

Administración y control de GNU/Linux Zentyal Server 5.0 como sistema operativo base para disponer de los servicios y plataformas de infraestructura IT

María Lucia Rueda Nieto – Código: 51967755, Rossana Rodríguez Reyes – Código: 46383168,
Carmen Beatriz Ramírez – Código: 43788120, Myriam Judith González Deantonio – Código:
52832993, Luz Mary Useche Salgado – Código: 40078455

Resumen— Este trabajo está orientado a la administración y control de una distribución GNU/Linux basada en Ubuntu, enfocada a la implementación de servicios de infraestructura IT de mayor nivel para intranet y Extranet en instituciones complejas. La distribución que se trabaja es GNU/Linux Zentyal Server 5.0 la cual es instalada y configurada como sistema operativo base para disponer de los servicios y plataformas de infraestructura IT. Los servicios y plataformas explicados en este trabajo son DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN.

Palabras Clave— GNU/Linux, Zentyal, Servicios, DHCP, DNS, Controlador de dominio, Proxy, Cortafuegos, VPN, Infraestructura.

I. Introducción

A través del desarrollo de esta actividad se pretende adquirir conocimiento sobre la administración y control de la distribución GNU/Linux Zentyal Server 5.0 basada en Ubuntu, enfocándonos a la implementación de servicios de infraestructura IT de mayor nivel para intranet y Extranet.

Se realiza la instalación y configuración de Zentyal Server 5.0 como sistema operativo base para disponer de los servicios y plataformas de infraestructura IT. Como aplicación práctica con esta actividad se pretende en primer lugar configurar una estación de trabajo GNU/Linux Ubuntu Desktop a la cual controlar el acceso a través de un usuario y contraseña dejando el registro de dicha estación en los servicios de Infraestructura IT de Zentyal mediante DHCP Server, DNS Server y el Controlador de Dominio, como segundo paso tener el control de acceso desde la estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128. Como tercera etapa mediante el cortafuegos se pretende lograr la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas anteriormente así como mostrar la validación

del funcionamiento del cortafuego aplicando las restricciones solicitadas, en un cuarto paso se pretende dar a la estación el acceso a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras y por último en un quinto paso se quiere evidenciar la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo configurada. Los roles y temáticas asignadas por cada integrante del grupo se describen a continuación.

Tabla 1 Roles y temáticas del grupo 201494_4		
Nombre	Rol	Temática
María Lucia Rueda Nieto	Compilar	Temática 1: DHCP Server, DNS Server y Controlador de Dominio.
Rossana Rodríguez Reyes	Evaluador	Temática 2: Proxy no transparente
Carmen Beatriz Ramírez	Revisor	Temática 3: Cortafuegos
Myriam Judith González	Entrega	Temática 4: File Server y Print Server
Luz Mary Useche	Alerta	Temática 5: VPN

II. Zentyal Server 5.0

A. Que es

Zentyal es un servidor basado en la arquitectura GNU/Linux, que permite a los profesionales de TI administrar los principales servicios de una red informática como son el acceso a Internet, la seguridad de la red, la compartición de recursos, la infraestructura de la red a través de una única plataforma y sobre una interfaz visual amigable e intuitiva. Zentyal incorpora aplicaciones independientes en funciones totalmente integradas que automatizan la mayoría de las tareas. Se desarrolló con el objetivo de acercar Linux a las pequeñas y medianas empresas y permitirles aprovechar al máximo su potencial como servidor corporativo.

Zentyal está constituida como la primera implementación nativa del conocido Directorio Activo de Microsoft en ambientes Linux con sencillez de implementación.

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

B. Características generales

Zentyal Server incorpora servicios de red que son necesarios en un entorno empresarial a nivel pequeño y mediano tales como:

- ✓ Servidor de oficina
- ✓ Servidor de comunicaciones unificadas
- ✓ Puerta de enlace a internet (Gateway)
- ✓ Servidor de infraestructura de red

Zentyal Server 5 se especializa en una mayor compatibilidad con Windows Server y Active Directory. Es compatible de forma nativa con Microsoft Outlook®. e implementa protocolos Microsoft® Exchange sobre componentes estándares de código abierto como Dovecot, Postfix, Samba entre otros para proporcionar compatibilidad nativa con clientes Microsoft Outlook®.

Los protocolos de correo electrónico soportados por Zentyal son: MAPI, ActiveSync, EWS, SMTP, POP, IMAP, CalDAV, CardDAV y Active Directory.

Zentyal Server tiene una edición de desarrollo gratuita y cuyo código fuente está disponible bajo los términos de la GNU (General Public License).

Zentyal se distribuye en dos paquetes:

- ✓ Zentyal Server para PYMEs
- ✓ Zentyal Cloud para proveedores de hosting.

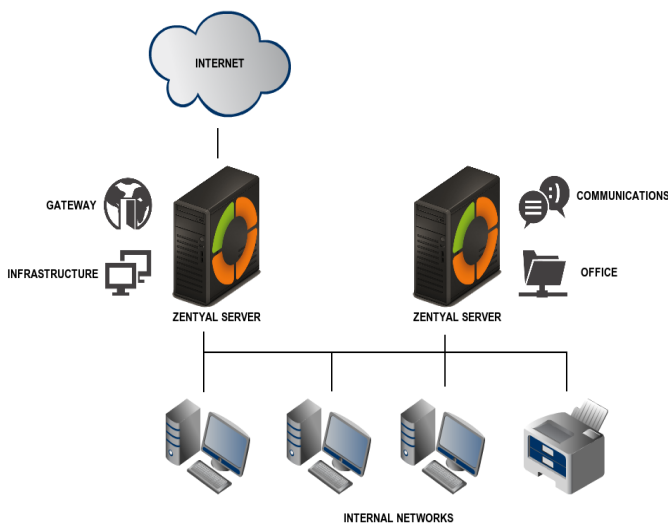


Fig.1. Implementación de Zentyal realizando diferentes roles.

C. Características por categoría

Existen diversas características que hacen de Zentyal una solución poderosa y están divididas por categorías de la siguiente forma:

1) Dominio y Directorio

- ✓ Gestión central de dominios y directorios
- ✓ Creación de Usuarios, Grupos de seguridad, Listas de distribución y Contactos
- ✓ Admite múltiples unidades organizativas (OUs) y objetos de directiva de grupo (GPO)
- ✓ Soporta scripts NETLOGON y perfiles móviles
- ✓ Autenticación de inicio de sesión único (SSO)
- ✓ Sistemas operativos compatibles con Zentyal: Windows® XP / Vista / 7/8/10
- ✓ Permite compartir archivos en entornos Windows (CIFS)
- ✓ Brinda permisos de acceso y modificación de usuarios y grupos (ACL)

2) Correo electrónico

- ✓ Soporta los protocolos: SMTP, POP3, IMAP, CalDAV, CardDAV, SIEVE
- ✓ Clientes soportados: Mozilla Thunderbird
- ✓ Soporta Webmail
- ✓ Sincronización con dispositivos móviles a través de ActiveSync
- ✓ Admite dominios de correo virtual
- ✓ Autenticación de inicio de sesión único (SSO)
- ✓ Gestión a través de Zentyal o Microsoft Active Directory
- ✓ Incluye antivirus y filtro de correo

3) Gateway

- ✓ Posee diversos valores de configuración de la red
- ✓ Enrutamiento
- ✓ Gateway
- ✓ Cortafuegos
- ✓ Proxy HTTP
- ✓ Incluye tecnología de balanceo del tráfico
- ✓ Conmutación por error de WAN

4) Infraestructura

- ✓ Servidor DNS
- ✓ Servidor DHCP
- ✓ Servidor NTP
- ✓ Autoridad de Certificación (CA)
- ✓ Redes privadas virtuales (VPN)
- ✓ Servicio de mensajería instantánea (MI)

D. Requisitos de hardware

Zentyal funciona sobre arquitecturas estándar x86 (32-bit) o x86_64 (64-bit).

Al estar modularizado los requerimientos de hardware dependen de los módulos que se instalen

Algunos módulos como Cortafuegos, DHCP o DNS tienen bajo requerimiento, pero normalmente los servicios como el

Filtrado de correo o el Antivirus necesitan más memoria RAM y CPU.

Los siguientes requerimientos son los mínimos recomendados para un servidor de uso general con los patrones de uso normales:

TABLA 2 REQUISITOS DE HARDWARE					
Perfil de Zentyal	Usuarios	CPU	Memoria	Disco	Tarjeta Red
Puerta de acceso	<50 50 o mas	P4 o superior	2G	80G	2 o mas
		Xeon Dual Core o superior	4G	160G	
Infraestructura	<50 50 o mas	P4 o superior	1G	80G	1
			2G	160G	
Oficina	<50 50 o mas	P4 o superior Xeon Dual Core o superior	1G	250G	1
			2G	500G	
Comunicaciones	<100 100 o mas	Xeon Dual Core o equivalente	4G	250G	1
			8G	500G	

E. Instalación y configuración



Fig.2. Símbolo de Zentyal

- Se descarga la imagen ISO
- Se puede instalar de dos formas sobre máquina virtual o directamente sobre un servidor
- Si se instala sobre máquina virtual esta debe crearse y seleccionar la imagen para iniciar la instalación
- Si se instala directamente sobre un servidor debe grabarse la imagen en un disco DVD o en un medio USB booteable para arrancar el equipo desde allí.
- Luego se accede a la BIOS del equipo y se establece el orden de arranque desde la opción adecuada, USB o CD/DVD.
- Luego de que arranque el equipo o la máquina virtual cualquiera que se haya escogido se inicia la instalación así:
 - Se define el idioma de instalación
 - Se selecciona la opción Install Zentyal 5.0.1-development (expert mode)
 - Se selecciona el idioma con el cual se configurará el proceso de instalación
 - Se selecciona la ubicación geográfica

- Se configura el teclado, ahí se puede o no probar la distribución del teclado
- Se selecciona la ubicación geográfica del teclado.
- Se define la distribución del teclado
- Se inicia el proceso de detección y comprobación de hardware
- Se asigna un nombre al servidor
- Se define el nombre de usuario de Zentyal
- Se asigna contraseña
- Se confirma la contraseña ingresada
- Se inicia la detección de zona horaria
- Se identifica y se confirma la ubicación
- Ya con todos estos pasos concluidos el sistema inicia la detección de discos
- Se selecciona la opción Guiado – utilizar todo el disco
- Se selecciona el disco donde se ha de instalar Zentyal
- Se confirma que se desea escribir la tabla de particiones en el disco.
- Se presenta la opción para instalar o no con entorno gráfico, para este caso se dirá que si se desea la instalación de este entorno.
- Por lo que se inicia automáticamente este proceso de instalación.
- Durante este proceso se verá una nueva ventana donde se solicita que se agregue una dirección de proxy para configurar el gestor de paquetes e instalar el software
- En caso de no contar con un servidor proxy se puede dejar esta opción en blanco
- El instalador configurará el gestor de paquetes apt, descarga e instala todo el software Zentyal necesario y el gestor de arranque GRUB útil para gestionar el arranque del sistema.
- Al instalar el cargador de arranque de GRUB se solicita que se instale el gestor de arranque de GRUB en su sector de MBR del disco duro, para lo cual se selecciona Sí
- Cuando el proceso de instalación llega al punto final, se puede elegir si ajustar el reloj del sistema a UTC y pulsar enter para finalizar la instalación
- Visualizando que la instalación ha finalizado de forma correcta
- Aquí es necesario reiniciar el sistema para tener acceso a Zentyal por primera vez, pero antes de cargarse por completo se descargarán e instalarán determinados paquetes del sistema. Finalmente se tendrá acceso a Zentyal donde se inicia sesión con el usuario creado durante el proceso de instalación.

F. Administración

- El sistema ofrece la posibilidad de administrarlo vía web ingresando la sintaxis: <https://direccionIP:8443>
- Al usar esta opción se visualiza un mensaje para seleccionar el tipo de configuración
- Se pulsa el botón Configuración avanzada y se selecciona la línea Acceder a Direccion-IP
- Se ingresa el respectivo usuario y contraseña de acceso

- Al acceder por primera vez se visualizan las opciones de configuración inicial del servidor
- Se pulsa en continuar y se seleccionan los paquetes a instalar
- Después de instalados los paquetes seleccionados se continua con el proceso de configuración
- Se configura el servidor (Tipo de servidor y nombre de dominio del servidor)
- Se aplican los cambios y se inicia Zentyal con éxito.
- Desde el Dashboard se tiene la oportunidad de configurar todos los parámetros que se han instalado en Zentyal

III. Temática 1: DHCP Server, DNS Server y Controlador de Dominio

Zentyal cuenta con perfiles prediseñados, estos perfiles son conjuntos de paquetes relacionados por funcionalidad. El perfil de infraestructura como su nombre lo indica gestiona la infraestructura de la red local con los servicios básicos de: DHCP, DNS, NTP, o la Autoridad de Certificación.

Se pueden desplegar y configurar fácilmente redes corporativas de área local (LANs) usando el módulo de infraestructura de Zentyal.

Usando Zentyal es posible establecer y gestionar la configuración automática de la red (DHCP), nombres de dominio internos (DNS) y sincronización de reloj del sistema (NTP). Estos servicios son necesarios en cualquier red, ya sea sencilla o grande y compleja.

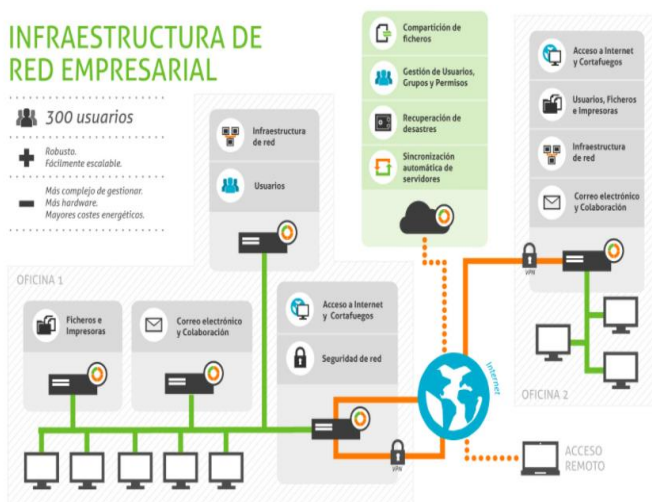


Fig.3. Infraestructura de red empresarial con Zentyal

A. DHCP Server

DHCP (Protocolo de configuración de host dinámico) es un protocolo que permite que un equipo conectado a una red pueda obtener una dirección IP de forma dinámica.

Su principal objetivo es simplificar la administración de la red mediante la distribución de direcciones IP.

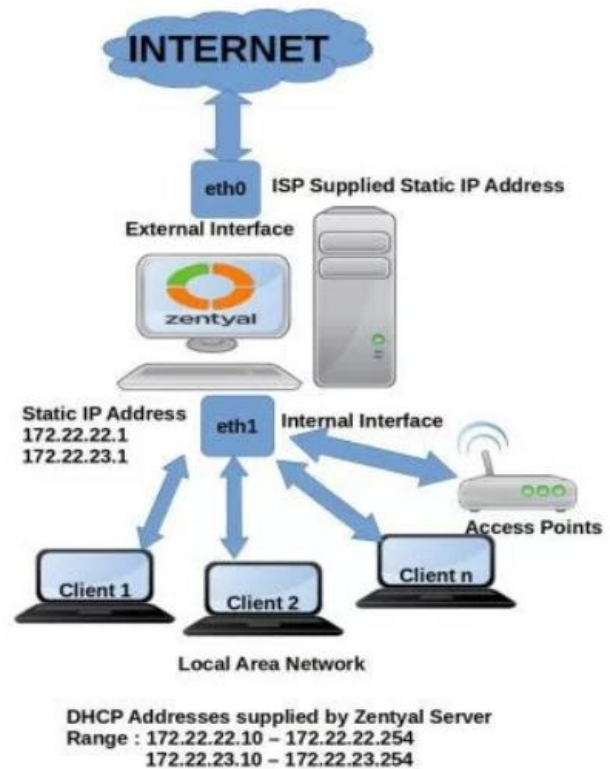


Fig.4. Protocolo de configuración de host dinámico - DHCP

B. DNS Server

DNS (Servicio de nombres de dominio) este servicio es el que traduce los nombres de dominio en direcciones IP permitiendo controlar la configuración de correo electrónico y sitio web de un nombre de dominio, es decir que los servidores DNS guían la información de manera que indican hacia qué servidor se debe encaminar una consulta para poder mostrar la información que se ha pedido, o marcan la ruta de un correo electrónico hacia su destino. Cuando un usuario visita un dominio, la configuración de DNS controla a cuál servidor se debe dirigir.

El DNS está conformado por varios elementos que controlan diferentes aspectos de un nombre de dominio.

1) Servidor de nombres

El servidor de nombres es el que direcciona un nombre de dominio a quien controla la configuración de DNS y la cual normalmente es la empresa donde se tenga registrado el nombre de dominio. Sin embargo, si el sitio web está alojado por otra empresa, algunas veces proporcionan servidores de nombres a los que tienes que apuntar

2) Archivo de zona

Son archivos que almacenan toda la configuración de DNS

de un dominio. Este archivo se almacena en el servidor de nombres de la empresa.

3) Registro

Existen varios tipos de registro:

- Registro A: Este registro se utiliza para convertir nombres de host en direcciones IP.
- Registro CNAME: Se utiliza para crear nombres de host adicionales (alias), y para crear diferentes servicios bajo una misma dirección IP.
- Registro NS: indica los servidores de DNS autorizados para el dominio, es decir, a quién hay que preguntar para saber acerca de los registros de midominio.com.
- Registro MX: Se utiliza para asociar un nombre de dominio a una lista de servidores de correo para la recepción de emails. Nos interesa si queremos realizar redirecciones de nuestro correo o utilizar nuestro correo electrónico con otro proveedor.
- Registro SPF: define qué servidores están autorizados para enviar correo electrónico con nuestro dominio.

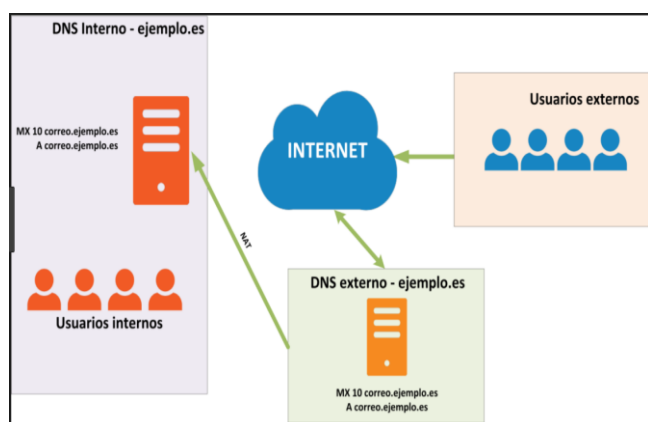


fig.5 Servicio de nombres de dominio - DNS

C. Controlador de dominio

Los controladores de dominio tienen una serie de responsabilidades y una principal es la autenticación que consiste en garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red mediante el uso de contraseña.

Mediante Kerberos que es un sistema de autenticación automática que se integra con Samba4/Active Directory y con todos los demás servicios compatibles en el dominio.

El cliente solo necesita introducir sus credenciales una vez para obtener el ticket TGT. Esta operación se realiza automáticamente en los clientes Windows unidos al dominio, las credenciales de inicio de sesión se envían al Controlador de Dominio (Cualquiera de ellos) y el usuario se verifica, el controlador envía el TGT junto con otros tickets necesarios

para la compartición de ficheros al cliente. En sistemas Ubuntu/Debian también es posible obtener el ticket TGT de Kerberos instalando el paquete heimdal-clients.

Cuando el cliente ha obtenido el ticket TGT de Kerberos ya los demás servicios del dominio compatibles con Kerberos aceptarán los tickets proporcionados por el, estos son obtenidos automáticamente cuando se solicita acceder al servicio.

Hay dos ventajas específicas en este mecanismo de autenticación:

- Seguridad: Las credenciales viajan seguras por la red local, el sistema es resistente al sniffing y a los ataques de replay.
- Comodidad: Los usuarios sólo necesitan introducir sus credenciales una vez, los demás tickets de autorización se obtienen de forma transparente.

Todos los Controladores de Dominio están integrados en el mismo contexto de Kerberos. Esto significa que un servidor Windows puede proveer el ticket TGT de Kerberos y más tarde el usuario puede usar un Proxy HTTP ofrecido por un servidor Zentyal unido al mismo dominio sin necesidad de introducir las credenciales de nuevo.

IV. Temática 2: Proxy no transparente

El Proxy No Transparente: Se refiere a que su configuración, en cada IP del servidor proxy se requiere configurar el puerto para uso en las diferentes opciones de conexión de cada browser como lo es Firefox o internet Explorer.



fig.6 Esquema de Red

A. Que es un Proxy

Es una red Informática la cual es un servicio, programa o dispositivo. El cual nos ayuda ser un intermediario entre la petición que realiza un cliente a otro Servidor.

B. Características

Encontramos dos tipos de configuración Proxy, el No Transparente y el Transparente, Los cuales se Caracterizan por:

- No transparente permite configurar IP en todos los equipos.
- Transparente, no es necesario configurar los datos del servicio Proxy. El Proxy transparente, mejora la calidad del servicio del Navegador.

C. Ventajas

- 1) Control; Se puede limitar permisos a los usuarios y dejar solo el permiso del proxy.
- 2) Velocidad: Si varios usuarios van a pedir el mismo recurso, el Proxy puede realizar un guardado de cache y así no se tiene que contactar de nuevo con el destino.
- 3) Filtrado: El proxy puede negar algunas peticiones si valida que está prohibido.

D. Diferencias

No hay gran diferencia entre un proxy Transparente y No Transparente, ya que hay momentos de configuración que suelen ser la misma maquina la única diferencia es que el Proxy transparente no se realiza configuración, por eso es llamado Transparente.

E. Configuración

Podemos evaluar si el Proxy tiene una configuración Trasparente o por el contrario hay que realizar una configuración Manual, en este caso utilizamos la configuración del Proxy Central, el cual solo acepta conexiones provenientes de interfaz de internet interna, por lo cual requiere usar una dirección interna en la configuración del Navegador.

V. Temática 3: Cortafuegos

El cortafuego Zentyal está basado en IPTables, de Netfilter. IPTables es un programa de línea de comandos usado para configurar el conjunto de reglas de filtrado de paquetes de los sistemas GNU/Linux. Este programa permite añadir, modificar y eliminar reglas de la configuración de filtrado establecida.

A. Políticas de acceso

- El tráfico desde el exterior a Zentyal o a las redes internas no está permitido.
- El tráfico desde las redes internas a Zentyal está regulado a unos servicios específicos.
- El tráfico desde las redes internas o Zentyal al exterior está totalmente permitido.

B. Elementos que definen cada una de estas reglas:

- Origen: cualquiera, una dirección IP o un objeto

(dirección MAC o conjunto de IPs).

- Destino: cualquiera, una dirección IP o un objeto (dirección MAC o conjunto de IPs).
- Servicio: protocolos y puertos a los que se aplica la regla.
- Configuración de acceso: acción que se aplica a la conexión que cumple los requisitos.

Se dispone de tres opciones de configuración de acceso, seleccionables por el administrador para ser llevadas a cabo por las reglas definidas, aplicables a una conexión: permitir, denegar o registrar. Las reglas de filtrado son evaluadas de arriba a abajo, y una vez que se acepta una conexión según una regla definida, no se evalúan más reglas. Por esto, puede que una regla genérica situada en la parte alta de la tabla de reglas anule una más específica situada en una posición más baja.

Redirección de puertos

- Interfaz: interfaz donde se recibe el tráfico.
- Origen: cualquiera, una dirección IP o un objeto (dirección MAC o conjunto de IPs).
- Destino original: Zentyal, una dirección IP o un objeto.
- Puerto de destino original: cualquiera, un puerto determinado o un rango de puertos.
- Protocolo: protocolo al que se aplica la regla.
- Descripción: comentario sobre la regla (propósito, aclaraciones).



fig.7 Uso de los cortafuegos

Temática 4: File Server y Print Server

A. Qué es

Zentyal usa Samba para implementar SMB/CIFS y gestionar el dominio, Kerberos para los servicios de autenticación. Un servidor de archivos e impresión es el término genérico para cualquier computadora que se utiliza para proporcionar almacenamiento e impresión de archivos para otras computadoras. Típicamente, una máquina en una LAN será designada como un servidor de archivos e

impresión; tendrá carpetas compartidas en toda la red para el acceso de otras computadoras, y tendrá una impresora conectada a la que otras computadoras pueden imprimir según sea necesario.

Los servidores de archivos se utilizan para almacenar datos en una ubicación central, por lo que deben mantenerse seguros para garantizar que solo aquellos que estén autorizados puedan usar los archivos. Los volúmenes en un servidor de archivos deben estar formateados con NTFS para permitir que se establezcan los permisos de archivos y carpetas y el Sistema de cifrado de archivos (EFS) se debe usar para proteger contra usuarios no autorizados y programas maliciosos. Aunque el cifrado y el descifrado pueden ser complejos, el cifrado de archivos EFS es completamente transparente para el usuario. Sin embargo, no puede encriptar los archivos del sistema y no puede compartir encriptados. Los archivos cifrados no se pueden comprimir y los archivos comprimidos se descomprimieron cuando los cifre.

1) Servidor de Impresión

Un uso habitual de Samba es configurarlo para compartir impresoras instaladas en un servidor Ubuntu, bien localmente o a través de la red. Esta sección (similar a Servidor de archivos) configurar Samba para permitir que cualquier cliente de la red local pueda usar las impresoras instaladas sin necesidad de introducir un nombre de usuario y una contraseña.

2) Modos de seguridad en Samba

Existen dos niveles de seguridad disponibles en el protocolo de red Common Internet Filesystem (CIFS): user-level (a nivel de usuario) y share-level (a nivel de recurso). La implementación que hace Samba de security mode permite más flexibilidad, ya que proporciona cuatro formas de implementar la seguridad user-level y una forma de implementar share-level:

- a. Security = user: requiere que los clientes proporcionen un nombre de usuario y una contraseña para conectarse a las acciones. Las cuentas de usuario de Samba son independientes de las cuentas de sistema, pero el paquete libpam-winbind sincronizará los usuarios del sistema y las contraseñas con la base de datos de usuarios de Samba.
- b. Security = domain: este modo permite que el servidor Samba se muestre a los clientes Windows como un controlador primario de dominio (Primary Domain Controller, PDC), un controlador secundario de dominio (Backup Domain Controller, BDC) o un servidor de miembros de dominio (Domain Member Server, DMS). Consulte *As a Domain Controller* para más información.
- c. Security = ADS: permite que el servidor Samba pueda

unirse a un dominio de Active Directory como si fuera un miembro nativo. Consulte *Active Directory Integration* para más información.

- d. Security = server: este modo se usaba antes de que Samba pudiera ser un servidor de miembros, pero ahora no debería usarse debido a ciertos problemas de seguridad. Consulte la sección sobre seguridad del servidor en la guía de Samba para más información.
- e. Security = share: permite que los clientes puedan conectarse a los recursos compartidos sin necesidad de proporcionar un nombre de usuario y una contraseña.

El modo de seguridad que vaya a elegir dependerá de su entorno y de lo que necesite que haga su servidor Samba.

B. Ventajas

- Ahorro de espacio: Ya no es necesario comprar una impresora dedicada para cada usuario, por lo tanto usted puede ahorrar el espacio, la electricidad y los costes de mantenimiento.
- Instalación rápida: Agregar una impresora a la red en cuestión de minutos. No hay necesidad de cerrar su red.
- Velocidad y Flexibilidad: Una impresora de red por lo general funciona más rápido que las impresoras láser o de inyección que no tienen la capacidad de ser conectadas a la red. Algunas impresoras multifunción pueden enviar faxes, imprimir documentos, imágenes de escaneo y copia, al momento.
- La flexibilidad, evitando colas o retrasos: Redes más de una o todas las impresoras pueden ofrecer una gran flexibilidad.

C. Desventajas

- Altos costos: La cantidad de potencia necesaria para mantener la máquina en funcionamiento es alto al igual que la cantidad de tinta.
- Mantenimiento: Puede ser un problema para las empresas que tienen una gran cantidad de impresión, fax y necesidades de copiado.
- Tiempo: Algunas personas pueden tener que esperar para usar la máquina, deteniendo su tiempo de producción.

Temática 5: VPN

VPN (Virtual Private Network) es una tecnología de red privada que nos permite conectar una o más computadoras para trabajar desde casa o desde otro lugar fuera de la empresa y accediendo a los recursos compartidos.

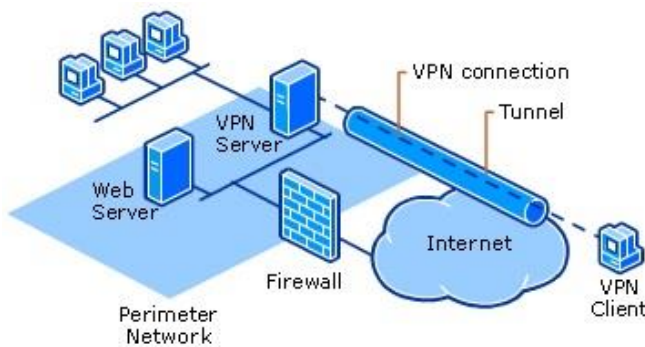


fig. 8 Configuración VPN

Es importante aclarar que no todos los empleados tienen el privilegio de acceso a la Van, son personas seleccionadas de acuerdo al cargo y responsabilidades que tienen. Por seguridad de la información, se tiene en cuenta los siguientes protocolos: Pise (Internet Protocol Security): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autenticación más exhaustivo. Pise posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (triple DES). PPTP/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo Microsoft Point to Point Encryption (MPPE). PPTP por sí solo no cifra la información.

L2TP/Pise (L2TP sobre Pise): tecnología capaz de proveer el nivel de protección de Pise sobre el protocolo de túnel L2TP. Al igual que PPTP, L2TP no cifra la información por sí mismo.

A. Ventajas

Nos permite desde cualquier lugar ingresar remotamente a los servidores de la empresa sin ninguna restricción geográfica.

Procedimiento de configuración

- Se crea la máquina virtual en Virtual Box con Ram 2048 y Disco de 150
- Asignación de Interfaz de red ETH0 y ETH1.
- Luego se descarga Central, se instala y se realizan las respectivas configuraciones como Idioma, Región, teclado, reloj, instalación de entorno gráfico, etc.
- Instalación de paquetes: Firewall, Van, Domain Controller and file sharing.
- Creación de certificado de autoridad: Es donde se expide el certificado para el servidor.
- Confirmación de módulos seleccionados o activos: Red y Van.
- Creación del servidor VPN.
- Se expide la certificación para cada cliente y luego se descarga el archivo de certificación dependiente del

sistema operativo por ejemplo: Windows, Linux o Mac.

- Descargar Open Van Clientes e instalarlo dependiendo del sistema operativo.
- Asociar el archivo de cliente Van en la conexión.
- NOTA: Si la activación de Van se realiza desde conexión doméstica se debe solicitar apertura de algunos protocolos y puertos, por ejemplo: UDP, TSP, 1194...

Conclusión

Este Diplomado en Linux, ayudó a afianzar mucho más los conocimientos, con respecto a las tareas de Linux y manejando la consola para ejecutar las diferentes instalaciones requeridas.

Este aporte nos ha llevado a una disciplina que involucra personas, procesos y tecnología de información, por lo cual nos ayuda a mejorar cualquier proceso ya que estamos enfocados únicamente en la escuela de Ingeniería y su desarrollo como tal, nos dio conocimiento manejar las diferentes instalaciones en Linux.

Agradecimientos

Hemos conseguido llegar hasta acá, un objetivo más en nuestras vidas y en nuestra carrera, agradecemos a la universidad nacional. Abierta y a distancia UNAD, a nuestras familias por su apoyo y comprensión a nuestros amigos, tutores, directores y a nosotras mismas como grupo de trabajo, a todo el grupo gracias por brindar sus conocimientos durante todo el proceso de formación, por su sincero anhelo de llegar hoy acá, por la dedicación y compromiso, lo hemos logrado.

Referencias

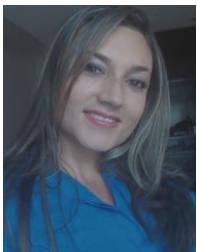
- [1] www.solvetic.com/tutoriales/articulo/4381-como-instalar-servidor-zentval-5-0-linux/
- [2] <http://www.ordenadores-y-portatiles.com/proxy-transparente.html>
- [3] https://wiki.zentval.org/wiki/Espanol/5.0/Servicio_de_Proxy_HTTP
- [4] <http://www.raulprietofernandez.net/blog/gnu-linux/como-configurar-proxy-squid-en-modo-no-transparente>
- [5] <http://www.chw.net/foro/gnu-linux-y-otros-sistemas-operativos/45849-configurar-servidor-proxy-squid-y-no-morir-el-intento.html>
- [6] <http://www.zentval.org>
- [7] <https://certificacionsanchez.wordpress.com/ventajas-y-desventajas-de-print-server/>
- [8] <https://www.youtube.com/watch?v=2MjtTU0rMIM>
- [9] <https://www.youtube.com/watch?v=2MjtTU0rMIM>
- [10] <https://www.youtube.com/watch?v=yvbd9aHEjWg>
- [11] <https://www.youtube.com/watch?v=AviThwz4eBQ>
- [12] <https://www.youtube.com/watch?v=2MjtTU0rMIM>
- [13] http://cuchillac.net/archivos/pre_pymes/infra03/guias/g10_VPN.pdf
- [14] http://www.zentval.com/wp-content/uploads/2014/06/Zentval_for_SMBs_Product_Description_ES.pdf
- [15] [https://wiki.zentval.org/wiki/Espanol/3.5/Servicio_de_resolucion_de_nombres_de_dominio_\(DNS\)](https://wiki.zentval.org/wiki/Espanol/3.5/Servicio_de_resolucion_de_nombres_de_dominio_(DNS))
- [16] <https://co.godaddy.com/help/que-es-el-dns-665>
- [17] <https://wiki.zentval.org/wiki/Espanol/3.5/Instalacion>
- [18] <https://www.hostinet.com/formacion/general/que-son-dns-tipos-registros/>



María Lucia Rueda Nieto, lugar de nacimiento Bogotá, Colombia. Es estudiante de ingeniería de sistemas de la Universidad Nacional Abierta y a Distancia UNAD. Su principal campo de estudio es la informática específicamente todo lo relacionado con diferentes lenguajes de programación. Ella se desempeña laboralmente como Services Manager de las Torres de desarrollo Java, Net y SQL en Softtek Colombia desde hace tres años, anteriormente trabajo en fábricas de software como Intergrupo e Imectech durante 6 años. Su especialización es el desarrollo en la plataforma Visual Studio .Net, actualmente realiza un diplomado de profundización en Linux.



Myriam Judith González Deantonio, nacida en la ciudad de Bogotá, Estudiante de Ingeniería de Sistemas de la Universidad Nacional Abierta y a Distancia UNAD, su principal campo de estudio es el relacionado con toda la parte funcional quien representa los requerimientos del cliente y del usuario final, reuniendo las entradas de los interesados para entender el problema que será solucionado, capturando y configurando prioridades para los requerimientos. Y dirección de proyectos



Carmen Beatriz Ramírez Giraldo, nacida en El Santuario Antioquia, vive actualmente en Bogotá. Realizó sus estudios secundarios en el Liceo Pbro Luis Rodolfo Gómez Ramírez. Estudios superiores: Confección industrial en el SENA, Procesadora de datos contables en el Sena, Digitadora Recepcionista en el SENA, 3 semestres de Psicología en la Universidad Cooperativa de Colombia. Actualmente cursa 10 semestre de ingeniería de sistemas en la UNAD, su enfoque es la programación en java, y como proyecto de grado realiza un Diplomado de profundización en Linux.



Luz Mary Useche, Nací en Florencia Caquetá, el 26 de marzo de 1.980, vengo de una familia humilde y trabajadora con unos padres emprendedores. Soy casada hace 19 años, tengo dos hijos John Styven de 17 y Angie de 10 años, mi mayor anhelo y sueño ha sido finalizar la carrera como Ingeniera de Sistemas. Sueño que será realidad, gracias a la oportunidad que ofrece la Universidad Nacional Abierta y a Distancia UNAD a todas las personas que trabajamos y que se nos dificultad asistir de manera presencial a un aula de clases. Actualmente me encuentro realizando como opción de grado un Seminario de Linux, el cual me ha permitido adquirir conocimiento de nuevas herramientas, habilidades y destrezas. Laboro en la empresa Softmat Services como Analista de Sistemas Nivel I y II.



Rossana Rodríguez Reyes, Nací en la ciudad de Sogamoso, Estudiante de Ingeniería de Sistemas de la universidad Nacional Abierta y a Distancia UNAD. Su principal campo de estudio es manejar software establecidos por los diferentes clientes según establecidos. Ella se desempeña como Auxiliar de información en la empresa Tap Solutions, el cual lleva desarrollando esta actividad 1 año, El cual desarrolla manejando información que envía los Clientes y por medio de Software entregará la respuesta establecida por cada Client. Actualmente realiza un Diplomado de profundización en Linux.