Zentyal for Network Administrators

VERSION 6.0

Preparation for the certification exam
Zentyal Certified Associate (ZeCA)

Index

EFFECT: The new certificates with the Common Name will be issue after save changes.

6. **ACTION** Click on *Save Changes* top button.

   EFFECT: All the certificates are generated and the modules are configured with these certificates.

2.6.5 Proposed exercises

Exercise A

Review all the certificates issued by the CA by using commands 'cat' and 'openssl'. Keep in mind that all the generated certificates are stored in `/var/lib/zentyal/CA/`.

2.7 Virtual private network (VPN) service with OpenVPN

2.7.1 Introduction to the virtual private networks (VPN)

The **virtual private networks** [27] were designed to allow secure access for remote users connected via the Internet to the corporate network as well as securely connect different subnets via the Internet.

Your users might need to access to the internal network resources when they are outside the company premises, for example sales people or teleworkers. The solution is to allow these users to connect to your system via the Internet, although this might mean risking the confidentiality, availability and integrity of the communication. To avoid these problems the connection is not made directly but through virtual private networks.

Using VPN you can create a secure communications tunnel over the Internet that will only accept connections from authorized users. Traffic is encapsulated and can only be read at the other end. Apart from the security advantages VPN connections are seen like another local network connection by the Firewall, thus, having access to local resources and simplifying the infrastructure needed to offer remote services.

The usefulness of the VPN is not limited to remote access by users. An organization may wish to interconnect networks located in different places, such as offices in different cities.

Similarly, Zentyal can operate in two modes, as a server for remote users and also as a VPN Client of a VPN hub server.

Zentyal integrates OpenVPN [28] to configure and manage virtual private networks. In this section you will see how to configure OpenVPN, who has the following advantages:

- Authentication using public key infrastructure.
- SSL-based encryption technology.
- Clients available for Windows, Mac OS and Linux.
- Easier to install, configure and maintain than IPSec, (another open source VPN alternative).
- Allows to use network applications transparently.

[27] http://en.wikipedia.org/wiki/Virtual_private_network
[28] http://openvpn.net/

2.7.2 Configuration of a OpenVPN server with Zentyal

Zentyal can be configured to support remote clients, (sometimes known as road warriors). This means a Zentyal server acting as a gateway and VPN server with multiple local area networks, (LAN), behind it, allows external clients, (the *road warriors*), to connect to the local network via the VPN service.

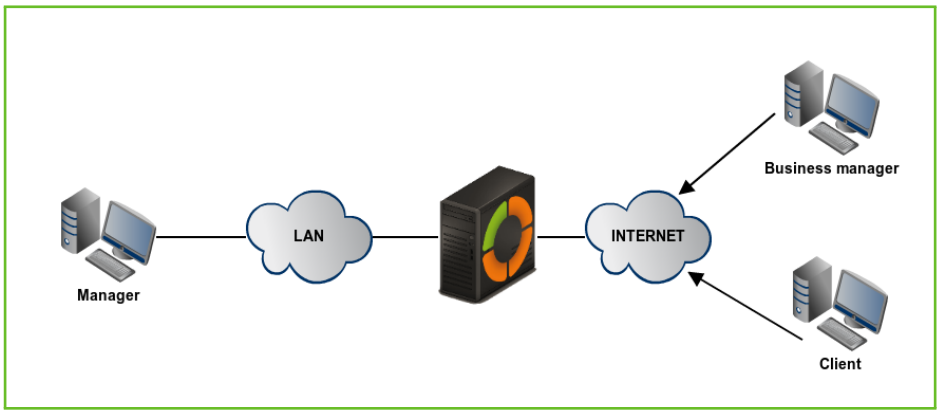

Figure 2.54: Zentyal and remote VPN clients

The goal is to connect the data server with other two remote clients, (Business manager and Client), and also the remote clients to each other.

First, you need to create a **Certification Authority** and individual certificates for the two remote clients. You need to explicitly create an **unique** certificate for each user that will connect to the VPN through *Certification Authority* → *General*.

Note that you also need a certificate for the VPN server. However, Zentyal will issue this certificate automatically when new VPN server is created.

In this scenario Zentyal acts as a **Certification Authority**.

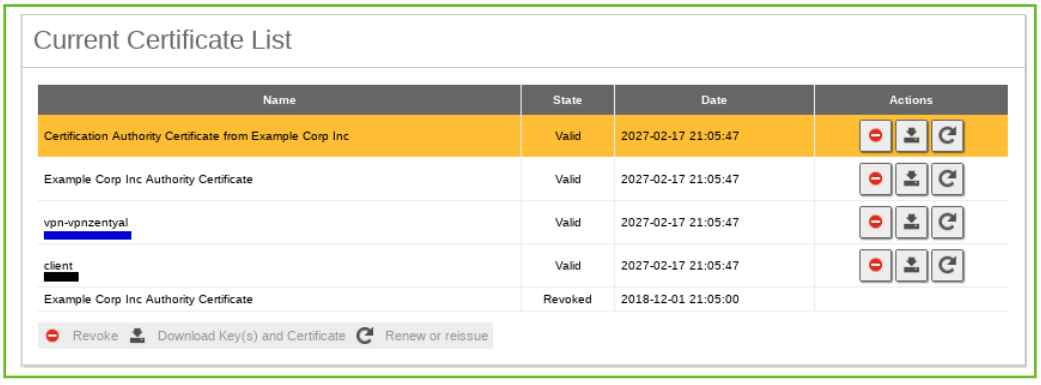

Figure 2.55: Server certificate (blue underline) and client certificate (black underline)

Once you have the certificates then configure the Zentyal VPN server by selecting *Create a new server*. The only value you need to enter to create a new server is the name. Zentyal ensures the task of creating a VPN server is easy and it sets the configuration values automatically.

Figure 2.56: New VPN server created

The following configuration parameters are added automatically and can be changed if necessary: *port/protocol*, *certificate*, (Zentyal will create one automatically using the VPN server name), and *network address*. The VPN network addresses are assigned both to the server and the clients. If you need to change the *network address* you must make sure that there is no conflict with a local network. In addition you will automatically be notified of local network detail, i.e. the networks connected directly to the network interfaces of the host, through the private network.

TIP: Zentyal allows the configuration of VPN with UPD or TCP protocols. UDP is faster and more efficient, as less control information is transmitted, therefore there is more room for data. TCP, on the other hand, is more reliable and can cope better with unstable connections and Internet providers that kill long lasting connections.

As you can see the VPN server will be listening on all external interfaces. Therefore you must set at least one of your interfaces as external at *Network* → *Interfaces*. In this scenario only two interfaces are required, one internal for LAN and one external for Internet.

If you want the VPN clients to connect between themselves by using their VPN addresses, you must enable the option *Allow connections among clients*.

In most of the cases you can leave the rest of the configuration options with their default values.

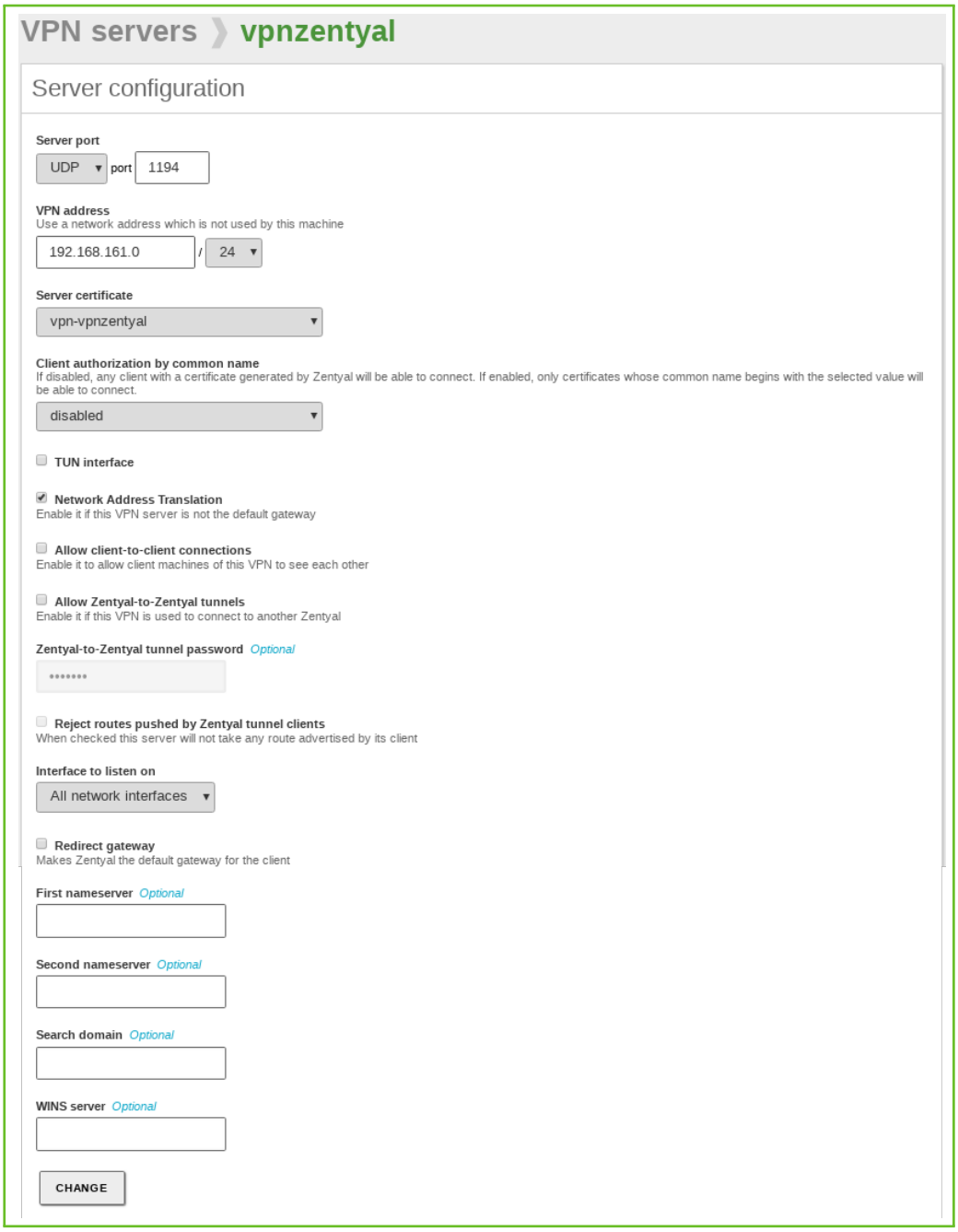

Figure 2.57: VPN server configuration

In case more advanced configuration is necessary:

- ***VPN ADDRESS:*** Indicates the virtual subnet where the VPN server will be located and the clients it has. You must take care that this network does not overlap with any other and for the purposes of firewall, it is an internal network. By default *192.168.160.1/24*, the clients will get addresses *.2*,*.3*, etc.
- ***SERVER CERTIFICATE:*** Certificate that will show the server to its clients. The Zentyal CA issues by default a certificate for the server, with the name vpn-<yourvpnname>. Unless you want to import an external certificate, usually you maintain this configuration.

- ***CLIENT AUTHORIZATION BY COMMON NAME:*** Requires that the *common name* of the client certificate will start with the selected string of characters to authorize the connection.
- ***TUN INTERFACE:*** By default a *TAP* type interface is used, more similar to a *bridge* of Layer 2. You can also use a *TUN* type interface more similar to a IP node of Layer 3.
- ***NETWORK ADDRESS TRANSLATION:*** **(NAT)** It is recommended to enable this translation if the Zentyal server that accepts the VPN connections is not a default gateway of the internal networks to which you can access from the VPN. Like this the clients of these internal networks respond to Zentyal's VPN instead of the gateway. If Zentyal server is both the VPN server and the gateway, (most common case), this option is indifferent.

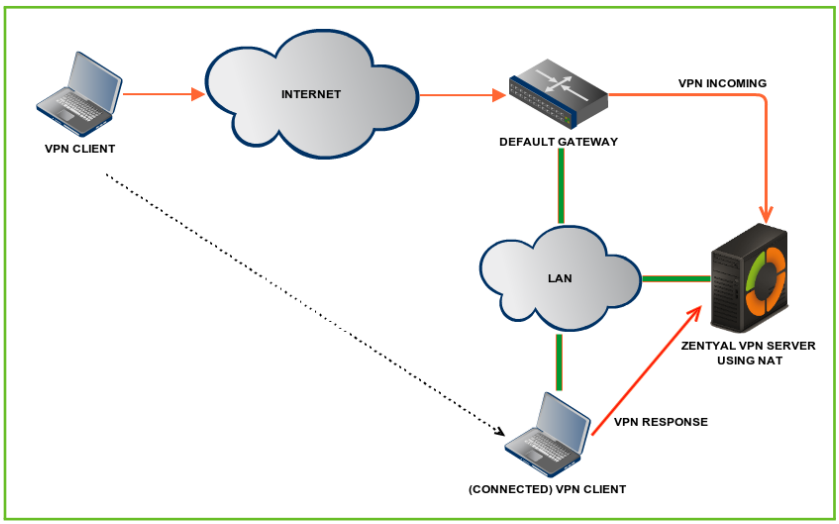

Figure 2.58: VPN server using NAT to become the gateway for the VPN connection

- ***REDIRECT GATEWAY:*** If this option is not checked, the external client will access through the VPN to the established networks, but will use his/her local connection to access to Internet and/or rest of the reachable networks. By checking this option you can achieve that all the traffic of the client will go through the VPN.

The VPN can also indicate name servers, search domain and WINS servers to overwrite those of the client. This is specially useful in the case you have redirected the gateway.

After having created the VPN server you must enable the service and save the changes. Later you must check in *Dashboard* that the VPN server is running.

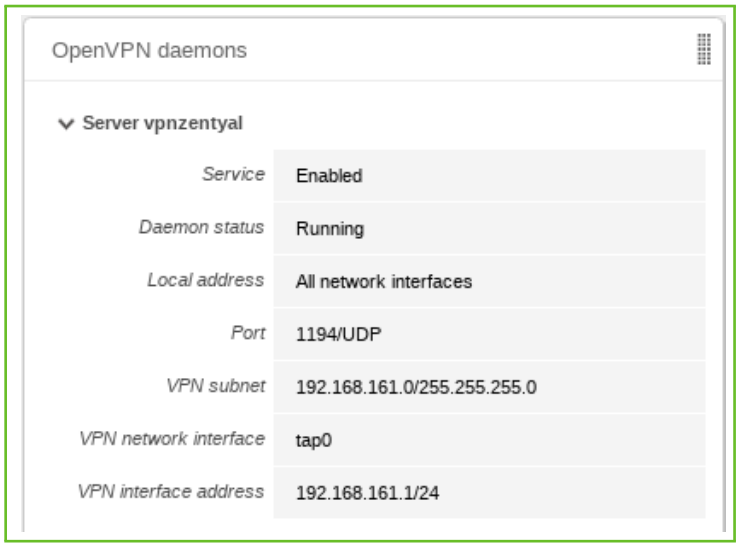

Figure 2.59: Widget of the VPN server

After this you must advertise networks, i.e. routes between the VPN networks and between other networks known by your server. These networks will be accessible by authorised VPN clients. To do this you have to enable the objects you have defined, (see *High-level Zentyal abstractions*), in the most common case, all internal networks. You can configure the advertised networks for this VPN server through the interface of *Advertised networks*.

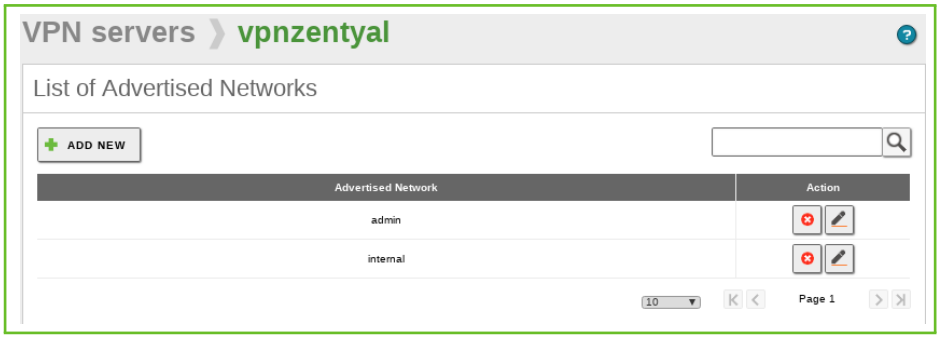

Figure 2.60: Advertised networks of your VPN server

Once you have done this, it is time to configure the clients. The easiest way to configure a VPN client is by using the Zentyal *bundles*, (installation packages that include the VPN configuration file specific to each user and optionally, an installation program). These are available in the table at *VPN* → *Servers*, by clicking the icon in the column *Download client bundle*. You can create *bundles* for Windows, Mac OS and Linux clients. When you create a *bundle* select those certificates that will be used by the clients and set the external IP addresses to which the VPN clients must connect.

As you can see the image below you can have one main VPN server and up to two secondary servers depending on the *Connection strategy* when defining the connection order or you can also try a random order.

Moreover, if the selected system is Windows, you can also add an OpenVPN installer. The Zentyal administrator will download the configuration *bundles* to the clients using the most appropriate method.

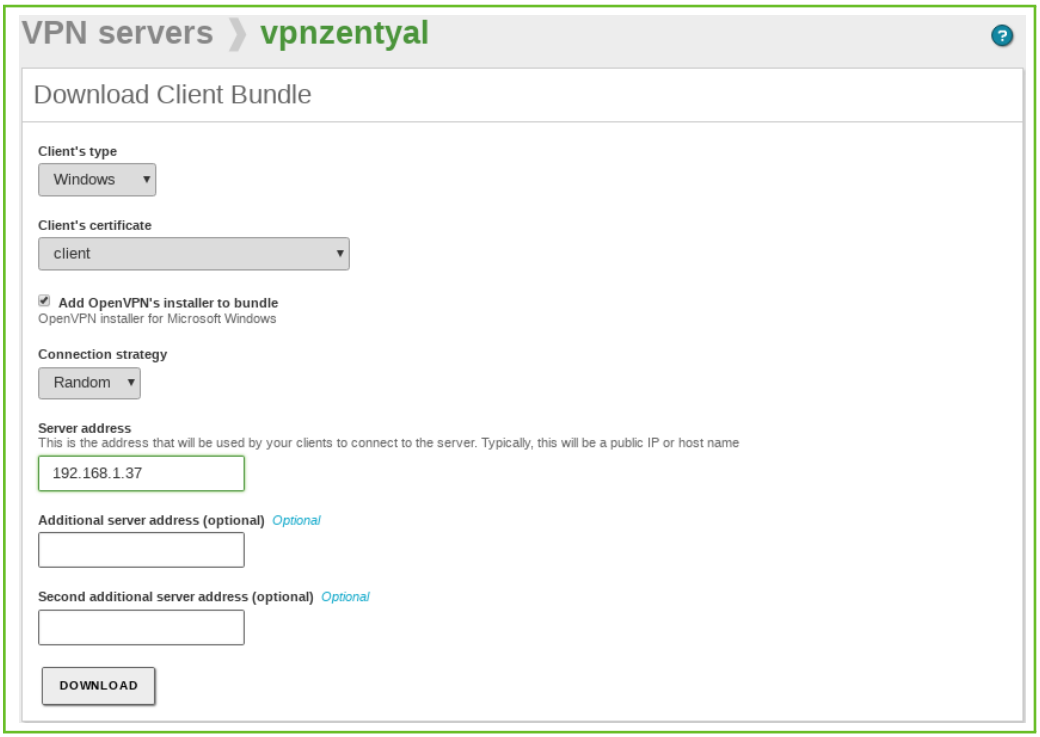

Figure 2.61: Download client bundle

A *bundle* includes the configuration file and the necessary files to start a VPN connection.

You now have access to the data server from both remote clients. If you want to use the local Zentyal DNS service through the private network you need to configure these clients to use Zentyal as name server. Otherwise it will not be possible to access services by the hosts in the LAN by name, but only by IP address. Also, to browse shared files from the VPN [29], you must explicitly allow the broadcast of traffic from the Samba server.

You can see the users currently connected to the VPN service in the Zentyal *Dashboard*. You need to add this *widget* from *Configure widgets*, located in the upper part of the *Dashboard*.

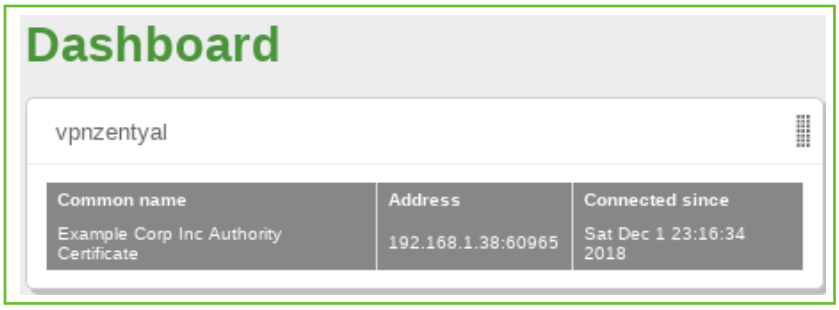

Figure 2.62: Widget with connected clients

[29] For additional information about file sharing go to section *Domain Controller and File Sharing*

2.7.3 Configuration of a VPN server for interconnecting networks

In this scenario two offices in different networks need to be connected via private network. To do this you will use Zentyal as a gateway in both networks. One will act as a VPN client and the other as a server. The following image clarifies the scenario:

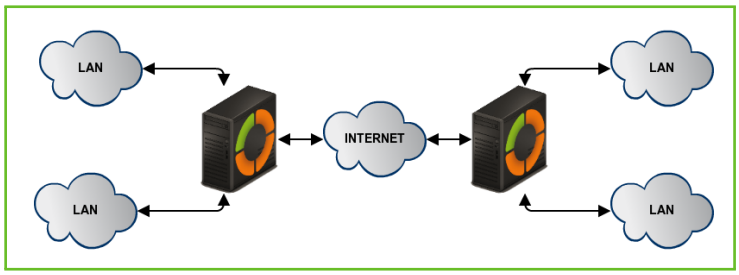

Figure 2.63: Office interconnection with Zentyal through VPN tunnel

The goal is to connect multiple offices, their Zentyal servers and their internal networks, so that one single network infrastructure can be created in a secure way through Internet. To do this you need to configure a VPN server similarly as explained previously.

However, you need to make two small changes. First, enable the *Allow Zentyal-to-Zentyal tunnels* to exchange routes between Zentyal servers, and then introduce a *Password for Zentyal-to-Zentyal tunnels* to establish the connection between the two offices in a safer environment. Take into account that you need to advertise the LAN networks in *Advertised Networks*.

Another important difference is the routing information exchange. In the *roadwarrior to server* scenario described previously the server pushes network routes to the client. In the *server to server* scenario routes are exchanged in both directions and propagated to other clients using the RIP [30] protocol. Therefore you can, as a client, configure the *Advertised Networks* that will be propagated to the other nodes.

Figure 2.64: Zentyal as VPN client

You can configure Zentyal as a VPN client at *VPN* → *Clients*. You must give a *name* to the client and enable the *service*. You can configure the client manually or automatically by using the *bundle* provided by the VPN server. If you do not use the bundle you must introduce the *IP address* and *protocol-port* for the server accepting requests. The *tunnel password* and *certificates* used by the client will also be required. These

[30] http://www.ietf.org/rfc/rfc1058

certificates must have been created by the same **certification authority** the server uses.

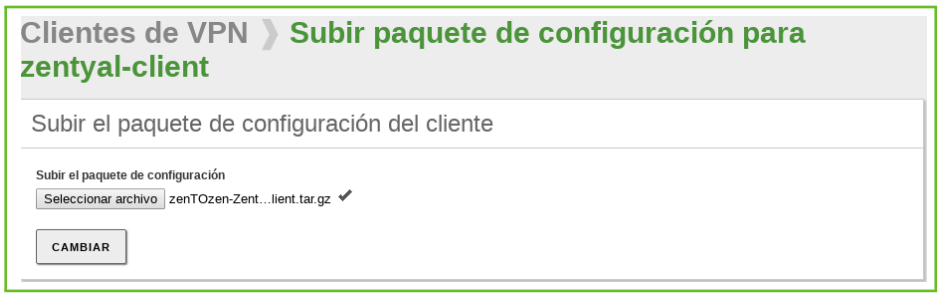

Figure 2.65: Automatic client configuration using VPN bundle

When you *Save changes* in the *Dashboard* you can see a new OpenVPN daemon running as a client and the objective connection directed towards another Zentyal server configured as a server.

Figure 2.66: Dashboard of a Zentyal server configured as a VPN client

The propagation of routes can take a few minutes.

2.7.4 Configuration of an OpenVPN client

In order to configure a VPN client on Windows first your system administrator must give you the *bundle* for your client.

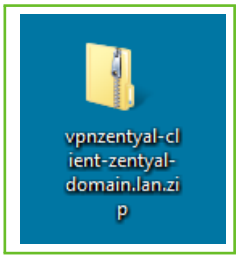

Figure 2.67: The system administrator gives you the bundle for your client

You must unzip it, (click on the file with right button and select *Extract all*). You will find all the VPN installation files and related certificates.

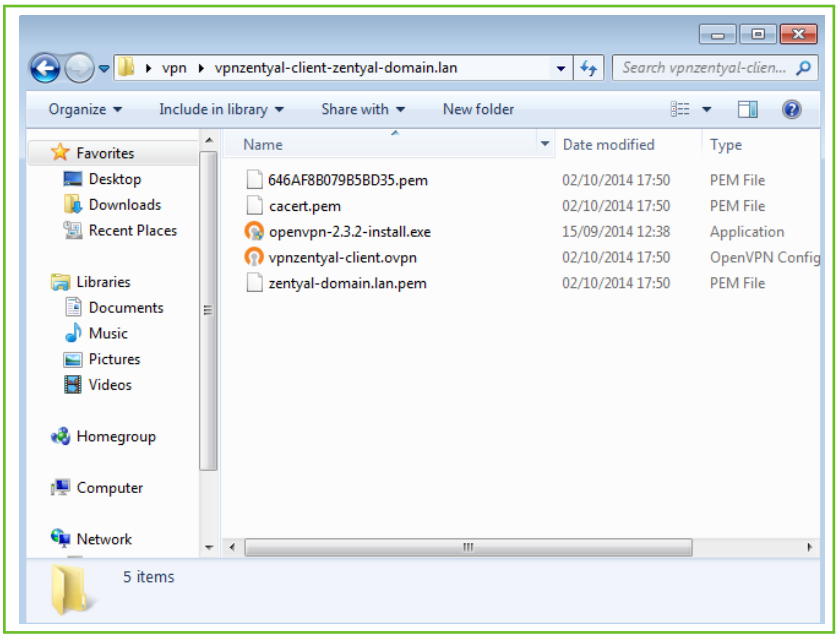

Figure 2.68: Extracted bundle files

Right click on the installer and click on *Run as administrator*. OpenVPN needs to create the virtual network interface and install the drivers.

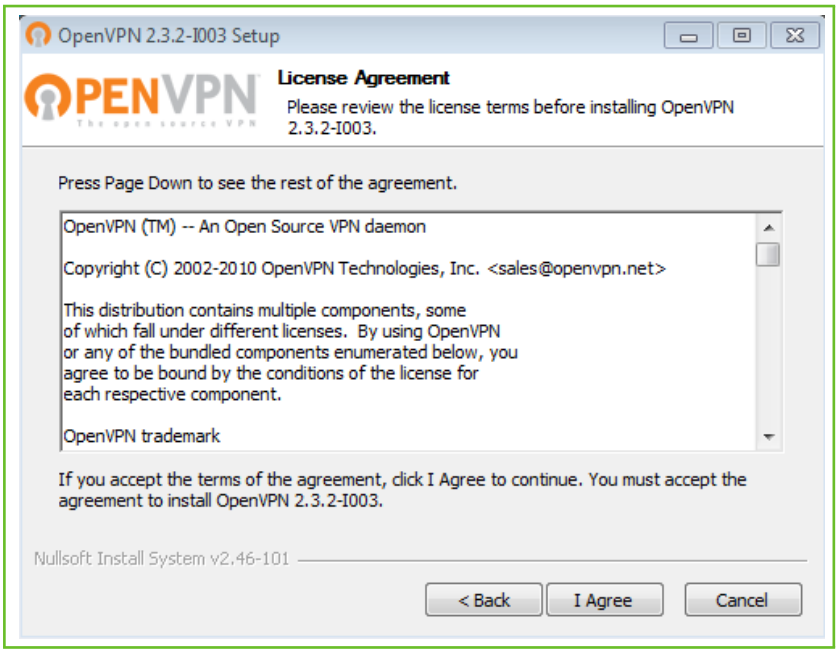

Figure 2.69: Accept the OpenVPN license

It is recommended you install all the modules.

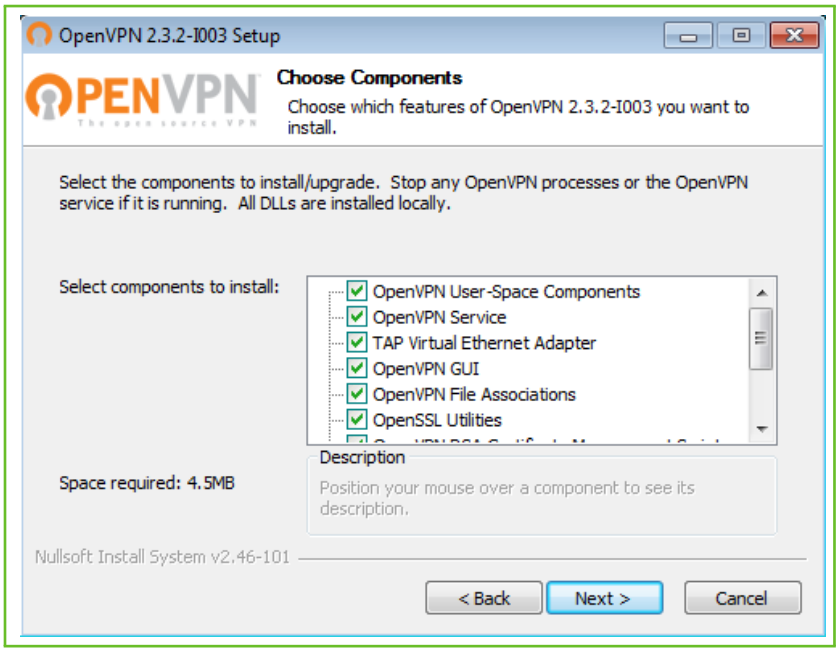

Figure 2.70: List of modules that will be installed

The network adapter software is not certified for Windows but it is totally safe to install.

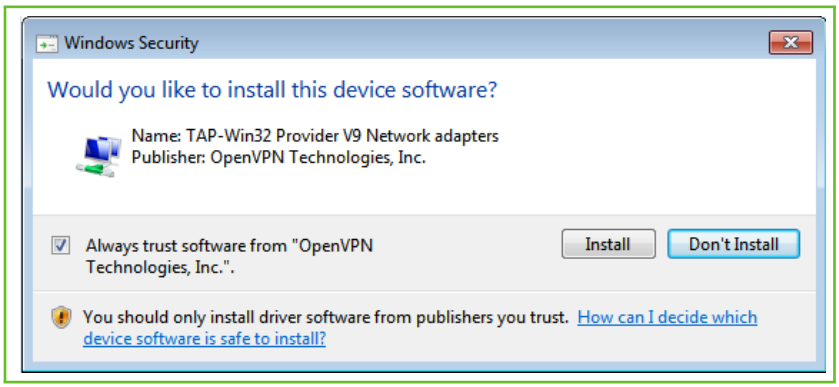

Figure 2.71: Despite the warning you can install the driver

TIP: You must copy all the files included in the *bundle*, except for the *OpenVPN* installer, to the folder *C:\Program Files (x86)\OpenVPN\config* to guarantee the *daemon* will automatically find them.

Once installed a double click on the shortcut that has appeared in your desktop allows you to connect to the VPN.

Figure 2.72: Shortcut to connect to the VPN

2.7.5 Practical examples

Practical example A

"JD Consulting Inc." has equipped its two sales agents with corporate laptops. These laptops need to have access to company intranet. Grant the sales agents access by using the *OpenVPN* module.

1. **ACTION** Access the Zentyal interface, go to side menu *Software Management* → *Zentyal Components*.

   EFFECT: Zentyal shows a list with all installable modules.

2. **ACTION** Select the *VPN* module and click on *Install* button.

   EFFECT: A modal window with module info is shown, once you have confirmed, the installation process starts to install the own module and its dependencies.

3. **ACTION** Go to *Module Status* and enable the *VPN* module, to do this, check the box at the *Select* column. It will inform us about what changes will be done in the System. Allow the operation clicking the *Accept* button.

   EFFECT: The button *Save Changes* has been enabled.

4. **ACTION** Go to side menu *VPN –> Servers*. Click on *Add new* and set a name to the VPN connection in *Name*. Click on *Add*.

   EFFECT: The new VPN connection is listed.

5. **ACTION** Click on *Configure* in the new VPN connection. Check the box *Allow client-to-client connections* and *Redirect gateway*. Click on *Change*.

   EFFECT: The configuration file is modified and is ready to be applied.

6. **ACTION** Go to the *VPN –> Servers*. Click on *Configure* in the *Advertised networks* column.

   EFFECT: All the networks that will be shared are listed.

7. **ACTION** Set the network that you want to share with the sales agents' laptops.

   EFFECT: The networks are listed.

8. **ACTION** Go to the *VPN –> Servers*. Check the box *Enabled*

   EFFECT: The VPN is ready to be started.

9. **ACTION** Click on *Save Changes* top button.

   EFFECT: The *VPN* module is configured and enabled.

10. **ACTION** Go to the side menu *Certification Authority –> General*. Set the FQDN of the sales's laptop in *Common Name* and click on *Issue*.

    EFFECT: The certificate is issued.

11. **ACTION** Repeat the action for the other laptop.

EFFECT: Both certificates are listed.

12. **ACTION** Go to *VPN –> Servers*. Click on *Download client bundle*. Select *Windows* in *Client's type*, the certificate of the sales' agent in *Client's certificate*, check the box *Add OpenVPN's installer to bundle* and set the public IP of the Zentyal server in *Server address*. Click on *Download*.

    EFFECT: The bundle with the VPN configuration for the client is downloaded.

13. **ACTION** Repeat the action for the other laptop.

    EFFECT: The bundle is downloaded for the other laptop.

Practical example B

After opening a new branch office in Chicago, the company wants to connect the new office with the headquarters located in Washington DC safely. You should connect the offices by using the *OpenVPN* module in both servers.

1. **ACTION** In the Washington DC server, access the Zentyal interface, go to the side menu *Certification Authority –> General*. Set the *FQDN* of second server in *Common Name* and click on *Issue*.

    EFFECT: The certificate is issued.

2. **ACTION** On both servers, access the Zentyal interface, go to *Software Management* → *Zentyal Components*.

    EFFECT: You will see a list of all modules available for installation.

3. **ACTION** Select the *VPN* module and click on *Install* button.

    EFFECT: You will see a pop-up window with module information. Upon confirmation the system proceeds with the installation of the module and its dependencies.

4. **ACTION** On both servers, go to *Module Status* and enable the *VPN* module by checking the corresponding box in the *Status* column. You are informed about the changes that will take place. Allow the operation by clicking on *Accept* button.

    EFFECT: The button *Save Changes* has been enabled.

5. **ACTION** In the Washington DC server, go to side menu *VPN –> Servers*.

    EFFECT: All the VPNs are listed.

6. **ACTION** Click on *Add new* and set a name to the VPN connection in *Name*. Click on *Add*.

    EFFECT: The new VPN connection is listed.

7. **ACTION** Click on *Configure* in the new VPN connection. Check the box *Allow Zentyal-to-Zentyal tunnels* and set the password in *Zentyal-to-Zentyal tunnel password*. Click on *Change*.

    EFFECT: The configuration file is modified and is ready to be applied.

8. **ACTION** Go to the *VPN –> Servers*. Click on *Configure* in the *Advertised networks* column.

    EFFECT: All the networks that will be shared are listed.

9. **ACTION** Modify the network that you want to shared with the other Zentyal server.

    EFFECT: The networks are listed.

10. **ACTION** Go to the *VPN –> Servers*. Check the box *Enabled*

EFFECT: The VPN is ready to be started.

11. **ACTION** Select the *Save Changes* top button.

    EFFECT: The *VPN* module is configured and enabled.

12. **ACTION** Go to *VPN –> Servers*. Click on *Download client bundle*. Select the certificate of the other Zentyal server in *Client's certificate* and set the public IP of the Zentyal server in *Server address*. Click on *Download*.

    EFFECT: The bundle with the VPN configuration for the Washington DC is downloaded.

13. **ACTION** In the Chicago server go to side menu *VPN –> Clients*. Click on *Add new* and set a name to the VPN connection in *Name*. Click on *Add*.

    EFFECT: The new VPN connection is listed.

14. **ACTION** Click on *Configure* in the column *Upload client bundle*. Click on *Browse* and search the bundle file with the VPN configuration. Click on *Charge*.

    EFFECT: The Client VPN is configured and is ready to be applied.

15. **ACTION** Go to the *VPN –> Clients*. Click on *Configure* in the *Advertised networks* column.

    EFFECT: All the networks that will be shared are listed.

16. **ACTION** Modify the network that you want to shared with the other Zentyal server.

    EFFECT: The networks are listed.

17. **ACTION** Go to side menu *VPN –> Clients*. Check the box *Enabled*.

    EFFECT: The Client VPN is ready to be started.

18. **ACTION** Select the *Save Changes* top button.

    EFFECT: The *VPN* module is configured and enabled.

2.7.6 Proposed exercises

Exercise A

Configure a VPN which will be only valid with a particular certificate. Check it with two clients, one will have the right certificate and the other won't have a valid one.

2.8 VPN Service with IPsec and L2TP/IPSEC

2.8.1 Introduction to IPsec and L2TP

The **IPsec** protocol [31] (*Internet Protocol security*) is a set of protocols that aim to implement security over the TCP/IP network communications. It provides both authentication and encryption of the session. Unlike other solutions like SSL or TLS, IPsec does not work in the application layer but in the network layer. This allows you to provide security to any communication without having to modify the application you are using.

Like OpenVPN™, IPsec is used to deploy virtual private networks (VPN). It can operate in several modes, host to host, network to host and network to network, being the last one the more frequent: you have subnetworks that you want to link in a secure way over an untrusted network, like the Internet.

[31] http://en.wikipedia.org/wiki/IPsec