Guía 10 – Configuración de una VPN

Contenido de la guía

Objetivo general de la guía.

- Crear una red VPN en el escenario de la EMPRESAY, que presente servicios a clientes externos.

Objetivos específicos.

- Configurar una VPN

Nomenclatura de la guía:

En esta guía se ha utilizado el siguiente formato:

- Fuente courrier en negrita para los comandos que deben digitarse, por ejemplo:
  `root@front-end:~# ps aux |grep sshd`
- Texto con resaltado en amarillo, para la información que debe visualizar cuando realice algún procedimiento o comando. Puede contener color rojo dentro del fondo amarillo.
  ```
  root@front-end:~# mcedit /etc/resolv.conf
  search empresay.com.sv
  nameserver   192.168.60.2
  ```
- Las notas o consideraciones se destacan con: **Nota:**

I. Indicaciones sobre la guía

1.1 Descripción del escenario global.

Usted y su equipo de trabajo han sido contratados para configurar una red DMZ que contiene los servicios de un DNS externo y un servidor HTTP a usuarios externos y anónimos de la EMPRESAY, manteniendo la seguridad de los servicios internos de la empresa. Es decir, mantener la configuración del Firewall que se ha utilizado en los escenarios anteriores.

- El servidor DNS deberá resolver solo las peticiones externas (desde Internet), acordes a los ítems 6 y 7 del cuadro 3, el servidor DNS externo se convertirá en el único reenviador del servidor DNS interno.
- El servidor HTTP deberá tener una página en HTML o PHP que muestre un mensaje diferente del HTTP del servidor02
- Los usuarios públicos pueden acceder al sitio web tanto desde equipos de escritorio como dispositivos móviles (usar Android)

Para realizar el desafío se debe:

- Instalar el servidor BIND 9.X en uno de los equipos Core Plus, (está en la libertad de instalar BIND en otra distribución de Linux, si los recursos de hardware le permiten hacer esto).
- Utilizar MaSSHandra para la administración remota de los servidores.
- Analizar la configuración de la sección 1.2 que más se les facilite para desarrollar el escenario.
- Puede utilizar cualquier sistema operativo para ejecutar la conexión de los clientes públicos (pub01 y pub02)
- Comenzar a trabajar con el uso de una página en PHP que consulte cualquier tabla en la base de datos der servidor02, esto será requerido en la evaluación práctica grupal

En la siguiente figura se ilustra el escenario de red para la guía

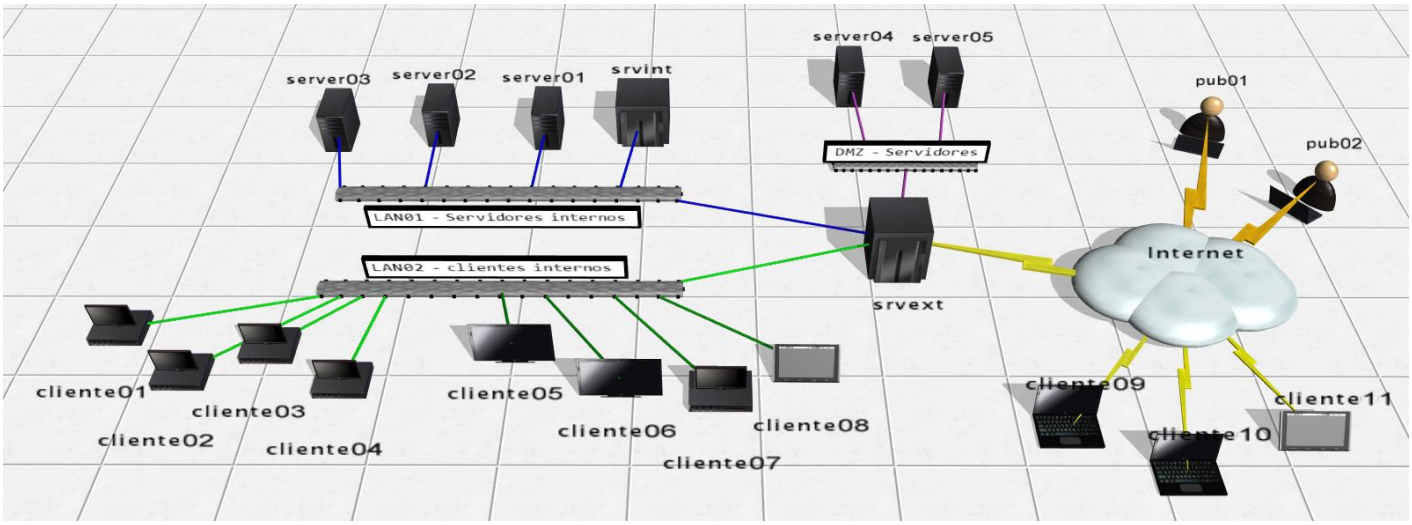


Figura 1 – Diagrama del escenario de la nube privada y pública de la EMPRESAY.

Servicios y clientes en los equipos a utilizar			
ID	**Nombre Equipo**	**Servicios / Software**	**S.O.**
1	srvext	DHCP, Router, Firewall, NAT, VPN	**Zentyal 4.X**
2	servint	DNS, AD, FS	**Zentyal 4.X**
3	servidor01	Servidor SSH, Servidor Web	CorePlus 7.X
4	servidor02	Servidor SSH, Servidor VNC,	CorePlus 7.X
5	servidor03	Servidor SSH, Servidos SMB, Servidor MySQL	CorePlus 7.X
6	cliente01	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
7	cliente02	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
8	cliente03	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
9	cliente04	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
10	cliente05	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Windows 7, 8, 10
11	cliente06	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Windows 7, 8, 10
12	cliente07	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Ubuntu 14.04
13	cliente08	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Android x86
14	cliente09	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Windows 7, 10
15	cliente10	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Ubuntu 14.04
14	cliente11	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Android x86

Cuadro 1 – Descripción de los equipos del escenario de la EMPRESAY

La red IPv4 de la EMPRESAY para cada equipo se detalla en el siguiente cuadro:

Direcciones MAC e IPv4 para los equipos de la EMPRESAY				
ID	**Equipo**	**Dirección MAC**	**Tipo IPv4**	**IPv4**
1	serext	02:AA:E0:Y:X:01	Dinámica	La del ISP
		02:AA:E1:Y:X:02	Estática	192.168.**60+Y**.1
		02:AA:E2:Y:X:03	Estática	192.168.**50**+Y.1
2	srvint	02:BB:00:Y:X:00	Estática	192.168.**60**+Y.2
3	servidor01	02:BB:00:Y:X:01	Reservada	192.168. **60+Y**.11
4	servidor02	02:BB:00:Y:X:02	Reservada	192.168. **60+Y**.12
5	servidor03	02:BB:00:Y:X:03	Reservada	192.168. **60+Y**.13
6	cliente01	02:CC:00:Y:X:01	Reservada	192.168.**50**+Y.11
7	cliente02	02:CC:00:Y:X:02	Dinámica	192.168.**50**+Y.12
8	cliente03	02:CC:00:Y:X:03	Dinámica	192.168.**50**+Y.13
9	cliente04	02:CC:00:Y:X:04	Dinámica	192.168.**50**+Y.14
10	cliente05	02:CC:00:Y:X:05	Dinámica	192.168.**50**+Y.15
11	cliente06	02:CC:00:Y:X:06	Dinámica	192.168.**50**+Y.16
12	cliente07	02:CC:00:Y:X:06	Dinámica	192.168.**50**+Y.17

Cuadro 2 – Datos generales de red para el escenario de la EMPRESAY según equipo de trabajo

Nota: Para garantizar que no exista una dirección MAC, una IPv4, un host y un dominio duplicado en la red del laboratorio, se utilizará la siguiente nomenclatura:

- Y = representa el número del grupo de trabajo, y se utilizan dos dígitos
- X = representa el número del estudiante, se utilizan dos dígitos

Ejemplos:	**Grupo 7 y estudiante 1**	**Grupo 05 y estudiante 2**	**Grupo 11 y estudiante 3**
02:BB:00:**Y**:**X**:01	02:BB:00:**07**:**01**:01	02:BB:00:**05**:**02**:01	02:BB:00:**11**:**03**:01
empresa**Y**.com.sv	empresa**07**.com.sv	empresa**05**.com.sv	empresa**11**.com.sv
192.168.**50+Y**.3	192.168.5**7**.3	192.168.5**5**.3	192.168.**61**.3

Nota: Imprima o elabore en una hoja con los datos de grupo y número de alumno, de forma que no halla consultas redundantes, pérdida de tiempo o errores ocasionados por la mala configuración de la red en el laboratorio.

Servicios y clientes en los equipos a utilizar				
ID	**Equipo / Nombre de host**	**Dirección IPv4**	**Alias**	**FQDN**
1	srvext	192.168.50+Y.1 192.168.60+Y.1 192.168.70+Y.1	router01	srvext.empresay.com.sv
2	servint	192.168.**60+Y**.2	fs01	servint.empresay.com.sv
3	servidor01	192.168. **60+Y**.11	www	servidor01.empresay.com.sv
4	servidor02	192.168. **60+Y**.12	bd01	servidor02.empresay.com.sv
5	servidor03	192.168. **60+Y**.13	fs02	servidor03.empresay.com.sv
6	servidor04	192.168. **70+Y**.14	---	servidor04.empresay.com.sv
7	servidor05	192.168. **70+Y**.15	www mail smtp	servidor05.empresay.com.sv

Cuadro 3 – Datos de resolución para equipos

1.2 Consideraciones técnicas para el laboratorio.

Recursos requeridos:

- Un equipo o MV con servidor **srvext**.
- Un equipo o MV con servidor **srvint**.
- Tres servidores TinyCore 7.X o superior (con servicio HTTP de preferencia)
- Cuatro clientes TinyCore 7.X o superior con aplicaciones cliente que estarán en la nube (simulando Internet)
- Conexión a Internet.
- Los servicios DHCP y DNS deberán estar bien configurados, proveyendo todos los datos de la red de la empresa EMPRESAY (sustituir Y por el número de grupo)
- El servidor **srvext** deberá tener salida a Internet.
- MaSSHandra para Windows
- WinSCP o FileZilla para Windows.
- Notepad+++ para Windows (opcional)

Consideraciones:

- Si utiliza máquinas virtuales se utilizará VirtualBox versión 5.X (De preferencia), y para cada equipo se utilizarán las direcciones físicas del cuadro 2.
- Escriba en un papel todas las direcciones IPv4 de su red, utilice el valor de Y con el número de grupo asignado, por ejemplo: Y=grupo01 192.168.50+**Y**.1 = 192.168.168.51.1 (ver cuadro 2)
- La máquina virtual del servidor01 se puede clonar las veces que sea necesario para obtener los servidores de la red LAN01, los clientes de la red LAN02 y equipos de la DMZ
- Utilice un fondo de escritorio con el nombre de cada servidor y cliente para identificar mejor cada equipo.
- Verifique que utiliza la dirección MAC para cada grupo y alumno.
- El equipo **srvext** tendrá tres interfaces y Puede configurarse de la siguiente manera:

Configuración 01 para las NIC de srvext con VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	Bridge a la tarjeta Ethernet de la computadora
Adaptador 2	eth1	Bridge a una loopback de MS o Ethernet
Adaptador 3	eth2	Bridge a una loopback de MS o Ethernet
Adaptador 4	eth3	Bridge a una loopback de MS o Ethernet
• Este escenario es útil si, se desean repartir las servidores y clientes virtuales entre dos o más computadoras del laboratorio. • Si es Windows donde está VirtualBox, se debe crear una loopback para micrososoft: Win + R, hdwwiz, seleccionar hardware manual, NIC, Seleccionar Microsft, loopback KM-Test • Si es Linux donde está VirtualBox, se debe crear una loopback tipo tap0 • Solo los Adaptadores con bridge a tarjetas Ethernet pueden comunicarse con otros equipos virtuales que se ejecutan en otra computadora del centro de cómputo. • Siempre se debe configurar la dirección IPv4 de la interfaz eth0 de srvext y el GW por default.		

Configuración 02 para las NIC de srvext con VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	NAT
Adaptador 2	eth1	Bridge a una loopback de Micrososft
Adaptador 3	eth2	Bridge a una loopback de Micrososft
Adaptador 4	eth3	Bridge a una loopback de Micrososft
• Este escenario es útil si hay una configuración de portal cautivo en la red Wifi, o si la comunicación es complicada de realizar • En Windows: se debe crear una loopback: Win + R, hdwwiz, seleccionar hardware manual, NIC, Seleccionar Microsft, loopback KM-Test • En Linux: Se debe crear una loopback tipo tap0 • No es necesario configurar la dirección eth0 del servidor srvext (siempre será dinámica con el valor 10.0.2.15)		

Configuración 03 para las NIC de srvext con VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	Bridge o NAT
Adaptador 2	eth1	Conexión a LAN interna (lan01)
Adaptador 3	eth2	Conexión a LAN interna (lan02)
Adaptador 4	eth3	Conexión a LAN interna (lan03)
• Este escenario es útil si se utiliza una laptop o computadora de escritorio que necesite permisos para instalar dispositivos. • No necesita crear interfaces loopback, por lo que hacer pruebas de comunicación es muy complejo		

Nota: Si se utilizan el escenario 01 o el escenario 02 se debe crear una interfaz loopback con las direcciones para la red LAN01 y LAN02

Por ejemplo:

```
C:\Users\cuchillac>ipconfig
Configuración IP de Windows
Adaptador de LAN inalámbrica Wi-Fi:
   Sufijo DNS específico para la conexión. . : uni.edu.sv
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.3.223
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.10.3.254
Adaptador de Ethernet loopback:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.50.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.60.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.70.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```

1.3 Teoría técnica requerida

Pendiente de finalizar

Para impedir que las personas externas a la compañía puedan obtener información de la red interna, utilice servidores DNS independientes para la resolución de nombres internos y de Internet. Su espacio de nombres DNS interno debe estar alojado en los servidores DNS detrás del servidor de seguridad de su red. Su presencia DNS externa en Internet debe administrarla un servidor DNS en una red perimetral (conocida también como DMZ, zona desmilitarizada o subred apantallada). Para proporcionar la resolución de nombres de Internet en hosts internos, puede hacer que sus servidores DNS internos utilicen un servidor de envío para enviar las consultas externas a su servidor DNS externo. Párrafo tomado de: https://msdn.microsoft.com/es-es/library/cc780338(v=ws.10).aspx

Si el servidor que ejecuta el servicio del Servidor DNS es un equipo de hosts múltiples, limite el servicio del Servidor DNS sólo para escuchar en la dirección IP de interfaz utilizada por sus clientes DNS y servidores internos. Por ejemplo, un servidor que actúa como servidor proxy puede tener dos tarjetas de interfaz de red, una para la intranet y otra para Internet. Si dicho servidor ejecuta también el servicio del Servidor DNS, puede configurar el servicio para que sólo escuche el tráfico DNS en la dirección IP utilizada por la tarjeta de interfaz de red de la intranet

Si el servidor que ejecuta el servicio del Servidor DNS es un controlador de dominio, utilice listas de control de acceso (ACL) de Active Directory para proteger el control de acceso del servicio del Servidor DNS.

Su infraestructura debe disponer de al menos tres DNS, los cuales se recomienda que estén replicados para alta disponibilidad (es decir, seis servidores DNS):

- El primer DNS es el encargado de responder a las peticiones externas que pregunten sobre un dominio de nuestra infraestructura y por tanto es el encargado de resolver las IP públicas de nuestra red. Éste debe estar en una zona dedicada y propia de la infraestructura, y dicho DNS no debe permitir peticiones recursivas y por supuesto peticiones desde nuestra infraestructura.
- El segundo DNS se encontrará en la red perimetral o DMZ. Contiene las IP privadas de los servidores de DMZ y a su vez será el encargado de consultar a los DNS externos de la infraestructura si recibe peticiones, si y solo si, de activos pertenecientes a la red perimetral o del DNS interno.
- El tercer DNS será el interno, que responderá única y exclusivamente a peticiones de los activos de la red interna y en caso de no disponer de la respuesta, siempre deberá preguntar al DNS de la red perimetral de la infraestructura y jamás, repito, JAMÁS, a un DNS externo de Internet.

Cuando se utiliza DNS externo:
Configuración de DNS para correo entrante
DNS desempeña un papel fundamental en la entrega de correo de Internet. Para recibir correo de Internet, se necesita la configuración siguiente:

- Debe existir un registro de intercambio de correo (MX) para su servidor de correo en el servidor DNS externo. Puede emplear la herramienta Nslookup para determinar si los registros MX están configurados correctamente. Asegúrese de que los servidores de correo que utiliza como servidores cabeza de puente o como servidores de correo de Internet tienen un registro MX en los servidores DNS externos.
- Para que los servidores DNS externos resuelvan el registro MX de su servidor de correo y se pongan en contacto con él, éste debe ser accesible desde Internet. Puede utilizar el programa telnet para determinar si otros servidores pueden tener acceso a su servidor de correo.
- Exchange Server debe estar configurado para ponerse en contacto con un servidor DNS o para resolver nombres DNS externos.
- El servidor DNS debe estar configurado correctamente.

Tomado de: https://technet.microsoft.com/es-es/library/aa996996(v=exchg.65).aspx

Ejemplos de protección de los datos de la empresa
http://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzakk/rzakkscenario5.htm

Tomado de: http://www.securityartwork.es/2011/06/30/¡no-quiero-a-mi-dns/
Se puede ver como se puede para la infección de malware por el uso de DNS (Sinkhole,) http://www.securityartwork.es/2011/06/30/¡no-quiero-a-mi-dns/, manual de Sinkhole https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

Información de bind en Español (http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_bind9.html)

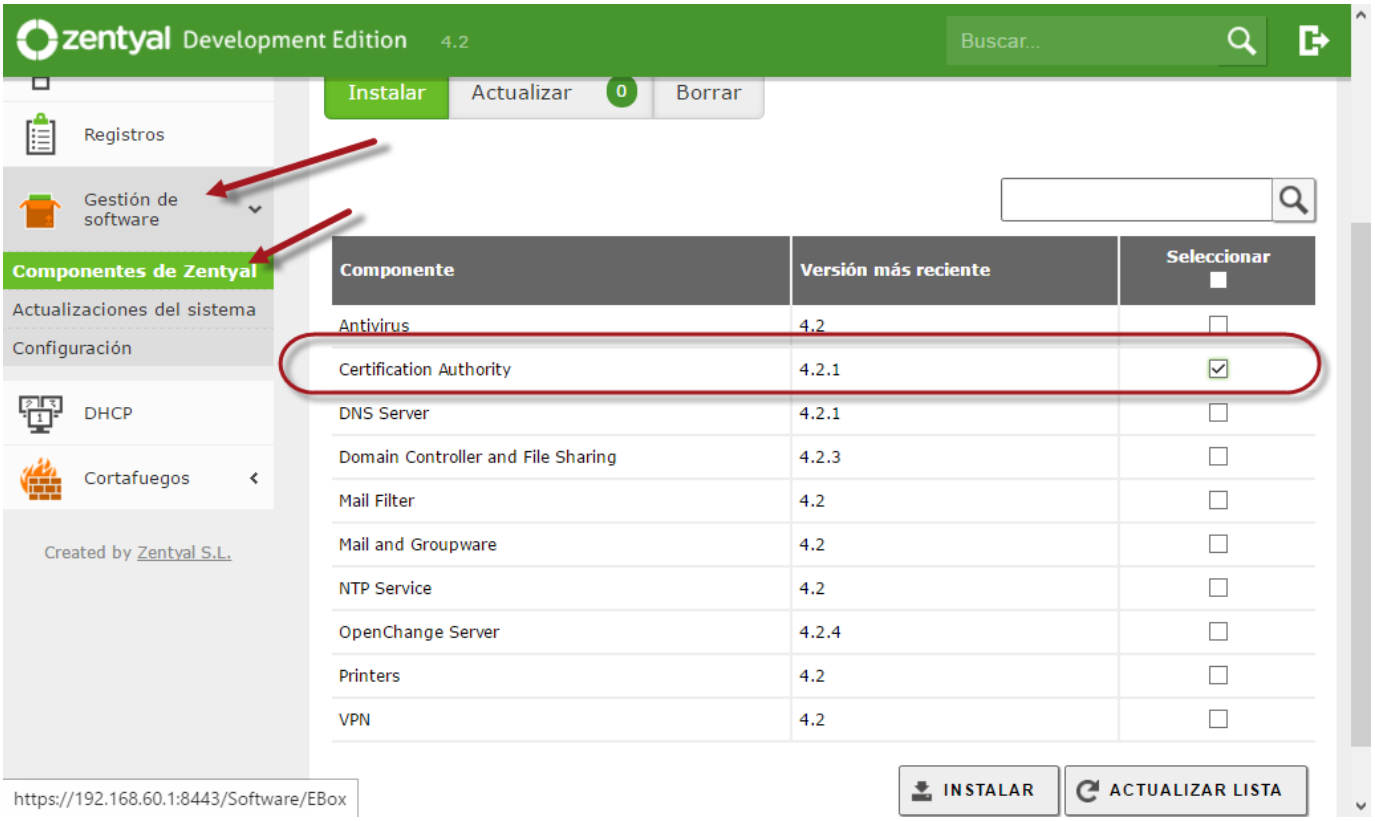
II. Desarrollo de la guía.

2.1 Instalación y configuración del servidor VPN

Paso 1 Instalar el servicio de Autoridad Certificadora

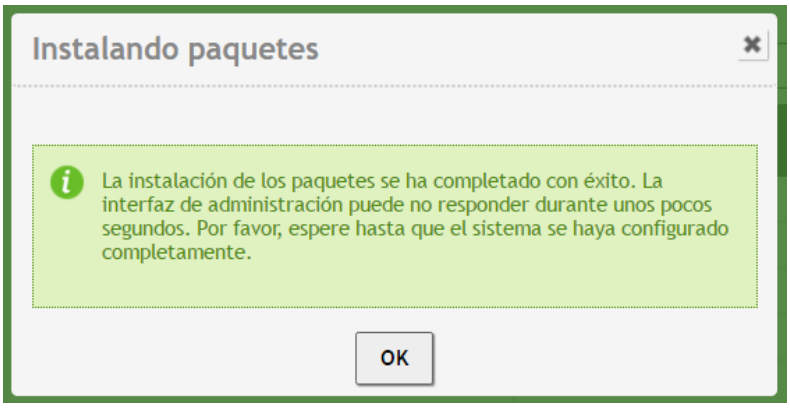
1.1 Abrir componentes de Zentyal

1.2 Seleccionar "Certification Authority"



1.3 Dar clic en botón "Instalar"

1.4 Confirmar instalación

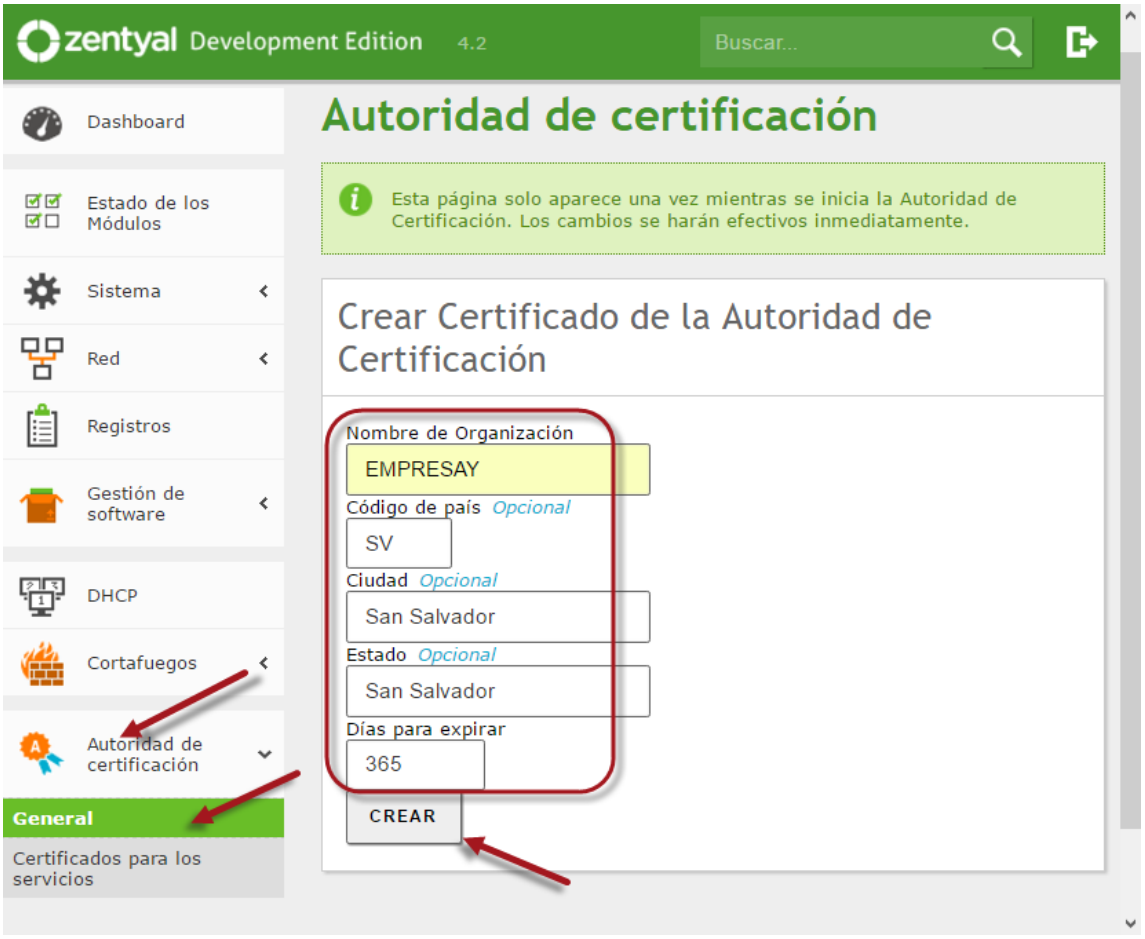


Paso 2. Crear certificado de la Autoridad de certificación

2.1 Seleccionar Autoridad de certificación
2.2 Seleccionar menú General

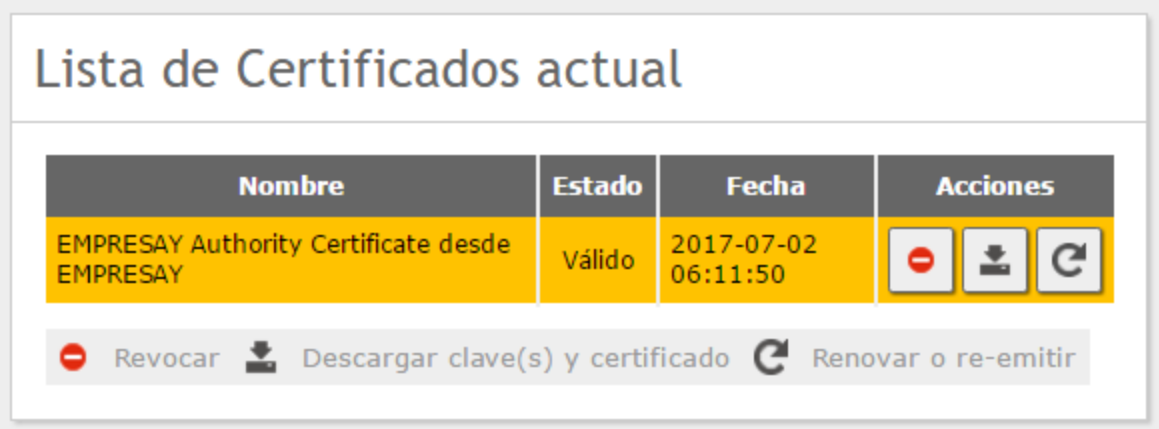
Digite los siguientes datos

- Nombre de la organización: **EMPRESAY**
- Código país: **SV**
- Ciudad: San_**Salvador**
- Estado: San_**Salvador**
- Días para expirar: **365**



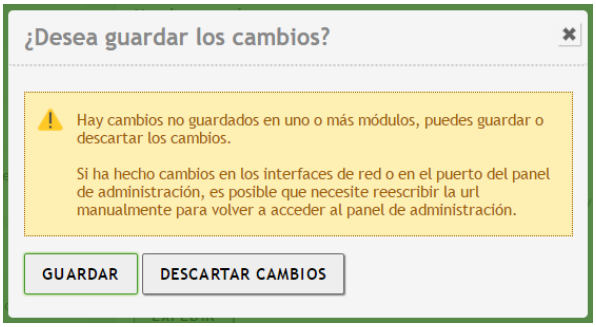
2.3 Dar clic en botón Crear

2.4 Verificar que se haya creado el certificado



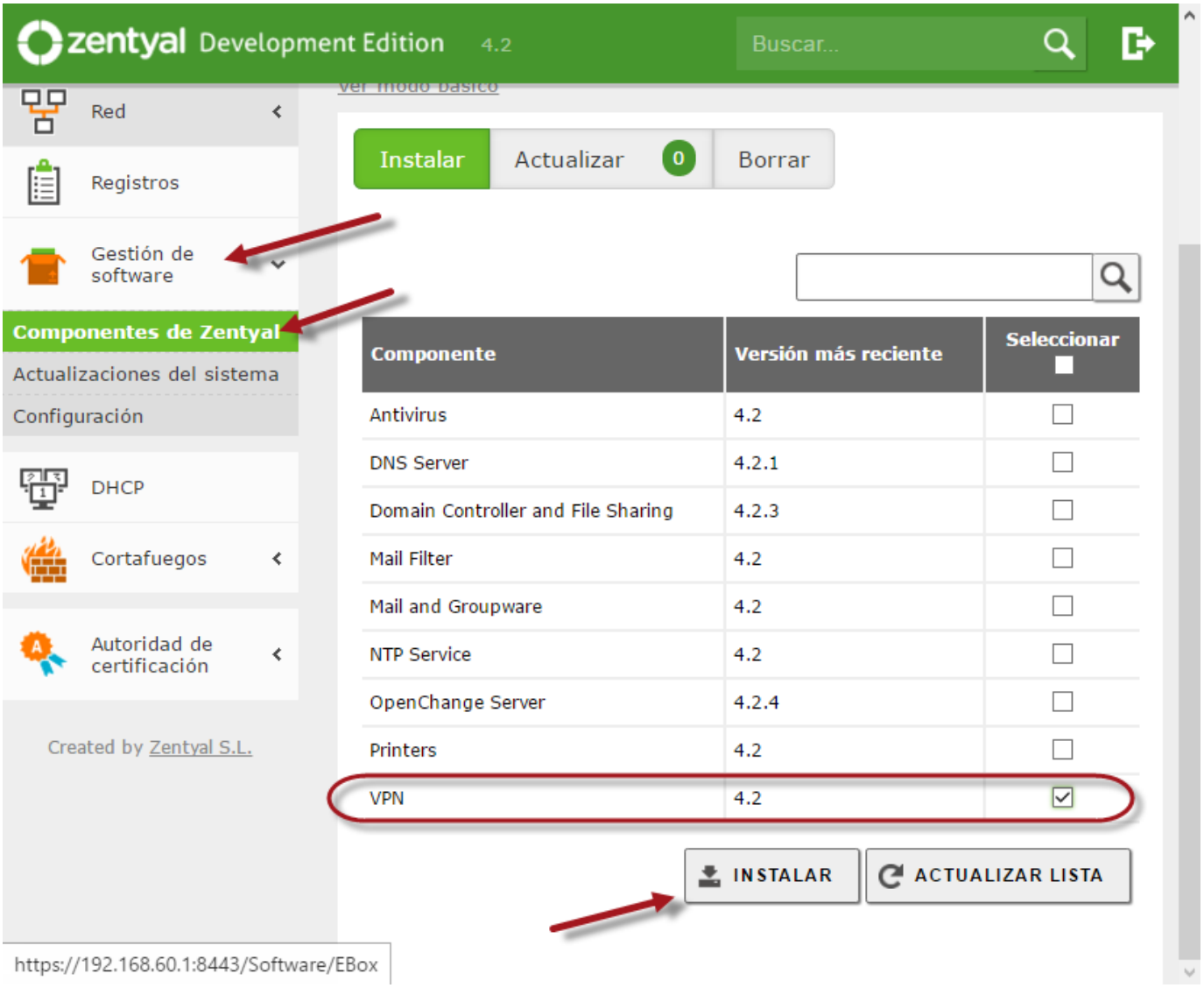
2.5 Dar clic en botón guardar configuración

2.6 Dar clic en botón guardar



Paso 3. Instalar servicio VPN

3.1 Seleccionar menú "Gestionar software"
3.2 Seleccionar "Componentes de Zentyal"
3.3 Seleccionar VPN



3.4 Dar clic en botón Instalar

3.5 Verificar los paquetes a instalar

3.6 Dar clic en botón Continuar

Paso 4. Configurar servidor VPN

4.1 Seleccionar menú VPN
4.2 Seleccionar opción Servidores
4.3 Dar clic en botón "+ Añadir nuevo/a"

4.4 Habilitar el servidor VPN

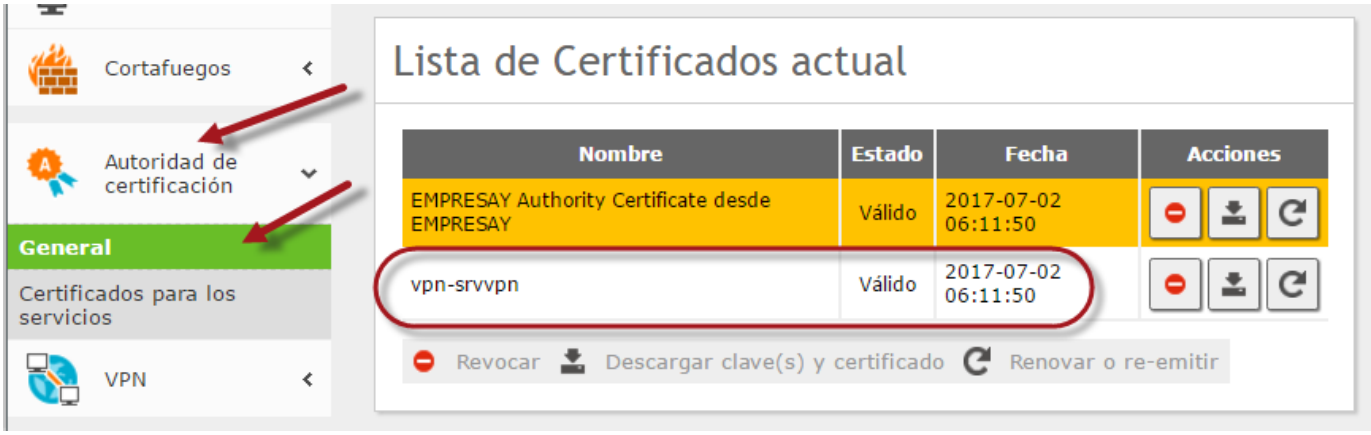
4.5 Definir nombre del servidor VPN

Para este caso se utilizará **srvvpn**

4.6 Dar clic en el botón "+ Añadir"

Paso 5. Verificar que se ha creado automáticamente un certificado para VPN en la AC

5.1 Seleccione el menú Autoridad de certificación
5.2 Seleccionar General
5.3 Verificar que existe un certificado con el nombre vpn-srvvpn

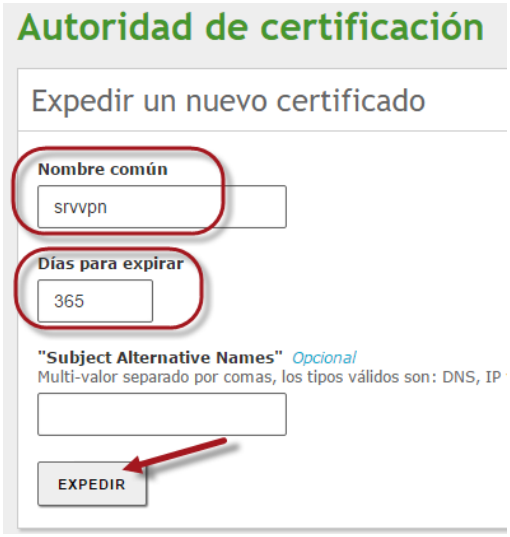


Paso 6. Crear un certificado para el servidor VPN

6.1 Seleccione el menú Autoridad de certificación

6.2 Seleccionar General

6.3 Expedir un certificado nuevo para el servidor VPN



- Nombre común: srvvpn
- Días para expirar: 365
- Dar clic en el botón “Expedir”

Verificar que se haya creado el certificado

6.4 Verificar que se hayan creado los certificados y las llaves

Digitar los siguientes comandos:

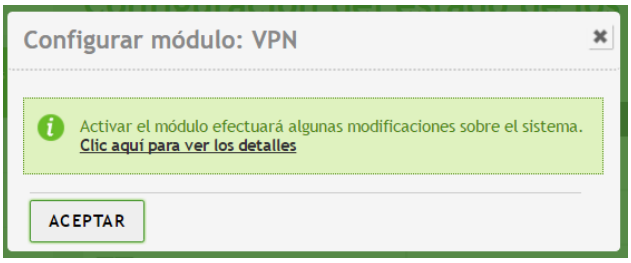
```
root@srvext:~# ll /var/lib/zentyal/CA/ca*

-rw-rw-rw- 1 ebox ebox 1574 jul 14 15:17 /var/lib/zentyal/CA/cacert.pem


root@srvext:~# ll /var/lib/zentyal/CA/private/
total 24
drwx------ 2 ebox ebox 4096 jul 14 15:17 ./
drwxr-x--x 9 ebox ebox 4096 jul 14 15:19 ../
-rw-rw-rw- 1 ebox ebox 1704 jul 14 15:17 cakey.pem
-rw-rw-rw- 1 ebox ebox 1704 jul 14 15:19 clientevpn01.pem
-rw-rw-rw- 1 ebox ebox 1708 jul 14 15:17 srvvpn.pem
-rw-rw-rw- 1 ebox ebox 1708 jul 14 15:19 vpn-srvvpn.pem


root@srvext:~# ll /var/lib/zentyal/CA/certs/
total 56
drwxr-x--x 2 ebox ebox 4096 jul 14 15:19 ./
drwxr-x--x 9 ebox ebox 4096 jul 14 15:19 ../
-rw-rw-rw- 1 ebox ebox 4564 jul  2 00:33 15E6982F68CBD9D8.pem
-rw-rw-rw- 1 ebox ebox 4570 jul  2 09:58 15E6982F68CBD9D9.pem
-rw-rw-rw- 1 ebox ebox 4564 jul 14 15:13 15E6982F68CBD9DA.pem
-rw-rw-rw- 1 ebox ebox 4569 jul 14 15:17 15E6982F68CBD9DB.pem
-rw-rw-rw- 1 ebox ebox 4577 jul 14 15:19 15E6982F68CBD9DC.pem
-rw-rw-rw- 1 ebox ebox 4583 jul 14 15:19 15E6982F68CBD9DD.pem
```

Paso 7. Activar el servidor VPN

7.1 Seleccionar menú "Estado de los módulos"

7.2 Seleccionar VPN

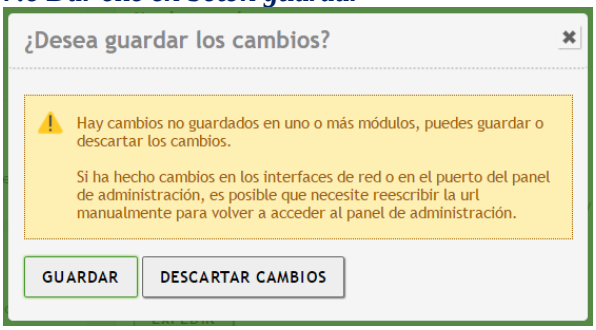
7.3 Confirmar módulo VPN



7.4 Dar clic en botón Aceptar

7.5 Dar clic en botón guardar configuración

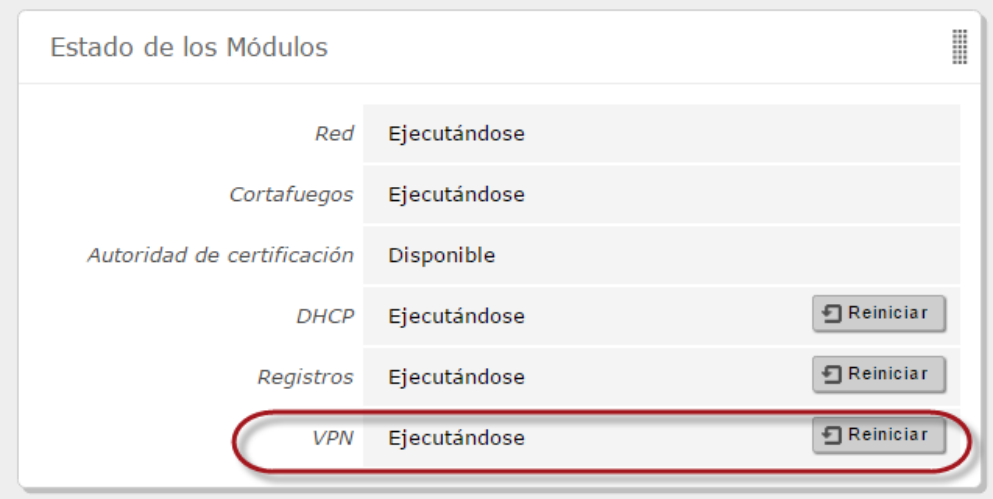
7.6 Dar clic en botón guardar



7.7 dar clic en botón Guardar

Paso 8. Verificar que el servidor VPN se ejecute correctamente

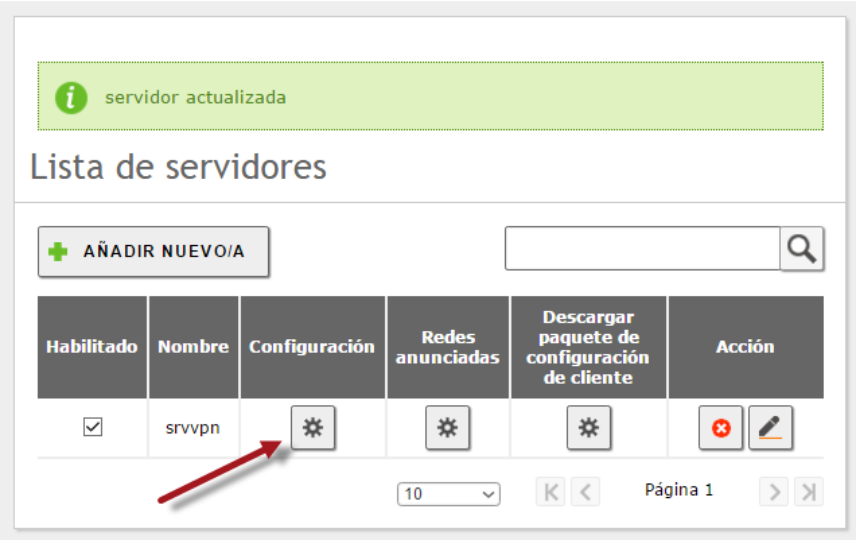
8.1 Seleccionar menú Dashboard
8.2 Ubicar Estado de los módulos



8.3 Comprobar que el servidor VPN se está ejecutando.

Paso 9. Configurar las opciones del servidor VPN

9.1 Seleccionar menú VPN
9.2 Seleccionar Servidores
9.3 Seleccionar el servidor srvvpn
9.4 Dar clic en botón configuración



9.5 Definir las siguientes opciones

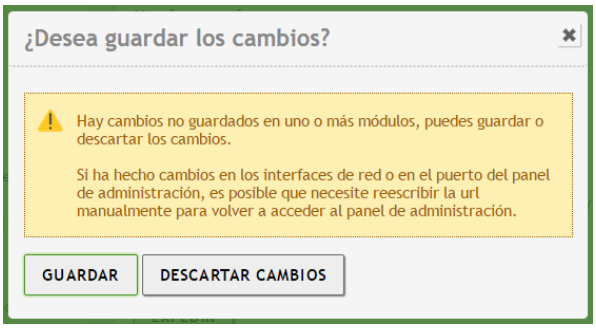
- Protocolo: **UDP puerto 1194**
- Dirección de la VPN **192.168.80.0 / 24**
- Certificado del servidor: **vpn-srvvpn**
- Interfaz TUN: **habilitado**
- Traducción de nombres NAT: **deshabilitado**
- Permitir conexiones entre cliente-cliente: **habilitado**

- Permitir túneles en Zentyal: **deshabilitado**
- Contraseña de túneles de Zentyal a Zentyal: **deshabilitado**
- Ignorar rutas enviadas por los Zentyal del túnel: **deshabilitado**
- Interfaz de escucha: **eth0**
- Redirigir puerta de enlace: **habilitado**
- Servidor DNS primario: **192.168.60.2**
- Servidor DNS primario: ---
- Dominio de búsqueda: **empresay.com.sv**
- Servidor WINS: ---

9.6 Dar clic en botón Cambiar

9.7 Dar clic en botón guardar configuración

9.8 Dar clic en botón guardar



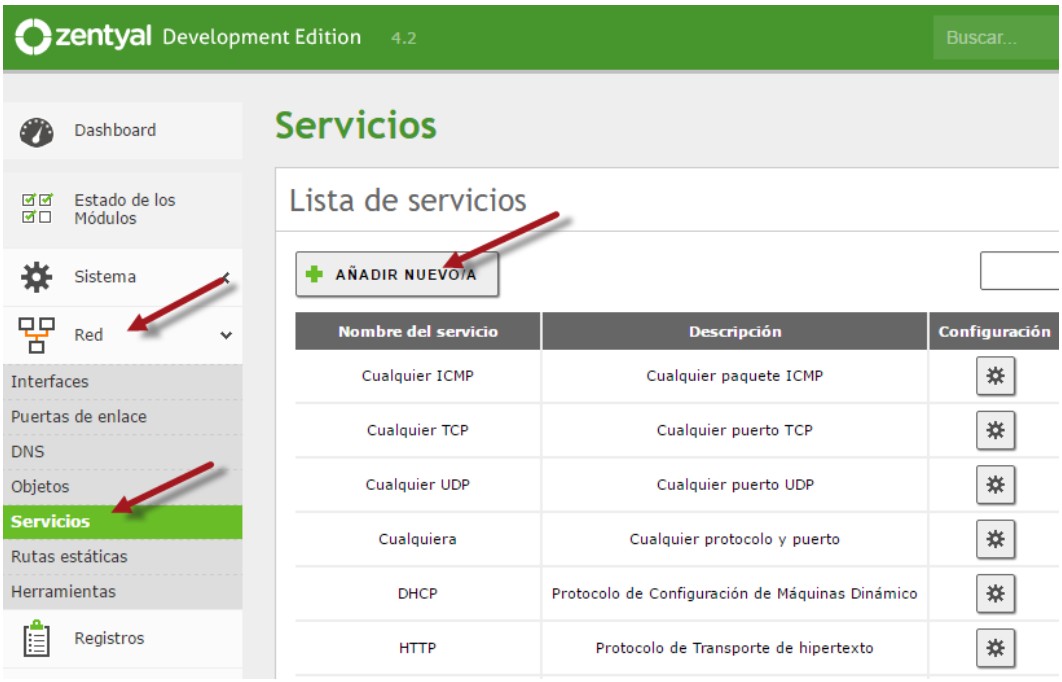
9.9 Verificar las redes que se publicarán

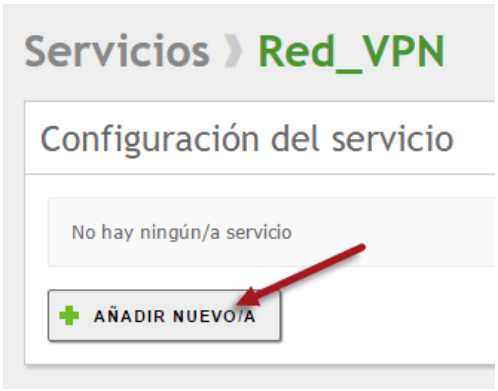
Dar clic en el botón Redes anunciadas

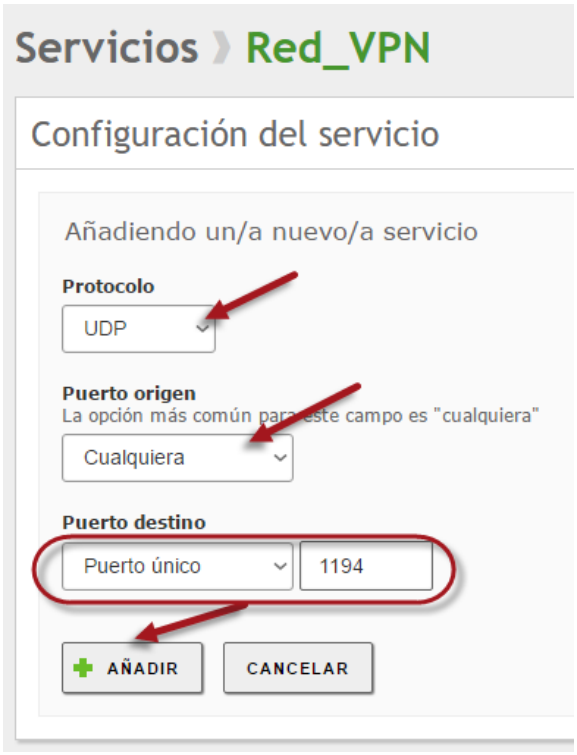
Verificar el listado de las redes 192.168.50.0, 192.168.60.0, 192.168.70.0

Paso 10. Configuración del cortafuego

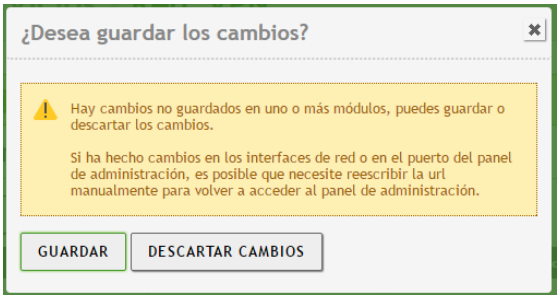
10.1 Crear servicio

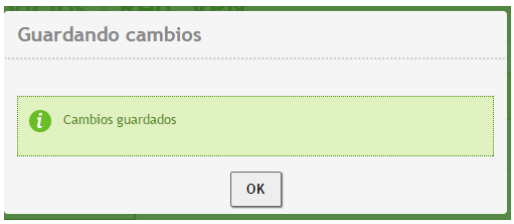



Servicios › Red_VPN
Configuración del servicio
No hay ningún/a servicio
AÑADIR NUEVO/A

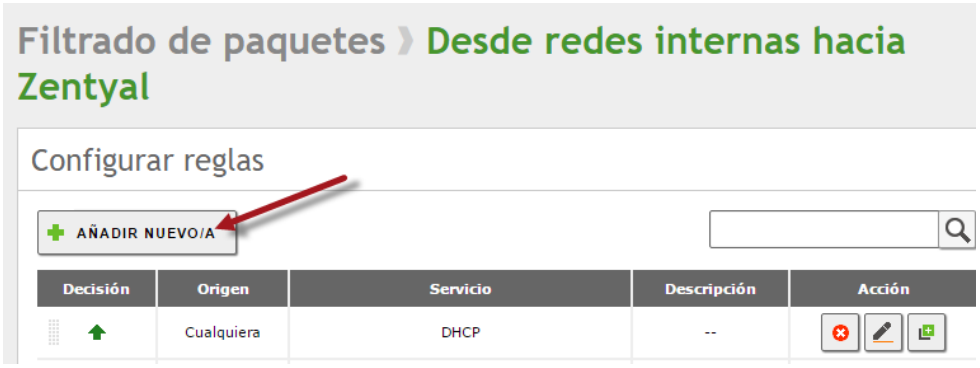

Servicios › Red_VPN
Configuración del servicio
Añadiendo un/a nuevo/a servicio
Protocolo
UDP
Puerto origen
La opción más común para este campo es "cualquiera"
Cualquiera
Puerto destino
Puerto único
1194
AÑADIR
CANCELAR

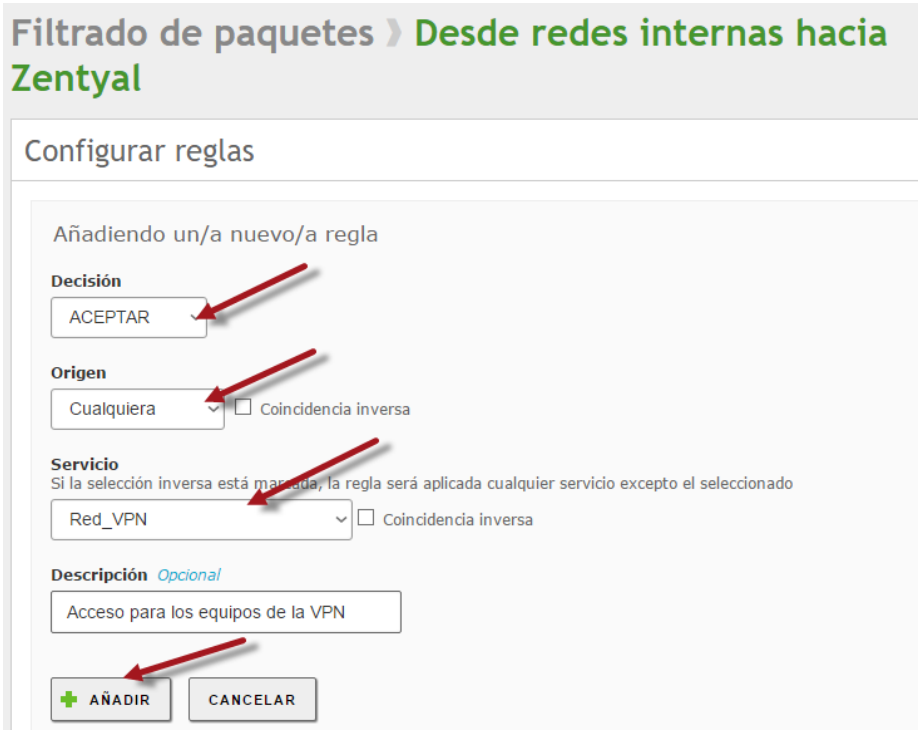

GUARDAR CAMBIOS

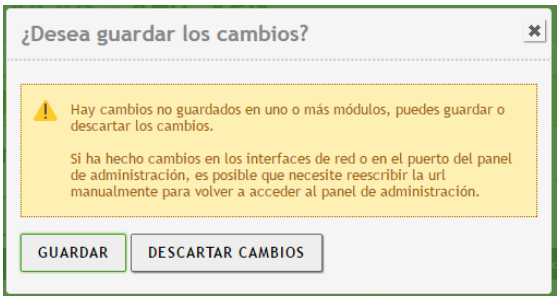

¿Desea guardar los cambios?
Hay cambios no guardados en uno o más módulos, puedes guardar o descartar los cambios.
Si ha hecho cambios en los interfaces de red o en el puerto del panel de administración, es posible que necesite reescribir la url manualmente para volver a acceder al panel de administración.
GUARDAR
DESCARTAR CAMBIOS

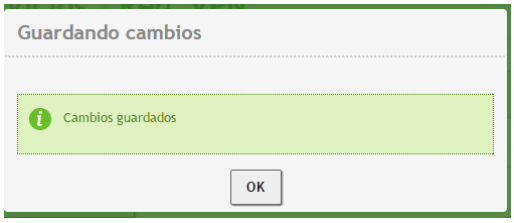

Guardando cambios
Cambios guardados
OK


Dashboard
Estado de los Módulos
DHCP
Cortafuegos
Filtrado de paquetes
Redirecciones de puertos
SNAT
Autoridad de certificación
VPN
Packet Filter
LAN
Reglas de filtrado desde las redes internas a Zentyal
Estas reglas le permiten controlar el acceso desde redes internas a servicios que corren en su máquina Zentyal
CONFIGURAR REGLAS

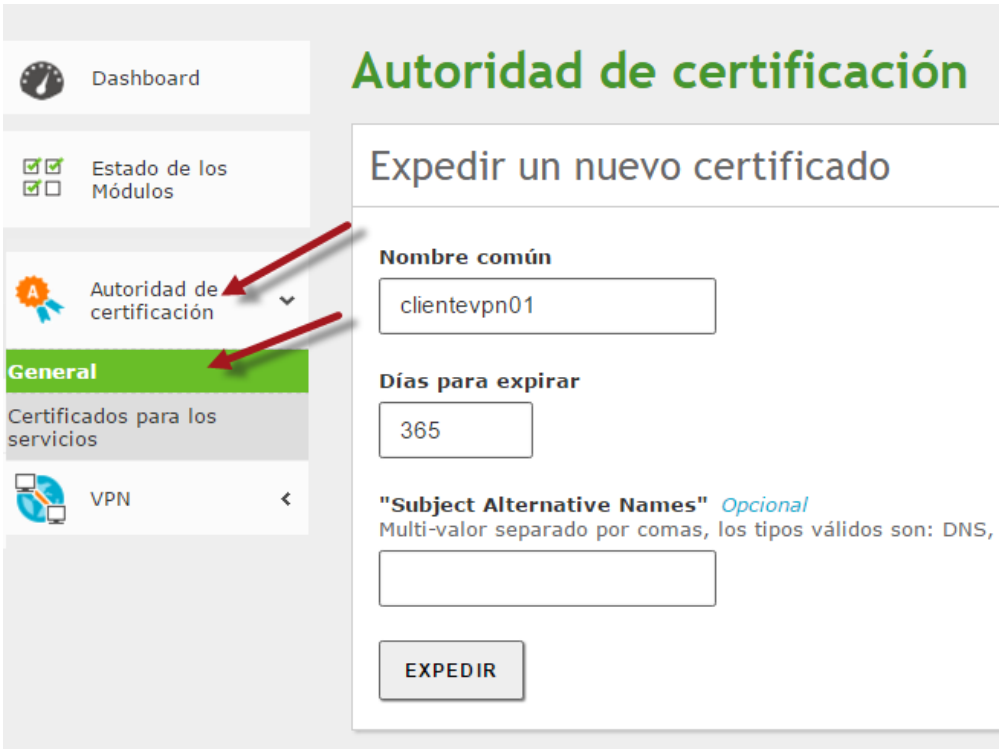

Filtrado de paquetes › Desde redes internas hacia Zentyal
Configurar reglas
AÑADIR NUEVO/A
Decisión
Origen
Servicio
Descripción
Acción
Cualquiera
DHCP
--


Filtrado de paquetes › Desde redes internas hacia Zentyal
Configurar reglas
Añadiendo un/a nuevo/a regla
Decisión
ACEPTAR
Origen
Cualquiera
Coincidencia inversa
Servicio
Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado
Red_VPN
Coincidencia inversa
Descripción Opcional
Acceso para los equipos de la VPN
AÑADIR
CANCELAR



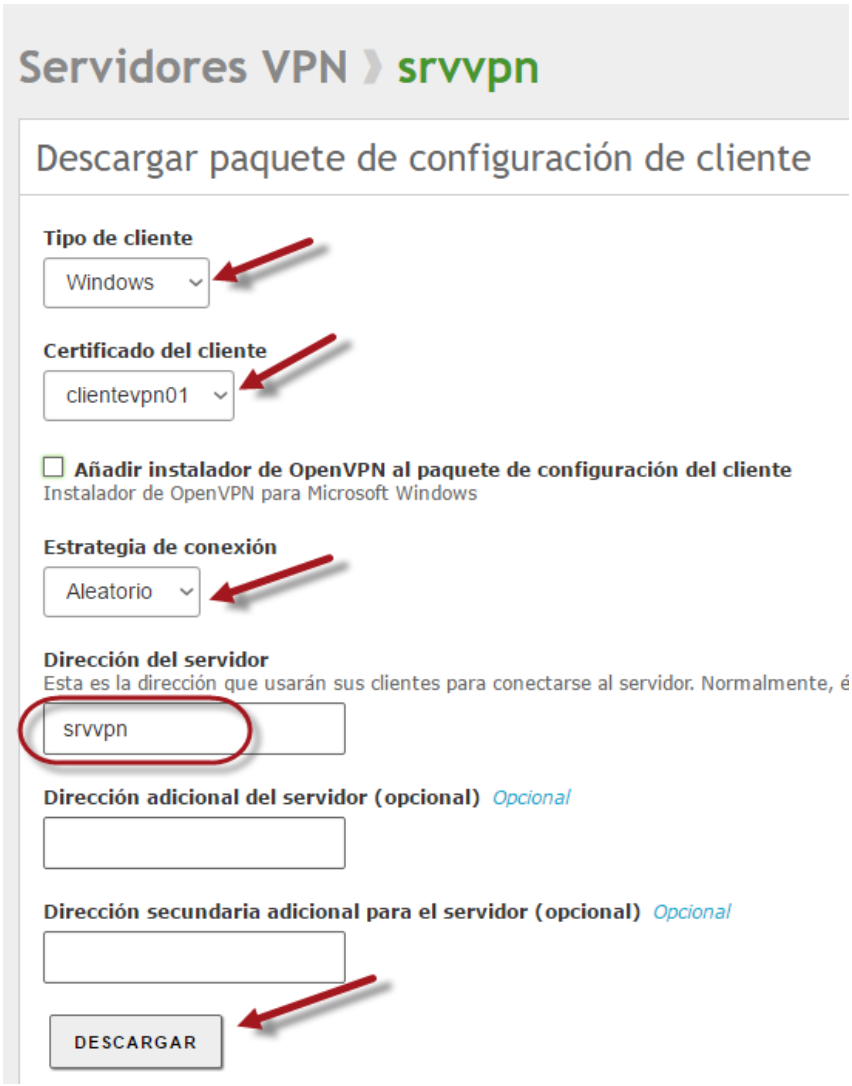


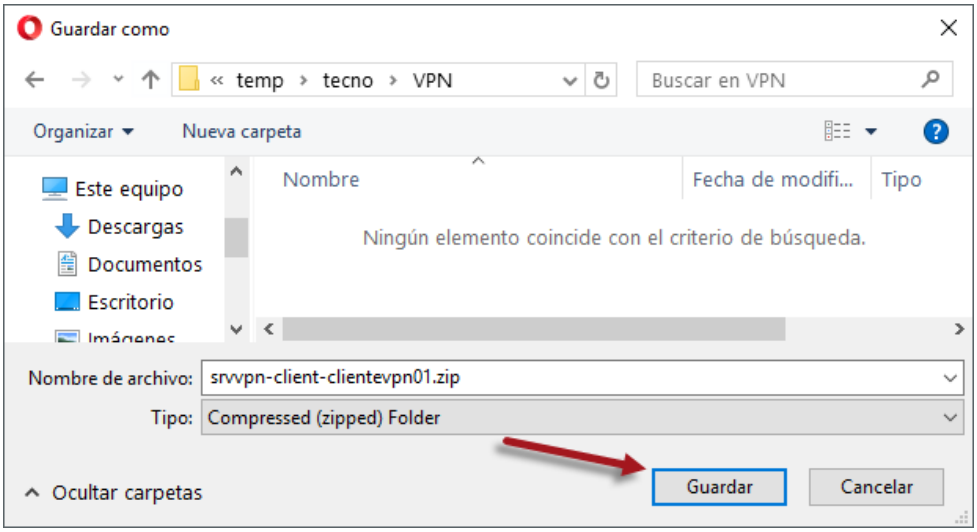
Paso 11. Configuración de los certificados para los clientes



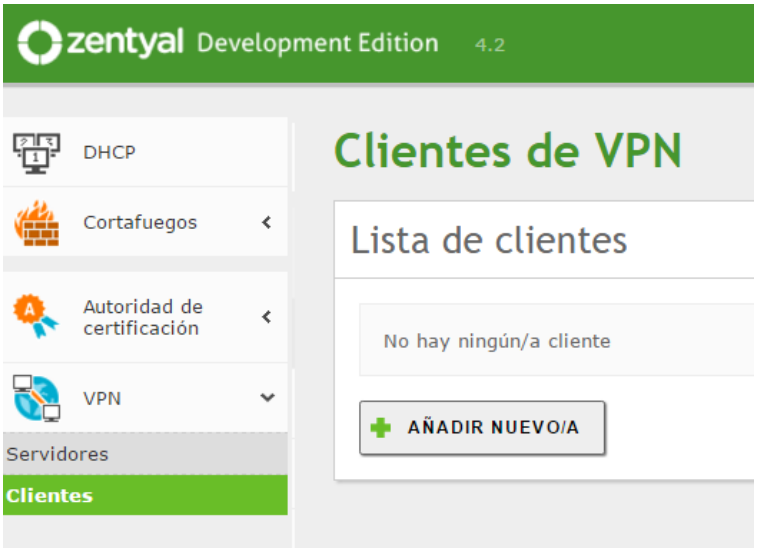

Lista de Certificados actual
Nombre
Estado
Fecha
Acciones
EMPRESAY Authority Certificate desde EMPRESAY
Válido
2017-07-14 07:21:27
vpn-srvvpn
Válido
2017-07-14 07:21:27
srvvpn
Válido
2017-07-14 02:10:34
clientevpn01
Válido
2017-07-14 02:46:24
Revocar
Descargar clave(s) y certificado
Renovar o re-emitir


Servidores VPN
Lista de servidores
AÑADIR NUEVO/A
Habilitado
Nombre
Configuración
Redes anunciadas
Descargar paquete de configuración de cliente
Acción
srvvpn
10
Página 1


Servidores VPN » srvvpn
Descargar paquete de configuración de cliente
Tipo de cliente
Windows
Certificado del cliente
clientevpn01
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, é
srvvpn
Dirección adicional del servidor (opcional) Opcional
Dirección secundaria adicional para el servidor (opcional) Opcional
DESCARGAR

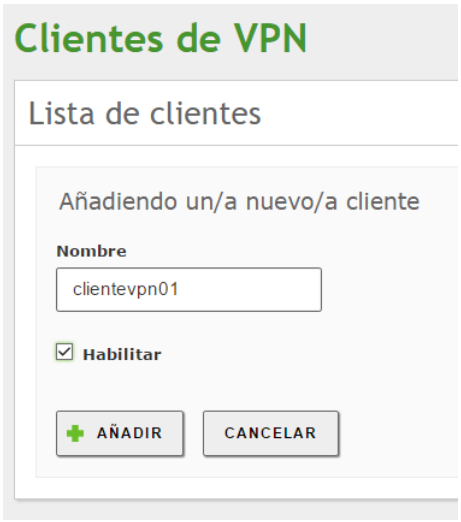

Guardar como
« temp › tecno › VPN
Buscar en VPN
Organizar
Nueva carpeta
Este equipo
Descargas
Documentos
Escritorio
Nombre
Fecha de modifi...
Tipo
Ningún elemento coincide con el criterio de búsqueda.
Nombre de archivo: srvvpn-client-clientevpn01.zip
Tipo: Compressed (zipped) Folder
Ocultar carpetas
Guardar
Cancelar

11.1 Seleccionar menú VPN
11.2 Seleccionar opción Clientes
11.3 Dar clic en el botón "+ Añadir nuevo"



11.4 Definir el nombre del cliente VPN

- Nombre: **clientevpn01**
- Habilitar el cliente: **Habilitado**



Paso 12. Comprobación de los archivos de configuración

Parámetros	srvext	servidor01	clienteVPN
IPv4	10.10.3.12	192.168.60.11	10.10.3.13
Máscara	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	10.10.3.155	192.168.60.1	10.10.3.12
DNS	192.168.60.2	192.168.60.2	---

12.1 Verificar el archivo de configuración

```
root@srvext:~# cat /etc/openvpn/srvvpn.d/srvvpn.conf

#multihome → si se desea que se escuche por todas las tarjetas de red
Local 10.10.3.12
port 1194
proto udp
dev tun0
ca '/var/lib/zentyal/CA/cacert.pem'
cert '/var/lib/zentyal/CA/certs/15E6982F68CBD9DC.pem'
key '/var/lib/zentyal/CA/private/vpn-srvvpn.pem'
crl-verify /var/lib/zentyal/CA/crl/latest.pem
dh /etc/openvpn/ebox-dh1024.pem
server 192.168.80.0 255.255.255.0
ifconfig-pool-persist '/etc/openvpn/srvvpn.d/srvvpn-ipp.txt'
client-to-client
keepalive 10 120
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
writepid /var/run/openvpn.srvvpn.pid
status '/var/log/openvpn/status-srvvpn.log'
log-append  '/var/log/openvpn/srvvpn.log'
verb 3
push "redirect-gateway def1"
push "dhcp-option DNS 192.168.60.2"
push "dhcp-option DOMAIN empresay.com.sv"
client-config-dir /etc/openvpn/srvvpn.d/client-config.d
push "route 192.168.60.0 255.255.255.0"
push "route 192.168.50.0 255.255.255.0"
push "route 192.168.70.0 255.255.255.0"
```

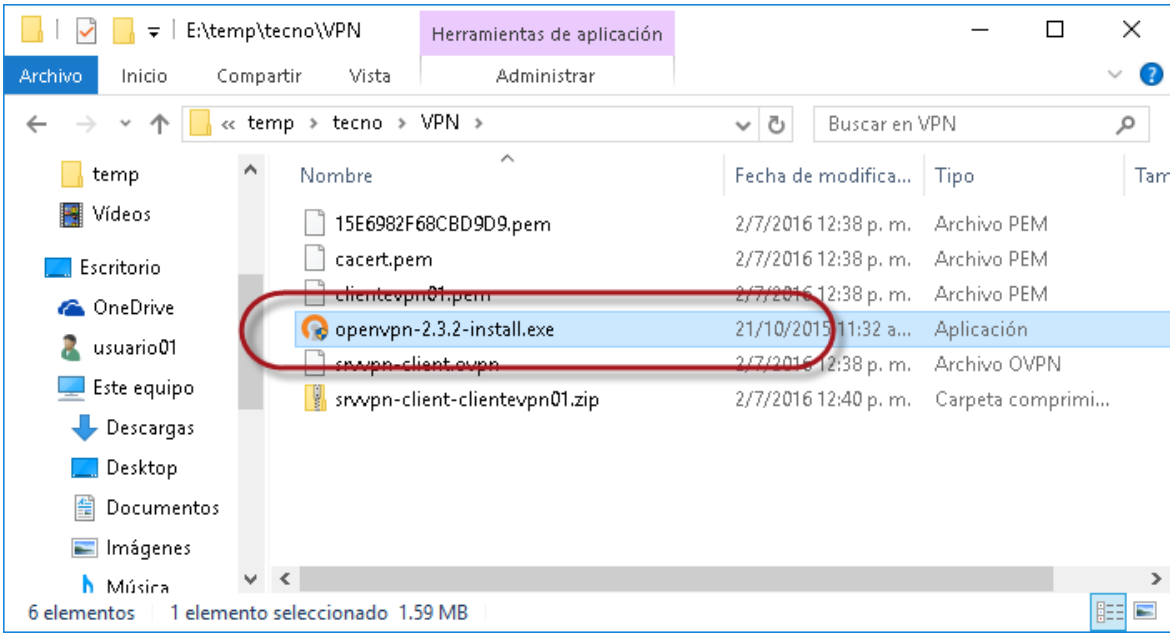
Configuración de cliente VPN

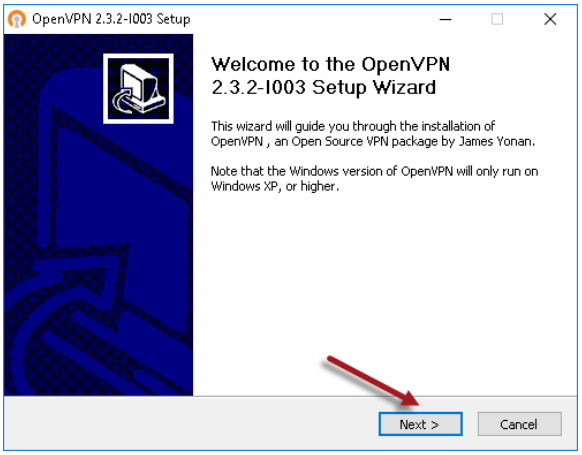
```
C:\Program Files (x86)\OpenVPN\config\ srvvpn-client.ovpn

client
dev tun
proto udp
remote  10.10.3.202 1194
float
remote-random
resolv-retry infinite
nobind
persist-key
persist-tun
```

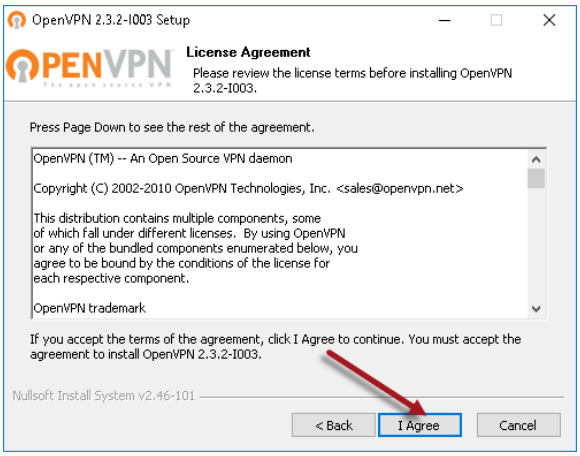
```
ca   "cacert.pem"
cert "15E6982F68CBD9DB.pem"
key  "srvvpn.pem"
verify-x509-name vpn-srvvpn name
comp-lzo
verb 3
explicit-exit-notify 3
```

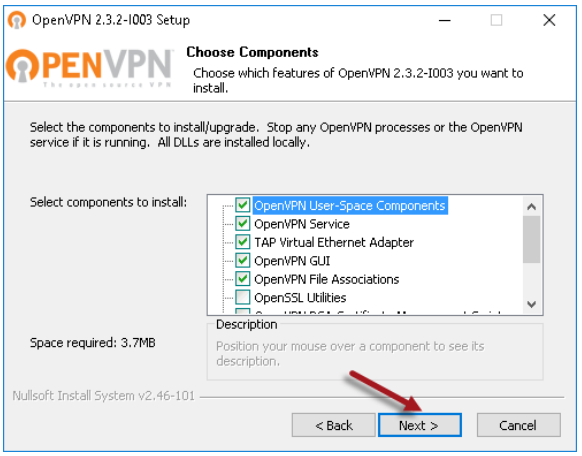
2.2 Instalación y configuración del cliente VPN

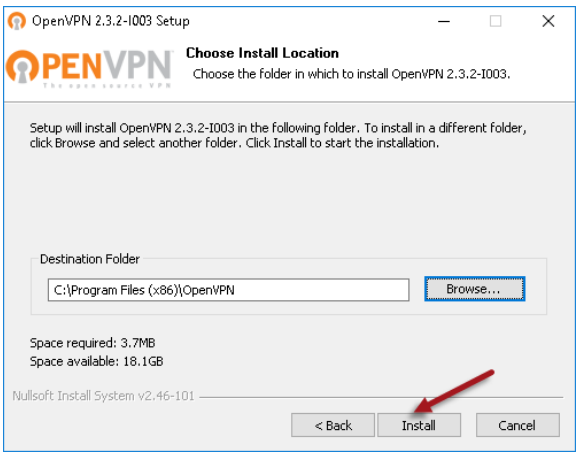
Cliente Windows

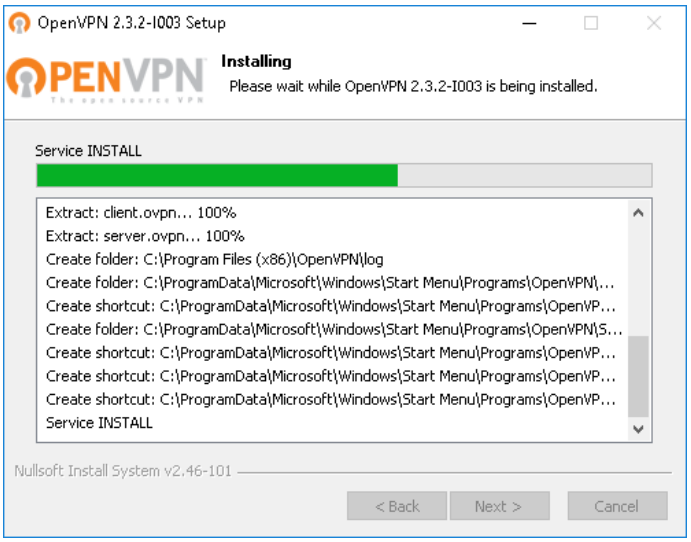


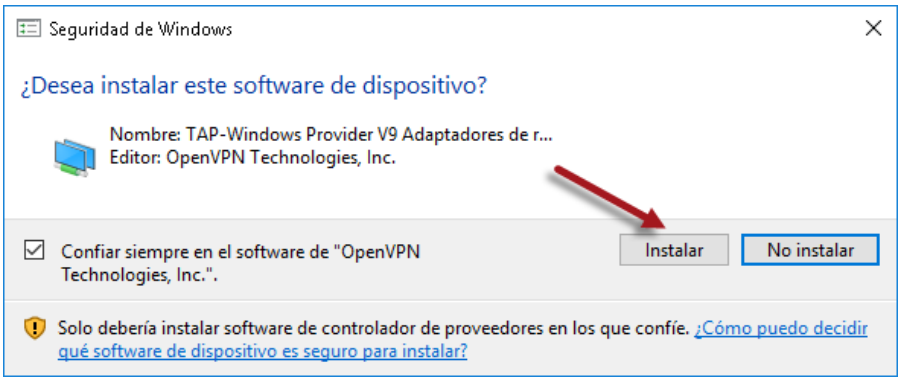


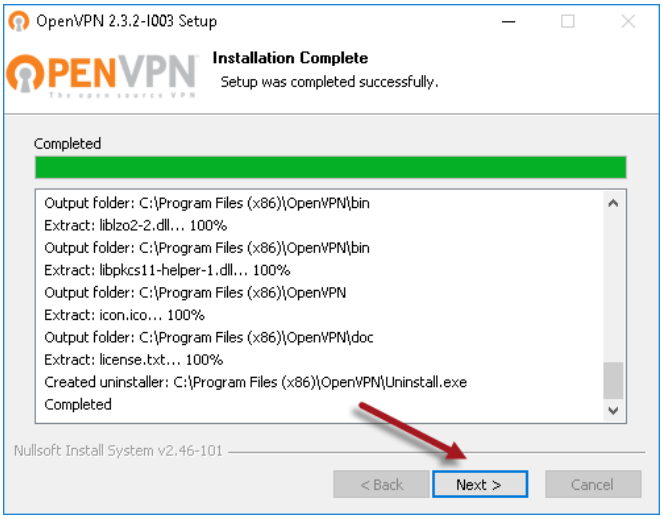


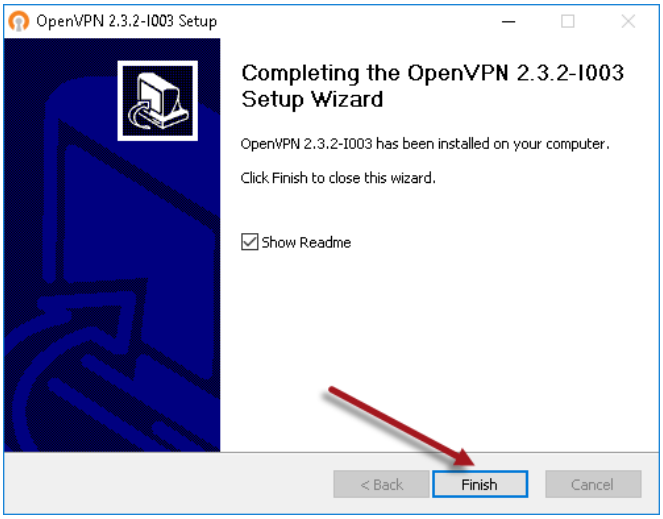





OpenVPN 2.3.2-I003 Setup
Installing
Please wait while OpenVPN 2.3.2-I003 is being installed.
Service INSTALL
Extract: client.ovpn... 100%
Extract: server.ovpn... 100%
Create folder: C:\Program Files (x86)\OpenVPN\log
Create folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVPN\...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVPN\S...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVP...
Service INSTALL
Nullsoft Install System v2.46-101
< Back
Next >
Cancel

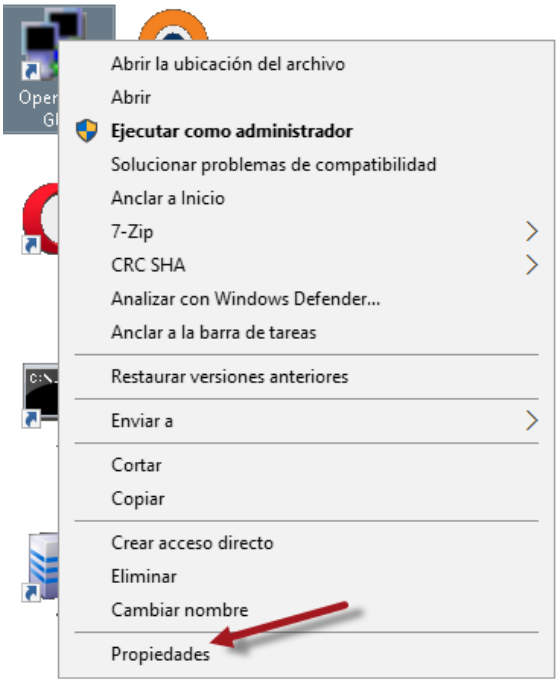

Seguridad de Windows
¿Desea instalar este software de dispositivo?
Nombre: TAP-Windows Provider V9 Adaptadores de r...
Editor: OpenVPN Technologies, Inc.
Confiar siempre en el software de "OpenVPN Technologies, Inc.".
Instalar
No instalar
Solo debería instalar software de controlador de proveedores en los que confíe. ¿Cómo puedo decidir qué software de dispositivo es seguro para instalar?

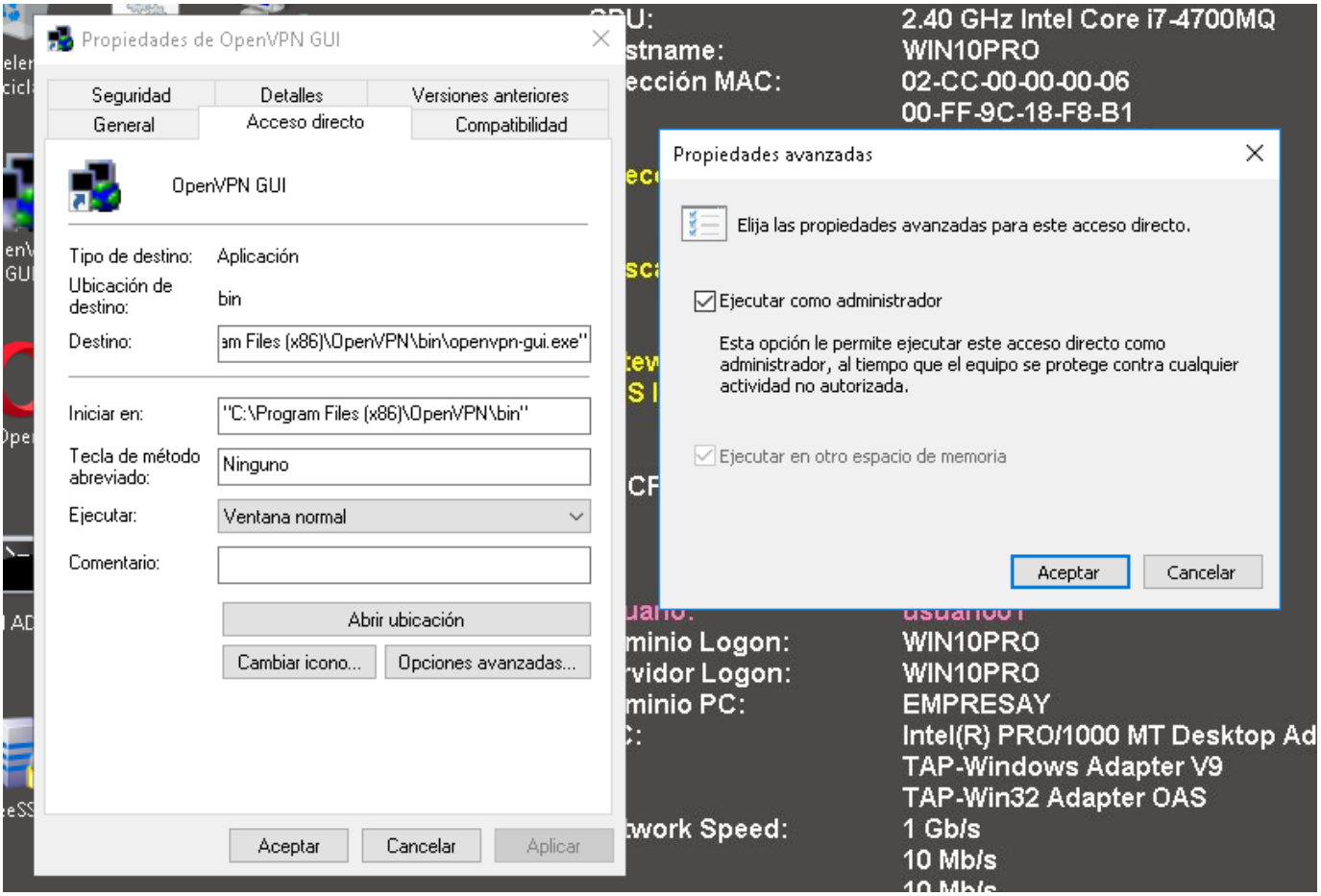

OpenVPN 2.3.2-I003 Setup
Installation Complete
Setup was completed successfully.
Completed
Output folder: C:\Program Files (x86)\OpenVPN\bin
Extract: liblzo2-2.dll... 100%
Output folder: C:\Program Files (x86)\OpenVPN\bin
Extract: libpkcs11-helper-1.dll... 100%
Output folder: C:\Program Files (x86)\OpenVPN
Extract: icon.ico... 100%
Output folder: C:\Program Files (x86)\OpenVPN\doc
Extract: license.txt... 100%
Created uninstaller: C:\Program Files (x86)\OpenVPN\Uninstall.exe
Completed
Nullsoft Install System v2.46-101
< Back
Next >
Cancel

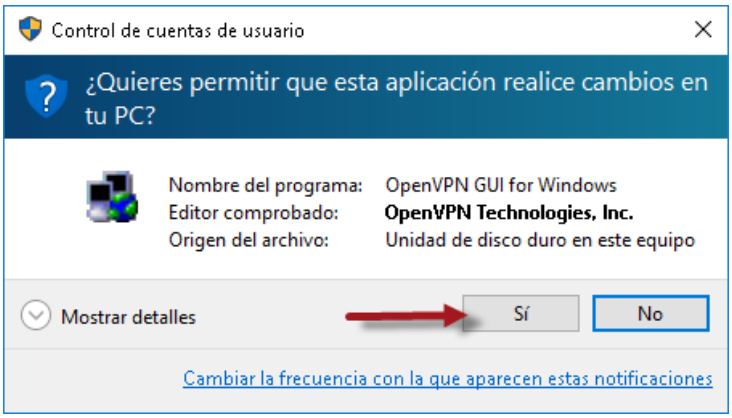

OpenVPN 2.3.2-I003 Setup
Completing the OpenVPN 2.3.2-I003 Setup Wizard
OpenVPN 2.3.2-I003 has been installed on your computer.
Click Finish to close this wizard.
Show Readme
< Back
Finish
Cancel

Ejecución del cliente OpenVPN

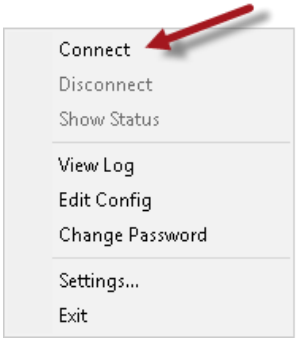
Configurar que el programa se ejecute con permisos administrador

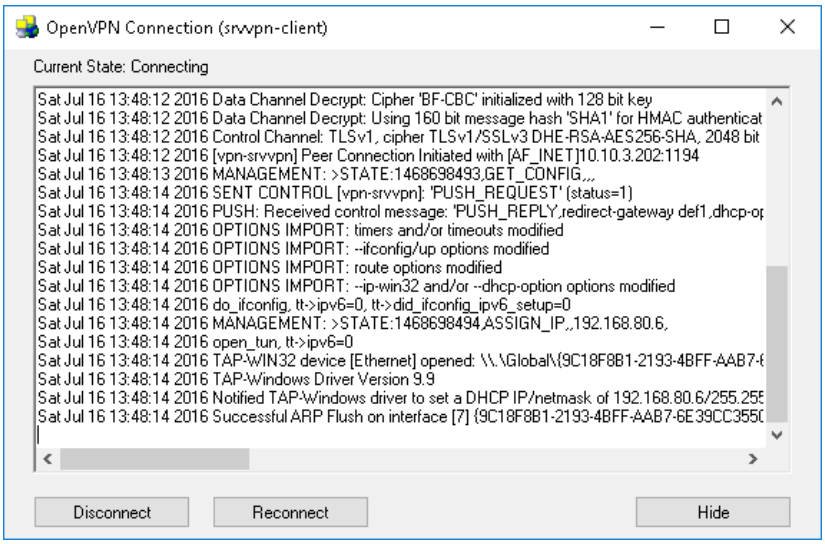





Control de cuentas de usuario
¿Quieres permitir que esta aplicación realice cambios en tu PC?
Nombre del programa: OpenVPN GUI for Windows
Editor comprobado: OpenVPN Technologies, Inc.
Origen del archivo: Unidad de disco duro en este equipo
Mostrar detalles
Sí
No
Cambiar la frecuencia con la que aparecen estas notificaciones


ESP
US


Connect
Disconnect
Show Status
View Log
Edit Config
Change Password
Settings...
Exit


OpenVPN Connection (srvvpn-client)
Current State: Connecting
Sat Jul 16 13:48:12 2016 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat Jul 16 13:48:12 2016 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authenticat
Sat Jul 16 13:48:12 2016 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit
Sat Jul 16 13:48:12 2016 [vpn-srvvpn] Peer Connection Initiated with [AF_INET]10.10.3.202:1194
Sat Jul 16 13:48:13 2016 MANAGEMENT: >STATE:1468698493,GET_CONFIG,,,
Sat Jul 16 13:48:14 2016 SENT CONTROL [vpn-srvvpn]: 'PUSH_REQUEST' (status=1)
Sat Jul 16 13:48:14 2016 PUSH: Received control message: 'PUSH_REPLY',redirect-gateway def1,dhcp-op
Sat Jul 16 13:48:14 2016 OPTIONS IMPORT: timers and/or timeouts modified
Sat Jul 16 13:48:14 2016 OPTIONS IMPORT: --ifconfig/up options modified
Sat Jul 16 13:48:14 2016 OPTIONS IMPORT: route options modified
Sat Jul 16 13:48:14 2016 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Sat Jul 16 13:48:14 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Sat Jul 16 13:48:14 2016 MANAGEMENT: >STATE:1468698494,ASSIGN_IP,,192.168.80.6,
Sat Jul 16 13:48:14 2016 open_tun, tt->ipv6=0
Sat Jul 16 13:48:14 2016 TAP-WIN32 device [Ethernet] opened: \\.\Global\{9C18F8B1-2193-4BFF-AAB7-
Sat Jul 16 13:48:14 2016 TAP-Windows Driver Version 9.9
Sat Jul 16 13:48:14 2016 Notified TAP-Windows driver to set a DHCP IP/netmask of 192.168.80.6/255.25
Sat Jul 16 13:48:14 2016 Successful ARP Flush on interface [7] {9C18F8B1-2193-4BFF-AAB7-6E39CC355
Disconnect
Reconnect
Hide

```
C:\Windows\system32>ipconfig

Configuración IP de Windows
Adaptador de Ethernet LAN:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.3.13
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.10.3.12

Adaptador de Ethernet Ethernet:
   Sufijo DNS específico para la conexión. . : empresay.com.sv
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.80.6
   Máscara de subred . . . . . . . . . . . . : 255.255.255.252
   Puerta de enlace predeterminada . . . . . :
```

Tabla de ruteo

```
C:\Windows\system32>route print
===========================================================================
ILista de interfaces
  3...02 cc 00 00 00 06 ......Intel(R) PRO/1000 MT Desktop Adapter
  7...00 ff 9c 18 f8 b1 ......TAP-Windows Adapter V9
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      10.10.3.12      10.10.3.13     266
          0.0.0.0        128.0.0.0     192.168.80.5     192.168.80.6      30
        10.10.3.0    255.255.255.0      En vínculo        10.10.3.13     266
       10.10.3.12  255.255.255.255       10.10.3.12       10.10.3.13      10
       10.10.3.13  255.255.255.255      En vínculo        10.10.3.13     266
      10.10.3.255  255.255.255.255      En vínculo        10.10.3.13     266
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1     306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1     306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1     306
        128.0.0.0        128.0.0.0     192.168.80.5     192.168.80.6      30
     192.168.50.0    255.255.255.0     192.168.80.5     192.168.80.6      30
     192.168.60.0    255.255.255.0     192.168.80.5     192.168.80.6      30
     192.168.70.0    255.255.255.0     192.168.80.5     192.168.80.6      30
     192.168.80.0    255.255.255.0     192.168.80.5     192.168.80.6      30
     192.168.80.4  255.255.255.252      En vínculo      192.168.80.6     286
     192.168.80.6  255.255.255.255      En vínculo      192.168.80.6     286
     192.168.80.7  255.255.255.255      En vínculo      192.168.80.6     286
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1     306
        224.0.0.0        240.0.0.0      En vínculo      192.168.80.6     286
        224.0.0.0        240.0.0.0      En vínculo        10.10.3.13     266
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1     306
  255.255.255.255  255.255.255.255      En vínculo      192.168.80.6     286
```

```
  255.255.255.255  255.255.255.255      En vínculo        10.10.3.13    266
===========================================================================
Rutas persistentes:
  Dirección de red  Máscara de red  Dirección de puerta de enlace  Métrica
          0.0.0.0          0.0.0.0       10.10.3.12  Predeterminada
===========================================================================

IPv6 Tabla de enrutamiento
===========================================================================
Rutas activas:
 Cuando destino de red métrica      Puerta de enlace
  1    306 ::1/128                  En vínculo
  1    306 ff00::/8                 En vínculo
===========================================================================
Rutas persistentes:
  Ninguno
```

Dirección de subredes

```
root@srvext:~# cat /etc/openvpn/srvvpn.d/srvvpn-ipp.txt

srvvpn,192.168.80.4
```

Solución de problemas

Direcciones IPv4

```
root@srvext:~# ip addr list |grep inet

    inet 127.0.0.1/8 scope host lo
    inet 127.0.1.1/8 scope host secondary lo
    inet 10.10.3.202/24 brd 10.10.3.255 scope global eth0
    inet 192.168.60.1/24 brd 192.168.60.255 scope global eth1
    inet 192.168.50.1/24 brd 192.168.50.255 scope global eth2
    inet 192.168.70.1/24 brd 192.168.70.255 scope global eth3
    inet 192.168.80.1 peer 192.168.80.2/32 scope global tun0


root@srvext:~# ip addr list

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 127.0.1.1/8 scope host secondary lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 02:aa:e0:00:00:01 brd ff:ff:ff:ff:ff:ff
    inet 10.10.3.202/24 brd 10.10.3.255 scope global eth0
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 02:aa:e1:00:00:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.1/24 brd 192.168.60.255 scope global eth1
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 02:aa:e2:00:00:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.1/24 brd 192.168.50.255 scope global eth2
       valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 02:aa:e3:00:00:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.1/24 brd 192.168.70.255 scope global eth3
       valid_lft forever preferred_lft forever
9: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN group default qlen 100
    link/none
    inet 192.168.80.1 peer 192.168.80.2/32 scope global tun0
       valid_lft forever preferred_lft forever
```

Tabla de ruteo del srvext

```
root@srvext:~# route -n

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.3.202     0.0.0.0         UG    0      0        0 eth0
10.10.3.0       0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.50.0    0.0.0.0         255.255.255.0   U     0      0        0 eth2
192.168.60.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.70.0    0.0.0.0         255.255.255.0   U     0      0        0 eth3
192.168.80.0    192.168.80.2    255.255.255.0   UG    0      0        0 tun0
192.168.80.2    0.0.0.0         255.255.255.255 UH    0      0        0 tun0
```

Nota: Si no hubiera un geteway por default debe agregarlo por comandos usando el comando **`route add default gw 10.10.3.X`** (si esa fuera la dirección de la eth0)

Configuración de Windows (7 o 10)

```
C:\Windows\system32>ipconfig

Configuración IP de Windows
Adaptador de Ethernet LAN:
   Sufijo DNS específico para la conexión. . : uni.edu.sv
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.3.203
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.10.3.254

Adaptador de Ethernet Ethernet:
   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : empresay.com.sv

Adaptador de Ethernet Ethernet 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :


C:\Windows\system32>route print
===========================================================================
ILista de interfaces
  3...02 cc 00 00 00 06 ......Intel(R) PRO/1000 MT Desktop Adapter
  7...00 ff 9c 18 f8 b1 ......TAP-Windows Adapter V9
  8...00 ff b2 b9 ca b9 ......TAP-Win32 Adapter OAS
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      10.10.3.155      10.10.3.203     266
        10.10.3.0    255.255.255.0      En vínculo       10.10.3.203     266
      10.10.3.203  255.255.255.255      En vínculo       10.10.3.203     266
      10.10.3.255  255.255.255.255      En vínculo       10.10.3.203     266
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1     306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1     306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1     306
```

```
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    306
        224.0.0.0        240.0.0.0      En vínculo       10.10.3.203    266
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
  255.255.255.255  255.255.255.255      En vínculo       10.10.3.203    266
===========================================================================
Rutas persistentes:
  Dirección de red  Máscara de red  Dirección de puerta de enlace  Métrica
          0.0.0.0          0.0.0.0      10.10.3.155  Predeterminada
===========================================================================

IPv6 Tabla de enrutamiento
===========================================================================
Rutas activas:
 Cuando destino de red métrica      Puerta de enlace
  1    306 ::1/128                  En vínculo
  1    306 ff00::/8                 En vínculo
===========================================================================
Rutas persistentes:
  Ninguno


C:\Windows\system32>route delete 0.0.0.0 mask 0.0.0.0 10.10.3.155
 Correcto
```

Comandos a utilizar para limpiar datos.

netsh winsock reset
netsh winsock reset catalog
netsh int ip reset c:\resetlog.txt
ipconfig /flushdns

```
C:\Windows\system32>netsh winsock reset

El catálogo Winsock se restableció correctamente.
Debe reiniciar el equipo para completar el restablecimiento.


C:\Windows\system32>netsh winsock reset catalog

El catálogo Winsock se restableció correctamente.
Debe reiniciar el equipo para completar el restablecimiento.


C:\Windows\system32>netsh inter ip reset c:\milog.txt

Global se restableció correctamente.
Interfaz se restableció correctamente.
Dirección de unidifusión se restableció correctamente.
Vecino se restableció correctamente.
Ruta de acceso se restableció correctamente.
Error al restablecer .
Acceso denegado.

 se restableció correctamente.
Reinicie el equipo para completar esta acción.


C:\Windows\system32>ipconfig /flushdns
```

```
Configuración IP de Windows
Se vació correctamente la caché de resolución de DNS.
```