Zentyal para Administradores de Redes

VERSIÓN 7.0

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

zentyal training

Zentyal para Administradores de Redes

VERSIÓN 7.0

PRODUCIDO POR

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

Índice

4. **ACCIÓN** Entrar en *Autoridad de Certificación* → *Certificados para los servicios*. Pulsar sobre el botón *Edit* en la columna *Acción* para el módulo *Administración Web de Zentyal*. Especificar el *FQDN* del servidor Zentyal en *Nombre común*, marcar la casilla *Habilitar* y pulsar sobre *Cambiar*.

   EFECTO: Un nuevo certificado con el *Nombre común* será expedido después de guardar los cambios. Se ha habilitado el botón *Guardar cambios* del menú superior.

5. **ACCIÓN** Realizar la acción anterior con el módulo de correo.

   EFECTO: Se generan los certificados para los módulos.

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

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

7. **ACCIÓN** Desde el listado de certificados, descargar el de la CA, un archivo con nombre *CA-key-and-cert.tar.gz* que dentro contiene la clave pública *ca-public-key.pem* y el certificado *ca-cert.pem*. Siguiendo el procedimiento descrito más arriba, importar el fichero del certificado *ca-cert.pem* en las máquinas Windows.

   EFECTO: El nuevo certificado aparecerá en el listado de certificados, y todo certificado emitido por esta CA será aceptado por las estaciones de trabajo de los usuarios con Windows.

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/` .

Servicio de redes privadas virtuales (VPN) con OpenVPN

Introducción a las redes privadas virtuales (VPN)

Las **redes privadas virtuales** [1] tienen como finalidad permitir el acceso a la red corporativa a usuarios remotos a conectados través de Internet y además conectar de manera segura subredes distintas, también a través de Internet.

Nuestros usuarios pueden necesitar acceder a recursos de nuestra red mientras se encuentran fuera de las instalaciones de la empresa, unidos a redes no confiables. 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 Internet, aunque ello puede implicar riesgos para la confidencialidad, disponibilidad e integridad de las comunicaciones. Para evitar esos problemas la conexión no se realiza de forma directa sino a través de redes privadas virtuales.

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 será posible leerlo en el otro extremo del túnel. Además, 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.

[1] **VPN:** http://es.wikipedia.org/wiki/Red_privada_virtual

De la misma manera, 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 [2] para configurar y gestionar las redes privadas virtuales. En esta sección concreta veremos como configurar OpenVPN, el cual posee 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.

Configuración de un servidor OpenVPN con Zentyal

Se puede configurar Zentyal para dar soporte a clientes remotos (conocidos como *Road Warriors*). Esto es, un servidor Zentyal trabajando como puerta de enlace y como servidor VPN, que tiene varias redes de área local (LAN) detrás, permitiendo a clientes externos (los *road warriors*) conectarse a dichas redes locales vía servicio VPN.

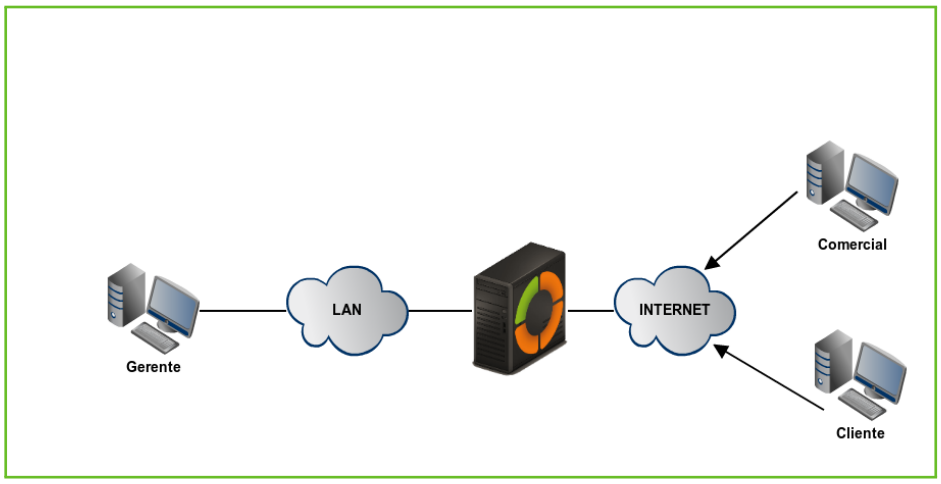

Figura 2.56: Zentyal y clientes remotos de VPN

Nuestro objetivo es conectar al servidor de datos con los otros dos 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 expedirá este certificado automáticamente cuando cree un nuevo servidor VPN. En este escenario, Zentyal actúa como una **Autoridad de Certificación**.

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

Figura 2.57: Certificados expedidos en el servidor

Una vez tengamos los certificados, deberíamos poner a punto el servidor VPN en Zentyal mediante *Crear un nuevo servidor*. El único parámetro que necesitamos introducir para crear un servidor es el nombre. Zentyal hace que la tarea de configurar un servidor VPN sea sencilla, ya que establece valores de forma automática.

Figura 2.58: Nuevo servidor VPN creado

Los siguientes parámetros de configuración son añadidos automáticamente y 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 y eficiente pues hay que transmitir menos información de control por lo tanto hay más espacio para datos. El segundo, TCP, es más resistente a conexiones inestables o a proveedores de Internet que cortan conexiones de larga duración.

Como vemos, el servidor VPN estará escuchando en todas las interfaces externas. Por tanto, debemos poner 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 los casos más habituales.

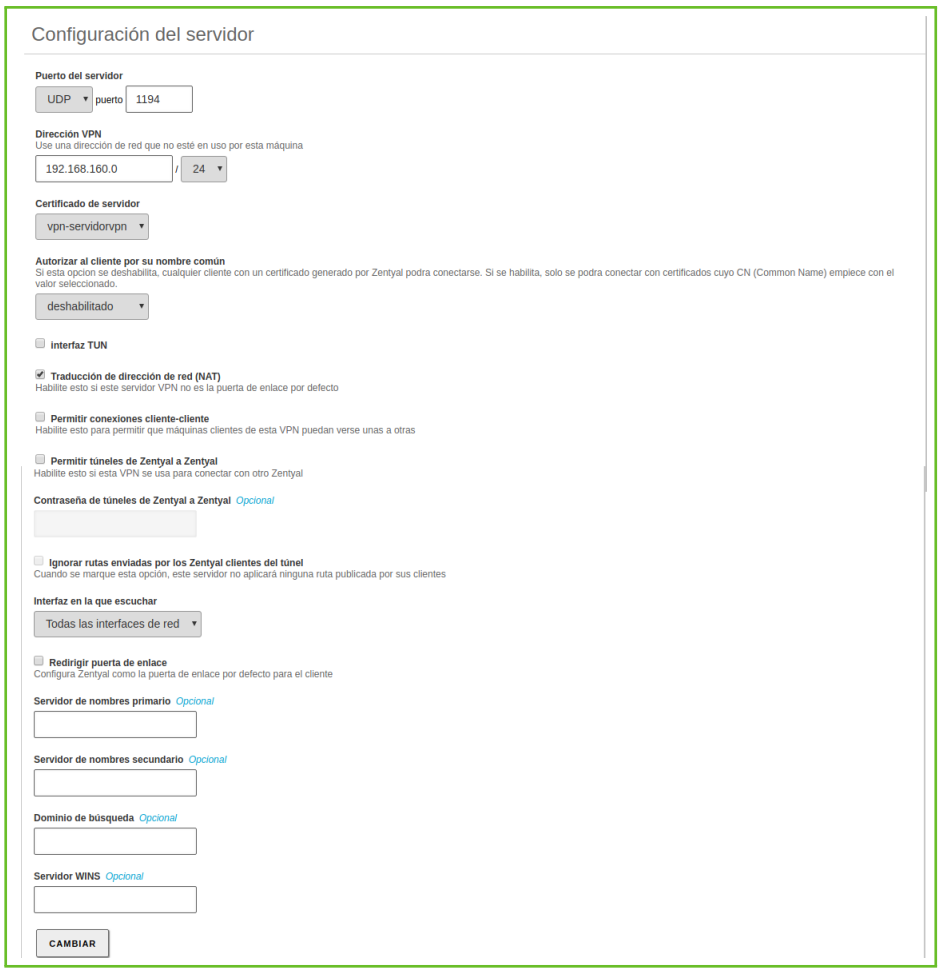

Figura 2.59: Configuración de servidor VPN

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 en cuenta que esta red no se solape con ninguna otra y que a efectos del cortafuegos, es una red interna. Por defecto *192.168.160.1/24*, los clientes irán tomando las direcciones *.2*,*.3*, etc.
- ***CERTIFICADO DE SERVIDOR:*** Certificado que mostrará el servidor a sus clientes. La CA de Zentyal expide un certificado por defecto para el servidor, con el nombre vpn-<nuestronombredevpn>. 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*, más semejante a un *bridge* de capa 2, podemos usar una interfaz de tipo *TUN* más semejante a un nodo de IP capa 3.
- ***TRADUCCIÓN DE DIRECCIÓN DE RED (NAT):*** Es recomendable tener esta traducción 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), es indiferente.

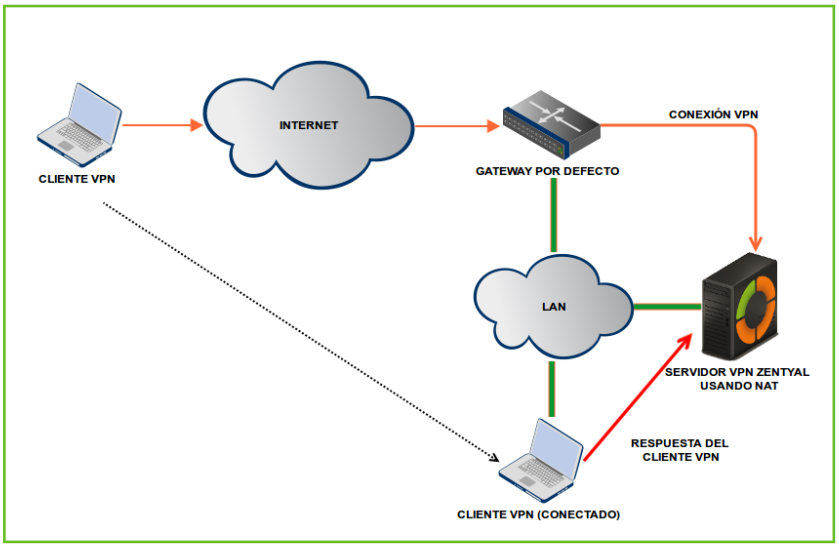

Figura 2.60: Servidor VPN usando NAT para convertirse en la puerta de enlace por defecto

☒ ***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, 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 el *Dashboard* que el servidor VPN está funcionando.

Figura 2.61: Widget del servidor VPN

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

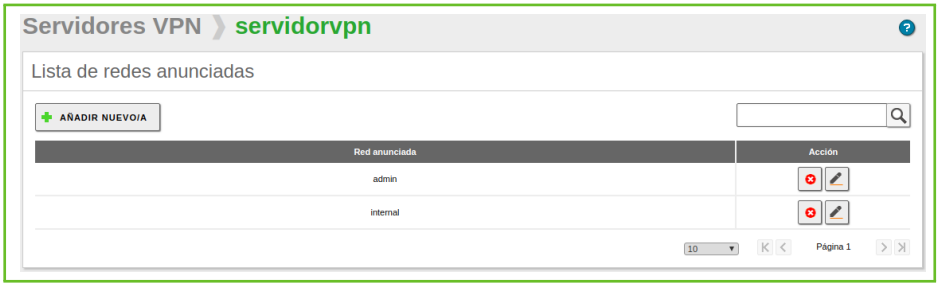

Figura 2.62: Redes anunciadas para nuestro servidor VPN

Una vez hecho esto, es momento de configurar los clientes. La forma más sencilla de configurar un cliente VPN es utilizando los *bundles* de Zentyal. Los *bundles* son paquetes de instalación que incluyen el archivo de configuración de VPN específico para cada usuario y, opcionalmente, un programa de instalación. Estos están disponibles en la tabla que aparece en *VPN* → *Servidores*, pulsando 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 más abajo, tenemos un servidor VPN principal y hasta dos secundarios. Dependiendo de la *Estrategia de conexión* definida, se intentará establecer la conexión en orden específica o en orden aleatorio.

Además, si el sistema seleccionado es Windows, se puede incluir también un instalador de OpenVPN™. Los *bundles* de configuración los descargará el administrador de Zentyal para distribuirlos a los clientes de la manera que crea más oportuna.

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 [3] 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*.

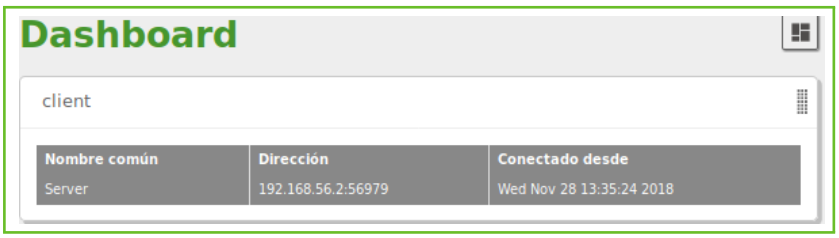

Figura 2.64: Widget con clientes conectados

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 Zentyal en ambas como puertas de enlace. Una actuará como cliente VPN y otra como servidor. La siguiente imagen ilustra esta situación:

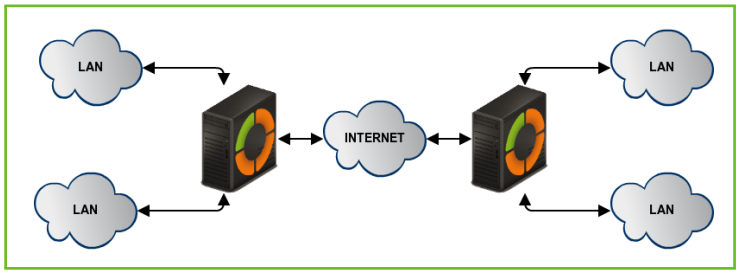

Figura 2.65: Interconexión de sedes con Zentyal mediante túnel VPN

Nuestro objetivo es conectar varias sedes, sus servidores Zentyal, así como sus redes internas, de tal forma que podemos crear una infraestructura única para nuestra empresa de forma segura a través de Internet. Para ello, debemos configurar un servidor VPN de forma similar al anterior punto.

Sin embargo, se necesita hacer dos pequeños cambios. En primer lugar, debemos habilitar la opción *Permitir túneles Zentyal a Zentyal* para intercambiar rutas entre servidores Zentyal y luego, introducir una *Contraseña de túneles de Zentyal a Zentyal* para establecer la conexión en un entorno más seguro entre las dos oficinas. Hay que tener en cuenta que tendremos que anunciar las redes *LAN* en *Redes anunciadas*.

[3] Para más información sobre compartición de ficheros, ir a la sección *Servicio de Dominio y Directorio*.

Otra diferencia importante es el intercambio de rutas. En el escenario de *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 a otros clientes usando el protocolo RIP [4]. Por lo que en los servidores que actúan como clientes VPN del nodo central también es posible 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 *bundle* dado por el servidor VPN. Si no se usa el *bundle*, se tendrá que dar la *dirección IP* y el par *protocolo-puerto* donde estará aceptando peticiones 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.

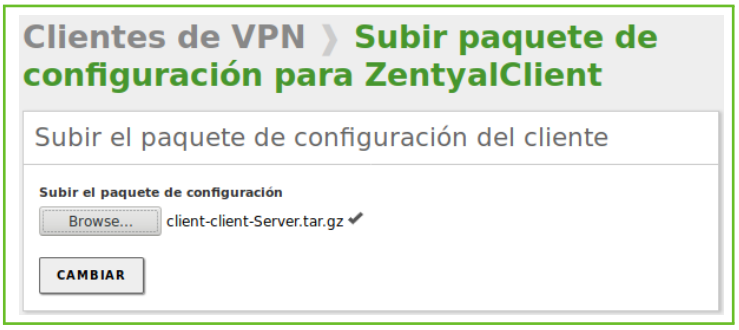

Figura 2.67: Configuración automática del cliente usando el paquete VPN

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

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

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

ADVERTENCIA: La propagación de rutas puede tomar unos pocos minutos.

Configuración del cliente OpenVPN

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

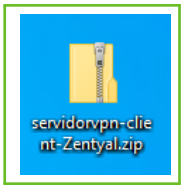

Figura 2.69: Bundle de la VPN

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.

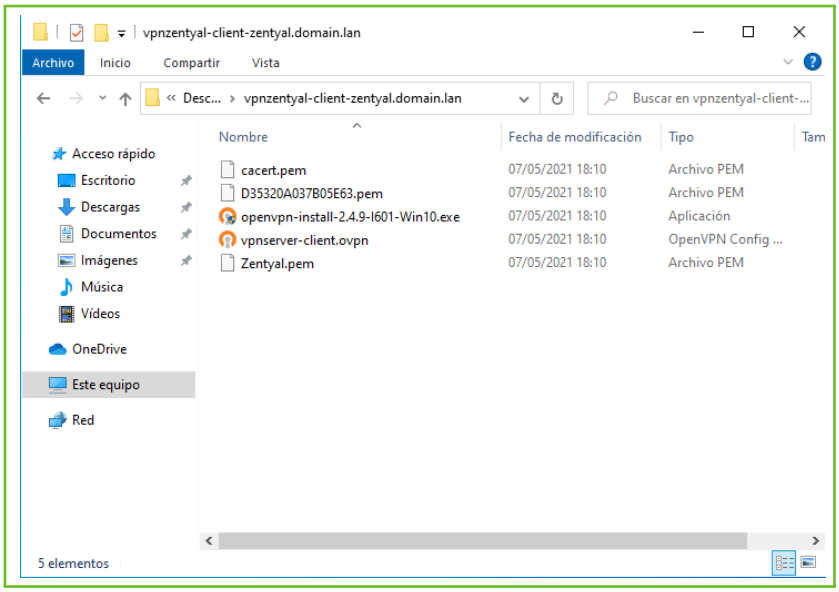

Figura 2.70: Archivos extraídos del bundle

Con el botón derecho elegimos 'Ejecutar como Administrador', ya que OpenVPN necesita crear la interfaz virtual e instalar los drivers

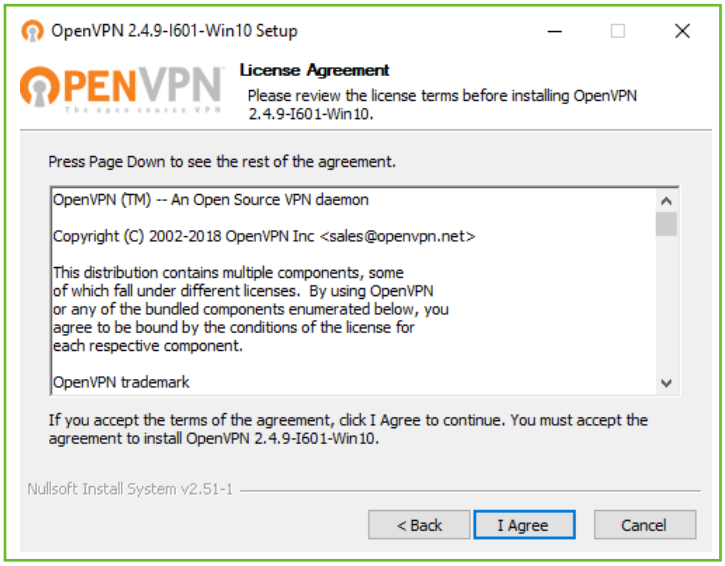

Figura 2.71: Aceptamos la licencia de OpenVPN

Dejamos los componentes por defecto y pulsamos sobre *Next*:

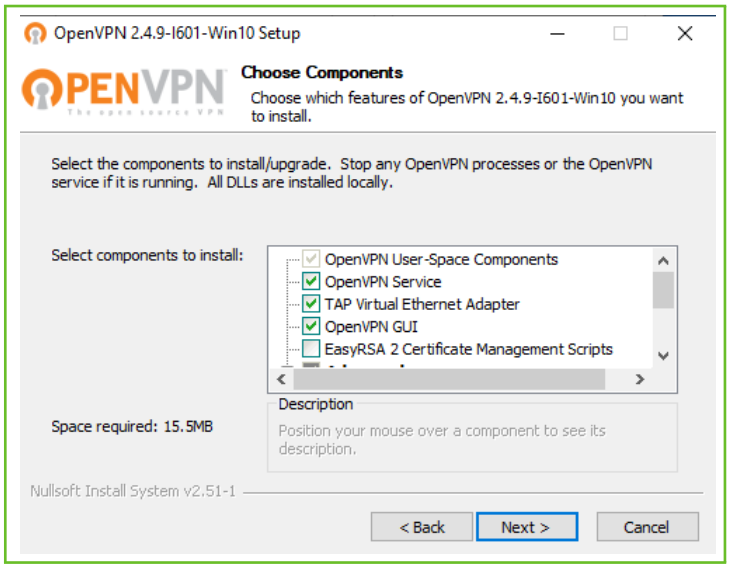

Figura 2.72: Listado de módulos a instalar

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 *daemon* los localice automáticamente.

Una vez instalado, tenemos un acceso directo en nuestro escritorio que nos permite conectar a la red VPN haciendo doble clic.

Figura 2.73: Acceso directo para conectar con la VPN

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 el módulo *VPN*, para ello marca su casilla en la columna *Estado*. Se proporcionar información

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*.

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

   EFECTO: 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*. Hacer click en el botón *Cambiar*.

   EFECTO: Se establece la configuración de la VPN para ser aplicada al guardar cambios.

6. **ACCIÓN** Acudir a *VPN –> Servidores*. Pulsar sobre el botón *Configurar* de la columna *Redes anunciadas*.

   EFECTO: Se muestran las redes que serán compartidas.

7. **ACCIÓN** Configurar las redes que se quieren compartir con los comerciales.

   EFECTO: Las redes son listadas.

8. **ACCIÓN** Acceder a *VPN –> Servidores*. Marcar la casilla *Habilitado*.

   EFECTO: El cliente VPN está listo para ser iniciado.

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

   EFECTO: Zentyal ya está configurado como servidor VPN.

10. **ACCIÓN** Acceder al menú *Autoridad de Certificación* → *General*. Especificar el *FQDN* del portátil del comercial en *Nombre común* y pulsar sobre *Expedir*.

    EFECTO: El certificado es expedido.

11. **ACCIÓN** Realizar la misma acción para el otro portátil.

    EFECTO: Ambos certificados son listados.

12. **ACCIÓN** Acceder al menú *VPN* → *Servidores*. Pulsar 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*. Hacer click en el botón *Descargar*.

    EFECTO: El paquete de configuración para la configuración VPN del cliente es descargado.

13. **ACCIÓN** Repetir para la misma acción para el otro portátil.

    EFECTO: 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*. Establecer como *FQDN* el servidor de Madrid en *Nombre común* y pulsa sobre *Expedir*.

EFECTO: 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** Acudir a *VPN –> Servidores*. Pulsar sobre el botón *Configurar* de la columna *Redes anunciadas*.

   EFECTO: Se muestran las redes que serán compartidas.

9. **ACCIÓN** Configurar las redes que se quieren 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 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*. Hacer 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. Hacer click en el botón *Cambiar*.

EFECTO: La configuración VPN está lista para ser aplicada.

15. **ACCIÓN** Acceder a *VPN –> Clientes*. Pulsar sobre el botón *Configurar* de la columna *Redes anunciadas*.

    EFECTO: Se muestra las redes que serán compartidas.

16. **ACCIÓN** Configurar las redes que se quieren compartir con el otro servidor Zentyal.

    EFECTO: Las redes son listadas.

17. **ACCIÓN** Acceder a *VPN –> Clientes*. Marcar la casilla *Habilitado*.

    EFECTO: El cliente VPN está listo para ser iniciado.

18. **ACCIÓN** Hacer click en el botón *Guardar cambios* del menú superior.

    EFECTO: El módulo *VPN* es configurado y habilitado.

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.

VPN con IPSEC y L2TP/IPSEC

Introducción a IPsec y L2TP/IPSEC

El protocolo **IPsec** [1] (*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 stándard 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/IP [2] , 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. En la implementación de Zentyal, L2TP lleva a cabo las tareas de tunelización y autenticación de usuarios, pero L2TP se apoya en IPsec para cifrar el tráfico.

Zentyal integra Libreswan [3] como solución IPsec y L2TP/IPsec. Este servicio utiliza los puertos 500, 1701 y 4500 UDP además del protocolo ESP.

[1] **IPSEC:** http://es.wikipedia.org/wiki/IPsec
[2] **RFC2661:** http://www.ietf.org/rfc/rfc2661.txt
[3] **Libreswan:** http://libreswan.org/