Seguridad Informática - 2º SMR
Tema 7: Seguridad de alto nivel en redes. Proxy.

7.1 Introducción

Una vez visto en el tema anterior que son los cortafuegos, en este tema conoceremos los proxys. Mientras que el cortafuegos lo usaremos para proteger el acceso desde el exterior a los servicios de los cuales somos proveedores, el proxy controlará el acceso desde la red interna hacia Internet, es decir añadirá seguridad cuando seamos consumidores de servicios de fuera.

Un Proxy desde un punto de vista general es un equipo que hace de intermediario, es decir, se encarga de realizar acciones en representación de otros. Dicho en términos informáticos, es un equipo de la red que se encarga de recibir peticiones de recursos de red de los equipos clientes y gestionarlas por ellos, respondiéndoles a sus peticiones cuando hayan terminado dicha gestión.

Un Proxy habitualmente y sobre todo desde el punto de vista de la seguridad hace de elemento de la red por el que pasa todo el tráfico entre la red interna y la externa (Internet), encargándose de realizar las peticiones externas en nombre de los equipos de la red interna y descartando aquellas peticiones que no cumplen las reglas establecidas por el administrador.

7.2 Características del proxy

- Permite definir los permisos que tienen los usuarios de la red interna sobre los servicios, dominios y direcciones IP externas.
- Todos los usuarios de la red interna comparten una única dirección IP (o un conjunto de direcciones), de forma que desde el exterior (Internet) 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 cache para aumentar el rendimiento de la red. Es decir, cuando se consulta una página se almacena en la cache del Proxy para que si posteriormente se vuelve a consultar se pueda servir más rápidamente.

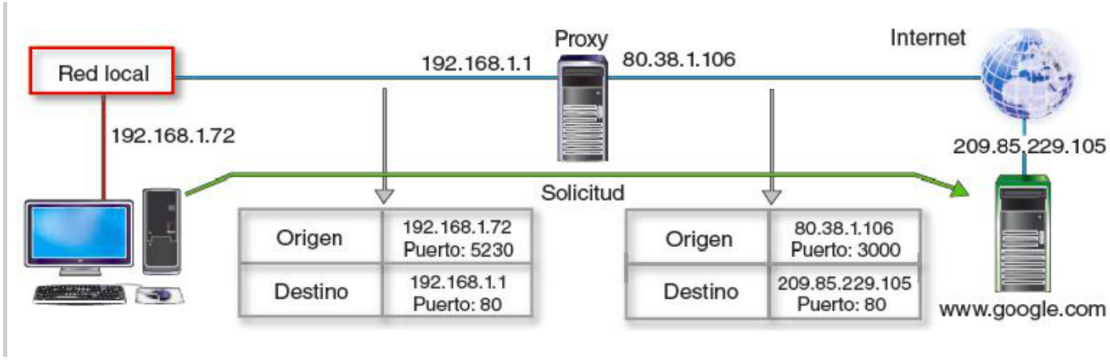
7.3 Funcionamiento del proxy

Los equipos que pertenecen a una red que tiene instalado un Proxy, cuando se comunican con el exterior a través de uno de los protocolos activos en el Proxy, en realidad están intercambiando paquetes con el Proxy, y es el Proxy el que intercambia paquetes con los equipos del exterior, de forma que cuando este recibe respuesta, a su vez contesta a los equipos internos.

Por ejemplo, cuando un equipo de la red interna solicita la página www.google.com. construye un paquete en el que el origen es su dirección IP y el puerto es uno aleatorio y libre asignado por el sistema operativo (por ejemplo IP 192.168.1.72 y puerto 5230). Como destino puesto que está utilizando un Proxy pone la dirección y el puerto del Proxy 182.168.1.1 y puerto 80.

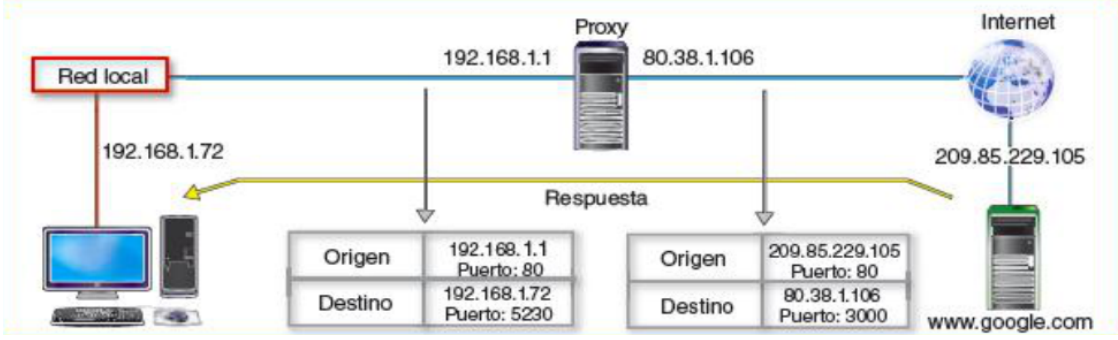
Esta solicitud llega al Proxy, y este tras comprobar que cumple las reglas establecidas, genera un paquete como si fuera él mismo el que realiza la consulta, es decir, genera su propio puerto cliente aleatorio y pone su propia IP como origen (IP 80.38.1.106 y puerto 3000). Con respecto al destino, pone la IP que corresponde con la petición del cliente, es decir www.google.com, 209.85.224.105, y el puerto correspondiente al servicio Web 80.

De esta manera cuando la solicitud llega a Google, en el paquete sólo hay referencias al Proxy, es decir, a la dirección IP 80.38.1.106.



Además anota qué equipo le solicitó la página para después poderle contestar, creando una tabla de estado para saber a qué equipo de la red interna le corresponde cada paquete que le llega de la red externa, conforme le van llegando solicitudes.

Cuando Google responde a la solicitud, responde a la dirección y el puerto que recibió como origen en la solicitud: la IP 80.38.1.106 y puerto 3000. Cuando llega la respuesta al Proxy, éste tras consultar la tabla de estado para saber cual es la dirección del equipo destino, tiene que modificar de nuevo la cabecera con el destino que le corresponda y se pone él mismo como origen.



Ejercicios propuestos

7.3.1. Teniendo en cuenta la configuración física del aula, si tuvieras que colocar un proxy para controlar el acceso a Internet desde tu aula, ¿dónde lo harías? ¿Necesitarías algún material adicional?

7.3.2. Haz dos gráficos similares a los del punto anterior representando la forma de acceder a Internet en el instituto desde el ordenador de clase, suponiendo que está instalado el proxy del ejercicio anterior.

7.3.3. Desarrolla la tabla de estado del proxy de los ejercicios anteriores.

7.4 Tipos de proxy

Dependiendo del tipo de tráfico que circulará por una red necesitaremos un proxy que cumpla con las necesidades del tráfico, ya sea para acelerar la descarga de contenidos o para autenticación de usuarios. En función de las características podemos clasificar los proxy de la siguiente manera.

- **Proxy caché web**: Mantienen copias locales de los archivos web más solicitados y los sirven bajo demanda, reduciendo la baja velocidad y coste en la comunicación con Internet.
- **Proxy NAT**: Integra los servicios de traducción de direcciones de red y proxy.
- **Proxy transparente**: Combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones al puerto 80 típicamente, son redirigidas hacia el puerto del servicio proxy de manera transparente al usuario.
- **Proxy anónimo**: Permite aumentar la privacidad y el anonimato de los clientes proxy, mediante una activa eliminación de características identificativas (dir IP, cabeceras, cookies, etc).
- **Proxy inverso**: Es un proxy instalado en una red con varios servidores web, sirviendo de intermediario a las peticiones externas, suponiendo una capa de seguridad previa, gestión y distribución de carga de las distintas peticiones externas, gestión de SSL o como caché de contenidos estáticos.
- **Proxy abierto**: Acepta peticiones de cualquier ordenador, esté o no conectado a su red. Esta característica, permite que este tipo de proxy se use como pasarela de envío masivo de spam, por lo que muchos servidores, como los de correo electrónico, deniegan el acceso a estos proxys a sus servicios.

7.5 Squid

Squid es uno de los Proxy más utilizados debido sobre todo a su potencia y estabilidad.

7.5.1 Instalación de Squid

Para instalar Squid podemos hacerlo a través de los tres caminos habituales:

- Compilando el programa a partir de los fuentes.
- Instalándolo directamente a partir de los binarios que podemos descargar de http://wiki.squid-cache.org/SquidFaq/BinaryPackages para nuestra distribución.
- A partir de los repositorios oficiales de nuestra distribución.

Una vez instalado Squid en el equipo servidor y configurados los interfaces de ambos equipos, podemos probar el funcionamiento configurando el navegador del equipo cliente para utilizar el Proxy que acabamos de instalar.

Comprobaremos que está accediendo al Proxy porque nos genera un error en el que al final hace referencia a Squid.

7.5.2 Configuración inicial

La configuración del Proxy Squid la tenemos que realizar a través de un fichero de configuración, como es habitual en sistemas GNU/Linux, llamado /etc/squid3/squid.conf. Como vamos a estar modificándolo, y por seguridad, haremos una copia de la versión original:

sudo cp /etc/squid3/squid.conf /etc/squid3/squid.conf.bak

Algunos de los parámetros más importantes del fichero de configuración de Squid son:

- **http_port**: Es el puerto del servidor en el que el servicio Squid estará escuchando peticiones de los clientes. Habitualmente suelen ser el 3128, 8080 o en algunos casos el propio 80 (del servicio Web). Nosotros dejaremos el valor por defecto: *http_port 3128*
- **cache_dir**: Es el directorio en el que Squid almacenará las páginas que decida mantener en la cache. El valor por defecto de este parámetro es:

  cache_dir ufs /var/spool/squid3 100 16 256
- **cache_mem**: Indica la cantidad de memoria cache que se utilizará para Squid. Por defecto son 8MB.
- **cache_mgr**: Indica a Squid el correo del administrador, de forma que si dejara de funcionar, este recibirá un correo alertando de esta situación.
- **access_log, cache_log y cache_store_log**: Indica el lugar en el que se almacenarán los ficheros de log de Squid. En el caso del access_log, lo define en la siguiente línea:

  access_log /var/log/squid3/access.log squid
- **cache_effective_user y cache_effective_group**: Indican respectivamente el nombre del usuario y grupo que ejecutará el Proxy.
- **ftp_user**: Para las conexiones anónimas FTP es una costumbre muy habitual utilizar el correo electrónico como nombre de usuario, así el administrador del FTP podrá contactarnos en caso de necesitarlo. Como ahora puede ser el Proxy el que se conecta en lugar del cliente, la cuenta de correo que aparecerá será la del Proxy, así que es necesario configurarla. Si un cliente de nuestro Proxy hiciera algo indebido en un servidor FTP, sería conveniente que el administrador de dicho FTP pudiera ponerse en contacto con nosotros para comunicárnoslo.
- **error_directory**: Indica el directorio en el que se encuentran los mensajes de error que el Proxy mostrará a los clientes. Para que los mensajes aparezcan a los clientes en castellano, tendremos que modificar este parámetro a */usr/share/squid3/errors/Spanish*.

7.5.3 Control de acceso en squid

En este punto nos vamos a referir a todos aquellos parámetros que nos permiten controlar el acceso dependiendo por ejemplo de quién haga o cuál sea la petición.

Definiremos primeramente las listas de acceso, es decir, definiremos grupos de equipos, de IP, de dominios, de horarios, etc, a los que luego permitiremos o denegaremos el acceso. Para ello usaremos el parámetro **ACL**.

El formato general del parámetro acl es:

acl aclname acltype valores

Y los tipos de acl que podemos definir son los siguientes:

- **src**: Define a través de sus direcciones IP un conjunto de equipos de origen. Por ejemplo podemos definir como origen el aula mediante la siguiente lista: *acl aula src 192.168.50.0/24*
- **dst**: Utilizando este parámetro podemos generar una lista de acceso por direcciones IP de destino, es decir, generar una lista de direcciones IP que coincidirá con una petición al Proxy cuando la petición vaya dirigida a una de esas direcciones IP. La sintaxis general de este parámetro es: *acl aclname dst dirección-IP-destino red-IP-destino*
- **dstdomain**: Permite generar la lista de destinatarios a partir de dominios. La sintaxis general de este parámetro es: *acl aclname dstdomain .dominio1 .dominio2*
- **url_regex**: Permite utilizar expresiones regulares para definir una lista de url de acceso. Cuando se reciba una petición a una dirección url, por ejemplo www.tucasino.es, se comprobará si se produce coincidencia con la expresión regular definida. Puedes utilizarlo para incluir todas las url que incluyan la palabra casino: *acl casinos url_regex casino*

Para definir una página en concreto también se puede utilizar este parámetro de la siguiente forma:

acl pcompras url_regex [-i] ^http://www.paginacompras.com

- **urlpath_regex**: Permite utilizar expresiones regulares para definir los caminos normalmente de ficheros a los que se intente acceder o descargar.

  acl fgif urlpath_regex [-i] .gif #para archivos .gif

  acl fmp3 urlpath_regex [-i] .mp3 #para archivos .mp3

- **time**: Permite generar una lista de acceso con ciertos horarios, de forma que luego podamos permitir el acceso o negarlo durante dichos horarios. El formato general de time es:

  acl aclname time [días] [horas]

Una vez realizadas las definiciones anteriores, se realizan las reglas de acceso en sí, mediante el comando **http_access**.

La sintaxis general de este parámetro es:

http_access allow|deny [!]aclname

Las reglas, como en el cortafuegos, se deben poner en el orden en el que queremos que sean evaluadas, de forma que si una es validada, ya no seguirá leyendo más reglas.

deny_info: Se puede especificar una página de error en concreto cuando se deniegue alguna de las peticiones al proxy. Se puede definir una página de error para las acl que queramos denegar con un mensaje en concreto de la siguiente forma:

deny_info NombrePaginaError.hml nombreacl

Donde el NombrePginaError.html puede ser también una URL del tipo http://... y si es una fichero html propio debe estar guardado en el directorio correspondiente a error_directory.

Cuando una regla http_access sea de tipo deny y la última acl evaluada es verdadera, saldrá esta página de error en vez de la estándar.

7.5.4 Clasificación de sitios en Squid

El control del acceso en un Proxy es una tarea muy tediosa debido a que el número de sitios de Internet es muy grande y además cambian constantemente (se generan nuevos sitios todos los días y desaparecen algunos que existían).

Para descargar una de las listas de sitios disponibles en Internet accede a la sección de descargas (download) de la página http://urlblacklist.com y descarga el fichero bigblacklist.tar.gz.

7.6 Bibliografía:

- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill