Interconexión de redes privadas con redes públicas.

Caso práctico

-¡Buenos días, Alicia!

Zorrillo-Estepa. (CC BY-SA)

-¡Buenos días, Juan! me envía mi empresa, por lo visto habéis comprado ordenadores nuevos.

-Sí. Los que tenemos son muy antiguos.

-En eso estoy de acuerdo –dijo Alicia.

-Así que por eso te hemos llamado, para que nos configures los nuevos ordenadores –dijo Juan.

-¿Has comprado alguno más potente, para funcionar como servidor? –preguntó Alicia.

-Sí –contestó Juan-. He comprado un servidor con Procesador Intel 2x6x2, 26 GHz con 16 GB ECC RAM, 3 Discos x 600 GB SAS 3.600 GB o 18 Mbps de Transferencia y RAID 5.

Stockbyte. (Uso educativo nc)

-Pues eso no lo había pensado yo –dijo Juan.-¡Vaya! –exclamó Alicia-, pues con esa pedazo de máquina deberíamos plantearnos mejorar la estructura de la red y la forma de conectarnos a Internet.

-Se me ocurre instalar en el servidor todos los programas de seguridad y centralizar las conexiones para hacer más eficiente el ancho de banda –explicó Alicia-. Si todos los empleados y empleadas salieran a Internet por el servidor, ganaríamos en seguridad y en rapidez.

-Ya sabes que confío en ti –dijo Juan.

-De acuerdo –respondió Alicia-, me pongo a trabajar.

Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

Aviso Legal

1.- Introducción.

Caso práctico

Estamos viviendo una época de grandes cambios en nuestra sociedad, todo ello gracias a que Internet se ha convertido en el medio más importante a la hora de distribuir información. Todas las empresas quieren estar en este medio, pero la información de las mismas requiere tratamientos distintos.

Stockbyte. (Uso educativo nc)

Alicia empezó a pensar sobre el trabajo ese mismo día…

"Tengo que distinguir entre la información expuesta en la Web y la confidencial que está reservada a clientela y empleados y empleadas del periódico. Esta última requiere más medidas de seguridad."

"Tengo que filtrar las conexiones para que las empleadas y empleados, no entren a páginas que no estén relacionadas con su trabajo -pensó Alicia-. Así se evitaran virus, pérdidas de tiempo, etc."

"También tendré que evitar que desde fuera accedan a la información confidencial del periódico".

"La línea ADSL que tiene contratada el periódico va bien. Pero igual conviene cambiarla a fibra óptica".

"Bueno, iré paso a paso –decidió Alicia-. Que todo a la vez no lo puedo decidir".

A la hora de pasar de una red privada a otra pública, tienes que conocer muy bien las tecnologías de acceso conmutado y de acceso dedicado. La elección de una u otra dependerá de ti si en un futuro trabajas como técnica o técnico, serás el encargado de contratar los servicios de datos, voz sobre IP (VoIP), videoconferencia, etc. Por ejemplo, el ancho de banda dependerá de los servicios que necesites utilizar. De cualquier forma siempre te serán necesarios aparatos de interconexión, sobre todo enrutadores, que dirigen y adaptan el tráfico entre diferentes redes. También necesitaras establecer unas medidas de seguridad como un **cortafuegos** y un **servidor proxy-caché** con los que controlar los accesos internos de los empleados en la zona exterior a la intranet. También tendrás que controlar los accesos de los visitantes o posibles atacantes.

Las tecnologías se consideran de **banda ancha**, cuando los enlaces de su ancho de banda de conexión son superiores a los 2 Mbps (Megabits por segundo). Por el contrario, cuando la velocidad es inferior se denominan de **banda estrecha**.

Autoevaluación

Rellena los huecos con los conceptos adecuados.

A la hora de pasar de una red privada a otra pública, se necesitan establecer unas medidas de seguridad como un _____ y un servidor _____ .

Enviar

Con el cortafuegos y el servidor Proxy-caché se controlan los accesos a la red.

2.- Tecnologías de acceso a Internet.

Caso práctico

Alicia sigue trabajando en el asunto que se trae entre manos y se encuentra con Pedro y Manuel, dos redactores del periódico.

Stockbyte. (Uso educativo nc)

-¡Buenas tardes! ¿Qué tal os va? –saludó Alicia.

-¡Muy bien! ¿Y tú? ¿Cómo vas con la configuración de los nuevos equipos? –preguntó Pedro.

-Pues muy liada, ya que ahora tenemos que replantearnos la forma de comunicarnos a Internet, -contestó Alicia.

-¿No va bien la línea ADSL? –pregunto Manuel.

-Sí, va bien. Pero hoy en día podemos encontrar otras opciones mejores –contesto Alicia.

- Pues entonces tienes mucho trabajo –dijo Manuel.

-Así es –contestó Alicia-. Ahora lo primero que tengo que hacer es seleccionar el mejor tipo de acceso a Internet.

- Pues con todos los tipos de acceso que existen en la actualidad y todos los proveedores que hay ¡Ya tienes trabajo! ¡Ya! –exclamó Pedro.

Las **líneas de acceso conmutado (LAC)**, empleadas a finales del siglo XX, necesitan establecer una llamada entre ambos extremos para realizar la comunicación. Esto es, deben conmutar o conectar las líneas a su paso por cada central, desde el origen al destino, tal como sucede cuando se llama por teléfono.

Las tecnologías **LAC** son las siguientes:

- Red Telefónica Conmutada o Red Telefónica Básica (**RTC/RTB**).
- Red Digital de Servicios Integrados **(RDSI**).
- Sistemas de telefonía **móvil analógicos**.
- Sistema Global de Comunicaciones Móviles (**GSM**).
- Servicio General de **Paquetes por Radio** Mejorado.

Las **líneas de acceso dedicado (LAD)**, mucho más actuales que las anteriores, son exclusivas de los clientes que las han contratado, estos las utilizan a tiempo completo. Siempre están activas y poseen un ancho de banda mayor.

Las tecnologías que funcionan como LAD son las siguientes:

- La familia de tecnologías de abonado digital (**xDSL**, siglas en ingles de Digital Subscriber Line).
- Redes **mixtas** de TV e Internet por cable (**CATV**).
- Conexión por **cable eléctrico**.
- Redes de fibra hasta el **hogar**.
- Vía satélite (**VSAT**).
- Servicio de distribución **multipunto**.
- Redes metropolitanas **inalámbricas**.
- Servicio de telefonía **móvil universal**.
- Servicio de telefonía **móvil universal avanzado**.
- Sistema de telefonía **móvil sobre IP.**

Para saber más

El siguiente enlace es un sitio oficial en Internet del Ministerio de Industria, donde puedes consultar tus derechos como consumidor de las compañías de telecomunicaciones. Desde este sitio puedes gestionar reclamaciones y denuncias sobre cualquier operador:

Oficina de atención al usuario de telecomunicaciones.

2.1.- Red telefónica/Red digital.

Para empezar, te propongo un poco de historia…

Stockbyte. (Uso educativo nc)

La primera tecnología que surgió fue la red de telefonía conmutada o básica **(RTC/RTB**). Se trata de una red de banda estrecha que funciona de manera analógica sobre un par trenzado de cobre, del cual solo utiliza **dos hilos**: uno para **transmisión** y otro para **recepción**. Durante mucho tiempo se ha utilizado para enviar mensajes de voz, y a finales del siglo XX se adaptaron para el envío de datos desde los ordenadores. Como los ordenadores trabajan con señales digitales, hubo que convertir las señales digitales en analógicas mediante el **módem.**

El módem es un modulador/demodulador de señales. Este dispositivo convierte la señal digital del ordenador en analógica hacia la RTC (modulación) y también realiza la operación inversa (demodulación), al pasar la señal analógica de la RTC a digital para enviarla al ordenador.

Estas tecnologías funcionan con cables de par trenzado de **4 hilos** con clavijas **RJ11**.

La red digital de servicios integrados (**RDSI**), de la misma forma que la anterior, funciona sobre un par trenzado de cobre, aunque de manera digital. Integra los servicios disponibles en el momento de su aparición que eran voz y datos, con señales digitales.

Existen dos tipos de RDSI:

- **De banda ancha**: Puede dar servicios avanzados de TV y videoconferencias. Se utiliza con velocidades superiores a 2 Mbps.
- **De banda estrecha:** Empleado en conexiones conmutadas de 64 Kbps, aunque se prevé que se aumente hasta los 2 Mbps. En este caso, se recurre a dos interfaces de abonado: **Acceso básico y Acceso primario.**

A diferencia de la tecnología RTC/RTB, la RDSI utiliza cables de par trenzado de **8 hilos** con clavijas **RJ45.**

Para saber más

La Comisión del Mercado de las Telecomunicaciones, es un Organismo Público regulador independiente de los mercados nacionales de comunicaciones electrónicas y de servicios audiovisuales, integrado desde 2013 en la Comisión Nacional de los Mercados y la Competencia (CNMC).

Autoevaluación

De entre los siguientes nombres, marca todas las interfaces que forman parte del acceso en banda estrecha de las RDSI:

- [ ] Acceso reducido.
- [ ] Acceso secundario.
- [ ] Acceso básico.
- [ ] Acceso primario.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Incorrecto
3. Correcto
4. Correcto

2.2.- Tecnologías de líneas de abonado digital (xDLS).

Ahora vas a ver una de las tecnologías más populares de acceso a internet, conocido por las siglas **xDSL** (siglas en inglés de Digital Subscriber Line, significa líneas de abonado digital), engloba la conocida **ADSL** (siglas en inglés de Asymmetric Digital Subscriber Line, significa línea de abonado digital asimétrica), así como otras más especializadas. Estas tecnologías utilizan el bucle de abonado actual de par trenzado de cobre de las tecnologías RTC o RDSI, sobre las que trabajan para convertirlo en una línea digital de alta velocidad de banda ancha, aprovechando la parte que no utilizan debido a que el canal de voz tan solo usa una mínima parte.

Stockbyte. (Uso educativo nc)

El bucle local o de abonado es el último tramo o la última milla de conexión entre el nodo cliente y la central de comunicaciones de la que depende. Suele ser el tramo de cable más caro y más importante. Se regula como dispone la ley de la Oferta de Bucle de Abonado (**OBA**).

Este grupo de tecnologías pueden ser:

- **Simétricas:** se usan para empresas que tienen mucho tráfico de subida a Internet.
- **Asimétricas:** para clientes finales que descargan mucho más que lo que suben a Internet.

Tienes que tener en cuenta que la calidad de la transmisión con cable de cobre empeora con la distancia, por lo tanto, la distancia a la central telefónica influye en la calidad de las mismas.

Existen 4 tipos de tecnologías xDSL:

- **VDSL**, acrónimo de siglas de Very high bit-rate Digital Subscriber Line (DSL de muy alta tasa de transferencia).
- **HDSL**, acrónimo de High bit rate Digital Subscriber Line (Línea de abonado digital de **alta velocidad** binaria.) El módem habilita el establecimiento telefónico de un circuito digital unidireccional.
- **ADSL**, acrónimo de Asymmetric Digital Subscriber Line (“Línea de Abonado Digital **Asimétrica**”).
- **SDSL**, acrónimo de Symmetric Digital Subscriber Line. (“Línea de Abonado Digital **simétrica**”).

La más adecuada para el uso domestico de acceso a Internet es la ADSL. Una vez comprobada su viabilidad, ha tenido un gran éxito. Al cabo de poco tiempo se creó una segunda versión, denominada ADSL2, que no llegó a comercializarse a causa de la inmediata puesta en marcha de la actual ADSL2+.

2.3.- Conexión de Cable eléctrico y Redes de Fibra.

Stockbyte. (Uso educativo nc)

Ahora vas a ver una tecnología de la que se habló mucho en su día, pero que no ha llegado a cuajar. **Power Line Communications**, también conocido por sus siglas **PLC**, es un término inglés que puede traducirse por **comunicaciones mediante cable eléctrico** y que se refiere a diferentes tecnologías que utilizan las líneas de energía eléctrica convencionales para transmitir señales de radio para propósitos de comunicación. La tecnología PLC aprovecha la red eléctrica para convertirla en una línea digital de alta velocidad de transmisión de datos, permitiendo, entre otras cosas, el acceso a Internet mediante banda ancha. Aunque experimentó un cierto auge en los primeros años del siglo XXI, el coste que supone la inversión en infraestructura para las empresas eléctricas y su lenta implantación la han dejado en un segundo plano. Sin embargo, hay ocasiones en que resulta práctica, por ejemplo para extender la red de internet dentro de un domicilio en el que las redes wifi no tienen suficiente alcance o hay demasiadas interferencias radioeléctricas.

La Banda ancha sobre líneas eléctricas (abreviada **BPL** por su denominación en inglés **Broadband over Power Lines**) representa el uso de tecnologías PLC que proporcionan acceso de banda ancha a Internet a través de líneas de energía ordinarias. En este caso, una computadora (o cualquier otro dispositivo) necesitaría solo conectarse a un módem BPL enchufado en cualquier toma de energía en una edificación equipada para tener acceso de alta velocidad a Internet. Esta tecnología no ha llegado a implantarse.

La tecnología de telecomunicaciones **FTTH (del inglés Fiber To The Home)**, también conocida como fibra hasta el hogar, enmarcada dentro de las tecnologías FTTx (donde x indica el alcance conseguido del tendido) se basa en la utilización de cables de fibra óptica y sistemas de distribución ópticos adaptados a esta tecnología para la distribución de servicios avanzados a los hogares y negocios de los abonados, como el Triple Play:

- Telefonía.
- Internet de banda ancha.
- Televisión.

La implantación de esta tecnología ya está muy avanzada en todo el mundo, y en España es la principal forma de acceso a internet, con una cobertura superior al 90% del territorio.

Autoevaluación

La tecnología xDSL puede ser:

- ○ Simétrica.
- ○ Asimétrica.
- ○ Simétrica y Asimétrica.
- ○ Simétrica y ADSL.

Incorrecto. Te falta otro más.

No es correcto. Te tienes que volver a leer el punto anterior.

Estás en lo cierto.

No es cierto. Pero casi lo consigues.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.4.- CATV y VSAT.

Te toca seguir con las tecnologías CATV y VSAT.

Christian Frausto Bernal. (CC BY-SA)

CATV (siglas en inglés de Community Antenna Television, significa Televisión por Cable), es un sistema de servicios de televisión prestado a los consumidores a través de señales de radiofrecuencia que se transmiten a los televisores fijos a través de **fibras ópticas** o **cables coaxiales**.

Este servicio te ofrece transferencia de imágenes de televisión hasta tu domicilio si estás abonado. Existen redes de televisión por cable desde los años 40. La primera red de cable fue montada en EEUU y han evolucionado mucho desde entonces.

VSAT (siglas de **Terminal de Apertura Muy Pequeña**, del inglés, Very Small Aperture Terminal). Designa un tipo de antena para comunicación de datos vía satélite y por extensión a las redes que se sirven de ellas, normalmente para intercambio de información punto-punto, punto-multipunto (broadcasting) o interactiva.

Los satélites usados para la transmisión pueden clasificarse en dos grupos:

- **Satélites banda-C**: más antiguos, utilizan frecuencias de 3,7 a 4,2 GHz y de 5,9 a 6,4 GHz que requieren de antenas parabólicas grandes.
- **Satélites banda-K**: más modernos, utilizan frecuencias de 11 a 12 GHz, habituales en el acceso doméstico y requieren antenas parabólicas pequeñas.

Esta tecnología puede usarse en caso de que no sea posible aprovechar las otras a causa de la distancia entre las viviendas y las centrales o las antenas. También se usa para embarcaciones.

Existen dos tipos de módem para la conexión por satélite en función de la conexión a Internet contratada:

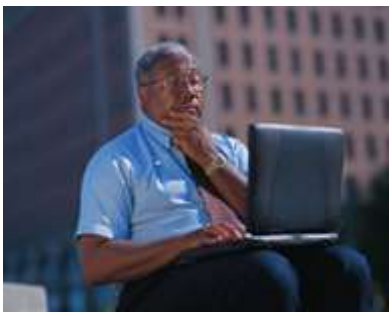
- Los **módem unidireccionales**: solo pueden recibir datos, si se requiere enviar y recibir datos desde internet tendrás que disponer de una conexión terrestre.
- Los **módem bidireccionales**: reciben y envían datos. Resultan más caros.

La tecnología digital de banda ancha se basa en el uso de satélites artificiales geoestacionarios. Estos describen órbitas sobre el ecuador terrestre con la misma velocidad angular que la Tierra, es decir, permanecen inmóviles sobre un determinado punto sobre nuestro globo. Un solo satélite geoestacionario de gran altitud puede proporcionar comunicaciones confiables aproximadamente a un 40% de la superficie terrestre.

Mediante una antena parabólica, se realiza una conexión directa desde el ordenador o red del usuario al satélite que proporciona el acceso.

2.5.- Servicios distribución multipunto y Redes inalámbricas de área metropolitana.

¿Y cómo te conectas a Internet en los lugares donde no llegan los cables? Aquí tienes dos respuestas.



Stockbyte. (Uso educativo nc)

El **Servicio de Distribución Multipunto Multicanal** o **MMDS** (del inglés Multichannel Multipoint Distribution Service) es un término que identifica a una tecnología inalámbrica de telecomunicaciones, usada para el establecimiento de una red de banda ancha de uso general o, más comúnmente, como método alternativo de recepción de programación de televisión por cable.

Se utiliza generalmente en áreas rurales poco pobladas, en donde instalar redes de cable no es económicamente viable. Un ejemplo es el del sistema **TRAC** que se utilizó en España para el acceso telefónico en zonas rurales.

Para saber más

Aquí tienes un enlace a la Wikipedia para conocer mejor el sistema TRAC:

TRAC.

Las redes inalámbricas de área metropolitana (**WMAN**) también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop). Las WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es **WiMAX** (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros. Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el IEEE 802.16. Una de sus ventajas es dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados (zonas rurales).

Esta tecnología sigue siendo usada en la actualidad en núcleos rurales, aunque algunas empresas han descontinuado su despliegue.

Autoevaluación

Cuál de las siguientes tecnologías es la mejor como red inalámbrica de área metropolitana:

- ○ WMAN.
- ○ MMDS.
- ○ WIMAX.
- ○ VSAR.

No es correcto. Pero vas encaminado.

No es cierto. No tiene nada que ver.

Efectivamente, veo que lees con atención.

Incorrecto. Estas muy lejos de la respuesta correcta.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.6.- Sistemas de telefonía móvil.

Seguramente tienes teléfono móvil y navegas con él por Internet. Vas a ver cómo ha ido evolucionando esta tecnología hasta nuestros días.

Stockbyte. (Uso educativo nc)

La telefonía móvil usa ondas de radio para poder ejecutar las operaciones desde el móvil a la base, ya sea llamar, mandar un mensaje de texto, etc., y esto es producto de lo que sucedió hace algunas décadas. La comunicación inalámbrica tiene sus raíces en la invención de la radio por **Nikola** Tesla en los años 1880, aunque formalmente presentado en 1894 por un joven italiano llamado Guglielmo Marconi. La tecnología móvil no es una tecnología en sí misma, sino el resultado de la evolución de sistemas en la que pueden distinguirse cuatro generaciones. Desde la primera, de funcionamiento analógico hasta la cuarta.

- **La primer generación 1G:** Esta generación hizo su aparición en 1979, se caracterizó por ser **analógica** y estrictamente para voz.
- **La segunda generación 2G: A** diferencia de la primera se caracterizó por ser **digital**. El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía móvil usados en la actualidad. Las tecnologías predominantes son: GSM (Global System for Mobile Communications). Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas para voz pero limitados en comunicaciones de datos.

La generación 2.5G: Muchos de los proveedores de servicios de telecomunicaciones, se cambiarán a las redes 2.5G antes de entrar masivamente a 3G. La tecnología 2.5G es más rápida y más económica para actualizar a 3G.

- **La tercer generación 3G:** Esta tecnología surgió en 1998 con el propósito de crear un estándar de telefonía móvil para el mundo. El proyecto auspiciado por la Unión Europea, ha contado con el respaldo de la Unión Internacional de Telecomunicaciones que le ha asignado la banda de frecuencia de 2 GHz. Entre las tecnologías contendientes de la tercera generación se encuentran **UMTS** (Universal Mobile Telephone Service).
- **La cuarta generación 4G:** La cuarta generación es un proyecto que está despegando actualmente. Está basada en la tecnología LTE (Long Term Evolution), que permitirán velocidades de más de **100 megas.**
- **La quinta generación 5G:** en pleno desarrollo en la actualidad. Ya se han implementado algunas redes comerciales, pero su expansión está empezando a hacerse realidad en estos momentos. Pronto permitirá navegar en dispositivos móviles a una velocidad de hasta 1,2 Gbps.

Autoevaluación

Rellena los huecos con los conceptos adecuados.

CATV, es un sistema de servicios de televisión, prestado a los consumidores a través de señales de radiofrecuencia que se transmiten a los televisores

fijos a través de _____ o _____ .

Enviar

Las fibra óptica o cable coaxial sirven para transmitir CATV.

3.- Redes Privadas Virtuales.

Caso práctico

Alicia se entrevista con Juan para contarle las decisiones que ha ido tomando.

Stockbyte. (Uso educativo nc)

-Buenas tardes Juan – dijo Alicia.

-Buenas tardes Alicia. ¿Qué tal va todo?

-He estado valorando las diferentes opciones para la nueva conexión a Internet. Creo que la mejor es conectarnos con un proveedor de fibra óptica.

-¿No será muy caro? –pregunto Juan.

-Pues he estado consultando ofertas y creo que al final te resultara hasta más barato –dijo Alicia.

-De acuerdo entonces –respondió Juan.

-Ahora lo que me preocupa es el tema de la seguridad y estoy pensando en configurar redes privadas virtuales –dijo Alicia.

-¿En qué consiste eso? –Preguntó Juan.

-Si te parece nos vemos mañana sobre esta hora y te resuelvo todas las dudas que tienes –respondió Alicia.

-¡Muy bien, hasta mañana entonces! –Exclamó Juan.

Como ya sabes, la estructura básica de cualquier empresa, son las redes de área local (LAN), ante la necesidad de comunicar puntos remotos, y lo costoso que significaría tener una WAN (Wide Area Network, significa rede de área amplía) ya que se tendrían que tirar líneas entre cada sucursal de una empresa "X", se pensó en la forma de utilizar **redes públicas** para comunicar estas sucursales.

Esto se consigue mediante el uso de **Redes Privadas Virtuales**. Para poder habilitar redes privadas, que comuniquen de forma segura cada uno de los nodos de una red pública hay una necesidad de aplicar algún sistema de seguridad, debido a que los datos de la empresa son valiosos, y no deben ser interceptados.

Con una Red Privada Virtual (VPN, del inglés Virtual Private Network), los usuarios remotos, que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de redes públicas.

Una VPN normalmente usa la red Internet como transporte para establecer enlaces seguros, extendiendo las comunicaciones a oficinas aisladas. Significativamente, decrece el

coste de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.

Una Red Privada Virtual transporta datos de manera segura por Internet. A través de un **túnel** establecido entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte. Una VPN te permite el acceso remoto a servicios de red de forma transparente y segura, con el grado de conveniencia y seguridad que los usuarios conectados elijan. Las VPN están implementadas con cortafuegos y routers para lograr esa encriptación y autentificación.

Autoevaluación

Rellena los huecos con los conceptos adecuados.

Para conectar las diferentes redes locales remotas de una empresa, y a bajo coste se usa: [ ]

Enviar

VPN es la respuesta correcta.

3.1.- Protocolos de túnel.

Natharael (CC BY-NC-ND)

Para terminar con este punto, te vamos hablar de los protocolos de **túnel**, que son en los que se basan las redes privadas virtuales. Estos protocolos cifran los datos que se transmiten desde un lado de la VPN hacia otro.

El protocolo de túnel es el encargado de g**arantizar que los datos estén cifrados** desde el momento que entran en la VPN hasta que salen de ella y, por lo tanto, no son comprensibles para cualquiera que no se encuentre en uno de los extremos. En una VPN hay un equipo que cifra y descifra los datos del lado del usuario y otro del lado del servidor VPN que es el elemento que descifra los datos del lado de la organización.

Así, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al equipo que realiza el cifrado que se conecta con la red remota mediante una red pública como es Internet, para transmitir la información cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y los envía al usuario que ha realizado la petición.

La mayoría de los routers tienen la posibilidad de actuar como clientes/servidores de VPN.

Los principales protocolos de túnel son:

- **PPTP** (del inglés Point to Point Tunneling Protocol, traducido es Protocolo de Túnel Punto a Punto) es un protocolo de capa 2 desarrollado por el conjunto de empresas: Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.
- **L2F** (del inglés Layer Two Forwarding, traducido es Reenvío de **Capa dos**) se creó en las primeras etapas del desarrollo de las redes privadas virtuales. Como PPTP, L2F fue diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas.
- **L2TP** (del inglés Layer Two Tunneling Protocol, traducido es Protocolo de Túnel de **Capa dos**) es un protocolo que incluye las características de PPTP y L2F. Surge como resultado del trabajo del IETF (RFC 2661).
- **IPSec** (del inglés Internet Protocol security, traducido Protocolo Seguro de Internet). Es un protocolo definido por IETF que se usa para transferir datos de manera segura en la capa de red (**capa tres)**.

4.- Servicio de Cortafuegos.

Caso práctico

Alicia ha sacado algunas conclusiones sobre el trabajo a realizar. Como, por ejemplo el tipo de conexión a Internet que quiere utilizar. El uso de VPN, es algo que tiene que sopesar en función de los datos que viajan por Internet relativos al periódico.

Stockbyte. (Uso educativo nc)

Ahora va a seleccionar un cortafuegos, tiene que decidir cuál es el mejor sitio para ponerlo. No quiere ponerlo en cada equipo, sino centralizarlo en el servidor. Así el resto de los equipos irán a más velocidad.

"Tengo que buscar un cortafuegos –pensó Alicia- no sé de qué tipo ponerlo, y tengo que decidir dónde ponerlo".

"Esto no me evitara los problemas de virus, pero me protegerá de los ataques externos y me dará protección adicional contra los troyanos y los gusano del correo electrónico".

"Creo que la mejor opción será un cortafuegos de Software y, por supuesto, acompañado de un buen antivirus."

Seguro que te suena esto del cortafuegos, después de leer este punto vas a resolver las dudas que tengas sobre esta herramienta. Si es que tienes alguna duda.

Un **cortafuegos o firewall** es un sistema que previene el uso y el acceso desautorizado a tu ordenador. Los cortafuegos pueden ser software, hardware, o una **combinación** de ambos. Se utilizan con frecuencia para evitar que los usuarios desautorizados de Internet tengan acceso a las redes privadas conectadas con Internet, especialmente **intranets**. Todos los mensajes que entran o salen de la Intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados.

Es importante recordar que **un cortafuegos no elimina problemas de virus del ordenador**, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, añadirá cierta seguridad y protección adicional para tu ordenador o red.

Los cortafuegos de hardware proporcionan una fuerte protección contra la mayoría de las formas de ataque que vienen del mundo exterior y se pueden comprar como producto independiente o en routers de banda ancha. Desafortunadamente, luchando contra virus, gusanos y troyanos, un cortafuegos de hardware puede ser menos eficaz que un cortafuegos de software, pues podría no detectar gusanos en correos electrónicos.

Para usuarios particulares, el más utilizado es un **cortafuegos de software**. Un buen cortafuegos de software protegerá tu ordenador contra los intentos de controlar o acceder a tu ordenador desde el exterior, y generalmente proporciona protección adicional contra los troyanos o gusanos de E-mail más comunes. La **desventaja** de los cortafuegos de software es que protegen solamente al ordenador en el que están instalados y **no protegen una red.**

La política general de diseño del tráfico que se permite pasar suele ser restrictiva: **no deja pasar ningún tipo de tráfico, salvo el que esté explícitamente permitido**.

Autoevaluación

Rellena los huecos con los conceptos adecuados.

Un cortafuegos no elimina problemas de _____ del ordenador, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software _____ , añadirá cierta seguridad y protección adicional para tu ordenador o red.

Enviar

Los cortafuegos no detectan virus, por lo tanto necesitas un programa antivirus.

4.1.- Tipos de Cortafuegos.

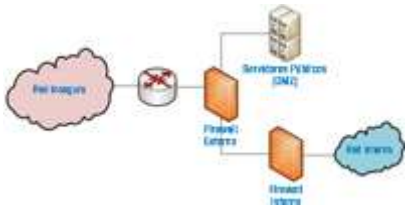
Tengo que decirte que aunque no hay una tipología oficial, normalmente se habla de 4 tipos de cortafuegos:

- Los **filtros de paquetes**, que suelen ser (aunque no siempre) encaminadores, que filtran el tráfico basándose en combinaciones de diferentes campos de las cabecera de cada mensaje.
- **Gateways de aplicaciones**, también llamados **servidores proxy**, que suelen ser equipos intermedios, que aceptan peticiones entrantes de servicios de red, y realizan las llamadas adecuadas, a favor de cada cliente del servicio correspondiente.
- Cortafuegos de tipo **stateful inspection, o de filtrado dinámico de paquetes**, que son capaces de mantener el estado de cada sesión a través del cortafuegos y cambiar las reglas de filtrado dinámicamente, conforme a lo definido en la política de seguridad.
- Cortafuegos **híbridos,** que suelen tener unas propiedades que son el resultado de combinar las propiedades de los citados previamente.

La técnica de **filtrado de paquetes** permite examinar las direcciones IP así como los puertos de E/S de origen y destino de cada paquete. Después, mediante un conjunto de reglas, los acepta o rechaza. Las reglas se utilizan para cerrar el tráfico de paqutes hacia determinados puertos y deja abiertos, única y exclusivamente, los que necesitan los servicios activados. Por ejemplo, si se desea que nadie descargue nada de la red interna mediante el protocolo FTP, se cerrará el puerto 20.

> Zona desmilitarizada (**DMZ**). Es una zona o red especial donde se sitúan los servidores públicos de las empresas. El objetivo es crear una red menos restrictiva entre la intranet e Internet para ofrecer servicios al exterior de la empresa.

No obstante, existen paquetes IP, que parecen correctos, cuya cabecera no contiene errores, pero contienen código malicioso, diseñado para aprovechar fallos de seguridad en los servicios, como ocurre con los virus informáticos. La construcción de cortafuegos seguros depende de la experiencia acumulada, esto requiere un buen dominio de las tecnologías utilizadas. Se pueden plantear diferentes tipos de construcciones:



Alicia Galán Gutiérrez. (Uso educativo nc)

- **Red perimetral**: es el modelo más seguro, costoso y completo. Requiere de una gran experiencia para configurarla, ya que puedes intercalar tantos cortafuegos en cascada como la empresa requiera. Dispone al menos de dos equipos que encierran la DMZ.
- **DMZ expuesta**: no dedica recursos a proteger los servidores públicos, solo se centra en la seguridad de la intranet.
- **DMZ protegida o cortafuegos compartido**: el modelo más básico y barato, pero menos seguro. La DMZ y la intranet tienen el mismo nivel de seguridad. Es usado por la mayoría de las PYME que no disponen de técnicas o técnicos especialistas en sus plantillas.

Autoevaluación

Cuál de las siguientes tecnologías utilizadas para diseñar cortafuegos es la más segura:

- ○ DMZ expuesta.
- ○ DMZ protegida.
- ○ Red perimetral.
- ○ Red total.

No es cierto, no es el más seguro.

No es correcto. Fíjate bien, es más barato, pero menos seguro que la Red perimetral.

Muy bien, esta es la respuesta adecuada.

Incorrecto. No se conoce un diseño con este nombre.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

4.2.- Cortafuegos en Linux Ubuntu.

En la mayoría de los sistemas Linux se utiliza el software “**iptables**” como firewall. Para aprender a manejar el firewall, se puede ver una guía básica en el siguiente enlace:

https://www.linuxadictos.com/introduccion-a-iptables-configura-un-firewall-en-linux.html

Este artículo presenta un tutorial más completo, con diferentes reglas y configuraciones:

https://www.linuxito.com/seguridad/793-tutorial-basico-de-iptables-en-linux

También existe la herramienta “ufw”, que permite manejar la configuración para iptables de una manera más sencilla.

Para saber más

Puedes visitar la página oficial del proyecto Iptables en el siguiente enlace:

Iptables.

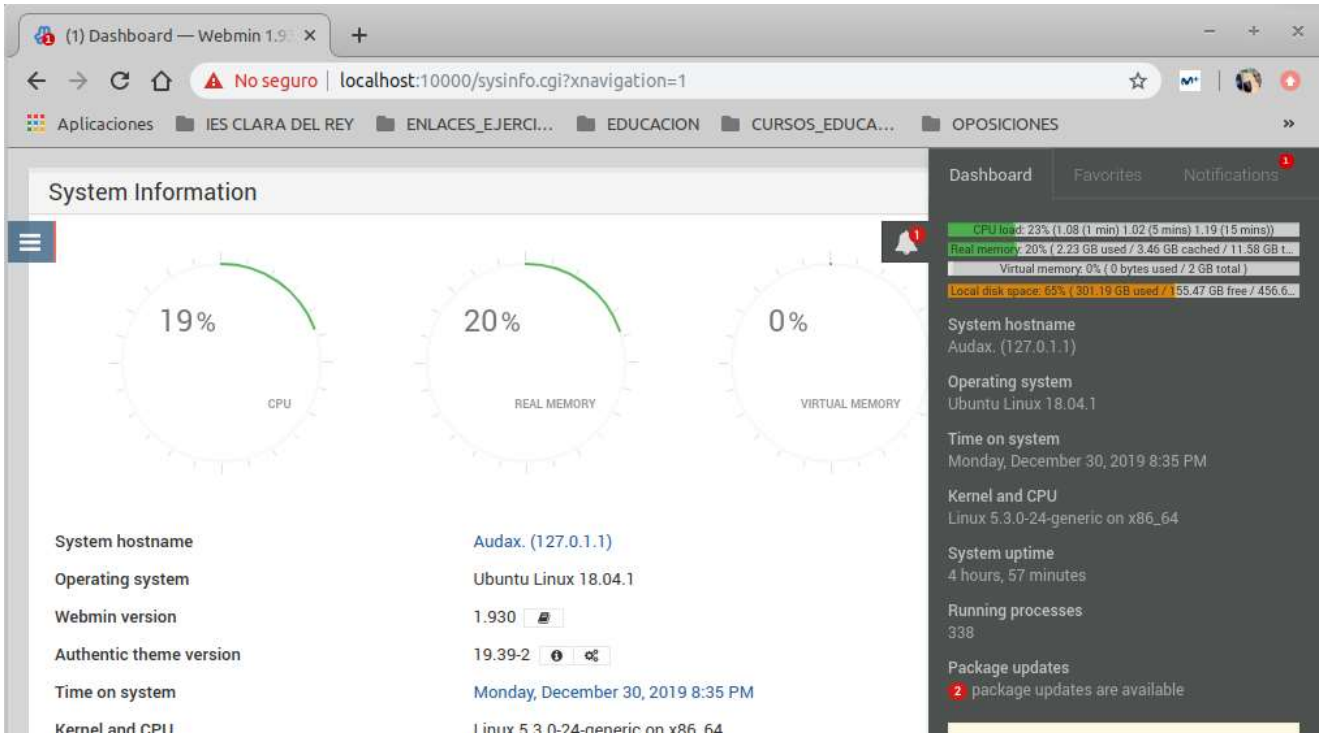
4.3.- Configuración de iptables desde Webmin.

El software de cortafuegos se puede gestionar desde la herramienta Webmin, que hemos visto en otros capítulos de este módulo.
Para saber la versión de iptables, podemos teclear:

```
$ iptables -V
iptables v1.8.3 (legacy)
```

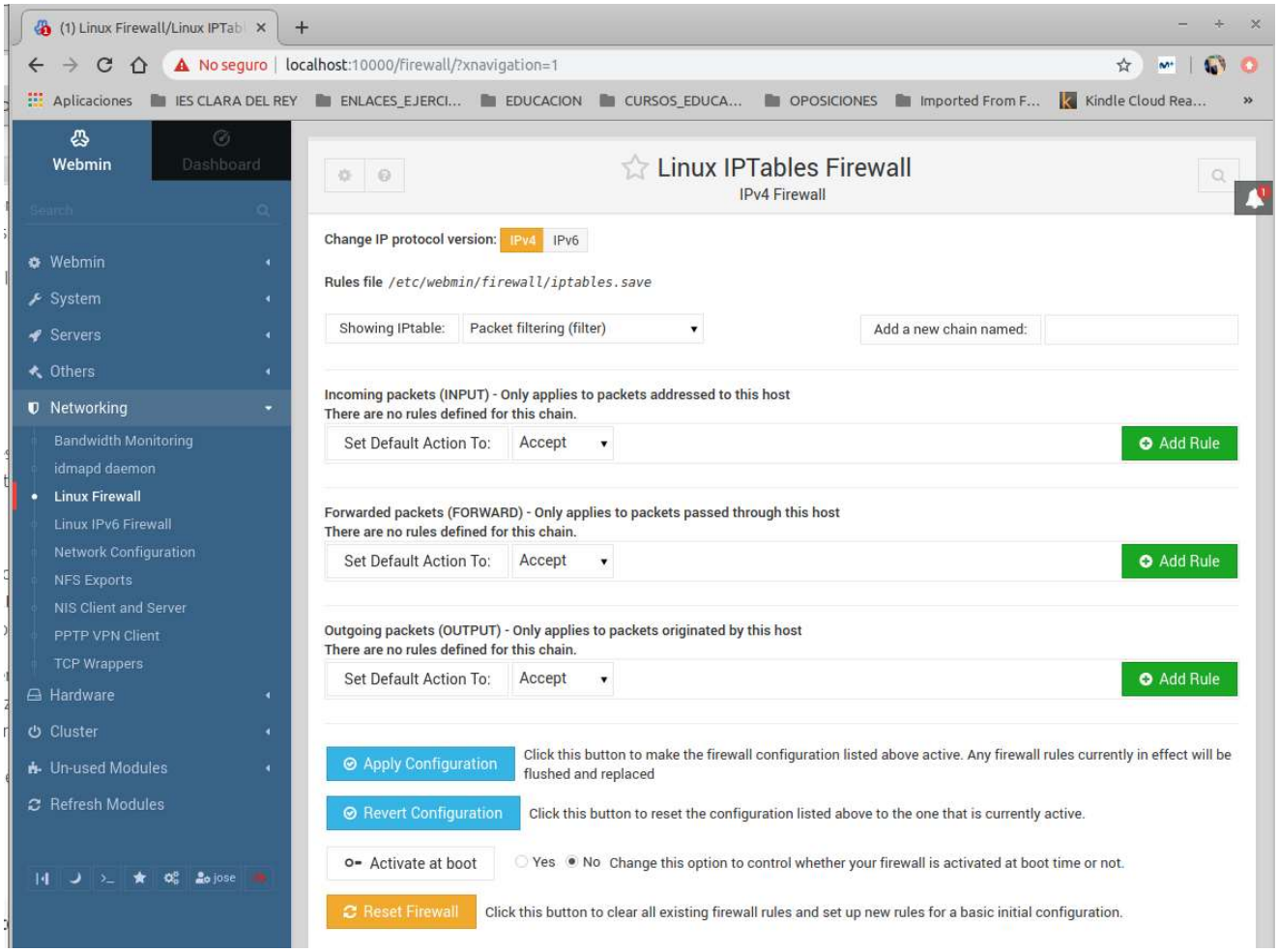
La administración de Webmin se realiza mediante el navegador web, accediendo a la URL

https://localhost:10000



José A. Jiménez (CC0)

Para acceder al menú de iptables, pulsamos en el menú de la izquierda, opción “Networking”, apartado “Linux Firewall”, y veremos una pantalla como la siguiente:



José A. Jiménez (CC0)

En esta pantalla podemos añadir y modificar reglas, resetear la configuración, etc…, tanto para IPv4 como para IPv6.

Autoevaluación

Rellena los huecos con los conceptos adecuados.

El cortafuegos por defecto de Ubuntu es: _____

Enviar

5.- El servidor Proxy-Caché.

Caso práctico

La idea inicial que tenia Alicia, era instalar toda la seguridad en el servidor. Por lo tanto, sería muy operativo que los accesos a Internet fueran gestionados por éste. Por otro lado, sería bueno que se pudieran restringir el acceso a algunas páginas Web, para evitar virus y pérdidas de tiempo por parte de algunos empleados y empleadas.

Stockbyte. (Uso educativo nc)

"El servidor proxy actúa como intermediario entre los equipos de una red de área local e Internet. Generalmente el servidor proxy se utiliza para la Web. Sin embargo, puede haber servidores proxy para cada protocolo de aplicación –pensó Alicia."

"Creo que me irá bien un servidor Proxy para el acceso a la Web. De esta forma podré restringir algunas páginas."

"También se gestionara mejor el ancho de banda de la conexión a Internet. Si instalo un servidor Proxy-Cache, muchas páginas las tendré ya en el servidor y no tengo que descargarlas de Internet."

"Tengo que seleccionar una herramienta para configurar el servidor como Proxy-Caché –pensó Alicia.

"Que no se me olvide, tener en cuenta que voy a instalar el cortafuegos también en el servidor, esto es importante a la hora de seleccionar la herramienta".

Es posible que alguna vez entrando en el apartado de conexiones de tu navegar, hayas visto una opción en la que pide la dirección de un servidor Proxy. Pues bien, vas a ver para qué sirve esto.

El principio operativo básico de un servidor proxy es bastante sencillo: se trata de un servidor que actúa como **"representante"** de una aplicación efectuando solicitudes en Internet en su lugar. De esta manera, cuando un usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un servidor proxy, la aplicación primero se conectará con el servidor proxy y le dará la solicitud. El servidor proxy se conecta entonces al servidor al que la aplicación del cliente desea conectarse y le envía la solicitud. Después, el servidor le envía la respuesta al proxy, el cual a su vez la envía a la aplicación del cliente.

La mayoría de los proxy tienen una **caché**, es decir, la capacidad de guardar en memoria (“en caché”) las páginas que los usuarios de la red de área local, que visitan comúnmente para poder proporcionarlas lo más rápido posible. De hecho, el término "caché" se utiliza con frecuencia en informática para referirse al espacio de almacenamiento temporal de datos (a veces también denominado "**búfer**").

Un servidor proxy con la capacidad de tener información en caché generalmente se denomina servidor "**proxy-caché**".

Esta característica, implementada en algunos servidores proxy, se utiliza para disminuir tanto el uso de ancho de banda en Internet como el tiempo de acceso a los documentos de los usuarios.
Sin embargo, para lograr esto, el proxy debe comparar los datos que almacena en la memoria caché con los datos remotos de manera regular para garantizar que los datos en caché sean válidos.

Para utilizar un servidor Proxy-caché tienes que contactar con la empresa suministradora del acceso a Internet y preguntar si disponen de este servicio. Si lo tienen, deberán facilitarte la dirección del servidor Proxy y el puerto. Con estos datos ya se puede configurar el navegador para que utilice este servicio.

5.1.- Funcionamiento del Proxy-Caché.

En primer lugar, tendrás que tener configurados los ordenadores clientes para acceder a Internet a través de un servidor Proxy-caché. El funcionamiento es el siguiente:

Alicia Galán Gutiérrez. (Uso educativo nc)

- El navegador Web (cliente) **solicita** una página HTML a un servidor Web pero en realidad lo que está haciendo es acceder al Proxy-caché.
- El Proxy-caché **recibe la petición y busca en la caché (**disco duro del Proxy) la página solicitada.
- Si es la primera vez que se accede a la página Web, el Proxy-caché no la tiene almacenada y **reenvía la petición al servidor Web** el cual se la proporciona. El Proxy la guarda en la caché y se la **envía al cliente** que la había solicitado.
- Si el Proxy-caché la tiene almacenada, solicita al servidor Web que le envíe la cabecera de la página. En la cabecera tiene: fecha de creación y fecha de modificación. El Proxy-caché la **compara** con la copia de la página HTML almacenada en la caché. Si la página no ha sido modificada se la envía al **navegador** del cliente. Si por el contrario, la página ha sido modificada se la envía el **servidor** Web.

Por otra parte, al utilizar un servidor proxy, las conexiones pueden rastrearse al crear **registros de actividad (logs)** para guardar sistemáticamente las peticiones de los usuarios cuando solicitan conexiones a Internet.

Gracias a esto, las conexiones de Internet pueden filtrarse al analizar tanto las solicitudes del cliente como las respuestas del servidor. El filtrado que se realiza comparando la solicitud del cliente con una lista de solicitudes autorizadas se denomina **lista blanca**; y el filtrado que se realiza con una lista de sitios prohibidos se denomina **lista negra**. Finalmente, el análisis de las respuestas del servidor que cumplen con una lista de criterios (como palabras clave) se denomina **filtrado de contenido**.

Como el proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, a veces se le puede utilizar para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña. También es fácil otorgarles acceso a recursos externos **sólo a las personas autorizadas** y registrar cada uso del recurso externo en archivos de registro de los accesos identificados.

Este tipo de mecanismo, cuando se implementa, obviamente genera diversos problemas relacionados con las libertades individuales y los derechos personales.

Autoevaluación

Rellena los huecos con los conceptos adecuados.

El principio operativo básico de un servidor proxy es bastante sencillo: se trata de un servidor que actúa como… _____

Enviar

5.2.- Proxy-Caché en Ubuntu GNU/Linux.

Sin duda, la herramienta proxy más utilizada es Squid, es un software de uso libre y gratuito, disponible para diversas plataformas que incluye a Windows y Linux.

Stockbyte. (Uso educativo nc)

Squid es un Servidor Intermediario (Proxy) de alto desempeño, que puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS, filtración de contenido y control de acceso por IP y por usuario.

Consiste básicamente en un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación, algunas herramientas para administración y herramientas para clientes.

En los sistemas Linux no se instala por defecto, pero se encuentra en los repositorios de Ubuntu, por lo que puede ser instalado a través de Synaptic, Aptitude o apt-get.

Para saber más

Squid es un software libre y cuenta con un sitio web oficial:

Squid.

Autoevaluación

El servidor Proxy más usado es:

- ○ Synaptic.
- ○ Iptables.
- ○ Squid.
- ○ No hay ninguno más usado que otros.

No es cierto. Con este programa puedes instalarlo.

Incorrecto. Esto tiene que ver con los cortafuegos.

Muy bien, esta es la respuesta esperada.

No es correcto. Es Squid.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

5.3.- Configuración básica de Squid.

El archivo de configuración se encuentra en **/etc/squid/** y se llama **squid.conf**. Si lo observas, es un archivo bastante grande ya que Squid es un servidor proxy bastante completo.

Alicia Galán Gutiérrez. (Uso educativo nc)

Una configuración básica debe incluir, al menos, los parámetros que se indican a continuación:

- **http-port**: Establece el puerto de escucha para squid (por defecto puerto 3128).
- **visible_hostname**: nombre del equipo.
- **acl**: a cada ACL o lista de control de acceso se le hace corresponder una regla de control de acceso (http_access) que es la que permite o deniega las conexiones definidas en cada ACL.

Parámetro cache_dir: ¿Cuanto deseas almacenar de Internet en el disco duro?

Este parámetro se utiliza para establecer el tamaño de la caché en el disco duro para Squid. Para entender esto un poco mejor, responde a esta pregunta: ¿Cuanto deseas almacenar de Internet en el disco duro? De modo predefinido Squid utilizará un caché de 100 MB, de modo que encontrará la siguiente línea:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Puedes incrementar el tamaño de la caché hasta donde lo desee el administrador. Cuanto más grande sea la caché, más objetos se almacenarán en ésta y por lo tanto se utilizará menos el ancho de banda. La siguiente línea establece un caché de 700 MB:

```
cache_dir ufs /var/spool/squid 700 16 256
```

Los números **16 y 256** significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno. No modifiques estos números, no tienes necesidad de hacerlo.

Es muy importante considerar que si se especifica un determinado tamaño de caché y éste excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente. Tienes que tener cautela con el tamaño de caché especificado.

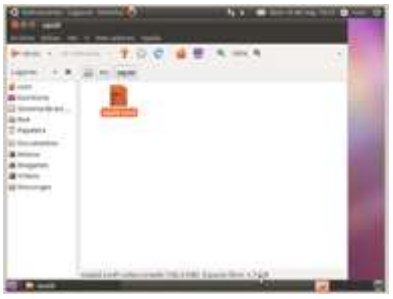
Para saber más

En el siguiente enlace puedes ver como se instala y configura Squid en Ubuntu 18.04:

https://www.sololinux.es/instalar-squid-proxy-server-en-ubuntu-18-04/

5.4.- Ejemplo de configuración básica de Squid.

Para que entiendas un poco mejor como se configura Squid, a continuación vas a ver un ejemplo de configuración muy frecuente, en el que vas a denegar el acceso a una dirección de internet.



Alicia Galán Gutiérrez. (Uso educativo nc)

Ejemplo: Denegar la dirección www.youtube.com a todas las máquinas.

Abres y editas el fichero de configuración de squid.conf:

```
#Parámetros obligatorios:
visible_hostname debian
http_port 3128
cache_mem 64 MB
cache_dir ufs /var/spool/squid 700 16 256
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
#Listas de control de acceso:
acl all src 0.0.0.0/0.0.0.0
acl denegado dstdomain www.youtube.com
acl localhost src 127.0.0.1
#Control de acceso:
http_access deny denegado !localhost
http_access allow all
error_directory /usr/share/squid/errors/Spanish
```

En esta configuración, puedes observar:

1. En el apartado de parámetros obligatorios: el puerto de escucha, el nombre del servidor (si no sabes cuál es el nombre de tu máquina, vete a un terminal y teclea "hostname"), el tamaño de la memoria cache y las rutas.
2. En el segundo apartado se encuentran las listas de control de acceso, en las cuales se asigna el rango de IP, asignación de dominio, etc.
3. En el tercer apartado defines el control de acceso. Una vez asignadas las listas de control con http_access **deny** se **deniegan** ya sea IP ó dominios, y con http_access **allow**, se **permite** lo mismo. También por ahí aparece una línea error_directory la cual muestra los mensajes de advertencia en idioma español.

Para Resetear squid:

```
# /etc/init.d/squid restart
```

Si no aparece ningún mensaje de error entonces tu proxy debe de funcionar de acuerdo a lo establecido. Para poder probarlo vete a un navegador de una máquina que esté conectada en la misma LAN, mira en las propiedades y habilita el uso de Proxy. En la IP, tienes que poner la IP de la máquina que tiene el squid corriendo.

Cuando hagas pruebas te bloqueará www.youtube.com, pero si pones youtube.com "sí" te dejará entrar, para eso se utiliza otra lista de control de acceso:

```
acl denegado url_regex “/home/tuusuario/denegados”
```

Dónde /home/tuusuario/denegados es un simple archivo de texto que contiene la palabra "youtube", con eso, todos los dominios youtube serán bloqueados.

Autoevaluación

El fichero de configuración donde se introducen los parámetros de Squid se llama, [ ] y está en el directorio /etc/squid/.

Enviar

Evidentemente es “squid.conf”.

6.- Cortafuegos y Proxy-caché en Windows.

Caso práctico

Stockbyte. (Uso educativo nc)

Alicia ya ha tomado todas las decisiones importantes. Instalará el servidor Proxy-caché en Linux con Squid. En estas, se vuelve a encontrar con Manuel y Pedro.

-¡Buenas días! ¿Qué tal? -dijo Alicia.

-Muy bien, gracias –respondió Manuel.

-¿Cómo vas con el trabajo? –preguntó Pedro.

-Ya he tomado todas las decisiones importantes. Ahora tengo que empezar a configurar todos los equipos nuevos –respondió Alicia.

-¿Qué sistema operativo instalaras en el servidor? –pregunto Pedro.

-Linux ya que voy a instalar un servidor Proxy con Squid. –respondió Alicia.

-Me gustaría que me recomendaras alguna herramienta para configurar un servidor Proxy en Windows –dijo Pedro-. En casa tengo varios ordenadores y me gustaría restringir el acceso a algunas páginas Web, para que no entren mis hijos.

-Es una buena solución, -contestó Alicia-. Aquí también vendría bien para la sucursal pequeña que tenéis en Madrid.

-Existen gran cantidad de aplicaciones de este tipo para Windows en general. En este caso me inclino por elegir Outpost Firewall Pro, de uso muy sencillo y eficaz a la hora de cubrir las necesidades de seguridad de un aula o de una PYME –respondió Alicia.

-Muchas gracias –contestó Pedro.

Estamos a punto de finalizar este módulo de Servicios de Red. Deseamos que todos estos contenidos te hayan sido de utilidad y te animamos a que sigas profundizando en estos servicios.

Aparte de las aplicaciones que hemos tenido ocasión de utilizar a lo largo de este módulo, existen diferentes soluciones comerciales y de código abierto para llevar a cabo la implementación y configuración de diferentes servicios en red. En un entorno cambiante, en el que no paran de surgir nuevas soluciones tecnológicas, debes acostumbrarte a estar siempre dispuesto a aprender más y conocer nuevas aplicaciones.

Volviendo al capítulo que nos ocupa, simplemente decir que también existen versiones de cortafuegos y proxy-caché disponibles para Windows, como el propio software squid, que hemos visto en el capítulo anterior.

Para saber más

En la página oficial de Squid puedes descargar versiones para cualquier sistema operativo con el que trabajes:

https://wiki.squid-cache.org/SquidFaq/BinaryPackages