Instalación y configuración del Zentyal Server 6.0 servicios de VPN.

James Fabian Lopez Manjarres; 1121869087.
Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI. Colombia
James.lopez@live.com

Resumen- Este documento presenta la instalación y puesta en marcha del servidor Zentyal en su versión 5.0 para dar solución a diferentes problemas de migración e infraestructura en tecnologías de información, enfocados en situaciones más complejas a niveles internos o externos de la red. Sobre el servidor Zentyal, se implantarán servicios como DNS, DHCP, Controladores de dominio, Firewall, Proxy no Transparente y VPN como solución a un entorno profesional de networking.

Abstract— This document presents the installation and start-up of the Zentyal server in its version 5.0 to solve different migration and infrastructure problems in information technologies, focused on more complex situations at internal or external levels of the network. On the Zentyal server, services such as DNS, DHCP, Domain Controllers, Firewall, Non-Transparent Proxy and VPN will be implemented as a solution to a professional networking environment.

Palabras clave - Zentyal, Firewall, DHCP Server, DNS Server, VPN, Controlador de Dominio, Proxy, Implementación, Servidor.

I. Introducción

Zentyal server es un sistema operativo que permite instalar diferentes servicios en servidor tales como Firewall, DHCP Server, DNS Server, VPN, Controlador de Dominio, Proxy, entre otros que además cuenta con un excelente controlador de dominio para sistemas operativos Linux. Este articulo pretende ilustrar y explicar la instalación de este sistema operativo e implantar diferentes servicios como Firewall, DHCP Server, DNS Server, VPN, Controlador de Dominio, Proxy, entre otros sobre una red de equipos Linux y a su vez administrar grupos y usuarios que permitan la vinculación de los mismos sobre un dominio configurado en Zentyal.

II. Zentyal Server 6.0

A. Requerimientos

Zentyal Server funciona sobre un hardware estándar bajo arquitectura x86 (64-bit), dependiendo del perfil de uso que se le quiera dar sus requerimientos pueden variar, pero por lo general un procesador de doble núcleo, 2GB de memoria RAM y 8GB de disco duro.

B. Url de Descarga.

Para iniciar con el desarrollo de esta actividad descargamos el Zentyal Server 6.0

Para esto en el link http://www.zentyal.org/server/ descargamos la versión Development Edition.

C. Temáticas.

Esta actividad se divide en 5 temáticas las cuales plantean la configuración y funcionamiento de varios servicios de red sobre una plataforma Zentyal Server.

Para comprobar el funcionamiento de estas temáticas se cuenta con un equipo cliente bajo la plataforma Sistema Operativo Ubuntu, la cual se encuentra bajo la misma red que el servidor Zentyal.

Las temáticas se muestran a continuación:

Tabla 1

#	Temática
5	VPN

DESARROLLO ACTIVIDAD

PLANTEAMIENTO Y CONTEXTUALIZACIÓN DEL PROBLEMA A RESOLVER:

Solucionada gran parte de las problemáticas de migración de sus sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, se entra en la fase final de la migración y puesta en marcha de los servicios solicitados.

El trabajo final que cada estudiante debe desarrollar en esta fase, se orienta a la administración y control de una distribución GNU/Linux basada en Ubuntu, pero enfocada a la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas.

Cada integrante de grupo participante en la actividad, debe seleccionar una (1) de las cinco (5) temáticas que encontrará a continuación. Entregará un informe técnicamente muy bien documentado que contenga el desarrollo o la solución del tema seleccionado, así:

Sistema operativo bajo el cual se implementaras los servicios y plataformas:

GNU/Linux Zentyal Server 5.0 (Instalar y configurar Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT).

TEMÁTICA 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

¿QUE ES ZENTYAL SERVER?

Zentyal es una solución de correo electrónico y groupware de código abierto, compatible de forma nativa con Microsoft Outlook®. Zentyal implementa protocolos Microsoft® Exchange sobre componentes estándares de código abierto (como Dovecot, Postfix, Samba, etc.) para proporcionar compatibilidad nativa con clientes Microsoft Outlook®. Los protocolos de correo electrónico y groupware

soportados por Zentyal son MAPI, ActiveSync, EWS, SMTP, POP, IMAP, CalDAV, CardDAV y Active Directory.

Zentyal se distribuye en dos paquetes: Zentyal Server para PYMEs y Zentyal Cloud para proveedores de hosting. Zentyal Server tiene una edición de desarrollo que puede descargarse de forma gratuita y cuyo código fuente está disponible bajo los términos de la GNU General Public License.

LISTA COMPLETA DE CARACTERÍSTICAS TÉCNICAS ZENTYAL 6.0

Tabla 2

Dominio & Directorio	*Gestión central del dominio y directorio* *Usuarios, Grupos de seguridad, Listas de Distribución, Contactos* *Múltiples Unidades Organizativas (OUs), Objetos de Directiva de Grupo (GPOs)* *Scripts NETLOGON, Perfiles móviles* *Autenticación Single Sign-On (SSO)* *SO soportados: Windows® XP/Vista/7/8/10* *Compartición de ficheros en entornos Windows® (CIFS)* *Permisos de acceso y modificación de Usuarios & Grupos (ACLs)* *Gestión de fotos de perfil* *Software integrado: Samba*
Correo	*Protocolos soportados: SMTP, POP3, IMAP, CalDAV, CardDAV, SIEVE* *Clientes soportados: Mozilla Thunderbird®* *Webmail* *Sincronización con dispositivos móviles via ActiveSync* *Múltiples dominios virtuales de correo* *Autenticación Single Sign-On (SSO)* *Administración a través de Zentyal o Microsoft® Active Directory* *Antivirus & Mail filter* *Software integrado: Postfix, Dovecot, Fetchmail, Sieve, SOGo, SOGo ActiveSync, Amavis, ClamAV, SpamAssasin*
Gateway	*Configuración de red* *Encaminamiento* *Gateway* *Cortafuegos* *Servicio de autenticación de red (RADIUS)* *HTTP Proxy* *IDS/IPS* *Autenticación de usuarios en HTTP Proxy* *Bloqueo de páginas web HTTPS basado en dominio* *Integrated software: Iproute2, Netfilter, Squid, Suricata, FreeRADIUS*
Infraestructura	*Servidor DHCP, DNS* *Servidor NTP* *Autoridad de Certificación (CA)* *Virtualization Manager* *Redes Privadas Virtuales (VPNs)* *Backup* *Servicio de Mensajería Instantánea (IM)* *Servidor FTP* *IPSec/L2TP* *Antivirus con análisis de ficheros en acceso* *Integrated software: BIND, ISC DHCP Software, ntpd, OpenSSL, OpenVPN, ejabbered, Libvirt/KVM, Duplicity, vsftpd, Libreswan*
Soporte & Actualizaciones	*Actualizaciones de software y de seguridad* *Actualizaciones entre versiones* *Acceso a la base de conocimiento* *Soporte técnico*

ANTES DE EMPEZAR LOS REQUISITOS DE HARDWARE PARA TENER EN CUENTA:

Zentyal funciona sobre hardware estándar de arquitectura x86_64 (64-bit). Sin embargo, es conveniente asegurarse de que Ubuntu Bionic 18.04.1 LTS (kernel 4.15) es compatible con el equipo que se vaya a utilizar. Se debería poder obtener esta información directamente del fabricante. De no ser así, se puede consultar en la lista de compatibilidad de hardware de Ubuntu Linux , en la lista de servidores certificados para Ubuntu 18.04.1 LTS o buscando en Google.

Los requerimientos de hardware para un servidor Zentyal dependen de los módulos que se instalen, de cuántos usuarios vayan a utilizar los servicios y de sus hábitos de uso.

Algunos módulos tienen bajos requerimientos, como Firewall, DHCP o DNS, pero otros como el Filtrado de correo o el Antivirus necesitan más memoria RAM y CPU. Los módulos de Proxy y Compartición de ficheros mejoran especialmente su rendimiento con discos rápidos debido al uso intensivo de E/S que realizan.

Es bueno tener en cuenta que una configuración RAID añade un nivel de seguridad frente a fallos de disco duro y aumenta la velocidad en operaciones de lectura.

Si usas Zentyal como puerta de enlace o cortafuegos necesitarás al menos dos tarjetas de red, pero si lo usas como un servidor independiente, una única tarjeta de red será suficiente. Si tienes dos o más conexiones de Internet puedes tener una tarjeta de red para cada router o conectarlos a una tarjeta de red teniéndolos en la misma subred. Otra opción es configurar segmentos VLAN.

Por otro lado, siempre es recomendable tener un SAI con tu servidor.

Para un servidor de uso general con los patrones de uso normales, los requerimientos siguientes serían los mínimos recomendados:

PERFIL DE ZENTYAL	USUARIOS	CPU	MEMORIA	DISCO	TARJETAS DE RED
Puerta de acceso	<50	P4 o superior	2G	80G	2 ó más
	50 ó más	Xeon Dual core o superior	4G	160G	2 ó más
Infraestructura	<50	P4 o superior	1G	80G	1
	50 ó más	P4 o superior	2G	160G	1
Oficina	<50	P4 o superior	1G	250G	1
	50 ó más	Xeon Dual core o superior	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Fig. 1, Tabla de requisitos hardware.

Si se combina en una sóla máquina más de un perfil se deberían aumentar los requerimientos. Si se está desplegando Zentyal en un entorno con más de 100 usuarios debería hacerse un análisis detallado, incluyendo patrones de uso, tras un benchmarking y considerando estrategias de alta disponibilidad

PASO A PASO, PARA LA DESCARGA ZENTYAL SERVER 6.0

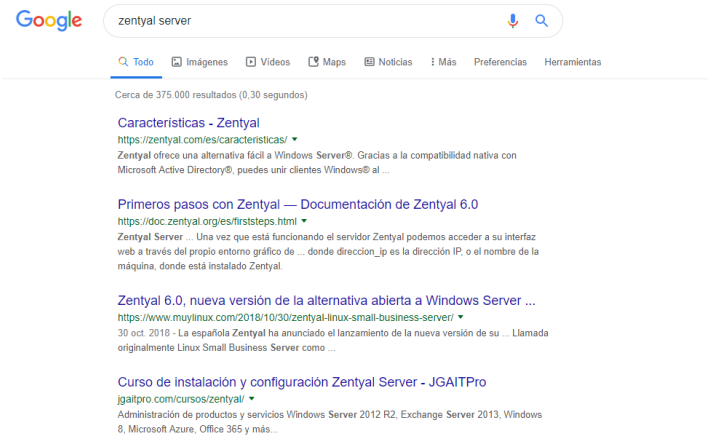

Fig. 2, Se realiza la búsqueda en el navegador de preferencia, en este caso google Chrome.

Fig. 3, Ingresamos a la página oficial de zentyal, posteriormente damos clic en comenzamos un trial gratuito.

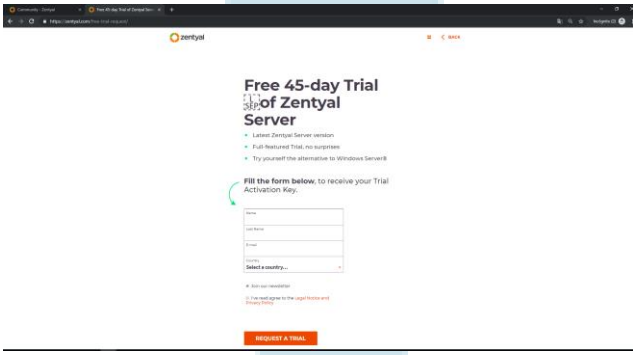

Fig. 4, Nos aparece el siguiente formulario.

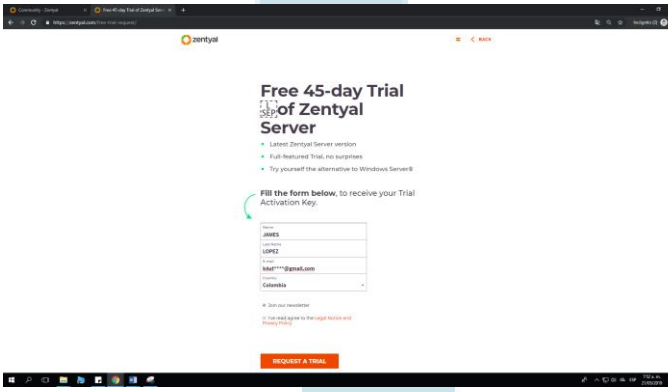

Fig. 5, Lo diligenciamos con los datos pertinentes.

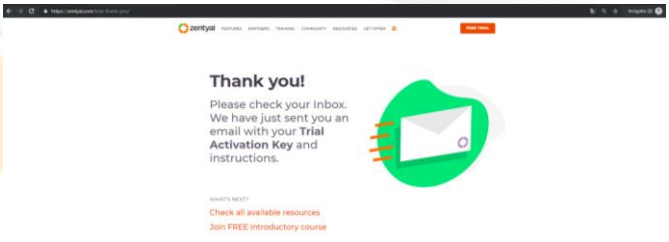

Fig. 6, Cuando finaliza la suscripción, nos envía un mensaje al correo ingresado.

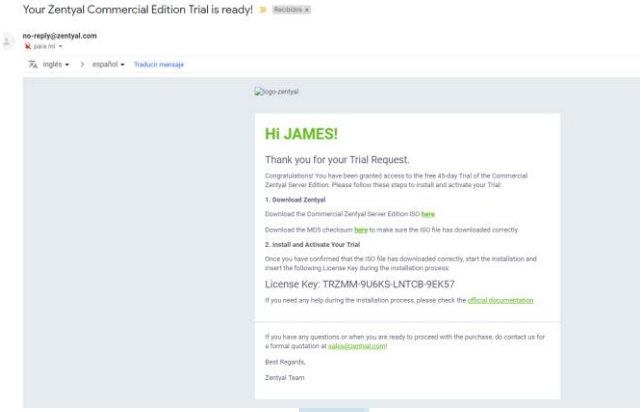

Fig. 7, En el correo, nos envían la siguiente información (descarga de zentyal, a su vez nos envían un código de licencia, recordar que es trial por cierto tiempo).

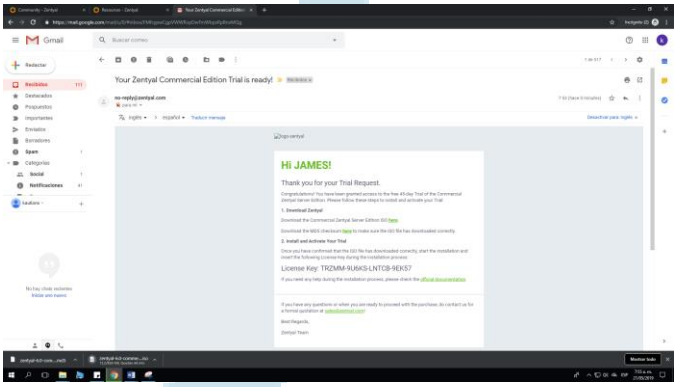

Fig. 8, En la parte inferior, se refleja los archivos a descargar.

INSTALACIÓN Y CONFIGURACION ZENTYAL

Zentyal está concebido para ser instalado en una máquina (real o virtual) de forma, en principio, exclusiva. Esto no impide que se pueda instalar cualquier otro servicio o aplicación adicional, (no gestionado a través de la interfaz de Zentyal), que deberá ser instalado y configurado manualmente.

Zentyal funciona sobre la distribución de GNU/Linux Ubuntu en su versión para servidores, usando siempre las ediciones LTS (Long Term Support), con cinco años de soporte.

- ✓ La instalación puede realizarse de dos maneras diferentes:
- ✓ Usando el instalador de Zentyal (opción recomendada),
- ✓ Instalando Zentyal sobre una distribución Ubuntu Server Edition.

En el segundo caso es necesario añadir los repositorios oficiales de Zentyal y tras actualizar los paquetes disponibles, proceder a la instalación de aquellos módulos que se deseen.

El primer método facilita la instalación y el despliegue de Zentyal ya que todas las dependencias se encuentran en un sólo DVD o USB y además se incluye un entorno gráfico que permite usar el interfaz web desde el propio servidor.

Es recomendable tener disponible una conexión a internet durante la instalación de Zentyal, de este modo se instalarán automáticamente las actualizaciones mas recientes.

- ✓ El instalador de Zentyal
- ✓ El instalador de Zentyal está basado en el instalador de Ubuntu Server así que el proceso de instalación resultará muy familiar a los usuarios de dicha distribución.

IMPORTANTE

Los pasos que se muestran a continuación son idénticos para todas las ediciones de Zentyal, pero en caso de que estemos instalando una edición comercial, habrá un paso adicional en el que tendremos que introducir una clave de licencia válida (obtenida al comprar dicha edición), en caso contrario la instalación no podrá continuar.

En primer lugar, seleccionaremos el lenguaje de la instalación, para este ejemplo usaremos Español.

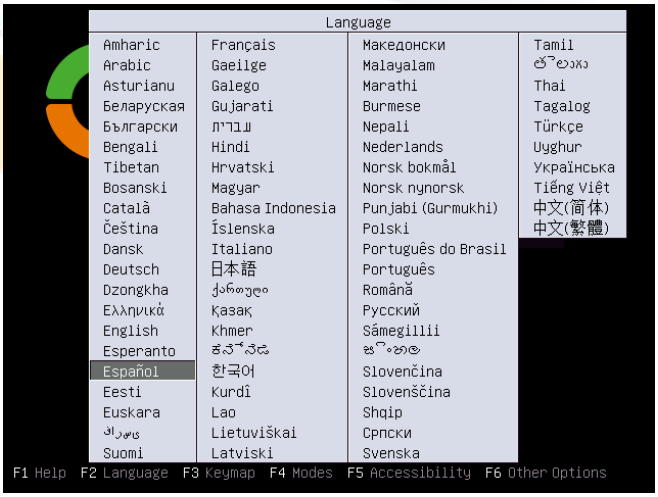

Fig. 9, Selección del idioma.

Podemos instalar utilizando la opción por omisión que elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal usando LVM o podemos seleccionar la opción expert mode que permite realizar un particionado personalizado. La mayoría de los usuarios deberían elegir la opción por omisión a no ser que estén instalando en un servidor sobre RAID por software o quieran hacer un particionado más acorde con sus necesidades concretas.

Usando el modo experto se puede realizar una instalación que no incluya el entorno de escritorio local.

Fig. 10, Inicio del instalador.

En el siguiente paso elegiremos la configuración local de nuestro sistema. Para ello escogemos el país en que nos encontramos, en este caso COLOMBIA.

Fig. 11, Localización geográfica.

Podemos usar la detección automática de la distribución del teclado, que comprueba el mapeado de ciertas teclas, o podemos seleccionarlo en un listado que nos presentará el sistema al seleccionar No.

Fig. 12, Autodetección del teclado.

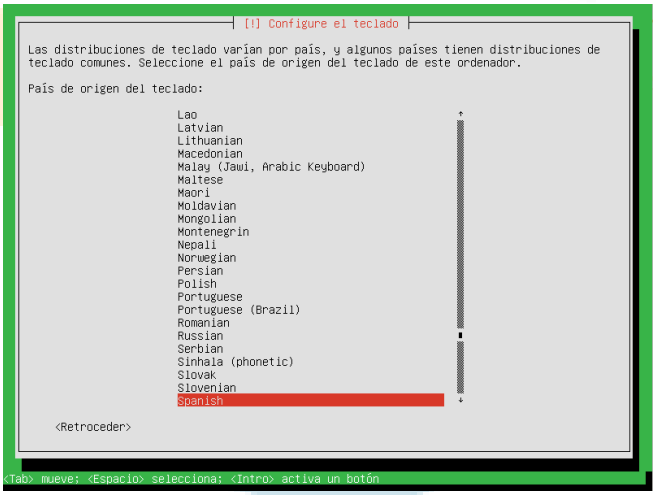

Fig. 13, Selección del teclado 1.

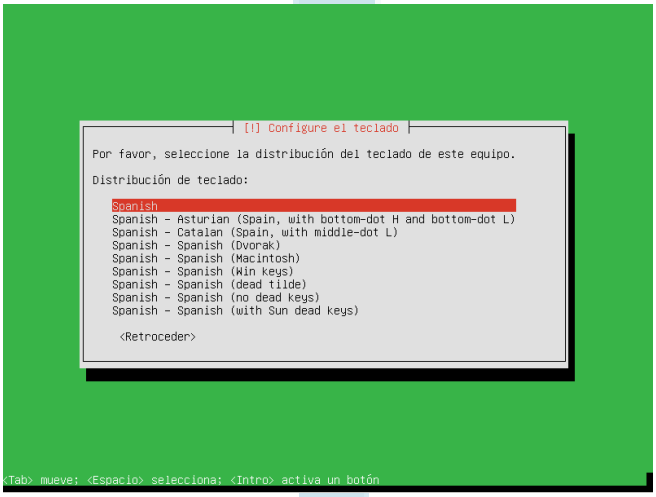

Fig. 14, Selección del teclado 2.

A continuación, el instalador procederá a configurar la red. En caso de que dispongamos de más de una interfaz deberemos especificar cuál usaremos durante la instalación, (para descargar actualizaciones, por ejemplo). Si sólo tenemos una interfaz de red el proceso se realizará de manera transparente.

Fig. 15, Selección de interfaz de red.

Después elegiremos el nombre de nuestro servidor o hostname. El hostname identifica la máquina dentro de la red y es utilizado por muchos de los servicios. El módulo DNS de Zentyal, por ejemplo, introducirá automáticamente este nombre en el correspondiente registro de BIND y Samba también lo usa como identificador.

Fig. 16, Nombre de la máquina.

Una vez establecido el 'hostname', pasaremos a configurar la cuenta del administrador del sistema. Este usuario tiene pleno acceso a la máquina y sus recursos y puede también acceder a la interfaz de administración de Zentyal.

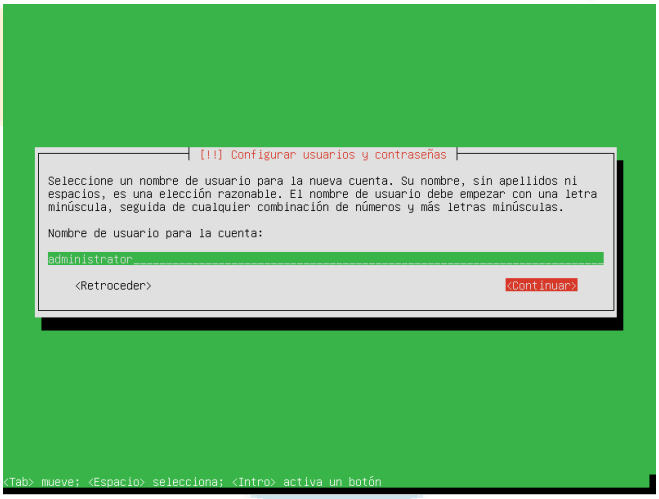

Fig. 17, Usuario administrator.

Terminaremos la configuración del usuario administrador estableciendo su contraseña. Debemos ser especialmente cuidadosos y elegir una contraseña segura (más de 12 carácteres incluyendo letras, cifras y símbolos de puntuación).

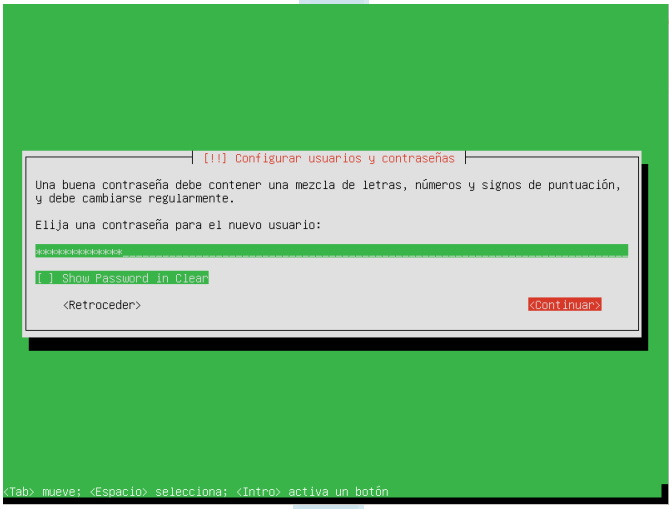

Fig. 18, Contraseña.

El sistema se asegura de que hemos tecleado correctamente la contraseña solicitando que la escribamos de nuevo.

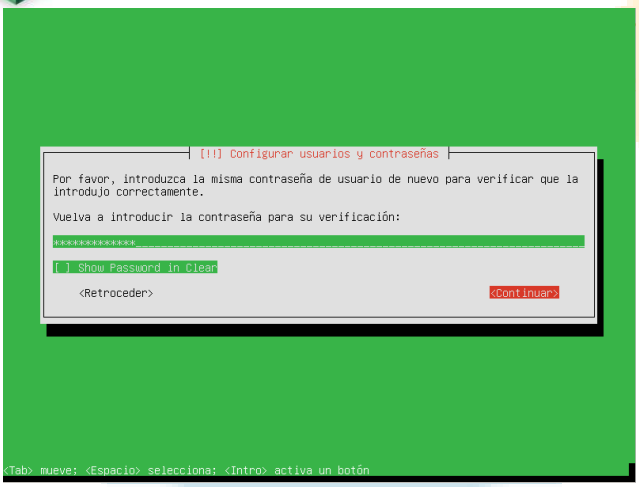

Fig. 19, Confirmar contraseña.

Configurado el usuario administrador, el sistema pasará a establecer los parámetros locales, para lo que nos solicitará que confirmemos la zona horaria en que operará el servidor.

Fig. 20, Zona horaria.

Esperaremos a que nuestro sistema básico se instale, mientras muestra una barra de progreso. Este proceso puede durar unos 20 minutos aproximadamente, dependiendo del servidor en cada caso.

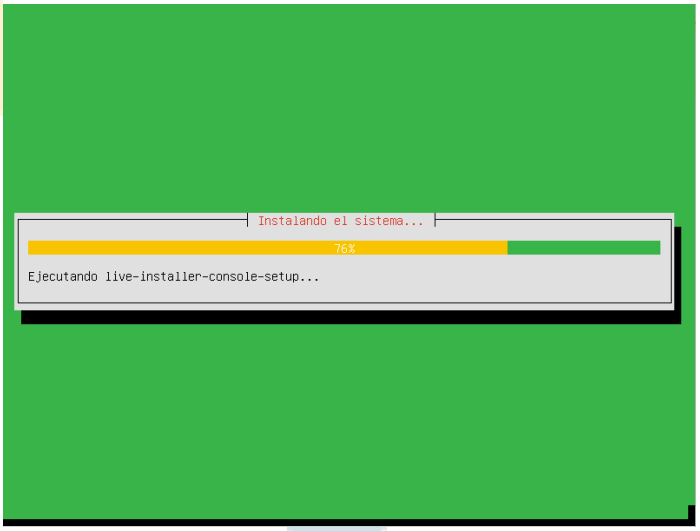

Fig. 21, Instalación del sistema base.

La instalación del sistema base está completada; ahora podremos extraer el disco de instalación y reiniciar.

Fig. 22, Reiniciar.

¡Nuestro sistema Zentyal está instalado!

El sistema arrancará una aplicación web de administración a la que podremos acceder, local o remotamente, mediante nuestro navegador. Aunque tras el primer reinicio el sistema haya iniciado la sesión de usuario automáticamente, de aquí en adelante, necesitará autenticarse antes de hacer login en el sistema. El primer arranque tomará algo más de tiempo, ya que necesita configurar algunos paquetes básicos de software.

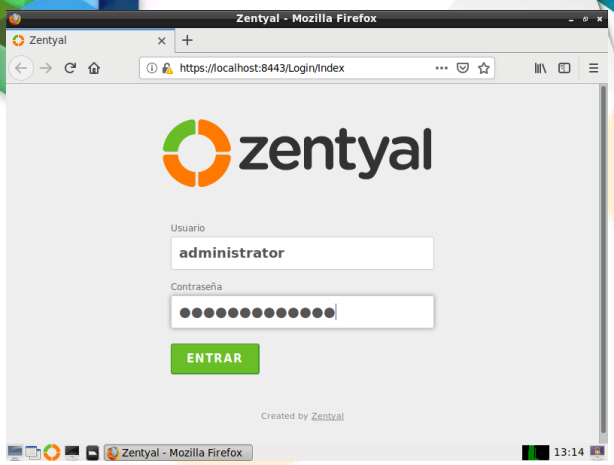

Fig. 23, Entorno gráfico con el interfaz de administración

Usaremos el usuario y contraseña indicados durante la instalación. Cualquier otro usuario que añadamos posteriormente al grupo sudo podrá acceder al interfaz de Zentyal al igual que tendrá privilegios de superusuario en el sistema.

Configuración inicial

Cuando se accede a la interfaz por primera vez aparecerá una pantalla de presentación mostrando los diferentes pasos del asistente.

Fig. 24, Presentación de los pasos del wizard

Una vez autenticado en la interfaz web comienza, durante este primer uso, un asistente de configuración. En primer lugar podremos seleccionar qué funcionalidades queremos incluir en nuestro sistema. Como algunos componentes dependen de otros, Zentyal debe administrar esas dependencias instalando automáticamente los modulos necesarios para el funcionamiento del que hemos escogido. Siempre se podrá instalar, desinstalar y actualizar mas adelante cualquiera de los componentes desde la interfaz del servidor.

En este ejemplo instalaremos Domain Controller and File Sharing, Mail and Groupware y Firewall.

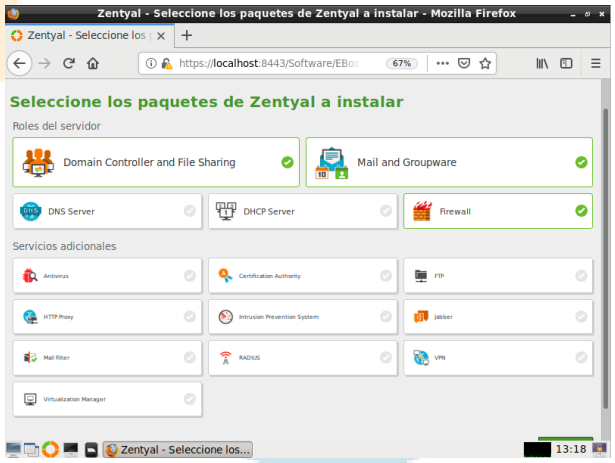

Fig. 25, Perfiles y paquetes instalables.

Zentyal te informará de la instalación de las dependencias que serán necesarias para el módulo selecionado anteriormente.

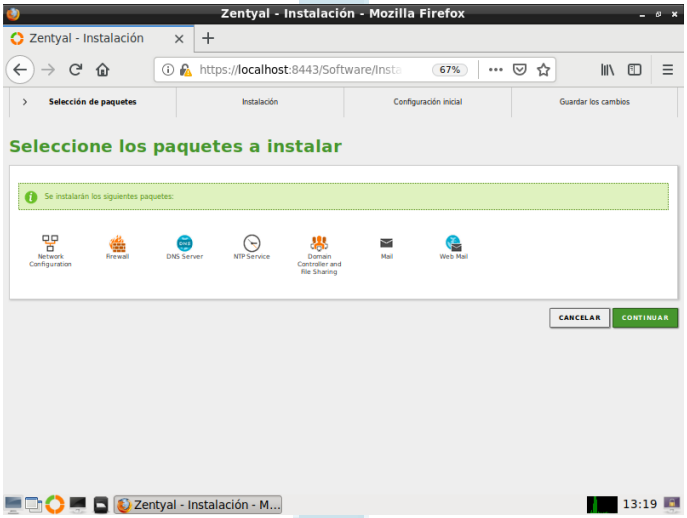

Fig. 26, Paquetes adicionales.

El sistema comenzará con el proceso de instalación de los módulos requeridos, mostrando una barra de progreso donde además podemos leer una breve introducción sobre las funcionalidades y servicios adicionales disponibles en Zentyal Server y los paquetes comerciales asociados.

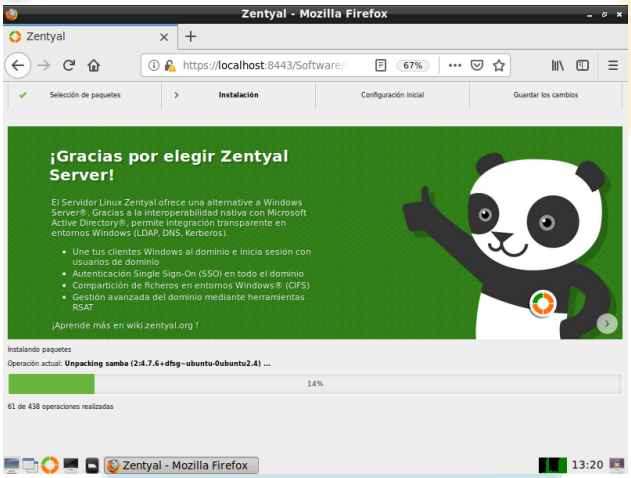

Fig. 27, Instalación e información adicional.

Una vez terminado el proceso de instalación se solicitará información sobre la configuración de red, definiendo cada interfaz de red como interna o externa. Es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local. Si se va a usar Zentyal como servidor DHCP se recomienda usar configuración estática.

Fig. 28, Configurar los tipos de interfaces de red.

Posteriormente podremos establecer diversos paramétros de configuración: ip asignada por DHCP o estática, IP asociada, etc. Estos parámetros pueden ser reconfigurados desde el interfaz de Zentyal en cualquier otro momento.

La siguiente pantalla que nos aparecerá sirve para configurar las interfaces del sistema:

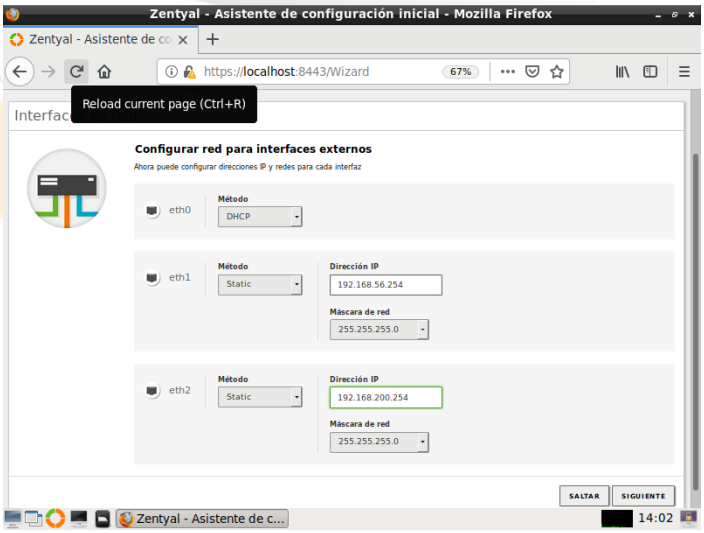

Fig. 29, Configurar las interfaces de red.

Definidas las interfaces de red, tenemos que configurar nuestro dominio y el tipo de 'Domain Controller' que queremos levantar. Zentyal puede funcionar en dos modos:

Servidor stand-alone: como primer controlador de dominio.

Controlador de dominio adicional: uniéndose a un dominio existente como controlador de dominio adicional.

Para simplificar, en este ejemplo, usaremos el modo 'stand-alone'. Para obtener más información acerca de los otros modos de 'Active Directory' ir a Controlador de Dominio y Compartición de ficheros.

Para configurar este modo, tan sólo hay que especificar el nombre de dominio de tus entidades de directorio. No debe confundirse con el dominio de nombres (DNS), que aunque está relacionado, se usa en un contexto diferente.

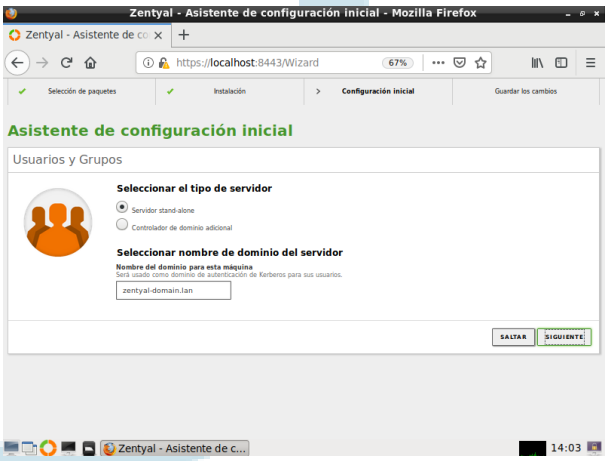

Fig. 30, Configurar dominio local del servidor.

En el siguiente paso seleccionaremos el dominio virtual de correo. Por defecto se usa el nombre de dominio escogido en el paso anterior pero puedes especificar el que desees.

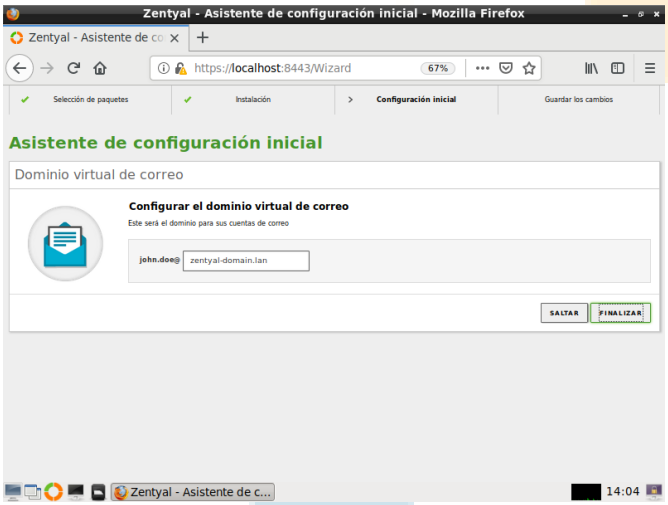

Fig. 31, Dominio de correo electrónico.

Finalmente se procede a la configuración de cada uno de los módulos instalados.

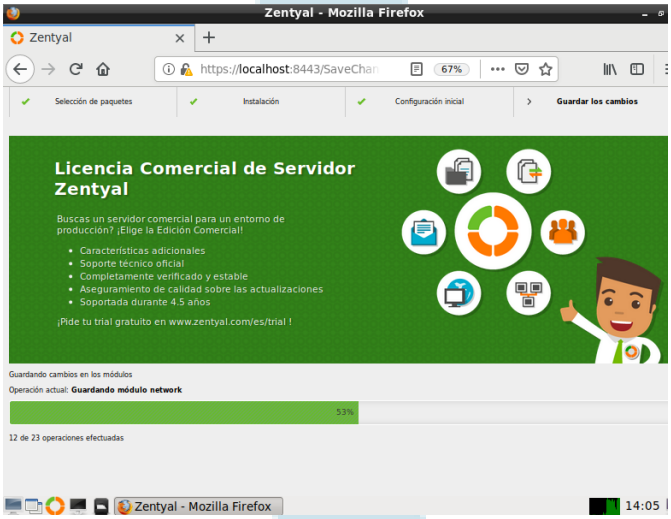

Fig. 32, Configuración inicial finalizada.

El instalador nos avisará cuando haya terminado el proceso.

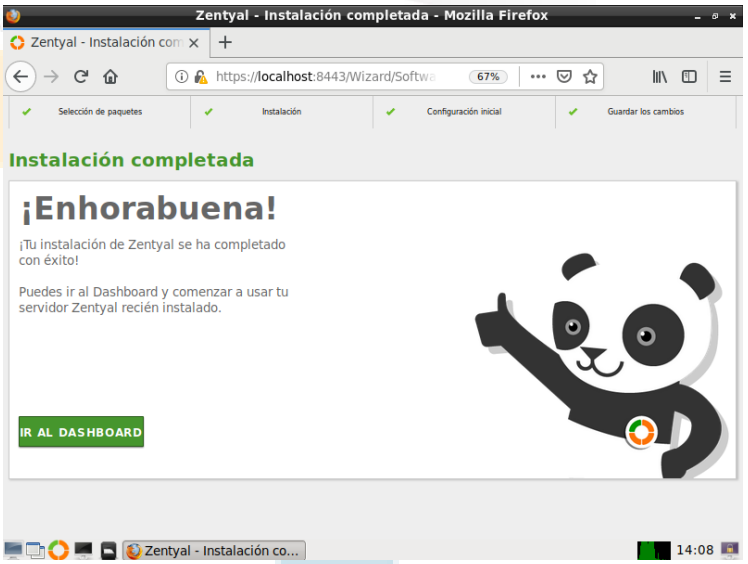

Fig. 33, Guardando cambios.

Ya podemos acceder al Dashboard y a la configuración específica de cada uno de los componentes. En el siguiente capítulo veremos los conceptos básicos y el funcionamiento de la interfaz de Zentyal.

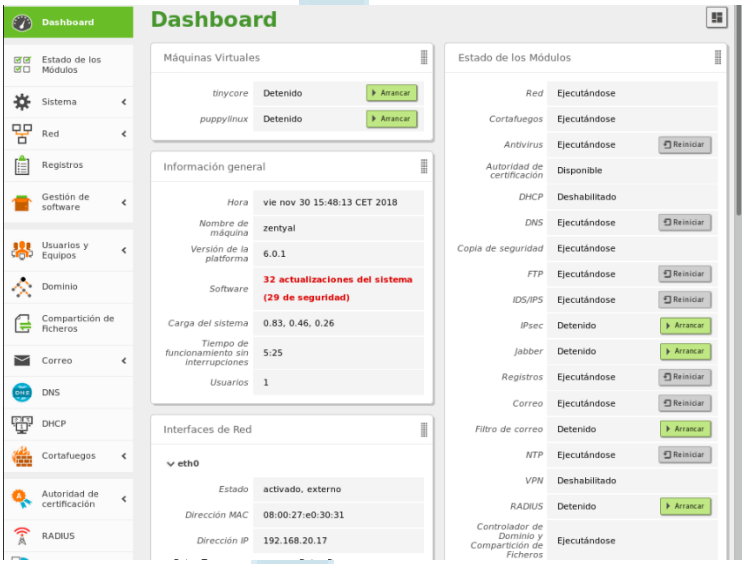

Fig. 34, Interfaz Dashboard.

IMPLEMENTACIÓN Y CONFIGURACIÓN DETALLADA DE LA CREACIÓN DE UNA VPN

PRIMERO DEBEMOS REALIZAR LA AUTORIDAD DE CERTIFICACIÓN (CA)

Zentyal integra OpenSSL®, para la gestión de la Autoridad de Certificación y del ciclo de vida de los certificados expedidos por esta.

CONFIGURACIÓN DE UNA AUTORIDAD DE CERTIFICACIÓN CON ZENTYAL

En Zentyal, el módulo Autoridad de Certificación es autogestionado, lo que quiere decir que no necesita ser habilitado en Estado de los Módulos como el resto sino que para comenzar a utilizar este servicio hay que inicializar la CA. Las funcionalidades del módulo no estarán disponibles hasta que no hayamos efectuado esta acción.

Accederemos a Autoridad de Certificación ‣ General y nos encontraremos con el formulario para inicializar la CA. Se requerirá el Nombre de Organización y el número de Días para expirar. Además, también es posible especificar opcionalmente Código del País (acrónimo de dos letras que sigue el estándar ISO-3166-1 [5]), Ciudad y Estado.

Fig. 35, Creando la Autoridad de Certificación.

A la hora de establecer la fecha de expiración hay que tener en cuenta que en ese momento se revocarán todos los certificados expedidos por esta CA, provocando la parada de los servicios que dependan de estos certificados.

Una vez que la CA ha sido inicializada, ya podremos expedir certificados. Los datos necesarios son el Nombre Común del certificado y los Días para Expirar. Este último dato está limitado por el hecho de que ningún certificado puede ser válido durante más tiempo que la CA. En el caso de que estemos usando estos certificados para un servicio como podría ser un servidor de correo, el Nombre Común deberá coincidir con el nombre de dominio del servidor. Por ejemplo, si utilizamos el nombre de dominio hq.zentyal.org para acceder al interfaz de administración web de Zentyal, será necesario un certificado con ese Nombre Común. En el caso de que el certificado sea un certificado de usuario, usaremos normalmente su dirección de correo como Nombre Común.

Opcionalmente se pueden definir Subject Alternative Names para el certificado. Estos sirven para establecer nombres comunes a un certificado, como una dirección de correo para firmar los mensajes de correo electrónico.

Advertencia

Todo certificado que expida la CA recién creada no será reconocido por software de terceros, como navegadores web o clientes de correo. Esto es debido a que la CA no es oficial, no obstante, a pesar de poder obtener mensajes como el de la siguiente imagen, el tráfico estará cifrado.

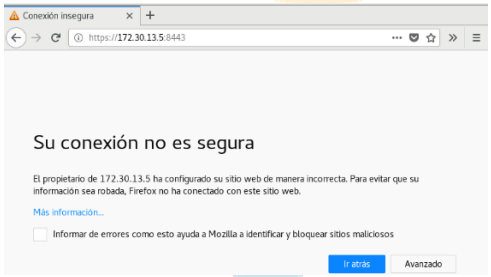

Fig. 36, Mensaje de un navegador web.

Consejo: LetsEncrypt, es una entidad certificadora gratuita que permite generar certificados reconocidos, por lo que si tu infraestructura requiere de tener certificados reconocidos, os recomendamos que sigáis este link [8] para su implementación en el servidor Zentyal.

Una vez el certificado haya sido creado, aparecerá en la lista de certificados, estando disponible para el administrador y el resto de módulos. A través de la lista de certificados podemos realizar distintas acciones con ellos:

- ✓ Descargar las claves pública, privada y el certificado.
- ✓ Renovar un certificado.
- ✓ Revocar un certificado.
- ✓ Reexpedir un certificado previamente revocado o caducado.

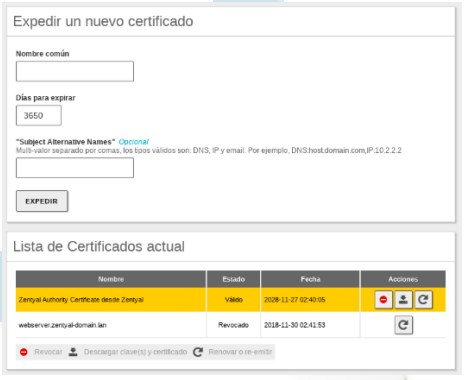

Fig. 37, Listado de certificados.

El paquete con las claves descargadas contiene también un archivo PKCS12 que incluye la clave privada y el certificado y que puede instalarse directamente en otros programas como navegadores web, clientes de correo, etc.

Si renovamos un certificado, el actual será revocado y uno nuevo con la nueva fecha de expiración será expedido. Y si se renueva la CA, todos los certificados se renovarán con la nueva CA tratando de mantener la antigua fecha de expiración. Si esto no es posible debido a que es posterior a la fecha de expiración de la CA, entonces se establecerá la fecha de expiración de la CA.

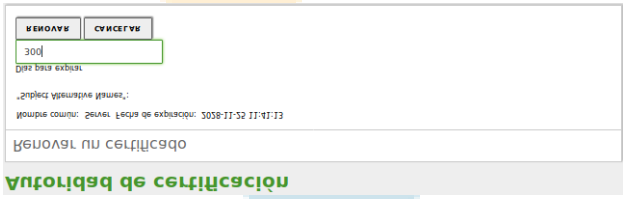

Fig. 38, Renovar un certificado.

Si revocamos un certificado no podremos utilizarlo más, ya que esta acción es permanente y no se puede deshacer. Opcionalmente podemos seleccionar la razón para revocarlo:

- ✓ **unspecified:** motivo no especificado,
- ✓ **keyCompromise:** la clave privada ha sido comprometida,
- ✓ **CACompromise:** la clave privada de la autoridad de certificación ha sido comprometida,
- ✓ **affilliationChanged:** se ha producido un cambio en la afiliación de la clave pública firmada hacia otra organización,
- ✓ **superseded:** el certificado ha sido renovado y por tanto reemplaza al emitido,
- ✓ **cessationOfOperation:** cese de operaciones de la entidad certificada,
- ✓ **certificateHold:** certificado suspendido,
- ✓ **removeFromCRL:** actualmente sin implementar, da soporte a los CRL diferenciales, es decir, listas de certificados cuyo estado de revocación ha cambiado.

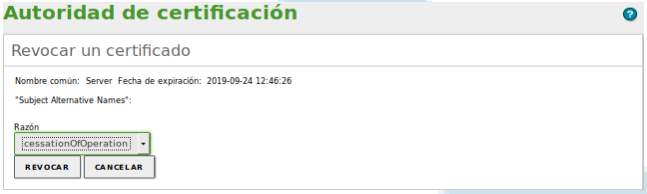

Fig. 39, Revocar un certificado, Cuando un certificado expire, el resto de módulos serán notificados. La fecha de expiración de cada certificado se comprueba una vez al día y cada vez que se accede al listado de certificados.

CERTIFICADOS DE SERVICIOS

En Autoridad de Certificación ‣ Certificados de Servicios podemos encontrar la lista de módulos de Zentyal que usan certificados para su funcionamiento. Cada módulo genera sus certificados autofirmados, pero podemos remplazar estos certificados por otros emitidos por nuestra CA.

Para cada servicio se puede generar un certificado especificando su Nombre Común. Si no existe un certificado con el nombre especificado, la Autoridad de Certificación lo creará automáticamente.

Fig. 40, Certificados de Servicios.

Una vez activado, tendremos que reiniciar el módulo sobre el que hemos activado el certificado para que lo comience a utilizar, al igual que si renovamos el certificado asociado.

Como hemos comentado anteriormente, para la versión segura de varios protocolos (como por ejemplo mail) es importante que el nombre que aparece en el Nombre común del certificado coincida con el nombre que ha solicitado el cliente. Por ejemplo, si nuestro certificado tiene como Nombre común hq.zentyal.org y el cliente teclea mail.hq.zentyal.org, su cliente le mostrará una alerta de seguridad y considerará que el certificado no es válido.

Lista de puntos a comprobar para desplegar un certificado:

- ✓ La autoridad de certificación ha sido creada, el módulo del servicio se ha instalado.
- ✓ Se ha creado un nombre en el DNS para el servicio (Registro A o CNAME), de tal forma que el cliente lo pueda resolver, por ejemplo 'hq.zentyal.org'.
- ✓ Se ha creado un certificado para el servicio específico, por ejemplo, servidor web con un Common Name que coincide con el DNS 'hq.zentyal.org', después de activar el certificado, podremos verlo en Autoridad de Certificación ‣ General.
- ✓ Se han configurado los protocolos seguros para el módulo de correo.
- ✓ Se ha importado el certificado de la CA (no el certificado del servicio específico) en el sistema o en la aplicación del cliente, por ejemplo el cliente de correo.

- ✓ El usuario configura su cliente de correo apuntando a hq.zentyal.org.
- ✓ El usuario es capaz de resolver la DNS a una dirección IP, el Common Name coincide perfectamente con su petición, y el certificado presentado por el servicio esta firmado por una autoridad de confianza.
- ✓ La aplicación del usuario es capaz de comenzar una sesión segura sin mostrar ningún aviso de seguridad

Servicio de redes privadas virtuales (VPN) con OpenVPN

Zentyal integra OpenVPN 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.

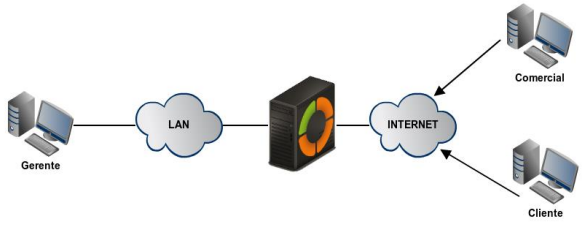

Fig. 41, Zentyal y clientes remotos de VPN.

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 expedirá este certificado automáticamente cuando cree un nuevo servidor VPN. En este escenario, Zentyal actúa como una Autoridad de Certificación.

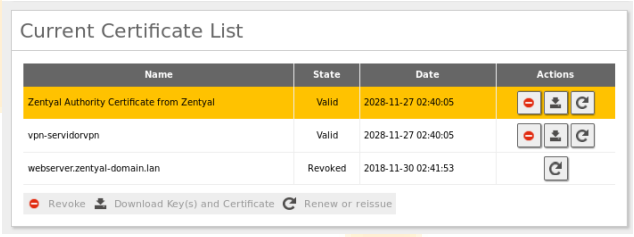

Fig. 42, Certificados expedidos en el servidor.

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.

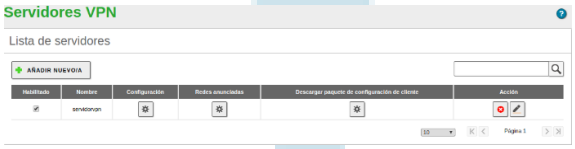

Fig. 43, Nuevo servidor VPN creado.

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.

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.

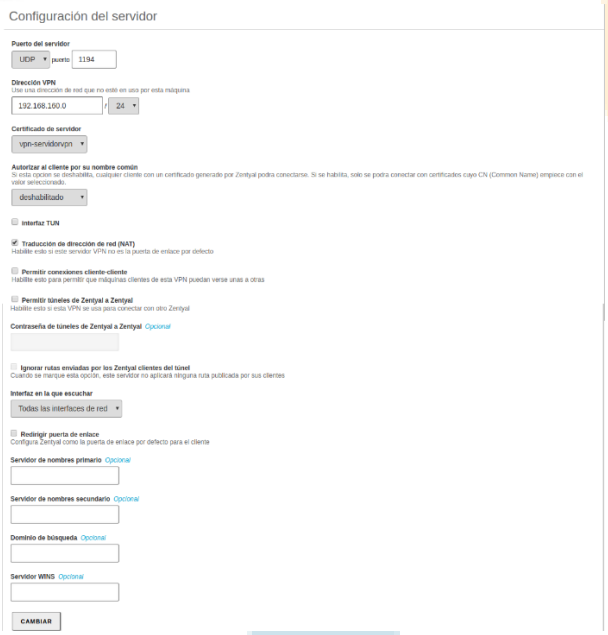

Fig. 44, Configuración de servidor VPN.

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 tal forma que los clientes de estas redes internas respondan al Zentyal de VPN en lugar de a su puerta de enlace. Si el servidor Zentyal es tanto servidor VPN como puerta de enlace (caso más habitual), es indiferente.

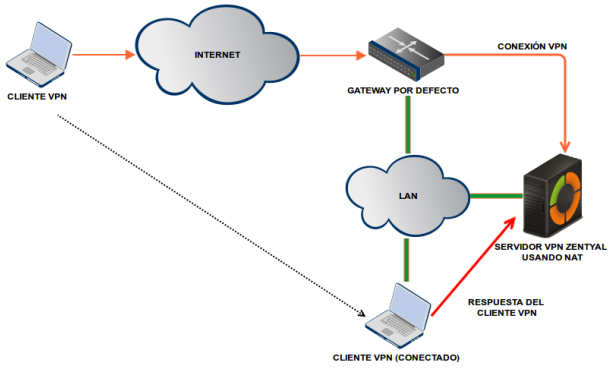

Fig. 45, Servidor VPN usando NAT para convertirse en la puerta de enlace por defecto.

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 Dashboard que un servidor VPN está funcionando.

Fig. 46, 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.

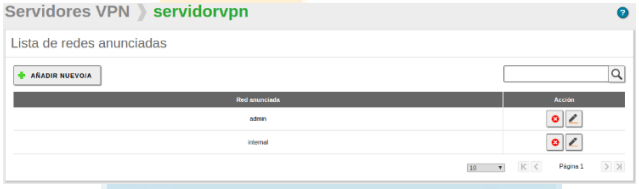

Fig. 47, Redes anunciadas para nuestro servidor VPN.

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, 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 columnaDescargar 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 intentaremos la conexión en orden o probaremos con uno 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.

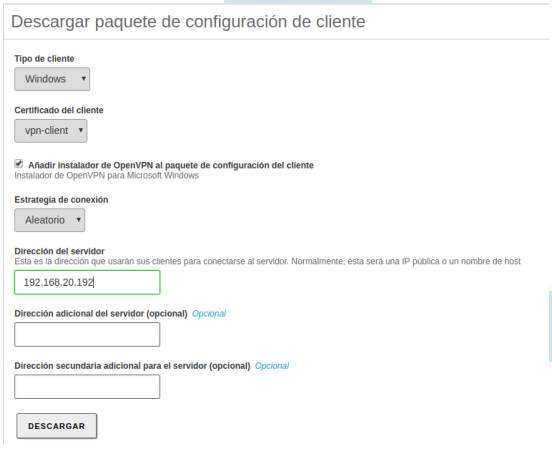

Fig. 48, Descargar paquete de configuración de cliente.

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.

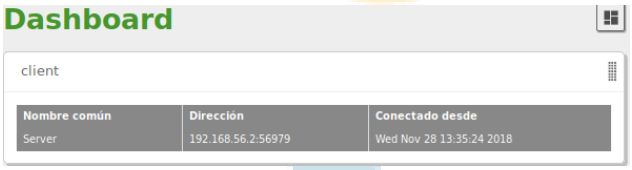

Fig. 49, Widget con clientes conectados.

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:

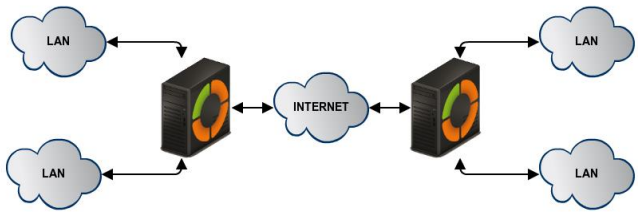

Fig. 50, Interconexión de sedes con Zentyal mediante túnel VPN.

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, 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. Hay que tener en cuenta que tendremos que anunciar las redes LAN en Redes anunciadas.

Otro 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.

Fig. 51, 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.

Fig. 52, 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.

Fig. 53, Dashboard de un servidor Zentyal configurado como cliente VPN.

La propagación de rutas puede tomar unos pocos minutos.

CONCLUSIONES

Zentyal server, es un servidor liviano, sencillo de instalar y fácil de configurar, ofrece al administrador de la red varias posibilidades gráficas para instalar diferentes servicios que funcionan de manera correcta como DHCP o DNS.

El acceso al Dominio creado en Zentyal server, requiere de una configuración previa del sistema operativo Ubuntu, en donde se hace necesario instalar los módulos de controlador de dominio, el cual permite la adición del equipo al dominio de Zentyal.

La instalación y configuración del Zentyal Server es muy sencilla e intuitiva, cumple con el propósito para el cual fue diseñado el cual es cumplir con las necesidades de una empresa, solo se debe prestar atención al momento de configurar las tarjetas de red ya que de estas depende el buen funcionamiento del sistema.

Ofrece un gran control del Firewall que permite una fácil administración, siendo muy sencillo la creación de reglas, es una muy buena opción evitar pagos.

BIBLIOGRAFÍA

Para realizar este trabajo, se consultaron las siguientes referencias:

[1] Wiki Zentyal. (2019). Instalación de Zentyal. Recuperado de: https://wiki.zentyal.org/wiki/Es/5.0/Instalacion
[2] Youtube. (2019). Parte III Configurar Zentyal DNS, Controlador de Dominio LDAP y Samba. Recuperado de: https://www.youtube.com/watch?v=-cCbsg5SDns
[3] Wiki Zentyal. (2019). Zentyal y DNS. Recuperado de: https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_resolucion_de_nombres_de_dominio_(DNS)
[4] How to setup OpenVPN Client, Louis Matthijssen (2017) Recuperado de: URL https://askubuntu.com/questions/460871/how-to-setup-openvpn-client
[5] Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN, Ricardo Rodríguez (2015) Recuperado de: URL https://www.youtube.com/watch?v=3rNfipxE-9o
[6] Connect VPN using OpenVPN on Ubuntu or Debian Linux, RicmediaPCHelp (2017) Recuperado de: URL https://www.youtube.com/watch?v=mc0nxWNwEDI