Redes Seguras.

Caso Práctico

A Juan le han encargado la difícil labor de encontrar por qué la red de la empresa ha disminuido su velocidad sin ninguna causa aparente, lo que antes se descargaba en un abrir y cerrar de ojos, resulta que ahora tarda unos minutos. Juan está preocupado y lleva todo el fin de semana pensando en la solución al problema, llama a Iván para que le solvente algunos problemas.

Diego Méndez (Uso educativo nc)

-Si lo que queremos es saber qué está pasando en la red de nuestra empresa lo mejor será analizar el tráfico de la red. Así podremos saber qué está pasando –sugirió Iván.

-Ya, no es mala idea, pero si analizamos todo el tráfico va a suponer un trabajo de al menos ocho horas diarias para una persona. ¿Has visto la cantidad de tramas que se capturan en cinco minutos? –observó Juan.

-Bueno, yo no estaba pensando en una persona, -dijo Iván- sino en algún programa especializado que hiciera esa labor por nosotros.

-¡Ah!, ya te entiendo, sería como un guardia de seguridad paseándose por la empresa observando aquí y allá, pero por la red de la empresa –supuso Juan.

-Sí, eso es, esa es la idea.

-Bueno, pero a lo mejor con que el guardia de seguridad esté en la puerta sería suficiente –valoró Juan.

-Ya, ya, igual sí, si controlas todo el tráfico que entra, entonces estás seguro de lo que hay dentro.

-Bueno, igual una combinación de las dos, -propuso Juan- controlar qué tráfico entra en la empresa y después comprobar que en el interior toda la actividad sea "bien intencionada".

-La actividad de quién ¿de las personas? –preguntó Iván.

-Bueno, yo estaba pensando en software "malintencionado" actuando en algún ordenador. –respondió Juan.

Para saber más

En el siguiente enlace dispones de un artículo de RedIRIS sobre qué son los IDS (en inglés, Intrusion Detect System, sistema detector de intrusos) y sus características principales, así como las utilidades de los mismos.

Sistemas de detección de intrusos

Debes conocer

Presentación sobre los contenidos fundamentales que se tratarán a lo largo de todo el tema. Es interesante que veas esta presentación para que te familiarices con los IDS

Descripción textual del vídeo

1.- Redes Seguras.

Caso Práctico

KIU es una proveedor de Servicios de Internet, es algo que tienen como otra actividad más, pues también se dedican a la compra-venta de cartuchos de impresora, tienen varias oficinas en la zona norte, en cada oficina tienen un servidor dedicado para alojar las páginas web de su clientela. Aparentemente han sufrido un ataque en una de las oficinas y quieren que no les ocurra en el resto, a Juan le van a encargar el caso:

Diego Méndez (Uso educativo nc)

-Hola Juan, te llamo ahora porque KIU, la empresa con la que tenemos un contrato de mantenimiento de hardware, quieren que les hagamos un estudio sobre la seguridad en sus servidores –dice Iván.

-Bueno, Iván, será sobre la vulnerabilidad de sus servidores ¿no?

-No, Juan, no, dicen que quieren estar seguros de que lo que tienen instalado es lo adecuado.

-Bueno, entiendo que estén preocupados, pero no han tenido ningún problema ¿no? –pregunta Juan.

-No, ellos, no. Pero la oficina que tienen en Vitoria sí los ha tenido –dijo Iván.

-¿Qué pasó? –continuó Juan.

-Pues no lo saben muy bien, Juan, pero tienen muchos equipos de la oficina totalmente inoperativos hasta ver qué ha pasado.

-Pero, ¿no pueden ser más concretos?, por lo que cuentas parece cosa de brujas –pensó Juna.

-Bueno, pues creen que alguien ha conseguido autentificarse suplantando la identidad de un empleado. El error que tienen es que un usuario se ha conectado de nuevo a la sesión del servidor VPN desconectada y ha realizado una exploración, es decir, que buscaba determinar los ordenadores encendidos en la red con barridos de ping –contestó Iván.

-El empleado dice que cerró la sesión –sigue Iván-, pero en la auditoría se desveló que no la cerró y alguien siguió operando con su sesión abierta, el caso es que los clientes de la empresa se empiezan a quejar de falta de servicio.

-Bueno, Iván, menudo problema, el empleado estará siendo acusado de exploración y enumeración, ya sabes, buscar debilidades en los servicios –recordó Juan.

-Está claro que el empleado no ha podido ser, porque el atacante buscaba una cuenta con privilegios que el usuario no tiene -concluye Iván.

Con todo lo que has visto en las unidades anteriores hasta ahora habrás comprendido que las amenazas informáticas ya no sólo son con la inclusión de troyanos en los sistemas o software espía, sino que los ataques se han profesionalizado y manipulan el significado del contenido virtual. Así los hackers optan por modificar los contenidos digitales para buscar la confusión del usuario, que asustado por lo que ve en la pantalla realiza acciones con consecuencias nefastas.

Carlos Martínez Rodríguez (CC BY-NC-SA)

¿Qué podemos hacer para evitar intrusiones en los servidores? Para que estas modificaciones de los sitios web no se produzcan hay que defender y observar los sistemas servidores, además de mantenerlos actualizados los sistemas operativos y las aplicaciones.

Seguro que tú, como usuario o usuaria avanzada te mantienes alerta, no sólo actualizas y proteges tu ordenador, sino también verificas los adjuntos, no descargas elementos potencialmente peligrosos y no realizas operaciones comerciales desde redes públicas.

Vamos a ver en esta unidad cómo tú, como técnico ó técnica en Sistemas Microinformáticos puedes defender los servidores de la empresa, observar los diferentes ataques que recibas y aprender de ellos a no caer en las trampas similares que puedan llegar de nuevo.

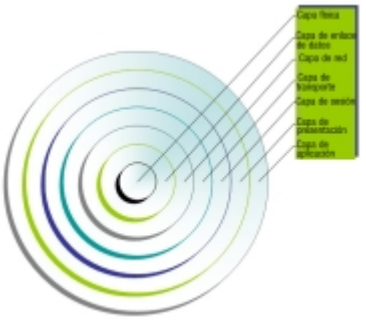
Para saber más

Siempre que navegas por la red, vas dejando rastro, rastros que pueden ser utilizados posteriormente para atacar tu sistema. Cuando envías un e-mail, además informas de tu dirección de e-mail. ¿Puedes enviar un email sin saber que lo estás haciendo, o mejor aún, puedes mandar un mail de manera anónima? En el siguiente enlace podrás ver que es posible enviar mails anónimos empleando un determinado conjunto de herramientas.

Enviando correos anónimos

1.1.- Niveles OSI.

Prácticamente todas las redes en uso hoy en día se fundamentan en alguna forma en la Interconexión de **Sistemas Abiertos (OSI)** de serie. Como ya sabes, esta norma es el modelo de referencia OSI, un conjunto de siete capas que definen las diferentes etapas que los datos deben pasar por viajar de un dispositivo a otro en una red.



Mª Belén Álava Millán (Uso educativo nc)

Las Capas y las pilas de protocolos.

Piensa en las siete capas de la línea de montaje en el ordenador. En cada nivel, suceden ciertas cosas a los datos que se preparan para la siguiente capa. Las siete capas, se separan en dos grupos, conjunto de aplicaciones con las capas 7, 6 y 5 y juego de transporte, el resto. Una pila de protocolo es un conjunto de protocolos que trabajan juntos para permitir que el software o hardware realicen una función. La pila de protocolos TCP/IP es un buen ejemplo.

Asignación de las capas OSI a la pila de protocolos TCP/IP.

Conjunto de aplicaciones.	Pilas de protocolos.
✓ **Nivel 7: Aplicación -** Interactúa con el sistema operativo o aplicación cuando decides transferir archivos, leer mensajes o realizar otras actividades relacionadas con la red. ✓ **Nivel 6: Presentación –** Toma los datos proporcionados por la capa de aplicación y la convierte en un formato estándar que las otras capas pueden entender. ✓ **Nivel 5: Sesión –** Establece, mantiene y termina la comunicación con el dispositivo receptor.	✓ **Capa 4: Aplicación –** Combina la sesión, presentación y las capas de aplicación del modelo OSI. Protocolos para funciones específicas, tales como el correo electrónico (Simple Mail Transfer Protocol, SMTP) y transferencia de archivos (File Transfer Protocol, FTP) residen en este nivel.
✓ **Nivel 4: Transporte -** Mantiene el control del flujo de datos y proporciona comprobación de errores y recuperación de datos entre los dispositivos. El control de flujo significa que la capa de transporte va a ver si los datos provienen de más de una aplicación e integra los datos de cada aplicación en un único flujo de la red física.	✓ **Capa 3: Transporte -** Correspondientes a la capa de transporte del modelo OSI, esta es la parte de la pila de protocolos en el control de transporte (TCP) que se puede encontrar. TCP trabaja al pedir a otro dispositivo en la red si está dispuesto a aceptar la información del dispositivo local.

Conjunto de aplicaciones.	Pilas de protocolos.
Nivel 3: Red - La forma en que los datos se envían al dispositivo receptor se determina en esta capa. Protocolos de enrutamiento y direccionamiento se manejan aquí.	**Capa 2: Internet -** Esta capa corresponde a la capa de red. El Protocolo de Internet (IP) utiliza la dirección IP, que consiste en un identificador de red y un identificador de HOST, para determinar la dirección del dispositivo que está comunicando.
Nivel 2: Los datos - En este nivel, el protocolo físico adecuado es asignado a los datos. Además, se define el tipo de red y la secuencia de paquetes. **Nivel 1: Física -** Es el nivel del hardware. En él se definen las características físicas de la red, como las conexiones, los niveles de voltaje y el tiempo.	**Capa 1: Interfaz de Red -** Combina la capa física y de datos y las rutas de datos entre los dispositivos en la misma red. También gestiona el intercambio de datos entre la red y otros dispositivos.

Como puedes ver, no es necesario el desarrollo de una capa separada para la función de todos y cada uno de los niveles que se indican en el modelo de referencia OSI.

Para saber más

En este vídeo puedes ver cómo funcionan las capas de TCP/IP.

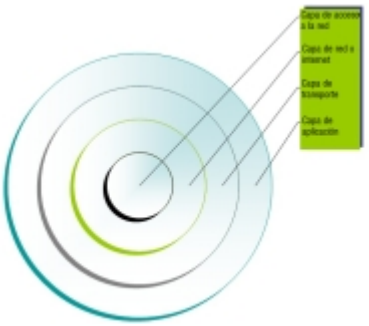
https://www.youtube.com/embed/OggT7734QHY

Descripción textual del vídeo

1.1.1.- Seguridad en las Capas.

Como sabes, una pila de protocolo es un conjunto de protocolos que trabajan juntos para permitir que el software o hardware puedan realizar una determinada función. La pila de protocolos **TCP/IP** es un buen ejemplo. En la práctica se utiliza la pila de protocolos llamada TCP/IP.

Elementos de seguridad que se instalan en cada una de las capas OSI y TCP/IP:



Mª Belén Álava Millán (Uso educativo nc)

Capas OSI y TCP/IP.

Niveles OSI.	Capas TCP/IP.	Seguridad.
Físico.	**Acceso a la red.**	SAI, Control de acceso al medio, Copias de seguridad.
Enlace.		Filtrado por MAC, cifrado en redes inalámbricas.
Red.	**Internet.**	Control de acceso por IP, filtros de correo, IDS, Firewall.
Transporte.	**Transporte.**	Control de puertos, PROXY e IDS.
Sesión. Presentación. Aplicación.	**Aplicación.**	Configuración del navegador. Firewall de HOST, IDS.

Puedes ver en esta tabla cómo los diferentes sistemas de seguridad trabajan principalmente en una capa, pero hay algunos que necesitan más de una, por ejemplo un IDS.

Que un sistema de seguridad no esté clasificado en una de las capas no significa que no la utilice, sólo trata de entender cómo cada uno de los elementos estudiados tiene una capa de la que necesitan los datos que allí se manejan.

Para saber más

El término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de

intrusión. Trabaja en diferentes capas, en este enlace podrás encontrar una explicación muy buena sobre cómo trabaja IDS en las diferentes capas.

IDS y las capas TCP/IP

Autoevaluación

¿En qué nivel TCP/IP no trabajan los IDS?

- Nivel de acceso a la red.
- Nivel de Internet.
- Nivel de transporte.
- Nivel de aplicación.

Correcta porque en esta capa se implementan las direcciones MAC y las definiciones de VLAN.

No es correcta, en esta capa se trabaja en los IDS con el protocolo IP.

Incorrecto, en esta capa se implementan los protocolos TCP y UDP sobre los que trabajan los IDS.

No es la respuesta correcta porque algunos IDS examinan nombre NETBIOS incorrectos, y esto es del nivel de aplicación.

Solución

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

1.2.- Redes Privadas Virtuales.

Hoy estaba fuera del trabajo cuando recordé no haber apuntado la falta de un empleado en la hoja de ausencias. Cuando llegué a casa me conecté al trabajo a través de una conexión privada virtual, y accedí a la unidad de red compartida donde tengo estos documentos. Allí apunté la ausencia del empleado. Después me desconecté.

Pablo María García LLamas. (CC BY-NC-SA)

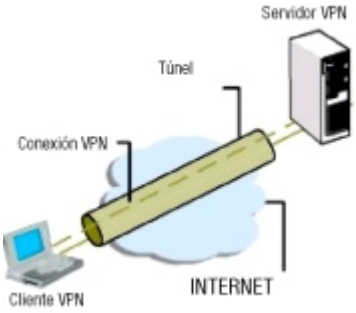
Como ves, los accesos remotos permiten a los usuarios, proveedores e invitados acceder a la LAN, aún cuando físicamente se encuentren fuera de la LAN. El servicio más seguro que proporcionan este tipos de conexión es a través de **VPN** (Virtual Private Network, en inglés, Red Privada Virtual).

- **Virtual**: Virtual porque no necesita de un circuito dedicado para funcionar.
- **Private**: Privada porque proporciona mecanismos de encriptación mediante distintos algoritmos.
- **Network**: Es una red dado que una vez establecida, funciona y se administra como una LAN estándar.

Tipos de VPN.

Por Hardware:

- **Firewall**: además de cumplir su función principal que es la de inspeccionar el tráfico, permiten la implementación de túneles seguros.
- **Gateway**: son dispositivos construidos para implementar VPN específicamente. Tienen gran velocidad y soportan mayor cantidad de túneles que los Firewalls.
- Servidores de acceso: permiten la implementación directa de VPN. Esta función puede negociarse con el ISP.



Licencia: Uso educativo nc

Por Software:

- Directamente con el sistema operativo: Linux, Windows 2008, Windows 2012, Windows 2016.
- Utilizando aplicaciones específicas para la creación, administración y monitoreo de VPN.

Reflexiona

¿Es seguro conectarse a través de VPN?

Puedes afirmar sin equivocarte que sí es seguro conectarse y enviar datos a través de VPN, pues cumple los cuatro principios de seguridad:

- **Confidencialidad**: Esta conexión realiza una encriptación de datos, de forma que todos los datos son cifrados y encapsulados en otra trama.
- **No repudio**: las personas que realizan la conexión VPN deben identificarse en el servidor, de manera que se evite que un usuario niegue ser el autor de la información que se genere en la VPN.
- **Integridad**: Un sistema de hash acompaña a los datos para comprobar la no modificación, pérdida o deterioro de los mismos durante el trayecto.
- **Autentificación**: La contraseña proporcionada al usuario permite que sólo sea éste el que se conecte a la red mediante este servicio.

Debes conocer

Los protocolos de VPN más populares y los que la mayoría de los fabricantes utilizan:

Protocolos de VPN

Autoevaluación

¿Qué protocolo VPN está incluido en todas las versiones de Windows?

- ○ IPSec.
- ○ PPTP.
- ○ L2TP.
- ○ PTTP.

Incorrecto, el IPSec es una extensión del protocolo IP ideado y administrado por la IETF (Internet Engineering Task Force) y que aporta seguridad al actual estándar universal IP (tanto v4 como v6). IPSec puede proteger cualquier protocolo que se ejecute sobre IP, por ejemplo, TCP, UDP e ICMP. IPSec proporciona servicios criptográficos para autentificación, seguridad, control de acceso y de confidencialidad.

Correcta, El PPTP es un protocolo de túnel VPN definido por el foro PPTP y en él los paquetes PPP se encapsulan en los paquetes IP.

Todas las versiones de Windows incluyen el software necesario para acceder a una VPN basada PPTP.

No es correcta. L2TP es una extensión del protocolo PPTP utilizado generalmente por proveedores de servicios de Internet (ISP) para creación de túneles seguros en su red IP.

No es cierto, no existe ningún protocolo PTTP sobre VPN.

Solución

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

1.2.1.- Introducción a las Redes Privadas Virtuales.

Imagina que tu negocio crece, y amplías de una a varias tiendas en todo el país y varias oficinas alrededor del mundo. Para mantener las cosas funcionando de manera eficiente, necesitarás una forma rápida, segura y fiable para compartir información a través de redes de datos con todos ellas. Además, tendrás empleados y empleadas que viajan, que necesitan una forma igual de segura y confiable para conectar a la red informática de tu negocio desde ubicaciones remotas.

Una tecnología popular para lograr estas metas es una VPN (red privada virtual). Una VPN es una red privada que utiliza una red pública (**usualmente Internet**) para conectar sitios remotos o usuarios entre sí. Una VPN usa conexiones "virtuales" enviadas a través de Internet desde la red privada de tu empresa hasta el lugar remoto donde se encuentre el empleado o empleada. Mediante una VPN, tu empresa puede **garantizar la seguridad** -cualquier persona que intercepte los datos cifrados no los podrá leer.

VPN no fue la primera tecnología para realizar conexiones remotas.

Stockbyte (Uso educativo nc)

Hace varios años, la forma más común para conectar ordenadores entre múltiples oficinas era mediante el uso de una **línea alquilada**. Líneas alquiladas, como RDSI (Red Digital de Servicios Integrados, 128 Kbps), eran las conexiones de red privada que una empresa de telecomunicaciones podía **arrendar** a sus clientes. Las líneas alquiladas proporcionaban a una empresa una forma de expandir su red privada más allá de su área geográfica inmediata. Estas conexiones forman una sola **red de área amplia (WAN)** para el negocio. A pesar de que las líneas arrendadas son fiables y seguras, los arrendamientos son **caros**, y aumenta el precio a medida que aumenta la **distancia** entre las oficinas.

Hoy en día, Internet es más accesible que nunca, y los proveedores de servicios Internet (ISP) están desarrollando servicios cada vez más rápidos y más fiables y a costos más bajos que las líneas alquiladas. Para aprovechar esto, la mayoría de las empresas han sustituido las líneas alquiladas con nuevas tecnologías que utilizan las conexiones a Internet como base pero sin sacrificar el rendimiento y la seguridad. Tu empresa, como casi todas, empezaría con el establecimiento de una **intranet**, que sería la red privada interna diseñada para uso exclusivo de los empleados y empleadas de tu compañía. Mediante la adición de una **VPN**, tu empresa puede extender toda su intranet de recursos a los empleados y empleadas que trabajan desde **oficinas remotas** o desde sus **hogares**.

Debes conocer

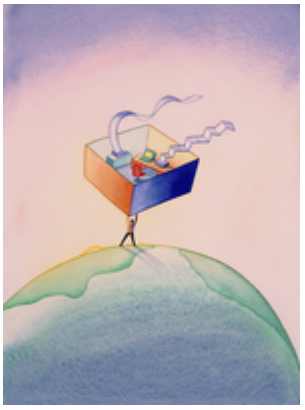
En esta página han realizado una comparativa de ofertas de Fibra para que puedas comprobar de forma sencilla qué empresas son las que ofrecen una

mayor velocidad a mejor precio. Sin duda alguna, comparar ofertas de Fibra es la mejor forma de no arrepentirte al contratar una oferta que en principio parecía atractiva y barata pero después no cumple las expectativas:

Mejores ofertas Fibra

1.2.2.- Analogía: Cada LAN es una isla.

Imagina que vives en una isla en un océano inmenso. Hay miles de otras islas a su alrededor, algunos muy cerca y otros lejos. El medio común de transporte entre las islas es a través del Ferry. Viajar en el **Ferry** significa que casi no tienes privacidad, pues otras personas ven todo lo que haces.



Stockbyte (Uso educativo nc)

Si cada isla representa una red de área local (LAN) y el océano es Internet, viajar en Ferry es como conectarse a un servidor Web u otro dispositivo a través de Internet. Tú no tienes control sobre los cables y los router que forman Internet, al igual que tú no tienes ningún control sobre las otras personas en el Ferry. Tratar de conectar dos de tus redes locales en dos islas diferentes a través de un recurso público puede ser problemático y cuanto menos poco confidencial.

Citas para pensar

"Si no sabes explicar algo de manera sencilla, es que no lo entiendes del todo". ***Albert Einstein.***

Continuando con la analogía, si construyen un **puente** entre las dos islas en las que tienes las oficinas se habrán creado una forma más fácil, más segura y directa para viajar entre las dos islas. Es caro construir y mantener el puente, incluso si las islas están muy juntas. Sin embargo, la necesidad de un camino seguro, es tan grande que habrá que hacerlo de todos modos. Tu isla desea conectarse a otra isla que está mucho más lejos, pero decide que los costos son demasiado difíciles de soportar.

Luis Serrano (CC BY-NC-SA)

Este escenario representa una **línea alquilada**. Los puentes (líneas arrendadas) son independientes de los océanos (Internet), sin embargo, son capaces de conectar las islas (LAN). Las empresas que eligen esta opción lo hacen debido a la necesidad de seguridad y fiabilidad en la conexión entre sus oficinas remotas. Sin embargo, si las oficinas están muy separadas, el costo puede ser prohibitivo –al igual que tratar de construir un puente que se extiende una gran distancia.

Entonces, ¿qué tiene que ver una VPN en todo esto? Usando la analogía, supongamos que cada habitante de su isla tiene un pequeño **submarino**. Vamos a suponer que cada submarino tiene estas propiedades sorprendentes:

- Es rápido.

- Es fácil de llevar con usted donde quiera que vaya.
- Es capaz de ocultarse y pasar inadvertido a otros barcos o submarinos.
- Es confiable.
- Cuesta poco añadir submarinos adicionales a su flota una vez que haya comprado la primera.

A pesar de que viaja por el océano, junto con el resto del tráfico, la gente podía viajar entre las islas cada vez que quisiera con privacidad y seguridad. Eso es fundamentalmente **cómo funciona una VPN**. Cada miembro remoto de la red se puede comunicar de forma segura y fiable a través de Internet como medio para conectarse a la LAN privada. Una VPN puede crecer para dar cabida a más usuarios y diferentes lugares con mucha más facilidad que una línea alquilada. De hecho, la **escalabilidad** es una gran ventaja que tienen las VPN sobre las líneas arrendadas. Por otra parte, la distancia no importa, porque las VPN pueden conectar fácilmente múltiples ubicaciones geográficas del mundo.

Reflexiona

¿Te has parado a pensar que una VPN es en realidad una **muñeca rusa**? Esas muñecas de madera que al abrirla dentro tiene otra muñeca igual pero más pequeña.

Autoevaluación

¿Es la escalabilidad una propiedad de las VPN? ¿Verdadero o falso?

- ○ Verdadero.
- ○ Falso.

Sí, es cierto, has entendido bien el concepto.

Incorrecto, la escalabilidad forma parte de las VPN, por favor, lee de nuevo los apuntes.

Solución

1. Opción correcta

2. Incorrecto

1.2.3.- ¿Qué hace una VPN?

StefanCoders (Licencia de Pixabay)

A continuación, vas a ver lo que constituye una buena VPN, incluyendo sus ventajas y características. El propósito de una VPN es el de ofrecer una conexión privada segura y fiable entre las redes de computadoras en una red pública existente, por lo general en Internet.

Antes de pasarte a la tecnología que hace posible una VPN, tendrás que considerar todos los beneficios y características que tu empresa debe esperar de una VPN.

Debes conocer

En este vídeo puedes ver cómo instalar y configurar una VPN (Red Privada Virtual) en Windows 10:

Instalar y configurar una VPN en Windows 10.

https://www.youtube.com/embed/zYRI_A_ARas

Descripción textual del vídeo

Una VPN bien diseñada ofrecerá a tu negocio los siguientes beneficios:

- Conexiones **extendidas** a través de múltiples ubicaciones geográficas sin necesidad de utilizar una línea dedicada.
- Mayor **seguridad** para el intercambio de datos.
- **Flexibilidad** para oficinas remotas y empleados y empleadas para utilizar la intranet de la empresa a través de una conexión a Internet existente como si estuvieran directamente conectados a la red.
- **Ahorro** de tiempo y dinero a los empleados y empleadas para viajar si el trabajo pueden hacerlo desde los lugares de trabajo virtuales.
- Mejora de la **productividad** de los empleados y empleadas remotos.

Debes conocer

En este vídeo puedes ver cómo instalar y configurar una VPN (Red Privada Virtual) en Linux.

Instalar y configurar una VPN en Linux.

https://www.youtube.com/embed/ywxSdN1Pn_M

Descripción textual del vídeo

Tu empresa no puede exigir a todos, estos beneficios de la VPN, pero debe exigir las siguientes características esenciales VPN:

Stockbyte (Uso educativo nc)

- **Seguridad** - La VPN debe proteger los datos mientras están viajando por la red pública. Si los intrusos intentan capturar los datos, deben ser incapaces de leerlos o utilizarlos.
- **Fiabilidad** - Los empleados, empleadas y oficinas remotas debe ser capaces de conectarse a la VPN sin problemas en cualquier momento (menos en las horas que estén restringidas), y la VPN debe proporcionar la misma calidad de conexión para cada usuario y usuaria, incluso cuando se llegue al número máximo de conexiones simultáneas.
- **Escalabilidad** - Como crece tu empresa, debe ser capaz de extender sus servicios VPN para ayudar al crecimiento sin tener que reemplazar la tecnología VPN.

Una cosa interesante a destacar en las VPN es que no existen normas sobre cómo configurarlas.

Para saber más

En este artículo se describe de una forma muy ligera qué es una VPN, cómo funciona y para qué se usa:

VPN

1.2.4.- VPN de Acceso Remoto y VPN Punto a Punto.

Stockbyte (Uso educativo nc)

Vas va ver la descripción de las que son quizás los modelo más usado actualmente de VPN, la VPN de acceso remoto y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

VPN de acceso remoto.

Una VPN de acceso remoto permite a los usuarios individuales establecer conexiones seguras con una red informática remota. Los usuarios pueden acceder a los recursos de seguridad en la red como si estuvieran directamente conectados a los servidores de la red.

Un ejemplo de una empresa que necesita una VPN de acceso remoto es una gran empresa con **cientos de vendedores itinerantes**, por ejemplo, una empresa de paquetería donde todos sus empleados y empleadas están localizados fuera de la empresa pero realizando labores para la empresa.

Hay dos componentes necesarios para una VPN de acceso remoto:

Stockbyte (Uso educativo nc)

1. **El primero** es un servidor de acceso de red también llamado un **Gateway** (Inglés Pasarela) o pasarela de medios o un servidor de acceso remoto (RAS, Remote Access Service). (Nota: También utiliza NAS en el sentido de almacenamiento conectado a red).
   Un **RAS** consiste en que un usuario se conecta a través de Internet con el fin de utilizar una VPN. La RAS requiere al usuario sus credenciales válidas para acceder a la VPN. Para autenticar las credenciales del usuario, la RAS utiliza su propio proceso de autenticación o bien accede a un servidor de autenticación independiente que se ejecute en la red.

2. **El otro componente** que necesitas para VPN de acceso remoto es un software de cliente. En otras palabras, los empleados o empleadas que quieran utilizar la VPN desde sus ordenadores necesitan software cliente en sus equipos para poder establecer y mantener una conexión VPN. La mayoría de los sistemas operativos de hoy en día han incorporado el software necesario para poder conectarnos a redes VPN de acceso remoto, aunque algunos pueden requerir a los usuarios o usuarias instalar una aplicación específica en su lugar. El software de cliente establece **la conexión de túnel** contra un RAS, al que el usuario accede porque conoce la dirección de Internet del servidor NAS. El software cliente también gestiona el cifrado necesario para mantener la conexión segura.

Debes conocer

Windows Server 2008 incluye varias características nuevas diseñadas para aumentar la seguridad y la capacidad de administración de Enrutamiento y acceso remoto. En esta sección podrás ver estas características nuevas, así como otros cambios reseñables que se han realizado en enrutamiento y acceso remoto en Windows Server 2008:

Novedades de Enrutamiento y acceso remoto en Windows Server 2008

VPN punto a punto.

Una VPN de acceso remoto es ideal para los empleados o empleadas fuera de la empresa, pero ¿qué pasa si los que necesitan realizar una conexión VPN son varias sucursales en las que trabajan decenas o incluso cientos de empleados? A continuación, vas a ver otro tipo de VPN utiliza para mantener a las empresas conectadas de **LAN a LAN.**

Una VPN punto a punto permite a las oficinas en varios lugares fijos establecer conexiones seguras entre sí a través de una red pública como Internet. Una VPN punto a punto extiende la red de la compañía, por lo que los recursos del equipo de un sitio están a disposición de los empleados en otros lugares. Un ejemplo de una empresa que necesita una VPN punto a punto es una empresa con decenas de sucursales en todo el mundo.

Para saber más

Los túneles permiten la encapsulación de un paquete de un tipo de protocolo dentro del datagrama a un protocolo diferente. Por ejemplo, VPN usa PPTP para encapsular paquetes IP a través de una red pública, como Internet. Es posible configurar una solución VPN basada en el protocolo de túnel punto a punto (PPTP), el protocolo de túnel de capa dos (L2TP) o el protocolo de túnel de sockets seguros (SSTP), veamos un ejemplo aplicable a Windows 2008:

Protocolos de túnel VPN

1.2.5.- Mantener el Tráfico en el Túnel VPN.

Stockbyte (Uso educativo nc)

Ahora que conoces los dos tipos de redes privadas virtuales que existen, vas a ver cómo sus datos se mantienen seguros a medida que viajan a través de otra red. La mayoría de las VPN se basan en un túnel para crear una red privada que se extiende a través de Internet.

Recordarás que para enviar un archivo a través de Internet, éste se divide en una serie de **paquetes** que se envían y se reciben por los ordenadores emisor y receptor.

Túnel es el proceso de colocar un paquete entero dentro de otro paquete antes de que sea transportado a través de Internet. El paquete exterior protege el contenido de la vista pública y asegura que el paquete se mueve dentro de un túnel virtual. Esta estratificación de los paquetes se llama encapsulación.

Stockbyte (Uso educativo nc)

Los ordenadores u otros dispositivos de red que están situados a ambos extremos del túnel se llaman **interfaces de túnel** y pueden encapsular los paquetes de salida y volver a abrir los paquetes entrantes. Los usuarios o administradores (en uno o ambos extremos del túnel) pueden configurar las interfaces de túnel para que utilicen un protocolo de túnel determinado, también llamado **protocolo de encapsulación**. Un protocolo de túnel es una forma estándar de encapsular paquetes.

El propósito del protocolo de túnel es añadir una capa de seguridad que **protege** a cada paquete en su viaje a través de Internet. El paquete está viajando con el mismo protocolo de transporte que se ha utilizado sin el túnel, este protocolo define la forma en que cada equipo envía y recibe datos a través de su ISP. Cada paquete interno mantiene el protocolo de pasajero, tal como el protocolo de Internet (IP), que define la forma en que viaja en la LAN en cada extremo del túnel.

El protocolo de túnel usado para la encapsulación añade una capa de seguridad para proteger el paquete en su viaje a través de Internet.

Vas a ver cómo funciona un túnel con un ejemplo. Si te compras un ordenador portátil por internet, el proveedor tiene que enviarte el equipo, le protegerá metiéndolo en un maletín de cuero con cerrojo (protocolo de **pasajeros**) y lo mete dentro de una caja donde escribe el usuario y contraseña (protocolo de **túnel**). Esta caja viaja junto con muchas otras en un camión de mensajería (protocolo de **transporte**). El camión (protocolo de transporte) viaja a través de las carreteras (**Internet**) a tu casa y entrega el equipo. Tú tienes que abrir la caja (protocolo de **túnel**) y escribir el código en el maletín, para finalmente acceder al

equipo (protocolo de **pasajeros**).

Dentro del camión hay muchas cajas, y no saben lo que hay dentro. El transportista lleva la caja sin saber que hay dentro de ésta. Las únicas personas que pueden llegar al ordenador sois tú y el proveedor. Pues **sólo tú y él sabéis la combinación** del candado del maletín metálico.

Para saber más

En este tutorial se describe cómo la red de la universidad de Granada ha apostado por acercar el campus a los hogares a través de Internet. Para conseguir esto sin correr graves riesgos de seguridad han optado por usar túneles VPN (Virtual Private Network).

Configuración de un túnel VPN en GNU/Linux

Autoevaluación

El protocolo de aplicación define la forma en que cada equipo envía y recibe datos a través de su proveedor de servicios de Internet. ¿Verdadero o falso?

- ○ Verdadero.
- ○ Falso.

Incorrecto, es conveniente que leas los apuntes con atención.

Correcto, efectivamente no es en el nivel de aplicación sino en el de transporte.

Solución

1. Incorrecto
2. Opción correcta

1.2.6.- Encriptación y Protocolos de Seguridad en una Red Privada Virtual.

Photodisc (Uso educativo nc)

Stockbyte (Uso educativo nc)

Ahora que ya sabes cómo funciona una VPN, vas a entender cómo se aseguran los datos para su transporte a través de la "insegura" Internet. El **cifrado** es el proceso de codificación de datos para que sólo un ordenador con el decodificador adecuado sea capaz de leerlos. Puedes utilizar la **encriptación** para proteger tus archivos en tu ordenador o para enviar correos electrónicos codificados. Una clave de cifrado le dice al ordenador los cálculos a realizar en los datos con el fin de cifrar o descifrar. Las formas más comunes de cifrado son las de **clave simétrica** de cifrado o/y la de clave **asimétrica** o encriptación de clave pública:

- **En el cifrado de clave simétrica**, todos los equipos (o usuarios) **comparten la misma clave** utilizada para cifrar y descifrar un mensaje.
- **En el cifrado de clave pública**, cada equipo (o usuario) tiene un **par de claves pública y privada**. Una computadora utiliza su clave privada para cifrar un mensaje, y otro que utiliza la clave pública correspondiente para descifrar el mensaje.

Sin embargo, una VPN necesita algo más que un par de claves para aplicar el cifrado. Los protocolos VPN punto a punto puede utilizar el protocolo de seguridad de Internet (IPSec) o la encapsulación de enrutamiento genérico (GRE). GRE proporciona la trama para empaquetar el protocolo para el transporte de pasajeros a través del protocolo Internet (IP). Esta trama incluye información sobre qué tipo de paquete está encapsulado y la conexión entre el emisor y el receptor.

IPSec es un protocolo ampliamente utilizado para proteger el tráfico en las redes IP, incluidas Internet. IPSec puede cifrar los datos entre varios dispositivos, incluyendo router a router, Firewall a router, o desde el escritorio al router, y el escritorio hasta el servidor. IPSec se compone de dos sub-protocolos que utilizan las instrucciones de VPN para asegurar las necesidades de sus paquetes:

- ESP (quiere decir encapsulado de seguridad) ESP cifra la carga útil del paquete con una clave simétrica.
- AH o Cabecera de Autenticación, utiliza una operación de hash en la cabecera del paquete para ayudar a ocultar la información del paquete determinado (como la identidad del remitente) hasta que llega a su destino.

Para saber más

En este enlace puedes ver las soluciones VPN de Claranet (claraVPN), lo

que es un ejemplo de cómo ofrecen a las empresas un circuito privado virtual (VPN) para la transmisión de datos entre diferentes sedes y/o delegaciones de la misma. Lo que da la posibilidad a las empresas de compartir los recursos de todas sus oficinas como si estuvieran en una misma localización física disponiendo así de una verdadera INTRANET entre las distintas oficinas y/o delegaciones.

Soluciones VPN

En este otro enlace tienes algunos escenarios de uso de las VPN:

Escenarios de uso de VPN

Los dispositivos de red pueden utilizar IPSec en uno de los dos modos de codificación. **En el modo de transporte**, los dispositivos cifran los datos que viajan entre ellos. **En el modo de túnel**, los dispositivos construyen un túnel virtual entre dos redes. Como puedes imaginar, las VPN IPSec se utilizan en modo de túnel IPSec con ESP y AH trabajando juntos.

En un acceso remoto VPN, los túneles generalmente se basan en el protocolo punto a punto (PPP), que forma parte de los protocolos nativos utilizados en Internet. Sin embargo, VPN de acceso remoto utilizan uno de los tres protocolos basados en **PPP**:

- **L2F** (Layer 2 Forwarding, desarrollado por Cisco): utiliza cualquier sistema de autenticación que admite PPP.
- **PPTP** (Point-to-point Tunel Protocol, punto-a-punto Protocolo de túnel): Soporta 40-bit y 128-bit de encriptación y cualquier esquema de autenticación que admite PPP.
- **L2TP** (Layer 2 Tunneling Protocol): **combina** las características de PPTP y L2F y es totalmente compatible con IPSec, también se aplica en las VPN de punto a punto.

Reflexiona

Con el tiempo, las personas irán desarrollado nuevas y mejores tecnologías para su uso en redes que mejorarán las características de las VPN existentes. Aunque hay que decir que las tecnologías VPN y los protocolos de túnel actuales, no han cambiado mucho en los últimos tiempos, tal vez porque realizan un buen trabajo conectando oficinas y negocios en todo el mundo.

2.- Cortafuegos o Firewall.

Caso Práctico

Juan e Iván están chateando el fin de semana. Al hermano de Juan le han contratado en un Cibercafé, y el primer día de trabajo llevó su ordenador portátil al trabajo, curiosamente ese mismo día había instalado la última versión de su juego favorito. Juan pregunta a Iván sobre el tema en el chat:

-Oye mira, que mi hermano ha tenido un problema con su ordenador, desde que se ha descargado la última versión de su juego favorito no podemos navegar por internet.

-Será cosa del proveedor de servicios. ¿Habéis llamado? –preguntó Iván.

-Pues sí, ya lo hicimos, llamamos y han hecho varias comprobaciones y resulta que sí que tenemos conexión, de hecho, ahora hay mucho tráfico sobre nuestra IP -le responde Juan.

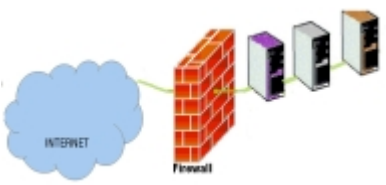
- Pero, eso es una contradicción. Resulta que hay mucho tráfico y no podéis navegar, algo raro pasa -opina Iván.

- Ya, por eso te llamo. ¿Qué puede ser? –dio intrigado Juan.

-Tu hermano ha comprado la última versión del juego o ha intentado descargarla en una red P2P –dice Iván.

- Sí, si, lo ha comprado, no la ha descargado de alguien que la compartía en la red. Pero casualmente hoy ha empezado a trabajar en un Ciber y ha llevado el ordenador al trabajo, conectándolo a la red –responde Juan.

- Vale, entonces voy para allá ahora mismo, hay que estudiar qué ha pasado –dijo Iván.



Mª Belén Álava Millán (Uso educativo nc)

Hasta ahora has oído hablar de seguridad aplicada a equipos o servidores, pero en empresas u organizaciones más grandes en los que el número de equipos es muy elevado hay que pensar en poner defensas análogas al tamaño de éstas. La mayor parte de los ataques se producen desde Internet, y las empresas salen a internet desde sus equipos, pues la mejor forma de defenderse es interponer una **barrera** que filtre el acceso desde internet a la empresa. Esta barrera es lo que se llama **cortafuegos**.

Un cortafuegos o Firewall (inglés: cortafuegos) es un dispositivo **hardware** o **software** que tiene como propósito proteger una red de otras redes a las cuales está conectada.

Estos dispositivos se sitúan en un punto en el cual pueden canalizar todo el tráfico que entra y sale de la red que tienen como objetivo proteger.

Para lograr esta protección efectúan algún tipo de filtrado mediante reglas que se aplican al tráfico que los atraviesa. **Definir estas reglas** será algo que tú como técnico ó técnica tendrás que realizar, teniendo en cuenta, por ejemplo, la dirección origen y la dirección destino del tráfico.

Según el tipo de filtrado que realicen se pueden distinguir dos tipos de Firewall: **Firewall de nivel de red y Firewall de nivel de aplicación.**

Para saber más

Entrevista a Lorenzo de SecurityByDefault, Lorenzo Martínez ha trabajado en seguridad perimetral (cortafuegos, IDs, antivirus, VPN, etc.), en ONO como consultor de seguridad informática y actualmente trabaja como preventa y responsable técnico para España y Portugal de un fabricante francés de cortafuegos de aplicaciones web o WAF (Web Application Firewalls).

Entrevista a Lorenzo de SecurityByDefault

Autoevaluación

Según el tipo de filtrado. ¿Qué tipos de cortafuegos hay? (varias respuestas correctas):

- [ ] Firewall de nivel de enlace.
- [ ] Firewall de nivel de transporte.
- [ ] Firewall de nivel de red.
- [ ] Firewall de nivel de aplicación.

Mostrar retroalimentación

Solución

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

2.1.- Tipos de Cortafuegos.

Cortafuegos de nivel de red.

Aunque se llame cortafuegos de nivel de red, es capaz de examinar el nivel de transporte y de red de los paquetes que los atraviesan. Lo que hace es analizar las cabeceras TCP e IP, y **extrae los parámetros más relevantes**. Por ejemplo, dirección IP de origen y destino, puerto TCP de origen y destino. Con estos parámetros puede filtrar el tráfico según las reglas que en él se hayan definido.

Tipos de políticas de configuración de las reglas de los cortafuegos:

- **Permisiva**: Se **permite** el paso de todo el tráfico excepto el que está contemplado por alguna regla. Esto se hace partiendo de una regla por defecto que se aplica cuando no hay otra regla que aplicar y que en este caso sería una regla que dejaría pasar todo el tráfico independientemente de sus parámetros. Para bloquear cierto tipo de tráfico se tendrían que definir reglas explícitas para ello.
- **Restrictiva**: Se caracteriza por **denegar** todo el tráfico excepto el que está explícitamente permitido. Para esto se crea una regla por defecto que deniegue todo el tráfico independientemente de sus parámetros. De esta forma para permitir algún tipo de tráfico se tienen que **definir reglas explícitas** para ello. Es claro que este tipo de política conlleva más trabajo y que el número de reglas necesarias es más alto, pero también lo es que mejora la seguridad de la red protegida ya que impide que por una configuración incompleta se comprometa la seguridad de la red protegida.

Reflexiona

En general, la política de configuración permisiva no es aceptable para la configuración de un Firewall y sólo en casos muy específicos puede ser conveniente usarla. Piensa si puede haber algún caso en que fuera conveniente esta política.

Según el lugar físico donde se ubique el Firewall en la red recibirá diferentes nombres, podemos entonces hacer otra clasificación de los cortafuegos en **función de su localización**:

- **Perimetrales**: Se sitúan en la zona más externa de la red, y es habitual que sea el mismo **router** de conexión el que **realiza las funciones de cortafuegos**. En algunos casos es un ordenador llamado HOST bastión el que realiza esta función.
- **De sistema**: Se colocan directamente sobre el ordenador que se quiere proteger. Es muy común que el **cortafuegos esté integrado en el sistema operativo**.

Cortafuegos de nivel de aplicación.

Los Firewalls de nivel de red tienen varias limitaciones, una muy importante es que no pueden filtrar tráfico a nivel de aplicación que es donde surgen las necesidades reales en el uso cotidiano de las aplicaciones. Por ejemplo, podrías filtrar el tráfico FTP con un Firewall de nivel de red, pero no podrías filtrar el uso de cierto comando FTP.

Para esto surgen los **Firewalls de aplicación** que se ocupan de analizar el tráfico de cada protocolo de aplicación y permite reglas de filtrado en función de los parámetros del protocolo de cada aplicación por separado.

El **inconveniente** de este tipo de Firewalls es que **requiere un módulo de control para cada aplicación**. Este tipo de Firewalls puede aparecer como HOST independientes o bien como módulos de software integrados en el sistema a proteger.

Para saber más

Firewall Builder, es una aplicación cliente que permite diseñar cómodamente la política de seguridad y luego aplicarla a la máquina cortafuegos de forma directa, mediante una conexión SSH. Dispone de una versión libre y funcional para Linux, así como versiones de pago, aunque con un coste muy bajo, para Windows y Mac OS X. En el enlace verás un pequeño tutorial sobre cómo utilizarla.

Firewall Builder: la GUI para tu cortafuegos

Autoevaluación

¿Son los cortafuegos de nivel de red complementarios a los de nivel de aplicación? ¿Verdadero o falso?

- Verdadero.
- Falso.

Correcto, esta era sencilla, ¿verdad?, trabajan en diferentes niveles y se complementan.

Incorrecto, creo que no has entendido bien el texto, por favor, vuelve a leerlo con atención.

Solución

1. Opción correcta
2. Incorrecto

2.2.- Arquitecturas de Firewall.

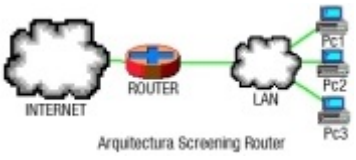
Quizás recuerdes el viejo dicho del refranero español: "hombre prevenido vale por dos", que también puedes aplicar en femenino "mujer prevenida, vale por dos".

Reflexiona

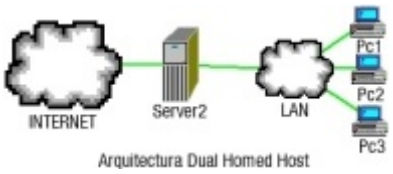
En las configuraciones reales en que tengas que instalar Firewall, puedes optar por instalar dos o más Firewall de diferente tipo. ¿Crees que es buena combinación un Firewall de nivel de red con uno de aplicación? y si lo que prima es la seguridad por encima de todo ¿complementarlos con Firewalls de sistema en las máquinas más críticas?

Según el tipo de cortafuegos instalado necesitarás diferentes tipos de arquitecturas. Las arquitecturas más conocidas son:

- Arquitectura Screening Router.
  - Se trata del modelo de cortafuegos más antiguo, que aprovecha la capacidad de algunos routers, los llamados screening routers, de hacer **enrutado selectivos**, es decir, para bloquear o permitir el tránsito de paquetes mediante listas de control de acceso en función de ciertas características de las tramas, de forma que el router actúe como pasarela de toda la red. Generalmente, tendrás que usar las direcciones origen y destino para determinar el filtrado con lo que **el router se convierte en la pasarela de toda la red**. Claro que también podrías usar, los puertos de origen y destino o el tipo de mensaje. Y si aún quieres más posibilidades podrías utilizar las interfaces de entrada y salida en el router.
- Arquitectura Dual-Homed HOST.
  - Puedes crear este modelo de cortafuegos con máquinas equipadas con **dos o más tarjetas de red**, denominadas **dual-homed HOSTs**, y en las que una de las tarjetas suele conectar a la red interna a proteger y la otra a la red externa a la organización. En esta configuración el screening router y el HOST bastión coinciden en el mismo equipo. Ahora bien, el sistema ha de ejecutar al menos un **servidor PROXY por cada uno de los servicios** que quieras que pase a través del cortafuegos. Esta es la arquitectura más **utilizada hoy en día**.
- Arquitectura Screened Subnet.
  - Screened subnet es la arquitectura más **segura**, pero también la más **compleja**. En esta configuración tendrás que usar **dos routers**, denominados exterior e interior, conectados ambos a la red perimétrica.



Arquitectura Screening Router



Arquitectura Dual Homed Host

M. Belén Álava Millán (Uso educativo nc)

Arquitectura Screened subnet

M. Belén Álava Millán (Uso educativo nc)

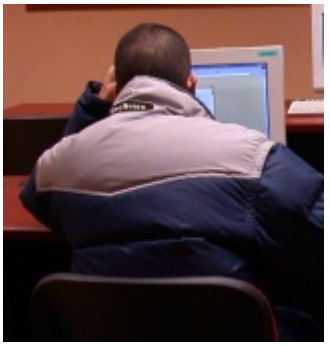
Para saber más

En el siguiente enlace encontrarás una buena explicación de las diferentes arquitecturas de Firewalls.

Arquitectura de Firewalls

3.- Proxy.

Caso Práctico



INTEF (CC BY-NC-SA)

Iván llama a Juan porque acaba de leer el correo del "Instituto de Organización y Negocios" en el que explica que están sin conexión a Internet, tienen 10 aulas con 15 ordenadores en cada aula. Todas ellas con topología de estrella conectadas a un switch y los switch a su vez en árbol al switch central, que es el que tiene la salida a Internet.

- Hola Juan, ¿dónde estás que no tienes cobertura?

- Estoy en el instituto que está cerca de la rotonda, ese que tenía problemas de ancho de banda. Ya sabes que está en la periferia de la ciudad e incluso la cobertura a veces deja mucho que desear –responde Juan.

- ¡Ah!, ahora recuerdo que llamaron porque en cuanto el alumnado ha vuelto a asistir a clase, Internet ha dejado de funcionar –menciona Iván.

- Sí, es un caso de ancho de banda, al menos eso parece –valora Juan.

- ¿De cuántos ordenadores estamos hablando? –pregunta Iván.

- Unos ciento cincuenta, el problema es que todos los alumnos y alumnas miran su correo, descargan vídeos, en fin, que no hay control, todo el mundo navega por donde quiere –indica Juan.

- Ya, ya veo, y no hay ancho de banda para todos, pues allí no tienen muchos megas de bajada –valora Iván.

- Exacto, poco ancho de banda para mucha gente –concluye Juan.

Ya hemos visto cómo el cortafuegos añade seguridad a la red controlando los accesos desde el exterior, pero ¿y si se te plantea el problema desde el interior? Muchas veces necesitarás controlar también el tráfico desde la red o intranet hacia el exterior o Internet, bueno, pues eso es justo la función de un PROXY. Así añades seguridad a la empresa, pues puedes controlar cuál es el tráfico permitido.

Debes conocer

Es interesante que veas esta presentación que explica, entre otras cosas, qué es y para qué sirve un PROXY.

00:00 00:43

Descripción textual del vídeo

El **PROXY es un intermediario** que recibe las peticiones de recursos de la red de equipos clientes y las gestiona en la red global, **encargándose de responder** a estas **peticiones**. Así, por el PROXY está circulando todo el tráfico desde tu empresa hacia la red externa o Internet. Por lo que puedes establecer unas reglas en el PROXY para que no resuelva aquellas peticiones que no cumplen las reglas establecidas. Lo más habitual es el PROXY web, que sirve para interceptar las conexiones con la web y puede ser **útil para incrementar la seguridad, rapidez de navegación o anonimato.**

INTEF (CC BY-NC-SA)

Otro caso típico de uso de un PROXY es para navegar anónimamente. Al ser el PROXY el que accede al servidor web, el PROXY sabe quién ha hecho la petición dentro, pero puede decirlo o no, es decir, el PROXY sabe quién es el usuario que lo está utilizando. El servidor web puede entonces haber recibido la petición desde la IP del PROXY, y piensa que el usuario que lo accede es el propio PROXY, en lugar del usuario real que hay detrás del PROXY. Hay proxies anónimos que **NO** informan de quién realiza las peticiones y los hay que sí informan del usuario real que está conectado a través del él.

Entonces cuando instales un PROXY tienen que tener **en cuenta sus desventajas**, por ejemplo, que los usuarios reciban información no actualizada o que el PROXY se sobrecargue cuando las peticiones son muy numerosas. Además, es un objetivo para los hackers que quieren atacar de forma anónima, si consiguen tomar el control de tu PROXY, atacarán desde él, en lo que se llama un **ataque anónimo**.

Autoevaluación

PROXY significa intermediario. ¿Verdadero o falso?

- ○ Verdadero.

○ Falso.

Correcto, esta era sencilla, ¿verdad?, esa es la traducción de PROXY del inglés al castellano.

Incorrecto, creo que no has entendido bien el texto, por favor, vuelve a leerlo con atención.

Solución

1. Opción correcta
2. Incorrecto

3.1.- Funcionamiento y Características.

Como ya sabes un PROXY permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el PROXY quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el PROXY añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una CACHÉ que permita **acelerar sucesivas consultas coincidentes**.

Reflexiona

PROXY significa intermediario. ¿Es ese su cometido cuando se instala en una red?

Las características más importantes de un PROXY son:

Aaronth (CC BY-NC-ND)

- Permite **definir los permisos** que tienen los usuarios de la red interna sobre los servicios, dominios, IP externas.
- Todos los usuarios de la red interna **comparten** una única dirección **IP** de forma que desde el exterior no se puede diferenciar a unos de otros.
- Puesto que todo el tráfico que circula de la red interna hacia internet y viceversa pasa por el PROXY, se puede auditar el uso que se hace de internet.
- Permite **almacenar** las páginas **recientemente** consultadas en una CACHÉ para aumentar el rendimiento de la red. Por ejemplo, la página que se almacena en la CACHÉ de un PROXY para que al recibir la petición cargue más rápido.

Ventajas.

- **Control de usuarios**: sólo el intermediario hace el trabajo real, por tanto, se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al PROXY.
- **Menos equipamiento**. Por tanto, sólo uno de los usuarios (el PROXY) ha de estar equipado para hacer el trabajo real.
- **Mejor respuesta**. Si varios clientes van a pedir el mismo recurso, el PROXY puede hacer CACHÉ: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- **Selección de la información**. El PROXY puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Pérdida de identidad**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo, cuando hay que hacer necesariamente la identificación.

Desventajas.

- **Sobrecarga**. Un PROXY ha de hacer el trabajo de muchos usuarios.
- **Intromisión**. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el PROXY. Y menos si hace de CACHÉ y guarda copias de los datos.
- **Falta de actualidad**. Si hace de CACHÉ, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores PROXY actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en CACHÉ sigue siendo la misma que la existente en el servidor remoto.
- **Problemas**. El hecho de que el PROXY represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre un emisor y un receptor (como TCP/IP).

Autoevaluación

Un PROXY puede proporcionar información no actualizada, ¿Verdadero o falso?

- ○ Verdadero.
- ○ Falso.

Correcto, creo que has entendido bien el texto, te felicito por tu trabajo.

Incorrecto, no has leído el texto con atención y por tanto no sería mala idea que volvieras a leerlo.

Solución

1. Opción correcta
2. Incorrecto

3.2.- Proxy Web y Proxy Caché.

PROXY de web o PROXY CACHÉ de web se trata de un PROXY para una aplicación específica: el acceso a la web. Aparte de la utilidad general de un PROXY, te **proporciona una CACHÉ** para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento.

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el PROXY CACHÉ recibe la petición, busca la URL resultante en su CACHÉ local. Si la encuentra, **contrasta la fecha** y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en CACHÉ la devuelve inmediatamente, **ahorrándose** de esta manera mucho **tráfico pues sólo intercambia un paquete para comprobar la versión**. Si la versión es antigua o simplemente no se encuentra en la CACHÉ, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o **actualiza una copia en su CACHÉ** para futuras peticiones.

Los *proxies* web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como ***proxies* Web**.

Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor PROXY que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su PROXY por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor PROXY ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

Ventajas:

M. Belén Álava Millán (Uso educativo nc)

- **Disminuye del Tráfico**: Al centralizarse todas las peticiones de páginas Web en el servidor PROXY y éste resolver algunas de estas peticiones, se disminuye el tráfico que desde nuestra red se solicita a Internet directamente. Por lo tanto, también los servidores de Internet recibirán menos peticiones, lo cual es una ventaja para su rendimiento.
- **Mejora el tiempo de respuesta**: El servidor PROXY crea un CACHÉ que utiliza con todas las peticiones similares, para el usuario supone una respuesta mucho más rápida de lo habitual.
- **Aumenta los Usuarios**: Al poder responder rápido puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
- **Selecciona los contenidos**: el servidor PROXY puede hacer un filtrado de páginas

o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.
- **Bloquea contenidos**: basándose en la misma función del filtrado, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies.

Desventajas:

- No actualiza. Falta de actualización de las páginas mostradas que están almacenadas en la CACHÉ.

Un diseñador o diseñadora de páginas web puede indicar en el contenido de su web que los navegadores no hagan una CACHÉ de sus páginas, pero este método no funciona habitualmente para un PROXY.

- El PROXY puede **impedir el acceso** a algunos puertos y protocolos. Esto te puede suceder si tratas de utilizar servicios **poco habituales** para los usuarios y usuarias de la red, por ejemplo FTP.
- Tendrás que configurar el PROXY para que **no almacene datos personales** y otros archivos que transgredan la norma **LODP**.

Para saber más

Muchas organizaciones usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de CACHÉ. Puedes ampliar esta información en:

Más tipos de PROXY

3.3.- Proxy en Windows.

Ahora te vas a poner manos a la obra y vas a instalar un PROXY en tu equipo, primeramente, sobre un sistema operativo Windows.

Debes conocer

Lo puedes obtener, en su versión de prueba en la página web de wingate. Hemos escogido este PROXY, pero podríamos haber escogido cualquier otro, pues todas las configuraciones de los PROXY son similares. La idea es que se instale en un equipo con dos tarjetas de red que hace de intermediario entre la red local e internet.

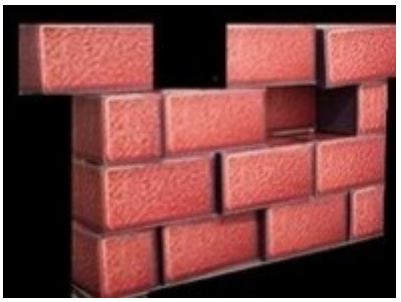
Descargar Wingate

Instalación.

M. Belén Álava Millán (Uso educativo nc)

Partimos de la red Windows que tú administras y que por tanto está funcionando con el protocolo TCP/IP. Una vez descargado el programa lo instalas en el HOST **bastión**, es decir, el ordenador que hace de intermediario entre la red de área local y la red externa o Internet.

Durante la instalación te hará algunas preguntas. Te recomiendo que no uses el DHCP, es decir, asignación de direcciones IP dinámicamente. Si tienes una intranet pequeña es mejor tener cada ordenador con una IP fija, asignada por ti "a mano", de esta forma tendrás un **control mayor** sobre tu red.



Johannes P Osterhoff (CC BY-NC)

Inicia la instalación de Wingate, y las respuestas a las diferentes pantallas del instalador son sencillas, pero tienes que tener en cuenta que:

- Debes aceptar las condiciones de uso del programa.
- Escoge la opción de PROXY server.
- No uses el usuario del sistema operativo para la base de datos.
- Si tienes más de un ordenador en la red, instala ENS, de lo contrario no hace falta.
- Deja activadas las actualizaciones.

Debes conocer

En este video de la propia empresa QBik (creadora de WinGate) puedes ver el proceso de instalación de WinGate de manera rápida y sencilla.

Instalación de WinGate.

https://www.youtube.com/embed/dU_s29vY9Tk

Descripción textual del vídeo

Autoevaluación

Un PROXY es lo mismo que un cortafuegos. ¿Verdadero o falso?

- ○ Verdadero.
- ○ Falso.

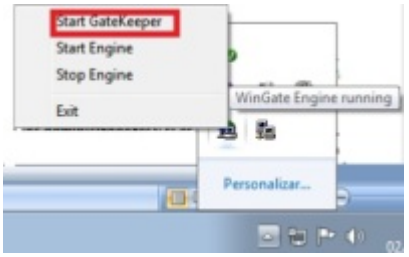
Incorrecto, pues creo que no has entendido bien el texto, por favor, vuelve a leerlo con atención.

Correcto, efectivamente, no es lo mismo. El Firewall defiende la red interna de ataques externos y el PROXY analiza y filtra el tráfico de la red interna hacia fuera.

Solución

1. Incorrecto
2. Opción correcta

3.3.1.- Proxy en Windows. Wingate.



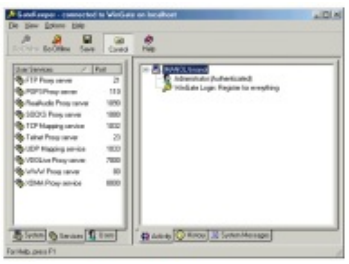
M. Belén Álava Millán (Copyright (Cita))

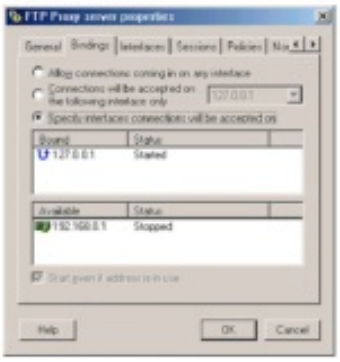
Configuración de wingate. Una vez instalado y reiniciado comprueba que en el área de notificación de Windows (los iconos que hay cerca de la hora y fecha) aparecen WINGATE Engine y WINGATE VPN. Si pulsamos el botón derecho sobre el icono WINGATE Engine, tienes la opción de iniciar el servicio de WINGATE (START engine), así nos aseguramos que está iniciado, posteriormente abrimos GATEKEEPER (o WinGate Management, según la versión), que es el centro de gestión del PROXY. Lo podemos hacer con el botón derecho sobre WINGATE Engine, y seleccionar WinGate Management, o siguiendo la ruta: Inicio → Todos los programas → WinGATE → WinGate Management

El usuario por defecto es "**administrator**" con la **contraseña en blanco**. Tras pulsar en OK, te pide una contraseña nueva para el administrador. (Recuerda crear una contraseña segura).

Tabla con los pasos de configuración de WINGATE:

Configuración de WINGATE.

 M. Belén Álava Millán (Copyright (Cita))	Ahora vas a ver cómo crear y configurar los servicios, para ello vas a la pestaña "Services" que (originalmente) aparecerá en blanco.
 M. Belén Álava Millán (Copyright (Cita))	Pulsamos con el botón derecho en cualquier parte de la pantalla izquierda (Services) y te saldrá un menú para crear nuevos servicios "New Service" con todos los servicios disponibles.
 M. Belén Álava Millán (Copyright (Cita))	Vas creando uno a uno todos los servicios hasta que la pantalla de la izquierda nos quede como la que aparece a la izquierda. Una vez creados pulsamos el icono del diskette, para guardar los cambios.

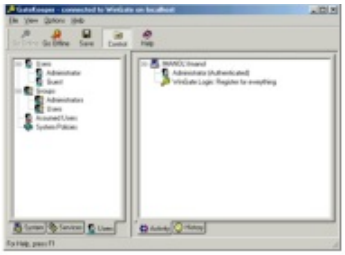


M. Belén Álava Millán (Copyright (Cita))

Ahora comprobamos que los protocolos estén activos, eligiendo uno a uno los servicios, mediante un doble clic y nos aparecerá una pantalla como esta:

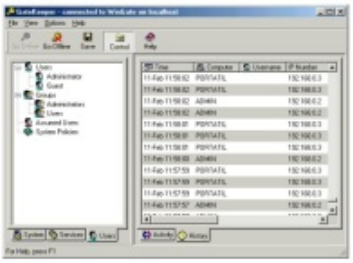
M. Belén Álava Millán (Copyright (Cita))

Vamos a la pestaña "Bindings" y comprobamos que ambas interfaces de conexión (127.0.0.1 y 192.168.0.1) estén situadas en la ventana superior. Si una aparece en la ventana inferior, hacemos doble clic sobre ella y pasa automáticamente a la ventana superior. Hay que comprobar todos los Bindings de todos los protocolos.



M. Belén Álava Millán (Copyright (Cita))

Cuando quede así, ya tenemos los servicios activados y con las interfaces activadas. Los puertos de conexión, los da el programa por defecto.
Las pantallas "System" y "Users" se dejan como vienen por defecto. En pantalla "Activity", se pueden ver las actividades de otros PC conectados y en "History", el histórico de conexiones.



M. Belén Álava Millán (Copyright (Cita))

A la derecha se pueden ver los distintos clientes conectados con sus IP y su nombre en la red..

El Gatekeeper también se puede activar mediante el icono que nos aparece en la barra de tareas, mediante un doble clic en él. Ya tenemos el Wingate configurado y residente en el arranque de Windows. A veces, tenemos que tener activada nuestra conexión en el PC principal para que puedan conectarse los otros, aunque al iniciar la sesión en cualquier cliente, se suele conectar automáticamente y se desconecta tras 3 minutos de inactividad

(de haber cerrado el Explorer) del cliente.

Debes conocer

En estos vídeos puedes ver cómo se configuran los navegadores para que utilicen PROXY:

Configurar el PROXY en los navegadores.

https://www.youtube.com/embed/eOb0_AY45vE

Descripción textual del vídeo

https://www.youtube.com/embed/N2_IG0ZrzHo

Descripción textual del vídeo

Autoevaluación

Un PROXY puede crear sus propios usuarios. ¿Verdadero o falso?

- ○ Verdadero.
- ○ Falso.

Exacto, podemos crear los usuarios en el software del PROXY.

Incorrecto, conviene que vuelvas a leer los apuntes para entender cómo se configura un PROXY.

Solución

1. Opción correcta
2. Incorrecto

3.3.2.- Proxy en Windows. Free Proxy.

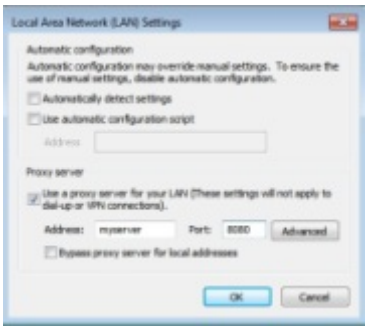
FreePROXY es un software gratuito, se trata de un PROXY que permite que una sola conexión a Internet compartida por otros ordenadores en una red sea controlada por él. Visto de otro modo, FreePROXY es un mecanismo para proporcionar acceso controlado a Internet. Los controles pueden ser por filtros avanzados de seguridad, por nombre de usuario y contraseña de verificación o por filtrado de IP.

El servidor web, aunque integrado en FreePROXY, se llama FreeWeb. FreePROXY puede funcionar como un servidor web, y como un PROXY.

Si quieres comenzar a usar FreePROXY debes ejecutarle en uno de los siguientes sistemas operativos: Windows 98, Windows NT con SP4, Windows 2000 Profesional, Windows 2000 Server, Windows XP Pro, Windows XP Home, o Windows 2003 server.

- Después de instalarlo ejecuta FreePROXY Control Centre, que estará en la ruta: Inicio → Programas → FreePROXY → FreePROXY Control Centre.
- El Control Centre cargará **Default.cfg** automáticamente la primera vez que se ejecute.
- Selecciona **Start/Stop** del menú de FreePROXY y selecciona START FreePROXY como servicio (SERVICE).

M. Belén Álava Millán (Uso educativo nc)



M. Belén Álava Millán (Uso educativo nc)

Esta acción instalará FreePROXY como un servicio y estará listo para su uso

en otros ordenadores de tu red. Siempre que cambies la configuración de FreePROXY, debes parar e iniciar el programa.

Cada navegador cliente debería ser actualizado para que utilice el PROXY en el Puerto 8080 en la IP del ordenador donde se ha instalado FreePROXY. Por ejemplo, si el nombre del ordenador conectado a Internet es MYSERVER y tú has instalado FreePROXY como se describe arriba, entonces, tu deberías cambiar la configuración en Internet Explorer en la ruta: Herramientas → opciones de internet → Conexiones → opciones LAN. Si es en Mozilla Firefox: Firefox → opciones → opciones → Avanzado → Red.

M. Belén Álava Millán (Uso educativo nc)

Permisos de acceso.

El acceso puede ser "**prohibido**"(forbid) o "**permitido**"(grant). Si no se especifica el acceso a un recurso, FreePROXY se supone que el acceso al recurso está permitido para todos los usuarios. El uso de este, sólo es necesario especificar los recursos que están específicamente prohibidos. Se concede el acceso o se deniega en el orden en que se presentan las reglas.

Ejemplo de reglas que se pueden configurar en FreePROXY:

Reglas que se pueden configurar en FreePROXY.

Ejemplo.	Explicación
Grant *.URLBUENA.*. Forbid *.URLBUENA.*	El acceso a www.URLBUENA.com siempre se concederá este permiso como se encontró en primer lugar. Para que sólo permita el acceso a determinadas direcciones URL que tendrían que estar en la lista.
Permiso acondicionado con una restricción de tiempo (A partir de versión 3.8 se puede conectar un calendario a una autorización de recursos. Si lo haces, puede especificar cuándo el permiso de los recursos es eficaz.)	
Grant *.URLBUENA.* Calendario: Todos los días, usuarios: DailyUsers. Grant *.URLBUENA.* Calendario: fin de semana, usuarios: WeekendUsers. Forbid *	En el ejemplo anterior, en el supuesto de que el calendario especifica **diario** de lunes a viernes y **fin de semana** al fin de semana, los usuarios diarios solamente tendrán acceso a una URL durante la semana y los usuarios de fin de semana sólo los fines de semana.

Reflexiona

El orden en que se sitúen las reglas en el PROXY será definitivo para la actuación de las mismas. ¿Crees que puede haber órdenes contradictorias

consecutivas?

3.4.- Proxy en Linux.

SQUID es un software que cachea datos de internet. Lo realiza guardando las peticiones que los usuarios realizan. En otras palabras, si quieres descargar una página web, pides a SQUID que obtenga dicha página. SQUID se conecta al servidor remoto y pide la página. Después te reenvía la petición, pero al mismo tiempo mantiene una copia. La próxima vez que desees dicha página, SQUID simplemente la leerá del disco y te la transferirá de forma instantánea. SQUID soporta actualmente los protocolos HTTP, FTP, GOPHER, SSL y WHAIS. No soporta otros protocolos como RealAudio, Streams y similares.

Stocklib (Uso educativo nc)

Conceptos sobre CACHÉ.

Dentro del campo de las CACHÉ, es necesario que tengas en cuenta de qué forma puede ser útil el realizar CACHÉ y que objetos deben ser cacheados. Es totalmente **inapropiado cachear**, por ejemplo, números de tarjetas de crédito, los resultados de un script ejecutado remotamente, sitios que cambian muy a menudo (como www.elprincipalperiodico.com) o incluso sitios que no desean ser cacheados.

SQUID cumple estos requerimientos, siempre y cuando los sitios remotos sigan los estándares.

Los scripts ejecutables cgi-bin no son cacheados, las páginas que indican en las cabeceras periodos de caducidad son tenidos en cuenta, y es posible especificar con reglas extra lo que se debe y lo que no se debe cachear, y por cuánto tiempo.

Para determinar la utilidad y rendimiento de la CACHÉ, es necesario tener en cuenta diversos factores. Utilizando una CACHÉ **pequeña** (un par de gigas) se obtienen unos resultados altos (cercanos al **25**%). Este espacio cachea los sitios más habituales. Si se **dobla el espacio** en disco, **no se dobla este porcentaje**. Esto es debido a que se está intentando capturar el resto de peticiones, que con frecuencia son poco utilizadas. Una CACHÉ grande (por encima de 20 Gb) probablemente no llegará al 50%, a no ser que las páginas se mantengan durante mucho tiempo.

Squid es un software libre y cuenta con un sitio web oficial donde puedes realizar la descarga:

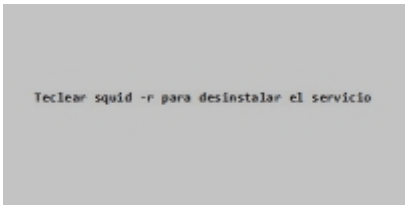
Squid

Tras haber descargado el archivo, debemos descomprimirlo a una carpeta con privilegios de escritura para todos los usuarios.

Instalación de SQUID: editar el fichero de configuración SQUID.conf.

Mª Belén Álava Millán (Uso educativo nc)

Desinstalación de SQUID.



Mª Belén Álava Millán (Uso educativo nc)

SQUID funciona como un demonio del sistema operativo.

Para saber más

En este enlace podrás aprender a configurar SQUID como un PROXY transparente:

SQUID cómo un PROXY transparente (0.19 MB)

Autoevaluación

Cuando estamos hablando del PROXY SQUID ¿Qué es un objeto?

- El rendimiento de la CACHÉ.
- La utilidad y el rendimiento de la CACHÉ.
- La CACHÉ.
- Una página web guardada en la CACHÉ.

No es correcta porque es el número de páginas que tiene almacenadas frente al total de páginas solicitadas. Es decir, cuántas páginas se han vuelto a consultar y estaban almacenadas.

Incorrecta, objeto es singular, lee de nuevo el texto.

No es la respuesta correcta porque la CACHÉ de SQUID no tiene otro nombre.

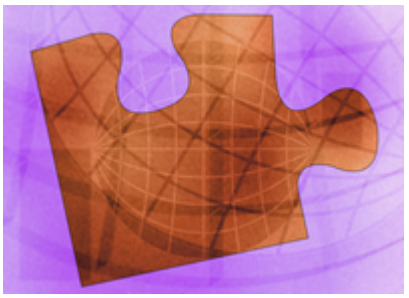
Muy bien. Has captado la idea.

Solución

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

3.4.1.- Proxy en Linux. Listas de Control de acceso.

Las listas de control de acceso o ACL (Inglés: Access Control List) es el punto que más problemas causa en la configuración de SQUID.



Stocklib (Uso educativo nc)

Permitir o denegar el acceso a la CACHÉ es sólo una de las funciones del ACL.

El ACL es usado también para las jerarquías de CACHÉ. Por tanto, primero se define una lista ACL y después se permite o deniega el acceso a una función de la CACHÉ. En la mayoría de las ocasiones, esta función es "**http_access**", que **permite o deniega** a un navegador el acceso a SQUID. Usaremos esta función como un ejemplo para los casos siguientes (como "icp_access").

SQUID lee las directivas de arriba a abajo, para determinar qué regla aplicar, e incluso determinar si debe permitir o denegar el acceso. Por tanto, si dispone de una clase C de direcciones, y quiere permitir sólo a esas máquinas acceder a la CACHÉ, utilizaremos estas directivas (asumiendo que la clase C 192.168.16.0 entera tendrá acceso).

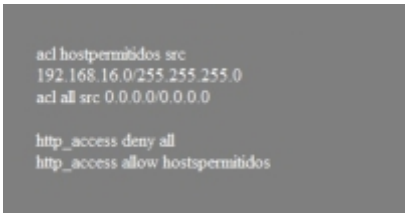
```
acl hostpermitidos src
192.168.16.0/255.255.255.0
acl all src 0.0.0.0/0.0.0.0

http_access allow hostpermitidos
http_access deny all
```

Mª Belén Álava Millán (Uso educativo nc)

La opción "**src**" de la primera línea es una de las opciones que se puede utilizar para decidir **en qué lista ACL** el usuario está incluido. Incluso es posible utilizar aspectos como el tiempo actual, o el sitio al que se dirigen. Para más opciones, mira el fichero por defecto de SQUID (**SQUID.conf.default**).

Si un usuario del rango 192.168.16.5 se conecta a SQUID usando TCP para solicitar una URL, SQUID leerá las líneas referentes a "http_access" (ya que es una conexión TCP y el cliente va a utilizar el método HTTP para solicitar el objeto). La lectura se realiza de **arriba hacia abajo**, y se **para en la primera coincidencia** para decidir si permite o deniega la petición. En el ejemplo anterior, SQUID leerá que la primera línea de "http_access" permite el acceso a 192.168.16.5, puesto que está en la lista de HOSTpermitidos, y procederá a aplicarla. En este caso, permitirá el acceso y ejecutará la petición.

Vamos a tener en cuenta el siguiente ejemplo:



En este caso **no funcionará**, ya que SQUID aplicará la primera coincidencia (la primera línea) y denegará el acceso.

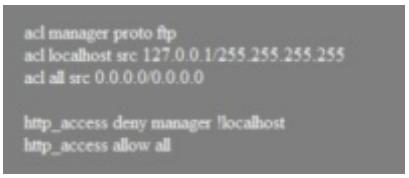
Para saber más

En esta página web puedes encontrar información sobre cómo configurar un Servidor Proxy con Squid en Debian 10:

Configuración de un servidor Proxy con Squid

3.4.2.- Proxy en Linux. Opciones avanzadas.

En el fichero de configuración encontramos otros parámetros:



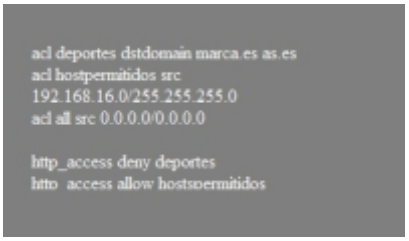
El campo "**proto**" de la primera línea se refiere que el ACL bloquea un protocolo específico, en este caso el protocolo "ftp". Puede utilizarse también otro protocolo, como "http" o "Cache_object". "CACHÉ_object" es un protocolo propio de SQUID que retorna información acerca de cómo está configurada la CACHÉ, o cómo se está ejecutando. Está dentro de la sección "http_access" ya que se trata de una petición HTTP a SQUID, pero en lugar de conectar a un servidor remoto, es SQUID quien gestiona la información.

El ejemplo anterior indica que si SQUID recibe una petición intentando utilizar el protocolo "ftp" (definido en el ACL de manager), debe denegarla, a no ser que provenga de localHOST. De este modo, un programa FT que esté ejecutándose en el servidor puede obtener conexiones internas, pero no externas. Recuerde que el carácter "!" significa NO, por lo que estamos diciendo "denegar manager NO localHOST".

ACL basados en direcciones de destino.

Existe un caso frecuente, consistente en prohibir el acceso a una lista de sitios que consideramos como "inapropiados". SQUID no está optimizado para gestionar una larga lista de sitios, pero puede gestionar un número concreto de sitios sin problemas.

Este ejemplo indica que las URL *marca.es* as.es serán denegadas, ya que así lo especifica la primera línea de la directiva "http_access deny deportes". Si se piden otras URL, lógicamente la primera línea no es aplicable, y SQUID pasa a considerar la segunda y tercera. Por tanto, si el cliente se conecta dentro del rango permitido obtendrá conexión FTP pero si lo hace desde cualquier otra IP NO obtendrá conexión.



Para saber más

SQUID pueden ser compilado en todas las distribuciones de Unix. Webmin apoya y trabaja casi idénticamente en todas ellas. Esto significa que el módulo Webmin de la interfaz de usuario es el mismo a través de los sistemas operativos, a excepción de las rutas por defecto que utiliza para el SQUID, tanto en el programa como en ficheros de configuración. En el siguiente enlace verás cómo se configuran las ACL con ayuda de Webmin.

ACL de SQUID con Webmin

Autoevaluación

Observa la configuración del SQUID siguiente:

"acl juegos dstdomain minijuegos.com juegos.com acl HOSTpermitidos src 192.168.116.0/255.255.255.0 acl all src 0.0.0.0/0.0.0.0 http_access allow juegos http_access deny HOSTspermitidos http_access deny all"
¿Será la petición del ordenador 192.168.116.0 rechazada si quiere ver la página www.google.es?:

- ○ Verdadero.
- ○ Falso.

Correcto, esta petición será rechazada porque no se conecta a ninguna página web de las permitidas en juegos.

Incorrecto, comprueba de nuevo las reglas.

Solución

1. Opción correcta
2. Incorrecto

4.- IDS Sistemas Detectores de Intrusos.

Caso Práctico

Juan tiene un amigo en la universidad, es un verdadero forofo de Internet y la informática en general, ha instalado en su casa un servidor, y le pide a Juan que se lo "asegure", es decir, que no quiere que su servidor sea atacado y si lo es quiere ser el primero en saberlo.

Stockbyte (Uso educativo nc)

Juan habla con Alberto, su amigo de la Universidad.

- Oye Juan, ya tengo instalado el servidor, puedes poner tu blog cuando quieras.

- Pero Alberto, ¿has tomado todas las medidas que te dije para que sea un servidor seguro?

- ¡Oh!, vamos Juan, ¿no crees que te estás pasando? Acabo de estrenar mi servidor y ya crees que va a ser atacado, igual es que estás trabajando últimamente mucho en temas de seguridad y ya ves peligros en todas partes.

- Mira, Alberto, a finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones. El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow).

Juan se toma un respiro y continúa con su exposición.

-Los problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados. Así, por ejemplo, un problema de seguridad del grupo rojo es un equipo que tiene el servicio de FTP anónimo mal configurado. Los problemas de seguridad del grupo amarillo son menos serios pero también reseñables. Implican que el problema detectado no compromete inmediatamente al sistema pero puede causarle serios daños o bien, que es necesario realizar tests más intrusivos para determinar si existe o no un problema del grupo rojo.

- Ya, Juan ¿Y a dónde quieres llegar?

- Pues que de los resultados se deduce que cerca de los dos tercios de los sistemas analizados tenían serios problemas de seguridad y que casi un

tercio de ellos podían ser atacados con un mínimo esfuerzo.

- Bueno, pero eso fue en 1996, hoy en día, todos los sistemas operativos se han puesto las pilas en seguridad y con eso ya vale.

- Ya, ya te veo muy optimista, desde entonces y hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

- Bueno, quizás tengas razón, pero ¿a quién va a interesarle mi servidor VACIO o con tu blog?

- El problema es que buscan lugares fácilmente atacables, pues el atacante puede ser cualquier adolescente de 15 años (Script Kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús. Este adolescente, sólo por probar, es capaz de dejar fuera de servicio tu servidor, simplemente siguiendo las instrucciones que acompañan la herramienta, y echar por tierra todas las horas que has dedicado a ponerlo en marcha. ¿qué te parece?

- Y, ¿Cómo me defiendo? –preguntó Alberto.

- Contrariamente a lo que probablemente piensas, los sistemas son difíciles de penetrar si están bien administrados y configurados. Ocasionalmente, los defectos propios de la arquitectura de los sistemas proporciona un fácil acceso, pero esto puede ser, en la mayoría de los casos, subsanado aplicando las soluciones que los fabricantes de sistemas operativos ponen a tú disposición. Para defenderte piensa que la mayoría de los ataques se fundamentan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo. La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

- ¿Es eso todo?

- No, no, aún tendrás que instalar más programas que protejan tu equipo.

- ¡Huf!, espero que no me cuentes ya más y vengas a mi casa a instalarlos tú mismo.

- Venga, voy para allá.

Reflexiona

Los administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. No sólo usan nuevas herramientas de seguridad disponibles en

el mercado sino que además se informan en los documentos explicativos sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por organizaciones como el CERT.

4.1.- Sistemas Detectores de Intrusos.

Alguna vez te habrás preguntado si es posible observar qué está ocurriendo en el ordenador, algún programa o software específico que vigile el sistema, y que nos avise si alguien está atacando tu ordenador. Pues bien, esta es la filosofía de los IDS, son mecanismos de defensa ante ataques.

Debes conocer

Es interesante que veas esta presentación que explica, entre otras cosas, qué es y para qué sirve un IDS:

Qué es un IDS.

00:00 00:44

Descripción textual del vídeo

Hasta ahora has estado aplicando defensas a los controles de acceso como la solución de seguridad.: Firewall, control de listas de acceso, etc., realmente la defensa debe de ser más compleja para que podamos detectar los ataques que hayan sobrepasado las barreras que el sistema tenía para defenderse.

Pilar Acero López (CC BY-NC-SA)

Por ejemplo, si has instalado un Firewall con una política que deje acceder al puerto 80 de nuestros servidores web a cualquier máquina de Internet; ese cortafuego sólo comprobará el **puerto de destino** de las tramas entrantes, pero **no la naturaleza** de esas tramas. Por tanto, si le llegan 3000 tramas iguales con destino al puerto 80 simplemente las deja pasar, alguna de esas tramas que han alcanzado el servidor por llevar el puerto 80 de destino podrían ser un ataque o un hacker intentando acceder a nuestro sistema de ficheros para encontrar el archivo de contraseñas aprovechando un bug del servidor web.

Desde un hacker externo a un usuario autorizado que intenta obtener privilegios que no le corresponden en un sistema, nuestro entorno de trabajo no va a estar **nunca a salvo** de intrusiones.

Intrusión es un conjunto de acciones que intentan **comprometer la integridad**, confidencialidad o disponibilidad de un recurso; analizando esta definición, podemos darnos cuenta de que una intrusión no tiene por qué consistir en un acceso no autorizado a una máquina, **también puede ser una denegación de servicio**. Al sistema utilizado para detectar las intrusiones o los intentos de intrusión se les denomina **sistemas de detección de intrusos** (IDS, Intrusion Detection Systems). Ningún sistema informático puede considerarse completamente seguro, pero incluso aunque nadie consiga violar nuestra políticas de seguridad, los sistemas de detección de intrusos se encargarán de mostrarnos todos los intentos, no dejándonos caer en ninguna **falsa sensación de seguridad**: si somos conscientes de que a diario hay gente que trata de romper nuestros sistemas, no caeremos en la tentación de pensar que nuestras máquinas estás seguras porque nadie sabe de su existencia o porque no son interesantes para un pirata.

Autoevaluación

Qué es un IDS (varias respuestas correctas):

- ☐ Un sistema que detecta capturas o mal uso de un ordenador en la red.
- ☐ Un detector de actividad inadecuada.
- ☐ Un detector de intentos de conectarse a un servicio autorizado.
- ☐ Un detector de usuarios para la red.

Mostrar retroalimentación

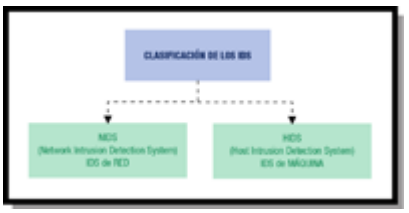
Solución

1. Correcto

2. Correcto
3. Incorrecto
4. Incorrecto

4.2.- Clasificación de Sistemas IDS.

Cuando trates de clasificar un IDS tendrás antes de nada escoger un criterio, pues si lo haces en función de qué sistemas vigilan, podrían ser IDS de RED o de HOST, pero si lo haces en función de qué técnicas emplean, es decir, de cómo vigilan podrán ser detectores de **ANOMALÍAS** ó detectores de **USO INDEBIDO**.



Ministerio de Educación (Uso educativo nc)

IDS de red.

Un IDS de red monitoriza los paquetes que circulan por nuestra red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella. El IDS puede situarse en cualquiera de los HOSTs o en un elemento que analice todo el tráfico. A estos elementos se les suele llamar "sensores".

IDS de HOST.

Si tienes sólo un dominio de colisión habrás instalado un IDS de red, pero si tienes solamente un ordenador sensible, por ejemplo el servidor, será un IDS de HOST el que debes instalar en esa máquina para que proteja ese sitio informático. En este caso la forma de actuar del IDS de HOST es muy parecida a la de un antivirus residente, pues el IDS trabaja en la "**sombra**" y de forma silenciosa buscando patrones que puedan denotar un intento de intrusión y te alerta cuando detecta un intento de intrusión. Cuando esto ocurre tú irás arbitrando las medidas oportunas en cada uno de los casos, y la próxima vez que ocurra, el IDS de HOST tomará las medidas oportunas en cada caso ya estudiado. Algunas de estas medidas ya son conocidas por el propio IDS de HOST.

La segunda gran clasificación de los IDS se realiza en función de cómo actúan estos sistemas. Actualmente existen **dos** grandes técnicas de detección de intrusos: las que **detectan anomalías** y las que **detectan usos indebidos**.

1. **Detección de anomalías.**
   Estos sistemas clasifican como anomalía cualquier intento de intrusión en nuestro sistema, por lo que lo importante es establecer cuál es el comportamiento habitual del sistema para detectar patrones que estadísticamente se desvíen del patrón. Cuando el **comportamiento se desvíe de la media** de una forma excesiva podremos afirmar que hay una **intrusión**.

Ministerio de Educación (Uso educativo nc)

   Lo difícil es que diseñes un buen patrón de comportamiento, pues la complejidad suele ser alta. Y una vez establecido, buscar qué desviación se considera un ataque y cuál no. El objetivo que tienes que buscar es no obtener muchos **falsos positivos**, pero que no se pasen por alto los ataque. No es una tarea fácil.

2. **Detección de usos indebidos.**
   El funcionamiento de los IDS de detección de usos indebidos presupone que podemos establecer patrones para los diferentes ataques conocidos y alguna de sus variaciones. Mientras que la detección de anomalías **conoce lo normal y detecta lo inusual**, en este caso se comparan los comportamientos de todos los ataques

conocidos con lo que está ocurriendo. En este caso debes de tener la base de datos siempre actualizada y aún así, si un ataque es totalmente nuevo, no podrá detectarlo hasta que no se incorpore a la base de datos.

Para saber más

Tripwire es una herramienta de seguridad que permite monitorizar y alertar de cambios no deseados en los ficheros de un sistema, en el siguiente enlace podrás ver sus características:

Tripwire: un HIDS

Autoevaluación

En los IDS de detección de usos indebidos lo más crítico es tener la base de datos actualizada. ¿Verdadero o Falso?

- Verdadero.
- Falso.

No es correcto, en este tipo de IDS se prima el estudio de los ataques anteriores para detectar un ataque.

Correcto, es crítica la creación del patrón.

Solución

1. Incorrecto
2. Opción correcta

4.3.- Arquitectura de Sistemas IDS.

Como en el caso de los sistemas con cortafuegos, cuando tengas que implantar un IDS optarás probablemente por una combinación de las categorías antes explicadas.

Pandafrance (CC BY-NC-ND)

Es frecuente que haya varias subredes en la empresa y por tanto te encuentres con que la situación de los sensores debería de ser en todas estas subredes. Además, si la red está segmentada también tendrás que colocar un sensor en cada segmento de ésta. Así, tendrás que tener en cuenta todos los factores de la **topología** de la red para colocar los sensores.

Otra decisión importante que debes tomar, es el tipo de respuesta que el IDS dará ante una detección de ataque. Quizá te gustaría que el IDS se pudiera comunicar con el Firewall para indicarle las nuevas reglas que debe aplicar para evitar este ataque que se está produciendo. Por ejemplo, si el IDS detecta un intento de ataque al servidor web desde la dirección IP w.x.y.z, el IDS le dirá al Firewall que añada una regla que deniegue todo el tráfico desde esa dirección hacia nuestra red.

Para saber más

Snort es un Sistema de detección de intrusiones basado en red que permite detectar ataques o barridos de puertos, registrándolos y generando alertas. En el siguiente enlace podrás ver los diferentes modos de uso que SNORT tiene:

Snort, un NIDS (NIDS)

Una vez que hayas colocado los sensores de red tienes que pensar que éstos no son infalibles, pues han podido diseñar métodos para evadirlos, o bien se trate de un ataque totalmente nuevo que no detecten, por lo que ahora te planteas fortalecer el IDS instalado con otro tipo de IDS. Como lo que más te preocupa son los ordenadores o servidores que tienen instalados algún tipo de servicio, probablemente sea un decisión acertada vigilar qué ocurre en estos equipos. Por lo que **decides instalar HIDS** en estos equipos tan sensibles. Estos HIDS se encargarán de examinar los log del sistema y de las aplicaciones más importantes **buscando trazas de intrusión** y también se ocupará de comprobar la integridad de los archivos esenciales del sistema, con el fin de **prever una modificación** no autorizada de los mismos.

Robin Hutton (CC BY-NC-ND)

Ejemplos de IDS.

Snort es un sniffer capaz de actuar como sistema de detección de intrusos en redes de tráfico moderado; su facilidad de configuración y su adaptabilidad, funciona en sistemas UNIX y Windows, y además se trata de un sistema no muy caro. Es una buena herramienta y es menos caro que Network Flight Recorder o ISS RealSecure, aunque estos últimos son más potentes.

Tripwire es una **comprobador** de integridad para ficheros y directorios de sistemas UNIX: compara un conjunto de estos objetos con la información sobre los mismos almacenada en la base de datos, y, alerta al administrador en caso de que **algo haya cambiado**. La idea es simple: Creas un fichero resumen de cada fichero o directorio importante para nuestra seguridad nada más instalar el programa. Almacenas esos resúmenes en un medio seguro, de forma que si alguno de los ficheros es modificado, por ejemplo por una versión infectada del mismo fichero, o añadiendo una contraseña al fichero de contraseñas, Tripware lo detectará y te avisará la próxima vez que realices la comprobación. Tripware utiliza MD5 y CRC-32 entre otras funciones de hash para generar los resúmenes, y como recuerdas, estos hash son imposibles de generar iguales si los ficheros son diferentes.

Reflexiona

Los sistemas IDS son un elemento más en la implementación de una política de seguridad. No se trata de una solución definitiva y es importante que no tengas una falsa sensación de seguridad solo por el hecho de instalar un IDS en el sistema. El peligro sigue existiendo y es necesaria la revisión continua de la política de seguridad para adecuarla a los cambios. Tú sistema seguirá siendo tan seguro como lo sea el **punto más débil del mismo**.