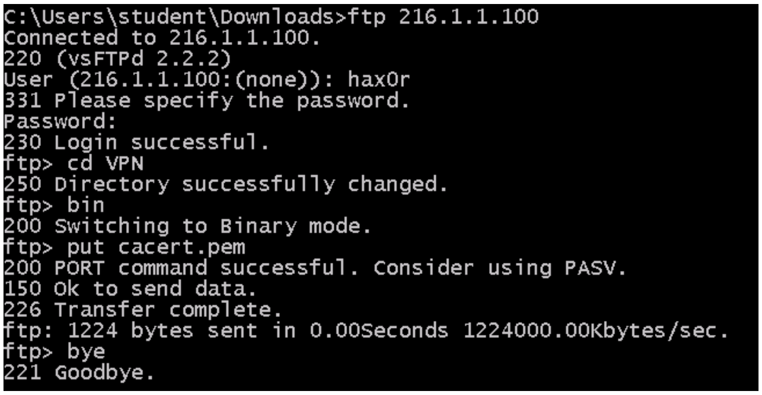


16. Switch to the Downloads Directory by typing the following command:
C:\>**cd Users\student\Downloads**



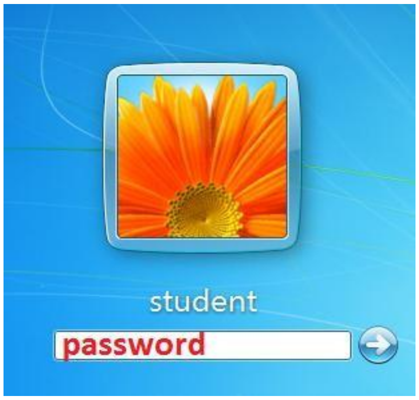
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>cd Users\student\Downloads
```

17. Type the following commands to upload the cert file to the BackTrack 5 External Machine:
C:\Users\student\Downloads>**ftp 216.1.1.100**
user: **hax0r**
Password**: hacker**
ftp> **cd VPN**
ftp> **bin**
ftp> **put cacert.pem**
ftp> **bye**



```
C:\Users\student\Downloads>ftp 216.1.1.100
Connected to 216.1.1.100.
220 (vsFTPd 2.2.2)
User (216.1.1.100:(none)): hax0r
331 Please specify the password.
Password:
230 Login successful.
ftp> cd VPN
250 Directory successfully changed.
ftp> bin
200 Switching to Binary mode.
ftp> put cacert.pem
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 1224 bytes sent in 0.00Seconds 1224000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```

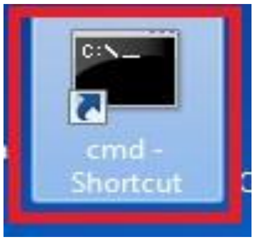
18. Log into the **Windows 7 External Machine** by clicking on the **Windows 7** icon on the topology. If required, enter the username, **student**. Type in the password, **password** and press **Enter** to log in.



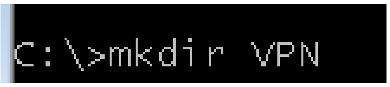
student

password

19. Open a command prompt by double-clicking on the **cmd-shortcut** on the desktop.

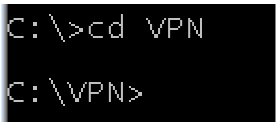


20. Type the following commands to make a directory named VPN on the root of C:
C:\>**mkdir VPN**



```
C:\>mkdir VPN
```

21. Type the following commands to make a directory named VPN on the root of C:
C:\>**cd VPN**



```
C:\>cd VPN

C:\VPN>
```

22. Type the following commands to download the files from External BackTrack.

    C:\VPN>**ftp 216.1.1.100**

    user: **hax0r**

    Password**: hacker**

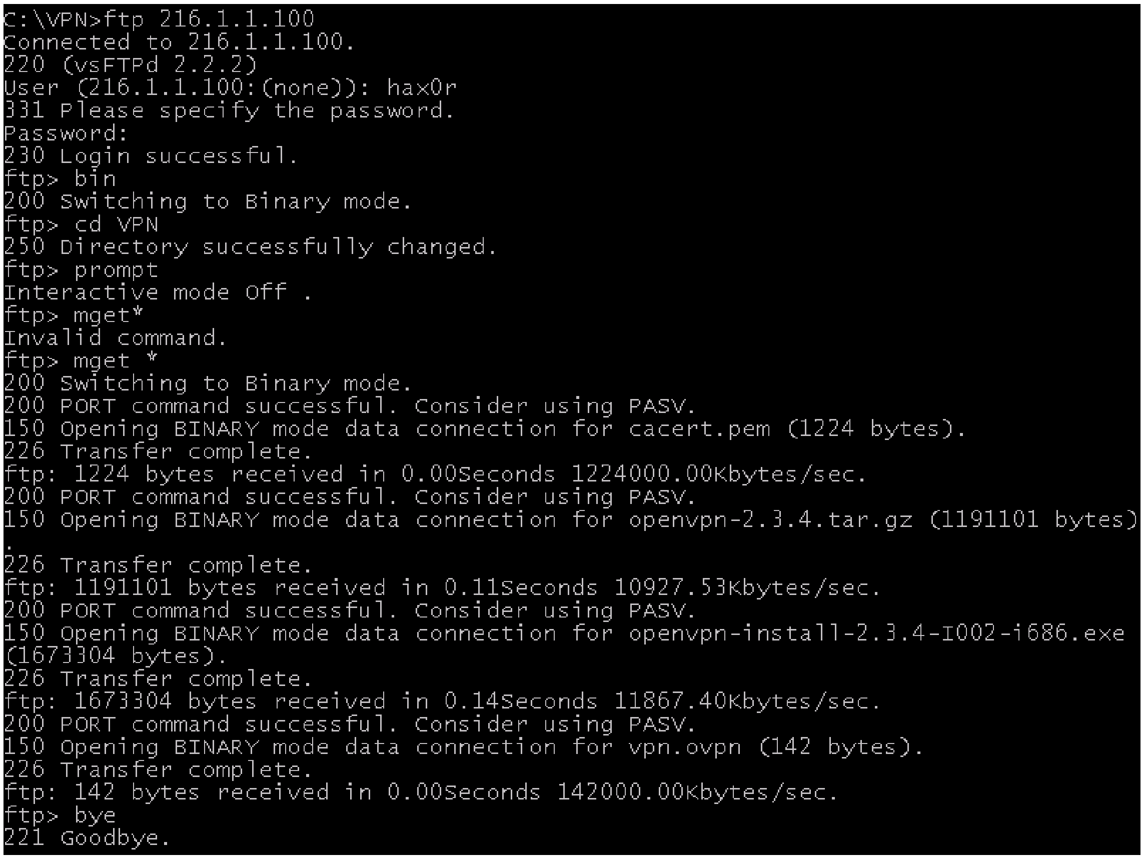
    ftp> **bin**

    ftp> **cd VPN**

    ftp> **prompt**

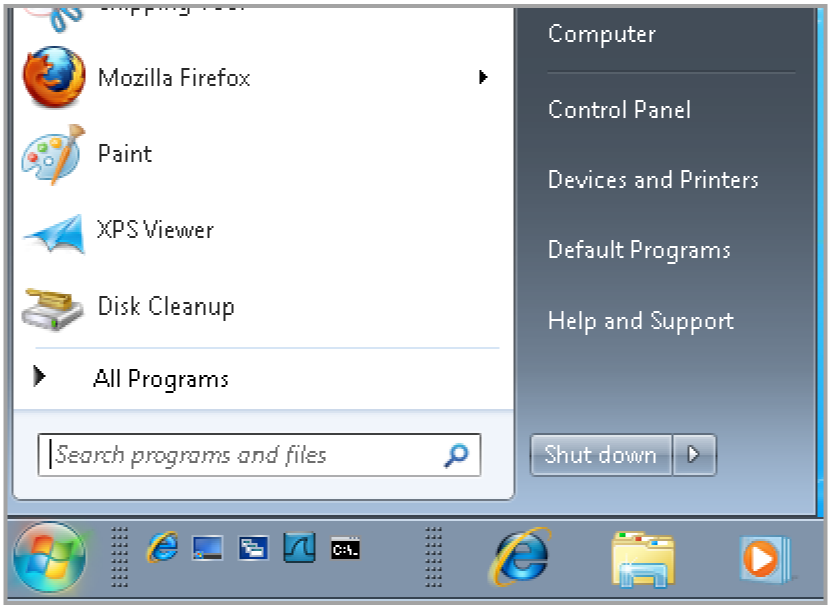
    ftp> **mget ***

    ftp> **bye**

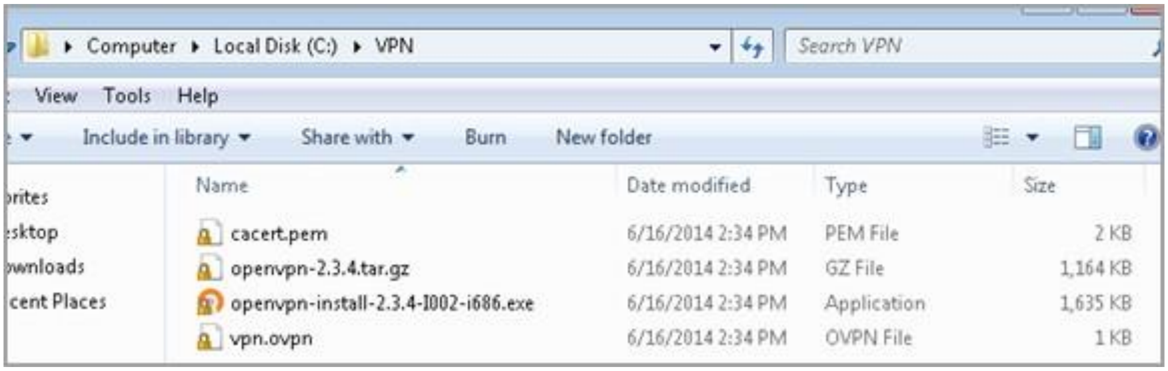


```
C:\VPN>ftp 216.1.1.100
Connected to 216.1.1.100.
220 (vsFTPd 2.2.2)
User (216.1.1.100:(none)): hax0r
331 Please specify the password.
Password:
230 Login successful.
ftp> bin
200 Switching to Binary mode.
ftp> cd VPN
250 Directory successfully changed.
ftp> prompt
Interactive mode Off .
ftp> mget*
Invalid command.
ftp> mget *
200 Switching to Binary mode.
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cacert.pem (1224 bytes).
226 Transfer complete.
ftp: 1224 bytes received in 0.00Seconds 1224000.00Kbytes/sec.
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for openvpn-2.3.4.tar.gz (1191101 bytes)
.

226 Transfer complete.
ftp: 1191101 bytes received in 0.11Seconds 10927.53Kbytes/sec.
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for openvpn-install-2.3.4-I002-i686.exe
(1673304 bytes).
226 Transfer complete.
ftp: 1673304 bytes received in 0.14Seconds 11867.40Kbytes/sec.
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for vpn.ovpn (142 bytes).
226 Transfer complete.
ftp: 142 bytes received in 0.00Seconds 142000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```

23. Click on Start and go to the Computer Link on the Windows 7 External Machine.

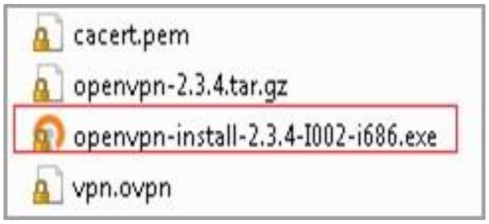


24. Double-click on Local Disk (C:). Double-click on the VPN folder. You should see the 4 files that were downloaded during the FTP session.



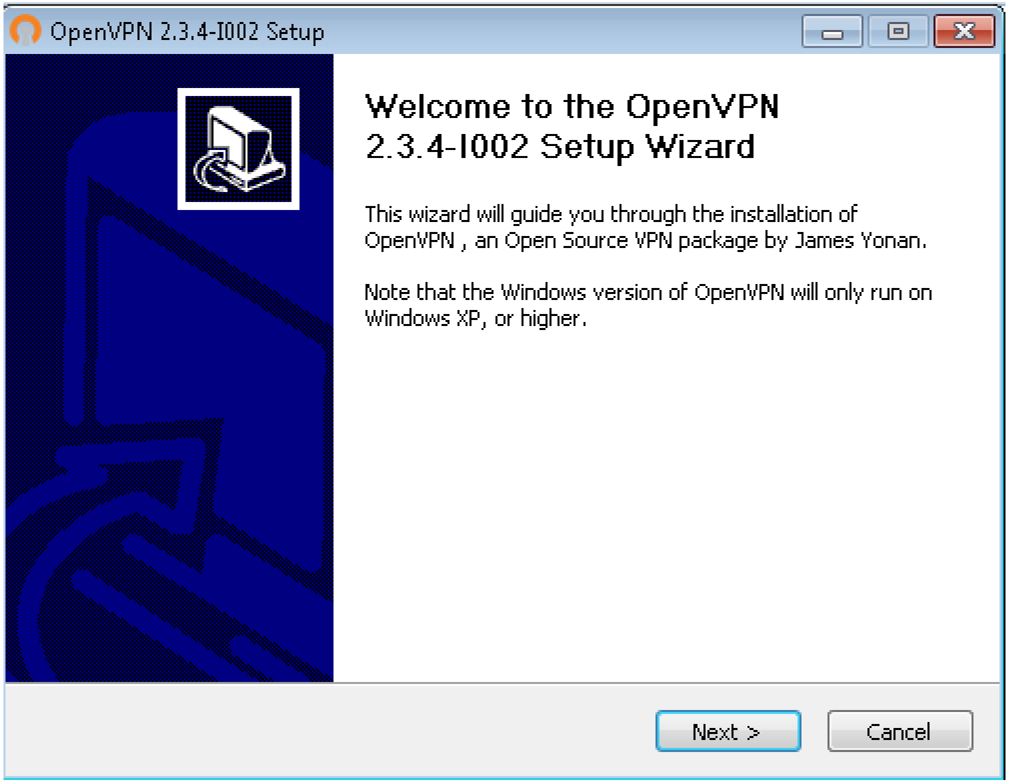
Name	Date modified	Type	Size
cacert.pem	6/16/2014 2:34 PM	PEM File	2 KB
openvpn-2.3.4.tar.gz	6/16/2014 2:34 PM	GZ File	1,164 KB
openvpn-install-2.3.4-I002-i686.exe	6/16/2014 2:34 PM	Application	1,635 KB
vpn.ovpn	6/16/2014 2:34 PM	OVPN File	1 KB

25. Double-click on the openvpn-install-2.3.4-I002-i686.exe file to install the client.



cacert.pem
openvpn-2.3.4.tar.gz
openvpn-install-2.3.4-I002-i686.exe
vpn.ovpn

26. Click **Next** at the Welcome to the OpenVPN Setup Wizard.

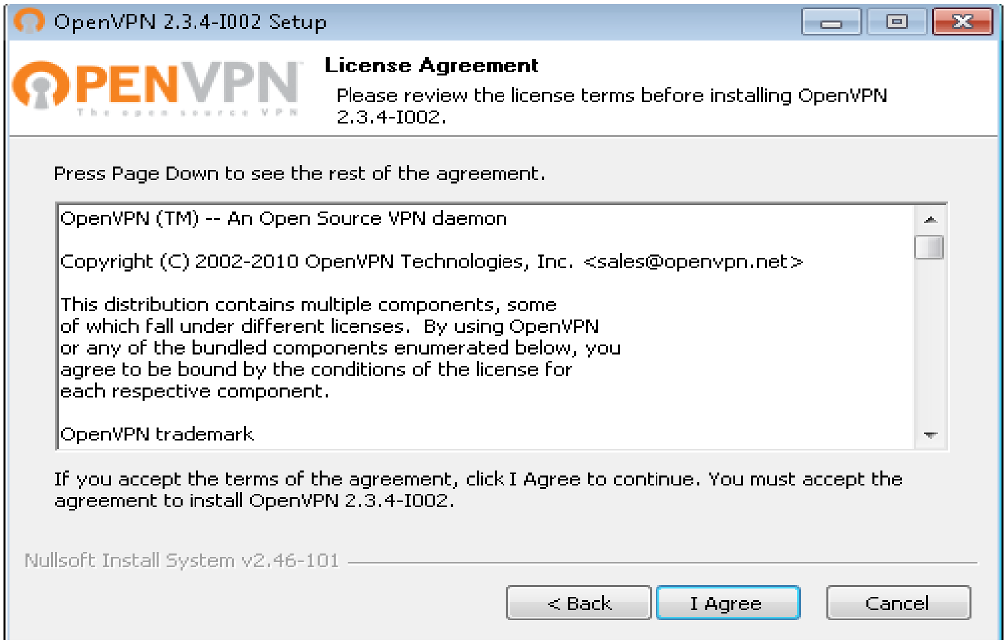


Welcome to the OpenVPN 2.3.4-I002 Setup Wizard

This wizard will guide you through the installation of OpenVPN , an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN will only run on Windows XP, or higher.

27. Read the license agreement and click **I Agree**, if you agree.



License Agreement

Please review the license terms before installing OpenVPN 2.3.4-I002.

Press Page Down to see the rest of the agreement.

OpenVPN (TM) -- An Open Source VPN daemon

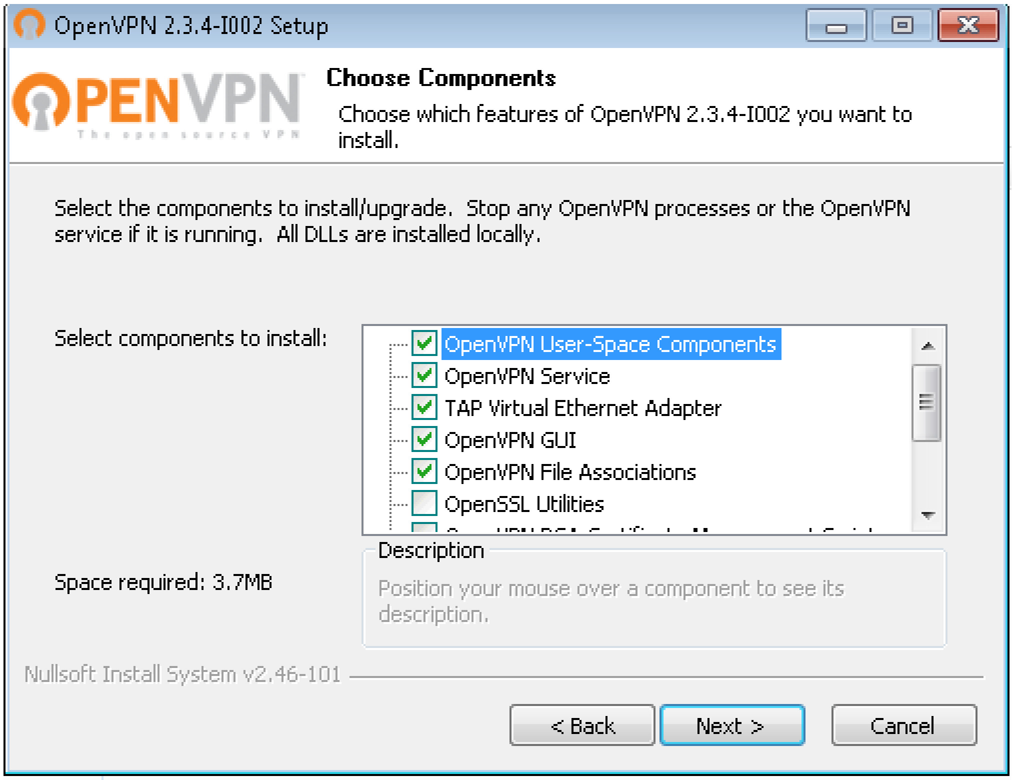
Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>

This distribution contains multiple components, some of which fall under different licenses. By using OpenVPN or any of the bundled components enumerated below, you agree to be bound by the conditions of the license for each respective component.

OpenVPN trademark

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.3.4-I002.

28. Click **Next** at the Choose Components Screen.


OpenVPN 2.3.4-I002 Setup

Choose Components

Choose which features of OpenVPN 2.3.4-I002 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

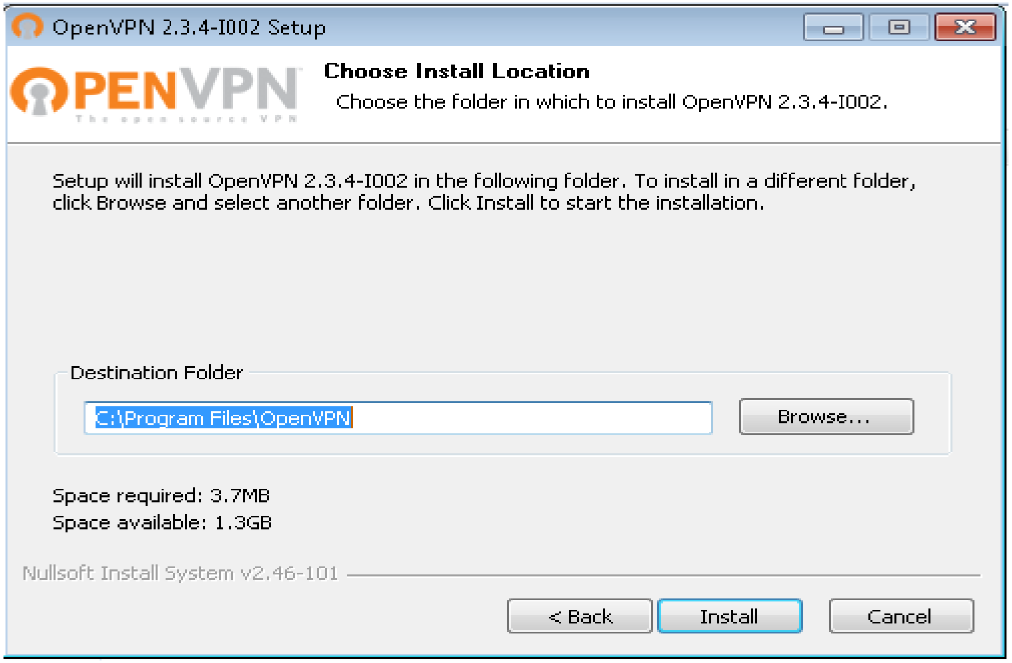
- ☑ OpenVPN User-Space Components
- ☑ OpenVPN Service
- ☑ TAP Virtual Ethernet Adapter
- ☑ OpenVPN GUI
- ☑ OpenVPN File Associations
- □ OpenSSL Utilities

Space required: 3.7MB

Description

Position your mouse over a component to see its description.

29. Accept the default installation directory and click **Install**.


OpenVPN 2.3.4-I002 Setup

Choose Install Location

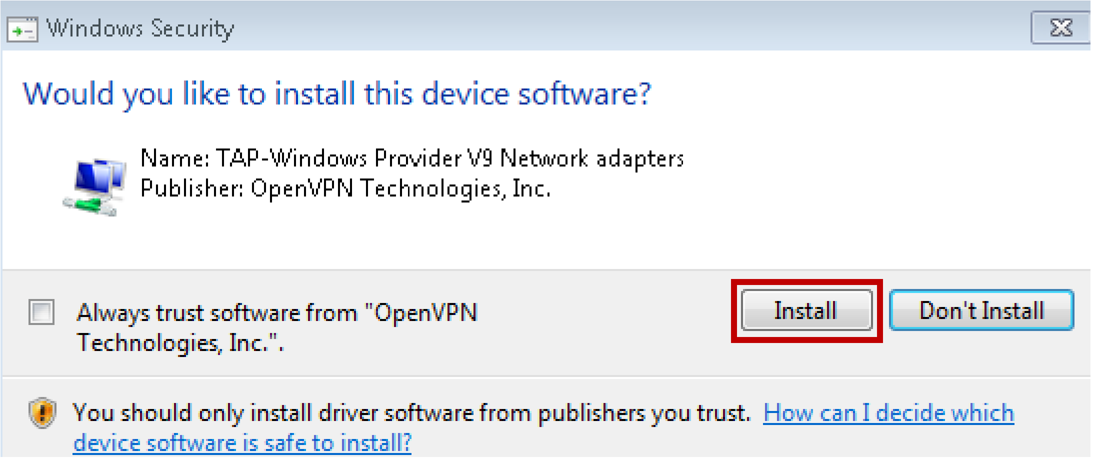
Choose the folder in which to install OpenVPN 2.3.4-I002.

Setup will install OpenVPN 2.3.4-I002 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\OpenVPN

Space required: 3.7MB
Space available: 1.3GB

30. Click **Install** to install the TAP adapter.



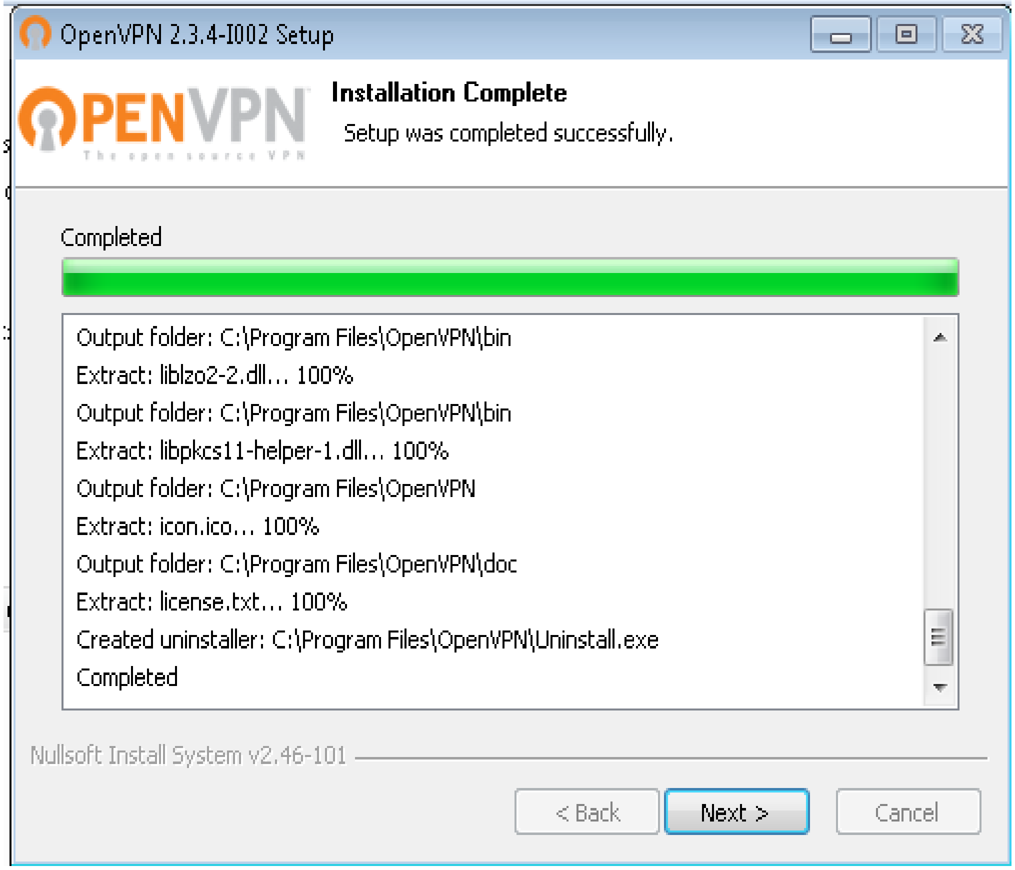
Would you like to install this device software?

Name: TAP-Windows Provider V9 Network adapters
Publisher: OpenVPN Technologies, Inc.

□ Always trust software from "OpenVPN Technologies, Inc.".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

31. Click **Next** at the Installation Complete Setup wizard.



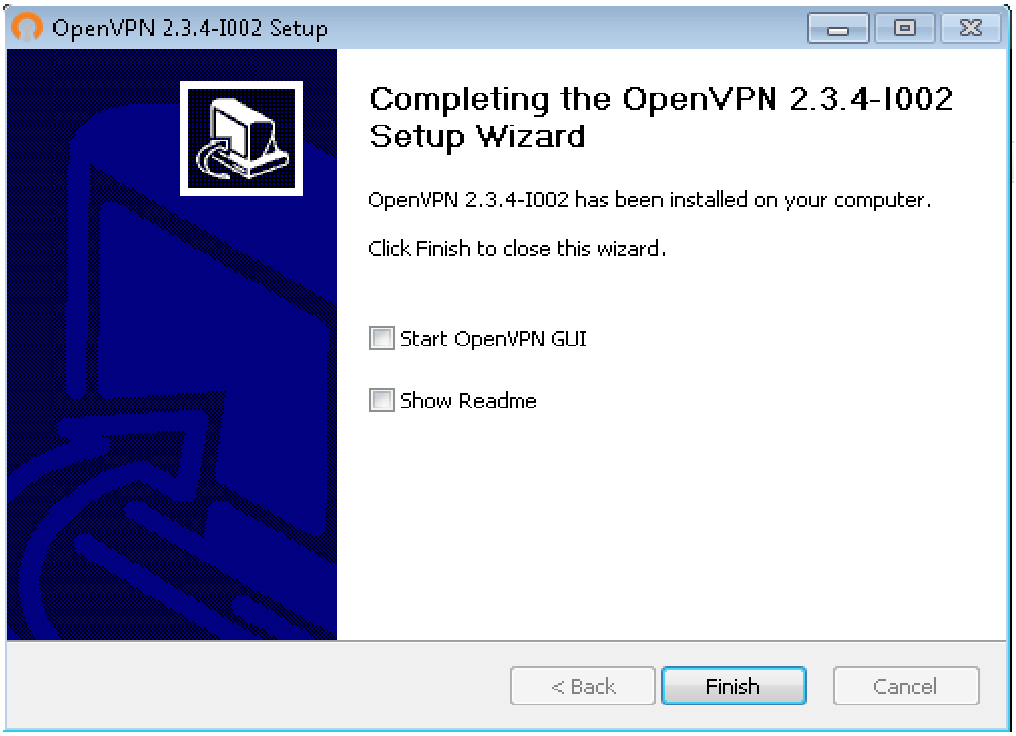
Installation Complete

Setup was completed successfully.

Completed

```
Output folder: C:\Program Files\OpenVPN\bin
Extract: liblzo2-2.dll... 100%
Output folder: C:\Program Files\OpenVPN\bin
Extract: libpkcs11-helper-1.dll... 100%
Output folder: C:\Program Files\OpenVPN
Extract: icon.ico... 100%
Output folder: C:\Program Files\OpenVPN\doc
Extract: license.txt... 100%
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Completed
```

32. Unclick Show Readme and click **Finish**.



Completing the OpenVPN 2.3.4-I002 Setup Wizard

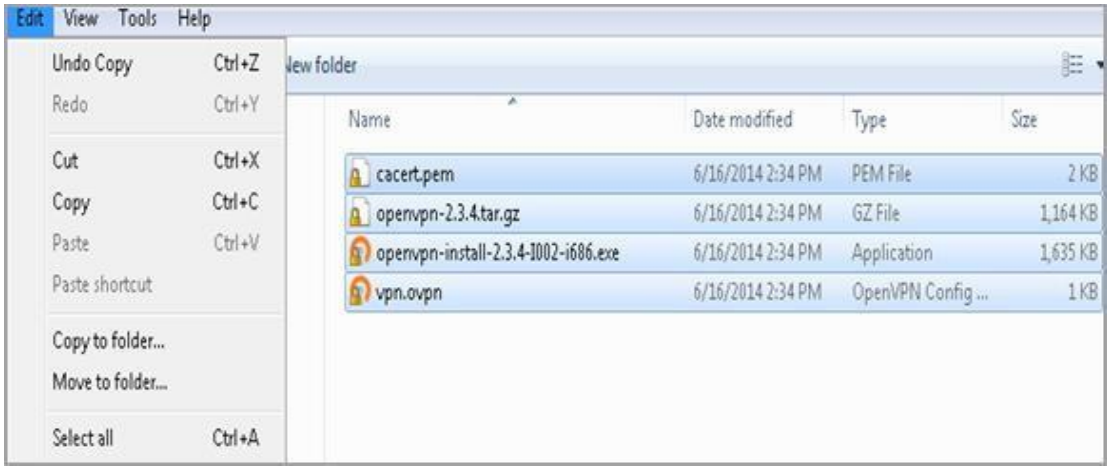
OpenVPN 2.3.4-I002 has been installed on your computer.

Click Finish to close this wizard.

☐ Start OpenVPN GUI

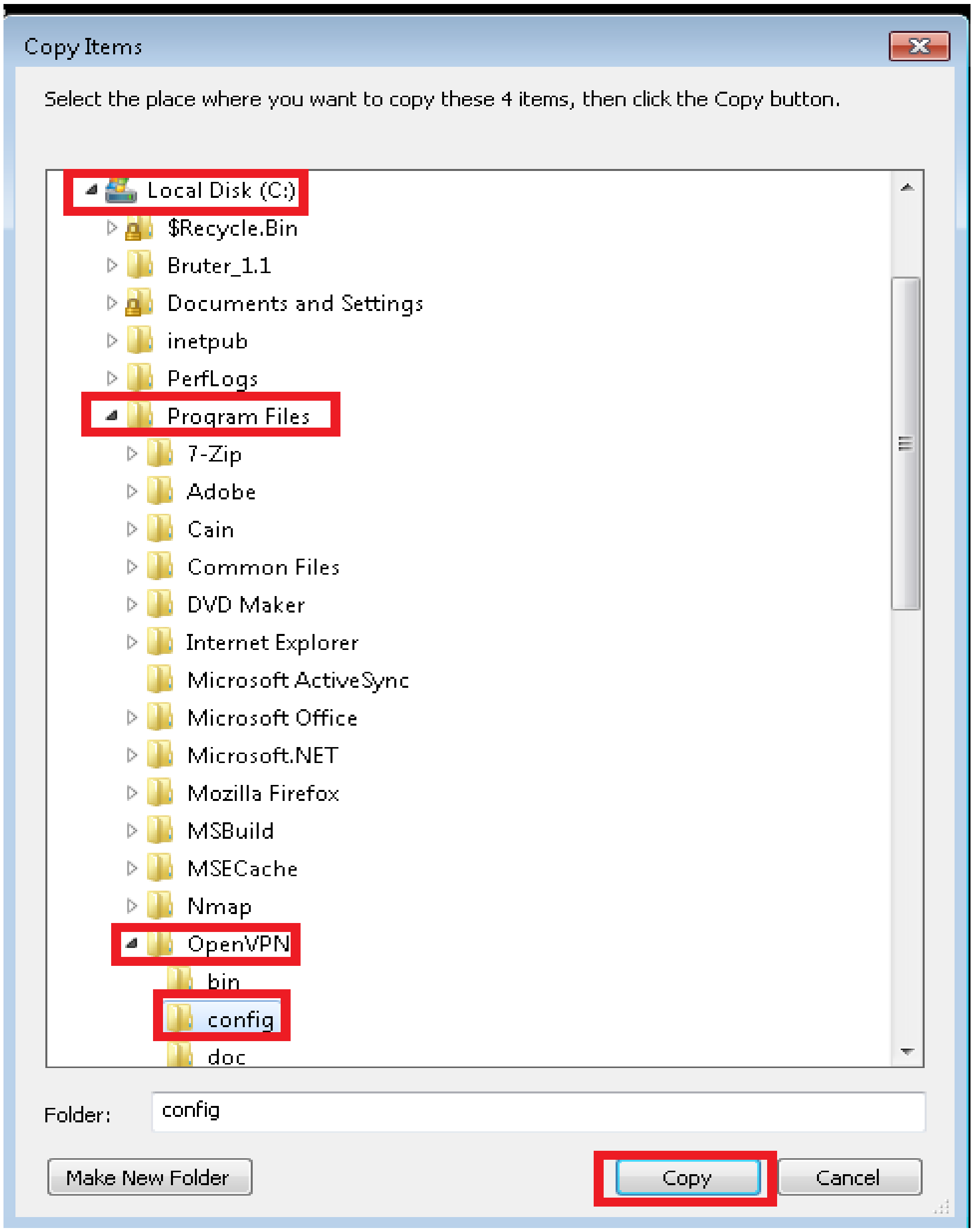
☐ Show Readme

33. After the install has completed, we will need to copy all of the files in the VPN directory to the config folder of the OpenVPN folder within Program Files. Select Edit from the menu bar, and choose **Select all**.



Name	Date modified	Type	Size
cacert.pem	6/16/2014 2:34 PM	PEM File	2 KB
openvpn-2.3.4.tar.gz	6/16/2014 2:34 PM	GZ File	1,164 KB
openvpn-install-2.3.4-I002-i686.exe	6/16/2014 2:34 PM	Application	1,635 KB
vpn.ovpn	6/16/2014 2:34 PM	OpenVPN Config ...	1 KB

34. Select Edit again and select copy to folder. Navigate to **Local Dick C: > Program Files > Open VPN**, and then select the config directory. Click the **Copy** button.

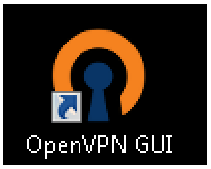


Copy Items

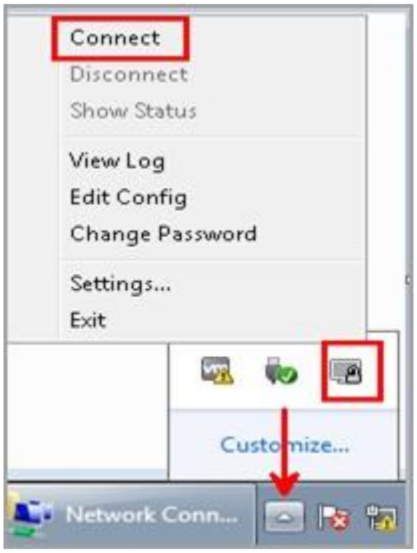
Select the place where you want to copy these 4 items, then click the Copy button.

Folder: config

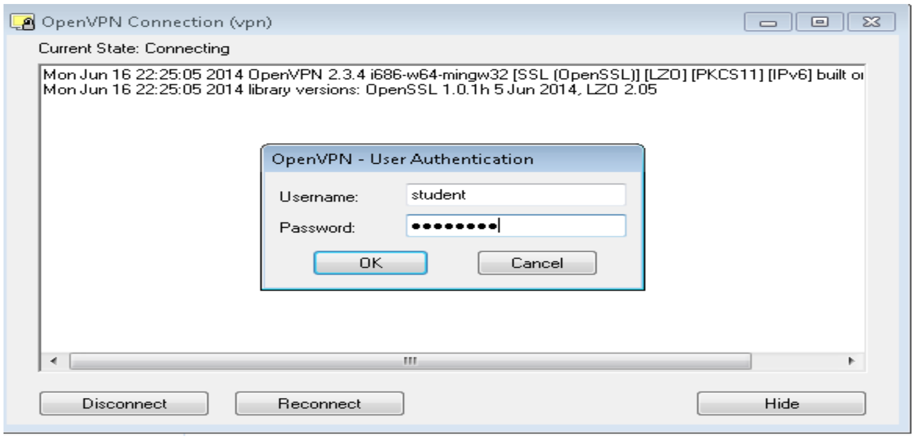
35. Double-click on the OpenVPN GUI shortcut on the desktop.



36. Click the arrow on the right side of the taskbar. Right-click the grey OpenVPN icon and click **Connect**.



37. For the username, put **student** and for the password, type **password.** Click OK**.**


OpenVPN Connection (vpn)

Current State: Connecting

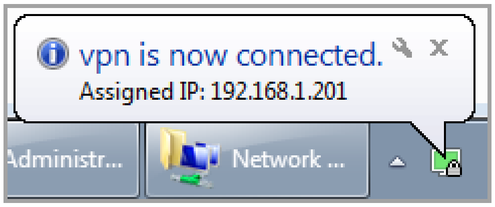
```
Mon Jun 16 22:25:05 2014 OpenVPN 2.3.4 i686-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [IPv6] built o
Mon Jun 16 22:25:05 2014 library versions: OpenSSL 1.0.1h 5 Jun 2014, LZO 2.05
```

OpenVPN - User Authentication

Username: student

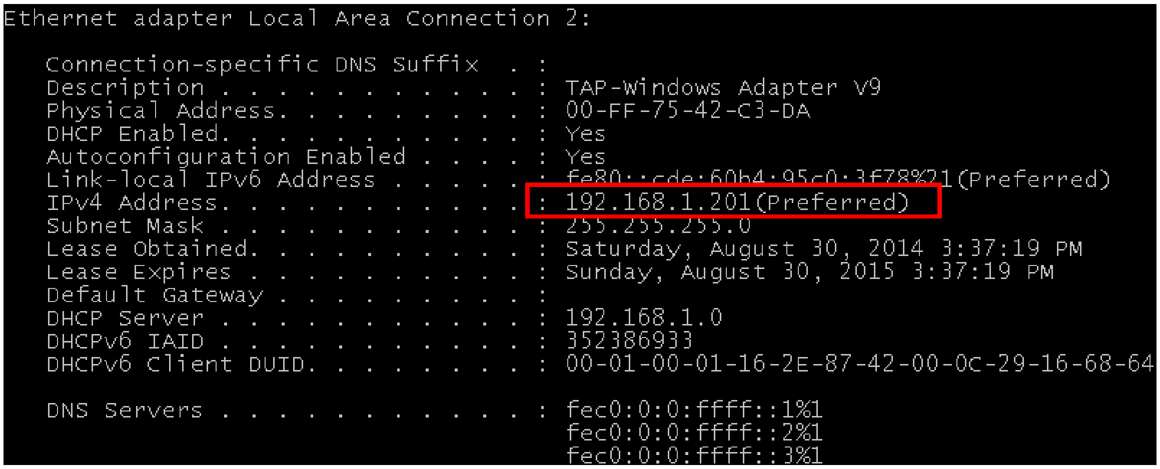
Password: ●●●●●●●●●

38. After the connection is successful, you will see a green icon in the right corner and notification of assigned IP address.


vpn is now connected.

Assigned IP: 192.168.1.201

39. Open a Command Prompt and type the following command on the External Windows 7 External Machine:
    C:\>**ipconfig /all**



```
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-75-42-C3-DA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cde:60b4:95c0:3f78%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.201(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, August 30, 2014 3:37:19 PM
   Lease Expires . . . . . . . . . . : Sunday, August 30, 2015 3:37:19 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.1.0
   DHCPv6 IAID . . . . . . . . . . . : 352386933
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-16-2E-87-42-00-0C-29-16-68-64

   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
```

Scroll up to view the IP address assigned to Ethernet adapter Local Area Connection2

2.2 Conclusion

When you use a Virtual Private Network (VPN), users can connect to internal systems and access resources. Users must have accounts with proper credentials in order to successfully authenticate to the server. After establishing a VPN connection with a remote server, the client will be issued an IP address allowing internal access.

2.3 Discussion Questions

1. Where do you go to connect to an OpenVPN server in Windows 7?
   Ans: Launch Open VPN GUI icon on the system.

2. Where do you configure user accounts in the OpenVPN settings?
   Ans: User accounts are generally configured on the OpenVPN server, rather than in the OpenVPN client software by entering the username and password of VPN.

3. When the client software is installed, what device is added to the system?
   Ans: When the client software Is installed, then adaptor is added to the system is Open VPN.

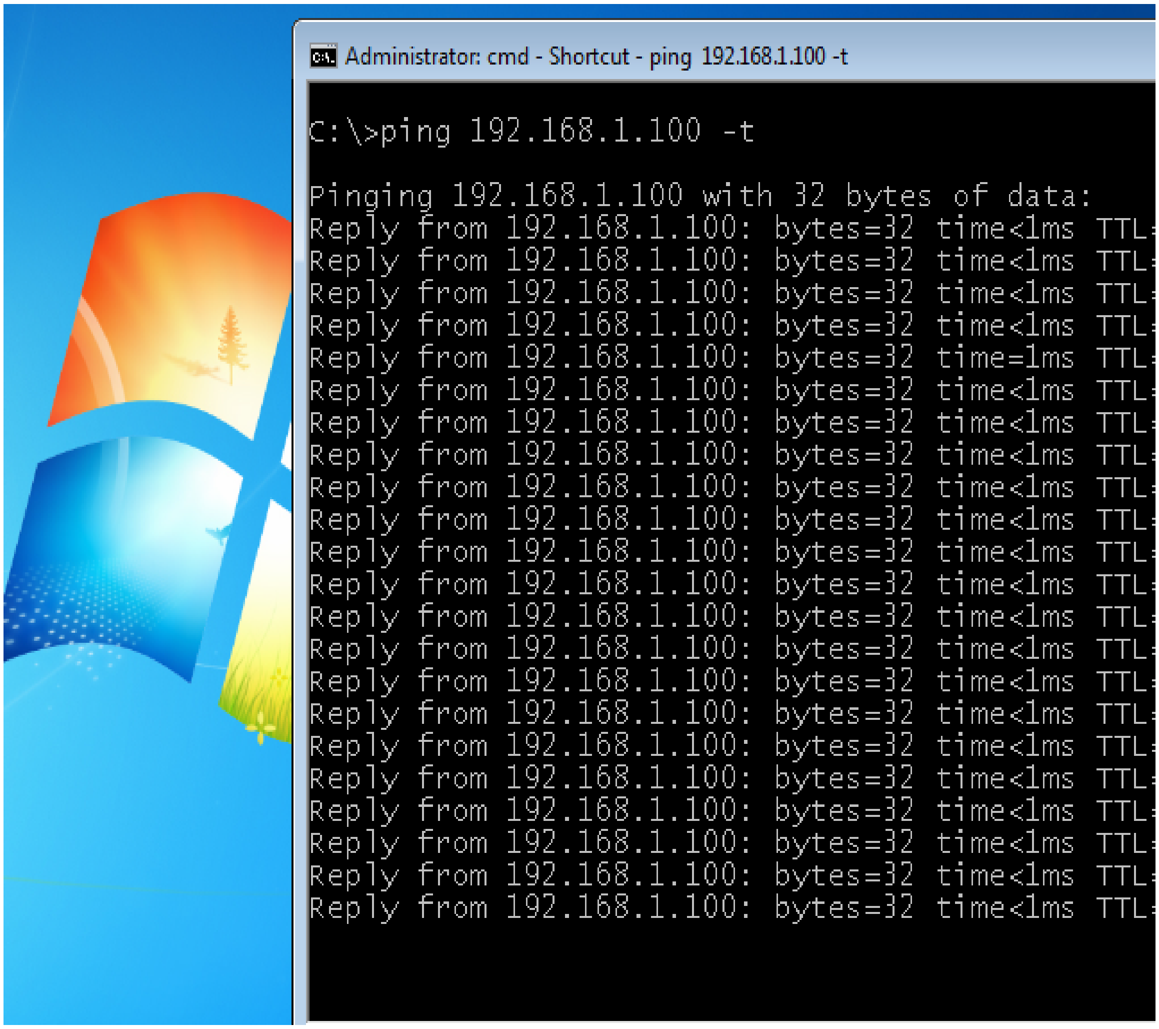
4. After connecting to a VPN server, will you have an additional address?
   Ans: Yes, after connecting to a VPN server, your computer will typically be assigned an additional IP address from the server's IP address. Because when you connect to a VPN server, your traffic is routed through the server's network and appears from the server's IP address.

3 Using Internal Services from an External Machine

Now that we have successfully connected to the VPN server and received an IP address on the 192.168.1.0/24 network, we can access some of the company's internal resources, all over a secure connection.

3.1 Testing the Firewall

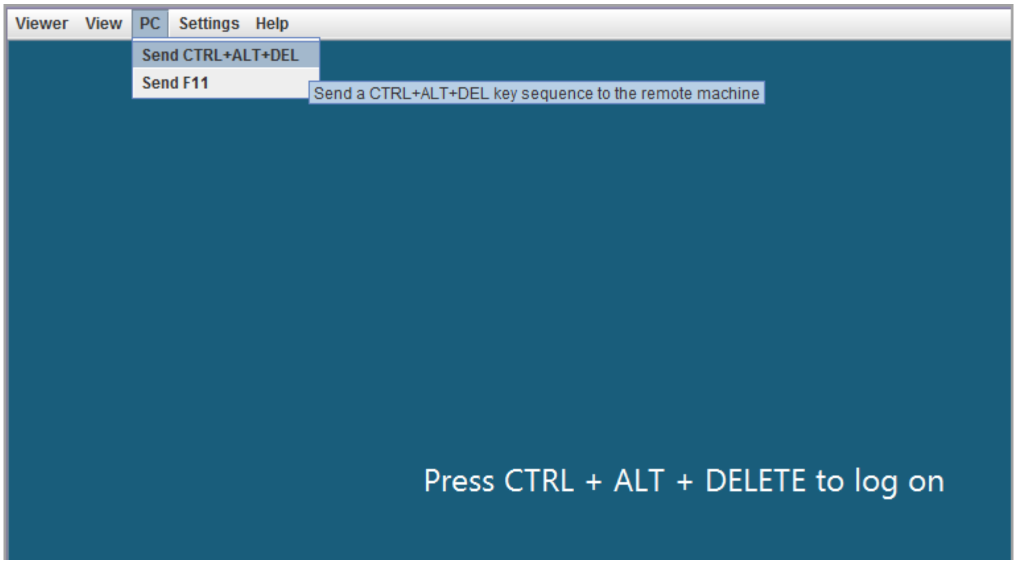
1. On the **Windows 7 External Machine**, type the following to continuously ping the internal Windows 2008 server machine that is a Domain Controller and running IIS:
   C:\>**ping 192.168.1.100 -t**



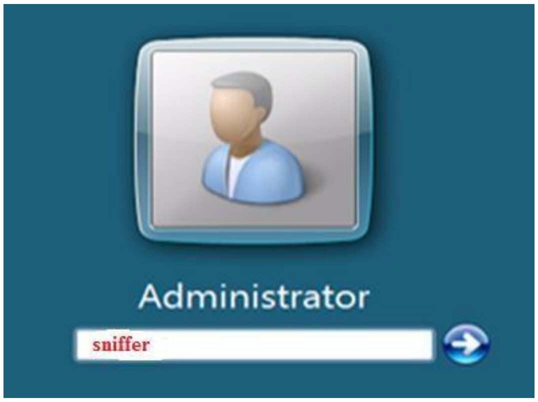
```
C:\>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time=1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
```

Do not stop the ping. At a later time, you can press **Ctrl+C** to stop the ping.

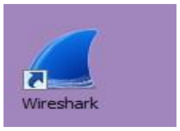
2. Log into the **Windows 2008 Server Sniffer** by clicking the Windows 2008 Sniffer icon on the topology. Click **PC** in the upper-left and **Send Ctrl+Alt+Del** in order to log on to the Windows 2008 server.


Viewer
View
PC
Settings
Help
Send CTRL+ALT+DEL
Send F11
Send a CTRL+ALT+DEL key sequence to the remote machine
Press CTRL + ALT + DELETE to log on

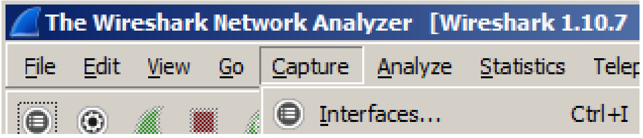
3. Enter **sniffer** for the Administrator password to the Windows 2008 Server.



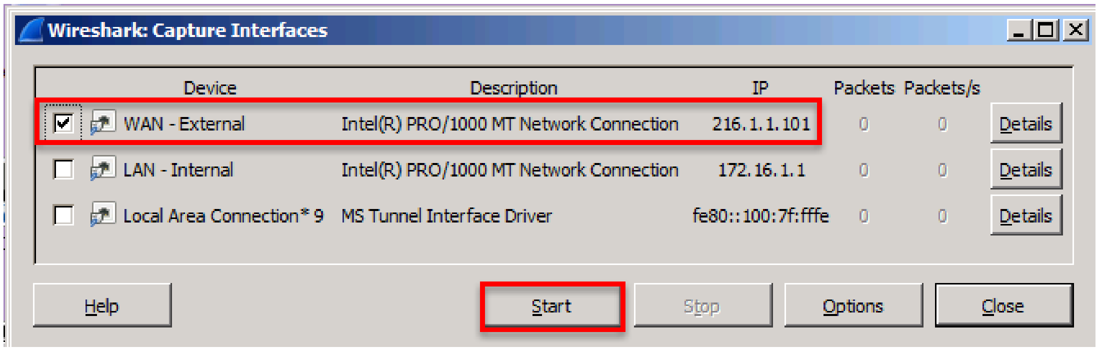
4. Click on the Shortcut to **Wireshark** on the desktop to launch the program.



5. Click on Capture from the menu bar and select **Interfaces**.

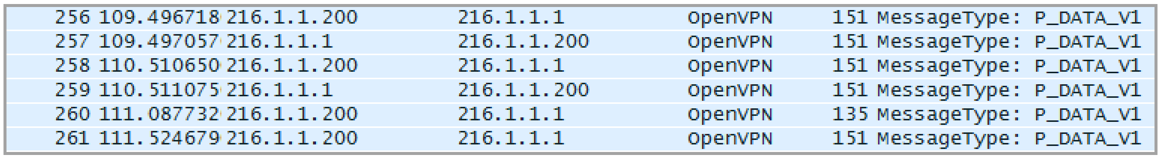


6. Select the **WAN – External** interface check-box. Click **Start**.



	Device	Description	IP	Packets	Packets/s	
☑	WAN - External	Intel(R) PRO/1000 MT Network Connection	216.1.1.101	0	0	Details
□	LAN - Internal	Intel(R) PRO/1000 MT Network Connection	172.16.1.1	0	0	Details
□	Local Area Connection* 9	MS Tunnel Interface Driver	fe80::100:7f:fffe	0	0	Details

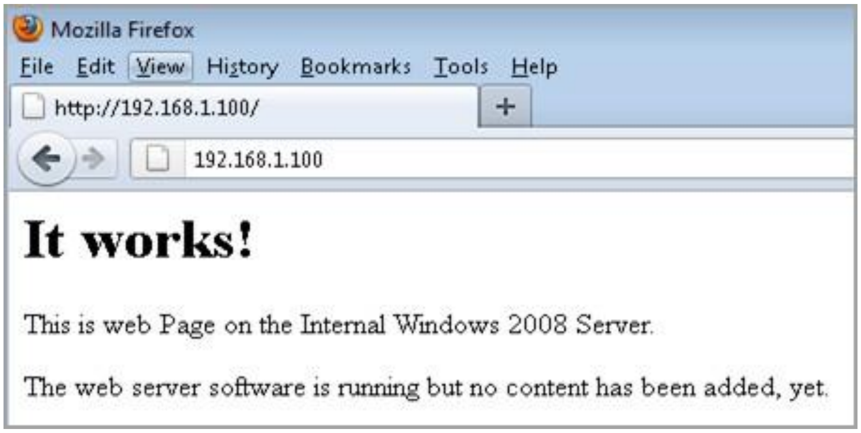
7. Notice the OpenVPN traffic is displayed. Close Wireshark. Click on Stop and Quit without Saving for Wireshark.



```
256 109.496718 216.1.1.200      216.1.1.1        OpenVPN     151 MessageType: P_DATA_V1
257 109.497057 216.1.1.1        216.1.1.200      OpenVPN     151 MessageType: P_DATA_V1
258 110.510650 216.1.1.200      216.1.1.1        OpenVPN     151 MessageType: P_DATA_V1
259 110.511075 216.1.1.1        216.1.1.200      OpenVPN     151 MessageType: P_DATA_V1
260 111.087732 216.1.1.200      216.1.1.1        OpenVPN     135 MessageType: P_DATA_V1
261 111.524679 216.1.1.200      216.1.1.1        OpenVPN     151 MessageType: P_DATA_V1
```

8. On the **Windows 7 External Machine**, close the command prompt. Click on the shortcut to Mozilla Firefox on the desktop.

9. Type **http://192.168.1.100** in the URL bar to connect to the internal web site.



192.168.1.100

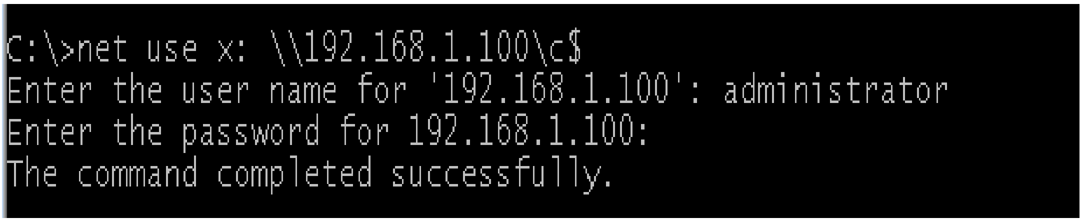
It works!

This is web Page on the Internal Windows 2008 Server.

The web server software is running but no content has been added, yet.

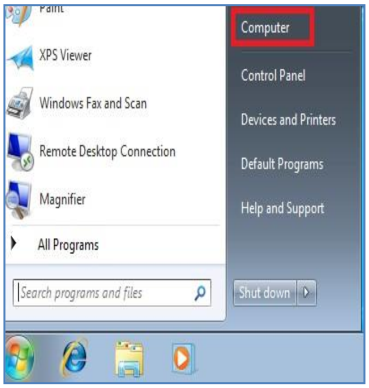
10. From the Windows 7 External Machine, open command prompt and type the following command:
    C:\>**net use x: \\192.168.1.100\c$**

    When you are asked to enter the user name, type **administrator**
    When you are asked for the password, type **P@ssw0rd**

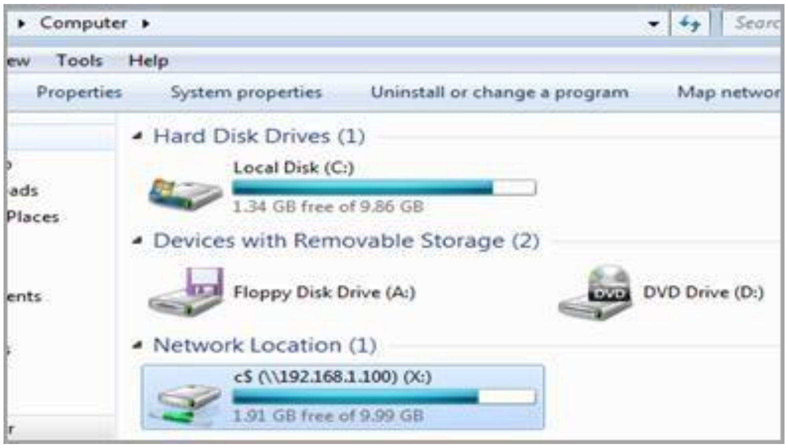


```
C:\>net use x: \\192.168.1.100\c$
Enter the user name for '192.168.1.100': administrator
Enter the password for 192.168.1.100:
The command completed successfully.
```

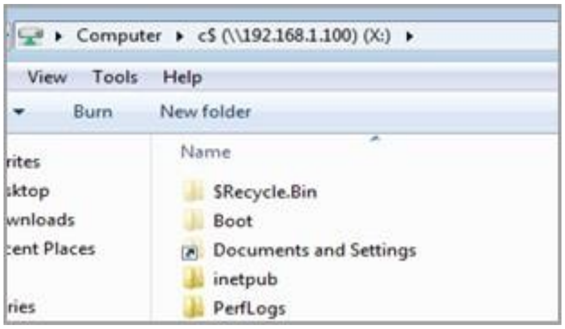
11. Click on the **Start** button and go to the **Computer** link.



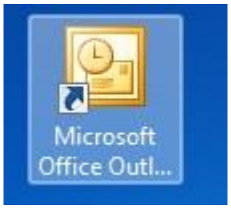
12. Double-click the Network Location Link for - c$ (\\192.168.1.100) (X:)



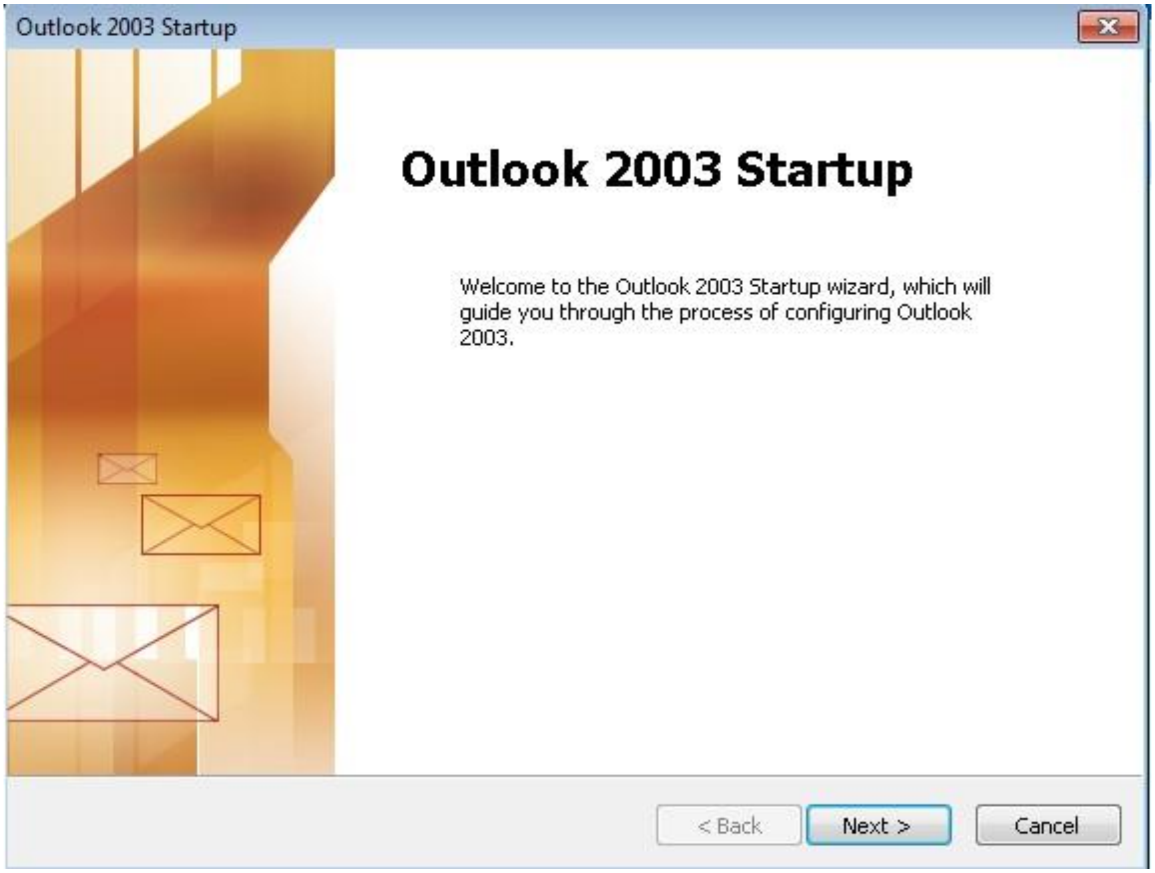
13. View the C: Drive of the Remote Computer.



14. On the Windows 7 External Machine desktop, click on the shortcut to Outlook.



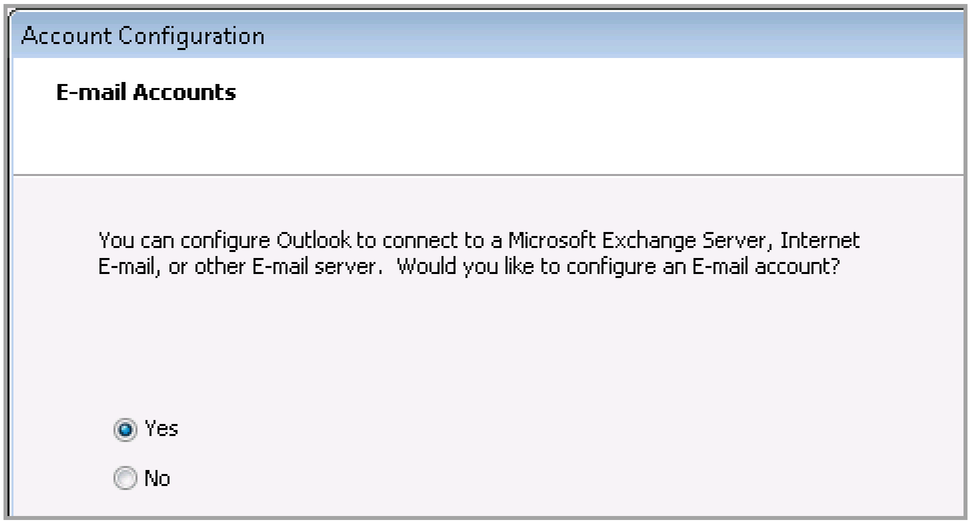
15. Click Next on the Outlook Setup screen. Click **Next** on the Account Configuration screen.



Outlook 2003 Startup

Welcome to the Outlook 2003 Startup wizard, which will guide you through the process of configuring Outlook 2003.

16. On the Account Configuration window, click **Next**.



Account Configuration

E-mail Accounts

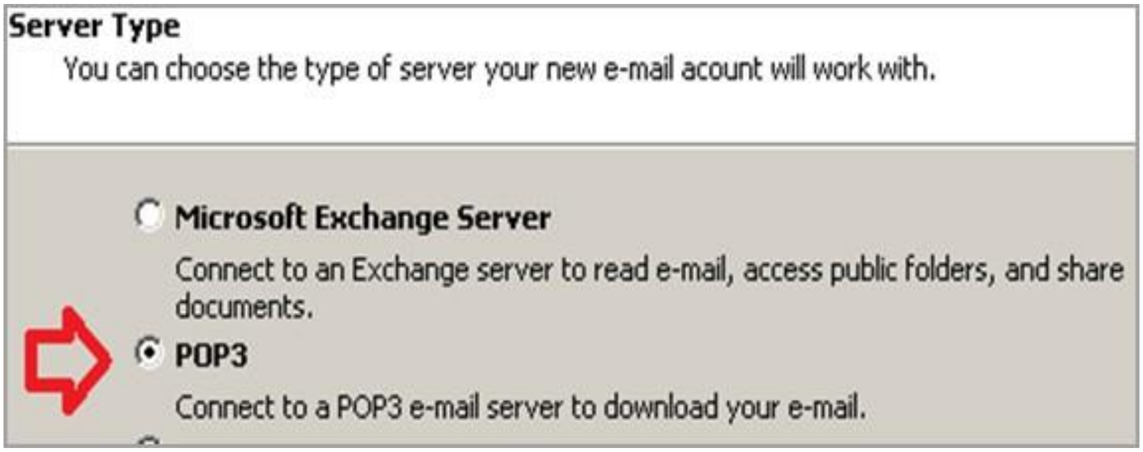
You can configure Outlook to connect to a Microsoft Exchange Server, Internet E-mail, or other E-mail server. Would you like to configure an E-mail account?

● Yes

○ No

`

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



Server Type

You can choose the type of server your new e-mail acount will work with.

○ Microsoft Exchange Server

Connect to an Exchange server to read e-mail, access public folders, and share documents.

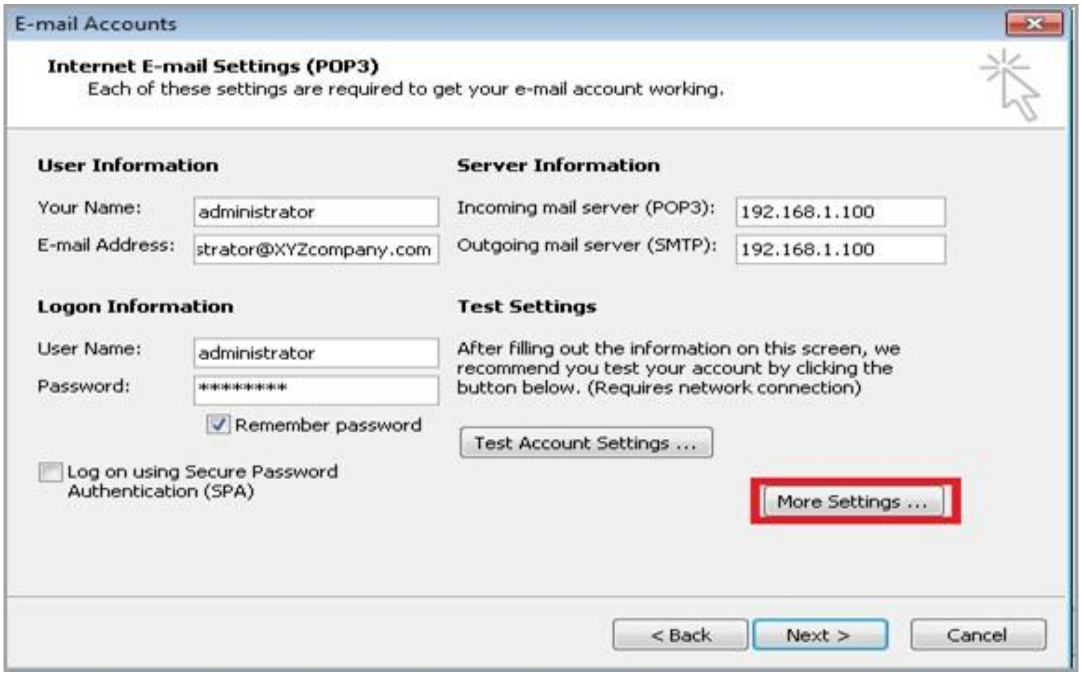
● POP3

Connect to a POP3 e-mail server to download your e-mail.

18. Fill out the following fields:

Name	administrator
Email Address	administrator@XYZcompany.com
User Name	administrator
Password	P@ssw0rd
Incoming and Outgoing Server	192.168.1.100 (Internal Mail)

19. Click the **More Settings** button.



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: administrator
E-mail Address: strator@XYZcompany.com

Logon Information

User Name: administrator
Password: *********

☑ Remember password

☐ Log on using Secure Password Authentication (SPA)

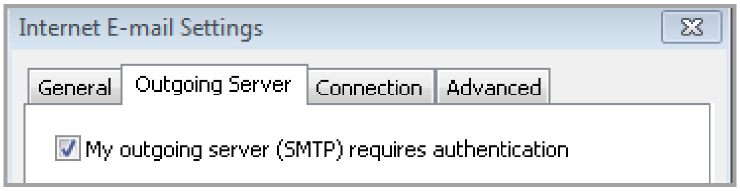
Server Information

Incoming mail server (POP3): 192.168.1.100
Outgoing mail server (SMTP): 192.168.1.100

Test Settings

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

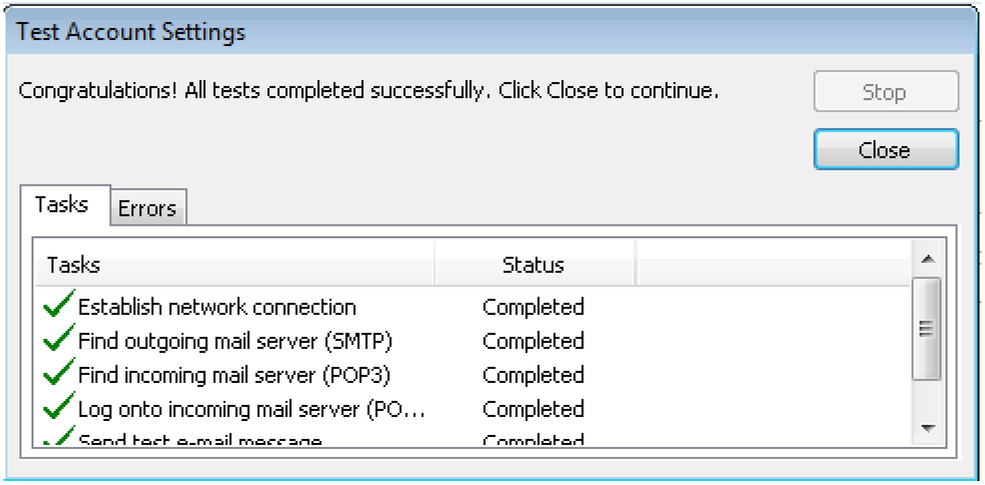
20. Click on the Outgoing Server tab and check the box that states **My outgoing server (SMTP) requires authentication**. Click **Ok**.



Internet E-mail Settings

☑ My outgoing server (SMTP) requires authentication

21. Click the Test Account Settings Button. You should receive 5 green checks.


Test Account Settings

Congratulations! All tests completed successfully. Click Close to continue.

Tasks	Status
✓ Establish network connection	Completed
✓ Find outgoing mail server (SMTP)	Completed
✓ Find incoming mail server (POP3)	Completed
✓ Log onto incoming mail server (PO...	Completed
✓ Send test e-mail message	Completed

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

3.2 Conclusion

In this section of the lab, we connected to the resources on the internal network, including an internal website, a share on the Domain Controller, and we used Internal Email. OpenVPN connections allow users to work from home as if they were on the physical computer network, all over an encrypted connection over the Internet.

3.3 Discussion Questions

1. What is the command to map a drive?
   Ans: The command to map a drive enter net use z:\\computer\folder.

2. How can you view a mapped drive?
   Ans: To view the mapped drive the command is -net .

3. What Wireshark interface will capture traffic on the internal network?
   Ans: The interface that need to select to capture traffic on the internal network will depend on network setup and the specific interface that internal network traffic is flowing through.

4. What Wireshark interface will capture traffic on the External network?
   Ans: The network interface that is connected to the external network. This may be a wired Ethernet interface, a wireless interface, or a virtual interface if using virtualization software.

s

References

1. nmap:
   www.nmap.org

2. OpenVPN:
   http://openvpn.net/

3. VPN:
   http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs

4. Endian Firewall:
   http://www.endian.com/us/#.U5-sUmzD8dU

5. More Open VPN Information:
   http://en.wikipedia.org/wiki/OpenVPN