

Zentyal Server, como proveedor de servicios de infraestructura TI (Diciembre 2018)

Sandra M. Serna, Uriel A. Cuellar, John E. Pineda, Alexander Jaramillo Hernández
Escuela de Ciencias Básicas, Tecnología e Ingeniería, UNAD
Medellín, Colombia

smsernaa@unadvirtual.edu.co
 jepinedame@unadvirtual.edu.co
 ajaramillohe@unadvirtual.edu.co
 uacuellara@unadvirtual.edu.co

Resumen—

En el presente artículo se llevará a cabo la migración y puesta en marcha de los sistemas de seguridad de la infraestructura de red, mediante el uso del GNU/LINUX basado en Ubuntu "Zentyal", implementando servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas.

Abstract—

In this article the migration and implementation of the security systems of the network infrastructure will be carried out, through the use of the GNU / LINUX based on Ubuntu "Zentyal", implementing higher level IT infrastructure services for Intranet and Extranet in complex institutions.

Palabras Clave— Open Source, Zentyal Server, DHCP server, DNS server, Cortafuegos, Proxy, VPN, controlador de dominio.

I. INTRODUCCIÓN

Al momento de pensar en seguridad para una red informática, el uso de servidores ha tomado un papel importante, ya que permiten establecer un control del tráfico entrante y saliente, la creación de un dominio y todo lo relacionado con la infraestructura de la red.

Por ello, distribuciones GNU/LINUX como Zentyal se han convertido en herramientas importantes por los diferentes servicios ofrecidos para una infraestructura IT. Por mencionar algunos de estos servicios como; Firewall, servidor de email, controlador de dominio, Servidor DHCP y DNS, servicio de filtrado de páginas mediante Proxy, entre otros.

En el presente artículo, se realizará la instalación de un DHCP server, DNS server y controlador de dominio, filtrado mediante un PROXY no transparente, instalación y configuración de un cortafuego, y montaje de una red VPN, File Server, Print Server. Realizando pruebas del funcionamiento de cada uno de los servicios de forma remota mediante un cliente Ubuntu y evidenciando cada uno de los resultados obtenidos.

II. PROXY NO TRANSPARENTE

En la actualidad la seguridad en las redes es más vulnerable frente a los ataques cibernéticos ya que las redes siempre están expuestas al conectarse a otras redes, es por ellos que los servidores proxy juegan un papel importante principalmente en redes corporativas, gubernamentales en donde el tráfico de información es elevado. Un servidor proxy actúa como

intermediario entre un cliente de internet y un servidor permitiendo el filtrado de la información, bloqueo de dominios, mantener anonimato de los clientes, mejorar el rendimiento de la red, entre otras.

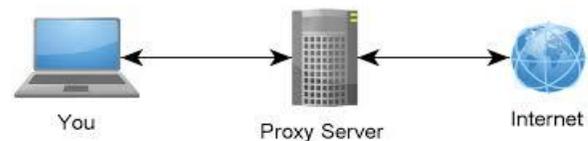


Fig. 1 Conexión a internet a través de un proxy

Existen servicios tales como Zentyal server basado en Ubuntu que permiten la administración de redes y que dentro de su portafolio contiene una serie de módulos en los cuales encontramos un servicio de proxy HTTP; el cual se instala a través de una interfaz gráfica web, para el cual realizamos la respectiva configuración para el tipo de proxy a configurar transparente o no transparente, así como el control de acceso y las reglas de filtrado sobre los dominios a restringir o permitir acceso.

Gracias a la interfaz tan amigable de Zentyal no se requiere de ser un profesional en Ubuntu para administrar este servicio, solo se requiere definir qué tipo de configuraciones se pretende realizar, que tipos de bloqueos se quieren llevar a cabo; tales como restringir totalmente el acceso a ciertos sitios web, permitir la descarga de cierto contenido con el fin de garantizar una navegación segura por medio de un servidor proxy.

Es necesario comprender que mientras se tenga acceso a la red existe un alto riesgo de responder a solicitudes que pongan en riesgo la seguridad del equipo o estación de trabajo; es por esto que en una red se deben implementar las mejores políticas de seguridad y configurar un proxy es una de ellas; aunque esto no quiere decir que no se esté expuesto a los ataques cibernéticos y se requiera reforzar aparte de configuración a través del proxy, otras reglas o medias.

Para finalizar este apartado podemos decir que, aunque el servidor proxy HTTP de zentyal sea un método seguro para prevenir riesgos en una red, nuestra era tecnológica desarrolla

a diario herramientas con el fin de vulnerar la seguridad o descubrir sus fallas para hacerlas más fuertes, por ende, existen otros servicios que se pueden manejar de manera integral con el servidor proxy que permiten un mejor control de acceso.

III. CORTAFUEGOS

Producto esperado: 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 Ubuntu Desktop.

En primer lugar, es necesario tener instalado el paquete de Network Configuration, ya que en este se configuran las interfaces de red necesarias para el funcionamiento del firewall.

Para instalar éste paquete es necesario dirigirse al módulo “Gestión de software” y luego “Componentes de Zentyal”, una vez allí se selecciona el paquete de Network Configuration y se da clic en instalar.

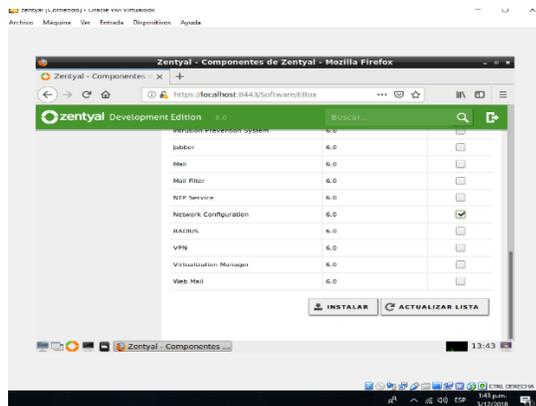


Fig. 2 Instalación de Network Configuration

Después concluir la instalación, aparecerá un módulo llamado “Red” en el cual se pueden configurar las interfaces de red, estas interfaces permitirán la comunicación entre el servidor y el cliente en la red local o LAN y la segunda interface será utilizada para el acceso a internet o red WAN.

La primera interface que se configurará será la eth0, la cual tendrá como método DHCP y tendrá marcada la opción “Externo (WAN)” ya que esta será utilizada para tener salida a internet.

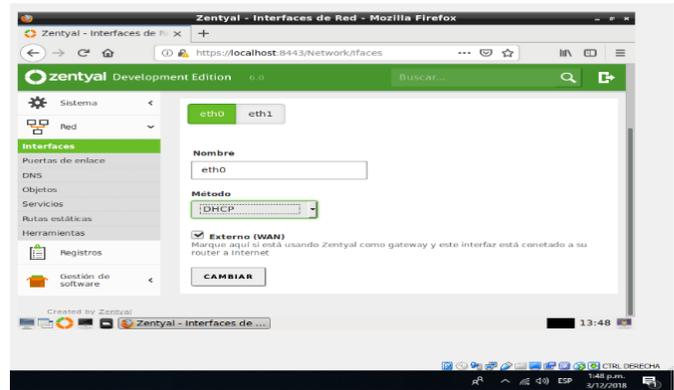


Fig. 3 Configuración de la interface eth0

La segunda interface será la eth1, ésta interface tendrá como método estático y como dirección IP 192.168.0.11, dirección que será utilizada para la comunicación entre el cliente y el servidor en la red LAN.

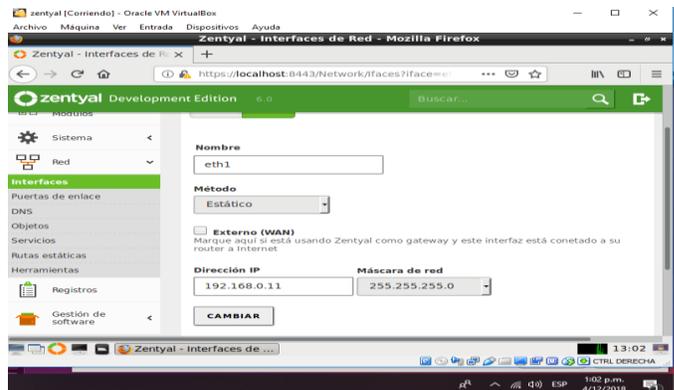


Fig. 4 Configuración de la interface eth1

Luego de configuradas las interfaces, se debe agregar una dirección del servidor DNS para resolver las direcciones al momento de navegar en internet, para ello se agrega el servidor DNS de google el cual es el 8.8.8.8

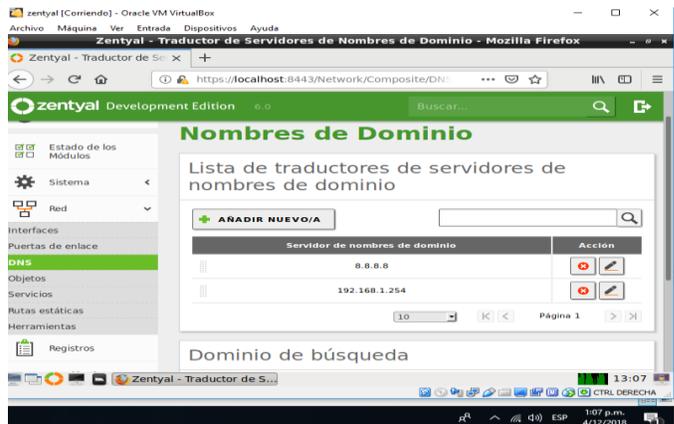


Fig. 5 Nombres de dominio DNS

Se guardan los cambios realizados y nuevamente es necesario dirigirse al módulo de “Gestión de software”, “Componentes de Zentyal” para descargar e instalar el paquete de Firewall ya

que con las configuraciones de red realizadas en los pasos anteriores Zentyal debe estar conectado a internet.

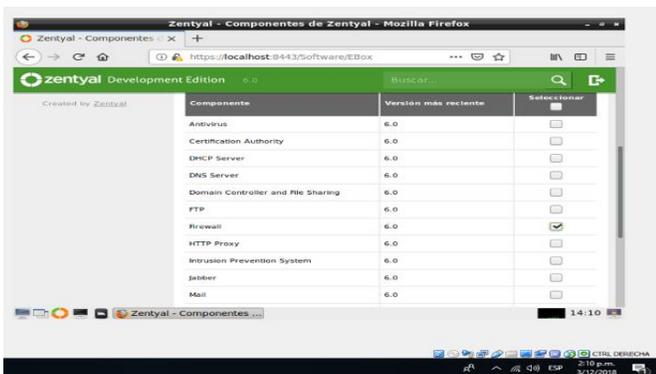


Fig. 6 Descarga e instalación del Firewall

De igual forma se debe configurar el cliente para que se conecte al segmento de red correcto, para ello se le asigna una dirección IP estática 192.168.0.2, con la dirección IP del servidor como puerta de enlace y servidor DNS, además el DNS de google 8.8.8.8 para las direcciones al navegar por internet.

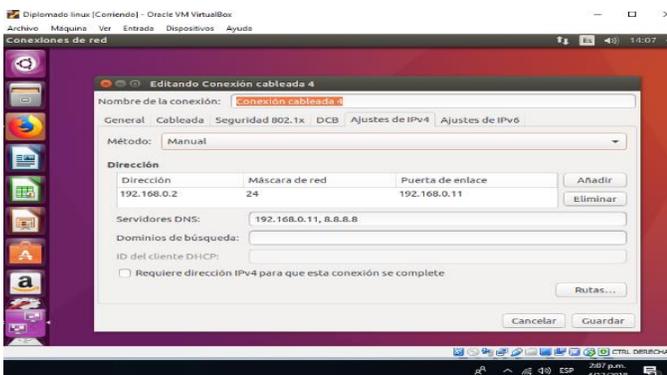


Fig. 7 Configuración del cliente

Para crear la restricción a un sitio web mediante el Firewall, primero se debe crear el objeto en el módulo de red, ya que un sitio web puede tener múltiples direcciones y utilizando un objeto se pueden asociar todas las direcciones pertenecientes al mismo sitio web. Estas direcciones IP se pueden obtener haciendo ping al sitio web, por ejemplo, con Facebook se puede hacer ping a www.facebook.com y es-la.facebook.com para obtener direcciones diferentes pertenecientes al mismo sitio.

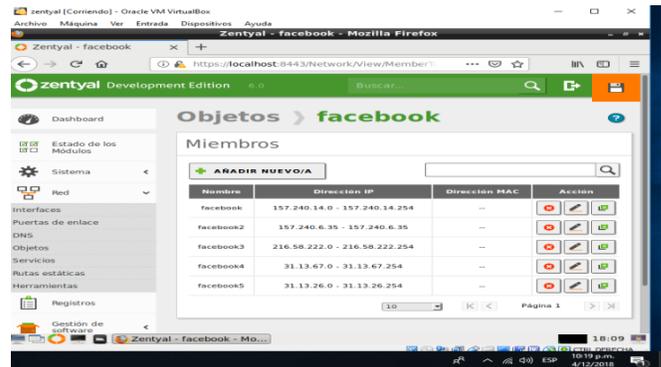


Fig. 8 Creación del objeto Facebook y direcciones IP del sitio

Ya con el objeto creado, es necesario desplazarse al módulo de Firewall y luego a la opción "Reglas de filtrado para las redes internas". Se configura una nueva regla utilizando el objeto "Facebook" creado en el módulo de red, prohibiendo la salida o el destino a la página en el servicio de HTTPS.

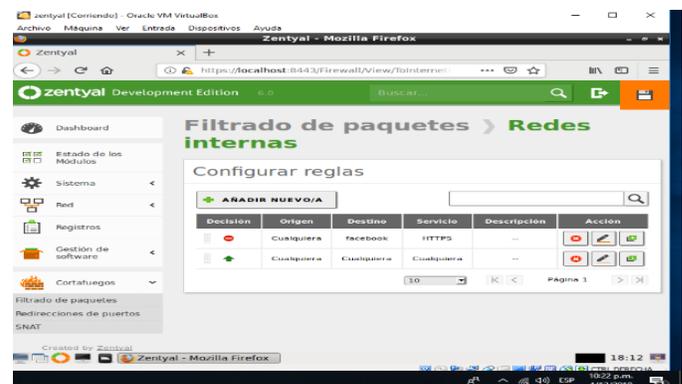


Fig. 9 Regla de firewall para redes internas

Ahora se debe probar el acceso al sitio web por medio del cliente, para ello se escribe la dirección www.facebook.com en el navegador.

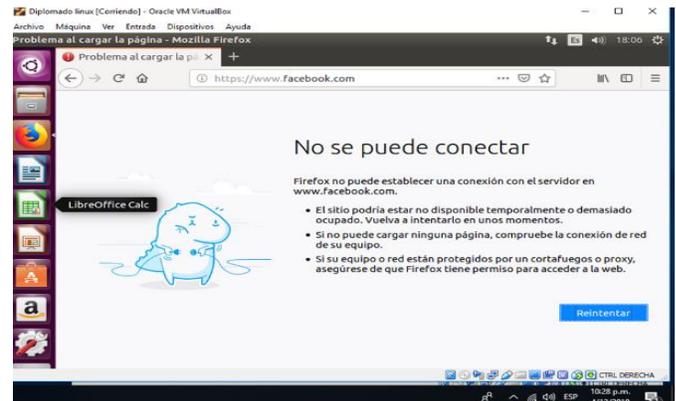


Fig. 10 Prueba de acceso a Facebook

Para finalizar, se realiza la misma prueba con un sitio diferente para verificar que la regla solo este aplicando para Facebook, para ello se ingresa la dirección www.wikipedia.com



Fig. 11 Prueba de acceso a otro sitio web

IV. FILE SERVER Y PRINT SERVER

Un servidor de archivos es aquel que guarda diferentes tipos de archivos y que los distribuye dentro de una red de computadoras. Tiene la función de permitir que se efectúe el acceso remoto a archivos almacenados dentro de él o que los son directamente accesibles.

En la práctica cualquier computadora conectada a una red, con un software adecuado, puede funcionar como un servidor de archivos. Pero para tener un manejo más profesional y contar con el respaldo de un software contamos con Zentyal Server, que nos permita administrar adecuadamente los archivos de nuestra empresa brindando seguridad y facilidad de acceso a la información solicitada.



Fig. 12 Zentyal Server

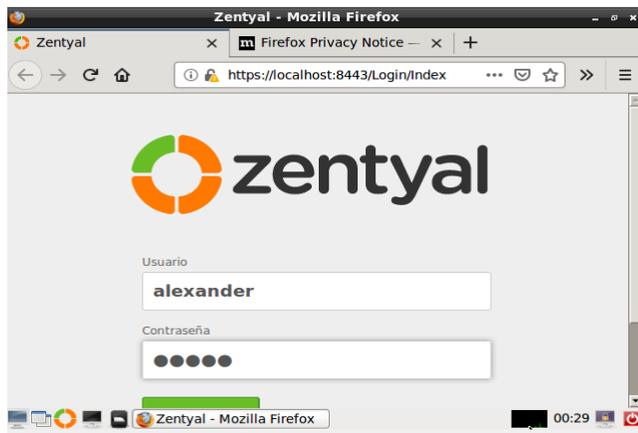


Fig. 13 Acceso a Zentyal Server

Hoy en día, en la mayoría de las empresas pequeñas, medianas o grandes del mundo, empleados y personal de dirección imprimen los incontables documentos que necesitan para hacer sus trabajos, sin embargo, pocas (o ninguna) de estas personas sabe realmente cómo circulan los datos de impresión desde la aplicación original hasta el dispositivo donde recogen el documento, o sea desconocen el concepto técnico de éste tipo de recursos que tenemos a nuestra disposición.

En algún lugar entre la aplicación del usuario y la impresora de destino, existen normalmente uno o más servidores de impresión; se trata de ordenadores o máquinas virtuales gestionadas normalmente por personal de la empresa calificado técnicamente y que es el responsable de que éste servicio sea transparente para el cliente. Los servidores de impresión aíslan las aplicaciones de negocio de la carga de tener que gestionar directamente el flujo de información hasta el dispositivo físico de impresión, esto genera muchas ventajas, por ejemplo, un usuario puede imprimir, aunque el dispositivo de destino esté desconectado o haya un atasco en la impresora, en lugar de bloquear la estación de trabajo del usuario con mensajes de error, el servidor de impresión mantiene los datos de impresión en su cola hasta que la impresora vuelva a estar conectada; es por esto, que Zentyal Server es una Sistema Operativo versátil para administrar éste tipo de servicios de una manera transparente y de forma eficiente. De forma similar Zentyal permite compartir a todos nuestros usuarios carpetas, archivos, de tal forma que puedan tener accesos a ellos bajo unas políticas Jerárquicas y niveles de permisos.

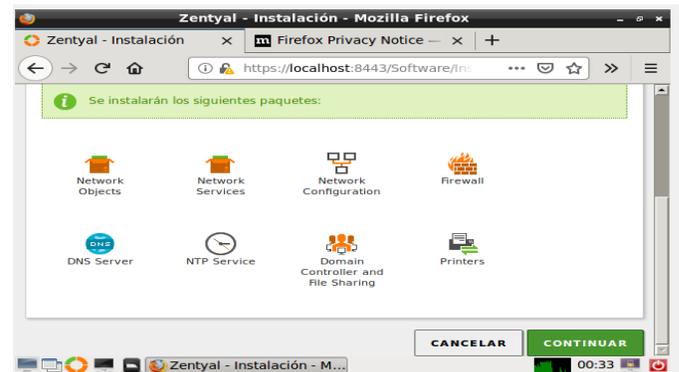


Fig. 14 Módulo de Impresión Zentyal Server



Fig. 15 Módulo de Compartición de Ficheros Zentyal Server

V. VPN

Las **redes privadas virtuales**, nos permiten acceder a nuestra red empresarial mediante una conexión remota, por medio de internet los usuarios establecen una comunicación segura desde otras subredes.

Es muy frecuente que en las empresas necesiten acceder a los recursos de sus servidores mientras se encuentran conectados en otras redes menos seguras, como redes públicas no confiables, en la actualidad existen modelos como el teletrabajo o e-commerce, modelos que representan nuevos retos en cuanto a mantener la confidencialidad, integridad y disponibilidad de la información, activo más valioso actualmente en las compañías.

Las ventajas de implementación de Zentyal integrando OpenVPN, se fundamentan en la autenticación mediante infraestructura de clave pública, maneja un cifrado usando tecnología SSL, permite conexión con clientes Windows, Mac OS y Linux, es muy sencillo de instalar e intuitivo para configurar y mantener, además de ser software libre. Todo este andamiaje nos ofrece el evento de usar programas de red transparentemente.

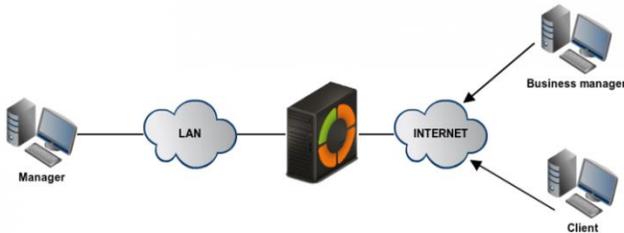


Fig. 16 VPN road-warrior

Para iniciar con la configuración de un servidor VPN, debemos primero verificar las Interfaces de red eth1 y organizar una subred,



Fig. 17 VPN Interfaces de red

Seleccionamos el módulo VPN y creamos un Certificado de la autoridad de certificación para iniciar.

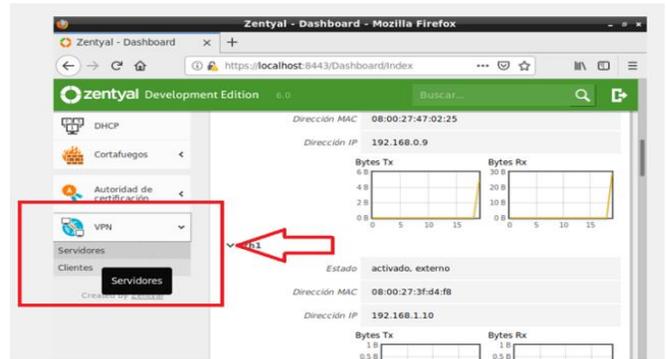


Fig. 18 Selección Modulo VPN

En esta opción encontramos /servidores, allí está la lista de nuestros servidores VPN

Lista de servidores



Fig. 19 Lista de servidores VPN

Se requiere para nuestro objetivo, el cual es conectar al servidor de datos otro cliente remoto, crear una Autoridad de Certificación y sus respectivos certificados individuales para los clientes remotos. Esto se debe crear mediante el menú Autoridad de certificación / General.

Lista de Certificados actual

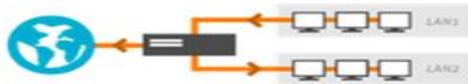
Nombre	Estado	Fecha	Acciones
unadlinux Authority Certificate desde unadlinux	Válido	2028-12-08 02:18:30	[Eliminar] [Descargar] [Actualizar]
vpn-UNADLINUX	Válido	2028-12-08 02:18:30	[Eliminar] [Descargar] [Actualizar]
LINUXVPN	Válido	2021-09-04 21:28:47	[Eliminar] [Descargar] [Actualizar]

Fig. 20 lista de certificados actuales

Luego configuramos nuestro servidor mediante /Crear un nuevo Servidor

Fig. 21 Configurar Servidor Nuevo

Configuramos reglas en los cortafuegos de Zentyal para el filtrado de paquetes en las redes internas.



Reglas de filtrado para las redes internas
Estas reglas le permiten controlar el acceso desde sus redes internas a Internet, y el tráfico entre sus redes internas. Si desea dar acceso a los servicios de Zentyal, debe usar la sección superior.

Fig.22 Filtrado de paquetes

En la siguiente imagen se puede observar “DEMONIOS OpenVPN” servidor UNADLINUX habilitado y en ejecución

Demonios OpenVPN	
Servidor UNADLINUX	
Servicio	Habilitado
Estado del demonio	Ejecutándose
Dirección local	Todas las interfaces de red
Puerto	1194/UDP
Subred VPN	192.168.160.0/255.255.255.0
Interfaz de red de la VPN	tun0
Dirección de la interfaz de la VPN	192.168.160.1/32

Fig.23 Servidor en Ejecución “DEMONIOS OpenVPN”

Después de configurar el Servidor, generamos y descargamos los archivos necesarios para la conexión de los clientes según el sistema operativo.

Fig.24 Paquete de configuración de cliente

Este paquete que se genera debe ser descargado en el cliente y configurado.



Fig.25 Descarga Paquete de configuración de cliente

Ejecutamos el instalador openvpn-install-2.46-1602.exe

Nombre	Fecha de modifica...	Tipo	Tamaño
A969F5C01C63DD04.pem	11/12/2018 06:31 ...	Archivo PEM	5 KB
cacert.pem	11/12/2018 06:31 ...	Archivo PEM	2 KB
LINUXVPN.pem	11/12/2018 06:31 ...	Archivo PEM	2 KB
openvpn-install-2.4.6-1602.exe	28/10/2018 09:43 ...	Aplicación	3,771 KB
UNADLINUX-client.ovpn	11/12/2018 06:31 ...	Archivo OVPN	4 KB

Fig.26 InstaladorOpenVPN

Luego en la barra de tareas seleccionamos la conexión a la VPN indicada con los usuarios asignados

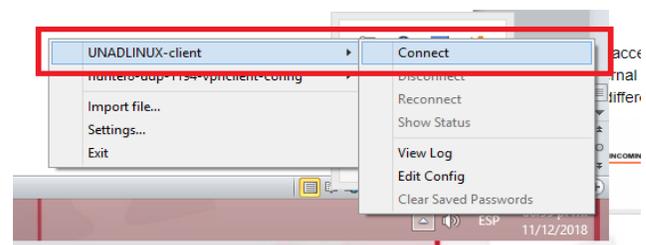


Fig.27 Conexión a OpenVPN

De esta forma ya se puede disfrutar de los recursos de la red interna a través de internet.

VI. CONCLUSIONES

Con el desarrollo de las anteriores temáticas, se logra un afinamiento y puesta en marcha de los contenidos GNU/LINUX específicamente la distribución Zentyal, claramente queda en evidencia que se puede configurar para dar soporte a clientes remotos también conocidos como Road Warriors. Se puede poner en marcha un servidor Zentyal que trabaja como puerta de enlace y como servidor VPN, que tiene

una red de área local detrás, permitiendo a los clientes conectados en redes externas conectarse a la red local vía servicio VPN. Permitiendo la autenticación mediante infraestructura de clave pública, cifrado basado en tecnología SSL que brinda la posibilidad de usar programas de red de forma transparente.

Con la implementación del servicio Proxy HTTP de zentyal se permite filtrar la navegación de las terminales que acceden a internet a través de una red, utilizando políticas de filtrado en las cuales se puede definir los sitios web o dominios que se quieren controlar definiéndose las reglas que una organización considere importante controlar o monitorear. Los servidores Proxy como intermediario de servidores cliente garantizan el filtrado de las peticiones realizadas impidiendo de esta forma vulnerar la seguridad de sitios malintencionados; además un servidor proxy en combinación del servidor firewall puede tener mayor certeza de filtrado en una red.

Se implementó un módulo de Cortafuego, añadiendo los rangos de direcciones IP que pertenecen al dominio del sitio web mediante un objeto, con el objetivo de prohibir cualquier intento de acceso a estos rangos IP destino mediante la creación de una regla, además, se realizaron las pruebas mediante el cliente Ubuntu, obteniendo resultados positivos ya que el Cortafuego permite el acceso a cualquier otra página a excepción de la o las páginas cuyos rangos direcciones IP fueron añadidos en la regla creada para denegar el acceso.

Implementar los servicios de File Server y Print Server dentro de una Pyme al plantear un proyecto tecnológico basado en Zentryal, garantizan que se optimicen los recursos financieros al momento de presupuestar el hardware y software requeridos frente a otras alternativas del mercado. Los usuarios puedan acceder de una forma rápida y transparente a compartir directorios, archivos, e impresoras, todo éste entorno de producción, es fundamental para que las pymes transiten en su evolución tecnológica de una forma adecuada y segura.

Es claro, que éstos servicios siempre tienen que ir acompañados de políticas de seguridad y acceso que también hacen parte de las características de Zentryal, como lo es el uso de VPNs y Firewall entre otros.

AGRADECIMIENTOS

Agradecimientos a la Universidad Nacional Abierta y a Distancia – UNAD, universidad pública, y en especial a nuestro Director Daniel Andrés Guzmán, que estuvo siempre presto a orientarnos en todos los conceptos técnicos desarrollados en éste Diplomado de profundización en Linux y que fueron fundamentales para el desarrollo del presente artículo.

REFERENCIAS

- [1] “Download Zentyal Server | Linux Small Business Server.” Accessed December 5, 2018. <http://www.zentyal.org/server/>.
- [2] “Zentyal S.L – Edición BSSC- C/ Eduardo Ibarra Zaragoza España” <http://www.zentyal.com>
- [3] “Alfonso, G. (2016) Zentyal 4.2 Funcionamiento y Recomendaciones de Seguridad [Video]. Recuperado de: <https://www.youtube.com/watch?v=BGDN-7Ve6z0&t=370s>”
- [4] “Antonio, L. (2016) Configuración do firewall en Zentyal [Video]. Recuperado de: <https://www.youtube.com/watch?v=kESyHFFoX-E>”
- [5] “Marín, D. (2018) Zentyal 4.1 crear carpetas e impresoras para compartir Parte 2 [Video]. Recuperado de: <https://www.youtube.com/watch?v=OY2X4x5ti8Q&t=11s>