Zentyal for Network Administrators

VERSION 7.0

zentyal

Preparation for the certification exam
Zentyal Certified Associate (ZeCA)

zentyal training

Zentyal for
Network Administrators

VERSION 7.0

PRODUCED BY

zentyal

Zentyal | Millsico LLC
info@zentyal.com
sales@zentyal.com
www.zentyal.com

Although every precaution has been taken in the preparation of this training guide, Zentyal | Millsico LLC assumes no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. The information provided is on an "as is" basis and no warranty or fitness is implied.

Index

EFFECT: A new certificate with the Common Name will be issued after saving changes. The *Save Changes* button has been enabled.

5. **ACTION** Do the same action for the Mail module.

   EFFECT: The new certificates with the Common Name will be issued after saving changes.

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

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

7. **ACTION** From the list of certificates, download the CA certificate, a file named *CA-key-and-cert.tar.gz* that contains the public key *ca-public-key.pem* and the certificate *ca- cert.pem*. Following the procedure described above, import the certificate file *ca-cert.pem* on your Windows clients.

   EFFECT: The new certificate will appear in the list of certificates, and all certificates issued by this CA will be accepted by the Windows workstations.

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/`.

Virtual private network (VPN) service with OpenVPN

Introduction to the virtual private networks (VPN)

The **virtual private networks** [1] 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 [2] to configure and manage virtual private networks. In this section you will see how to configure OpenVPN. This solution offers the following advantages:

- Authentication using public key infrastructure.

[1] **VPN:** http://en.wikipedia.org/wiki/Virtual_private_network

[2] **OpenVPN:** http://openvpn.net/

- 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.

Configuration of an 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, allowing external clients (the *road warriors*) to connect to the local network via the VPN service.

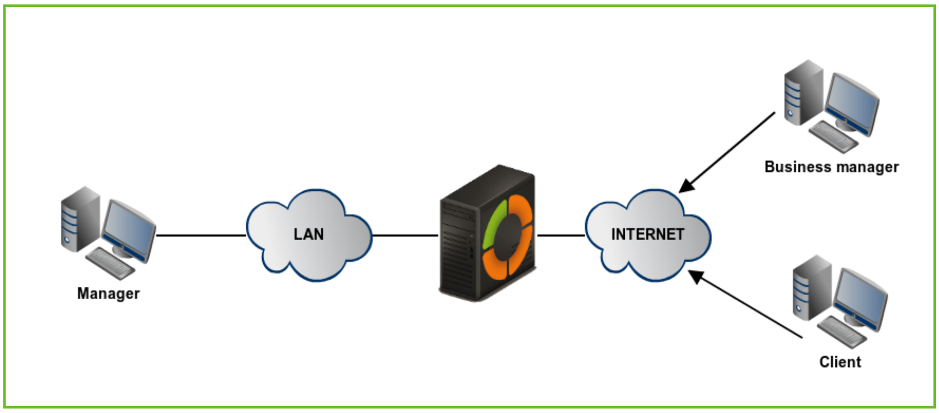
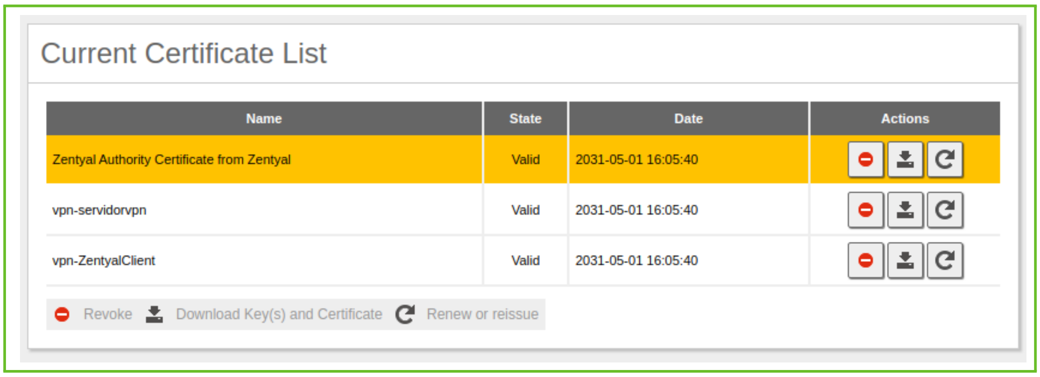


Fig. 2.56: Zentyal and remote VPN clients

Your 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 can do this at *Certification Authority* → *General*. Note that you also need a certificate for the VPN server. However, Zentyal will issue this certificate automatically when the new VPN server is created. In this scenario, Zentyal acts as a **Certification Authority**.



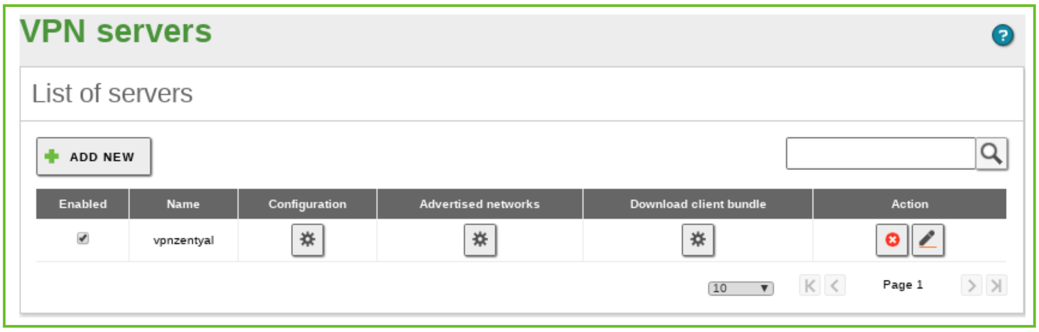
Current Certificate List

Name	State	Date	Actions
Zentyal Authority Certificate from Zentyal	Valid	2031-05-01 16:05:40	⊖ ⤓ ↻
vpn-servidorvpn	Valid	2031-05-01 16:05:40	⊖ ⤓ ↻
vpn-ZentyalClient	Valid	2031-05-01 16:05:40	⊖ ⤓ ↻

⊖ Revoke ⤓ Download Key(s) and Certificate ↻ Renew or reissue

Fig. 2.57: List of issued certificates

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 that the task of creating a VPN server is easy and it sets the configuration values automatically.



VPN servers

List of servers

✚ ADD NEW

Enabled	Name	Configuration	Advertised networks	Download client bundle	Action
☑	vpnzentyal	⚙	⚙	⚙	✖ ✎

Fig. 2.58: Newly created VPN server

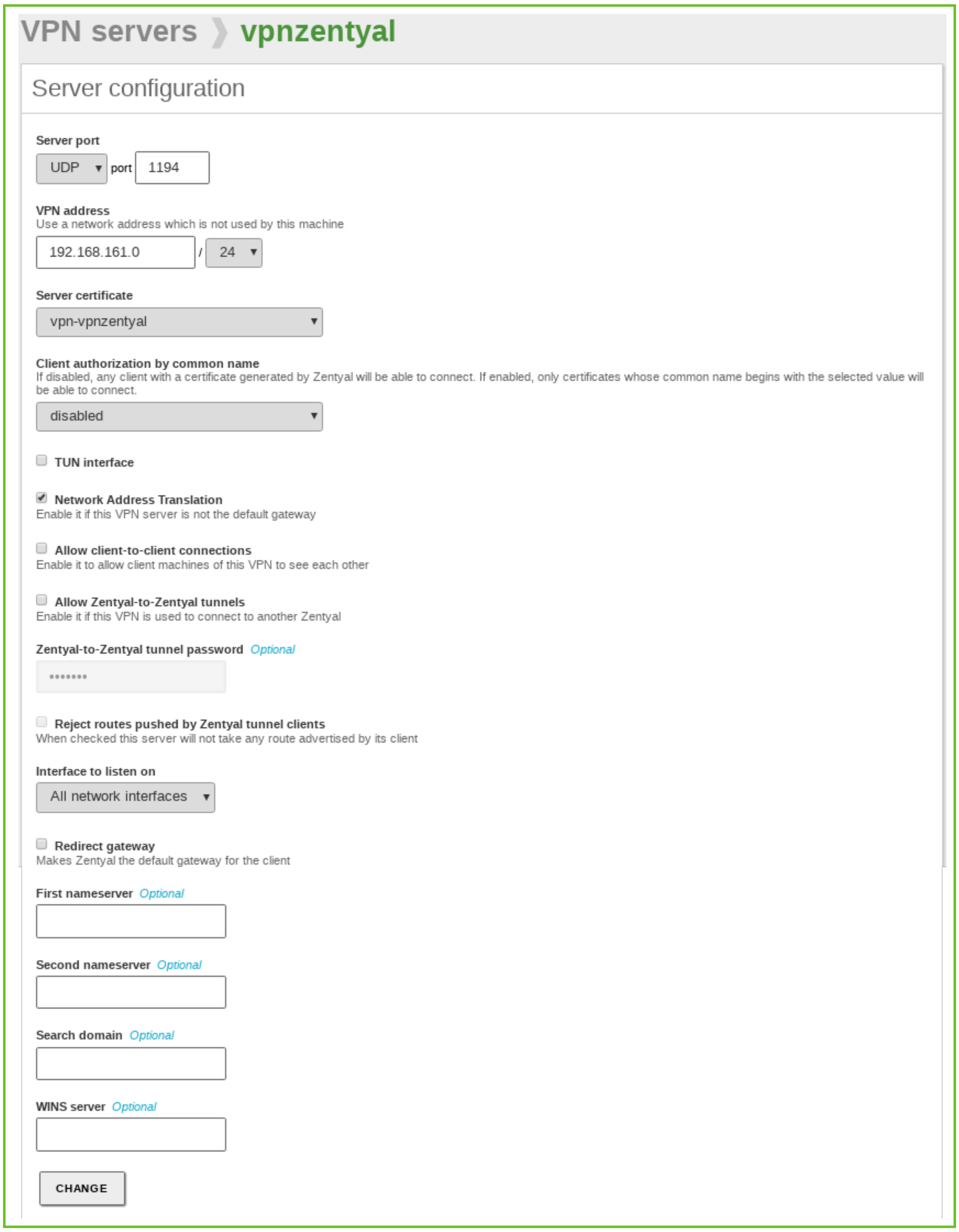
The following configuration parameters are added automatically and can be edited if necessary: *Port/Protocol*, *Certificate* (Zentyal will create one automatically using the VPN server name) and *Network address*. The VPN network addresses are assigned both to the server and the clients. If you need 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 networks, 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 and 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 be able to connect between themselves by using their VPN addresses, you must enable the option *Allow client-to-client connections*.

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



VPN servers ❯ vpnzentyal

Server configuration

Server port
UDP ▾ port 1194

VPN address
Use a network address which is not used by this machine
192.168.161.0 / 24 ▾

Server certificate
vpn-vpnzentyal ▾

Client authorization by common name
If disabled, any client with a certificate generated by Zentyal will be able to connect. If enabled, only certificates whose common name begins with the selected value will be able to connect.
disabled ▾

□ TUN interface

☑ Network Address Translation
Enable it if this VPN server is not the default gateway

□ Allow client-to-client connections
Enable it to allow client machines of this VPN to see each other

□ Allow Zentyal-to-Zentyal tunnels
Enable it if this VPN is used to connect to another Zentyal

Zentyal-to-Zentyal tunnel password *Optional*
•••••••

□ Reject routes pushed by Zentyal tunnel clients
When checked this server will not take any route advertised by its client

Interface to listen on
All network interfaces ▾

□ Redirect gateway
Makes Zentyal the default gateway for the client

First nameserver *Optional*

Second nameserver *Optional*

Search domain *Optional*

WINS server *Optional*

CHANGE

Fig. 2.59: VPN server configuration

In case more advanced configuration is necessary:

- ☒ ***VPN ADDRESS:*** Indicates the virtual subnet where the VPN server and its clients will be located. 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 a certificate for the server by default, 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 the default gateway of the internal networks to which you can access from the VPN. Like this, the clients of these internal networks will use the Zentyal VPN as gateway, instead of their default gateway. If Zentyal server is both the VPN server and the gateway (most common case), this option is indifferent.

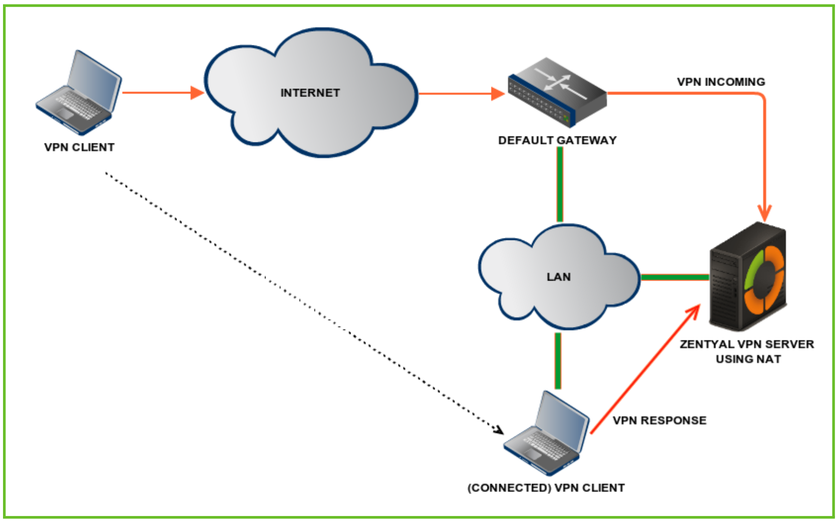
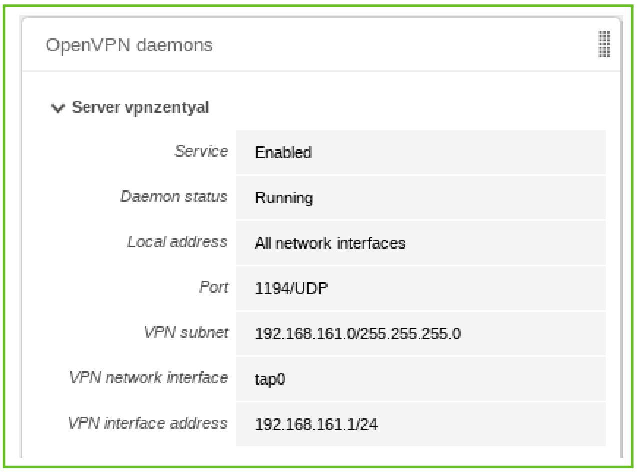


Fig. 2.60: VPN server using NAT to become the default gateway for the VPN connection

- *REDIRECT GATEWAY*: If this option is not checked, the external client will access through the VPN to the advertised networks, but will use the 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 the *Dashboard* that the VPN server is running.



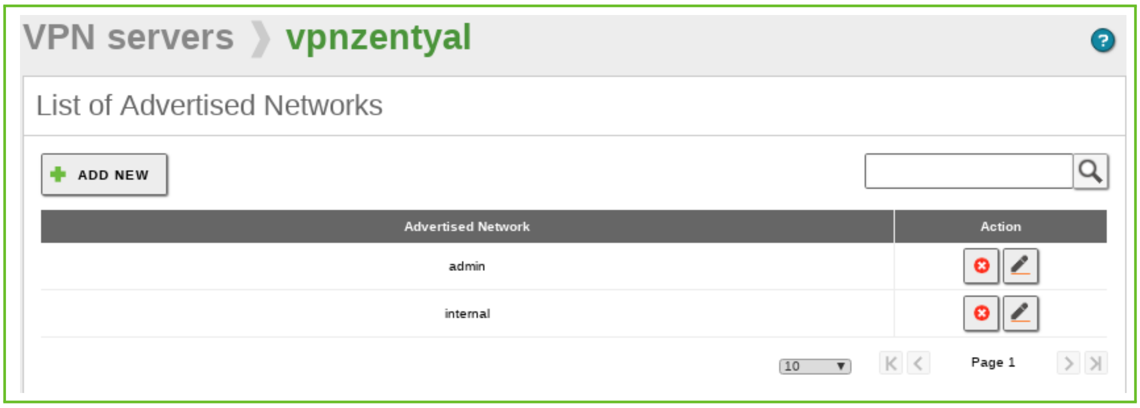
OpenVPN daemons

Server vpnzentyal

Service	Enabled
Daemon status	Running
Local address	All network interfaces
Port	1194/UDP
VPN subnet	192.168.161.0/255.255.255.0
VPN network interface	tap0
VPN interface address	192.168.161.1/24

Fig. 2.61: 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 the internal networks. You can configure the advertised networks for this VPN server through the interface of *Advertised networks*.



VPN servers ❯ vpnzentyal

List of Advertised Networks

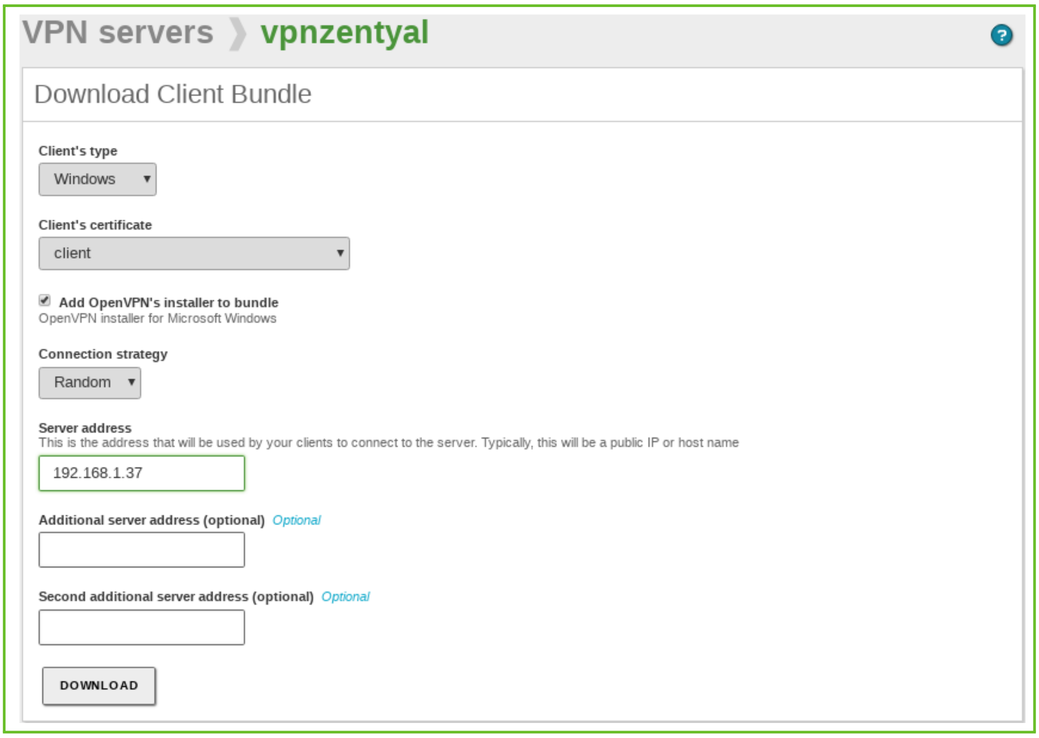
Advertised Network	Action
admin	
internal	

Fig. 2.62: 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*. These are installation packages that include the VPN configuration file specific to each user and optionally, an installation program. The *bundles* are available in the table at *VPN* → *Servers*, by clicking the **Download** button in the *Download client bundle* section. 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 defined *Connection strategy*, the connection can be established in a specific order or in random order.

In addition, 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.



VPN servers ❯ vpnzentyal

Download Client Bundle

Client's type
Windows

Client's certificate
client

☑ Add OpenVPN's installer to bundle
OpenVPN installer for Microsoft Windows

Connection strategy
Random

Server address
This is the address that will be used by your clients to connect to the server. Typically, this will be a public IP or host name
192.168.1.37

Additional server address (optional) Optional

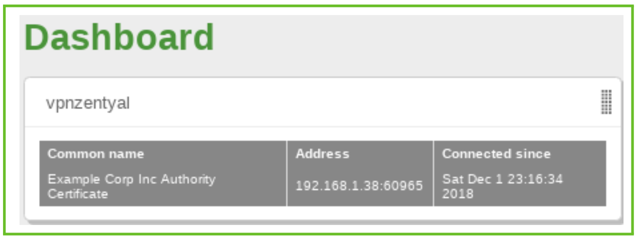
Second additional server address (optional) Optional

Fig. 2.63: 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 a name server. Otherwise, it will not be possible to access services offered by the hosts in the LAN by name, but only by IP address. Also, to browse shared files from the VPN [3], 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*.



Dashboard

vpnzentyal

Common name	Address	Connected since
Example Corp Inc Authority Certificate	192.168.1.38:60965	Sat Dec 1 23:16:34 2018

Fig. 2.64: Widget with connected clients

[3] For additional information about file sharing, go to section *Domain Controller and Directory Services*.

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:

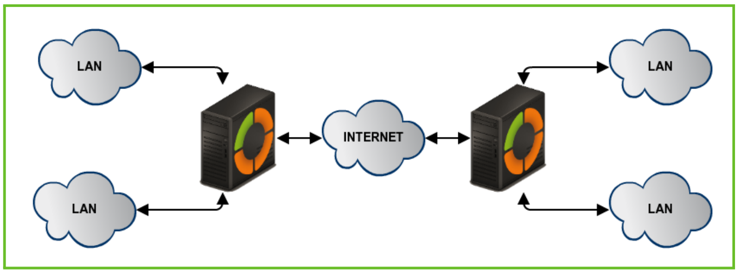
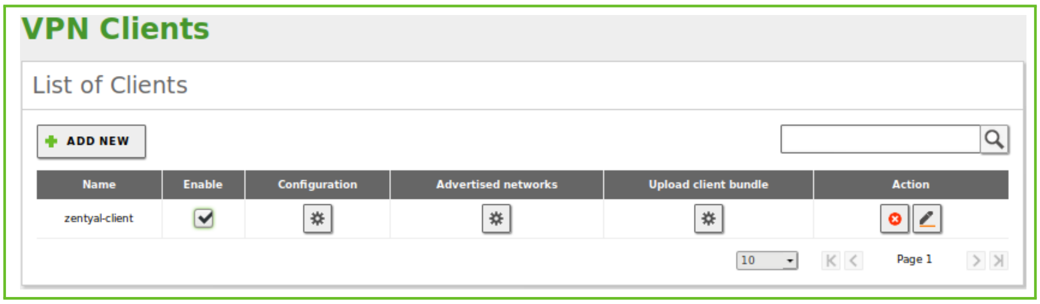


Fig. 2.65: Office interconnection with Zentyal through VPN tunnel

The goal is to connect multiple offices, their Zentyal servers and their internal networks, creating one single network infrastructure in a secure way through the 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 [4] protocol. Therefore, in the servers that act as VPN clients of the central node, it is also possible to add the *Advertised Networks* that will be propagated to the other nodes.



VPN Clients

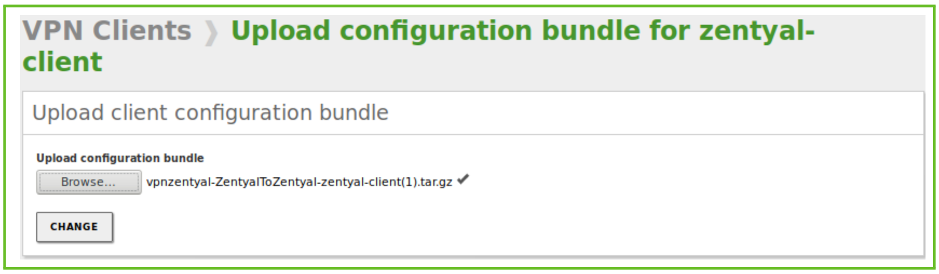
List of Clients

Name	Enable	Configuration	Advertised networks	Upload client bundle	Action
zentyal-client	☑	⚙	⚙	⚙	⊗ ✎

Fig. 2.66: Zentyal as VPN a 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 certificates must have been created by the same **certification authority** that the server uses.

[4] **Routing Information Protocol (RIP)**: http://www.ietf.org/rfc/rfc1058



VPN Clients 〉 Upload configuration bundle for zentyal-client

Upload client configuration bundle

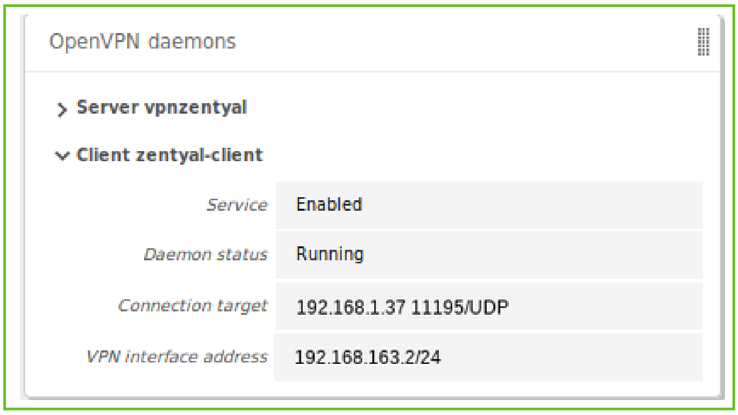
Upload configuration bundle

Browse... vpnzentyal-ZentyalToZentyal-zentyal-client(1).tar.gz ✓

CHANGE

Fig. 2.67: 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 target connection directed towards another Zentyal server configured as a server.



OpenVPN daemons

› Server vpnzentyal

⌄ Client zentyal-client

Service	Enabled
Daemon status	Running
Connection target	192.168.1.37 11195/UDP
VPN interface address	192.168.163.2/24

Fig. 2.68: Dashboard of a Zentyal server configured as a VPN client

WARNING: The propagation of routes can take a few minutes.

Configuration of an OpenVPN client

In order to configure a VPN client on Windows, first the system administrator must provide the *Bundle* for your client.

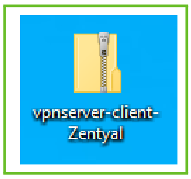
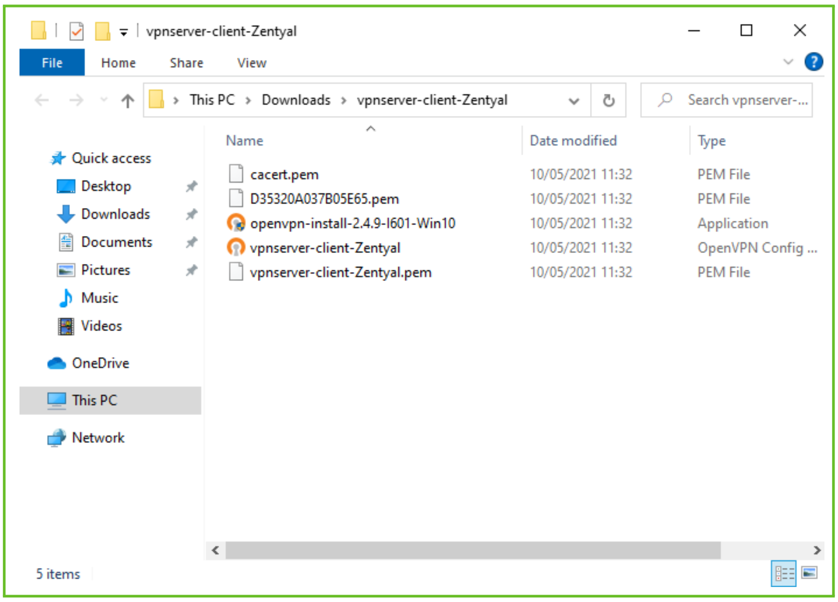


Fig. 2.69: The system administrator provides the client bundle

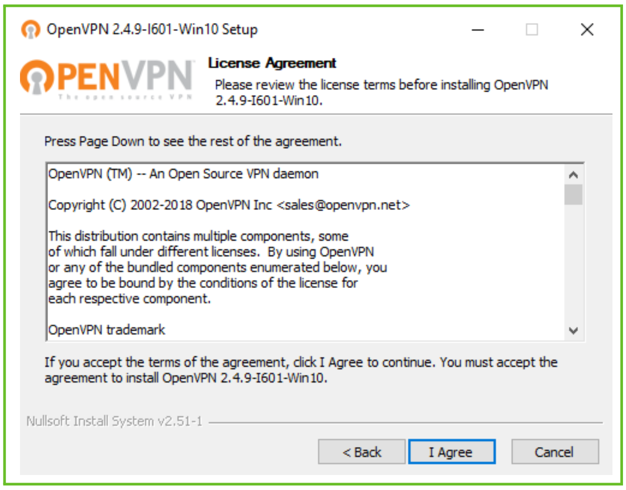
You must unzip it (click on the file with right button and select *Extract all*). You will find all the VPN installation files and related certificates.



Name	Date modified	Type
cacert.pem	10/05/2021 11:32	PEM File
D35320A037B05E65.pem	10/05/2021 11:32	PEM File
openvpn-install-2.4.9-I601-Win10	10/05/2021 11:32	Application
vpnserver-client-Zentyal	10/05/2021 11:32	OpenVPN Config ...
vpnserver-client-Zentyal.pem	10/05/2021 11:32	PEM File

Fig. 2.70: 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.


OpenVPN 2.4.9-I601-Win10 Setup
OPENVPN
Nullsoft Install System v2.51-1
< Back
I Agree
Cancel

License Agreement

Please review the license terms before installing OpenVPN 2.4.9-I601-Win10.

Press Page Down to see the rest of the agreement.

OpenVPN (TM) -- An Open Source VPN daemon

Copyright (C) 2002-2018 OpenVPN Inc <sales@openvpn.net>

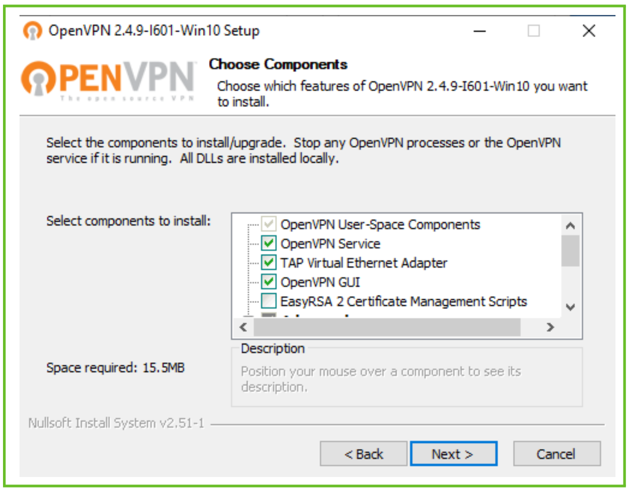
This distribution contains multiple components, some of which fall under different licenses. By using OpenVPN or any of the bundled components enumerated below, you agree to be bound by the conditions of the license for each respective component.

OpenVPN trademark

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.4.9-I601-Win10.

Fig. 2.71: Accept the OpenVPN license

It is recommended that you install all the modules.



OpenVPN 2.4.9-I601-Win10 Setup

Choose Components

Choose which features of OpenVPN 2.4.9-I601-Win10 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
- ☐ EasyRSA 2 Certificate Management Scripts

Space required: 15.5MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.51-1

Fig. 2.72: List of modules that will be installed

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 that 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.

Fig. 2.73: Shortcut to connect to the VPN

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

3. ACTION Go to *Module Status* and enable the *VPN* module by checking the corresponding box at the *Select* column. You will be informed of the changes that will take place. Allow the operation by clicking the *Accept* button.

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

4. ACTION Go to the 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 VPN 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 Configure the networks 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 the *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 agent'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*. In *Client's type*, select *Windows* and in *Client's certificate* the sales agent´s certificate, check the box *Add OpenVPN's installer to bundle* and establish 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 the 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 Configure the networks that you want to share 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 Chicago server in *Client's certificate*. Add the public IP of the Washington DC server in *Server address*. Click on *Download*.

    EFFECT: The bundle with the VPN configuration for the Chigago server 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 *Change*.

    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.

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 correct certificate and the other one an invalid certificate.

VPN Service with IPsec and L2TP/IPSEC

Introduction to IPsec and L2TP

The **IPsec** protocol [1] (*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™ or PPTP, IPsec is used to deploy virtual private networks (VPNs). It can operate in several modes, host to host, network to host and network to network, the latter being the most common option: you have subnetworks that you want to interconnect in a secure way over an untrusted network, like the Internet.

IPsec is an optional annex of the IPv4 protocol, but it is integrated in IPv6. The main advantage of IPsec compared to other VPN protocols like OpenVPN™ integrated in Zentyal or PPTP, is that IPsec is an standard defined by the Internet Engineering Task Force (IETF) that many manufacturers have implemented in their devices, so it is the ideal option to connect Zentyal with third party UTM devices (Cisco, Fortinet, Check-Point, etc).

L2TP operates at layer 2 of the TCP/IP model [2] . Because of this, remote clients can operate on the local network just like any other host of the LAN, instead of behaving as a Point-to-point type connection. L2TP performs the tunneling and user authentication tasks, but Zentyal's implementation relies on IPsec for traffic encryption.

Zentyal integrates Libreswan [3] as its IPsec and L2TP/IPsec solution. This service uses the ports 500, 1701 and 4500 of UDP and the ESP protocol.

Configuring an IPsec tunnel in Zentyal

Before starting with the configuration, note that this module is only available in the Commercial Editions.

To configure IPsec in Zentyal, go to *VPN* → *IPsec*. Here you can define all the tunnels and IPsec connections you need. You can enable or disable each one of them and add an explanatory note.

[1] **IPsec:** http://en.wikipedia.org/wiki/IPsec
[2] **RFC 2661:** http://www.ietf.org/rfc/rfc2661.txt
[3] **Libreswan:** http://libreswan.org/