

Zentyal para Administradores de Redes

VERSIÓN 6.0



Preparación para el examen de certificación
Zentyal Certified Associate (ZeCA)

Índice

1. INTRODUCCIÓN A ZENTYAL	9
1.1. PRESENTACIÓN	9
1.1.1. Las pymes y las TICs	9
1.1.2. Zentyal: servidor Linux para pymes	10
1.1.3. Acerca del manual.....	11
1.2. INSTALACIÓN	11
1.2.1. El instalador de Zentyal.....	12
1.2.2. Configuración inicial.....	23
1.2.3. Requisitos de hardware	30
1.3. PRIMEROS PASOS CON ZENTYAL	31
1.3.1. La interfaz web de administración de Zentyal	31
1.3.2. Configuración básica de red en Zentyal	39
1.3.3. Ejemplos prácticos	50
1.3.4. Ejercicios propuestos.....	51
1.4. ACTUALIZACIÓN DE SOFTWARE	51
1.4.1. La actualización de software en Zentyal.....	51
1.4.2. Gestión de componentes de Zentyal.....	52
1.4.3. Actualizaciones del sistema.....	54
1.4.4. Actualizaciones automáticas.....	55
1.4.5. Ejemplos prácticos	56
1.4.6. Ejercicios propuestos.....	56
1.5. REGISTROS	57
1.5.1. Consulta de registros en Zentyal.....	57
1.5.2. Configuración de registros en Zentyal	59
1.5.3. Registro de auditoría de administradores.....	60
1.5.4. Ejemplos prácticos	62
1.5.5. Ejercicios propuestos.....	63
1.6. BACKUP DE CONFIGURACIÓN	63
1.6.1. Función del backup de configuración de Zentyal.....	63
1.6.2. Gestión del backup de configuración	63
1.6.3. Ejemplos prácticos	65
1.6.4. Ejercicios propuestos.....	65
1.7. PREGUNTAS DE AUTOEVALUACIÓN	66
2. ZENTYAL COMO INFRAESTRUCTURA	67
2.1. INTRODUCCIÓN	67
2.2. ABSTRACCIONES DE RED DE ALTO NIVEL EN ZENTYAL	68
2.2.1. Objetos de red	68
2.2.2. Servicios de red	70
2.2.3. Ejemplos prácticos	72
2.2.4. Ejercicios propuestos.....	74
2.3. SERVICIO DE RESOLUCIÓN DE NOMBRES DE DOMINIO (DNS)	74

2.3.1. Introducción a DNS.....	74
2.3.2. Configuración de un servidor DNS <i>caché</i> con Zentyal	78
2.3.3. Proxy DNS transparente.....	80
2.3.4. Redirectores DNS.....	80
2.3.5. Configuración de un servidor DNS autoritativo con Zentyal.....	81
2.3.6. Ejemplos Prácticos	85
2.3.7. Ejercicios propuestos.....	86
2.4. SERVICIO DE SINCRONIZACIÓN DE HORA (NTP)	87
2.4.1. Introducción a NTP	87
2.4.2. Configuración de un servidor NTP con Zentyal.....	87
2.4.3. Ejemplos prácticos	89
2.4.4. Ejercicios propuestos.....	89
2.5. SERVICIO DE CONFIGURACIÓN DE RED (DHCP).....	89
2.5.1. Introducción a DHCP.....	90
2.5.2. Configuración de un servidor DHCP con Zentyal	91
2.5.3. Ejemplos Prácticos	97
2.5.4. Ejercicios propuestos.....	97
2.6. AUTORIDAD DE CERTIFICACIÓN (CA)	98
2.6.1. Infraestructura de clave pública (PKI)	98
2.6.2. Importación de certificados en los clientes.....	100
2.6.3. Configuración de una Autoridad de Certificación con Zentyal	108
2.6.4. Ejemplos prácticos	113
2.6.5. Ejercicios propuestos.....	114
2.7. SERVICIO DE REDES PRIVADAS VIRTUALES (VPN) CON OPENVPN	114
2.7.1. Introducción a las redes privadas virtuales (VPN)	114
2.7.2. Configuración de un servidor OpenVPN con Zentyal	115
2.7.3. Configuración de un servidor VPN para la interconexión de redes con Zentyal	121
2.7.4. Configuración del cliente OpenVPN	123
2.7.5. Ejemplos prácticos	125
2.7.6. Ejercicios propuestos.....	128
2.8. VPN CON IPSEC Y L2TP/IPSEC.....	128
2.8.1. Introducción a IPsec y L2TP/IPSEC	128
2.8.2. Configuración de un túnel IPsec con Zentyal	128
2.8.3. Configurando un túnel L2TP/IPSEC en Zentyal	130
2.8.4. Ejemplos prácticos	132
2.8.5. Ejercicios propuestos.....	133
2.9. SERVICIO DE TRANSFERENCIA DE FICHEROS (FTP)	133
2.9.1. Introducción a FTP	133
2.9.2. Configuración del cliente FTP.....	134
2.9.3. Configuración de un servidor FTP con Zentyal	138
2.9.4. Ejemplos prácticos	139
2.9.5. Ejercicios propuestos.....	140
2.10. GESTIÓN DE MÁQUINAS VIRTUALES	140
2.10.1. Introducción a la virtualización.....	140
2.10.2. Creación de máquinas virtuales con Zentyal	141
2.10.3. Mantenimiento de máquinas virtuales	144
2.10.4. Ejemplos prácticos	145
2.10.5. Ejercicios propuestos.....	146
2.11. COPIAS DE SEGURIDAD	146
2.11.1. Diseño de un sistema de copias de seguridad	146
2.11.2. Configuración de las copias de seguridad de datos en un servidor Zentyal	147

2.11.3. Ejemplos prácticos	153
2.11.4. Ejercicios propuestos.....	154
2.12. PREGUNTAS DE AUTOEVALUACIÓN.....	155
3. ZENTYAL COMO PUERTA DE ACCESO	157
3.1. INTRODUCCIÓN.....	157
3.2. CORTAFUEGOS.....	157
3.2.1. Introducción al sistema de cortafuegos	157
3.2.2. Configuración de un cortafuegos con Zentyal.....	158
3.2.3. Redirección de puertos con Zentyal	163
3.2.4. Reescritura de direcciones de origen (SNAT) con Zentyal.....	164
3.2.5. Ejemplos prácticos	166
3.2.6. Ejercicios propuestos.....	167
3.3. ENCAMINAMIENTO.....	167
3.3.1. Introducción al encaminamiento o routing	167
3.3.2. Configuración del encaminamiento con Zentyal.....	168
3.3.3. Configuración del balanceo con Zentyal	171
3.3.4. Configuración de la tolerancia a fallos con Zentyal	173
3.3.5. Ejemplos prácticos	175
3.3.6. Ejercicios propuestos.....	177
3.4. SERVICIO DE AUTENTICACIÓN DE RED (RADIUS)	177
3.4.1. Introducción a RADIUS	177
3.4.2. Configuración del Punto de Acceso con RADIUS	178
3.4.3. Configuración del cliente RADIUS	179
3.4.4. Configuración de un servidor RADIUS con Zentyal	182
3.4.5. Ejemplos prácticos	184
3.4.6. Ejercicios propuestos.....	184
3.5. SERVICIO DE PROXY HTTP.....	184
3.5.1. Introducción al servicio de Proxy HTTP	184
3.5.2. Configuración en el navegador de un Proxy HTTP	185
3.5.3. Configuración general del Proxy HTTP con Zentyal	188
3.5.4. Reglas de acceso	190
3.5.5. Filtrado de contenidos con Zentyal.....	192
3.5.6. Limitación de ancho de banda.....	197
3.5.7. Bloqueo HTTPS por dominio	198
3.5.8. Ejemplos prácticos	199
3.5.9. Ejercicios propuestos.....	201
3.6. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS/IPS).....	201
3.6.1. Introducción al Sistema de Detección/Prevención de Intrusos	201
3.6.2. Configuración de un IDS/IPS con Zentyal.....	202
3.6.3. Alertas del IDS/IPS	204
3.6.4. Ejemplos prácticos	204
3.6.5. Ejercicios propuestos.....	205
3.7. PREGUNTAS DE AUTOEVALUACIÓN.....	206
4. ZENTYAL COMO OFICINA.....	207
4.1. INTRODUCCIÓN.....	207
4.2. CONTROLADOR DE DOMINIO Y COMPARTICIÓN DE FICHEROS.....	207
4.2.1. Introducción al servicio de directorio y dominios	207
4.2.2. Samba: La implementación de directorio activo y SMB/CIFS en Linux.....	209
4.2.3. Configuración de un servidor de dominio con Zentyal	209
4.2.4. Configurar Zentyal como un servidor de Dominio <i>Standalone</i>	214

4.2.5. Uniendo un cliente Windows al dominio	217
4.2.6. Autenticación con Kerberos	219
4.2.7. Cambiar la contraseña de usuario	220
4.2.8. Políticas de Grupo (GPO).....	220
4.2.9. Unir Zentyal Server a un dominio existente	221
4.2.10. Migración Total	224
4.2.11. Limitaciones conocidas	225
4.2.12. Configurar un servidor de ficheros con Zentyal	225
4.2.13. Ejemplos prácticos	228
4.2.14. Ejercicios propuestos.....	230
4.3. ANTIVIRUS	231
4.3.1. Introducción al antivirus	231
4.3.2. Configuración del módulo Antivirus.....	231
4.3.3. Ejemplos prácticos	232
4.3.4. Ejercicios propuestos.....	233
4.4. PREGUNTAS DE AUTOEVALUACIÓN.....	234
5. ZENTYAL COMO COMUNICACIONES	235
5.1. INTRODUCCIÓN.....	235
5.2. SERVICIO DE CORREO ELECTRÓNICO (SMTP/POP3-IMAP4)	235
5.2.1. Introducción al servicio de correo electrónico	235
5.2.2. Configuración de un servidor SMTP/POP3-IMAP4 con Zentyal.....	238
5.2.3. Configuración del cliente de correo	246
5.2.4. Cliente de Webmail.....	254
5.2.5. Soporte ActiveSync®.....	256
5.2.6. Ejemplos prácticos	257
5.2.7. Ejercicios propuestos.....	258
5.3. FILTRADO DE CORREO ELECTRÓNICO	258
5.3.1. Introducción al filtrado de correo electrónico	258
5.3.2. Esquema del filtrado de correo en Zentyal.....	259
5.3.3. Lista gris.....	259
5.3.4. Verificadores de contenidos	260
5.3.5. Antivirus	260
5.3.6. Antispam	261
5.3.7. Filtrado de Correo SMTP	264
5.3.8. Listas de control de conexiones externas	266
5.3.9. Ejemplos prácticos	266
5.3.10. Ejercicios propuestos.....	267
5.4. SERVICIO DE MENSAJERÍA INSTANTÁNEA (JABBER/XMPP)	268
5.4.1. Introducción al servicio de mensajería instantánea.....	268
5.4.2. Configuración de un servidor Jabber/XMPP con Zentyal.....	269
5.4.3. Configuración de un cliente Jabber	271
5.4.4. Configurando salas de conferencia Jabber.....	276
5.4.5. Ejemplos prácticos	281
5.4.6. Ejercicios propuestos.....	281
5.5. PREGUNTAS DE AUTOEVALUACIÓN.....	283
6. APÉNDICES.....	285
6.1. APÉNDICE A: ENTORNO DE PRUEBAS CON VIRTUALBOX	285
6.1.1. Acerca de la virtualización	285
6.1.2. VirtualBox.....	286
6.2. APÉNDICE B: ESCENARIOS AVANZADOS DE RED.....	298

6.2.1. Escenario 1: Escenario base, conexión a Internet, red interna y anfitrión	298
6.2.2. Escenario 2: Varias redes internas	300
6.2.3. Escenario 3: Varias puertas de enlace	301
6.2.4. Escenario 4: Escenario base + cliente externo	302
6.2.5. Escenario 5: Multisede	303
6.3. APÉNDICE C: DESARROLLO Y USOS AVANZADOS	304
6.3.1. Importación de datos de configuración	304
6.3.2. Personalización avanzada de servicios	305
6.3.3. Entorno de desarrollo de nuevos módulos	307
6.3.4. Política de publicación de la Edición Comercial	308
6.3.5. Política de publicación de la Edición Development	308
6.3.6. Política de gestión de errores	308
6.3.7. Soporte de la comunidad	309
6.4. APÉNDICE D: RESPUESTA A LAS PREGUNTAS DE AUTOEVALUACIÓN	309
6.4.1. Respuesta a las preguntas de autoevaluación	309

6. **ACCIÓN** Seleccionar el botón de *Guardar los cambios* de la parte superior.

EFECTO: Todos los certificados son generados y los módulos son modificados con los nuevos certificados.

2.6.5 EJERCICIOS PROPUESTOS

□ EJERCICIO A

Comprueba los certificados expedidos por la CA usando los comandos `'cat'` y `'openssl'`. Como pista mencionar que todos los certificados generados son almacenados en: `/var/lib/zentyal/CA/`.

2.7

SERVICIO DE REDES PRIVADAS VIRTUALES (VPN) CON OPENVPN

2.7.1 INTRODUCCIÓN A LAS REDES PRIVADAS VIRTUALES (VPN)

Las **redes privadas virtuales** ²⁷ tienen como finalidad permitir el acceso a las intranets a usuarios remotos a través de la Internet así como conectar de manera segura subredes distintas a través de redes no seguras.

Es muy común que nuestros usuarios necesiten acceder a recursos de nuestra intranet, mientras se encuentran fuera de las instalaciones de la empresa, Es un caso habitual para comerciales o teletrabajadores, por poner un ejemplo. La solución pasa por permitir la conexión de estos usuarios a nuestras instalaciones a través de redes privadas virtuales que aseguran la confidencialidad de las comunicaciones.

Usando una red privada virtual o VPN, (*Virtual Private Network*, de sus siglas en inglés), podemos crear un túnel seguro que sólo aceptará conexiones que provengan de usuarios autorizados. El tráfico viaja encapsulado y sólo es posible leerlo en el otro extremo del túnel. Para facilitar su uso y configuración, las conexiones aparecen como si estuviesen dentro de las redes internas, aprovechando así todos los recursos y configuraciones dispuestas por el administrador de sistemas para la red local.

La utilidad de las VPN no se limita al acceso remoto de los usuarios; una organización puede desear conectar entre sí redes que se encuentran en sitios distintos, como por ejemplo, oficinas en distintas ciudades.

Por éso Zentyal ofrece dos modos de funcionamiento, como servidor para usuarios individuales y también como nodo central para la conexión de otros servidores.

Zentyal integra **OpenVPN** ²⁸ para configurar y gestionar las redes privadas virtuales. En esta sección veremos como configurar OpenVPN para disfrutar de las siguientes ventajas:

- Autenticación mediante infraestructura de clave pública.
- Cifrado basado en tecnología SSL.
- Clientes disponibles para Windows, Mac OS y Linux.
- Más sencillo de instalar, configurar y mantener que IPSec,(otra alternativa para VPNs en software libre).
- Posibilidad de usar programas de red de forma transparente.

²⁷ http://es.wikipedia.org/wiki/Red_privada_virtual

²⁸ <http://openvpn.net/>

2.7.2 CONFIGURACIÓN DE UN SERVIDOR OPENVPN CON ZENTYAL

Se puede configurar Zentyal para dar soporte a clientes remotos, (conocidos como *Road Warriors*). En esta modalidad el servidor Zentyal trabaja como puerta de enlace y como servidor VPN permitiendo a clientes externos (los *road warriors*) conectarse a las redes locales configuradas para ello vía servicio VPN.

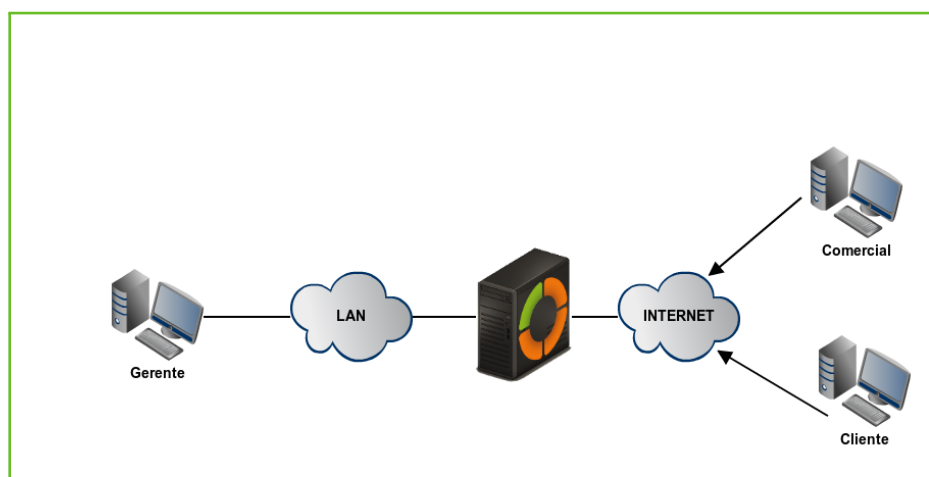









Figura 2.56: Zentyal y clientes remotos de VPN

Nuestro objetivo es conectar al servidor de datos con los otros 2 clientes remotos (Comercial y Cliente) y estos últimos entre si.

Para ello necesitamos crear una **Autoridad de Certificación** y certificados individuales para los dos clientes remotos que crearemos mediante *Autoridad de certificación* → *General*. También se necesita un certificado para el servidor VPN sin embargo, Zentyal expide este certificado automáticamente cuando se crea un nuevo servidor VPN. En este escenario, Zentyal actúa como **Autoridad de Certificación**.

Current Certificate List			
Name	State	Date	Actions
Zentyal Authority Certificate from Zentyal	Valid	2028-11-27 02:40:05	  
vpn-servidorvpn	Valid	2028-11-27 02:40:05	  
webserver.zentyal-domain.ian	Revoked	2018-11-30 02:41:53	




 Revoke  Download Key(s) and Certificate  Renew or reissue

Figura 2.57: Certificados expedidos en el servidor

Una vez tenemos los certificados, debemos poner a punto el servidor VPN en Zentyal usando el botón *Crear un nuevo servidor*. El único parámetro que necesitamos introducir para crear un servidor es el nombre. Zentyal hace trivial la tarea de configuración del servidor VPN ya que establece gran parte de los valores necesarios de manera automática.



Figura 2.58: Nuevo servidor VPN creado

Éstos son los parámetros de configuración añadidos automáticamente por Zentyal, (que pueden ser modificados si es necesario): una pareja de *puerto/protocolo*, un *certificado* (Zentyal creará uno automáticamente usando el nombre del servidor VPN) y una *dirección de red*. Las direcciones de la red VPN se asignan tanto al servidor como a los clientes. Si se necesita cambiar la *dirección de red* nos deberemos asegurar que no entra en conflicto con una red local. Además, se informará automáticamente de las redes locales, es decir, las redes conectadas directamente a los interfaces de red de la máquina, a través de la red privada.

TRUCO: Zentyal permite la configuración de VPN sobre el protocolo UDP o TCP. El primero tiene la ventaja de ser más rápido pues transmite menos información de control y, por tanto, hay más espacio para datos en cada paquete. El segundo, TCP, es resistente a errores y es preferible en el caso de conexiones inestables o sometidas a políticas de ahorro de ancho de banda como el corte de conexiones de larga duración por parte del ISP.

Como vemos el servidor VPN está escuchando en todas las interfaces externas. Por tanto debemos configurar al menos una de nuestras interfaces como 'externa' vía *Red* → *Interfaces*. En nuestro escenario sólo se necesitan dos interfaces, una interna para la LAN y otra externa para Internet.

Si queremos que los clientes de VPN puedan conectarse entre sí usando su dirección de VPN, debemos activar la opción *Permitir conexiones entre clientes*.

El resto de opciones de configuración las podemos dejar con sus valores por defecto en la mayor parte de los casos.

Configuración del servidor

Puerto del servidor
 UDP puerto

Dirección VPN
 Use una dirección de red que no esté en uso por esta máquina
 /

Certificado de servidor

Autorizar al cliente por su nombre común
 Si esta opción se deshabilita, cualquier cliente con un certificado generado por Zentyal podrá conectarse. Si se habilita, solo se podrá conectar con certificados cuyo CN (Common Name) empiece con el valor seleccionado.

Interfaz TUN

Traducción de dirección de red (NAT)
 Habilite esto si este servidor VPN no es la puerta de enlace por defecto

Permitir conexiones cliente-cliente
 Habilite esto para permitir que máquinas clientes de esta VPN puedan verse unas a otras

Permitir túneles de Zentyal a Zentyal
 Habilite esto si esta VPN se usa para conectar con otro Zentyal

Contraseña de túneles de Zentyal a Zentyal *Opcional*

Ignorar rutas enviadas por los Zentyal clientes del túnel
 Cuando se marque esta opción, este servidor no aplicará ninguna ruta publicada por sus clientes

Interfaz en la que escuchar

Redirigir puerta de enlace
 Configura Zentyal como la puerta de enlace por defecto para el cliente

Servidor de nombres primario *Opcional*

Servidor de nombres secundario *Opcional*

Dominio de búsqueda *Opcional*

Servidor WINS *Opcional*

Figura 2.59: Configuración de servidor VPN

En caso de que necesitemos una configuración más avanzada:

- ☒ **DIRECCIÓN VPN:** Indica la subred virtual donde se situará el servidor VPN y sus clientes. Debemos tener cuidado de que esta red no se solape con ninguna otra. Para el cortafuegos es una red interna más. Por defecto está en la subred 192.168.160.1/24, donde los clientes irán recibiendo las direcciones .2,*.3*, etc.
- ☒ **CERTIFICADO DE SERVIDOR:** Certificado que muestra el servidor a sus clientes. La CA de Zentyal expide un certificado por defecto para el servidor con el nombre vpn-<nuestro nombre de vpn>. A menos que queramos importar un certificado externo lo habitual es mantener esta configuración.
- ☒ **AUTORIZAR AL CLIENTE POR SU NOMBRE COMÚN:** Requiere que el *common name* del certificado del cliente empiece por la cadena de caracteres seleccionada para autorizar la conexión.
- ☒ **INTERFAZ TUN:** Por defecto se usa una interfaz de tipo TAP, semejante a un *bridge* de capa 2, pero podemos usar una interfaz de tipo TUN más semejante a un enlace en capa 3.
- ☒ **TRADUCCIÓN DE DIRECCIÓN DE RED (NAT):** Es recomendable tener esta traducción

CAPÍTULO 2

ZENTYAL COMO INFRAESTRUCTURA

activada si el servidor Zentyal que acepta las conexiones VPN no es la puerta de enlace por defecto de las redes internas a las que podremos acceder desde la VPN. De esta forma los clientes de estas redes internas utilizarán la VPN de Zentyal como gateway en lugar de a su puerta de enlace predeterminada. Si el servidor Zentyal es tanto servidor VPN como puerta de enlace (caso más habitual), esta opción no tiene ningún efecto.

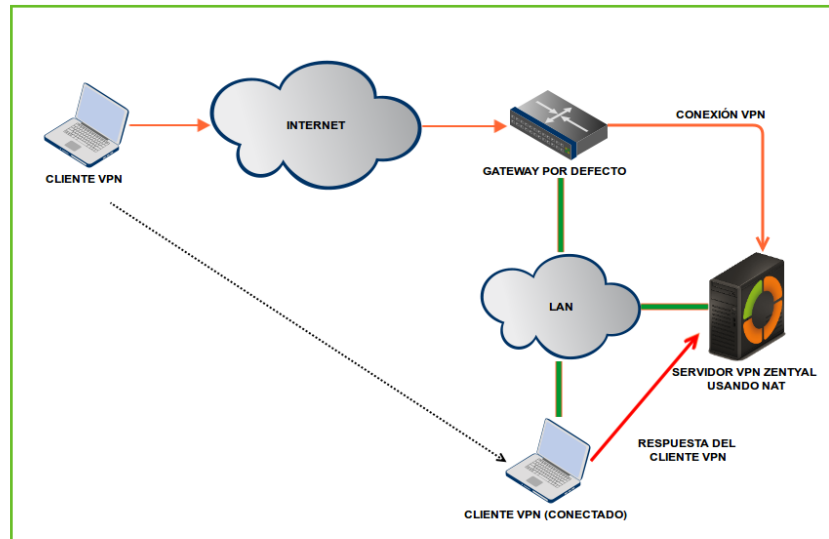


Figura 2.60: Servidor VPN usando NAT para convertirse en la puerta de enlace por defecto

- ❌ **REDIRIGIR PUERTA DE ENLACE:** Si esta opción no está marcada el cliente externo accederá a través de la VPN a las redes anunciadas pero usará su conexión local para salir a Internet y/o resto de redes alcanzables. Marcando esta opción podemos conseguir que todo el tráfico del cliente viaje a través de la VPN.

La VPN puede indicar además servidores de nombres, dominio de búsqueda y servidores WINS para sobrescribir los propios del cliente. Ésto es especialmente útil en caso de que hayamos redirigido la puerta de enlace.

Tras crear el servidor VPN debemos habilitar el servicio y guardar los cambios. Posteriormente, se debe comprobar en *Dashboard* que un servidor VPN está funcionando.



Figura 2.61: Widget del servidor VPN

Tras ello debemos anunciar las redes, es decir, establecer rutas entre las redes VPN y el resto de redes conocidas por nuestro servidor. Dichas redes serán accesibles por los clientes VPN autorizados. Para ello daremos de alta objetos definidos al efecto, ver *Abstracciones de red de alto nivel en Zentyal*, en el caso más habitual todas nuestras redes internas. Podemos configurar las redes anunciadas para este servidor VPN mediante la interfaz *Redes anunciadas*.

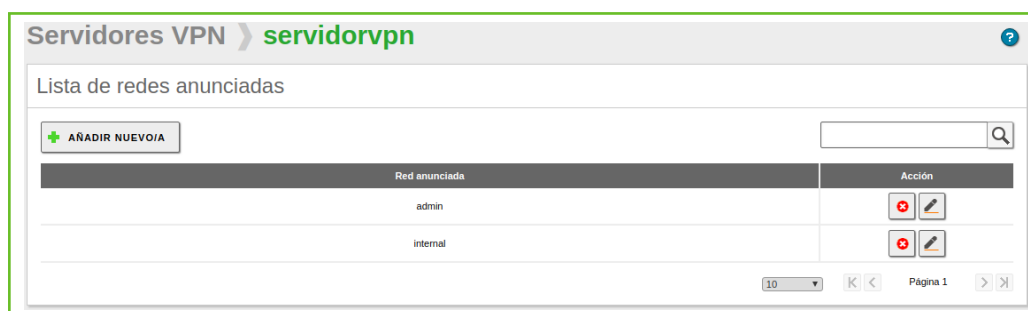



Figura 2.62: Redes anunciadas para nuestro servidor VPN

Una vez hecho ésto es momento de configurar los clientes. La forma más sencilla de configurar un cliente VPN es utilizando los *bundles* de Zentyal. Éstos son paquetes de instalación que incluyen el archivo de configuración VPN específico para cada usuario y, opcionalmente, el programa de instalación del software cliente openVPN. Los paquetes quedan disponibles en *VPN → Servidores*, al pulsar el icono de la columna *Descargar bundle del cliente*. Se pueden crear *bundles* para clientes Windows, Mac OS y Linux. Al crear un *bundle* se seleccionan aquellos certificados que se van a dar al cliente y se establece la dirección externa del servidor a la cual los clientes VPN se deben conectar.

Como se puede ver en la imagen de abajo podemos configurar sistemas complejos con un servidor VPN principal y hasta dos secundarios. Dependiendo de la *Estrategia de conexión* podemos establecer las conexiones a los diferentes servidores de manera linealmente ordenada o de modo aleatorio.

Además si el sistema cliente es Windows se puede incluir en el paquete el propio

programa instalador del cliente OpenVPN™, como decíamos más arriba. Los *bundles* de configuración los descarga el administrador de Zentyal para distribuirlos a los clientes de la manera que crea oportuna.



Descargar paquete de configuración de cliente

Tipo de cliente
Windows

Certificado del cliente
vpn-client

Añadir instalador de OpenVPN al paquete de configuración del cliente
Instalador de OpenVPN para Microsoft Windows

Estrategia de conexión
Aleatorio

Dirección del servidor
Esta es la dirección que usarán sus clientes para conectarse al servidor. Normalmente, ésta será una IP pública o un nombre de host
192.168.20.192

Dirección adicional del servidor (opcional) *Opcional*

Dirección secundaria adicional para el servidor (opcional) *Opcional*

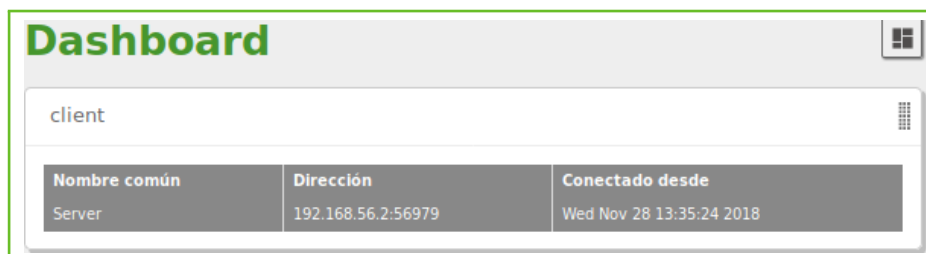
DESCARGAR

Figura 2.63: Descargar paquete de configuración de cliente

Un *bundle* incluye el fichero de configuración y los ficheros necesarios para comenzar una conexión VPN.

Ahora tenemos acceso al servidor de datos desde los dos clientes remotos. Si se quiere usar el servicio local de DNS de Zentyal a través de la red privada será necesario configurar estos clientes para que usen Zentyal como servidor de nombres, de lo contrario no se podrá acceder a los servicios de las máquinas de la LAN por nombre, sino únicamente por dirección IP. Así mismo para navegar por los ficheros compartidos desde la VPN ²⁹ se debe permitir explícitamente el tráfico de difusión del servidor Samba.

Los usuarios conectados actualmente al servicio VPN se muestran en el *Dashboard* de Zentyal. Tendremos que añadir este *widget* desde *Configurar widgets*, situado en la parte superior del *Dashboard*.



Nombre común	Dirección	Conectado desde
Server	192.168.56.2:56979	Wed Nov 28 13:35:24 2018

Figura 2.64: Widget con clientes conectados

²⁹ Para más información sobre compartición de ficheros ir a la sección *Controlador de Dominio y Compartición de ficheros*

2.7.3 CONFIGURACIÓN DE UN SERVIDOR VPN PARA LA INTERCONEXIÓN DE REDES CON ZENTYAL

En este escenario tenemos dos oficinas en diferentes redes que necesitan estar conectadas a través de una red privada. Para hacerlo usaremos en ambas sendos servidores Zentyal como puertas de enlace. Uno actuará como cliente VPN y otro como servidor. La siguiente imagen ilustra esta situación:

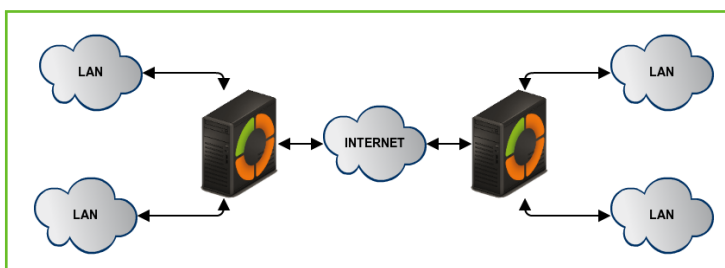


Figura 2.65: Interconexión de sedes con Zentyal mediante túnel VPN

Nuestro objetivo es conectar las redes internas de varias sedes de tal forma que podamos mantener una infraestructura única para nuestra empresa, de forma segura, a través de Internet sin necesidad de tener que recurrir a enlaces dedicados. Para ello debemos configurar un servidor VPN de forma similar al anterior punto haciendo tan sólo dos pequeños cambios: habilitar la opción *Permitir túneles Zentyal a Zentyal* para intercambiar rutas entre servidores Zentyal e introducir una *Contraseña de túneles de Zentyal a Zentyal* para establecer la conexión en un entorno más seguro entre las dos oficinas. Como en el caso anterior tendremos que anunciar las redes LAN en *Redes anunciadas*.

Otra diferencia importante viene determinada por el intercambio de rutas. En el escenario *roadwarrior*, descrito más arriba, el servidor envía las rutas al cliente. En el escenario *de servidor a servidor* las rutas se intercambian en ambos sentidos y se propagan al resto de clientes usando el protocolo RIP³⁰. Por éso en los servidores que actúan como clientes VPN del nodo central también es necesario añadir las *Redes Anunciadas* que serán propagadas a los demás nodos.



Figura 2.66: Zentyal como cliente de VPN

Para configurar Zentyal como un cliente VPN, podemos hacerlo a través de *VPN → Clientes*. Tendremos que darle un *nombre* al cliente y activar el *servicio*. Se puede establecer la configuración del cliente manualmente o automáticamente usando el

³⁰ <http://www.ietf.org/rfc/rfc1058>

CAPÍTULO 2

ZENTYAL COMO INFRAESTRUCTURA

bundle generado por el servidor VPN. Si no se usa el *bundle* se tendrá que dar la *dirección IP* y el par *protocolo-puerto* donde estará escuchando el servidor. También será necesaria la *contraseña del túnel* y los *certificados* usados por el cliente. Estos certificados deberán haber sido creados por la misma **autoridad de certificación** que use el servidor.

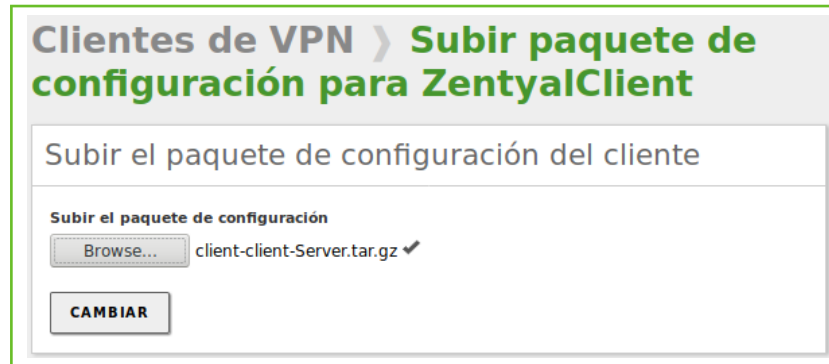


Figura 2.67: Configuración automática del cliente usando el paquete VPN

Cuando se guarden los cambios podremos ver en el *Dashboard*, un nuevo demonio OpenVPN™ ejecutándose como cliente con la conexión objetivo dirigida a la máquina Zentyal que actúa como servidor.

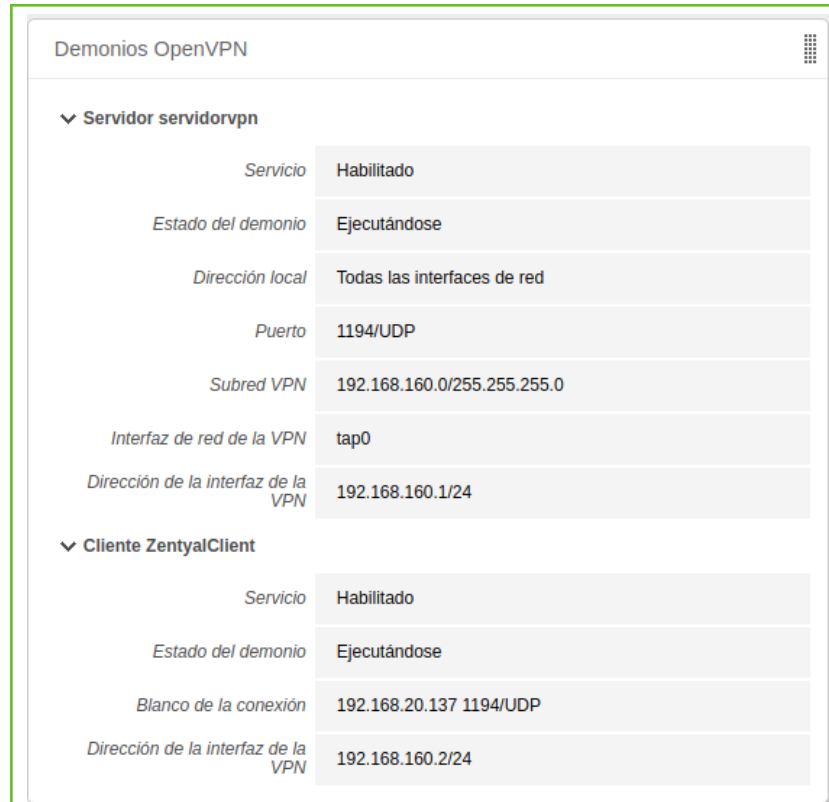


Figura 2.68: Dashboard de un servidor Zentyal configurado como cliente VPN

La propagación de rutas puede tomar unos pocos minutos.

2.7.4 CONFIGURACIÓN DEL CLIENTE OPENVPN

Para configurar un cliente VPN sobre Windows nuestro administrador de sistemas nos deberá facilitar el *bundle* para nuestro cliente.

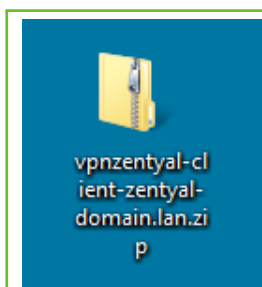


Figura 2.69: El administrador de sistemas nos facilitará el bundle para nuestro cliente

Debemos descomprimirlo (botón derecho sobre el archivo y seleccionando *Extraer aquí*). Encontraremos todos los ficheros relativos a la instalación de VPN y los certificados asociados.

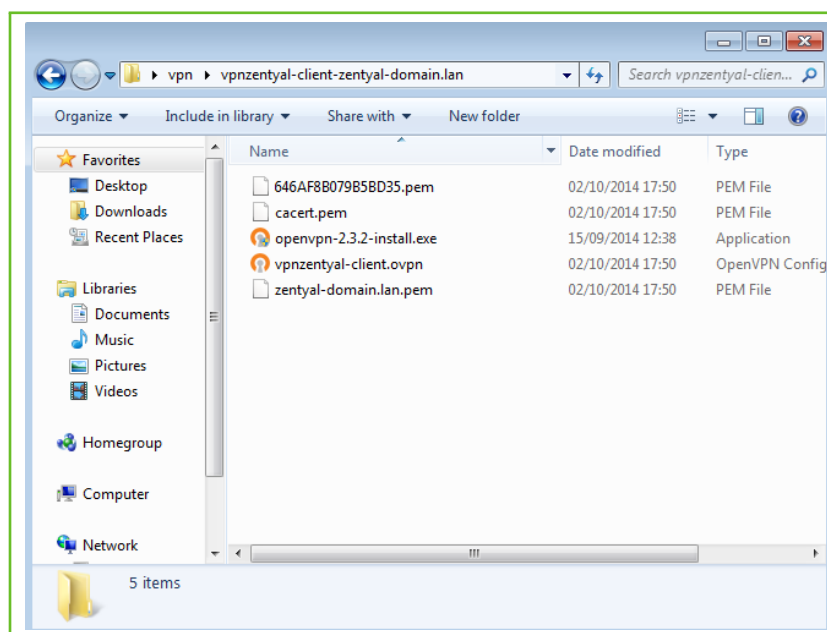


Figura 2.70: Archivos extraídos del bundle

Con el botón derecho tendremos que 'Ejecutar como Administrador' el instalador del cliente openVPN que procederá a crear la interfaz virtual e instalar los drivers

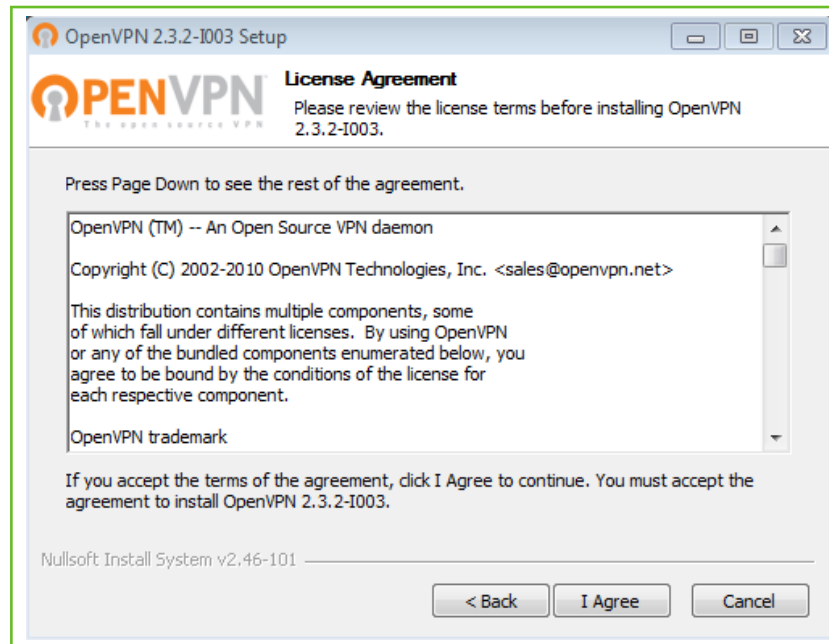


Figura 2.71: Aceptamos la licencia de OpenVPN

Se recomienda instalar todos los módulos.

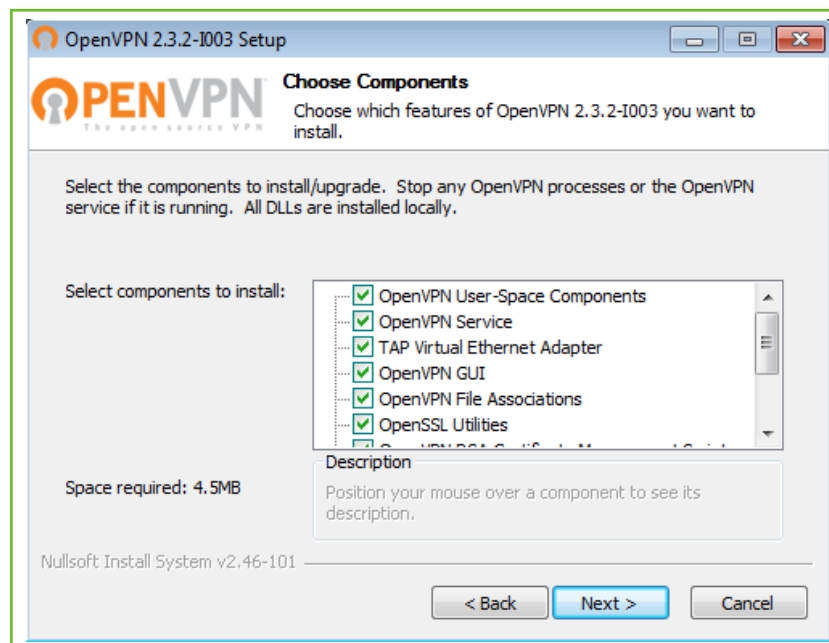


Figura 2.72: Listado de módulos a instalar

El software del adaptador de red no está certificado para Windows. Aun así es completamente seguro continuar.

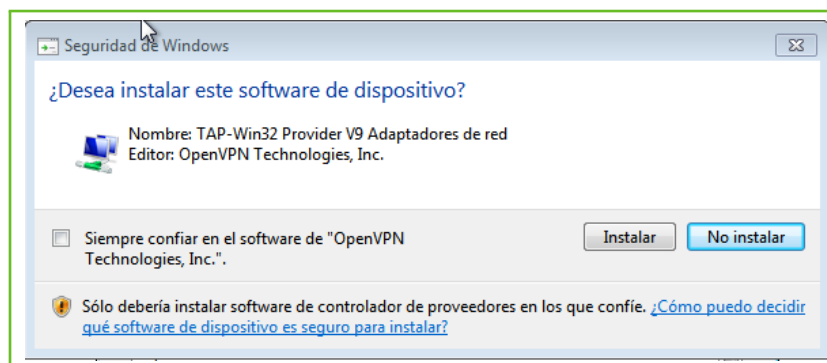


Figura 2.73: Pese a la advertencia se debe de continuar

TRUCO: Tendremos que copiar todos los ficheros que vienen en el *bundle*, (excepto el instalador de *OpenVpn* si lo hemos incluido), a la carpeta *C:\Archivos de Programa (x86)\OpenVpn\config* para que el *servicio* los localice automáticamente.

Una vez instalado veremos un acceso directo en nuestro escritorio que nos permitirá conectarnos a la red VPN haciendo doble clic.

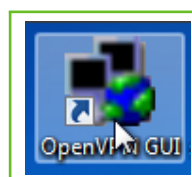


Figura 2.74: Acceso directo para conectar con la VPN

2.7.5 EJEMPLOS PRÁCTICOS

□ EJEMPLO PRÁCTICO A

Ventas García S.L. ha decidido dotar a sus dos comerciales de portátiles corporativos y pretende aprovechar la nueva infraestructura de red para dar acceso a estos dispositivos portátiles a la intranet. Se propone proporcionar acceso a los comerciales a través del módulo *OpenVPN*.

1. **ACCIÓN** Acudir al menú lateral *Gestión de software* → *Componentes de Zentyal*.
EFECTO: Zentyal presenta un listado con todos los módulos instalables.
2. **ACCIÓN** Seleccionar el módulo *VPN* y pulsar el botón *Instalar*.
EFECTO: Se muestra una ventana emergente con información del módulo, tras confirmar se procede a la instalación del módulo con sus dependencias.
3. **ACCIÓN** Acceder a Zentyal, entrar en *Estado de los Módulos* y activar los módulos *Mail* y *Web Mail*, para ello marca su casilla en la columna *Estado*. Nos informa de los cambios que va a realizar en el sistema. Permitir la operación pulsando el botón *Aceptar*.
EFECTO: Se ha activado el botón *Guardar cambios*.

CAPÍTULO 2

ZENTYAL COMO INFRAESTRUCTURA

- 4. ACCIÓN** Seleccionar en el menú lateral *VPN* → *Servidores*. Click en el botón *Añadir nuevo/a* del panel *Lista de servidores*. Introducir el nombre del servidor y confirmar con el botón *Añadir*.

EFEECTO: Se muestra la nueva conexión VPN.
- 5. ACCIÓN** Seleccionar el botón *Configuración* de la nueva conexión VPN. Habilitar la casilla de verificación *Permitir conexiones cliente-cliente* y *Redirigir puerta de enlace*. Click en el botón *Cambiar*.

EFEECTO: Se establece la configuración de la VPN para ser aplicada al guardar cambios.
- 6. ACCIÓN** Ve a *VPN* → *Servidores*. Pulsa sobre el botón *configurar* de la columna *Redes anunciadas*.

EFEECTO: Se muestra las redes que serán compartidas.
- 7. ACCIÓN** Configura las redes que quieras compartir con los comerciales.

EFEECTO: Las redes son listadas.
- 8. ACCIÓN** Acceder a *VPN* → *Servidores*. Marcar la casilla *Habilitado*.

EFEECTO: El cliente VPN está listo para ser iniciado.
- 9. ACCIÓN** Seleccionar el botón de *Guardar los cambios* de la parte superior.

EFEECTO: Zentyal ya está configurado como servidor VPN.
- 10. ACCIÓN** Accede al menú *Autoridad de Certificación* → *General*. Especifica el FQDN del portátil del comercial en *Nombre común* y pulsa sobre *Expedir*.

EFEECTO: El certificado es expedido.
- 11. ACCIÓN** Realiza la misma acción para el otro portátil.

EFEECTO: Ambos certificados son listados.
- 12. ACCIÓN** Accede al menú *VPN* → *Servidores*. Pulsa sobre el botón *Descargar paquete de configuración de cliente* del servidor. Seleccionar en *Tipo de cliente* *Windows* y el certificado generado para el primer comercial en *Certificado del cliente*, habilitar la casilla de verificación *Añadir instalador de OpenVPN al paquete de configuración del cliente* y establecer la IP pública del servidor VPN en *Dirección del servidor*. Click en el botón *Descargar*.

EFEECTO: El paquete de configuración para la configuración VPN del cliente es descargado.
- 13. ACCIÓN** Repetir para la misma acción para el otro portátil.

EFEECTO: Se descargan los archivos para la configuración de la VPN para el portátil.

EJEMPLO PRÁCTICO B

Tras abrir la nueva delegación en Madrid, la empresa quiere comunicar las nuevas instalaciones con la central ubicada en Zaragoza de forma segura. Se propone unir ambas instalaciones usando el módulo *OpenVPN* en ambos servidores.

- 1. ACCIÓN** En el servidor de Zaragoza, acceder a la interfaz de Zentyal e ir al menú *Autoridad de Certificación* → *General*. Establece como FQDN el servidor de Madrid en *Nombre común* y pulsa sobre *Expedir*.

EFEECTO: El certificado es generado.
- 2. ACCIÓN** En ambos servidores, acudir al menú lateral *Gestión de software* → *Componentes de Zentyal*.

- EFECTO:** Zentyal presenta un listado con todos los módulos instalables.
3. **ACCIÓN** Seleccionar el módulo *VPN* y pulsar el botón *Instalar*.
EFECTO: Se muestra una ventana emergente con información del módulo, tras confirmar se procede a la instalación del módulo con sus dependencias.
 4. **ACCIÓN** En ambos servidores, seleccionar en el menú lateral *Estado de los módulos* y habilitar el módulo *VPN*.
EFECTO: El botón de *Guardar cambios* del menú superior es habilitado.
 5. **ACCIÓN** En el servidor de Zaragoza, seleccionar en el menú lateral *VPN* → *Servidores*.
EFECTO: Las conexiones VPN son listadas.
 6. **ACCIÓN** Pulsar en el botón *Añadir nuevo* e introducir el nombre del servidor en *Nombre*. Pulsar sobre el botón *Añadir*.
EFECTO: La nueva conexión VPN es listada.
 7. **ACCIÓN** Seleccionar el botón *Configuración* de la nueva conexión VPN. Habilitar la casilla de verificación *Permitir túneles de Zentyal a Zentyal* y establecer una contraseña en el campo *Contraseña de túneles de Zentyal a Zentyal*. Pulsar en el botón *Cambiar*.
EFECTO: El archivo de configuración es modificado y está listado para ser aplicado.
 8. **ACCIÓN** Ve a *VPN* → *Servidores*. Pulsa sobre el botón *configurar* de la columna *Redes anunciadas*.
EFECTO: Se muestra las redes que serán compartidas.
 9. **ACCIÓN** Configura las redes que quieras compartir con el otro servidor Zentyal.
EFECTO: Las redes son listadas.
 10. **ACCIÓN** Acceder a *VPN* → *Servidores*. Marcar la casilla *Habilitado*.
EFECTO: El cliente VPN está listo para ser iniciado.
 11. **ACCIÓN** Seleccionar el botón de *Guardar los cambios* de la parte superior.
EFECTO: Zentyal ya está configurado como servidor VPN.
 12. **ACCIÓN** Acceder a *VPN* → *Servidores*. Seleccionar el botón *Descargar paquete de configuración de cliente*. Seleccionar el certificado generado para el servidor de Madrid en *Certificado del cliente*. Añadir la IP pública del servidor de Zaragoza en *dirección del servidor*. Click en el botón *Descargar*.
EFECTO: El archivo de configuración para el servidor VPN de Madrid es descargado.
 13. **ACCIÓN** En el servidor de Madrid, acceder al menú lateral *VPN* → *Clientes* e introducir el nombre de la conexión VPN en el campo *Nombre*. Click en el botón *Añadir*
EFECTO: Se lista la nueva conexión VPN.
 14. **ACCIÓN** Pulsar sobre *Subir paquete de configuración del cliente*. Seleccionar el paquete de configuración VPN descargado previamente. Click en el botón *Cambiar*.
EFECTO: La configuración VPN está lista para ser aplicada.
 15. **ACCIÓN** Ve a *VPN* → *Clientes*. Pulsa sobre el botón *configurar* de la columna *Redes anunciadas*.
EFECTO: Se muestra las redes que serán compartidas.

16. **ACCIÓN** Configura las redes que quieras compartir con el otro servidor Zentyal.
EFECTO: Las redes son listadas.
17. **ACCIÓN** Acceder a VPN → *Cientes*. Marcar la casilla *Habilitado*.
EFECTO: El cliente VPN está listo para ser iniciado.
18. **ACCIÓN** Click en el botón *Guardar cambios* del menú superior.
EFECTO: El módulo VPN es configurado y habilitado.

2.7.6 EJERCICIOS PROPUESTOS

EJERCICIO A

Configura una VPN para que sólo sea válida con un certificado concreto. Compruébalo con dos clientes, uno con el certificado correcto y otro con uno incorrecto.

2.8

VPN CON IPSEC Y L2TP/IPSEC

2.8.1 INTRODUCCIÓN A IPSEC Y L2TP/IPSEC

El protocolo **IPsec**³¹ (*Internet Protocol security*) es un conjunto de protocolos para garantizar la seguridad de las comunicaciones de red usando el protocolo TCP/IP. Proporciona tanto autenticación como encriptación de la sesión. A diferencia de otras soluciones como SSL o TLS, IPsec no funciona en la capa de aplicación sino en la capa de red. Esto permite dotar de seguridad a cualquier comunicación sin tener que modificar la aplicación usada.

Al igual que OpenVPN o PPTP, IPsec se utiliza para desplegar redes privadas virtuales (VPN). Puede operar en varios modos, de host a host, de red a host o de red a red, siendo este último el más habitual: tenemos subredes que queremos interconectar de manera segura a través de una red no fiable, como puede ser Internet.

IPsec es un anexo opcional del protocolo IPv4 pero forma parte de IPv6. La principal ventaja de IPsec frente a otros protocolos de VPN incluidos en Zentyal como OpenVPN o PPTP es que es un estándar definido por el Internet Engineering Task Force (IETF) que muchos fabricantes han implementado en sus dispositivos por lo que es la opción ideal para conectar Zentyal con dispositivos UTM de otros fabricantes (Cisco, Fortinet, CheckPoint, etc.).

L2TP opera en la capa 2 del modelo TCP/IP³², de esta forma permite que los clientes remotos operen en las redes locales como cualquier otra máquina unida a la LAN, en lugar de comportarse como una conexión punto a punto. L2TP lleva a cabo las tareas de tunelización y autenticación de usuarios, en la implementación de Zentyal, L2TP se apoya en IPsec para cifrar el tráfico.

Zentyal integra Libreswan³³ como solución IPsec. Este servicio utiliza los puertos 500 y 4500 UDP además del protocolo ESP.

2.8.2 CONFIGURACIÓN DE UN TÚNEL IPSEC CON ZENTYAL

Antes de proceder con la configuración del módulo, mencionar que únicamente está disponible en versiones comerciales.

Para configurar IPsec en Zentyal iremos a VPN → IPsec. Aquí podremos definir todos los túneles o conexiones IPsec que deseemos. Para cada una, la podemos activar o desactivar, y añadir un comentario aclarativo.

³¹ <http://es.wikipedia.org/wiki/IPsec>

³² <http://www.ietf.org/rfc/rfc2661.txt>

³³ <http://libreswan.org/>