Seguridad y Alta Disponibilidad

INDICE

Servidores proxy:

1.SERVIDORES PROXY:

Es un programa o dispositivo que realiza una acción en representación de otro.Una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A.

Su finalidad más habitual es la de servidor proxy, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

TIPOS DE «PROXY».

Proxy de web / Proxy cache de web

Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidosdescargados, 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.

Ventajas

-**Ahorro de Tráfico:** las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.

-**Velocidad en Tiempo de respuesta:** el servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.

-**Demanda a Usuarios:** puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.

-**Filtrado de 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.

-**Modificación de contenidos:** basándose en la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado

para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Desventajas

-Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.

-Un diseñador 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 hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.

-Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

Proxies transparentes:

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración.

Una ventaja de tal es que se puede usar para redes de empresa.Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP).Reverse Proxy / Proxy inversoUn reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.

-Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).

-Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).

-Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

Proxy NAT (Network Address Translation) / Enmascaramiento

La traducción de direcciones de red (NAT, Network Address Translation)

también es conocida como enmascaramiento de IPs. Es una técnica mediante

la cual las direcciones fuente o destino de los paquetes IP son reescritas,

sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy. La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador..

Proxy abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS

o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido.

Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

En el caso de Ajax, por seguridad sólo se permite acceder al mismo dominio origen de la página web que realiza la petición. Si se necesita acceder a otros servicios localizados en otros dominios, se instala un Cross-Domain proxy en el dominio origen que recibe las peticiones ajax y las reenvia a los dominios externos.

En el caso de flash, también han solucionado creando la revisión de archivos xml de Cross-Domain, que permiten o no el acceso a ese dominio o subdominio.

B. CARACTERÍSTICAS.

Ventajas

En general (no sólo en informática), los proxies hacen posible:

- **Control:** 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.

-**Ahorro**. Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.

Velocidad. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer ca ché: 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.

-Filtrado. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

-Modificación. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

-**Anonimato.** Si todos lo 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

En general (no sólo en informática), el uso de un intermediario puede provocar:

-Abuso. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.-Carga. 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.

-Incoherencia. 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 cache sigue siendo la misma que la existente en el servidor remoto.

-Irregularidad. 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 1 emisor y 1 receptor (como TCP/IP).

C.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.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

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. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA.

Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

D. INSTALACIÓN DE SERVIDORES «PROXY».

Instalar el proxy

Para instalar Squid escribe en un terminal:

sudo aptitude install squid

2. Configurar el proxy

La configuración de Squid se hace editando el archivo /etc/squid/squid.conf

Para editar este archivo, presiona Alt+F2 y:

gksu gedit /etc/squid/squid.conf

2.1 Nombrar el proxy

Squid necesita conocer el nombre de la máquina. Para ello, ubica la línea visible_hostname.

Por ejemplo, si la máquina se llama “ubuntu”, pon: visible_hostname Ubuntu

2.2 Elegir el puerto

Por defecto, el puerto de escucha del servidor proxy será 3128. Para elegir otro puerto, ubica la línea:

http_port 3128

Y cambia el número de puerto, por ejemplo:

http_port 3177

2.3 Elegir la interfaz

Por defecto el servidor proxy escucha por todas las interfaces. Por razones de seguridad, sólo debes hacer que escuche en tu red local.

Por ejemplo si la tarjeta de red ligada a tu LAN tiene el IP 10.0.0.1, modifica la

línea a:

http_port 10.0.0.1:3177

2.4 Definir los derechos de acceso

Por defecto, nadie está autorizado a conectarse al servidor proxy, excepto tu

máquina.

Entonces hay que crear una lista de autorización.

Por ejemplo vamos a definir un grupo que abarca toda la red local.

Ubica la línea del archivo que comienza por acl localhost...

Al final de la sección, agrega:

acl lanhome src 10.0.0.0/255.255.255.0

(lanhome es un nombre arbitrario que hemos elegido)

2.6 Autorizar los puertos no estándar

Por defecto, Squid sólo autoriza el trafico HTTP en algunos puertos (80, etc.)

Esto puede ocasionar problemas a algunas páginas web que utilizan otros

puertos .

Para evitar que lo bloquee, encuentra la línea:

http_access deny !Safe_ports

Y agrega un comentario:

#http_access deny !Safe_ports

3. Iniciar el proxy

(Re)inicia el proxy para que tome en cuenta la nueva configuración que

acabamos de realizar.

Escribe:

sudo /etc/init.d/squid restart

INSTALACIÓN Y CONFIGURACIÓN DE CLIENTES «PROXY».

Si queremos conectar varios equipos a Internet a través de uno de ellos, sin necesidad de utilizar un router lo podemos hacer utilizando un Proxy. Vamos a ver con un ejemplo cómo configurar varios equipos en Windows para que utilicen la conexión a Internet de otro, que es el que hará de servidor Proxy.

Para nuestro ejemplo, los equipos tendrán como S.O. Windows XP y es necesario que estén conectados en red entre sí.

PASO 1. Configuración del PC que hará de servidor

-Para ello, pulsamos en “Inicio“, “Configuración“, “Panel de control” y ejecutamos “Conexiones de red“.

-Ejecutamos la opción “Configurar una red doméstica o para pequeña oficina“. Entonces, aparecerá un asistente para configuración de red, pulsamos “Siguiente“. Comprobamos que cumplimos los requisitos, es decir, tenemos un adaptador de red, módem u otro tipo de dispositivo utilizado para la conexión a Internet y estamos conectados en este momento a Internet.

En la siguiente ventana, marcamos la primera opción “Este equipo se conecta directamente a Internet. Los otros equipos de mi red se conectan a Internet a través de este equipo“. Pulsamos “Siguiente“.

-Escogemos la conexión a Internet que estamos utilizando, y “Siguiente“.

-Seleccionamos el adaptador de red (u otro dispositivo) mediante el cual se conecta el equipo con los demás de la red local (LAN).

Introducimos la descripción del equipo y el nombre. Y en la siguiente

ventana, el grupo de trabajo para la red y “Siguiente“.

-Es importante que si queremos permitir que los otros equipos puedan acceder a carpetas e impresoras compartidas del PC que hace de Servidor de Proxy marquemos la primera opción: “Activar el uso compartido de archivos e impresoras“.

-En la última ventana nos aparece un resumen de las opciones seleccionadas, pulsamos “Siguiente” si todo es correcto.

PASO 2. Configuración de la red

-En este momento, el asistente inicia el proceso de configuración de la red.

-Tras la configuración nos aparece una ventana que nos permite la posibilidad de crear un disco de configuración de red para ejecutarlo en los PC’s clientes. Pulsamos en “Crear Disco de configuración de red“, introducimos un disquete formateado y vacío. Y “Siguiente“.

-Tras la creación del disquete de configuración nos aparece una última ventana indicando que el proceso ha finalizado. También nos indica los pasos necesarios para configurar los demás equipos de la red mediante el disquete creado. Es necesario reiniciar el PC Servidor para finalizar con la configuración.

-Para consultar la configuración de red que ha dejado el asistente, pulsamos el botón derecho del ratón sobre “Mis sitios de red” y “Propiedades“. Seleccionamos la tarjeta de red que utilizamos para la conexión entre los equipos de nuestra red y pulsamos con el botón derecho del ratón, “Propiedades“. Seleccionamos “Protocolo Internet (TCP/IP)” y pulsamos en “Propiedades“.

-El asistente configura como dirección IP del equipo que hará de servidor Proxy, la dirección 192.168.0.1 y la máscara de subred: 255.255.255.0.

PASO 3. Configuración de los equipos clientes

 Introducimos el disquete, generado en el proceso de configuración

del Servidor Proxy, en cada equipo y accederemos a la unidad A:

para ejecutar el fichero “netsetup.exe“. Se abrirá el asistente de

configuración.

 En este paso seleccionamos “Este equipo se conecta a Internet a través de una puerta de enlace residencial o de otro equipo de mi red“.

 Tras la finalización del asistente, reiniciamos el equipo y probamos la conexión a Internet.

En este caso, el asistente marca todas las opciones como automáticas para que las IP’s y la puerta de enlace se asignen automáticamente (las asignará el Servidor Proxy). Si queremos ver la IP que le ha asignado el Servidor Proxy al equipo cliente podemos hacerlo pulsando en “Inicio” – “Ejecutar” y escribiendo “cmd“, y “Aceptar“. Nos aparece una ventana de consola donde escribimos el comando “ipconfig” y pulsamos “Enter“.

Este comando nos mostrará la configuración de la red, algo de este estilo:

-IP: 192.168.0.48

-Puerta de enlace: 192.168.0.1 (la del equipo Servidor Proxy).

VENTAJAS

Más importantes del Proxy de Windows XP es que funcionará casi cualquier tipo de aplicación que utilice Socket (conexión directa puerto a puerto), POP3, SMTP y cualquier otro programa que utilice vías de conexión a Internet diferentes al protocolo HTTP. Además, no se necesita ningún software adicional.

Como inconveniente resaltar que se tienen que cambiar todas las direcciones IP’s de la red, utilizando el rango 192.168.0.xxx.

Configuración de filtros.

Cuando un ordenador se conecta a Internet, no lo hace de forma directa, sino a través de equipos intermedios. Por un lado están los switches y routers, y por otro los servidores, ordenadores configurados para proporcionar servicios de red (descarga de archivos, obtención de IPs, resolución de nombres de dominio, etc). El tipo de servidor que se analiza en este tutorial es el servidor proxy(o proxy a secas).

Veamos un ejemplo de cómo funciona un proxy. En una red de área local, hay diez ordenadores, uno de los cuales es un proxy. Éste es el único que se conecta directamente a Internet, y a través del cual se conectan todos los demás; del proxy depende íntegramente el acceso de los otros ordenadores a Internet. Si un usuario externo a esta red quisiera rastrear el **origen de un paquete de red procedente de uno de estos ordenadores, sólo podría llegar hasta** el proxy, ya que es el único que puede crear los paquetes de red.

Debido a estas características, el proxy puede controlar completamente la conexión de red de los equipos que dependan de él. Y esto nos lleva al filtro de contenidos. Un filtro de contenidos es un proxy configurado para limitar el acceso a la red de sus equipos clientes en base a unos parámetros preestablecidos, mediante una aplicación de filtrado. Se puede utilizar una aplicación para Ubuntu llamada Squid.

Métodos de autenticación en un «proxy».

Como el proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, a veces se lo puede utilizar para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña. También es fácil otorgarles acceso a recursos externos sólo a las personas autorizadas y registrar cada uso del recurso externo en archivos de registro de los accesos identificados. Este tipo de mecanismo, cuando se implementa, obviamente genera diversos problemas relacionados con las libertades individuales y los derechos personales. Existen dos conceptos importantes para entender los modos de autenticación.

Tipo de desafío (type of challenge): indica el tipo de desafío que se le presentara al cliente.

Credenciales sustitutas (surrogate credentials): las credenciales sustitutas son algo que se utiliza para autenticar la transacción en lugar de las credenciales “reales”.

modos de Autenticación

Auto: el modo default es seleccionado basándonos en la petición que haga el cliente. Auto puede seleccionar cualquier de las opciones, proxy, origin, origin-ip, o origincookie-redirect dependiendo en el tipo de conexión (explicita o transparente) y la configuración de la cookie de autenticación en modo transparente.

Proxy-IP: El proxy utiliza un desafío en forma explícita y la IP del cliente como credenciales sustitutas. Proxy-IP específica un forward proxy inseguro. En algunos casos el desafío del proxy no funciona por lo que “origin” desafíos deben de ser generados.

Origin: El proxy actúa como una OCS y genera desafíos OCS. La conexión autenticada sirve como credenciales sustitutas.

Origin-IP: el proxy actúa como una OCS y genera desafíos OCS. La dirección del cliente es usada como credenciales sustitutas. Origin-IP es usado para soportar autenticación por IWA cuando el cliente no puede manejar credenciales por cookies.

Origin-Cookie: El ProxySG actual como un servidor de origen y genera desafíos de servidor de origen. Una cookie es generada como credenciales sustitutas. OriginCookie es usado en forward proxies para soportar autenticación pass-through de manera más segura que Origen-IP si en cliente entiende cookies. Solamente los protocolos HTTP y HTTPS soportan cookies; todos los demás protocolos son degradados a utilizar automáticamente Origin-IP.

SG2: Este modo es seleccionado automáticamente, basando en la petición, y usa las reglas definidas del SGOS 2.x.

From-IP: una forma es presentada para recolectar las credenciales del usuario. La forma es presentada cada vez que el caché de las credenciales del usuario expiren.

From-Cookie: Una forma es presentada para colectar las credenciales del usuario. Las cookies son setiadas en el dominio OCS solamente y el usuario es presentado con una nueva forma para cada dominio. Este modo es más utilizado en escenarios de proxy reverso donde hay un número limitado de dominios.

«proxys» inversos.

Un proxy inverso es un servidor proxy-caché "al revés". Es un servidor proxy que, en lugar de permitirles el acceso a Internet a usuarios internos, permite a usuarios de Internet acceder indirectamente a determinados servidores internos. El servidor de proxy inverso es utilizado como un intermediario por los usuarios de Internet que desean acceder a un sitio web interno al enviar sus solicitudes indirectamente. Con un proxy inverso, el servidor web está protegido de ataques externos directos, lo cual fortalece la red interna. Además, la función caché de un proxy inverso puede disminuir la carga de trabajo del servidor asignado, razón por la cual se lo denomina en ocasiones acelerador de servidor. Finalmente, con algoritmos perfeccionados, el proxy inverso puede distribuir la carga de trabajo mediante la

redirección de las solicitudes a otros servidores similares. Este proceso se denomina equilibrio de carga. Hay varias razones para instalar un "reverse proxy":

Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.

Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).

Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de

cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).

Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido.

proxys» encadenados.

Pues ahora vamos a rizar el rizo usando proxys encadenados por lo que incrementaremos el anonimato respecto a las formas que hemos visto hasta ahora, aunque ello también significa que ralentizaremos más nuestra navegación porque usaremos varios intermediarios por lo que el recorrido de la señal es mas largo, debemos tener esto en cuenta para elegir el procedimiento adecuado dependiendo de cada ocasión.

Para ello vamos a utilizar un programa que nos servirá para encadenar los proxies, en este caso usare SocksChain, pero hay más programas.

La ventaja que tiene este programa es que nos facilita la tarea de comprobar los proxies y tampoco tenemos que buscar la lista porque nos rastrea el mismo desde varios servidores, así que lo único que tenemos que hacer para echar a andar el programa es hacer clic en tool, luego en Proxy manager para empezar a buscar y a testear proxys.

Reverse Proxy / Proxy inverso

Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

-**Seguridad:** el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.

-**Cifrado / Aceleración SSL:** cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL(Security Sockets Layer).

-**Distribución de Carga:** el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada)

Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT.

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x.

Proxy abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido.

Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").