Secure VPN Configuration and Management

Module 09

Lab 1

Establishing VPN Connection using OpenVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections

Lab Scenario

VPN allows communicating securely with different computers over insecure channels. It uses the Internet and ensures secure communication to distant offices or individual users in their enterprise's network. As a network administrator you need to know how to establish a VPN connection for your organization.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Objectives

This lab will demonstrate on how to establish a VPN connection using OpenVPN.

Lab Environment

To carry out the lab, you need:

- Download OpenVPN from the link **https://openvpn.net/index.php/open-source/downloads.html**
- You can download configuration files from **http://www.vpnbook.com**
- A virtual machine running Windows Server 2012
- A Web browser with Internet connection
- **Administrative** privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of OpenVPN

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using a signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

Lab Tasks

TASK 1

Installing and configuring OpenVPN

1. Launch **Windows Server 2012**
2. Navigate to **Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\Open VPN** and double-click **OpenVPN-install-2.3.11-I001-x86_64.exe** to start the installation
3. If an **Open File – Security Warning** window appears click **Run** and follow the wizard driven installation steps to install

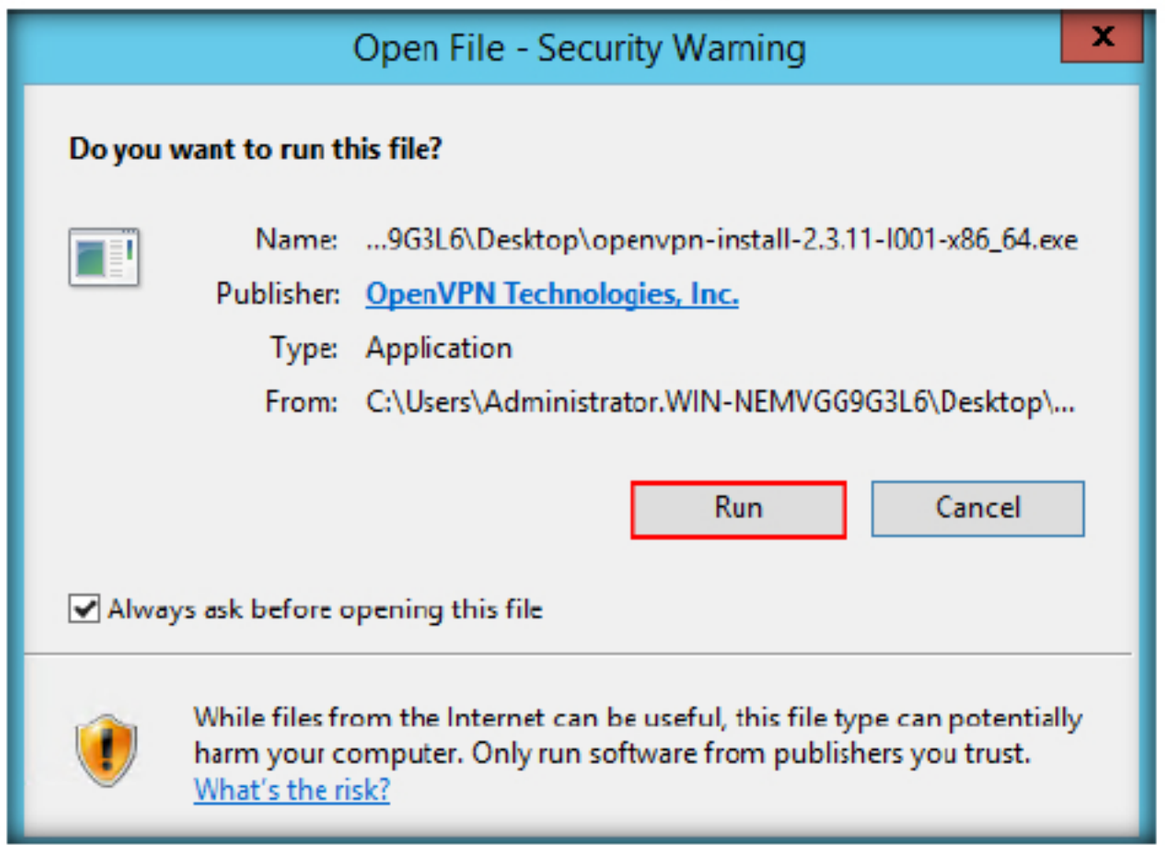

FIGURE 1.1: Windows security warning

4. While installing **Windows Security** pop-up appears as shown in the screenshot, click **Install**, and follow the wizard driven instructions and complete the installation

When OpenVPN is started as a service, a separate OpenVPN process will be instantiated for each configuration file.

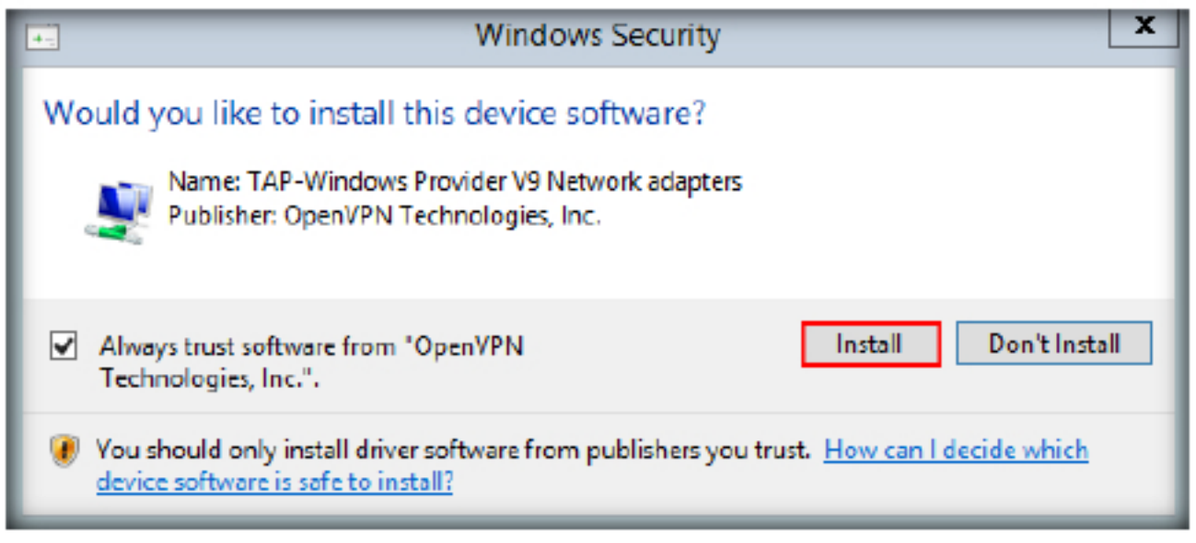

FIGURE 1.2: Windows device software warning

5. After completing the installation, check **Start OpenVPN GUI** option and uncheck **Show Readme** option and click **Finish** in order to launch OpenVPN once the installation is completed

   Note: Alternatively you can also launch from Installed start menu apps or by double-clicking the short-cut icon on the Desktop.

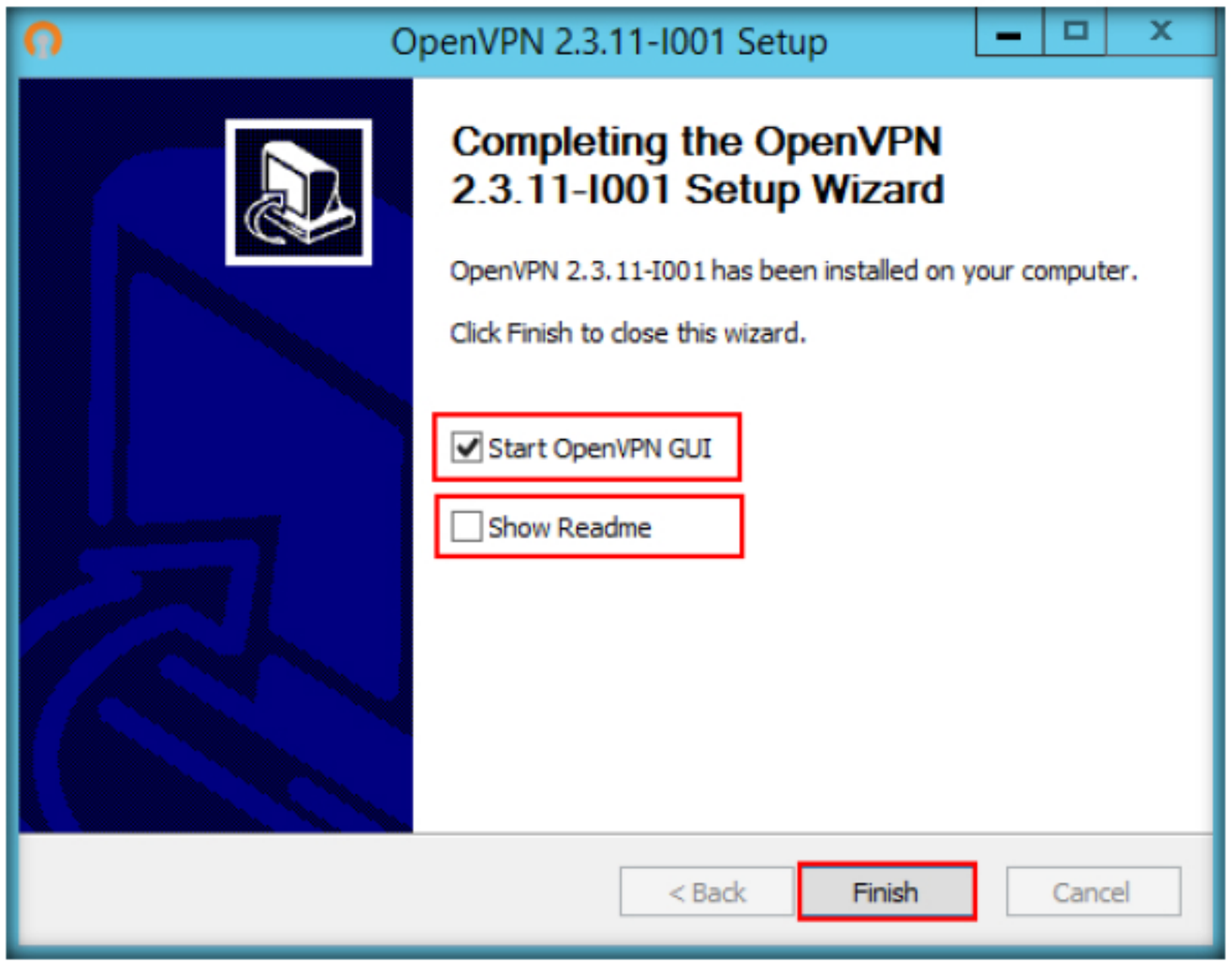

FIGURE 1.3: OpenVPN GUI

6. After clicking the **Finish** button the OpenVPN GUI icon appears in the Notification area with the status offline (Grey in Color) as shown in the screenshot

7. In this lab we are demonstrating how to connect to Open VPN networks that are available, to do this we have placed Open VPN configuration files in the following location **Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\Open VPN Config Files**

FIGURE 1.4: OpenVPN GUI in Notification Area

8. Navigate to **Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\Open VPN Config Files\TCP** and copy the **vpngate_2016-2.opengw.net_tcp_443.ovpn**

📖 The VPN server is the underlying component in OpenVPN Access Server that does all of the background work; routing, tunneling, encryption, user management, authentication etc. OpenVPN Access Server comes with a Web GUI that helps to manage the underlying components of the VPN server.

📖 OpenVPN application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

9. Paste the file in the following location **C:\Program Files\OpenVPN\config**

   Note: If you have your own VPN configuration file, you can place that file in the following location

📖 OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

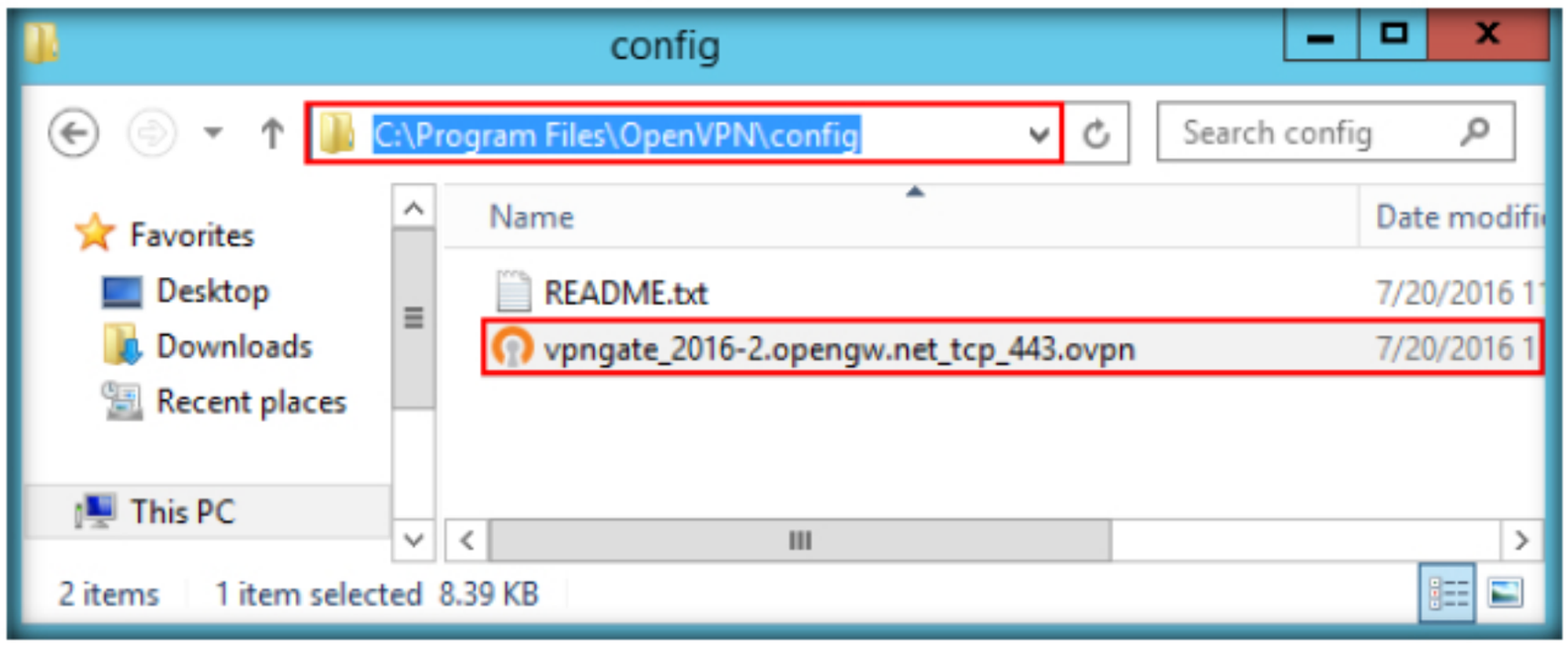

FIGURE 1.5: Sample OpenVPN Configuration File

10. Close the **config** folder and right click the **Windows** icon and select **Command Prompt** from the context menu

📖 OpenVPN has been ported and embedded to several systems. For example, DD-WRT has the OpenVPN server function. SoftEther VPN, a multi-protocol VPN server, has an implementation of OpenVPN protocol.

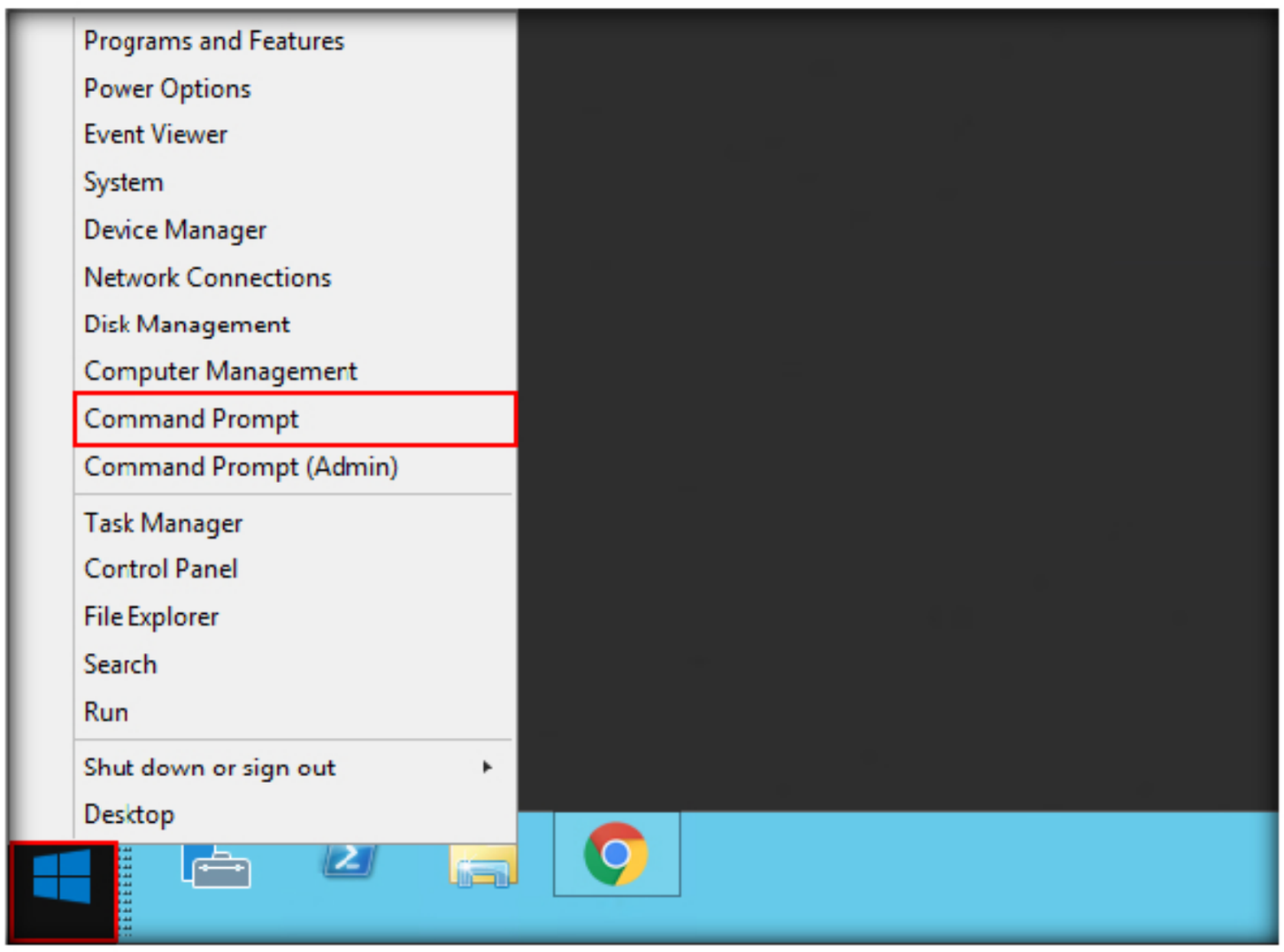

FIGURE 1.6: Navigating to Command prompt

11. Type **ipconfig** to check the system IP address.(Here, it is 10.10.10.12)

Note: IP addresses may vary in your lab environment, if you have assigned different IP addresses to your machines.

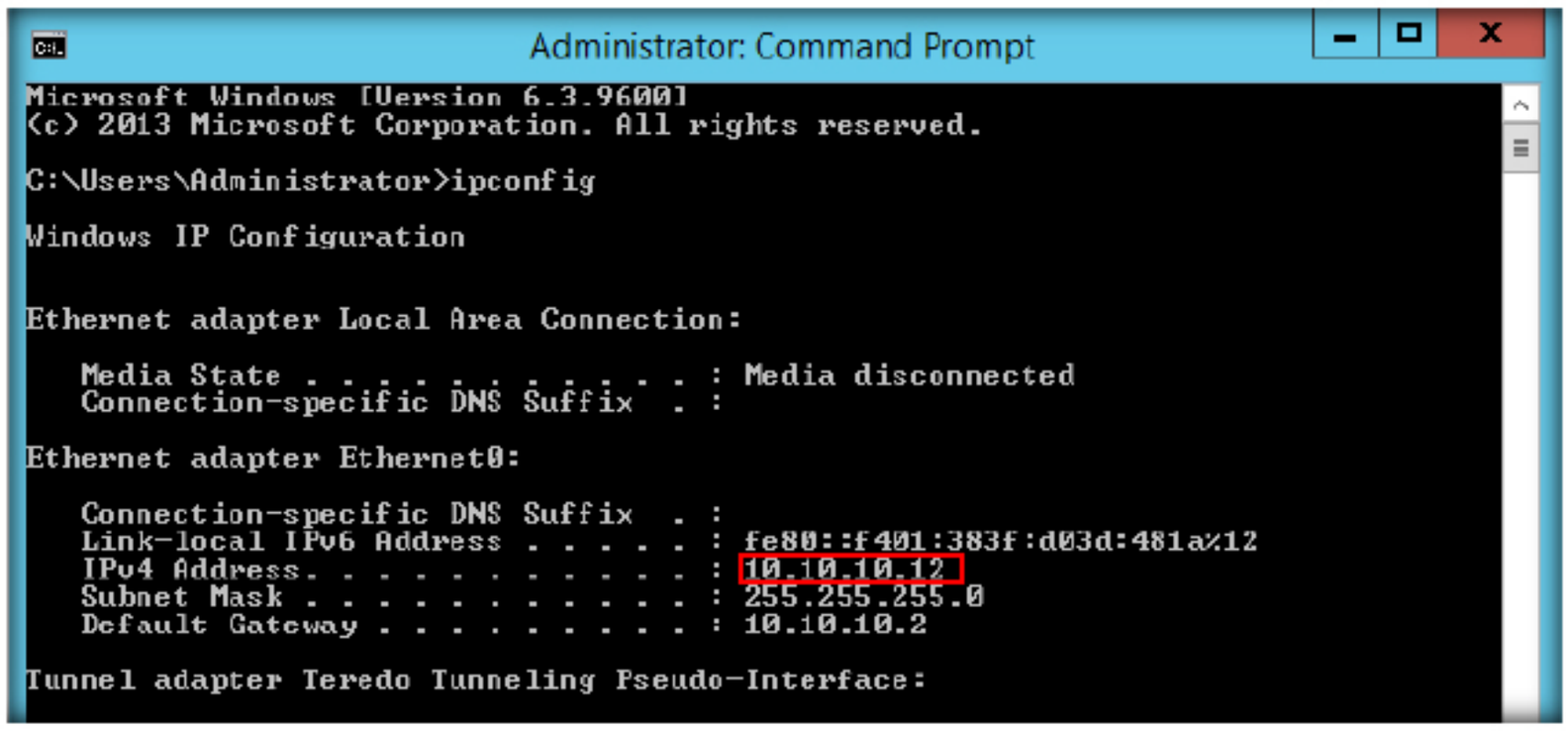

FIGURE 1.7: Checking System IP address

12. Minimize the **Command Prompt** window and click the up arrow in the system tray. You will find the **OpenVPN GUI**

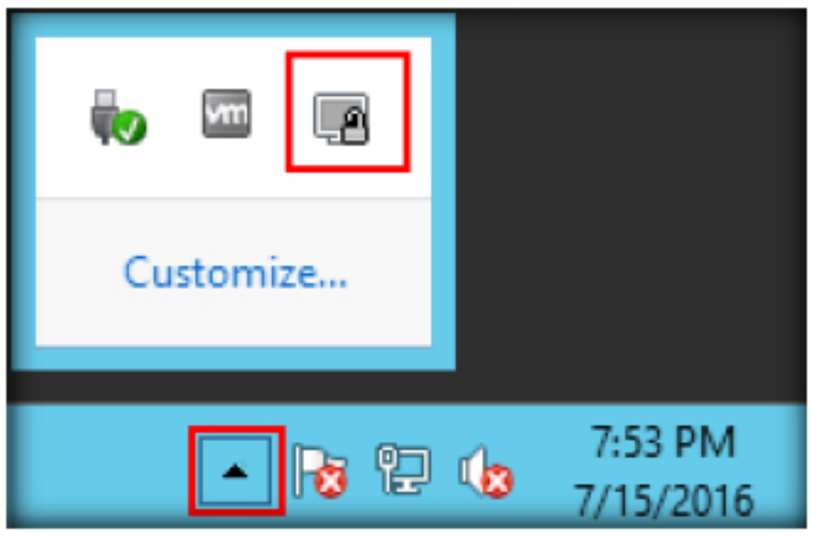

FIGURE 1.8: Starting Open VPN

13. Right-click **OpenVPN GUI** and select **Connect** from the context menu

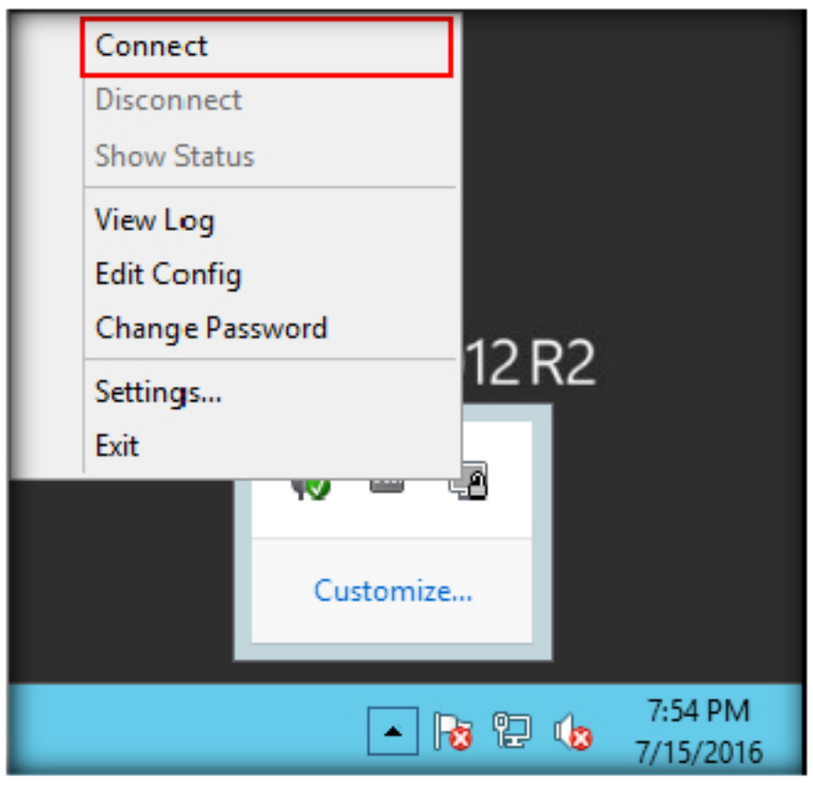

FIGURE 1.9: Connecting to VPN

OpenVPN uses the OpenSSL library to provide encryption of both the data and control channels. It lets OpenSSL do all the encryption and authentication work, allowing OpenVPN to use all the ciphers available in the OpenSSL package. It can also use the HMAC packet authentication feature to add an additional layer of security to the connection (referred to as an "HMAC Firewall" by the creator). It can also use hardware acceleration to get better encryption performance.

TASK 2

Establishing Connection with OpenVPN

14. As soon as you click Connect from the context menu, OpenVPN will initiate the connection to the provided OpenVPN network in configuration file

    Note: If the configuration file that is demonstrated in the lab doesn't work, you can choose one of the different configuration files that are placed in the following location Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\Open VPN Config Files. But before using another file delete the old configuration file and paste the other configuration file in the following location **C:\Program Files\OpenVPN\config and paste another file**

    If any of the configuration files ask for credentials, you can find the credentials in OpenVPN Credentials.txt file which is available in the following location Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\Open VPN Config Files.

📖 OpenVPN has several ways to authenticate peers with each other. OpenVPN offers pre-shared keys, certificate-based, and username/password-based authentication. Pre-shared secret key is the easiest, with certificate based being the most robust and feature-rich. In version 2.0 username/password authentications can be enabled, both with or without certificates. However to make use of username/password authentications, OpenVPN depends on third-party modules.

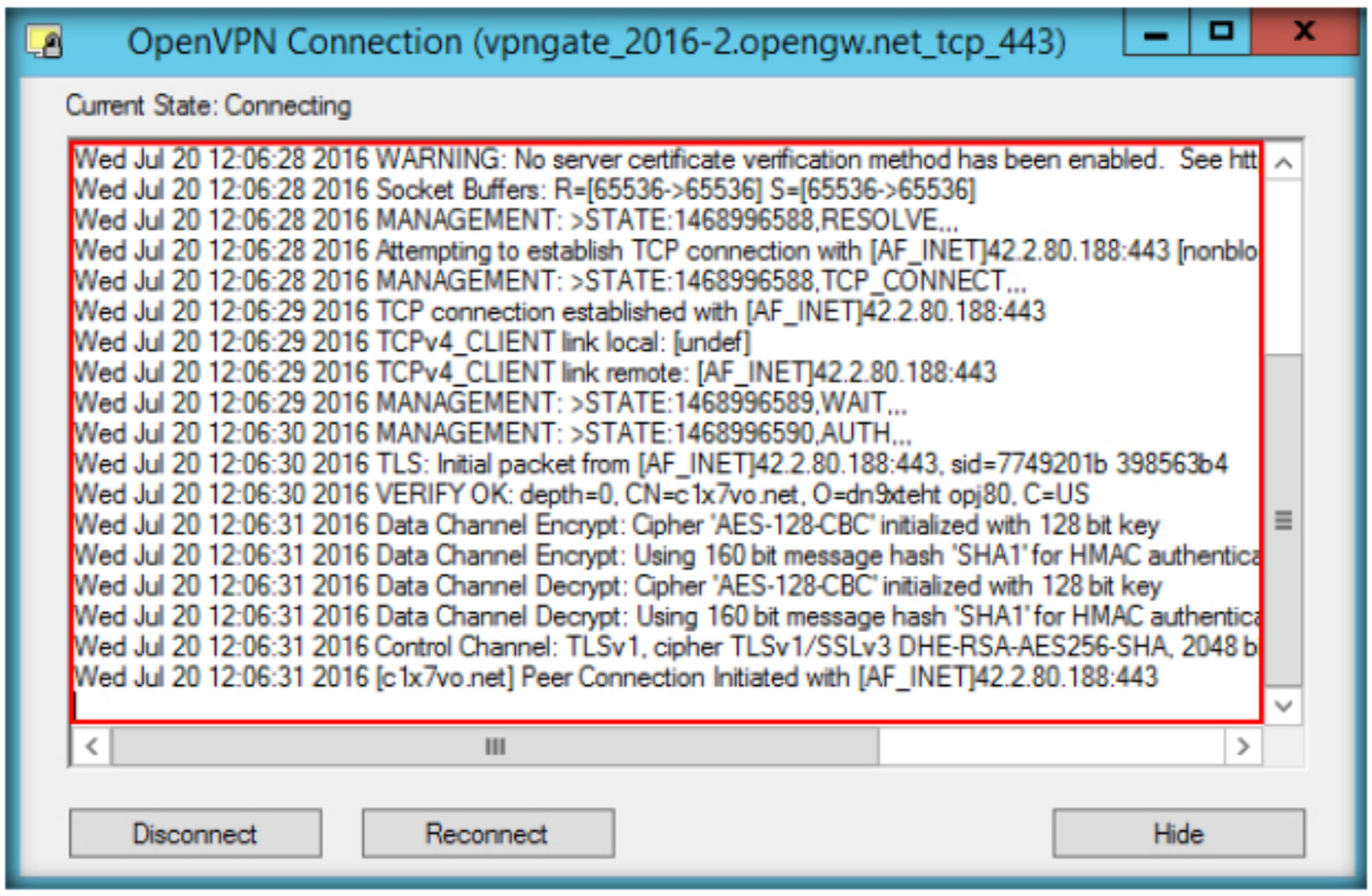

FIGURE 1.10: Logging in to VPN

📖 OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port (RFC 3948 for UDP).

15. Once the authentication is successful, a message will appear as shown in following screenshot in the Notification area. This indicates that the VPN connection is successfully established

16. A new IP will be assigned (10.211.2.33) and the Open VPN icon turns green.

    Note: The newly assigned IP address may vary in your environment.

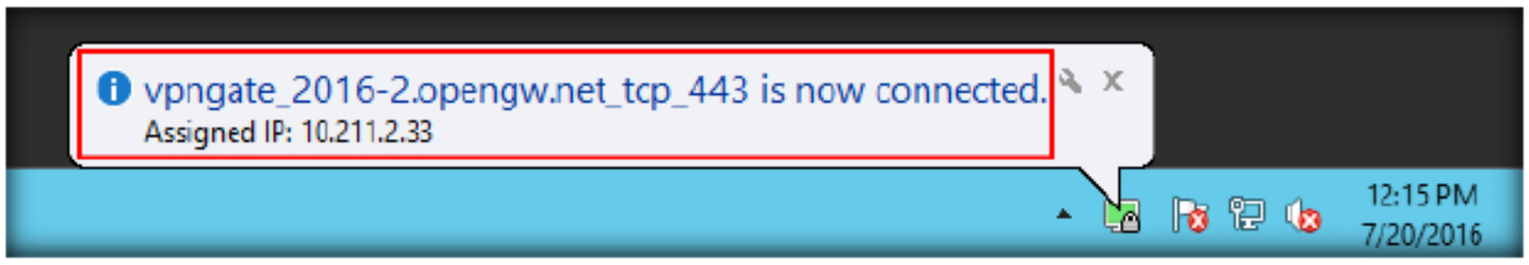

FIGURE 1.11: OpenVPN Connected and Newly Assigned IP Address

TASK 3

Verifying established VPN connection

17. To confirm whether a VPN is established or not, type **ipconfig /all** command on the Windows Command Prompt and check for a newly assigned IP address (10.211.2.33).

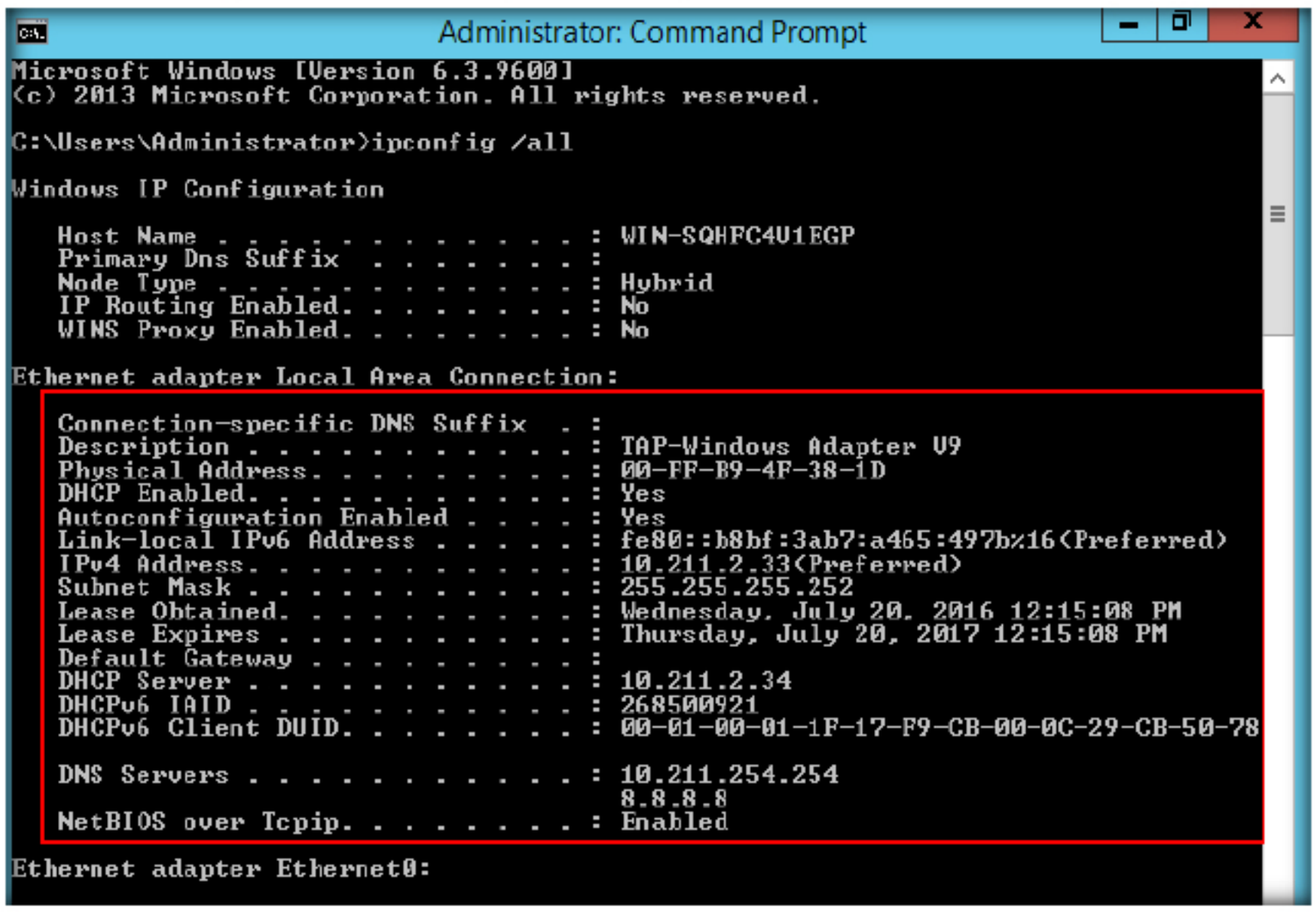

FIGURE 1.12: Checking VPN Configuration in Command Prompt

OpenVPN has the ability to work through most proxy servers (including HTTP) and is good at working through Network address translation (NAT) and getting out through firewalls.

18. Now when a VPN is established, all communications toward the Internet will be relayed via the VPN Server.

19. Type **tracert 8.8.8.8** in command prompt and press **Enter**

OpenVPN offers two types of interfaces for networking via the Universal TUN/TAP driver. It can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic.

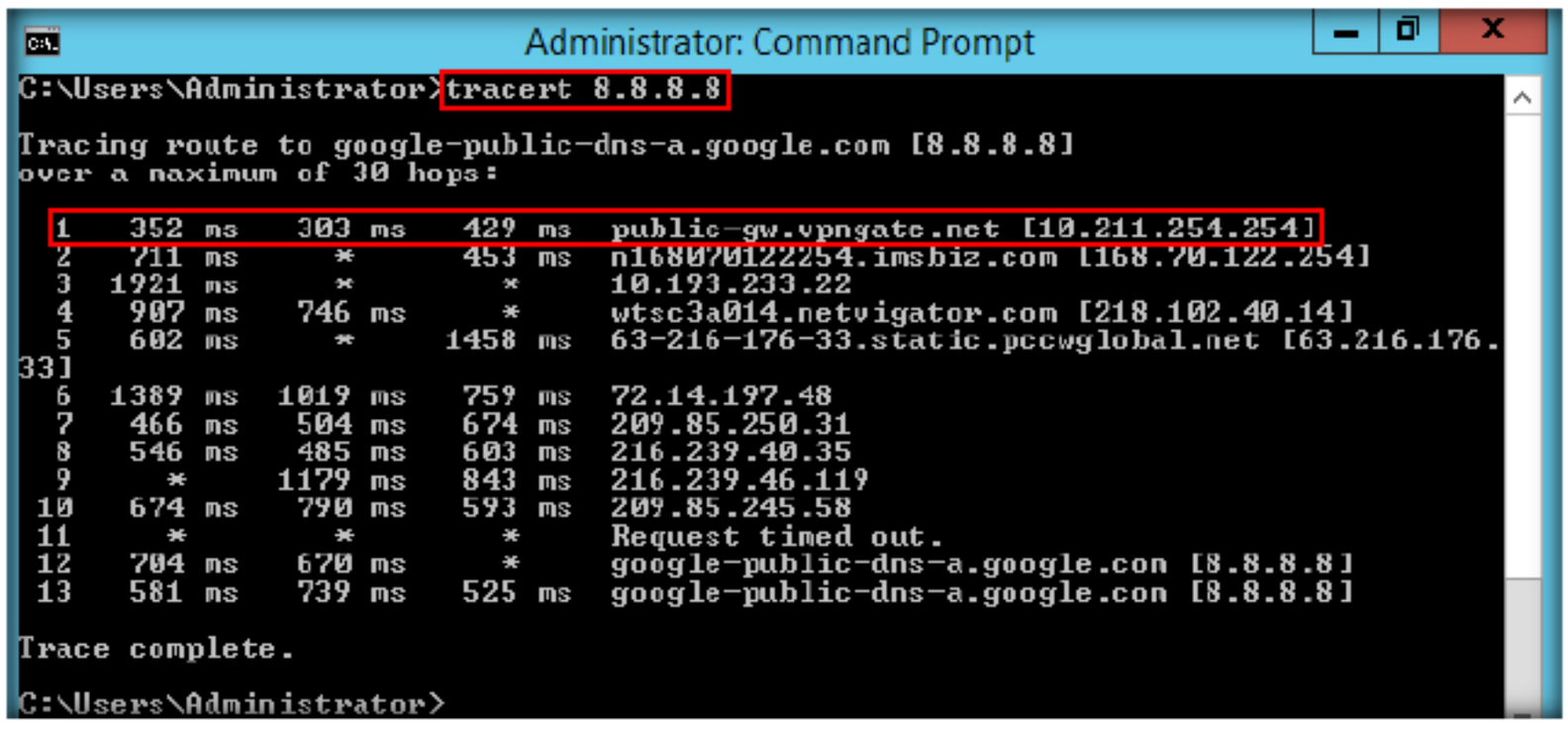

FIGURE 1.13: Verifying VPN Connectivity

20. From the above screenshot, it is concluded that packets are passing through the VPN network. Thus your communication is now relayed through OpenVPN.

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 2

Establishing VPN Connection using SoftEther VPN

SoftEther VPN Server, Client and Bridge are free software, and released as open-source. SoftEther VPN is an overly strong tool to build a VPN tunnel.

Lab Scenario

In an organization's network infrastructure, there are firewalls to isolate inside and outside network traffic to ensure security. Not only to resolve security issues, but also organizations use firewalls, proxies and NATs in order to share the IP addresses with the users in the office. These devices play a crucial role today.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Objectives

This lab will demonstrate on how to establish a VPN connection using SoftEther VPN.

Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows Server 2008
- A virtual machine running Windows 10
- Navigate to Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\SoftEther VPN
- A Web browser with Internet connection
- **Administrative** privileges to run tools
- If you have downloaded the latest version then screenshots will differ

Lab Duration

Time: 30 Minutes

Overview of SoftEther VPN

SoftEther VPN is one of the most powerful and easiest to use VPN software in the world. It is freeware. One of the key features of SoftEther VPN is the transparency for firewalls, proxy servers and NATs (Network Address Translators). NATs are sometimes implemented on broadband router products.

SoftEther VPN uses HTTPS protocol in order to establish a VPN tunnel. HTTPS (HTTP over SSL) protocol uses the 443 of TCP/IP port as destination. This port is well-known and almost all firewalls, proxy servers and NATs can pass the packet through using the HTTPS protocol.

Lab Tasks

TASK 1

Install SoftEther VPN

Note: Before starting this lab exercise, make a note of your public IP. To know your public IP open up any web browser and browser google.com. In google search type **what is my IP** and click **search**. It will display your public IP.

1. Launch **Windows Server 2008** and login as **Administrator**
2. To install SoftEther VPN, navigate to Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\SoftEther VPN and double-click **softether-vpnserver_vpnbridge-v4.21-9613-beta-2016.04.24-windows-x86_x64-intel.exe**

   Note: If the Open File – Security warning window appears click **Run**.
3. The SoftEther VPN setup wizard appears, click **Next** as shown in the screenshot

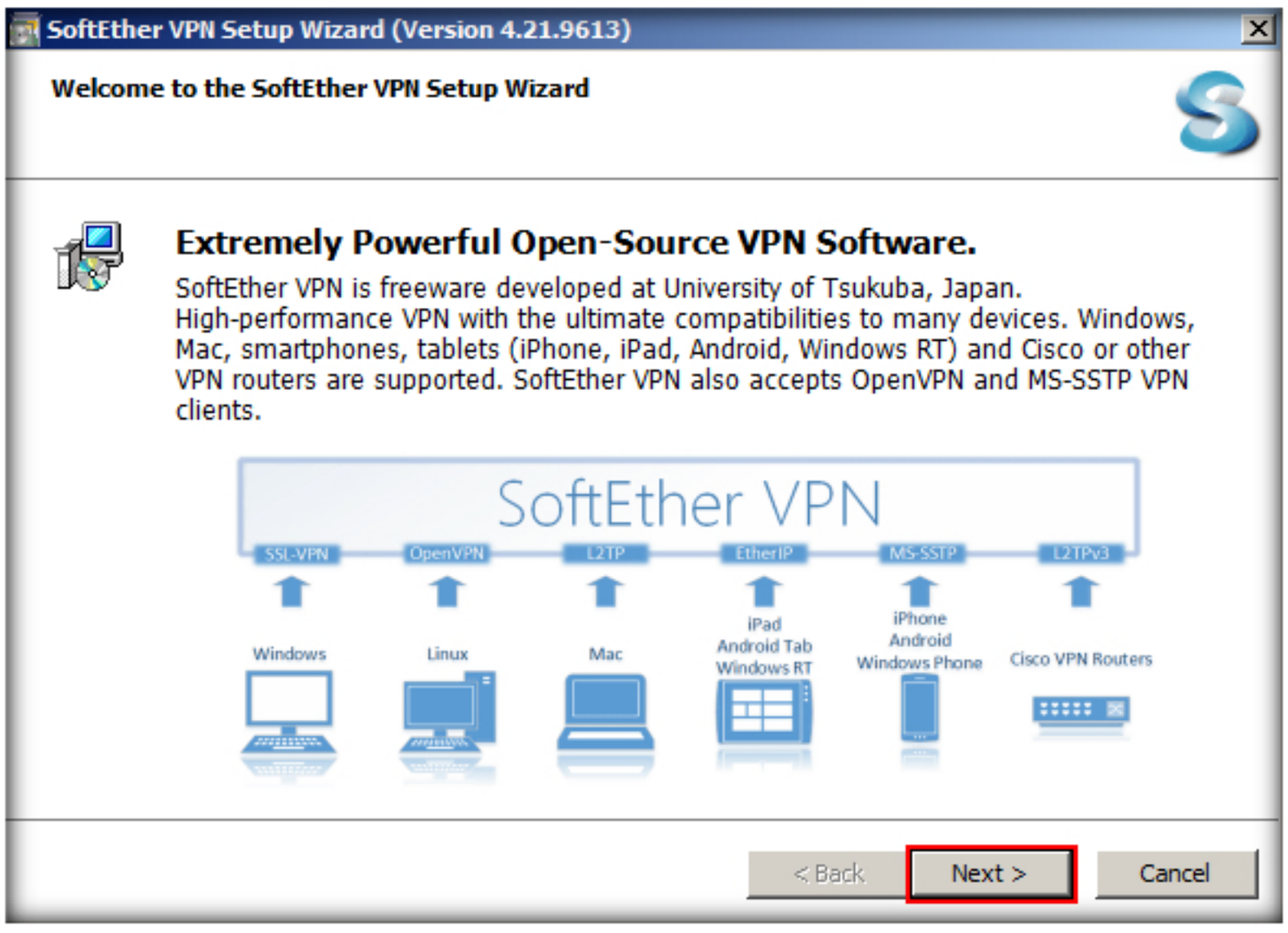

FIGURE 2.1: SoftEther VPN Server Setup Wizard

Virtualization of Ethernet devices is the key of the SoftEther VPN architecture. SoftEther VPN virtualizes Ethernet devices in order to realize a flexible virtual private network for both remote-access VPN and site-to-site VPN.

4. In the Software Components to install wizard, **SoftEther VPN Server** is selected by default, leave the selection as default and click **Next**

SoftEther VPN implements the Virtual Network Adapter program as a software-emulated traditional Ethernet network adapter. SoftEther VPN implements the Virtual Ethernet Switch program (called Virtual Hub) as a software-emulated traditional Ethernet switch.

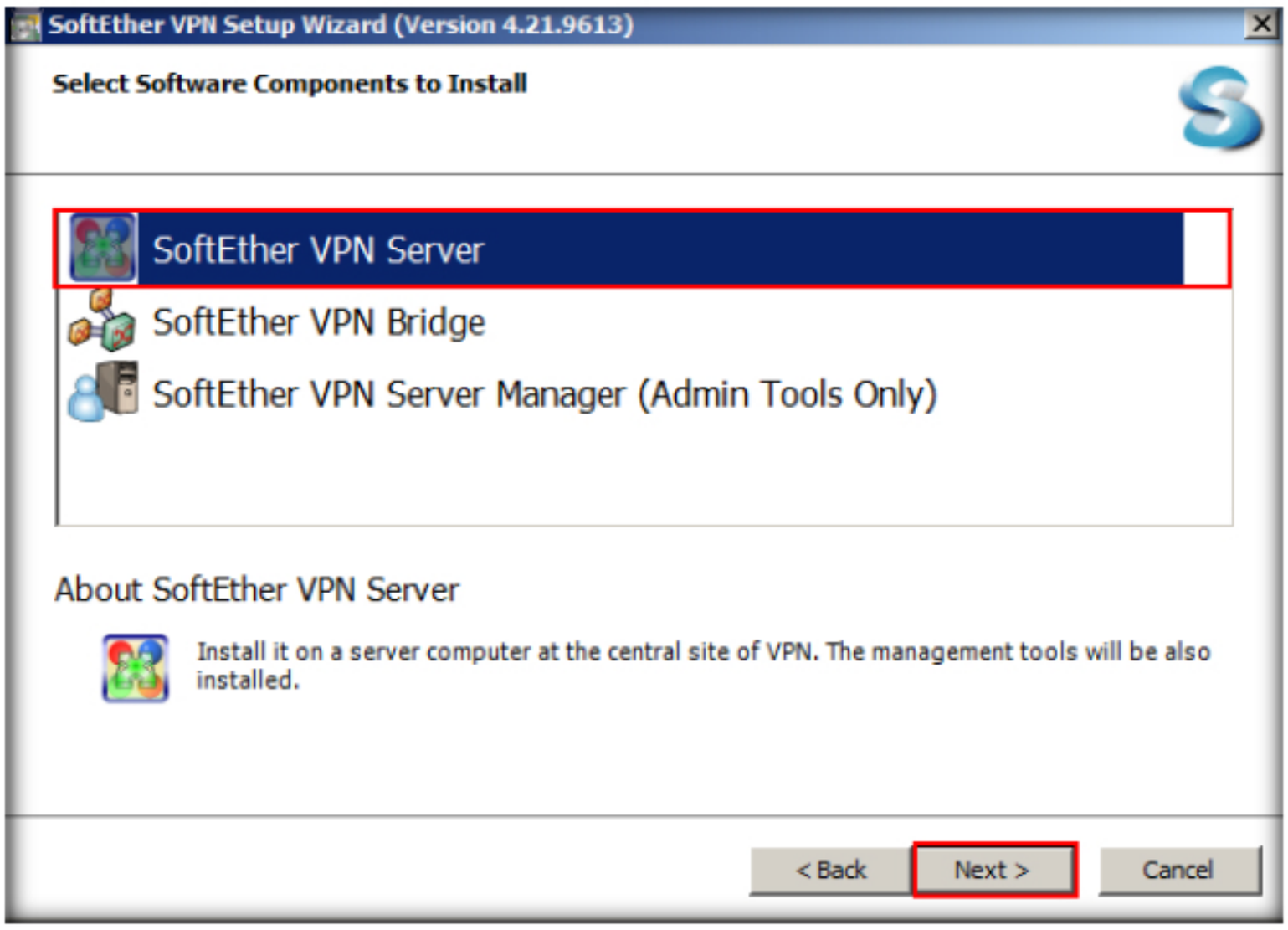

FIGURE 2.2: SoftEther VPN Server Software Components

5. End User License Agreement wizard appears, check **I agree to the End User License Agreement** check box and click **Next**
6. Follow the wizard driven installation steps to install **SoftEther VPN Server Manager**

SoftEther VPN implements a VPN Session as a software-emulated Ethernet cable between the network adapter and the switch.
You can create one or many Virtual Hubs with SoftEther VPN on your server computer. This server computer will become a VPN server, which accepts VPN connection requests from VPN client computers.

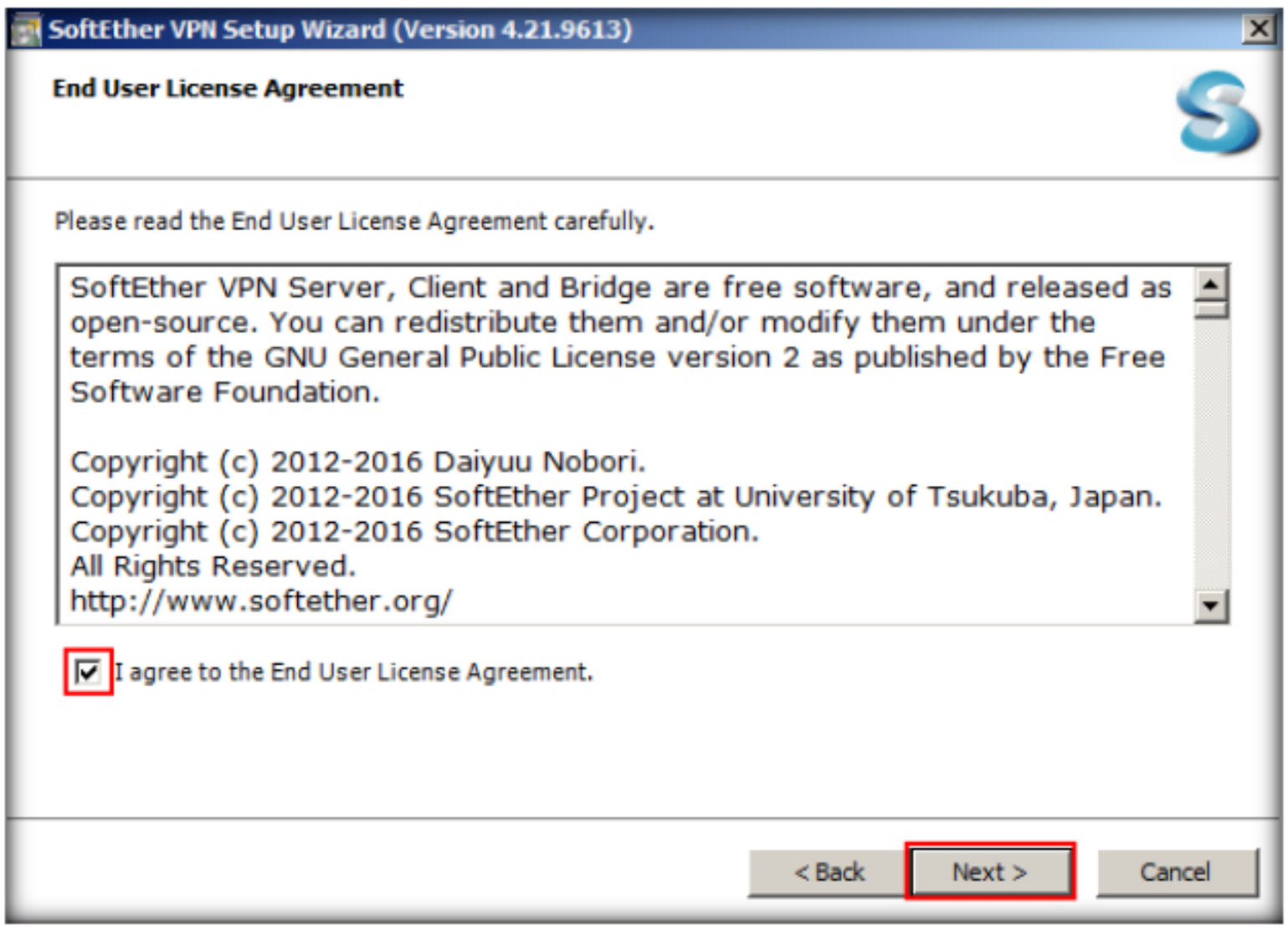

FIGURE 2.3: SoftEther VPN Server License Agreement

7. When the Setup Finished wizard appears after completing the installation, make sure that **Start the SoftEther VPN Server Manager** option is checked to launch automatically once you click **Finish**
   Note: Alternatively you can also launch the application by double-clicking the short-cut icon on the **Desktop**

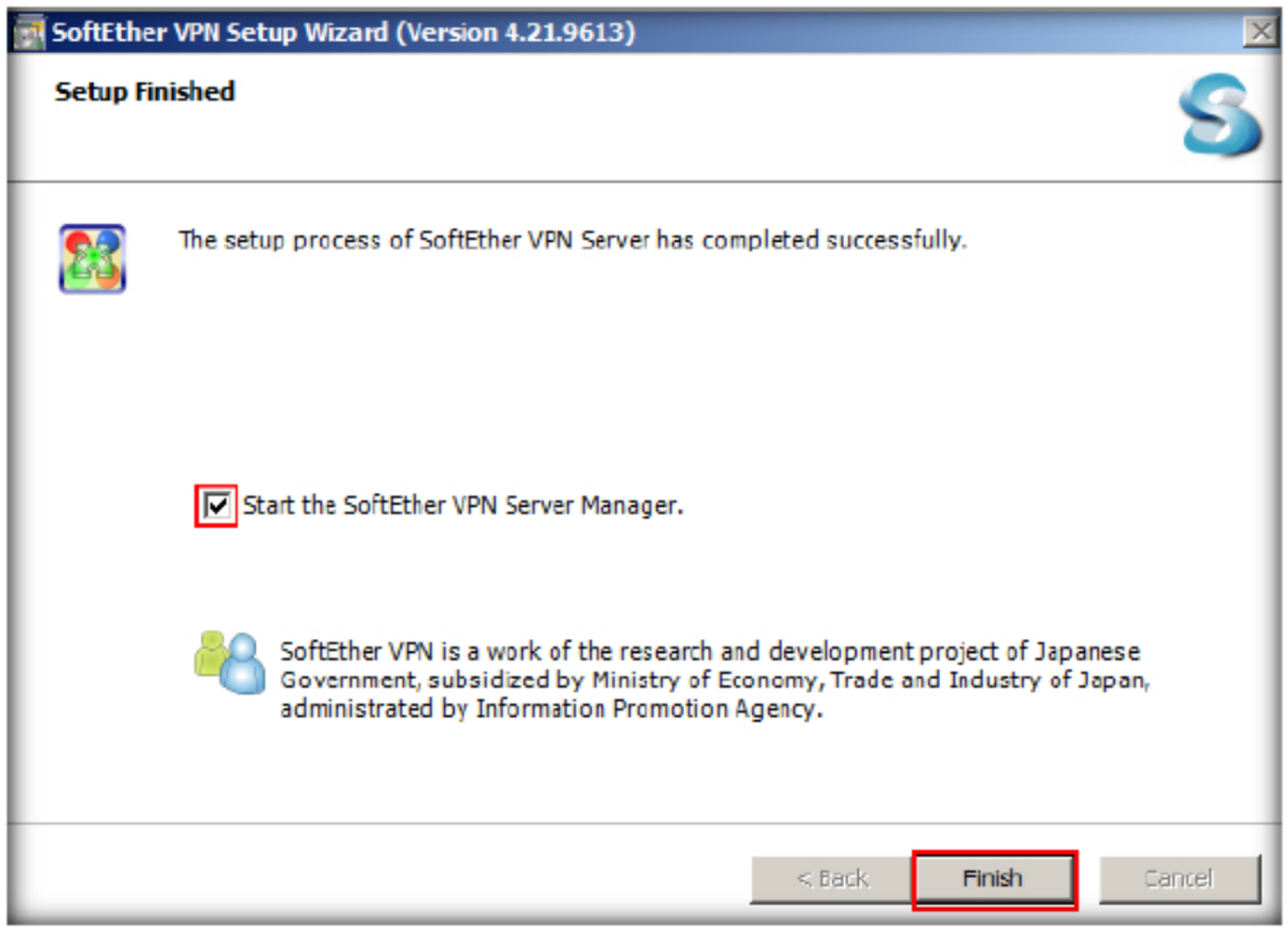

FIGURE 2.4: Launching SoftEther VPN Server

📖 You can create one or many Virtual Network Adapter with SoftEther VPN on your client computer. This client computer will become a VPN client, which establishes a VPN connections to the Virtual Hub on the VPN server.

8. The SoftEther VPN Server Manager window appears, click the **Connect** button to configure the VPN Server

FIGURE 2.5: SoftEther VPN Server Manager

📖 You can establish VPN sessions, as called 'VPN tunnels', between VPN clients and VPN servers. A VPN session is the virtualized network cable. A VPN session is realized over a TCP/IP connection. The signals through the VPN session are encrypted by SSL.

9. Connecting for the first time will prompt you to set the Administrator password for the Server Manager, type in the password in the **New Password** field and retype the same password in the **Confirm Password** field (here in this lab we kept password as **test@123**) and click **OK**
10. The Password has been changed pop-up appears click **OK** to continue

FIGURE 2.6: SoftEther VPN Server Manager Administrator Password

11. Check the **Remote Access VPN Server** check box, and click **Next** in the SoftEther VPN Server / Bridge Easy Setup wizard

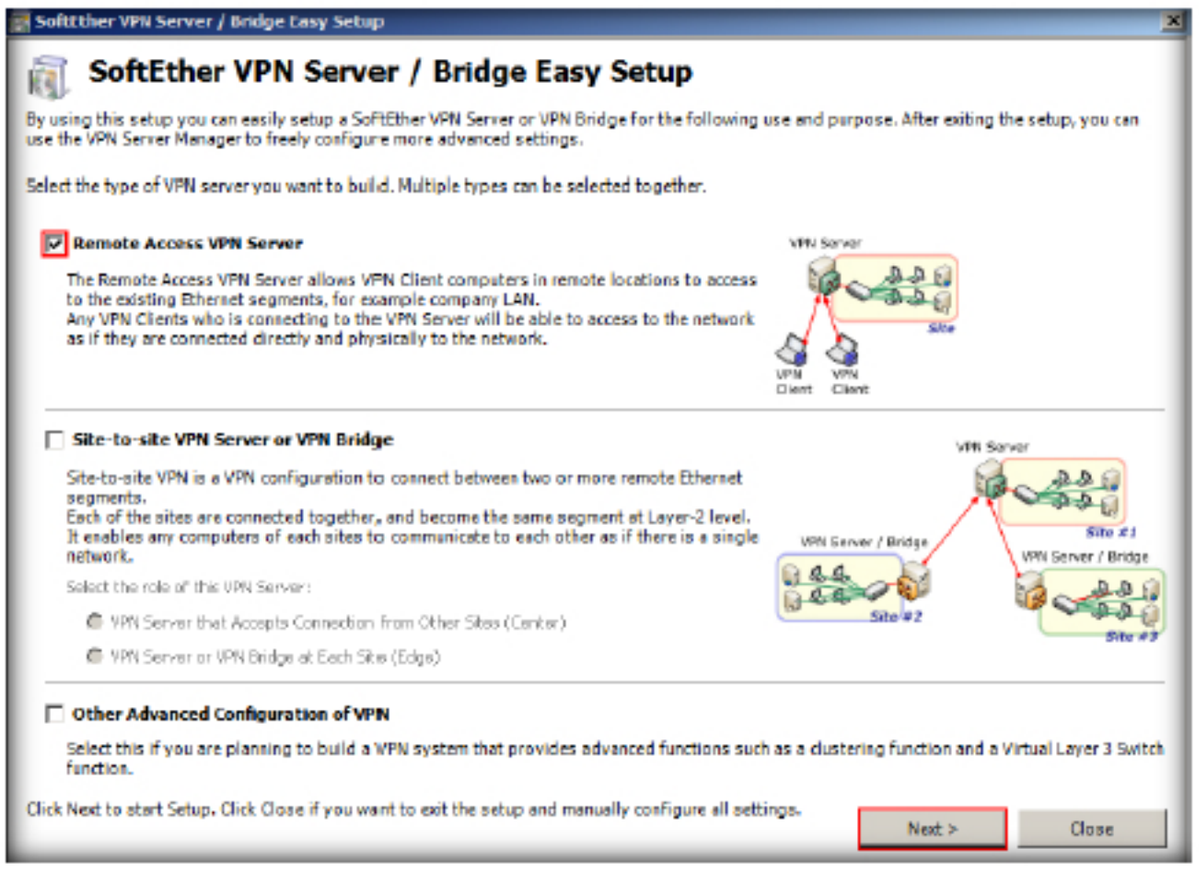

FIGURE 2.7: SoftEther VPN Server / Bridge Easy Setup

12. The SoftEther VPN Server Manager pop-up appears click **Yes** to continue

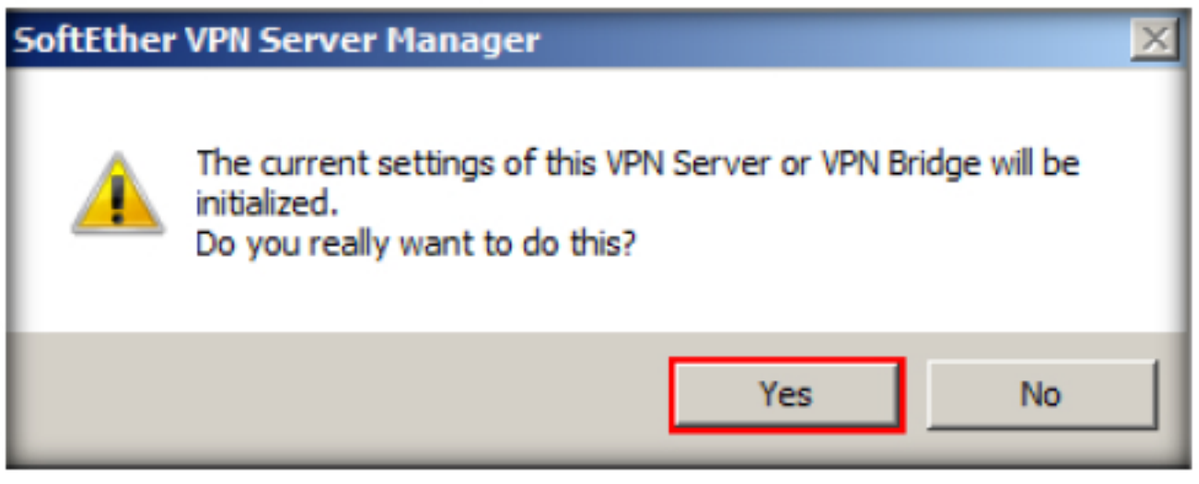

FIGURE 2.8: SoftEther VPN Server / Bridge Easy Setup pop-up

📖 Therefore, you can safely establish a VPN session beyond the Internet. A VPN session is established by SoftEther VPN's "VPN over HTTPS" technology. It means that SoftEther VPN can create a VPN connection beyond any kinds of firewalls and NATs

📖 The Virtual Hub exchanges all Ethernet packets from each connected VPN session to other connected sessions. The behavior is the same as with traditional Ethernet switches. The Virtual Hub has a FDB (forwarding database) to optimize the transmission of Ethernet frames.

13. The Easy Setup pop-up appears where you need to specify the Virtual Hub Name. Type the name of the Virtual Hub in the respective field and click OK as shown in the screenshot. In this lab we are providing the name as **CND-VPN**

📖 You can define a local bridge between the Virtual Hub and the existing physical Ethernet segment by using the Local Bridge function. The Local Bridge exchanges packets between the physical Ethernet adapter and the Virtual Hub. You can establish a remote-access VPN from home or mobile to the company network by using the Local Bridge function.

FIGURE 2.9: Virtual HUB Name

14. Dynamic DNS Function window appears, click **Exit** to continue
15. Check Enable L2TP Server Function (L2TP over IPsec) check box, and leave the other settings as default and click **OK**

📖 You can define a cascading connection between two or more remote Virtual Hubs. With cascading, you can integrate two or more remote Ethernet segments to a single Ethernet segment. For example, after you establish cascading connections between sites A, B and C, then any computers in site A will be able to communicate with the computers in site B and site C. This is a site-to-site VPN.

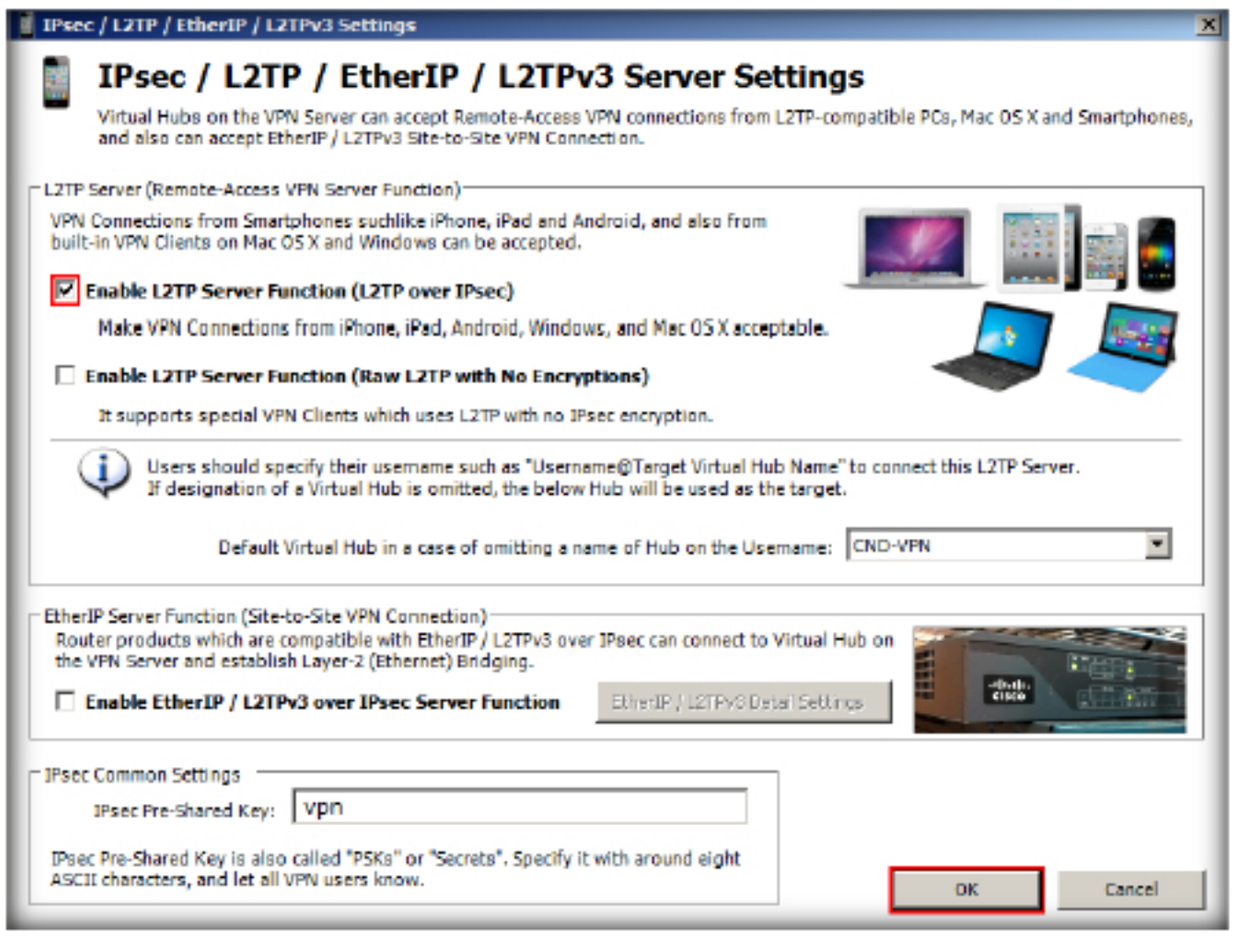

FIGURE 2.10: Enabling L2TP Server Function

16. The VPN Azure Service Settings wizard appears, you can choose any option according to your organization network policy, in this lab we are selecting the Disable VPN Azure radio button and click **OK**

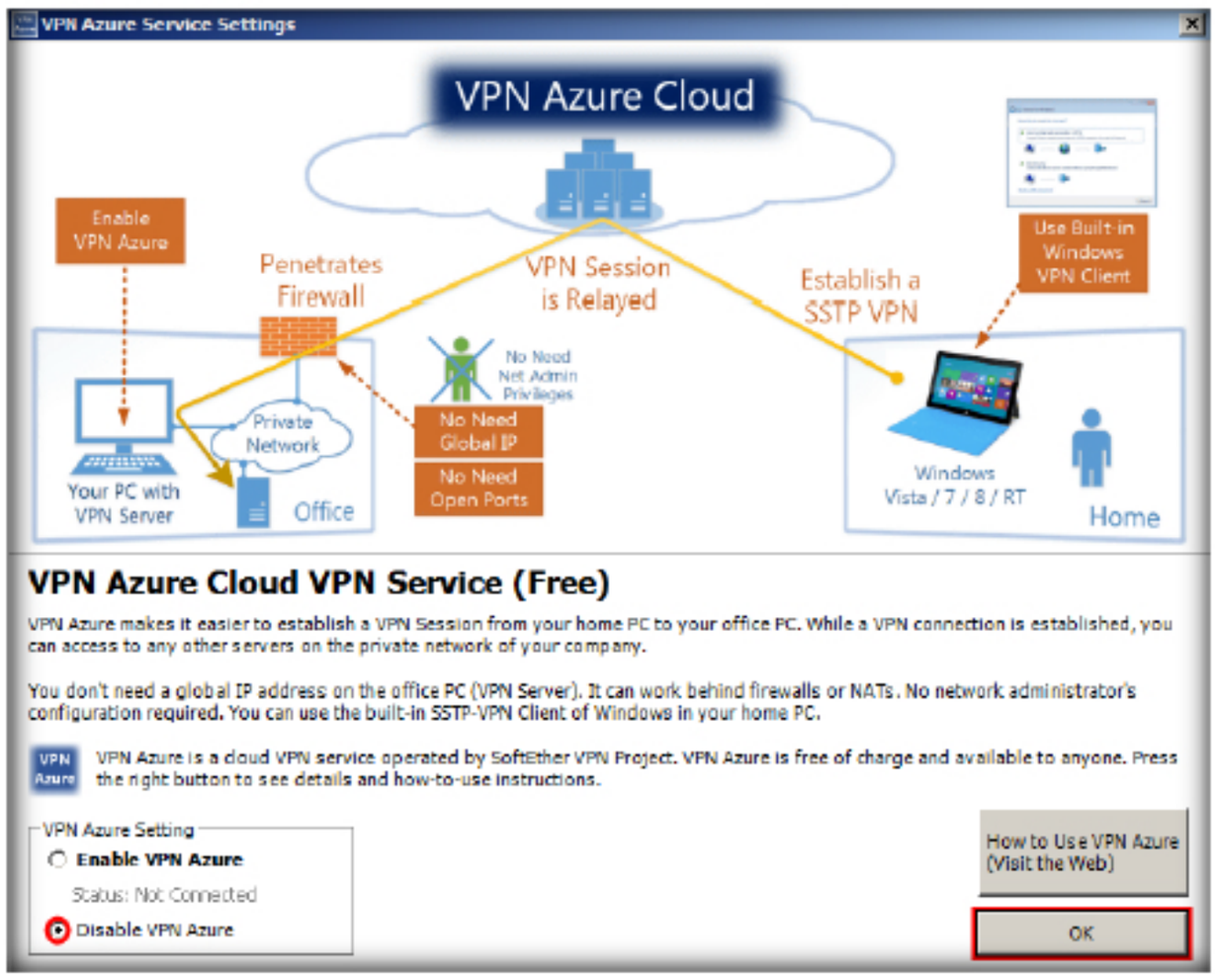

FIGURE 2.11: Disable VPN Azure Service

17. The VPN Easy Setup Tasks wizard appears where we need to create Users who will access the organization network through a VPN. To create new users click **Create Users**

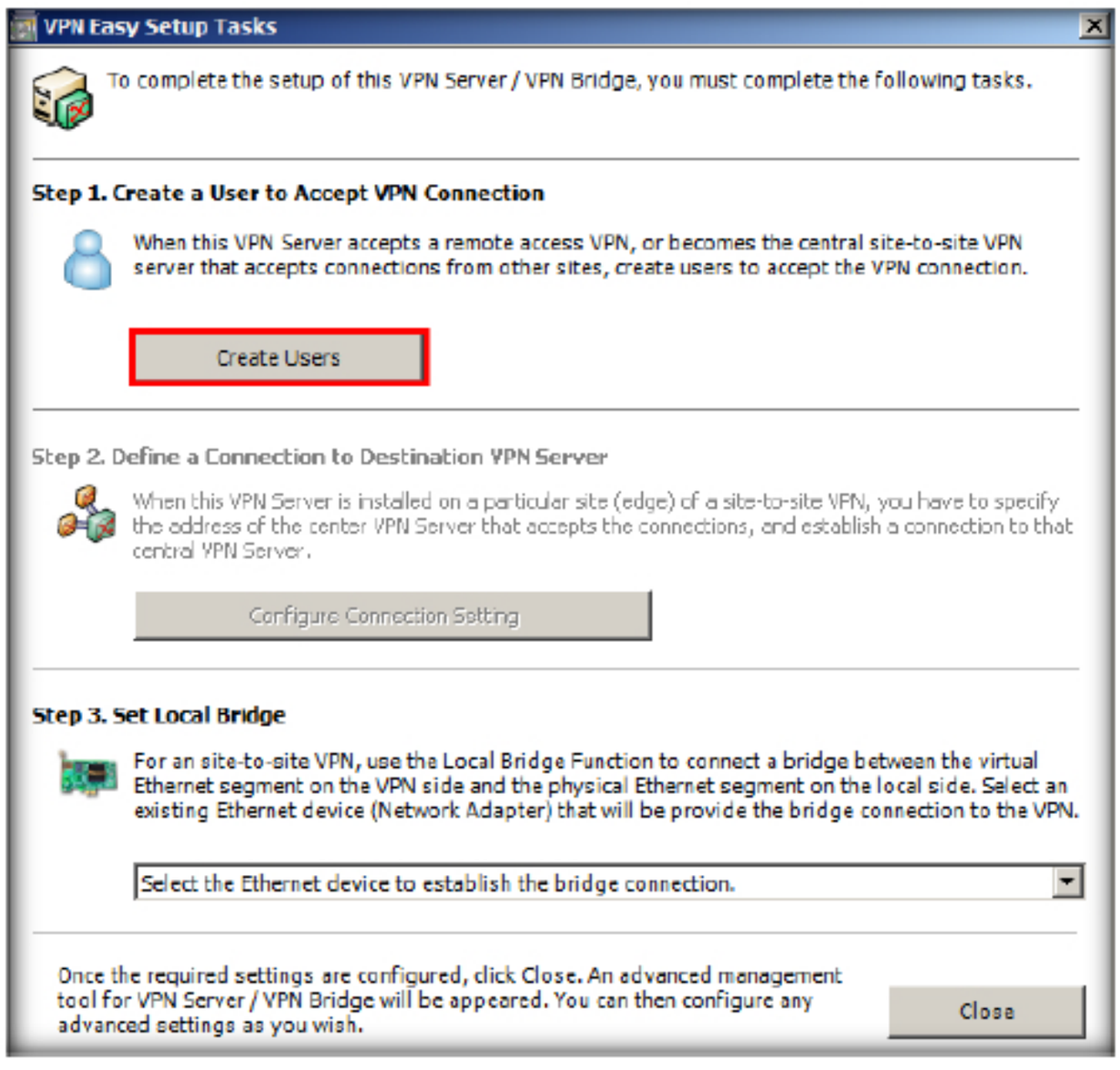

FIGURE 2.12: Creating Users in Server Manager

📖 SoftEther VPN can also establish a VPN session over UDP. The UDP-mode of SoftEther VPN supports NAT traversal. The NAT traversal function allows the VPN server behind existing NATs or firewalls to accept incoming VPN sessions. You need no network administrator's special permission before setting up a VPN server on the company network behind firewalls or NATs. Additionally, SoftEther VPN Server may be placed on the dynamic IP address environment since SoftEther VPN has a built-in Dynamic DNS (DDNS) function.

📖 SoftEther VPN Server supports additional VPN protocols, including L2TP/IPsec, OpenVPN, Microsoft SSTP, L2TPv3 and EtherIP. These create the interoperability with built-in L2TP/IPsec VPN clients on iPhone, iPad, Android, Windows and Mac OS X, and also with Cisco's VPN routers and other vendors VPN products.

18. The Create a new user wizard appears, fill in the required details as shown in the screenshot, click **OK**
19. We have created a new username as **martin** and the password is **qwerty@123**

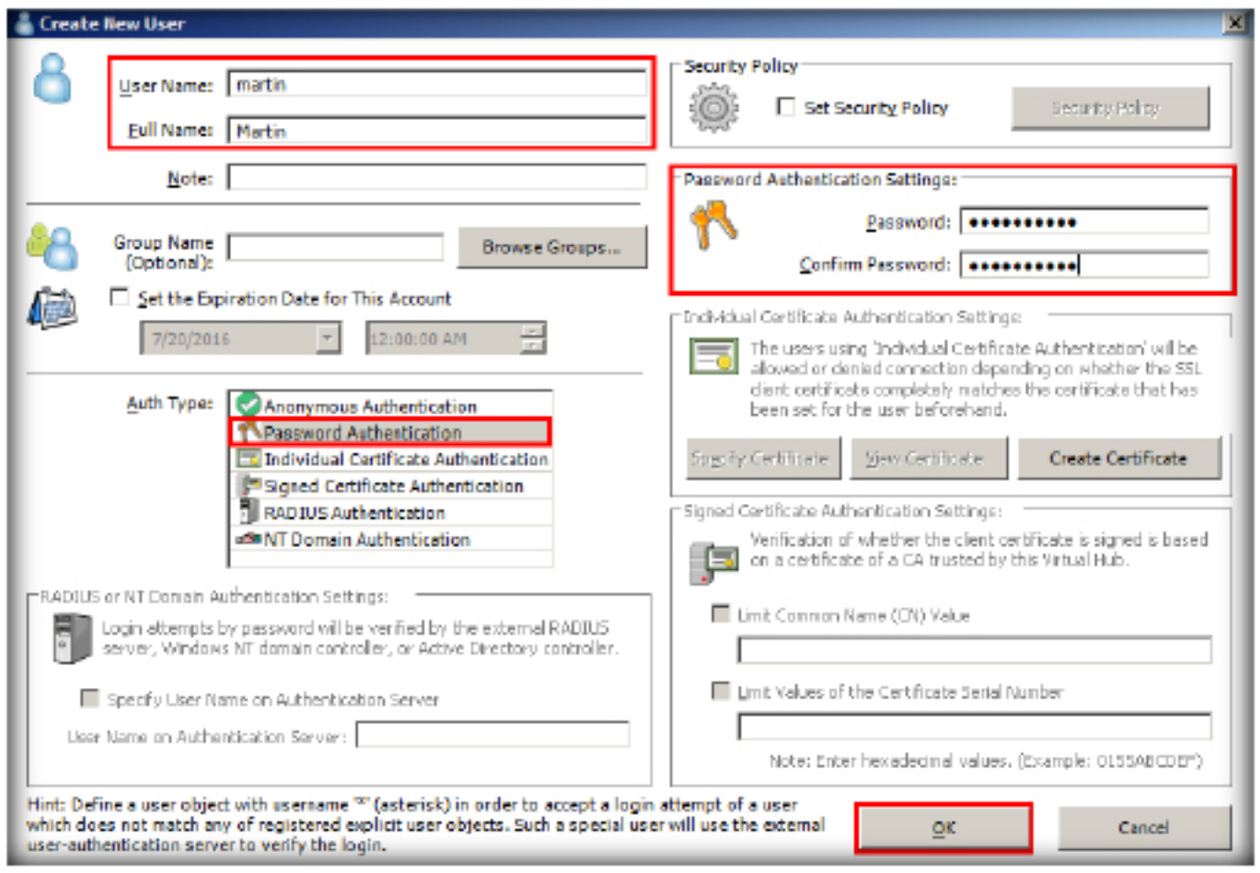

FIGURE 2.13: New User Creation

20. The User created pop-up appears as shown in the screenshot, click **OK**

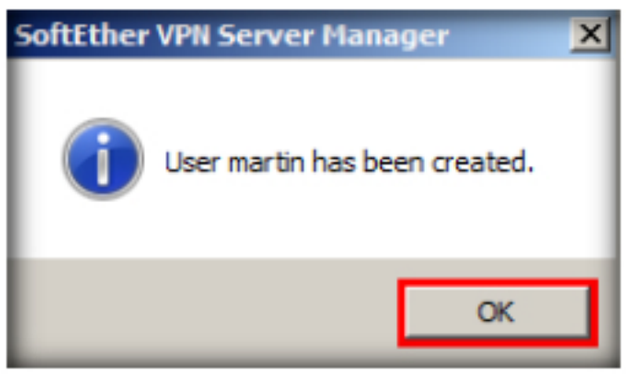

FIGURE 2.14: New User Created pop-up

21. The Manage Users window appears, where you can create new users, edit created users, View User Information, and Delete users. Now click the **Exit** button

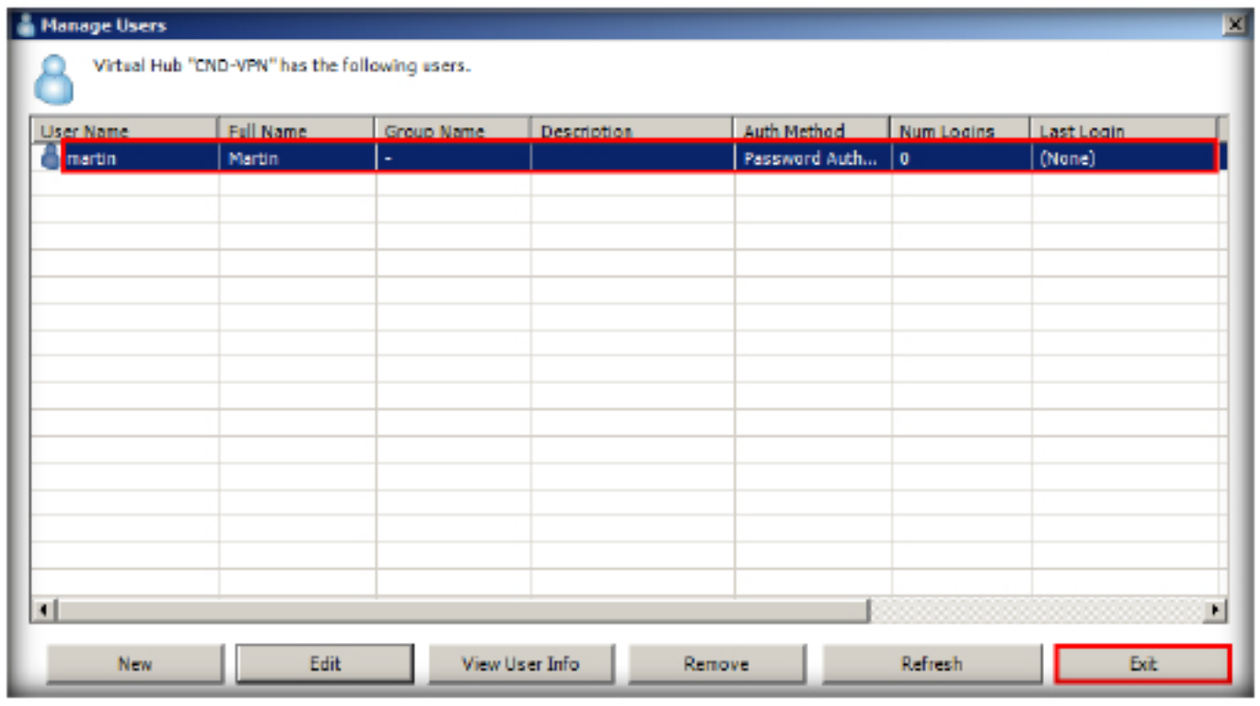

FIGURE 2.15: Manage Users Screen

SoftEther VPN supports additional VPN protocols, including L2TP/IPsec, OpenVPN, Microsoft SSTP, L2TPv3 and EtherIP. These create the interoperability with built-in L2TP/IPsec VPN clients on iPhone, iPad, Android, Windows and Mac OS X, and also with Cisco's VPN routers and other vendors VPN products.

An ad-hoc VPN consists of the small-number computers with SoftEther VPN. Despite the long-distance, it is easy to communicate mutually with any kind of LAN-oriented protocols.

22. The VPN Easy Setup Tasks wizard appears click **Close**

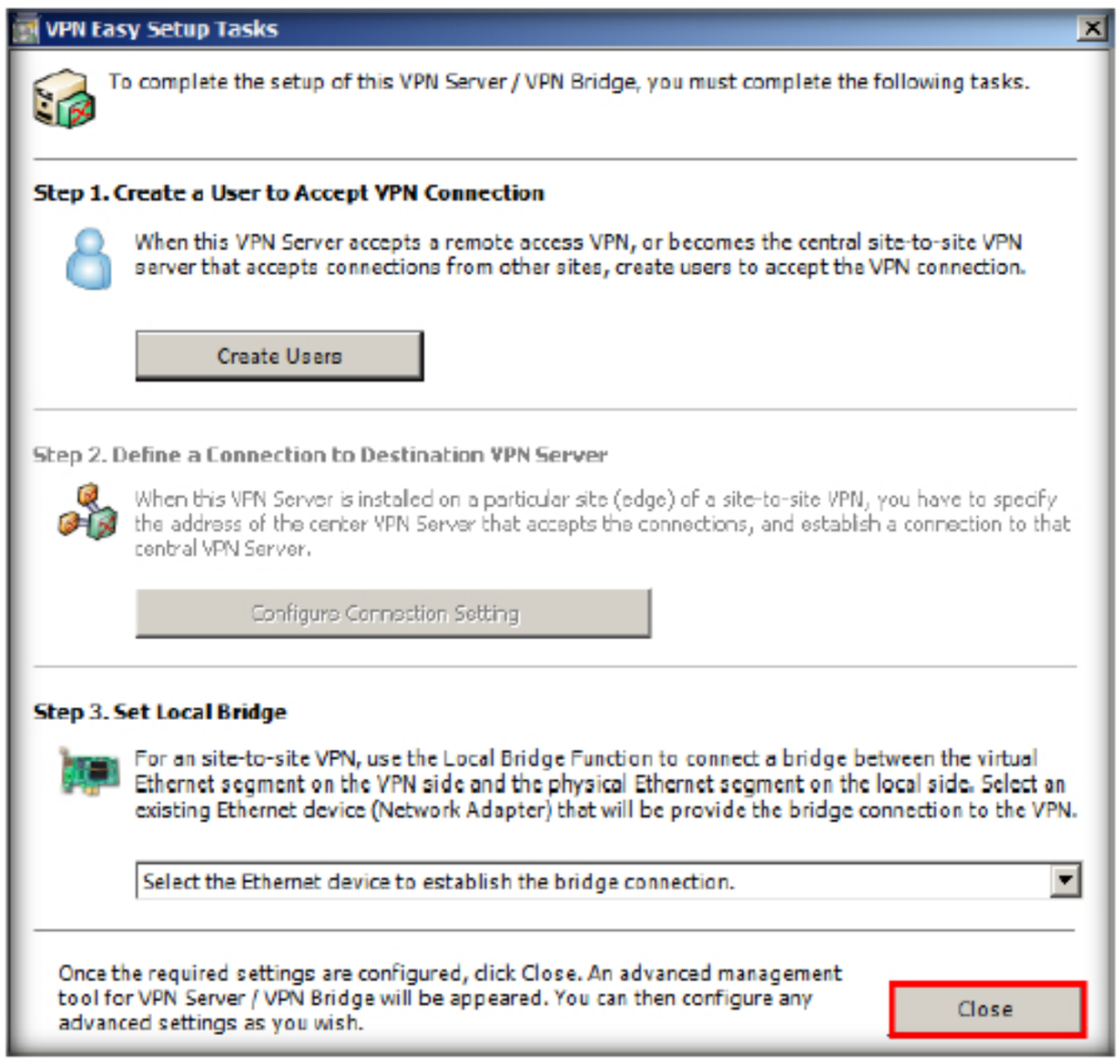

FIGURE 2.16: VPN Easy Setup Tasks

23. The Manage VPN Server dashboard appears, where you can see the connected users through the VPN network. You can also manage the VPN settings from the different options of this dashboard

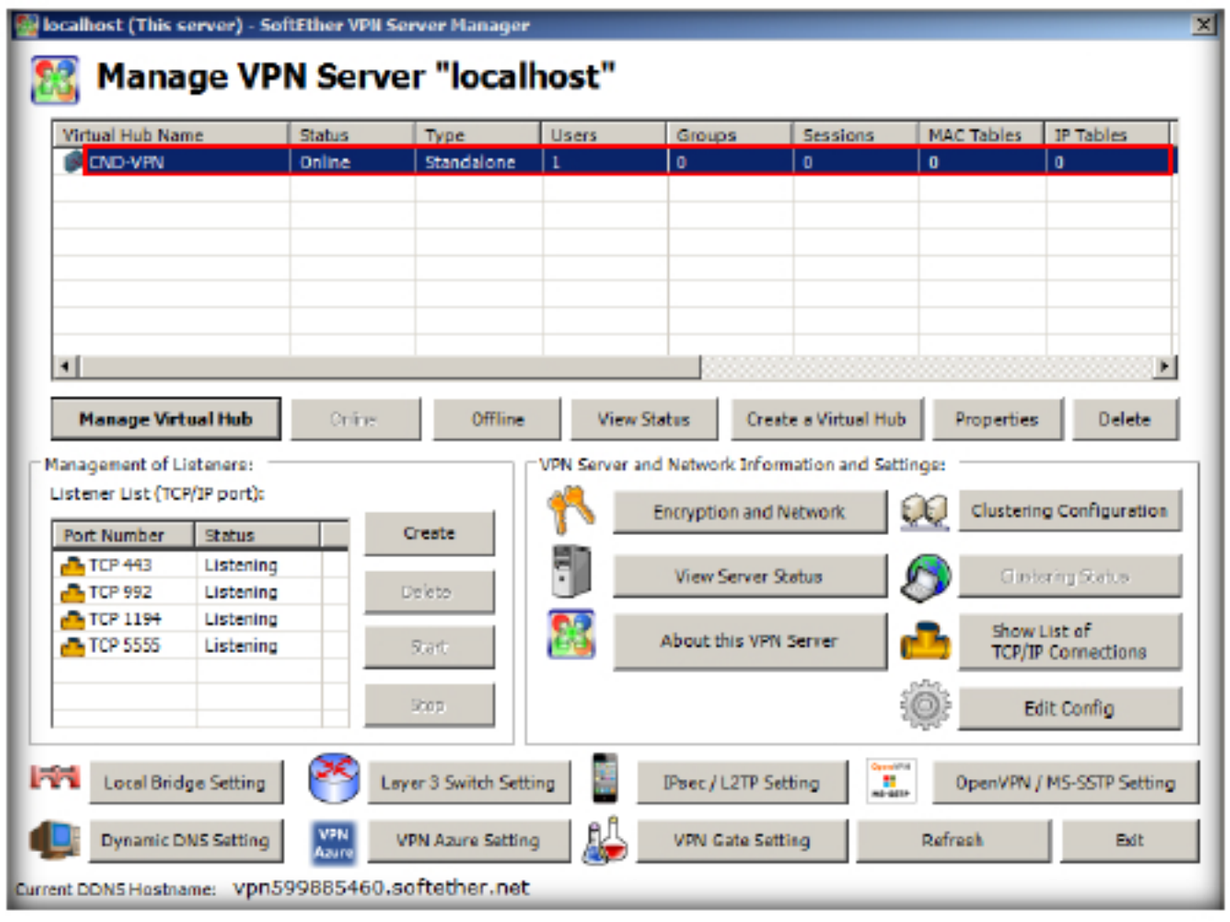

FIGURE 2.17: Manage VPN Server Dashboard

24. Now, switch to the **Windows 10** machine and login as the Local Admin and install the **SoftEther VPN client**

📖 SoftEther VPN can construct distributed virtual Ethernet segments. If you want to enable geologically distributed computers to communicate each other as if they are connected to the single Ethernet network, using SoftEther VPN is the easiest way.
First, set up a VPN Server. Next, set up VPN Clients on each member PCs. Finally start VPN connections on each VPN client. Then each client can use any kind of IP-based or Ethernet-based protocols via the VPN even if they are distributed around the world.

📖 Do employees need to connect to the company LAN from outside or home? Remote Access VPN provide a virtual network cable from a Client PC to the LAN from anywhere and at anytime.

TASK 2

Installing and Configuring SoftEther VPN Client

25. To install the SoftEther VPN client, navigate to Z:\CND-Tools\CND Module 09 Secure VPN Configuration and Management\Software VPN\SoftEther VPN and double-click **softether-vpnclient-v4.21-9613-beta-2016.04.24-windows-x86_x64-intel.exe**
26. The SoftEther VPN setup wizard appears click **Next**

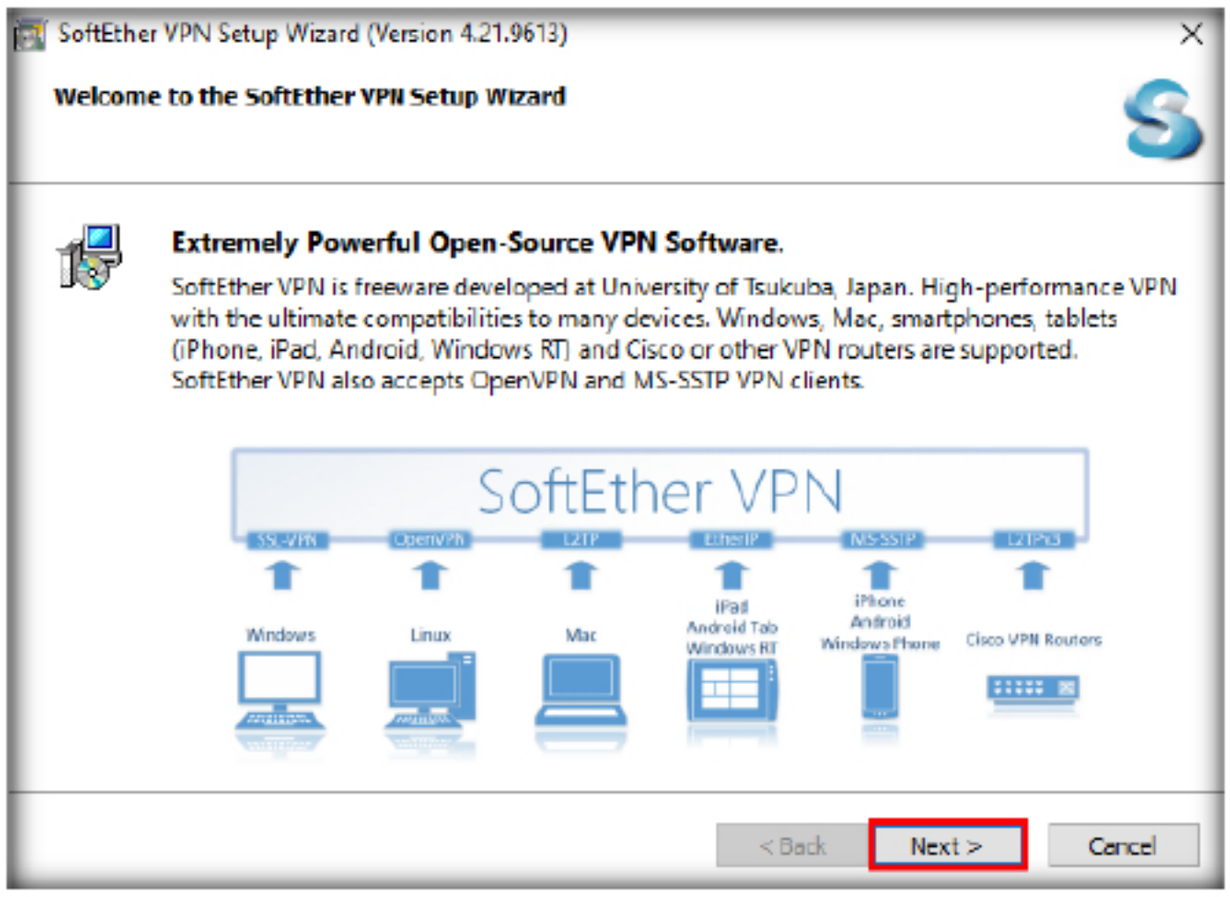

FIGURE 2.18: SoftEther VPN Client Setup

27. If the User Account Control pop-up appears, click **Yes**
28. The Select Software Components to Install wizard appears, choose the **SoftEther VPN Client** and click **Next**
29. Follow the wizard driven installation steps to complete the installation process

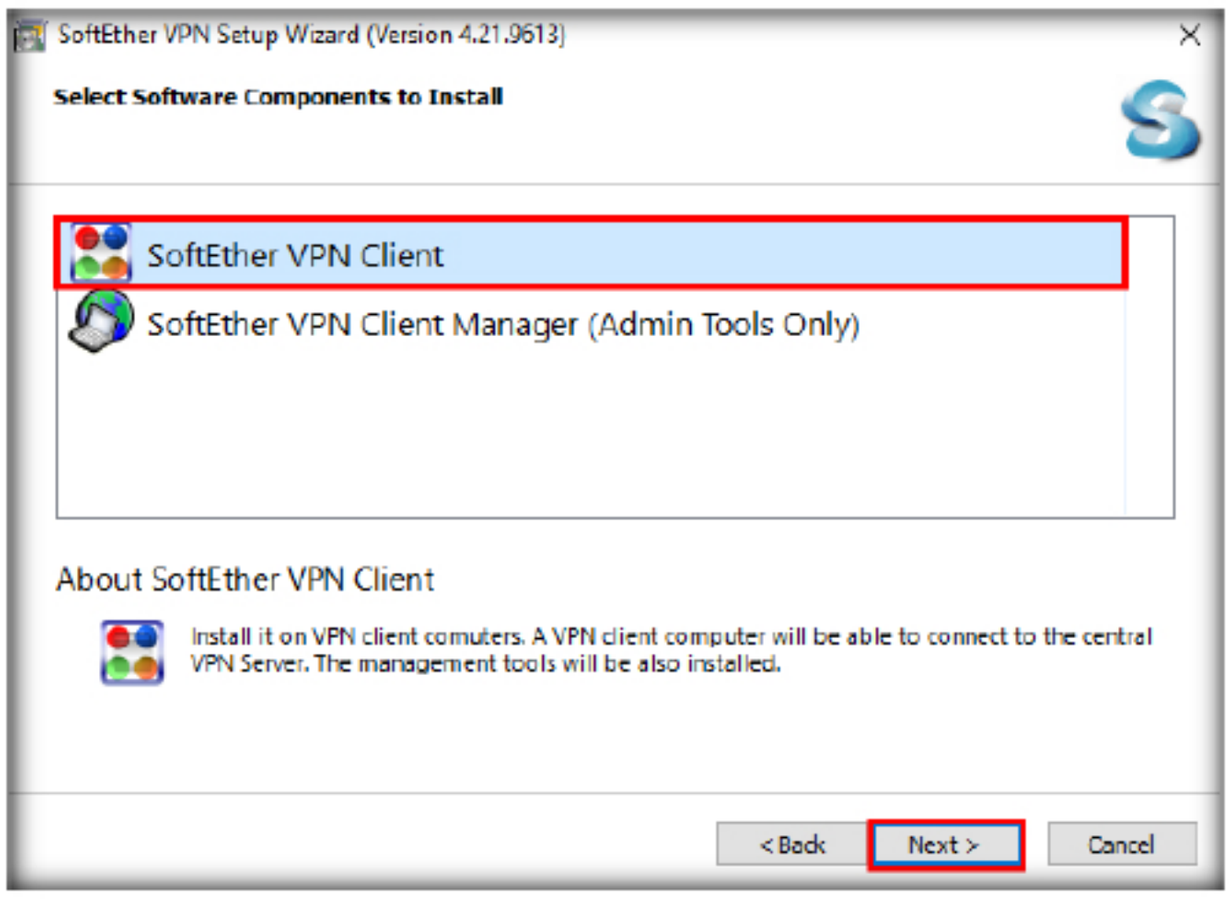

FIGURE 2.19: SoftEther VPN Client Software Components

📖 The ad-hoc network allows communications for VPN-established member PCs. However if your company has a lot of computers on the corporate network, it is not practical to install VPN Clients on all PCs in your company. This is the reason why Remote Access VPN is necessary for middle and large-scale corporate networks.

30. The Setup Finished wizard appears, make sure that the **Start the SoftEther VPN Client Manager option** is checked to launch the application automatically and click **Finish**
31. Alternatively, you can also launch the application by double-clicking the short-cut icon on the desktop or from the Start menu installed apps

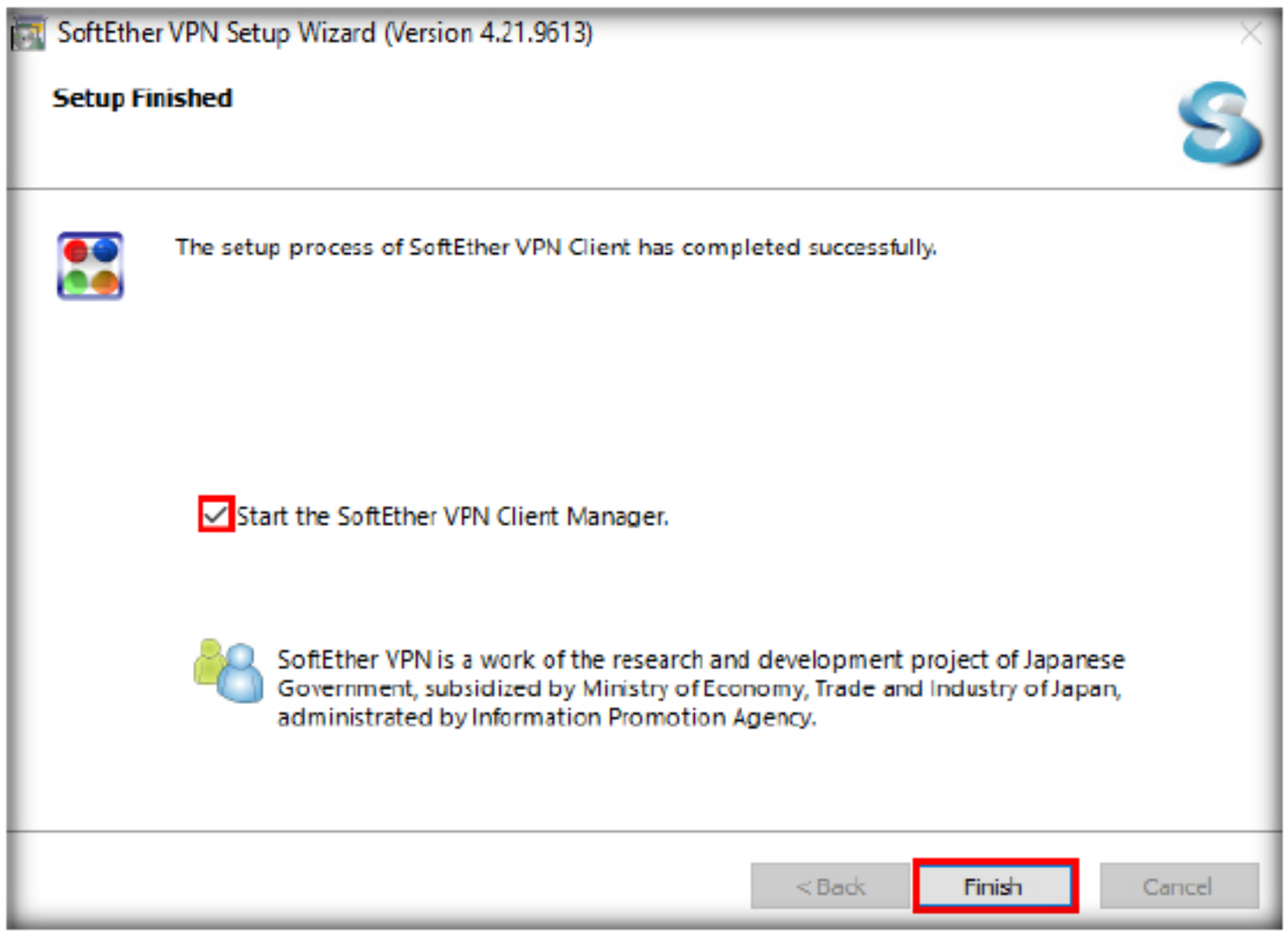

FIGURE 2.20: Launching SoftEther VPN Client

32. The SoftEther VPN Client Manager window appears, double-click on the Add VPN Connection to add a system to the VPN network

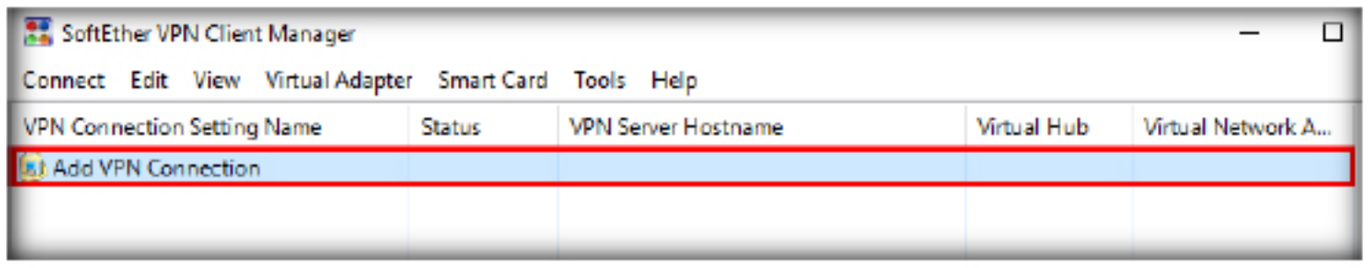

FIGURE 2.21: SoftEther VPN Client Manager

TASK 3

Adding New VPN Connection

33. Before creating a VPN Connection Setting, we need to create a Virtual Network Adapter, the SoftEther VPN Client will ask you to create a Virtual Network Adapter, click **Yes**

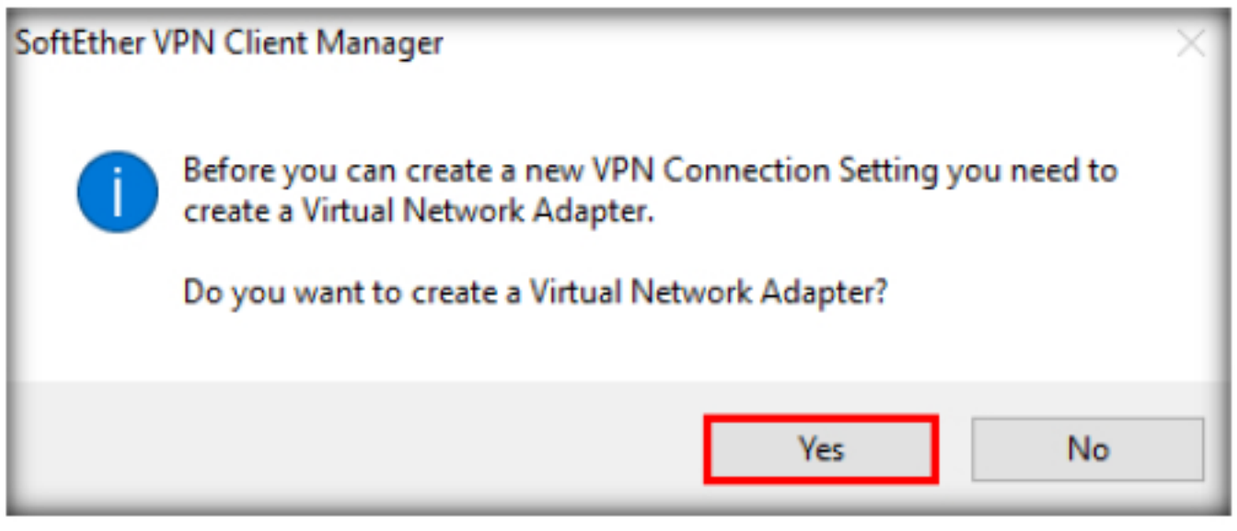

FIGURE 2.22: Creating a New Virtual Network Adapter

📖 Remote Access VPN is an extended topology of the ad-hoc network. The difference between ad-hoc VPN and remote-access VPN is similar to Wi-Fi Ad-hoc mode and Wi-Fi Infrastructure mode.

📖 With Wi-Fi Ad-hoc mode, every computer must be connected to a single Wi-Fi segment. Wi-Fi Infrastructure mode allows communicating computers on both a Wi-Fi segment and a Physical Ethernet segment.

TASK 4

Creating New Virtual Network Adapter

34. The Create New Virtual Network Adapter pop-up appears, type the name in the **Virtual Network Adapter Name** field and click **OK**. Leave the settings as default.

    Note: The Virtual Network Adapter Name should be VPN or VPN2 to VPN127 (You can create a maximum of 127 Virtual Network Adapters)

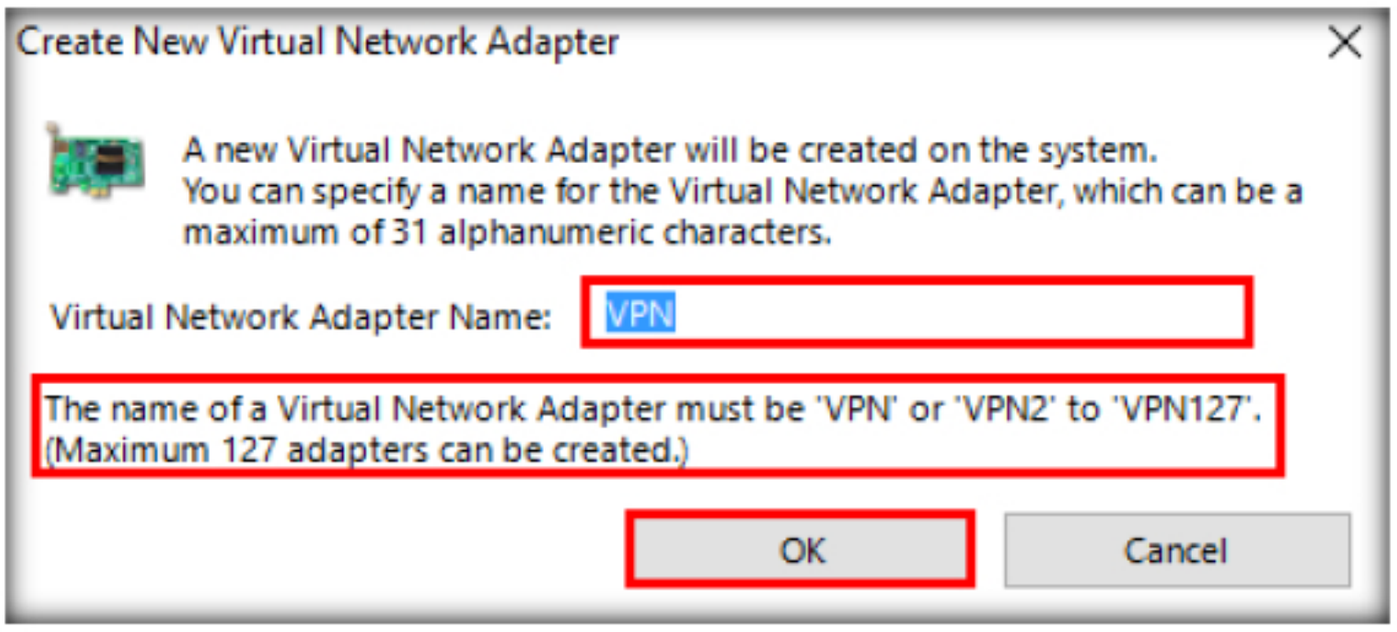

FIGURE 2.23: Virtual Network Adapter Configuration

35. The SoftEther VPN client will create a new Virtual Network Adapter, as shown in the screenshot, wait until the process is completed

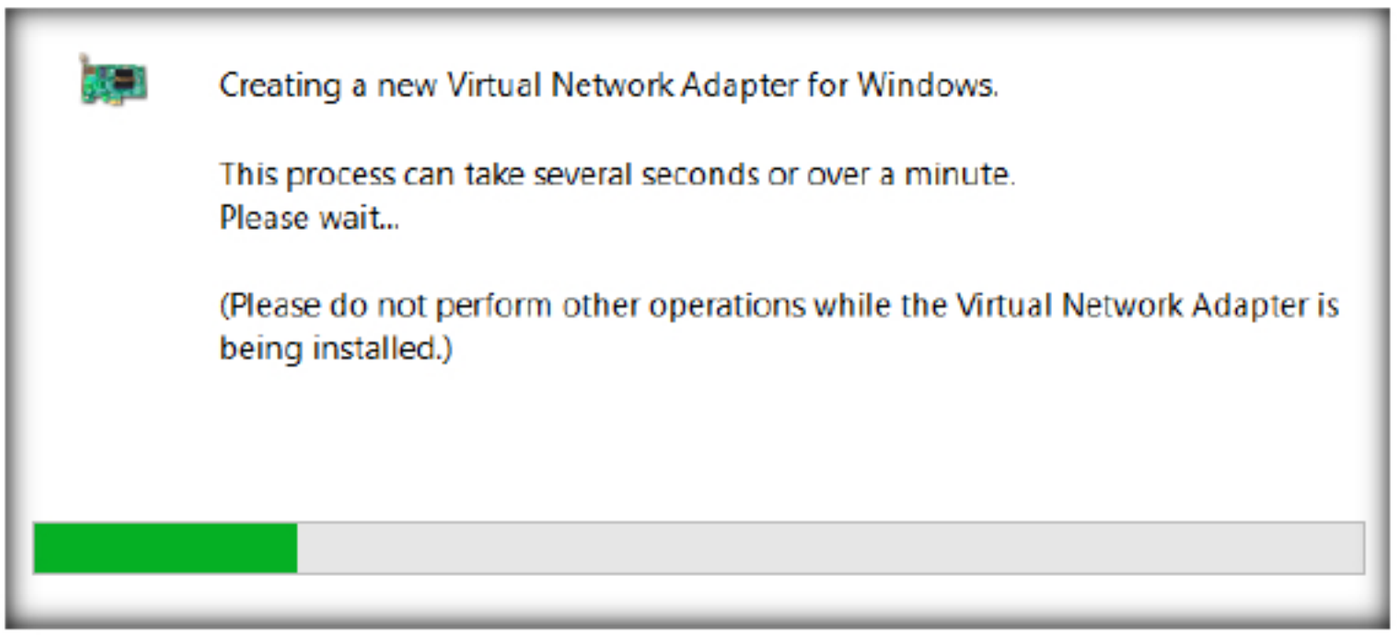

FIGURE 2.24: Virtual Network Adapter Configuration Process

📖 In order to build a Remote Access VPN you can use the Local Bridge function in order to connect between Virtual Private Network segments and physical Ethernet network segments. After that, any remote computers which are connected to the Virtual Hub via VPN will be treated as a part of the existing physical Ethernet segment.

36. The newly created virtual network adapter can be seen in the lower pane of the SoftEther VPN Client Manager window with the assigned MAC Address, Status and Version. Now, we need to configure the adapter. Double-click on newly created Virtual Network Adapter

37. In this lab, the newly created Virtual Network Adapter **is VPN Client Adapter – VPN** as shown in the screenshot

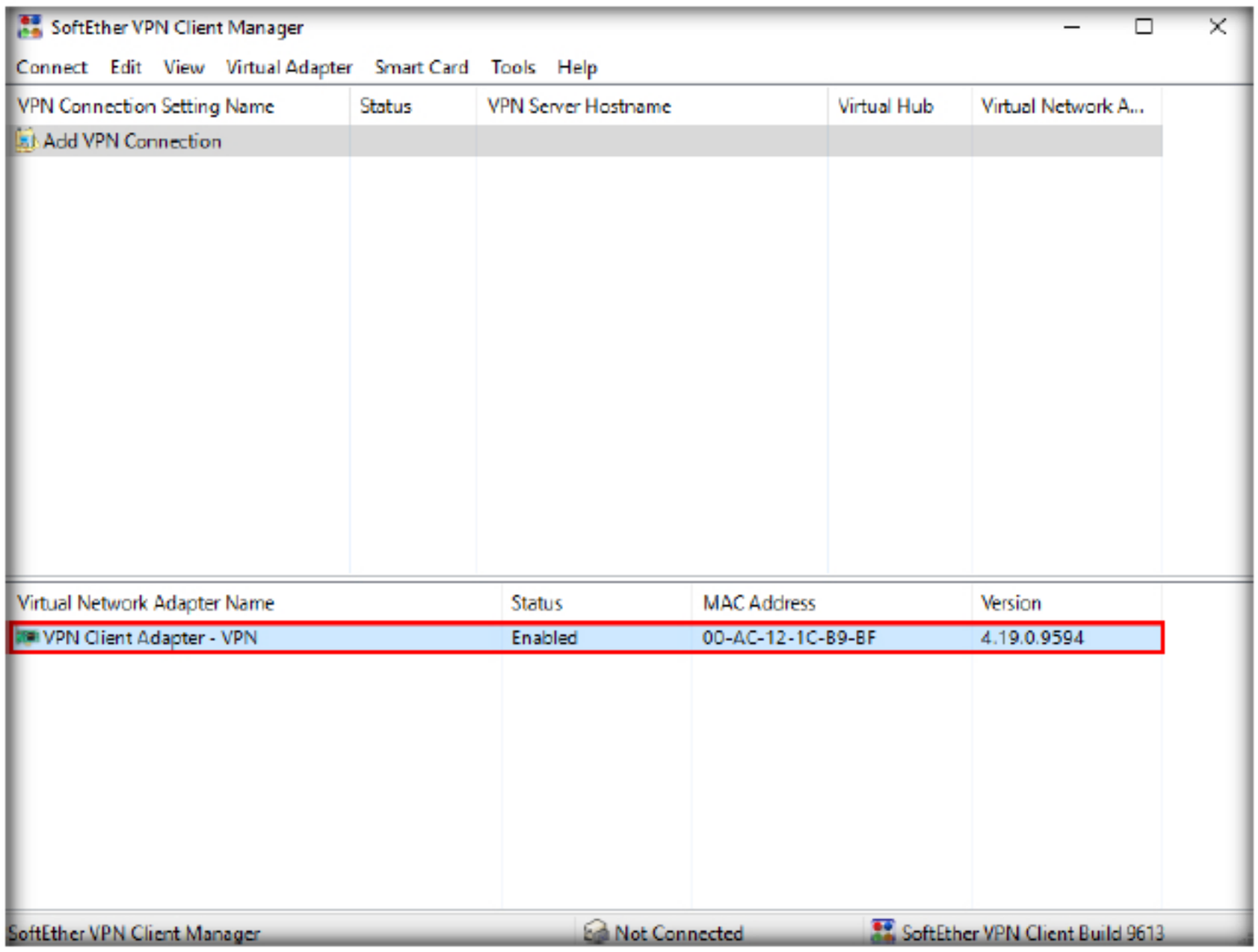

FIGURE 2.25: Virtual Network Adapter Created

📖 Traditional legacy VPNs require static and global IP addresses for the VPN Server. The IP address must be reachable from the Internet. However, a static and global IP address is very expensive. It costs monthly. It has also a security risk because your VPN Server must be exposed to the public Internet. SoftEther VPN has a solution. SoftEther VPN Server has built-in Dynamic DNS and NAT Traversal functions. Static IP addresses are no longer required to set up a VPN Server. Even global IP addresses are no longer required. SoftEther VPN Server can be set up on the private IP address behind the NAT.

38. The New VPN Connection Setting Properties wizard appears, as shown in the screenshot
39. In the **Settings Name** field provide a name for VPN Connection. In the **Destination VPN Server** section type your public IP in the Host Name field, you can choose any port from the Port Number drop-down
40. In the Virtual Hub Name field choose the appropriate name, in this lab we have created a virtual hub name as **CND-VPN** at **step 13**. If you have multiple virtual hubs created choose the appropriate one. Leave the other settings as default

41. On the right-hand side of the window, type the Username and password of the user that you have created in **Step 18**. In this lab the Username is **martin** and the Password is **qwerty@123**, click **OK** and leave the other settings as default

📖 The Dynamic DNS function assigns a world-wide unique identifier on your SoftEther VPN Server. Your global IP address of the SoftEther VPN Server will follow dynamic IP address changes. If the IP address of SoftEther VPN Server suddenly changed, the IP address record which is registered to the Dynamic DNS hostname changes automatically and immediately.

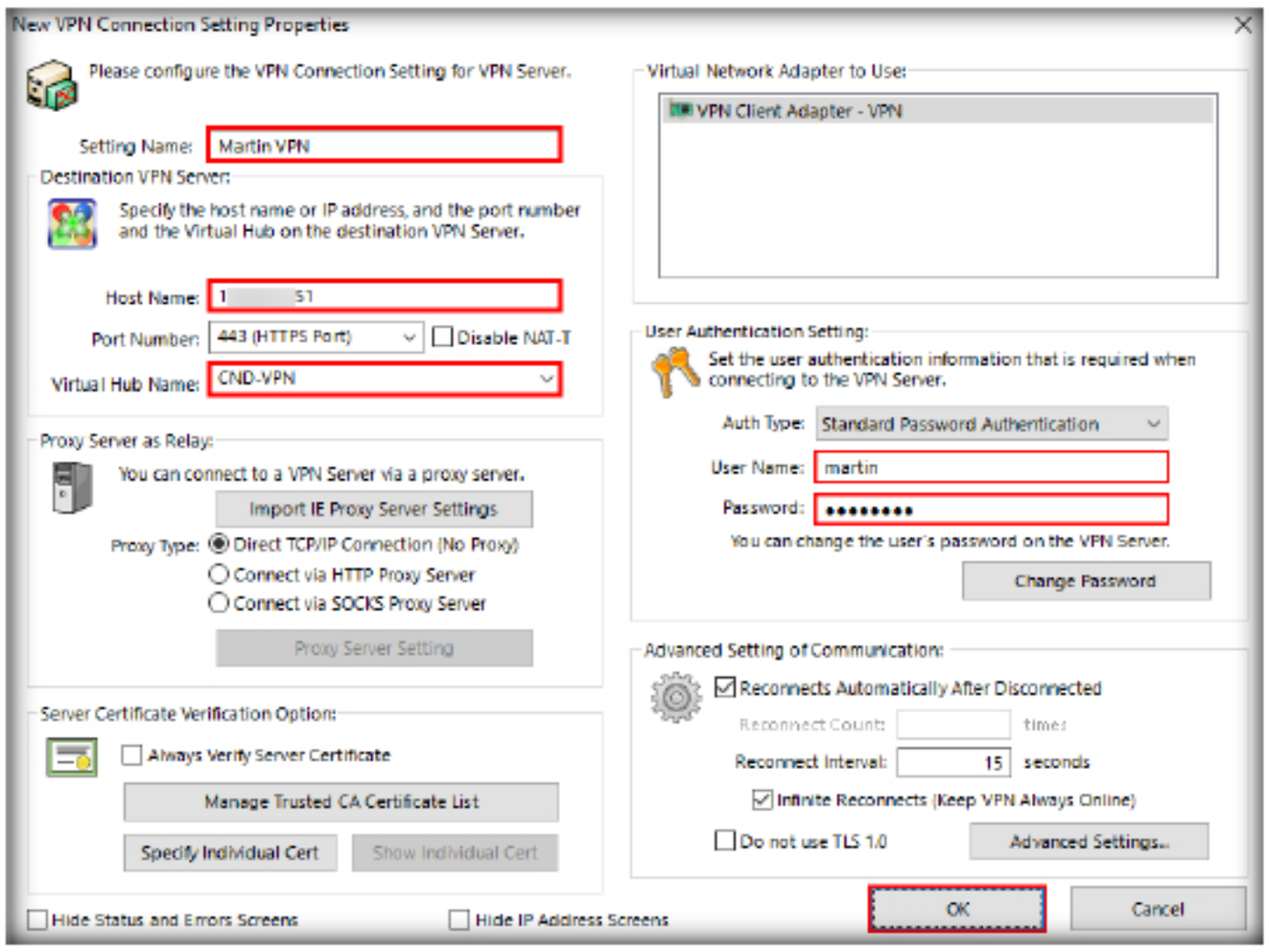

FIGURE 2.26: VPN Connection Setting Properties

42. A newly created VPN connection appears in the SoftEther VPN Client Manager window with a status showing as Offline, as shown in the screenshot
43. Now, click **Connect** from the context menu to connect the organization network through the VPN

📖 A VPN client user can specify the Dynamic DNS hostname as the destination VPN Server's hostname instead of the IP address. VPN Clients and VPN Bridges can keep stable connections to your SoftEther VPN Server even if the server-side Internet connection is not a static IP address contact.

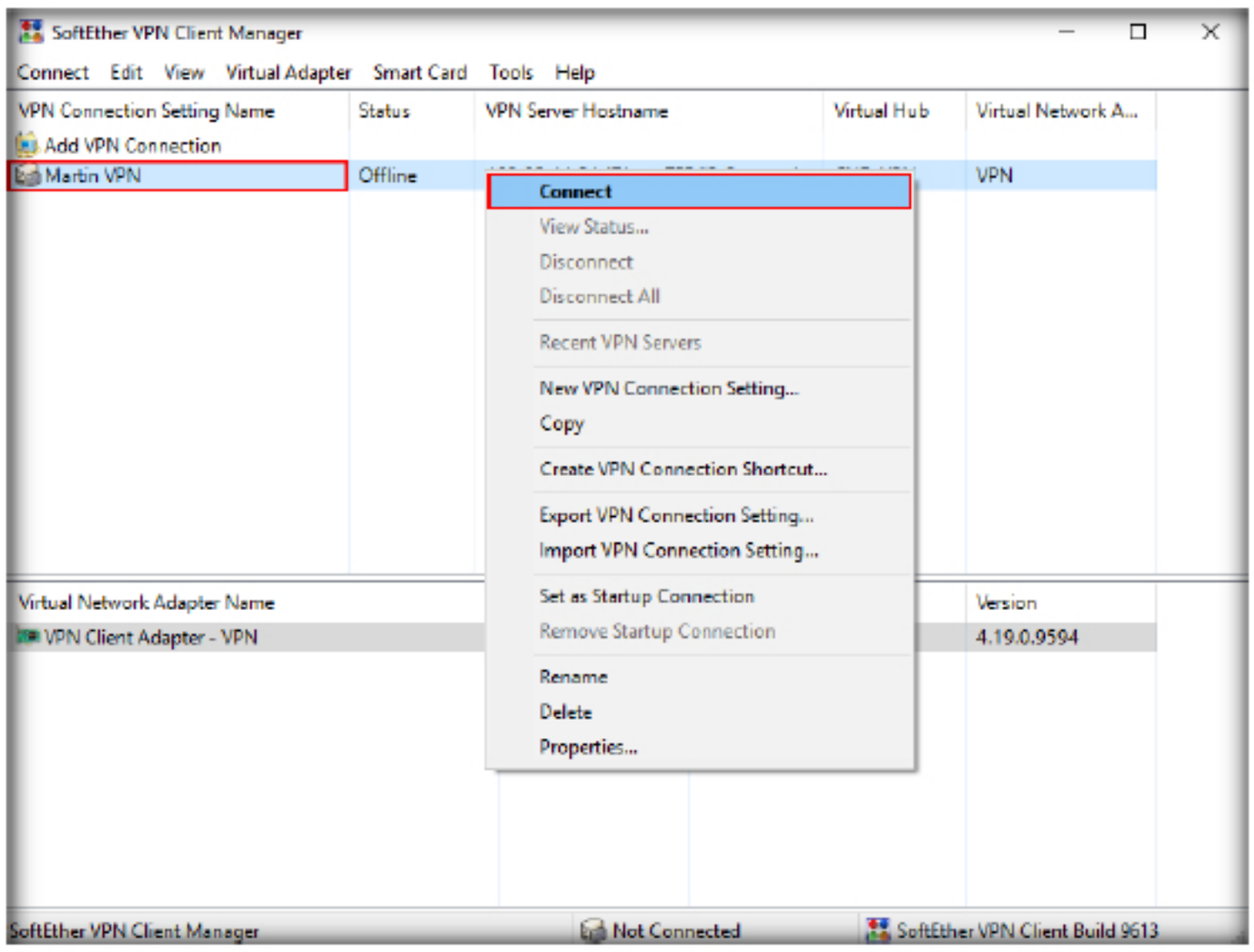

FIGURE 2.27: Connecting Through VPN Network

44. The Connected to VPN Server pop-up appears, and it will request you to assign an IP. Wait until the process is completed

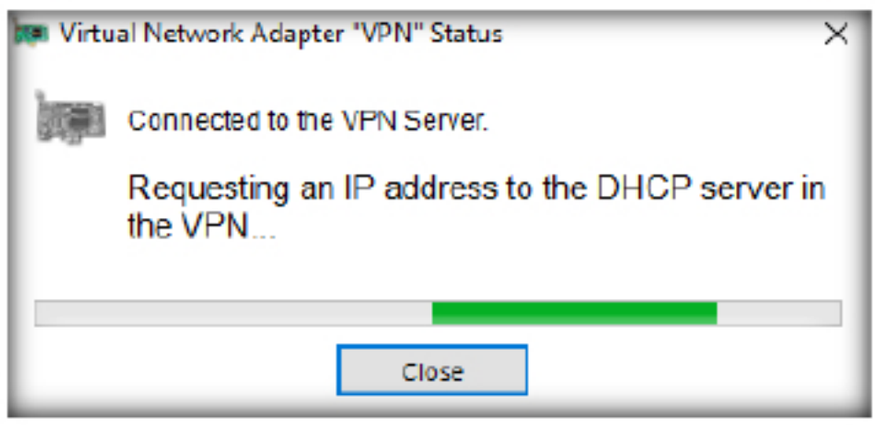

FIGURE 2.28: Requesting for IP Address

45. The VPN Server connected pop-up appears, check the box 'Do not show this message again' and click **OK**

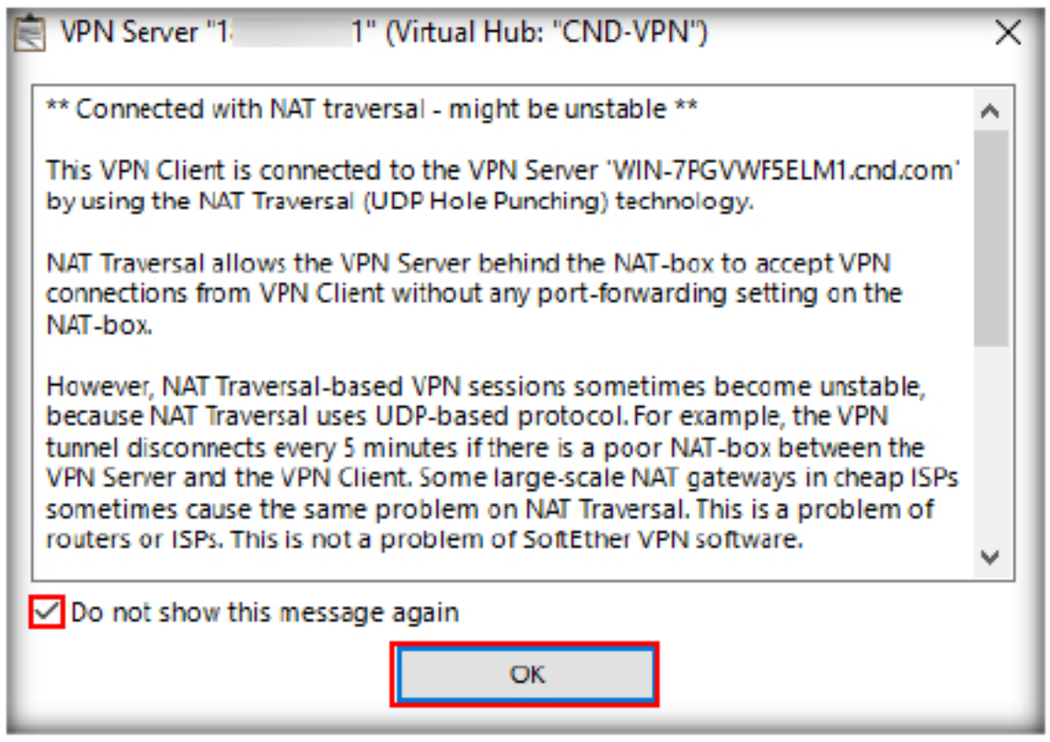

FIGURE 2.29: VPN Server Connected pop-up

46. As soon as you click **OK**, the status of the VPN changes to **Connected** from **Offline** as shown in the screenshot

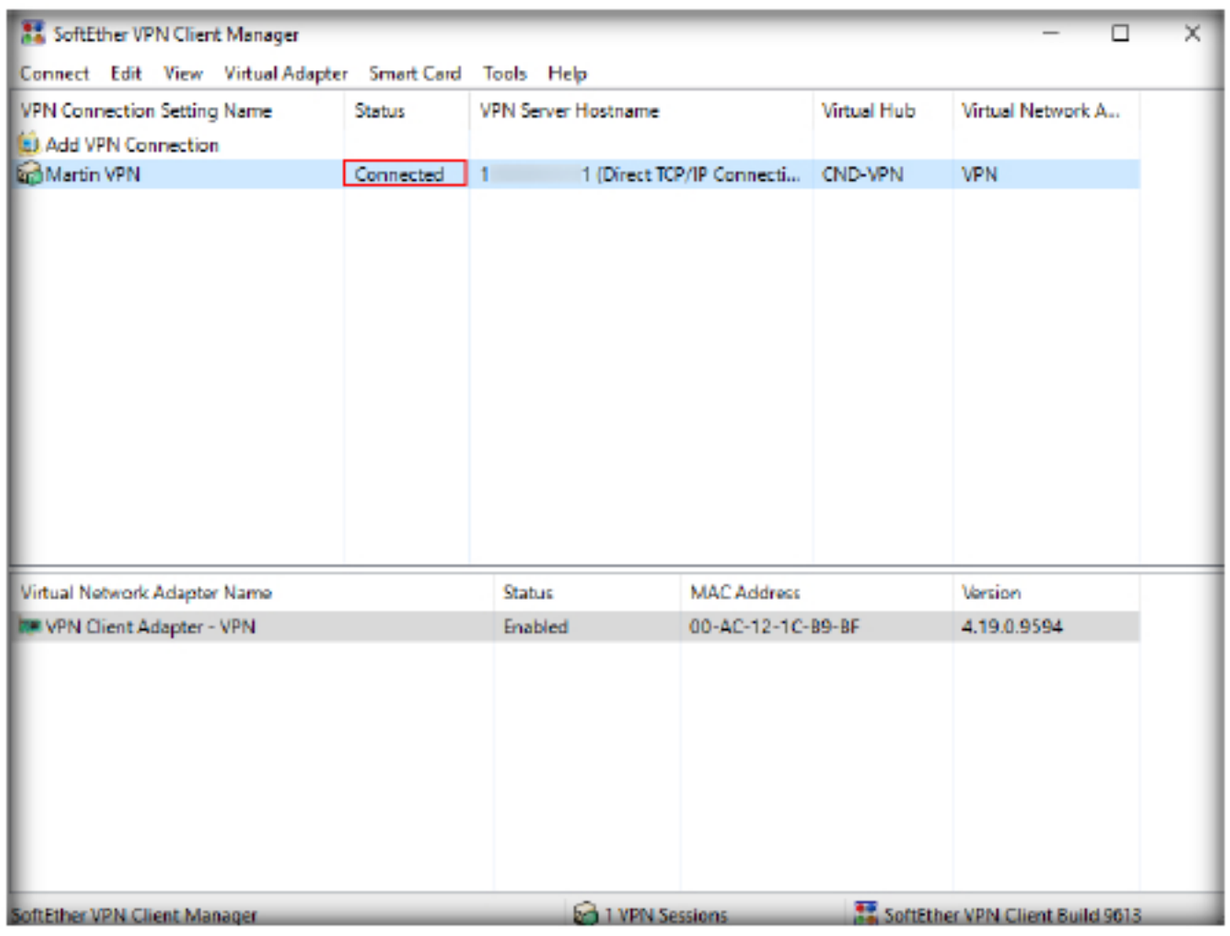

FIGURE 2.30: VPN Client Connected to VPN Server

📖 The NAT Traversal function penetrates firewalls or NATs. This technology is almost the same to Skype's NAT Traversal, but SoftEther VPN's NAT Traversal is more optimized for VPN-use. Legacy IPsec-based or OpenVPN-based VPN Servers cannot be placed behind the NAT, because VPN Clients must reach the VPN Server through the Internet.

📖 Some NAT's can be configured to define a "DMZ" or "Port-mapping" to relay any packets toward the outside IP address of NAT to the internal VPN Server. However, it has compatibilty problems. Moreover it requires a special permission by the administrator of the NAT. If your network administrator is not cooperative with you, he may be hesitant to set up the NAT device to open a hole from the Internet.

47. Now switch back to the Windows Server 2008 machine, where the SoftEther VPN Server is installed and click the **Refresh** button to view the active Sessions using the VPN
48. In the screenshot you can **0** Sessions

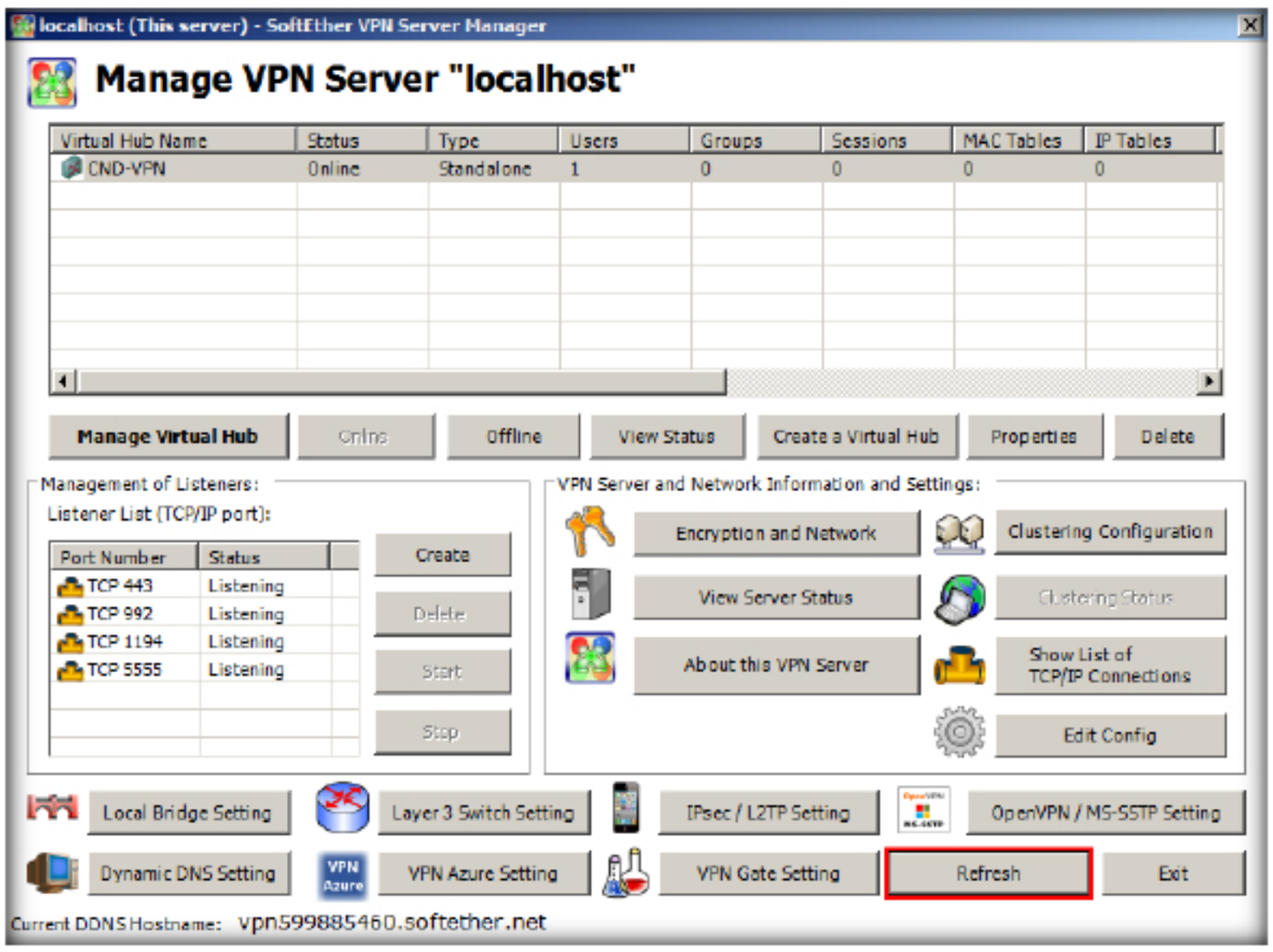

FIGURE 2.31: VPN Server Manager Dashboard

49. Once you click the **Refresh** button you can see the active sessions which are accessed by users as shown in the screenshot

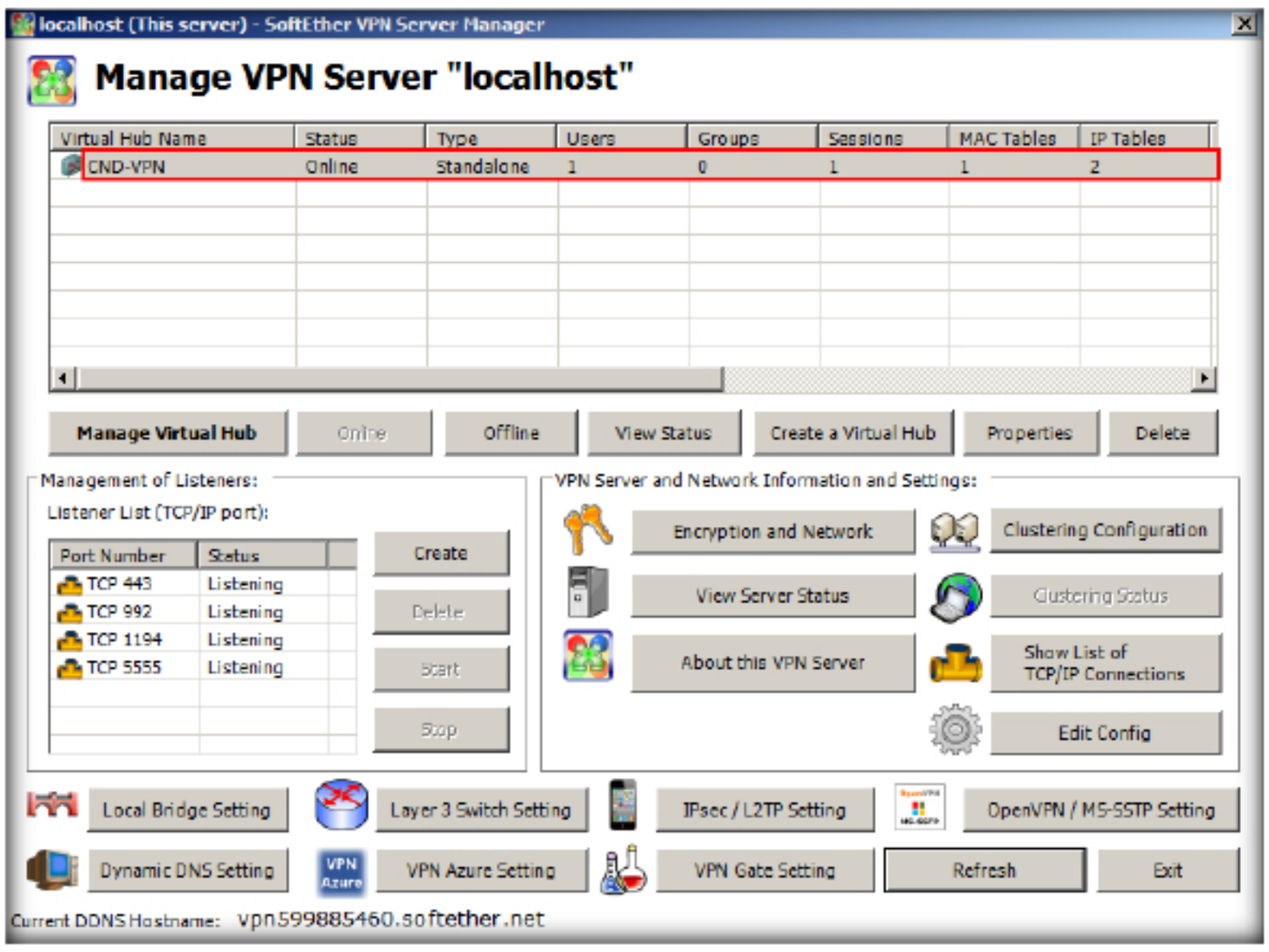

FIGURE 2.32: VPN Server Active Sessions

📖 Unlike legacy VPNs, SoftEther VPN Server can be set up on a private network behind the NAT. No special configuration on the NAT device is required. You need no permission by your network administrator of the NAT. The built-in NAT Traversal Function opens a "Punched Hole" on the NAT or firewall.

📖 When the VPN Client or VPN Bridge attempts to connect to your VPN Server behind the NAT, the connection packets will be lead through the hole. The hole is created by the SoftEther VPN Server automatically, so you need nothing special on the NAT.

📖 SoftEther VPN keeps a virtual dedicate Ethernet line from the Cloud to the LAN 24h/365d. You can consider the remote Cloud private network as a part of your corporate network.

50. To view and manage the sessions double-click on the available VPN Hub in the dashboard. Management of the Virtual Hub – (Name of the Virtual Hub) here in this lab CND-VPN appears as shown in the screenshot
51. Traverse through all the required options available in wizard, and you can manage the sessions and settings of the VPN Network
52. For instance we are going to see the Manage Sessions option, to do this click **Manage Sessions** button as shown in the screenshot

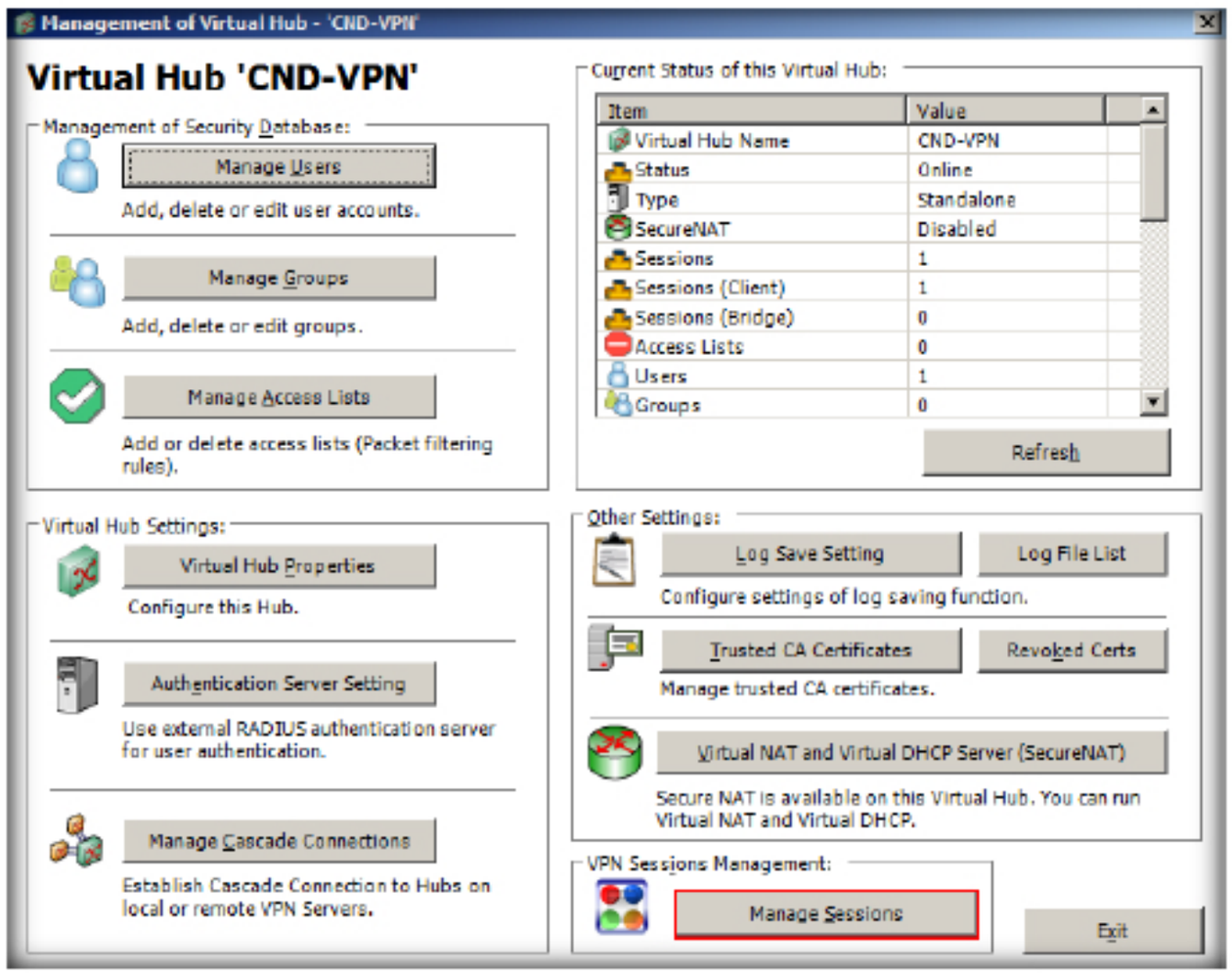

FIGURE 2.33: VPN Server Manage Sessions

53. The Manage Sessions wizard appears, where you can see connected users through the VPN Network, you can use different options to manage the VPN users as shown in the screenshot

📖 If you are using a lot of Cloud VMs, and operating private networks between Cloud VMs, SoftEther VPN can make a bridge between a Cloud-based private network and your corporate network. It means that you can build a virtual dedicated Ethernet line between your company and a Cloud Provider's network.

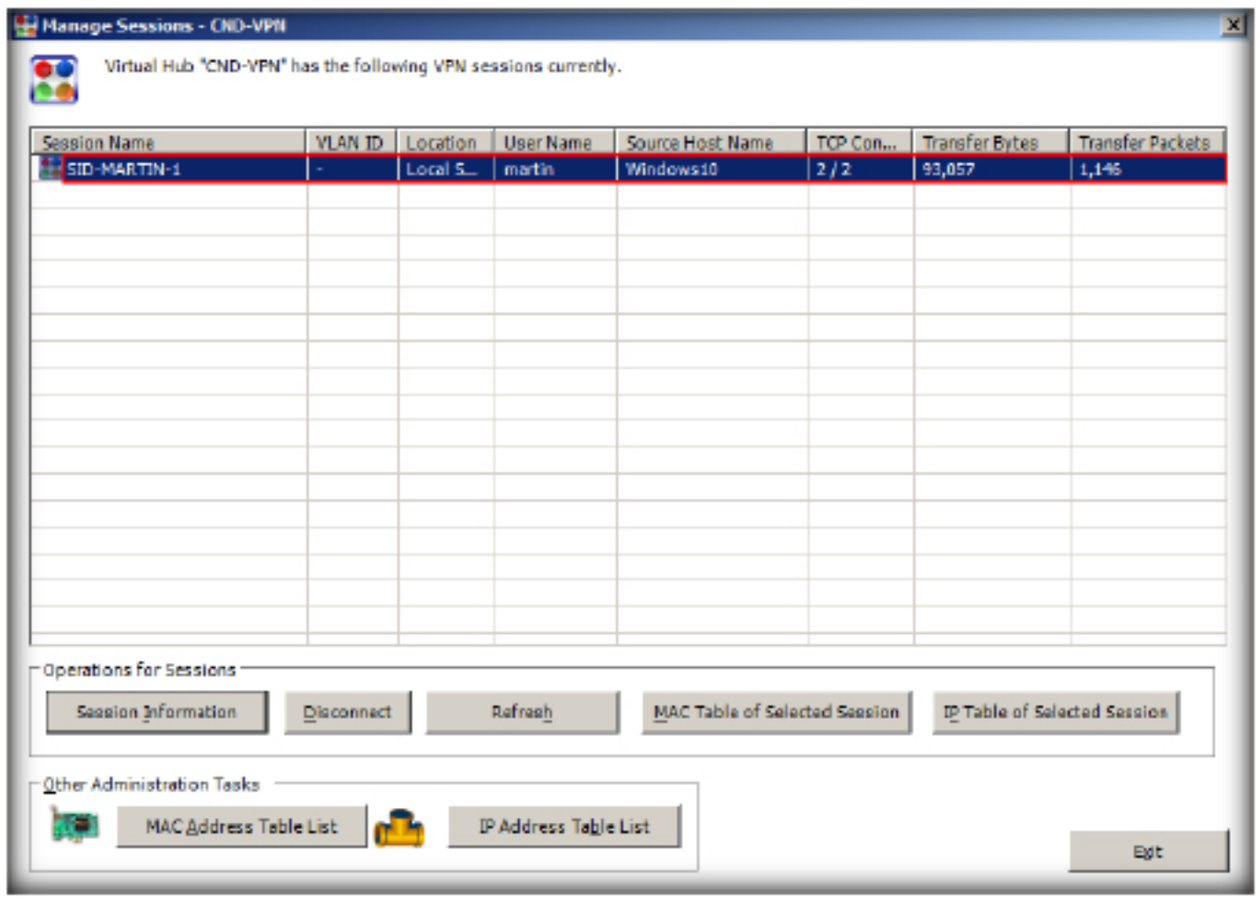

FIGURE 2.34: Manage Sessions Dashboard

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs