

Implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet a partir de Soluciones a necesidades específicas con GNU/Linux.

Dueñas Vega, Jhon Jairo.
jjduenasv@unadvirtual.edu.co
Hurtado Pico, Oscar Dustin.
odhurtadop@unadvirtual.edu.co
Mosquera Bonilla, Yhurleyver.
ymosquerabo@unadvirtual.edu.co
Organista, Edison Eduardo.
eeorganistam@unadvirtual.edu.co
Tibaduiza García, Nora Beatriz.
nbtibaduizag@unadvirtual.edu.co

RESUMEN: La seguridad es un aspecto que se trata en Linux como sistema operativo para brindar soluciones a gran parte de las problemáticas con respecto a migración y puesta en marcha de los sistemas de seguridad de la infraestructura de red por lo que este trabajo desarrolla la fase final del diplomado de Linux orientada a la administración y control de una distribución GNU/Linux como Zentyal Server y los servicios que este presta, ya que se enfoca en la ejecución de servicios de infraestructura IT para Intranet y Extranet por lo cual se tratan los aspectos de implementación y configuración detallada de acceso de una estación de trabajo GNU/Linux con el apoyo de un usuario y contraseña, por medio de estación en los servicios de Infraestructura IT de Zentyal para conectividad a Internet con restricciones de la apertura de sitios o portales Web evidenciando las reglas y políticas creadas por medio del cortafuego, controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras, tanto para VPN que permite establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux.

PALABRAS CLAVE: Administración, Infraestructura IT, seguridad de red.

1 INTRODUCCIÓN

Este artículo comprende los aspectos de implementación y puesta en marcha de un firewall o cortafuegos en un servidor Zentyal basado en Ubuntu 18.04, demostrando el funcionamiento bloqueando el acceso a sitios web identificando el origen y destino de las configuraciones de un servidor DHCP Server, DNS Server y Controlador de Dominio, proxy no transparente, cortafuegos, file server y print server y VPN partir de la asignación de las IP's en la red interna, y la red NAT o Network Address Translation (Traducción de Direcciones de Red) desde máquina virtual.

Correspondiente a la evaluación del tráfico que se puede dar dentro de una red para este aparte y como parte del proceso de necesidades específicas de Linux, tratando dichos temas del cual se desprende entre otros los lineamientos de restricción de acceso aun a usuarios dentro de la misma red, por lo que se apoya en la virtualización de sistemas como el Zentyal y creación de zona delimitada o DMZ, gestionando accesos a sitios web al interior y exterior de la red.

2 ASPECTOS PREVIOS PARA EL USO DE ZENTYAL

Una vez creada la máquina virtual en VirtualBox, se inicia para la instalación de Zentyal, se procede a la instalación del mismo y los componentes descritos a continuación.

2.1 CONFIGURACIÓN BÁSICA DE ZENTYAL.

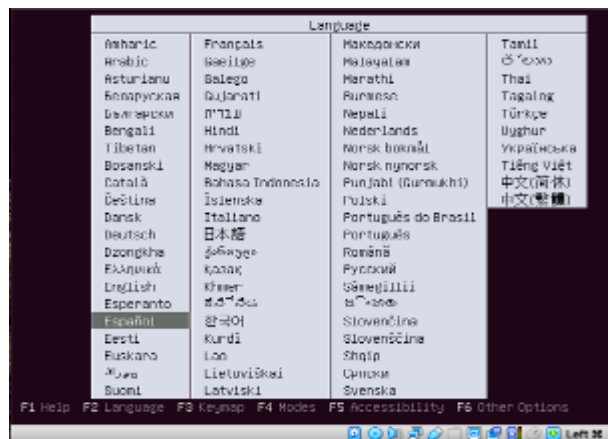


Figura 2.1.1. Selección de idioma

Seguidamente se elige la opción de instalar Zentyal [1, 3, 6, 8].

Solucionando necesidades específicas con GNU/Linux

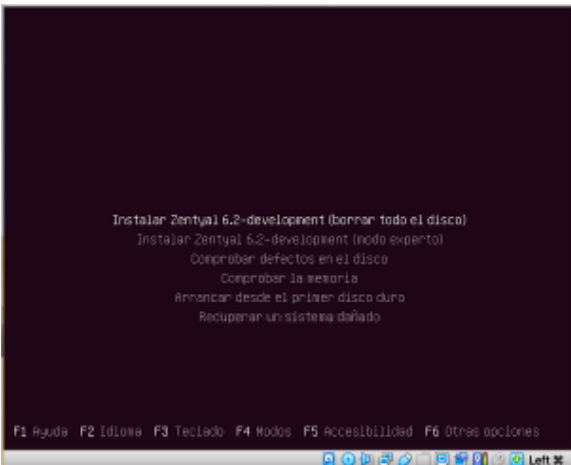


Figura 2.1.2. Selecciona instalar

Selecciona la ubicación territorial para la fijación de la zona horaria de la instalación.



Figura 2.1.3. Zona horaria

Selecciona el país de origen para la configuración del teclado, se elige español.

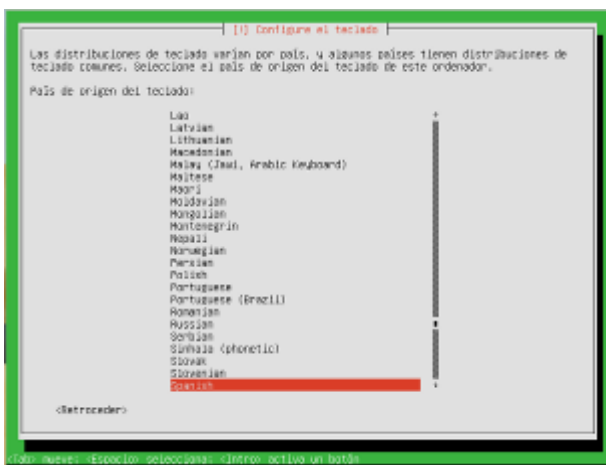


Figura 2.1.4. Configuración de teclado

Luego de haber realizado los pasos de configuración el sistema inicia a cargar los componentes.

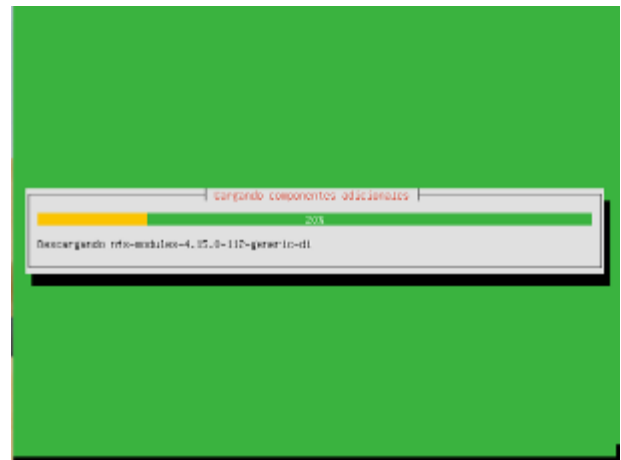


Figura 2.1.5. Cargando componentes

Después de que se carguen los componentes el sistema indica que se debe configurar la red, para este paso se elige el primer controlador de la red reconocida.

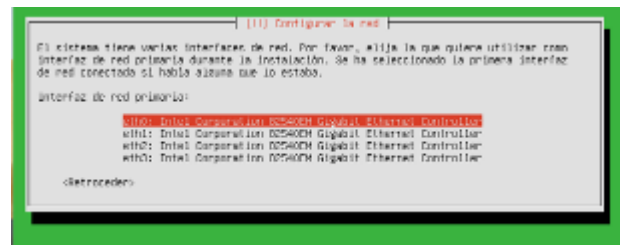


Figura 2.1.6. Configuración de red

Asigna nombre a la máquina, para este caso se deja como por defecto Zentyal.

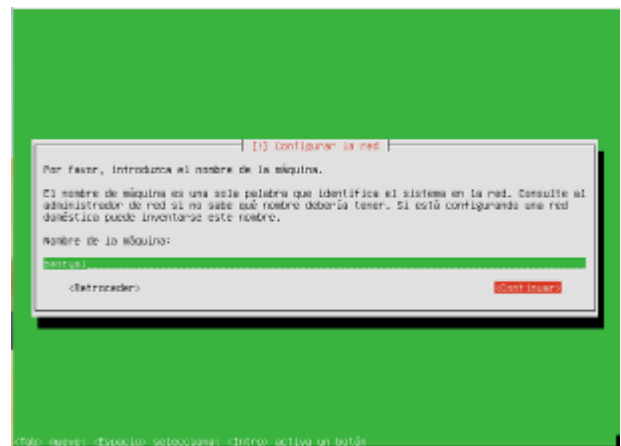


Figura 2.1.7. Asignación nombre a la máquina

De la misma manera se establece el nombre de usuario y contraseña al sistema.



Figura 2.1.8. Asignación nombre de usuario.

Para la asignación de la contraseña el sistema solicita dos veces el ingreso de contraseña, debe ingresarse la misma contraseña en los dos pasos sugeridos.

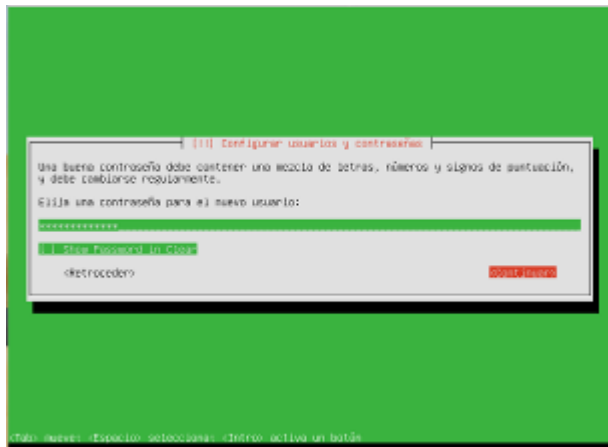


Figura 2.1.9. Asignación de contraseña.

El sistema inicia la instalación y nos informa que ha finalizado la instalación.

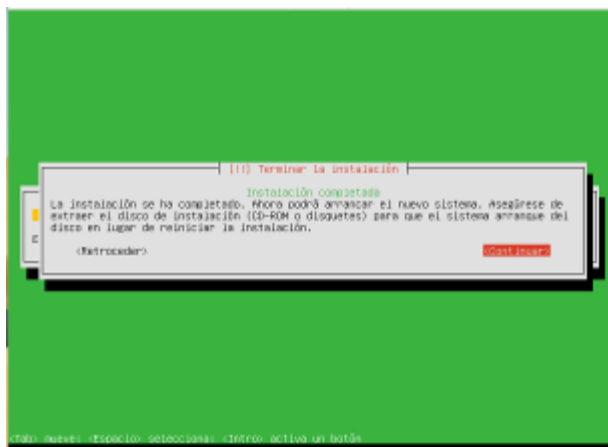


Figura 2.1.10. Finalización de la instalación

Al finalizar la instalación, el sistema se reinicia y empieza a cargar el sistema.

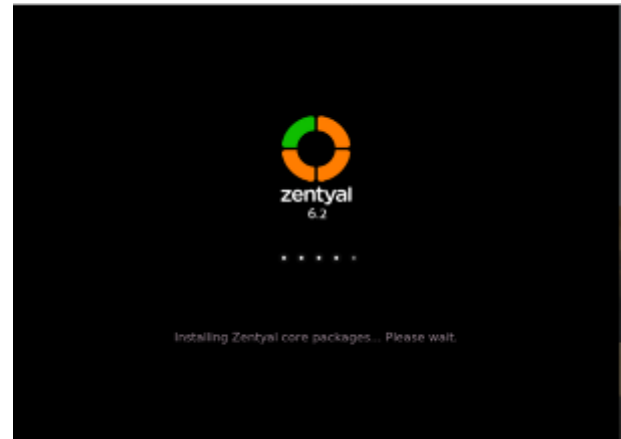


Figura 2.1.11. Iniciación de Zentyal.

Una vez cargado el sistema, valida datos de usuario y contraseña, los cuales son los mismos que se crearon durante la instalación.



Figura 2.1.12. Validación de datos.

Después de haber ingresado el usuario y contraseña, ingresa a la página inicial de Zentyal, desde allí se pueden elegir los módulos que se requiera instalar para la función específica que se pretenda.

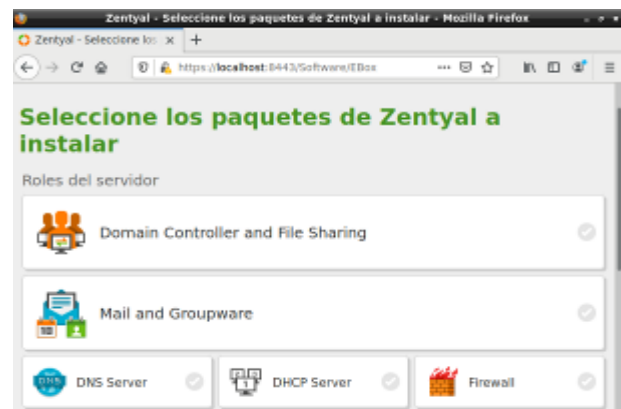


Figura 2.1.13. Página de inicio Zentyal

2.2 CONFIGURACIÓN BÁSICA DE ZENTYAL

Para realizar la configuración básica de Zentyal, en el menú del sistema se procede a indicar los componentes de Zentyal, allí se podrán ver todos los módulos que se requiera instalar.

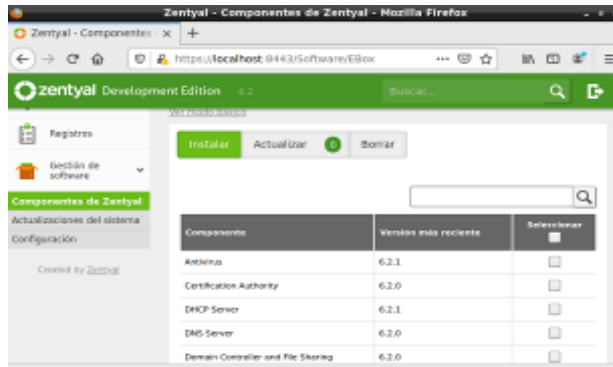


Figura 2.2.1. Componentes de Zentyal.

Uno de los componentes primordiales para configurar después de haber instalado Zentyal es el componente de red. Estando en los componentes se elige configuración de red y se instala.

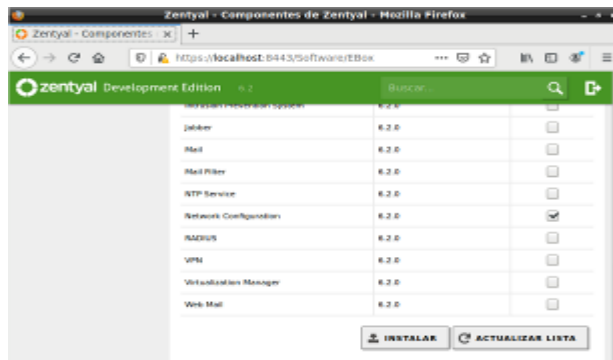


Figura 2.2.2. Configuración de red.

El sistema nos indica que los paquetes han sido instalados, en el menú de Zentyal (parte izquierda) se selecciona el componente de red y se elige interfaces para iniciar la configuración, allí se configuran las interfaces de LAN y WAN.



Figura 2.2.3. Configuración de interfaces.

Después configurar la red, se debe activar el componente, para esto se debe ir a Estado de los Módulos y selecciona el componente para activarlo. No olvidar guardar cambios ya que si no se realiza este paso no funciona la configuración.

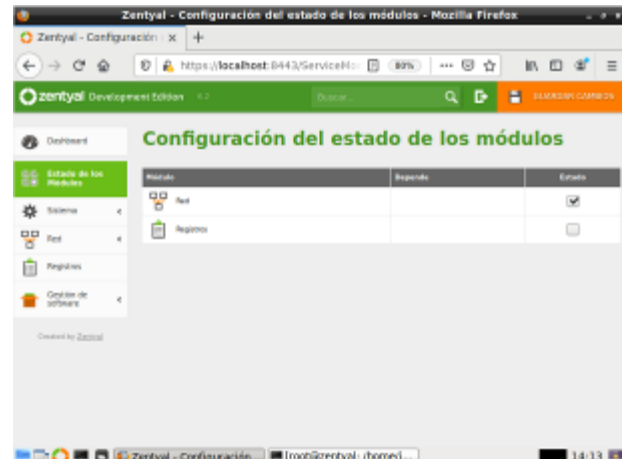


Figura 2.2.4. Activación de los componentes.

3 SERVICIOS DE INFRAESTRUCTURA IT DE ZENTYAL

Correspondiente a la definición de aspectos propios de servicios de Zentyal Server se describen a continuación una serie de procesos que responden a las configuraciones y funcionamiento de dichos servicios.

3.1 DHCP Server, DNS Server y Controlador de Dominio.

A continuación, se describen los aspectos más relevantes alrededor de la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux permitiendo un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal [5, 7].

Uno de los primeros aspectos para implementar servicio DHCP desde nuestro sistema de Zentyal Server consiste en que configurando y poniendo en marcha servicios de infraestructura tecnológica que permita dar respuesta a los requerimientos específicos del cliente dependerá para este aparte de instalar el servicio correspondiente a DHCP desde el cual se gestiona las IPs de los equipos conectados.

Además, da de alta servicios de directorio, implementando la funcionalidad de un controlador de dominio para compartir ficheros de Zentyal Server.

Solucionando necesidades específicas con GNU/Linux

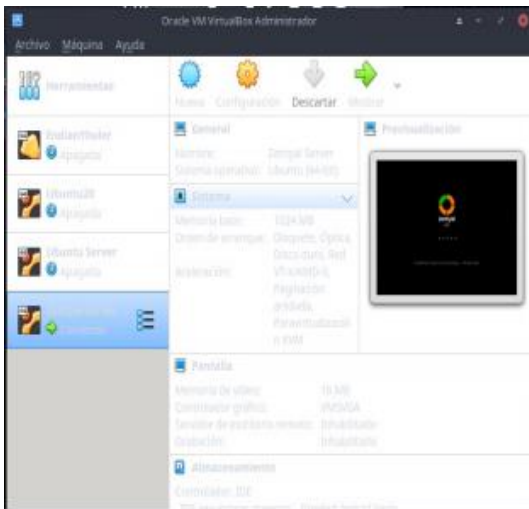


Figura 3.1.1. Inicialización de máquina virtual con Zentyal Server.

Para la configuración del servicio DHCP se evidencia la configuración una vez instalado el servicio DHCP en el Zentyal Server y el rango asignado, que está entre 10 y 20.

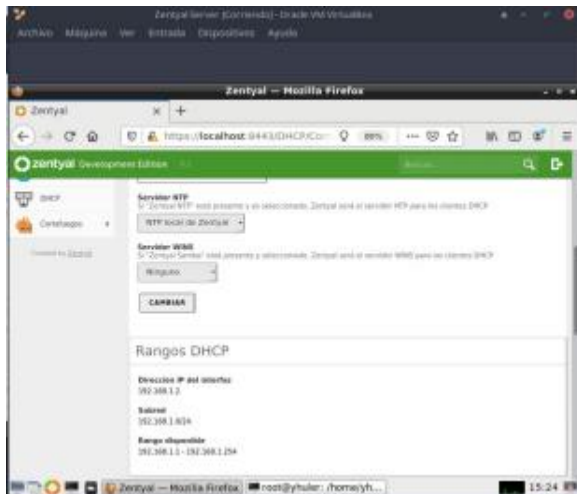


Figura 3.1.2. Luego de instalación de servicio DHCP, se procede a configurar IPs.

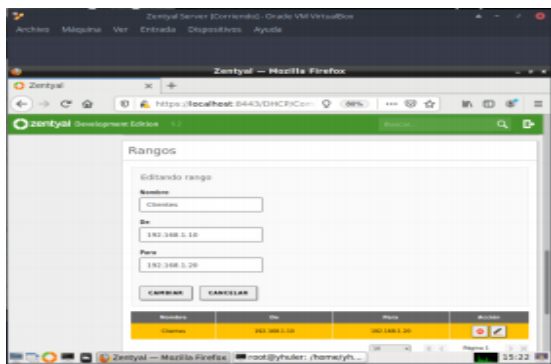


Figura 3.1.3. Asignación de segmento de red DHCP.

Observa como el direccionamiento IP estático asignado al server y la IP asignada dinámicamente al equipo cliente, correspondiente al registro de acceso a los servicios de infraestructura IT Zentyal.

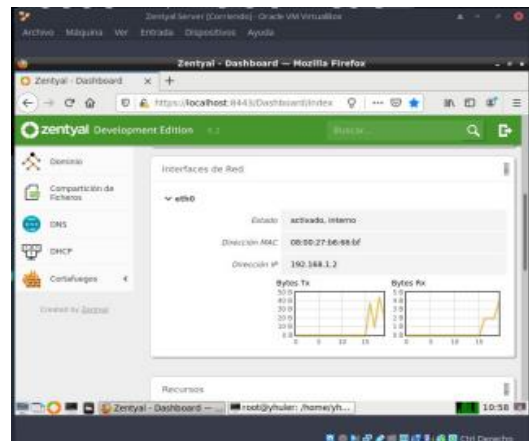


Figura 3.1.4. Direccionamiento estático.

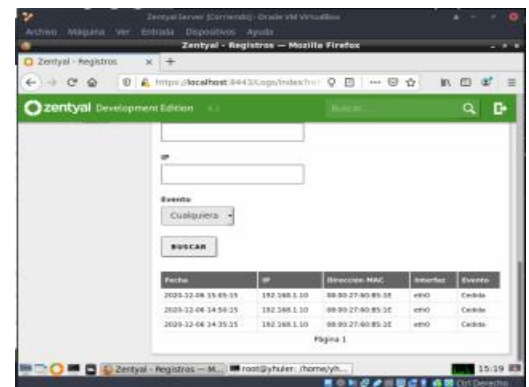


Figura 3.1.5. Direccionamiento dinámico.

Realiza prueba de conectividad entre el cliente y el servidor Zentyal, considerando las condiciones del modo de direccionamiento IP dinámico asignado previamente y del cual depende.

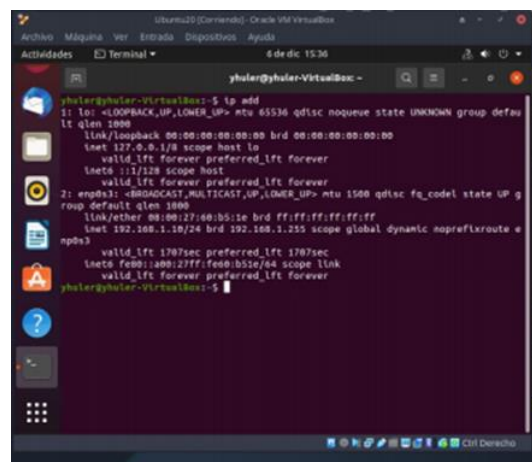


Figura 3.1.6. Prueba de agregación de IP desde consola de sistema Ubuntu.

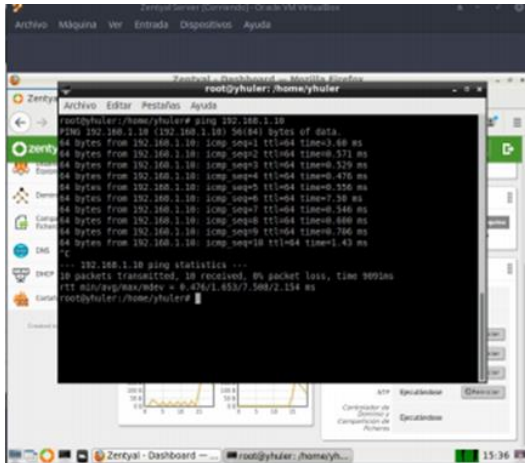


Figura 3.1.7. Confirmación de respuesta al interior de la red.

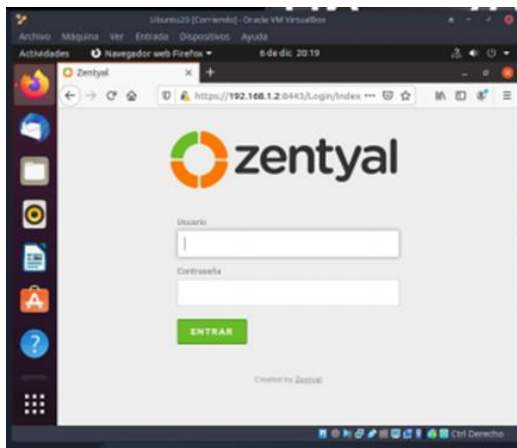


Figura 3.1.8. Ingreso a plataforma Zentyal para validar direccionamiento.

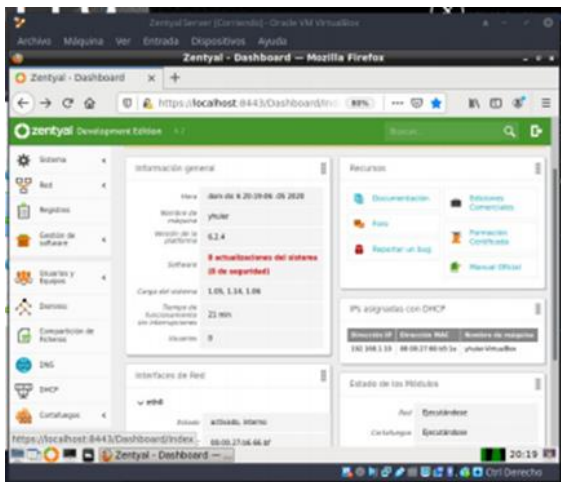


Figura 3.1.9. Dashboard de control luego de asignación DHCP a la red NAT.

Ahora bien, cuando ingresa al servidor Zentyal desde el cliente, las direcciones IPs se manejan en el rango asignado desde el servidor DHCP, teniendo con ello mayor control del proceso.

3.2 Proxy no transparente.

Del lado de la implementación y configuración detallada del control del acceso de una estación GNU/Linux a los servicios de conectividad a Internet desde Zentyal con el uso de un proxy que filtra la salida por medio del puerto 1230. En este sentido se deben apreciar los aspectos de configuración de servicios de Proxy HTTP, desde el cual configura este aspecto del sistema.

Una vez dentro de Zentyal, al abrir el navegador desde el cual se puede ingresar a la plataforma de administración vía web, en nuestro primer uso de esta nos indicara un fallo de seguridad para lo cual desde opciones avanzadas en la cual se indica que confía en el sitio [5].

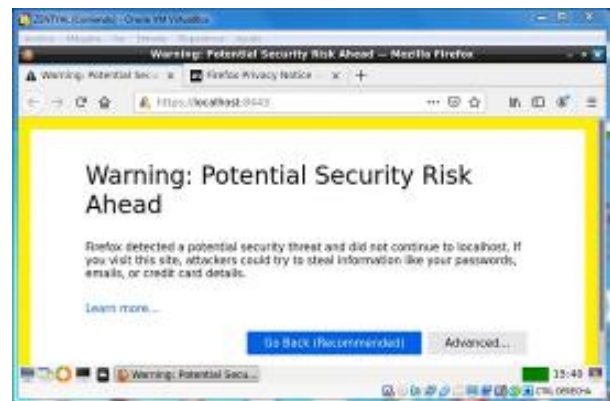


Figura 3.2.1. Mensaje de riesgo ingreso Zentyal.

Acceptando el riesgo nos queda consultar el certificado si desea.

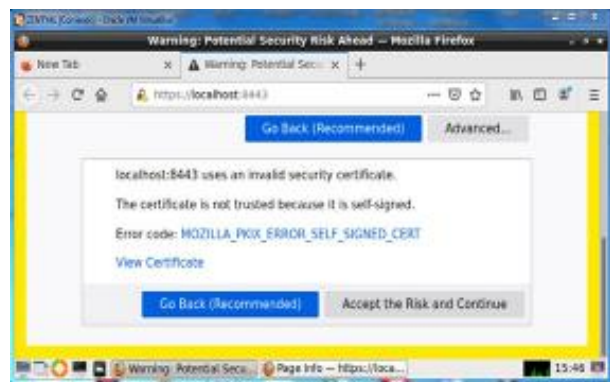


Figura 3.2.2 Aprobación de riesgo Zentyal para ingreso.

Por parte del entorno inicial de Zentyal nos solicitará credenciales de acceso, las cuales han sido asignadas previamente, nuestro caso **el usuario definido** con el correspondiente password.



Figura 3.2.3. Ingreso plataforma usuario login.

Se encuentra pues con una primera bienvenida la cual nos indica que se debe realizar unas configuraciones iniciales, el sistema nos dará la indicación a lo cual se define en cada paso del proceso.



Figura 3.2.4. Configuración previa Zentyal.

Primeramente, el aspecto de dominio y servidor de correo como aspectos obligatorios, además del componente usado para nuestras pruebas que corresponde a **HTTP Proxy**.



Figura 3.2.5. Selección de servicios a instalar.

Una vez se define el o los paquetes, se procede desde el botón instalar.

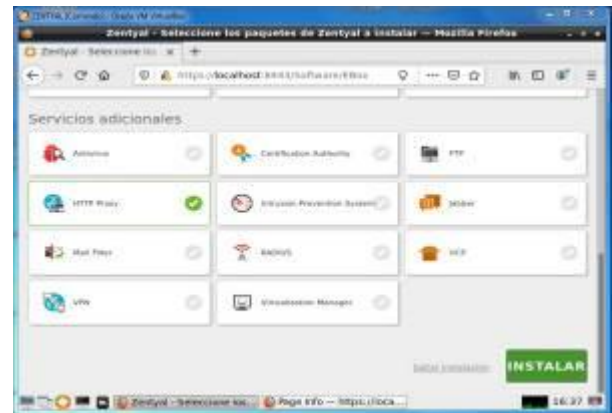


Figura 3.2.6. Selección servicio HTTP Proxy.

El resultado de esto corresponde a los servicios básicos de firewall, configuración de red y **HTTP Proxy** disponibles para ser usados.



Figura 3.2.7. Instalación de servicio HTTP Proxy.

Por lo tanto, se nos informa de un mensaje de bienvenida para poder iniciar desde el entorno de trabajo asignado.



Figura 3.2.8. Bienvenida a Zentyal Server.

Es preciso que las configuraciones que se ha indicado se actualicen para un correcto funcionamiento, por lo cual espera a que se realice dicha actualización.

Solucionando necesidades específicas con GNU/Linux

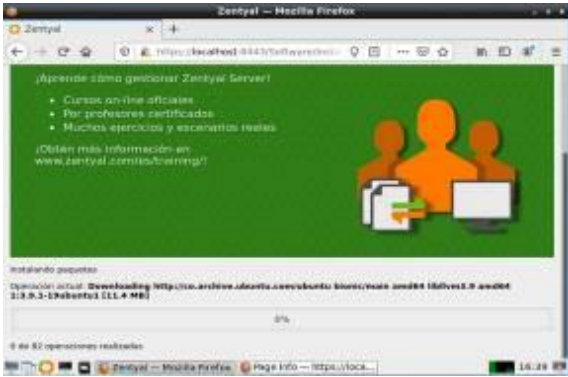


Figura 3.2.9. Validación de paquetes de instalación.

Siendo algunos de los paquetes el CLAMAV.



Figura 3.2.10. Descarga de repositorios de servicio.



Figura 3.2.11. Confirmación de repositorios de servicio.

Y se puede dar inicio a los procesos de validación de inicio considerando las características de HTTP Proxy que se configuran posteriormente.



Figura 3.2.12. Validación de IP vía DHCP.



Figura 3.2.13. Mensaje de alerta de servicios instalados.



Figura 3.2.14. Servicio Proxy HTTP no iniciado.



Figura 3.2.15. Activación de servicio Proxy HTTP.



Figura 3.2.16. Módulo HTTP Proxy habilitado.



Figura 3.2.17. Asignación de puerto 1230 para servicio.



Figura 3.2.18. Guardado correcto de cambios HTTP Proxy para limitar acceso.

Una vez asignado el puerto 1230 como criterio de restricción para acceso en la red se considera la opción de configurar desde el panel de gestión las URLs y sitios permitidos y no a partir de este criterio.



Figura 3.2.19. Puerto 1230 habilitado.



Figura 3.2.22. Acceso Facebook vía Proxy no transparente.

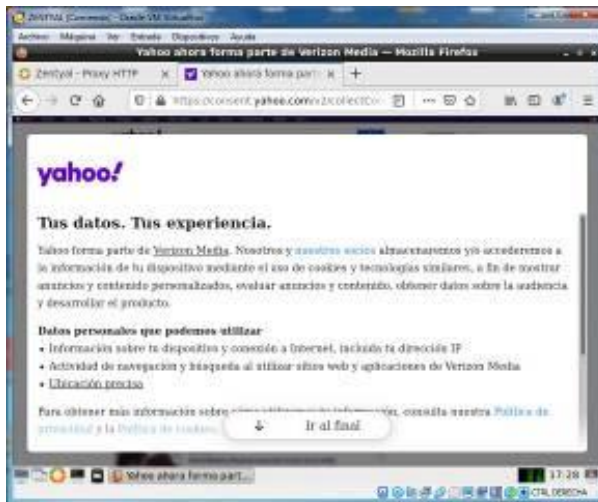


Figura 3.2.20. Url con acceso previo sin restricción.

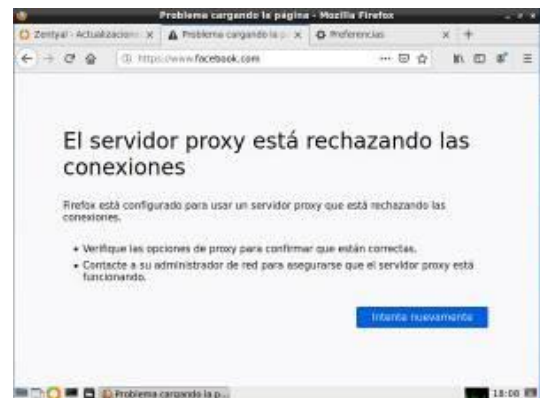


Figura 3.2.23. Sitio web restringido vía proxy HTTP, luego de aplicar cambios.



Figura 3.2.21. Configuraciones de sitio para acceso vía HTTP Proxy.

Aplica los correspondientes cambios de proxy no transparente para evidenciar las correspondientes restricciones de acceso a sitios específicos ya definidos desde los perfiles de grupos de HTTP Proxy.

Como se puede apreciar luego de las validaciones de sistema en la red y dentro de los correspondientes equipos se restringe el acceso cuando no se cumplen las condiciones de puerto y políticas de seguridad asignadas previamente desde el método de Proxy no transparente difiriendo del transparente en que puede ser oculto al usuario aun conociendo las credenciales de acceso.

3.3 Cortafuegos.

Del lado de los cortafuegos la implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas.

La validación del funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux.

3.3.1 INSTALACIÓN FIREWALL

Una vez instalado el Zentyal, se va a iniciar sesión y proceder con el asistente de instalación.



Figura 3.3.1.1. Ingreso principal Zentyal Server.

Para este caso va a indicar que desea instalar el Firewall. Adicionalmente se instala el DHCP si se quiere que la red interna tenga asignación de IP automáticas.

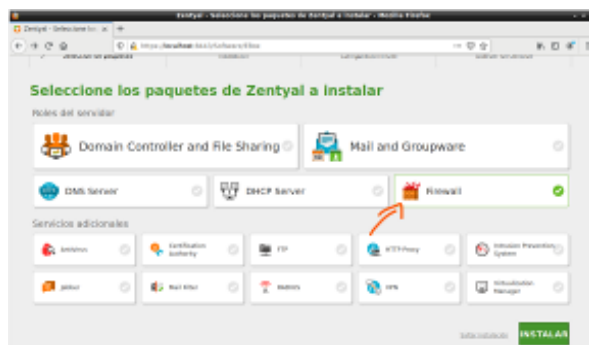


Figura 3.3.1.2. Selección de servicio Firewall.

Confirma la instalación de los paquetes.



Figura 3.3.1.3. Instalación de servicio exitoso Firewall.

Luego nos indicara el uso de cada interfaz, como es un cortafuegos va a usar 2 interfaces. Una para el exterior (eth0, internet) y otra para la red local (eth1, interna).



Figura 3.3.1.4. Asistente de configuración de interfaces.

Ahora se indica la ip y configuración de cada interfaz. En la eth0 maneja la ip 192.168.100.100. La eth1 como es red interna va a indicarle una ip diferente 192.168.0.100.



Figura 3.3.1.5. Configuración de interfaces hecha.

Con ello se ha finalizado la instalación básica de Zentyal para efectos de Firewall.

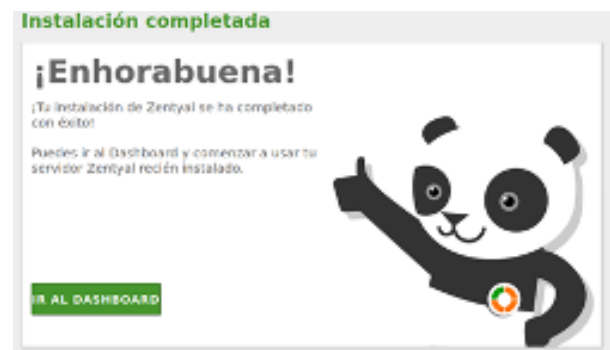


Figura 3.3.1.6. Instalación exitosa de cortafuegos.

Ahora, si desea se configura y asigna un DHCP a la red interna. Para esto simplemente configura el DHCP en la interfaz de la red interna. En este caso es la "eth1"



Figura 3.3.1.7. Asignación de interfaces.

Asigna un rango de direcciones que van desde 192.168.0.101 hasta 192.168.0.149.



Figura 3.3.1.8. IP asignada.

Comproba que nuestro Zentyal tenga acceso a internet (ping a google.com)

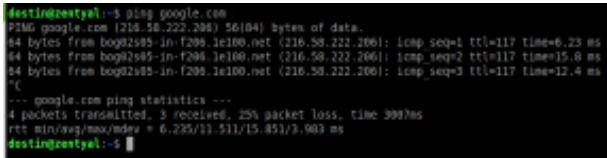


Figura 3.3.1.9. Ping de respuesta a Google.

Y ahora, verifica que nuestro/s cliente/s tenga la configuración de la red interna y acceso a internet.

Recordar que la red interna está configurada automáticamente gracias a nuestro DHCP que se configuró en Zentyal.

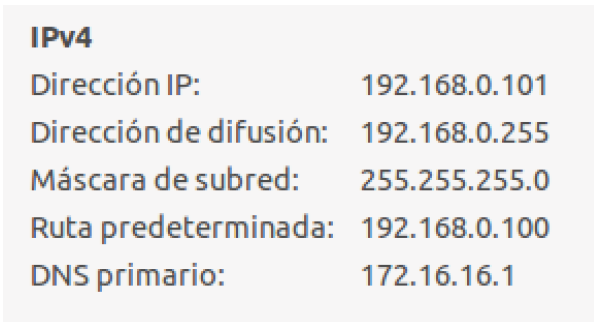


Figura 3.3.1.10. Direccionamiento IP.

El DNS primario es el que nos brinda el proveedor de internet.

Verifica el acceso a internet en la red interna.

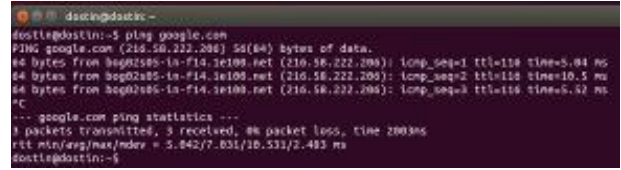


Figura 3.3.1.11. Respuesta desde sistema Ubuntu a ping en url www.google.com. Conexión Ok.

O por medio de un cliente Windows.

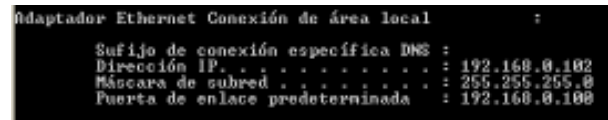


Figura 3.3.1.12. Confirmación de conexión desde host con sistema Windows.

IP's asignadas por DHCP:



Figura 3.3.1.13. Confirmación de servicio DHCP.

3.3.2 CONFIGURANDO FIREWALL

Para configurar el acceso de nuestros equipos en la red LAN a internet, configura el firewall en la opción "Reglas de filtrado para las redes internas".



Figura 3.3.2. Asignando reglas de filtrado.

Por defecto, hay una regla que permite el acceso a cualquier servicio.



Figura 3.3.2.2. Panel de asignación de reglas.

Va a probar el servicio. Por ejemplo, que se niegue a todos los accesos al servicio HTTPS.

Solucionando necesidades específicas con GNU/Linux

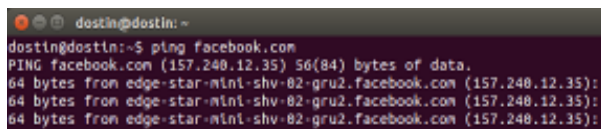
En ese orden de ideas, ningún equipo podrá acceder al servicio https. Por ejemplo, al intentar acceder a <https://www.google.com>



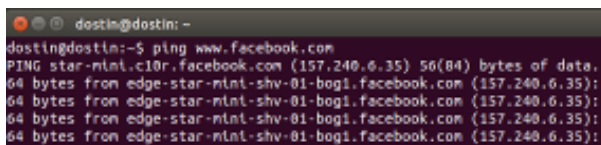
Figura 3.3.2.3. Aplicación de reglas con efecto sobre la url www.google.com.

Así mismo, se configura la regla para que bloquee una IP exacta, para el caso de la actividad, va a bloquear la IP de Facebook.com y www.facebook.com

Al hacer un ping, la IP de Facebook es 157.240.12.35 (facebook.com).



Y 157.240.6.35 (www.facebook.com)



Así que configura la regla con estas IP's.

Figura 3.3.2.4 y 5: Ping de respuesta con cifrado.

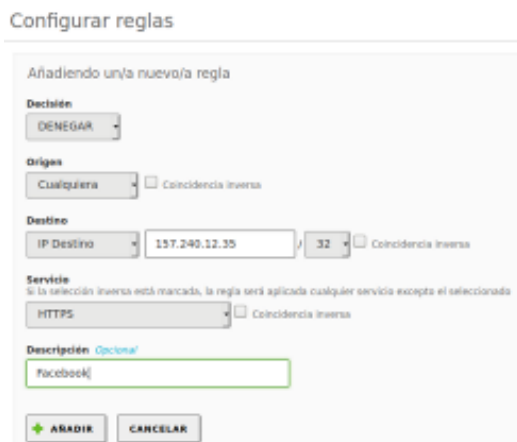


Figura 3.3.2.6. Opciones de denegación de servicio.

(Se repite el mismo proceso con la otra ip)

Quedando las reglas de la siguiente manera:



Figura 3.3.2.7. Configuración de reglas específicas.

Ahora, si intenta acceder a Facebook desde nuestros clientes, el resultado será un mensaje de error por tiempo agotado.



Figura 3.3.2.8. Rechazo de conexión luego de aplicación de reglas de cifrado desde panel administrativo.

Es de resaltar, que este método **NO es recomendable**. Existen muchas formas de saltar esta "restricción" ya que, por ejemplo, Facebook maneja muchos dominios. Básicamente cada idioma y país tienen su propio dominio de Facebook (Ej: www.facebook.es).

Este mismo método de bloqueo se podría repetir para más redes sociales y/o páginas de entretenimiento.

3.4 File Server y Print Server

Ahora bien, los aspectos alrededor de la implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux con la ayuda del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux haciendo uso del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras corresponde a que una vez realizada la configuración básica de Zentyal, configura el DNS para que tenga una conexión a internet de manera óptima para poder descargar demás paquetes. Se añade los DNS 8.8.8.8 y 8.8.4.4. Se realizan los cambios necesarios y se guardan los cambios para que la configuración tenga efecto.

Solucionando necesidades específicas con GNU/Linux

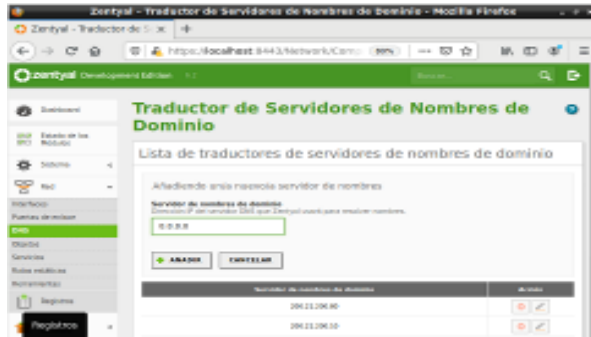


Figura 3.4.1. Configuración DNS.

Un paso importante es actualizar el servidor, para esto desde la terminal con el comando `apt-get update` y `apt-get upgrade` se realizan las actualizaciones necesarias.

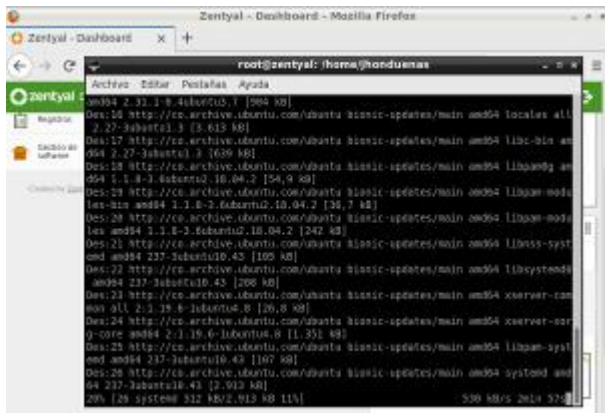


Figura 3.4.2. Actualización de servidor Zentyal.

[4] Ahora desde la pestaña de componentes y selecciona la casilla de controlador de dominio y da clic en instalar para corresponder a los componentes requeridos.

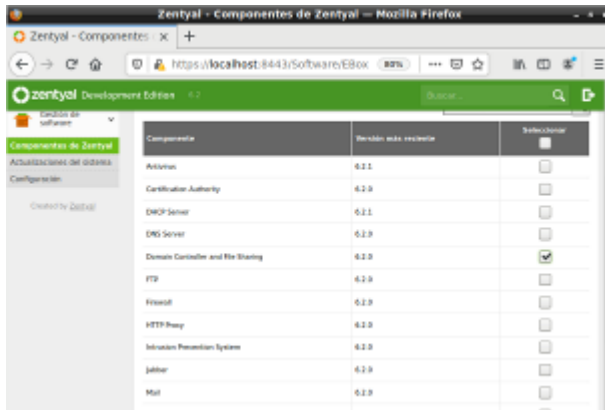


Figura 3.4.3. Instalación de controlador de dominio

Aparece un listado de paquetes que se van a instalar, se da clic en continuar para iniciar la instalación de estos paquetes.

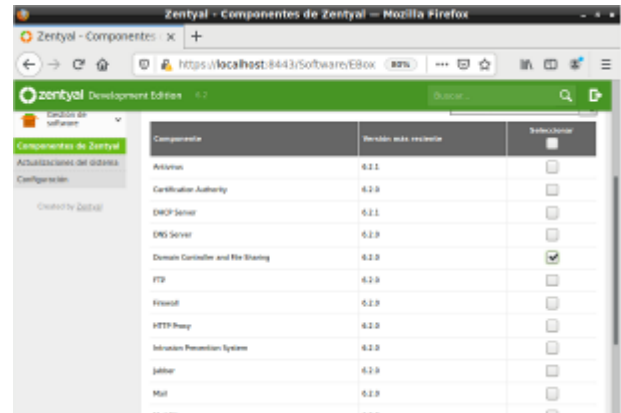


Figura 3.4.4. Paquetes que se instalan.

Luego de ser instalados los paquetes, aparecen los módulos de usuarios y equipos, dominio, compartición de ficheros, DNS y cortafuegos en la página de inicio de Zentyal.

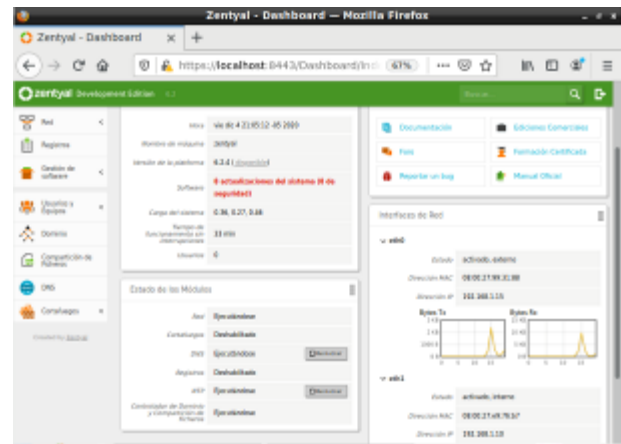


Figura 3.4.5. Paquetes instalados.

Activa el módulo de controlador de dominio junto con los módulos DNS y NTP, se guardan los cambios realizados.

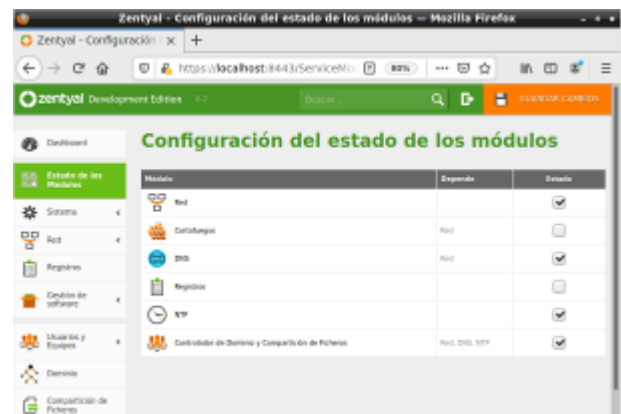


Figura 3.4.6. Activación de módulos

Se revisan los puertos y protocolos de samba, para esto se ingresa al módulo de red y en servicios se verifica que esté samba.

Solucionando necesidades específicas con GNU/Linux

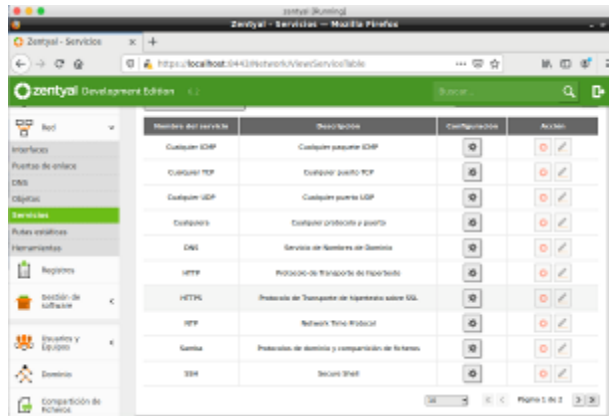


Figura 3.4.7. Protocolos samba.

Revisa los puertos en samba, donde los puertos 139 y 636 corresponden a los protocolos de LDAP.

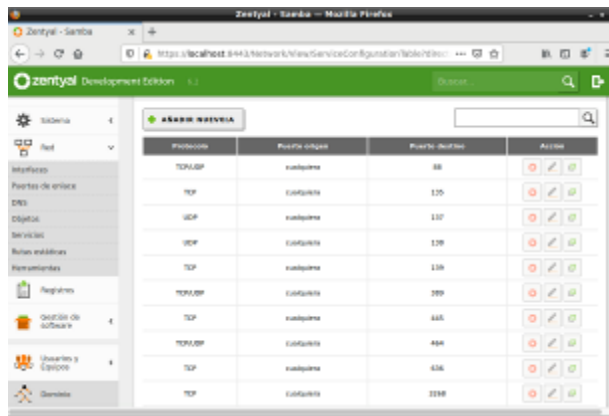


Figura 3.4.8. Puertos en samba.

Asegura que todos los dispositivos que están interconectados en la red puedan utilizar samba, para esto se selecciona el módulo de cortafuegos y en filtrado de paquetes se verifican las reglas.



Figura 3.4.9. Verificación de reglas.

Luego en el módulo de dominio configura el controlador de dominio.



Figura 3.4.10. Configuración controladora de dominio.

Verifica que el controlador de dominio esté ejecutándose, para esto selecciona Estado de los módulos, se activa el servicio y se guardan los cambios.

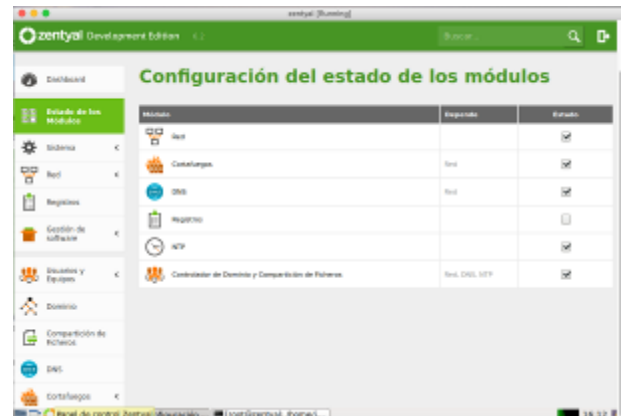


Figura 3.4.11. Activación de controlador.

Selecciona el módulo de Sistema y verifica que el controlador de dominio se esté ejecutando.



Figura 3.4.12. Activación de módulos.

Estando en el módulo de Usuarios y Equipos, selecciona la opción de Gestionar y en el dominio base, en este caso corresponde a Zentyal-domain.ian crea una nueva unidad organizativa con el nombre ADMIN.

Solucionando necesidades específicas con GNU/Linux

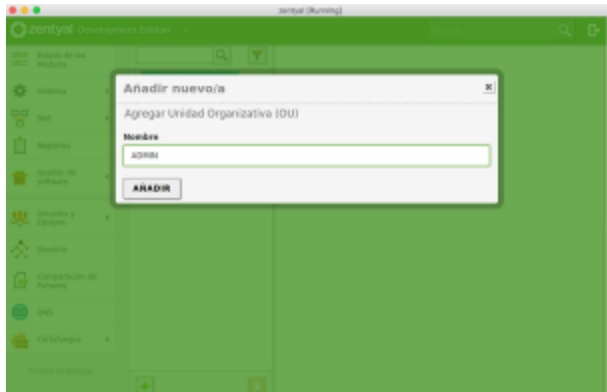


Figura 3.4.13. Nueva unidad organizativa.

En esta nueva unidad crea un grupo con el nombre de AdminDominio

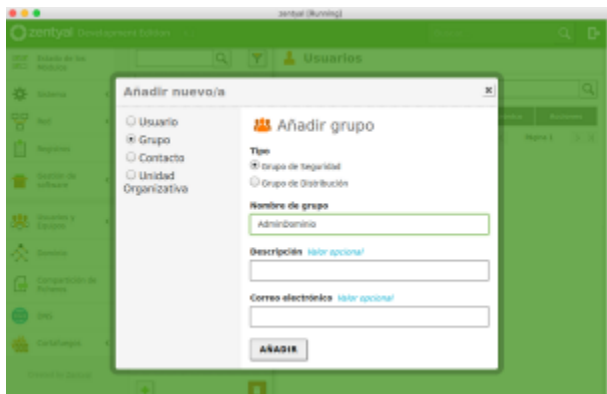


Figura 3.4.14. Crear grupo

Luego crea un nuevo usuario y se asigna al grupo anteriormente creado que corresponde a AdminDominio.

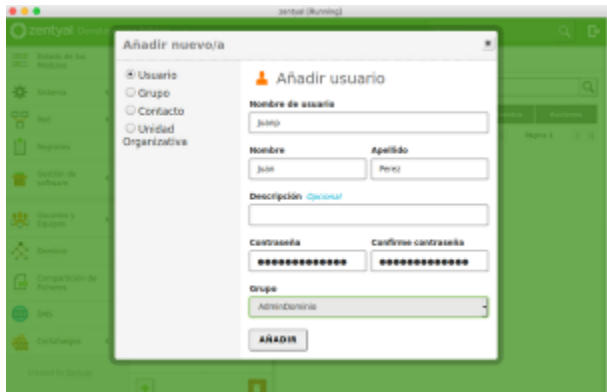


Figura 3.4.15. Crear nuevo usuario

Ahora se realizan las pruebas de conexión con la configuración de dominio realizado, para este caso toma una máquina virtual con Windows 10 y realiza la configuración del dominio, y se asigna el dominio zentyal-domain.lan

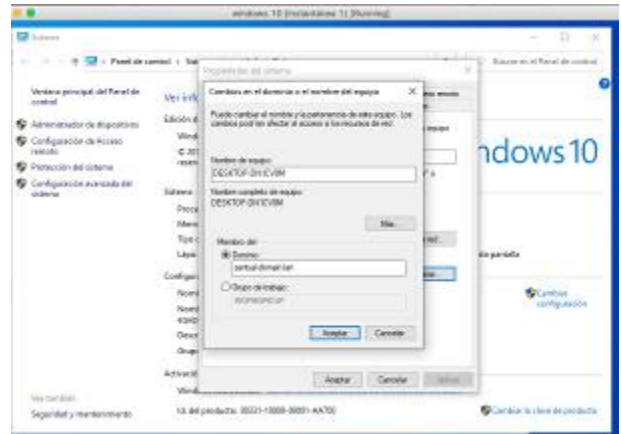


Figura 3.4.16. Configuración dominio en Windows.

El sistema nos indica que se debe ingresar los datos de usuario y contraseña, estos datos son los mismos cuando se creó un nuevo usuario en Zentyal, el sistema valida los datos y nos indica que la máquina Windows 10 ha sido unida al dominio de Zentyal, se guardan cambios y reinicia la máquina.

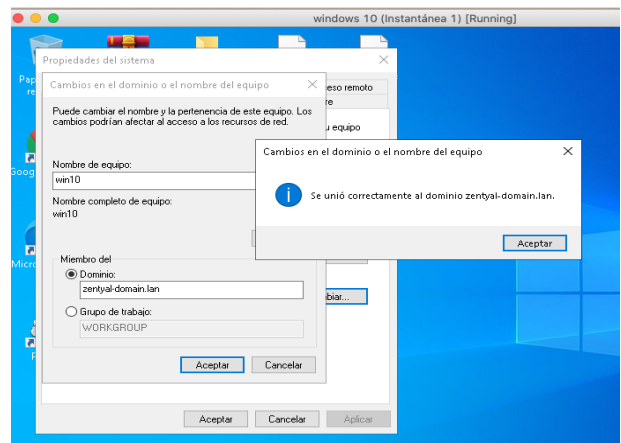


Figura 3.4.17. Unión de Windows al dominio.

Después de haber reiniciado Windows 10 nos aparece el nuevo usuario creado en Zentyal, se debe validar la contraseña.

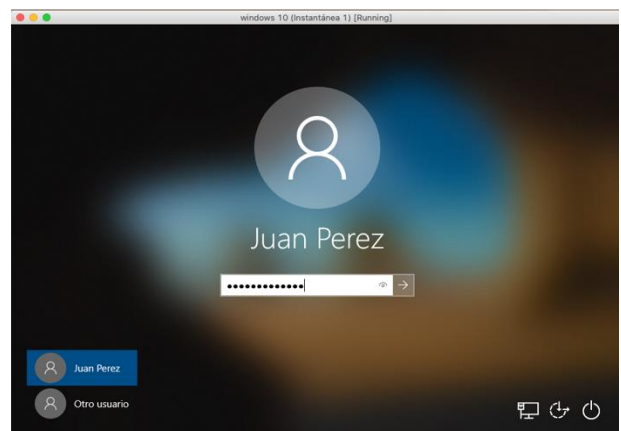


Figura 3.4.18. Inicio sesión Windows.

Solucionando necesidades específicas con GNU/Linux

En el estado de red en Windows se puede verificar que el sistema está bajo el dominio de Zentyal.

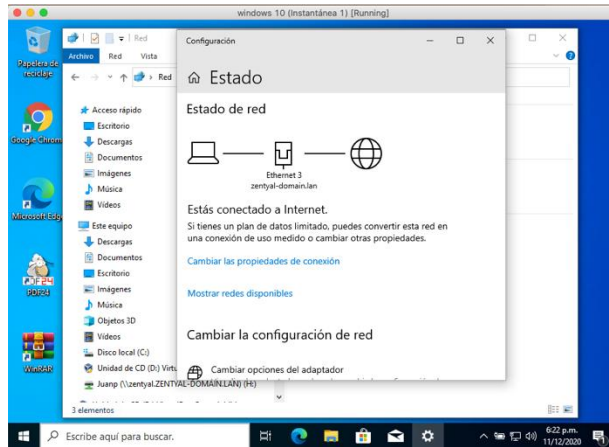


Figura 3.4.19. Verificación de dominio en Windows

Después de unir Windows 10 al dominio Zentyal, ahora va al módulo de compartición de ficheros y realiza la configuración.

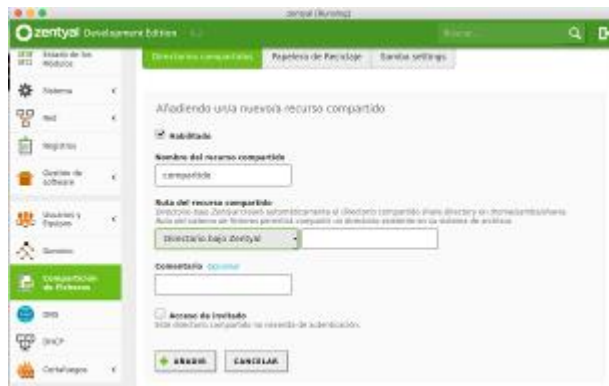


Figura 3.4.20. Configuración compartición de ficheros.

Se verifica que el fichero este activo para compartir.



Figura 3.4.21. Crear fichero compartido.

De la misma manera en Windows verifica que el fichero compartido aparezca en el sistema.

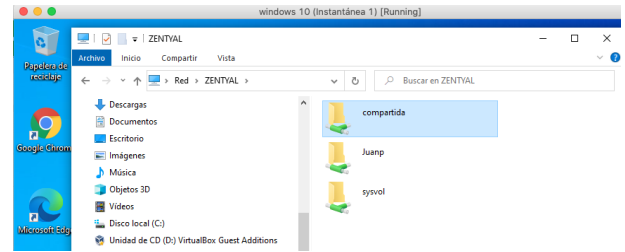


Figura 3.4.22. Compartición de fichero en Windows.

Ahora se crea un fichero para compartir impresora, este se realiza del mismo modo al fichero compartido, se crea el fichero y se guardan cambios, luego verifica que el fichero este activo en Zentyal.



Figura 3.4.23. Compartición de fichero en Zentyal.

También verifica que el fichero de impresora esté activo en Windows.

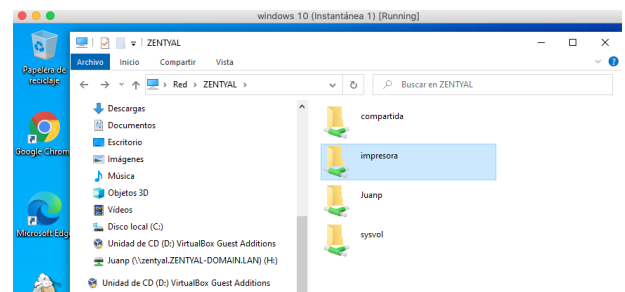


Figura 3.4.24. Compartición de impresora en Windows.

3.5 VPN.

Finalmente como se realiza el proceso de 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 evidenciando el ingreso de contenido o aplicación de la estación de trabajo.

[2] Una vez se ingresa por primera vez al servicio de Zentyal, se configuran los servicios de VPN, que compete a esta sección para luego ya seleccionado los servicios de VPN iniciar la correspondiente instalación para continuar:

Solucionando necesidades específicas con GNU/Linux

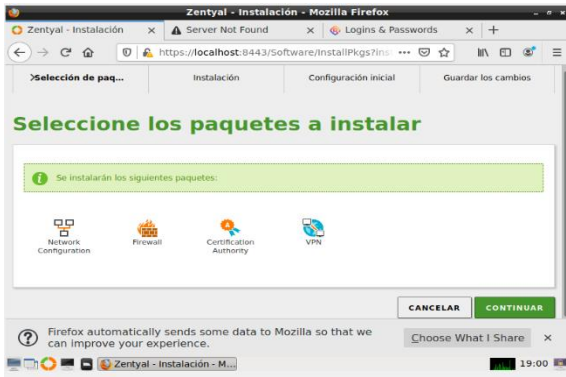


Figura 3.5.1. Selección de servicio VPN en Zentyal.

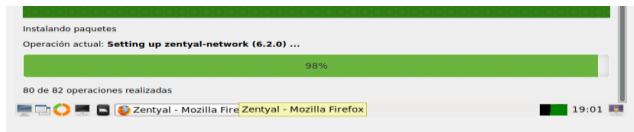


Figura 3.5.2. Instalación de paquetes VPN.

Selecciona los parámetros correctos para continuar con la configuración.

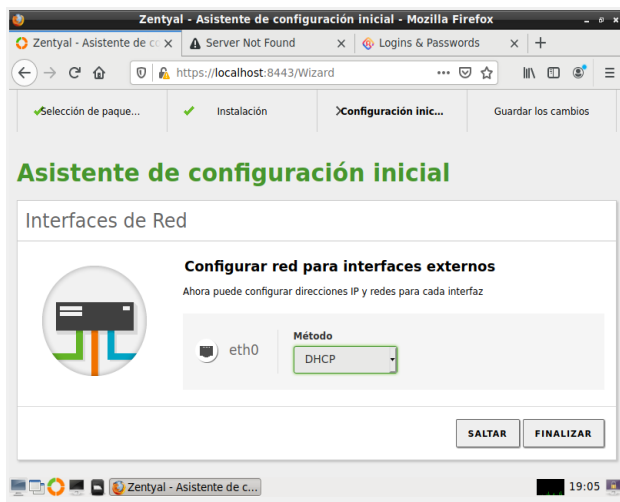


Figura 3.5.3. Selección de interfaz de control externa.

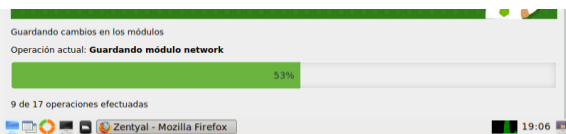


Figura 3.5.4. Descarga de paquetes requeridos VPN.

Hasta este punto se establecen los componentes principales que controlan el tráfico VPN que luego se usa para gestionar las conexiones seguras desde los dispositivos de red que se hayan vinculado previamente.

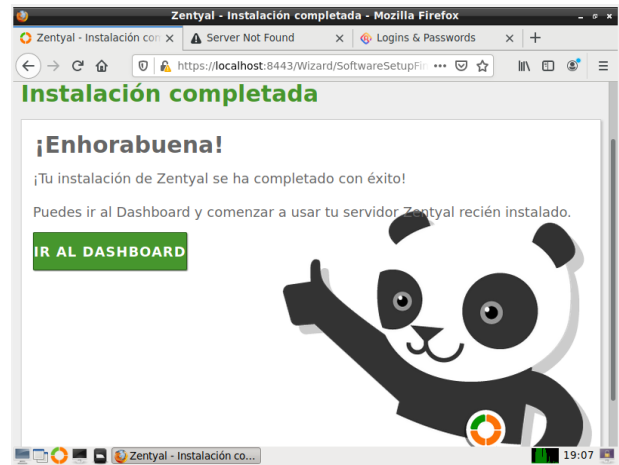


Figura 3.5.5. Instalación exitosa de VPN.

Luego se procede a crear el certificado para Zentyal.

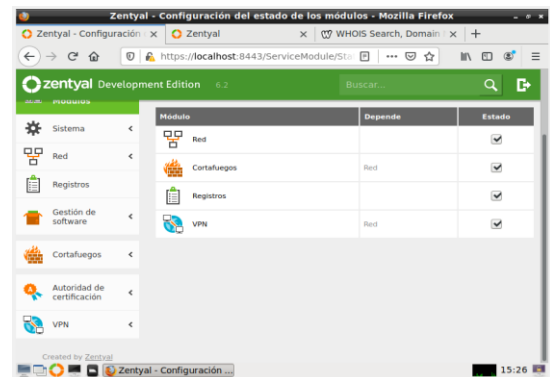


Figura 3.5.6. Servicio habilitado de Zentyal – VPN.

En el menú va a Autoridad de Certificación:

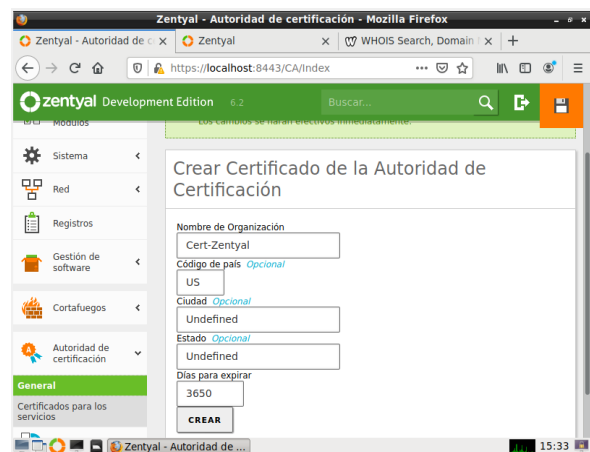





Figura 3.5.7. Asignación de certificado para conexión segura.

Verifica que los datos estén bien:

Solucionando necesidades específicas con GNU/Linux

Lista de Certificados actual

Nombre	Estado	Fecha	Acciones
Cert-Zentyal Authority Certificate desde Cert-Zentyal	Válido	2030-12-06 20:34:49	  




 Revocar
  Descargar clave(s) y certificado
  Renovar o re-emitir

Figura 3.5.8. Lista de certificados generados.

Y le da click en guardar:

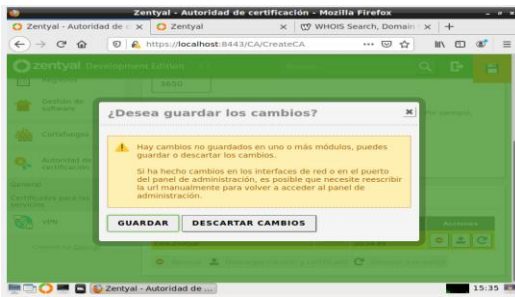


Figura 3.5.9. Guardado correcto de certificados.

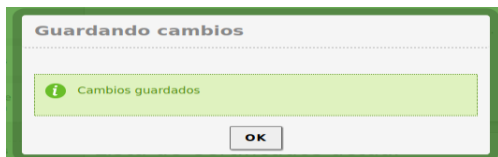


Figura 3.5.10. Operación exitosa de guardado.

En la sección Lista de servidores de la opción VPN:

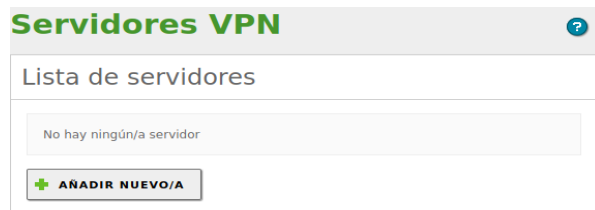


Figura 3.5.11. Sección de añadir servidores.

Añadir un servidor, pero sin habilitarlo aún:

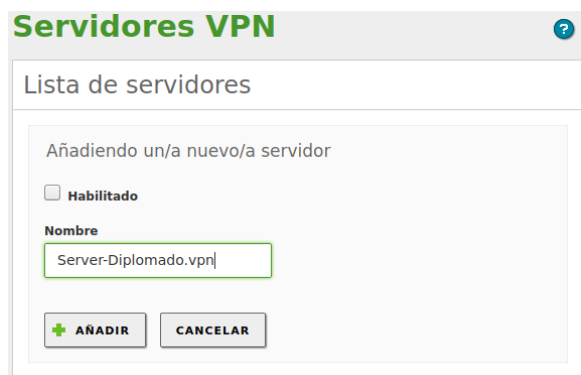


Figura 3.5.12. Creación de servidor VPN.

Habilitado	Nombre	Configuración	Redes anunciadas	Descargar paquete de configuración de cliente	Acción
<input type="checkbox"/>	Server-Diplomado.vpn				 

10 | < > | Página 1

Figura 3.5.13. Gestión de servidor VPN creado.

Y luego se guardan los cambios para dirigirnos nuevamente a **Autoridad de certificación**, se crea un nuevo certificado que será para nuestro servidor VPN que acaba de crear.

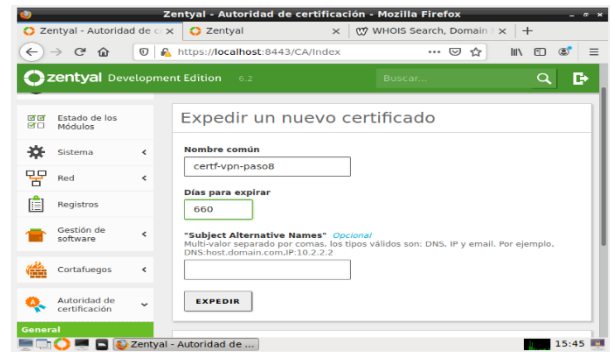


Figura 3.5.14. Administración de servidor VPN.

Lista de Certificados actual

Nombre	Estado	Fecha	Acciones
Cert-Zentyal Authority Certificate desde Cert-Zentyal	Válido	2030-12-06 20:34:49	  
vpn-Server-Diplomado.vpn	Válido	2030-12-06 20:34:49	  
certf-vpn-paso8	Válido	2022-09-29 15:45:37	  

 Revocar
  Descargar clave(s) y certificado
  Renovar o re-emitir

Figura 3.5.15. Certificados adicionales creados para el servidor VPN.

Va a la ficha VPN y selecciona la lista de servidores y lo configura:



Figura 3.5.16. Panel administrativo de servicios VPN.

Es necesario configurarlo con el certificado creado anteriormente:



Figura 3.5.17. Configuración de puertos de servicio VPN.

Se realiza un guardado de los cambios:

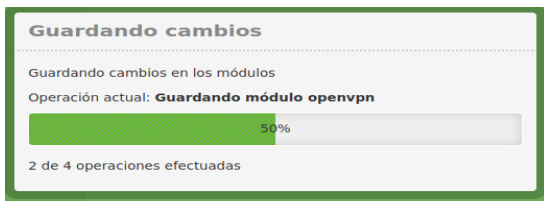


Figura 3.5.18. Aplicación de cambios realizados a Servidor VPN.

Luego en la sección red y en la pestaña de servicios se debe crear el servicio para permitir la VPN:

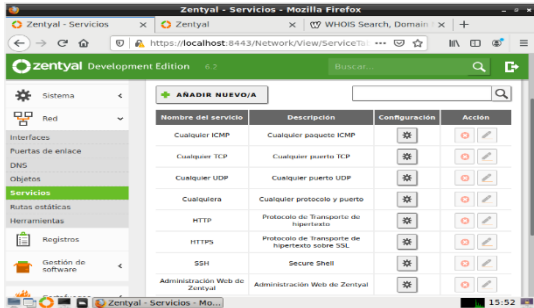


Figura 3.5.19. Gestión de servicios VPN.

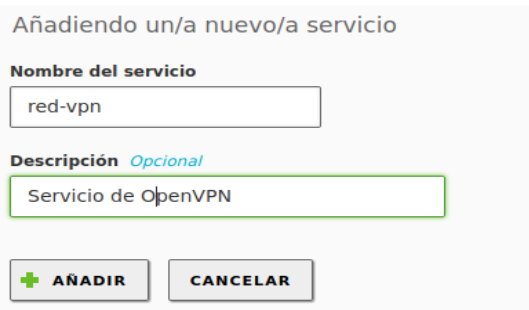


Figura 3.5.20. Creación de servicio VPN adicional.



Figura 3.5.21. Asignación de nuevo puerto de gestión.

Después se da ingreso a la sección del Cortafuegos, a la ficha filtrado de paquetes y añado una nueva regla que es para el servicio red VPN.



Figura 3.5.22. Creación de reglas de filtrado vía VPN.

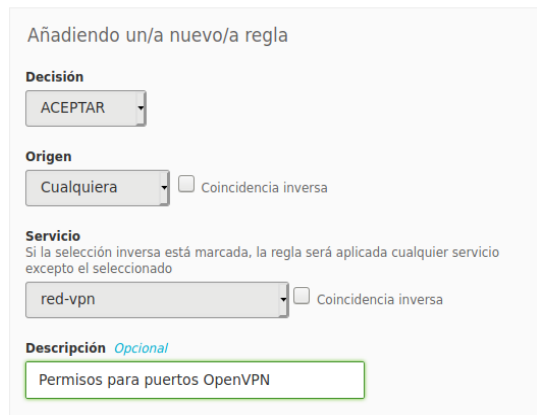


Figura 3.5.23. Generación de permisos a regla creada.

Desde la sección VPN, servidores, va a configurar las redes de nuestro servidor VPN:

Solucionando necesidades específicas con GNU/Linux



Figura 3.5.25. Validación de servidor VPN creado.

Descarga los datos para acceder desde nuestro cliente y configura.



Figura 3.5.26. Confirmación de red.

Para que desde la sección IP del servidor busca nuestra IP Pública que nos provee el ISP:



Figura 3.5.27. Confirmación de IP pública.

Averigua I IP que se ha asignado en el Zentyal:

```
edisonorga@zentyal-edisonorganista-diplomadolinux:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.101.13 netmask 255.255.255.0 broadcast 192.168.101.255
    ether 08:00:27:86:cf:dd txqueuelen 1000 (Ethernet)
    RX packets 26418 bytes 13051190 (13.0 MB)
    RX errors 0 dropped 31 overruns 0 frame 0
    TX packets 7242 bytes 762961 (762.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 3.5.28. Confirmación de datos de red del host.

Por lo tanto, verifica y descarga:

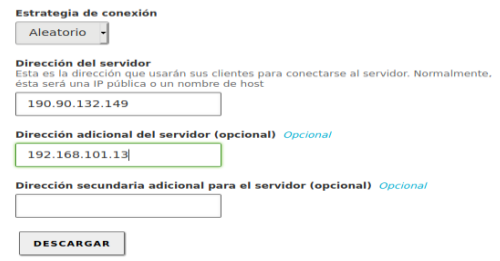


Figura 3.5.29. Confirmación de datos de red.

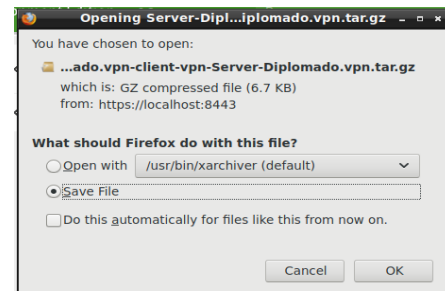


Figura 3.5.30. Descarga de archivos en el servidor local.

De esta manera se guardan los cambios.

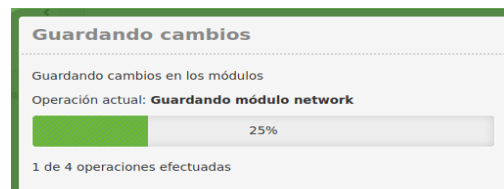


Figura 3.5.31. Descarga efectiva de archivos.

Habilita el servidor VPN y va al Dashboard y verifica que esté en ejecución:

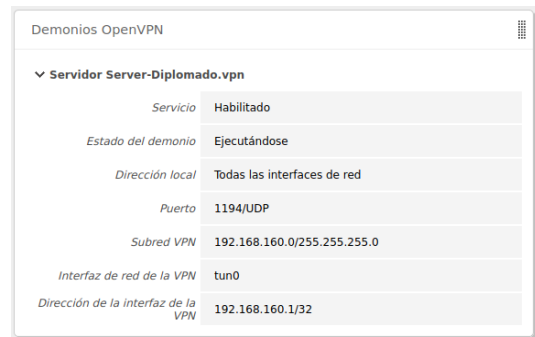


Figura 3.5.31. Confirmación se servicios VPN habilitados.

Luego desde nuestra terminal Ubuntu Desktop 18.04 ya descargados los archivos que nos arrojó Zentyal en el paso correspondiente para lo cual se añade una conexión VPN configurando de la siguiente forma:

Solucionando necesidades específicas con GNU/Linux

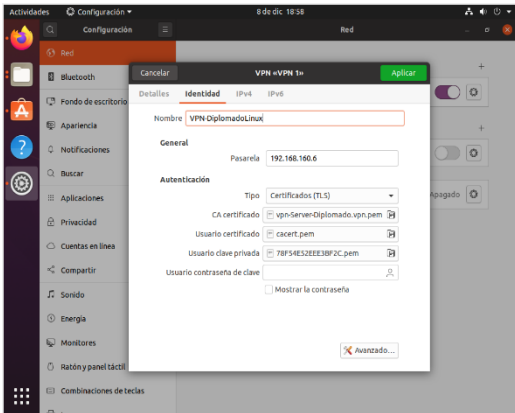


Figura 3.5.32. Configuración VPN de acceso desde distro Ubuntu.

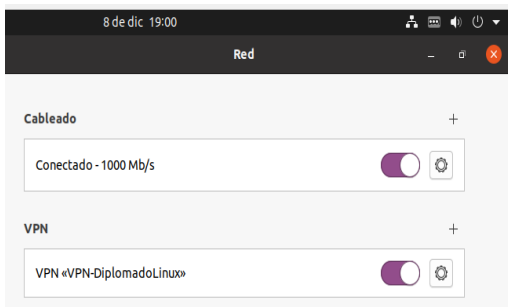


Figura 3.5.33. Control de acceso VPN desde Ubuntu.

Y de este modo se tiene control sobre la VPN. En un cliente con sistema operativo Windows 10 descarga el programa con sistema operativo Windows 10 descarga el programa el programa Open Vpn de la página oficial <https://openvpn.net/download-open-vpn/> y carga el archivo de configuración que descarga desde Zentyal:



Figura 3.5.34. Cliente VPN desde sistema Windows.

Con esto se accede por la VPN previamente configurada a nuestro servidor.

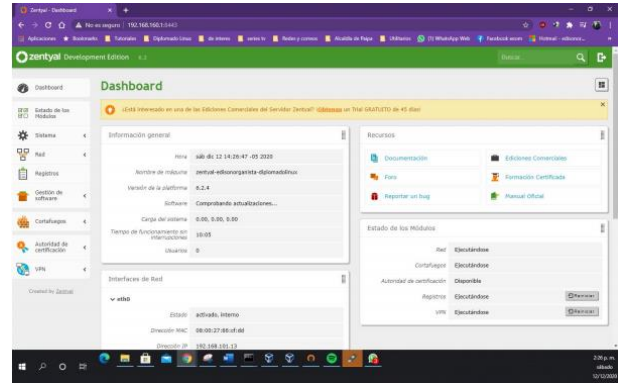


Figura 3.5.35. Acceso vía VPN desde sistema Windows.

Para comprobar la conexión al Zentyal va a un navegador y le da la url que nos asigna para conectar a la VPN, en este caso voy a entrar por el puerto 8443 para ingresar al panel de control de Zentyal: <https://192.168.160.1:8443/>

De este modo el punto de acceso creado es accesible tanto desde Ubuntu u otra distro de Linux, mientras que con los permisos correspondientes se puede acceder desde Windows.

4 CONCLUSIONES.

Zentyal como alternativa a Windows Server permite interesantes soluciones de infraestructura de redes configurando servicios esenciales para gestión de tráfico y permisos tanto de grupos como de usuarios particulares, cuando se registra el primer proceso de instalación de Zentyal debemos prever las condiciones de la red en la cual se generaran los procesos, si bien desde la red NAT se establecen los criterios de privacidad inicial estos deben en gran parte apuntar a segmentos propios de la misma red para garantizar una armonía frente a los servicios de red evaluados ya que en una red que no pase por virtualización estos aspectos suelen ser más tediosos en cuando a ajustar los parámetros de tarjetas de red disponibles y aspectos tales como la MAC de cada equipo participante desde los cuales se pueda establecer los modos de restricción posteriores.

Alrededor del tema de proxy no transparente, se puede determinó que al acondicionar el entorno de trabajo en Linux puede permitirse la correcta configuración de servicios en red a partir del control de permisos de los que dispone Zentyal Server en el la gestión por medio de zonas delimitadas conocidas como DMZ hacen posible el uso de segmentos de red local configuradas como NAT para pruebas de red aplicadas para este caso de manera interna con salida por una de las zonas creadas o naranja; esto conlleva a opciones de administración de servicios específicos de red y a identificar como beneficios un mayor control de tráfico dentro de la red además de que se puede establecer

condiciones que se presentan con el uso de Proxy no transparente a partir del alcance de sus aplicaciones en Zentyal de manera segura sin interferir en los equipos vinculados.

También se identificó que como parte de la respuesta a necesidades específicas de Linux haciendo uso de herramientas de gestión de red, tratando el tema de proxy no transparente el cual tiene la capacidad de redirigir los puertos a los servicios y del cual también se desprenden lineamientos de restricción de usuarios en una misma red, apoyada en los servicios de conectividad a internet desde Zentyal a través del puerto de salida 1230; esta condición permitió evidenciar un potencial incalculable de posibilidades de restricción y acceso desde la red creada, lo cual es significativo para coordinar esfuerzos en controlar el tráfico de red tanto desde el servidor como a partir de los equipos que hacen parte de la red, dando una panorámica más acertada como administradores del sistema informático y en conjunto con la red a la cual se está expuesta.

Ahora bien, el tema de File Server y Print Server deja en evidencia que la compartición de ficheros y de impresoras bajo el dominio de Zentyal es un proceso de configuración de gran importancia, ya que con el dominio configurado en el servidor todos los usuarios y maquinas unidas al sistema bajo un dominio se logra una comunicación fluida entre usuarios y máquinas. De esta manera el administrador del servidor puede implementar los permisos restringidos y necesarios para los usuarios en los ficheros compartidos. Lo significativo en este sentido es el alcance que se logra al permitir no solo compartir archivos sino el modo de gestión que implica su uso.

Con respecto al servicio de VPN, en este se puede apreciar que con la correcta descarga y configuración de los servicios VPN, se puede ingresar a nuestro servidor Zentyal y consumir los servicios o recursos que estén disponibles simulando que estuviera bajo la misma red, así el ordenador se encuentre en cualquier ubicación geográfica. Un aspecto a considerar con respecto a las VPN es el de la restricción específica de los usuarios que desean trabajar bajo segmentos de red específicos, es importante reconocer que cuando no se conocen los aspectos que denotan la red propiamente dicha estos pasan a elevar los niveles de seguridad de la red con respecto a reconocimiento de accesos y configuraciones específicas de uso de VPN aun entre sistemas operativos y/o distribuciones de linux diferentes.

En general los servicios tratados en este documentos solo constan de cinco aspectos o componentes de Zentyal, los demás aspectos configurables hacen del sistema una muy buena herramientas para apoyar a las empresas en sus procesos de desarrollo de administración de red, importante es definir los criterios de segmentos de red antes de configurar aspectos de seguridad y reconocer como trabajan de la mano cada uno de los componentes disponibles dentro de Zentyal, otro aspecto es el de los equipos disponibles en los que se pueden llevar a cabo pruebas, para nuestro caso virtualizados los cuales

aportan escenarios de simulación adecuados para idear los elementos de entornos reales de trabajo, pues mientras se presentan algunas fallas en la instalación de paquetes de cada uno de los componentes a utilizar, estos se ven relacionados a la arquitectura de los equipos en los que se pueda llegar a correr la distribución de Linux.

5 CITAS Y/O REFERENCIAS

- [1]. M, Cabrera (2018, 8 abril). Zentyal Server Instalación y primeros pasos detallados para ti YouTube. Youtube. Consultado en la página: https://www.youtube.com/watch?v=tG_NHAUYUbU&feature=youtu.be
- [2]. J, E, Martínez (25 de julio de 2015). Configuración de Servidor VPN con Zentyal [Archivo de Video]. Youtube. <https://youtu.be/2MjtTU0rMIM>
- [3]. Zentyal (26 de marzo de 2019). Tutorial: Instalación y configuración de Zentyal Server para la implementación de servicios de Infraestructura IT. Consultado en la página: <https://zentyal.com/es/news/tutorial-instalacion-y-configuracion-de-zentyal-server-para-la-implementacion-de-servicios-de-infraestructura-it/>
- [4]. Zentyal (s.f.). HTTP Proxy configuration in Zentyal. Consultado en la página: <https://doc.zentyal.org/en/proxy.html>
- [5]. Zentyal Community. Documentación Zentyal 6.2. Controlador de Dominio y Compartición de ficheros. Recuperado de <https://doc.zentyal.org/es/directory.html>
- [6]. Zentyal Org [Online]. Documentación de Zentyal 6.2. Instalación. Consultado en la página: <https://doc.zentyal.org/es/installation.html>
- [7]. Zentyal Org [Online]. Servicio de configuración de red (DHCP). Consultado en 8 de diciembre de 2020 en: <https://doc.zentyal.org/2.2/es/dhcp.html>
- [8]. Zentyal S.L. (s. f.). Zentyal 6.2 Documentación Oficial. Documentación de Zentyal 6.2. Zentyal. <https://doc.zentyal.org/es/>