

CONFIGURACION E IMPLEMENTACION DEL SERVICIO VPN (VIRTUAL PRIVATE NETWORK) SOBRE SERVIDORES ZENTYAL 6.2.

Miguel Angel Garcia Ferro
e-mail: magarciafe@unadvirtual.edu.co

RESUMEN: la implementación de un servicio VPN (Virtual Private Network) en un servidor basado en el sistema operativo Zentyal 6.2. El cual tiene la finalidad de conceder el acceso a usuarios remotos a intranets a través de la Internet, de igual manera permitir la conexión de manera segura a subredes distintas a través de redes no seguras.

Este servicio. Nos brinda un alto nivel de seguridad ya que el tráfico viaja encapsulado y sólo es posible leerlo en el otro extremo del túnel.

PALABRAS CLAVE: Certificado, Firewall, Linux, Vpn

1 INTRODUCCIÓN

El siguiente artículo tiene como finalidad, dar a conocer la instalación del sistema operativo Zentyal y la implementación del servicio Vpn, en la implementación se puede observar que este sistema operativo presenta varias funcionalidades y ventajas para proteger nuestra red empresarial en este caso Zentyal es una buena herramienta para administrar servicios y controlar el acceso a usuarios.

2 INSTALACION ZENTYAL

La instalación del sistema operativo se realizó desde la imagen iso la cual fue descargada de la página oficial de Zentyal, este instalador está basado en Ubuntu server. Dicha instalación se realizó desde una máquina virtual en VirtualBox, la cual en su configuración tiene el nombre ZENTYAL en memoria fue asignado un total de tamaño de 3747 MB y en disco fue 8GB.



Figura 1. configuración máquina virtual Zentyal.

Iniciada la máquina virtual, el primer paso de instalación que nos muestra el sistema operativo es escoger el idioma de preferencia, como se observa en la imagen 2

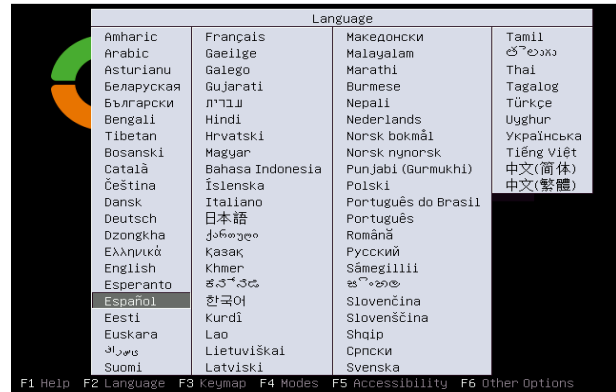


Figura 2. Idioma de instalación

con el idioma de preferencia inicia la ejecución del instalador, en la cual se tomó la primera opción delete all disk el cual elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal

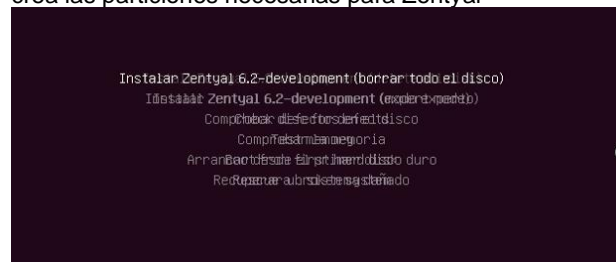


Figura 3. Inicio de instalación

En el paso siguiente se elige la configuración de la ubicación. Para ello escogemos el país en que nos encontramos, en este caso Colombia

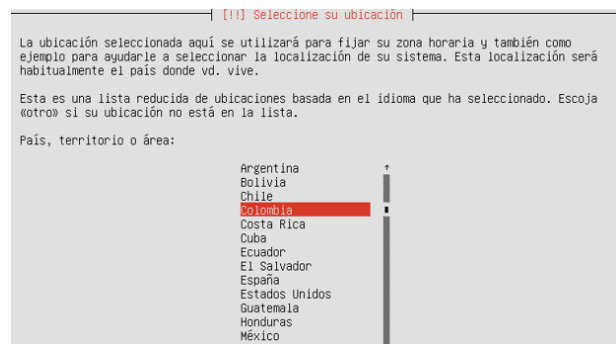


Figura 4. Selección de ubicación

Escogemos el idioma de nuestro teclado que para este caso se tomó la opción Spanish latinoamericana



Figura 5. Selección de idioma del teclado

Una vez establecido el idioma del teclado, pasamos a configurar la cuenta del administrador del sistema. Dicho usuario tiene todos los privilegios suficientes para la administración del sistema operativo y acceso a todos los recursos

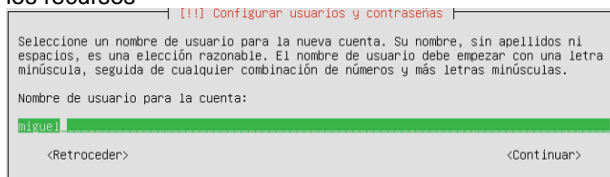


Figura 6. Configuración de usuarios y contraseñas

terminado el proceso de creación de usuario y contraseña se inicia el proceso de instalación de nuestro sistema básico este proceso puede durar entre 10 a 20 minutos.

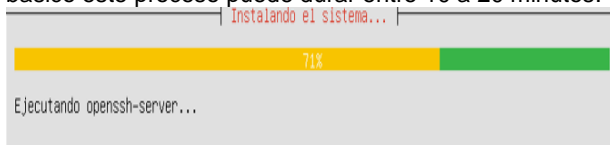


Figura 7. instalación del sistema base.

Al terminar la instalación del sistema base se extrae el disco de instalación y se reinicia el sistema.

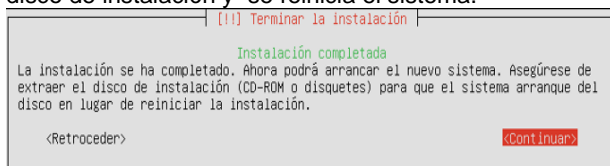


Figura 8. Instalación base completada

Una vez reiniciado el sistema operativo, se procede a cargar los componentes y paquetes necesarios para su primer inicio

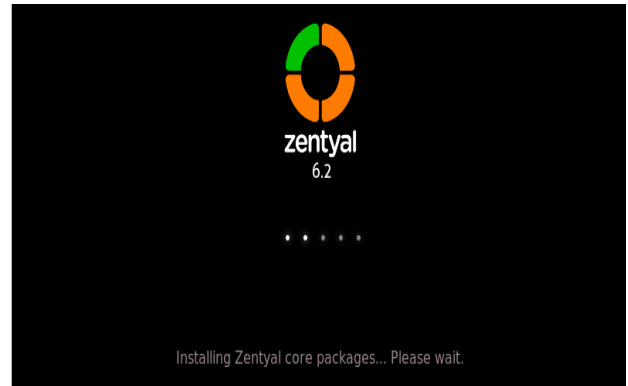


Figura 9. instalación core

Finalizado el proceso anterior el sistema operativo cargará su interfaz gráfica y accederemos a la administración que es una aplicación web con el fin de autenticarnos con las credenciales que se parametrizaron en el proceso configuración de usuarios y contraseñas



Figura 10. autenticación de usuario

Al autenticarse por primera vez nos mostrará un asistente de configuración



Figura 11. Asistente de configuración.

Seleccionamos la funcionalidad VPN la cual es la que incluiremos en nuestro sistema para poder realizar la práctica

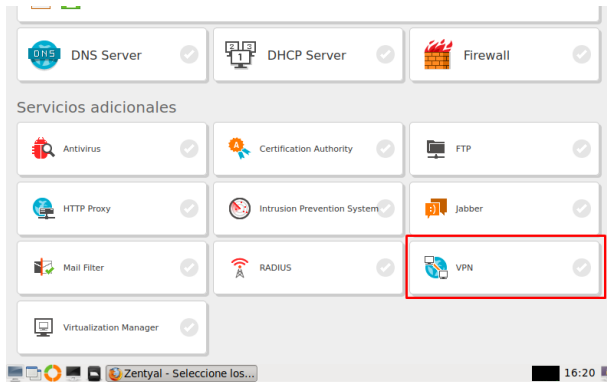


Figura 12. Selección de funcionalidad Vpn

En la instalación el sistema operativo nos muestra las dependencias necesarias para el módulo Vpn.

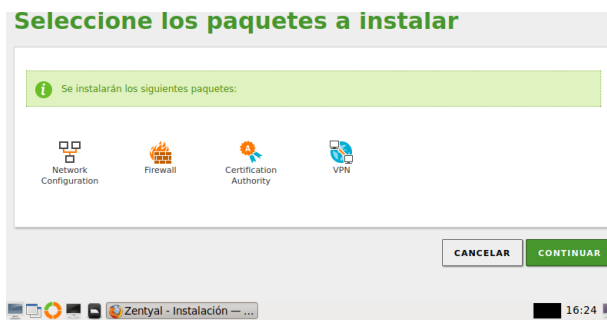


Figura 13. Instalación de paquetes adicionales.

Al terminar la instalación se puede evidenciar los nuevos módulos



Figura 14. Lista de módulos

Se activan los modulos de Red y Vpn como se aprecia en la siguiente imagen

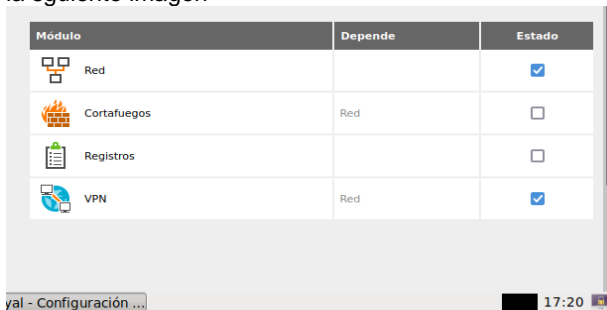


Figura 15. Lista de módulos activados

El primer proceso es crear una Autoridad de Certificación y certificados individuales para los dos

clientes remotos que crearemos mediante Autoridad de certificación → General.

Nombre	Estado	Fecha	Acciones
Certification Authority Certificate desde VPN-DIPLOMADO	Válido	2024-09-09 20:29:55	[Red] [Down] [Refresh]
vpn-VPN-DIPLOMADO12	Válido	2024-09-09 20:29:55	[Red] [Down] [Refresh]
VPN-DIPLOMADO	Válido	2024-09-09 15:33:15	[Red] [Down] [Refresh]

Figura 16. Certificados expedidos en el servidor

Con los certificados expedidos, se crea un nuevo servidor. El cual solo exige como requisito el nombre.



Figura 17. Creación del servidor

Procederemos a Configurar las reglas del firewall

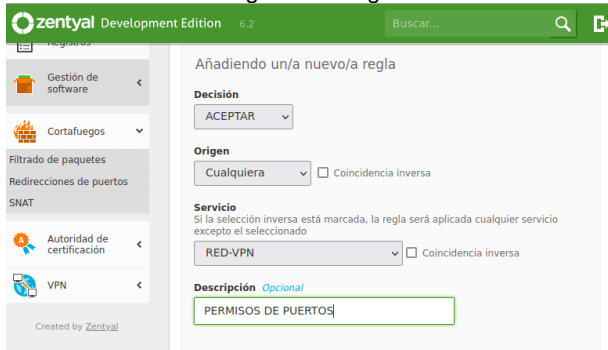


Figura 18. Configuración reglas de firewall

Procedemos a configurar los clientes. VPN la forma más sencilla de es manejando los bundles. Éstos son paquetes de instalación que incluyen el archivo de configuración VPN específico para cada usuario en este caso se escogió Windows como tipo de cliente y nuestro certificado creado en pasos anterior en esta configuración se establece la dirección externa del servidor a la cual los clientes VPN se deben conectar n este caso la ip es 192.168.0.18

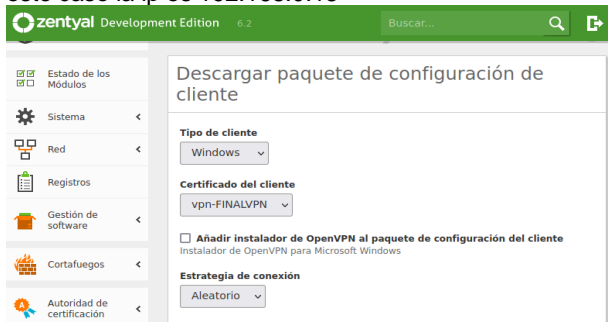


Figura 19. configuración de paquetes de configuración del cliente



Figura 20. configuración de paquetes de configuración del cliente

Configurado el cliente procedemos activar el servidor para que este se encuentre habilitado



Figura 21. activación del servidor vpn

Al guardar los cambios se revisa el módulo dashboard en el cual nos muestra que el servicio se encuentra habilitado

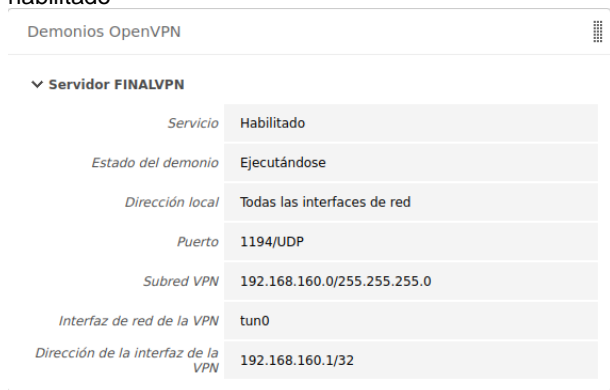


Figura 22 validación de configuración en el dashboard

Con la configuración terminada procedemos a descargar el certificado del cliente y lo alojamos en la maquina principal windows .

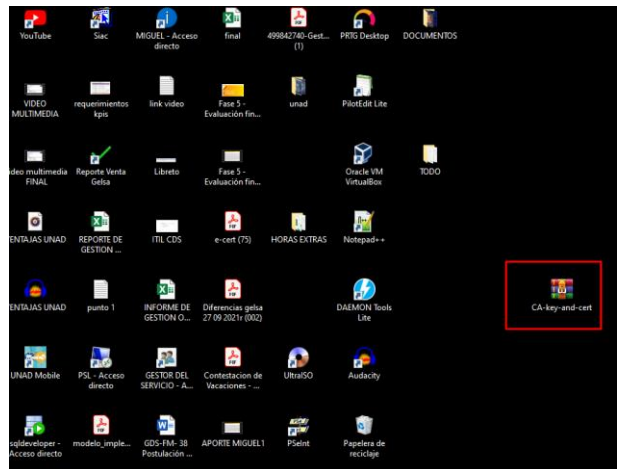


Figura 23. Copia de certificado en maquina cliente

Se procede a instalar la aplicación openvpn que sera nuestra aplicación que nos servira como puente de conexion.

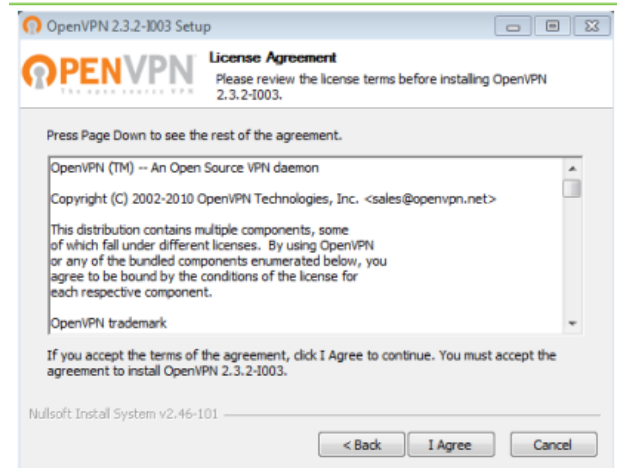


Figura 24. Instalación de aplicación openvpn

Al instalar la aplicación importamos el certificado que dejamos en la maquina principal

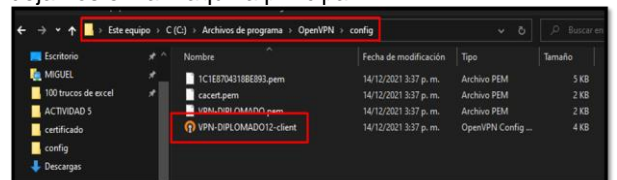


Figura 25. certificado cliente extraído

Realizamos la conexión desde openvpn para probar la configuración a nuestra vpn

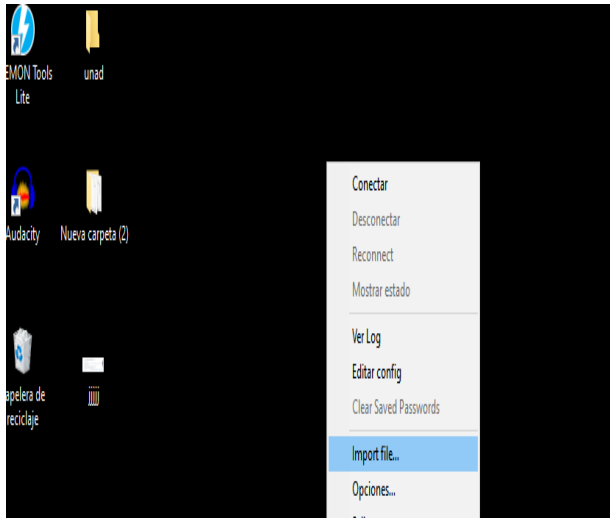


Figura 26. importación de certificado en la aplicación open Vpn

Validamos la conexión a la Vpn validando el log de conexion

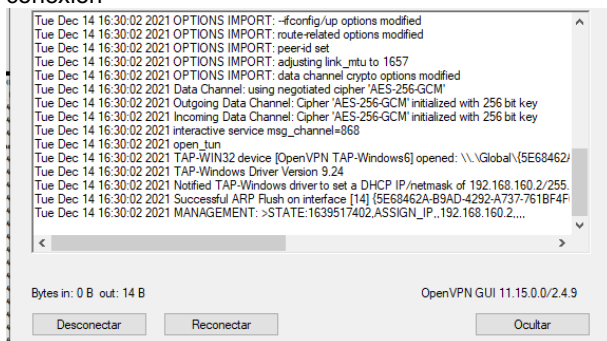


Figura 27. Validación del log para comprobar el estado de conexion

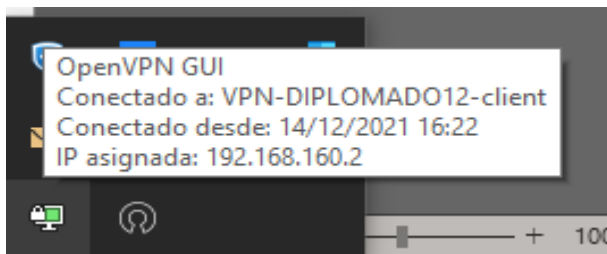


Figura 28. Conexión exitosa

3 CONCLUSIONES

Se realizó la correcta instalación del sistema operativo Zentyal en un ambiente virtualizado

Se logró implementar con éxito el servicio de VPN desde la distribución GNU/Linux Zentyal.

En el manejo del sistema operativo se puede concluir que es la distribución de Servidores más intuitiva y amigable que en la actualidad existe

4 REFERENCIAS

[1] Zentyal community. (s.f.). Obtenido de zentyal community: <https://doc.zentyal.org/en/>

[2] Zentyal community, " Configuración de un cortafuegos con Zentyal", Documentación de Zentyal 6.2. Disponible en: <https://doc.zentyal.org/6.2/es/firewall.html>

[3] Servicios de redes privadas virtuales (VPN) con OpenVPN Obtenido de : https://zentyal.com/wpcontent/themes/storefront/zentyalchild/assets/files/sample_chapter_zentyal_vpn_open_vpn_es.pdf