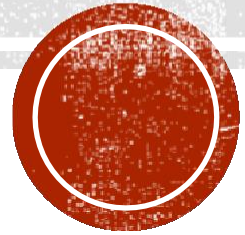
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

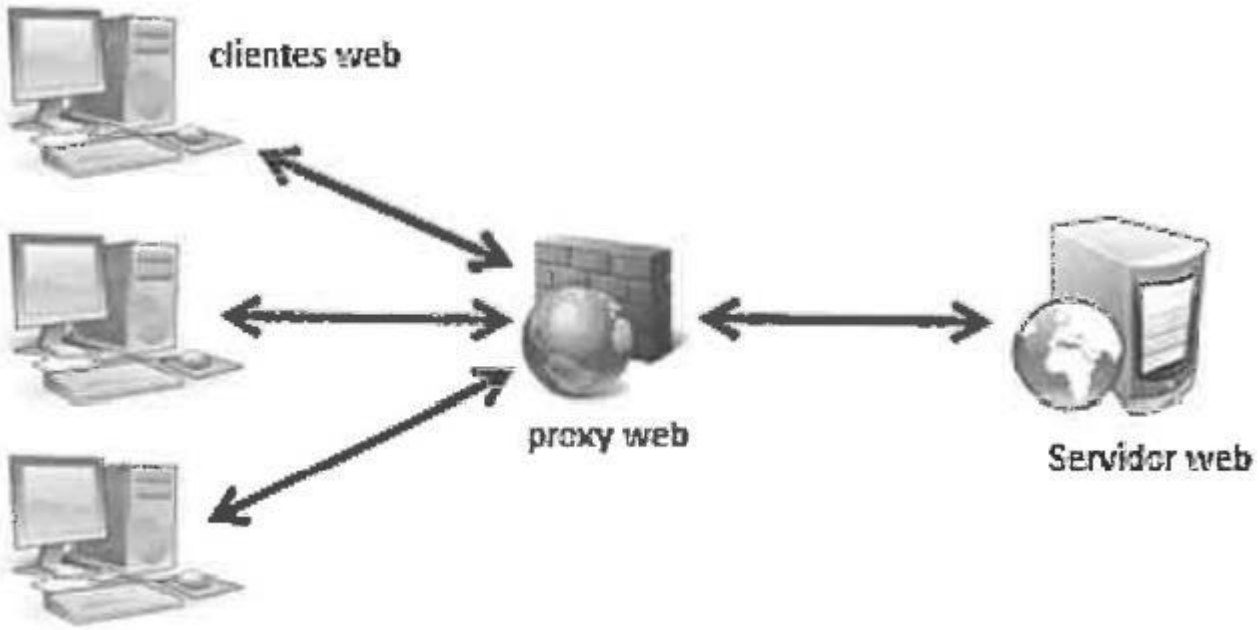


INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Es un software o dispositivo que realiza una función en nombre de otro sistema o aplicación que se denomina cliente proxy
  - Proxy transparente
  - Proxy no transparente
  - Aglutina todas las peticiones de los clientes de una red para impersonarse en nombre de los clientes ante un servicio externo

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy

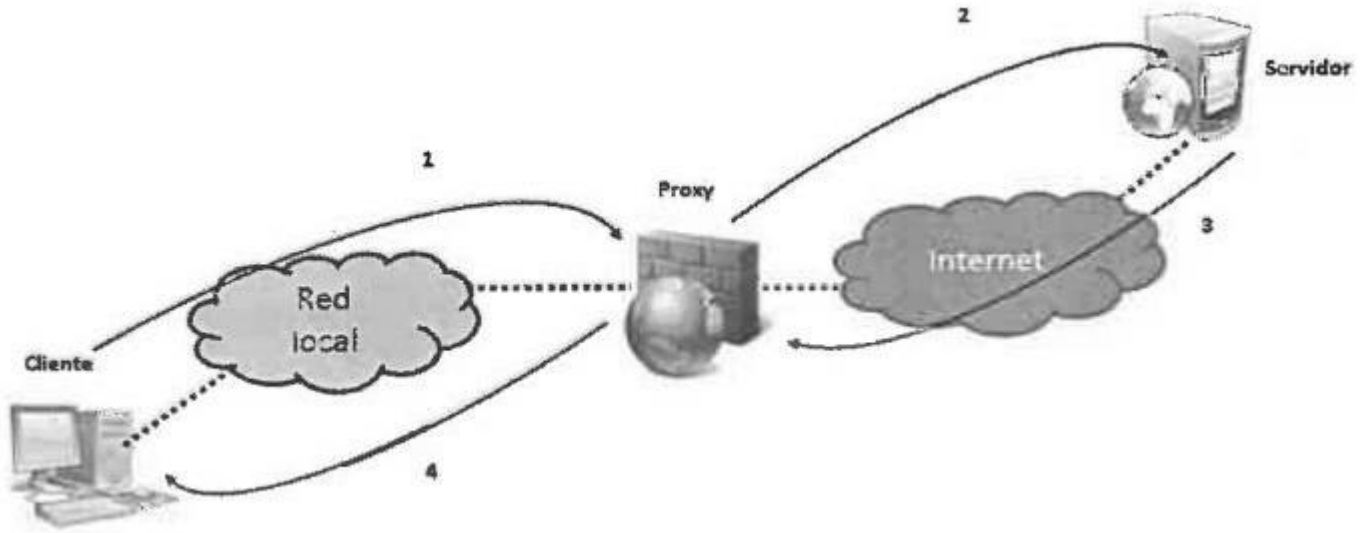


INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Fases a realizar en el entorno proxy para el acceso a un servicio remoto:
    1. El cliente solicita el recurso al servidor adecuado
    2. Para ello hace llegar la petición al servidor proxy
    3. El servidor proxy puede trasladar la petición como le llega o modificarla
    4. El proxy contacta con el servidor remoto y presenta la petición del cliente proxy en su nombre
    5. El servidor remoto acepta la petición ignorando si la petición viene del proxy realmente o es de un cliente anterior, por lo que el cliente proxy queda oculto al servidor remoto
    6. El servidor remoto gestiona la petición y devuelve los resultados al proxy
    7. Una vez que el servidor proxy tiene los resultados puede operar con ellos
    8. Finalmente el proxy traslada los resultados de la petición al cliente proxy que hizo la petición

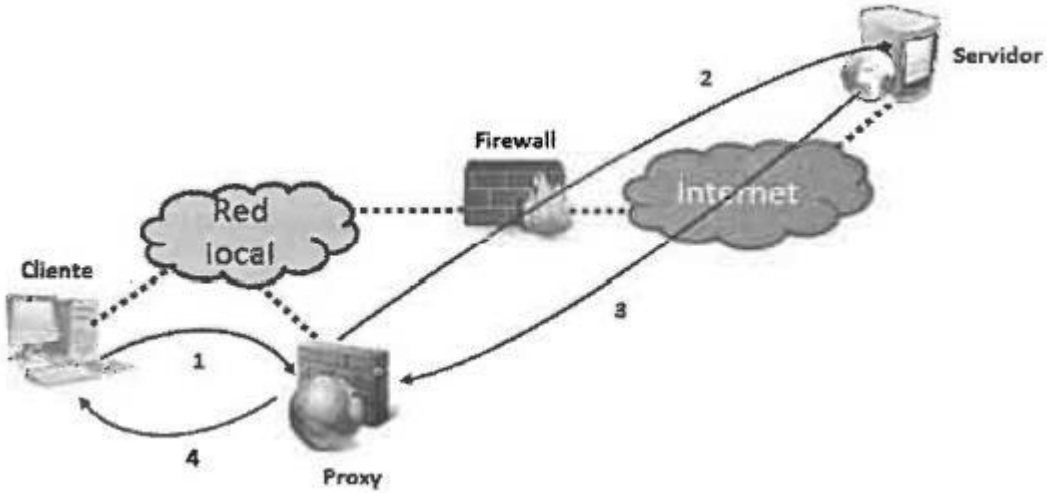
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

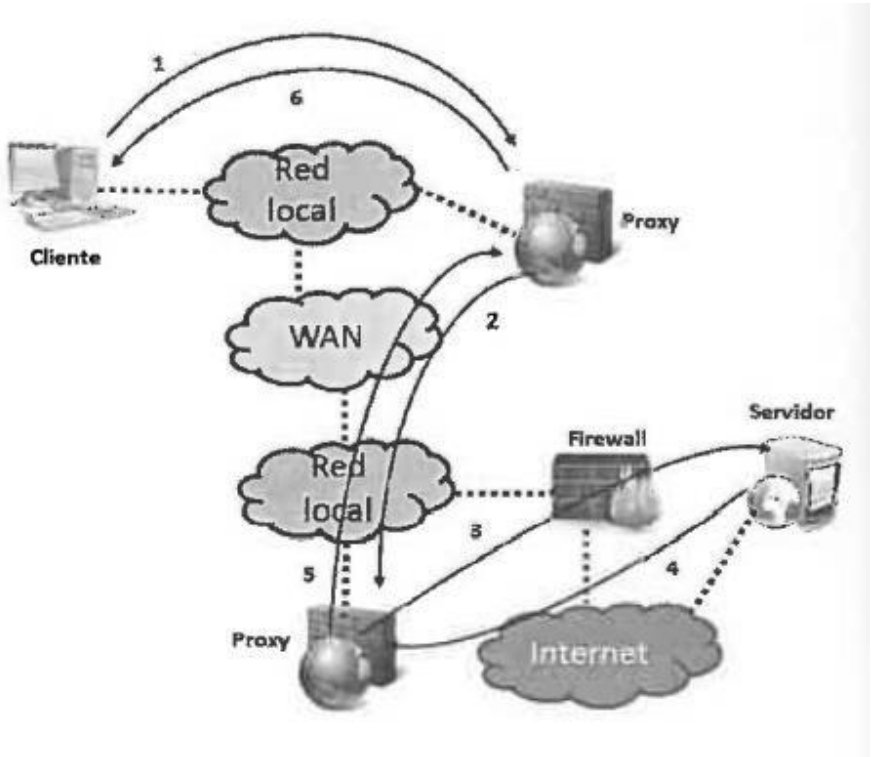
- Caracterización del servidor proxy
  - Fases a realizar en el entorno proxy para el acceso a un servicio remoto:



INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

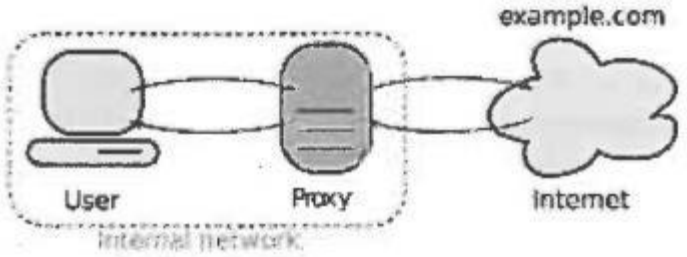
- Caracterización del servidor proxy
  - Los servidores proxy se pueden encadenar, esto aporta la ventaja de que en cada salto se pueden integrar nuevas funcionalidades de valor añadido, aunque presenta el problema de la latencia



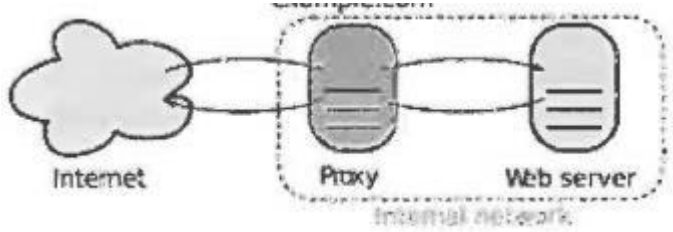


INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Tipos de servidores proxy por la relación con sus clientes:
    - Forward proxy: el cliente debe invocar el nombre del servidor destino para realizar la conexión



    - Reverse proxy: recupera recursos de uno o más servidores en nombre del cliente, los recursos son devueltos al cliente como si vinieran del proxy inverso en vez del servidor



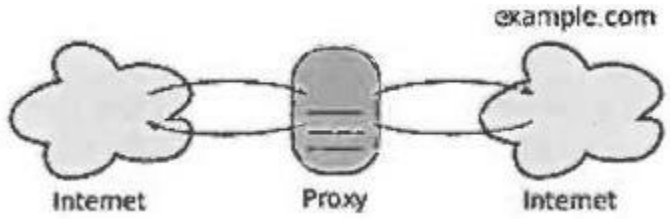
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Los reverse proxy son muy útiles para asegurar los servicios ofrecidos por los servidores públicos

    - Ocultan la existencia y características del servidor al que representan.
    - Dificultan la penetración de malware en la LAN del servidor.
    - Pueden finalizar los túneles de cifrado SSL liberando de esta función al servidor y pudiendo establecer entre el proxy y el servidor una conexión equivalente no cifrada dentro de la LAN del servidor, que se supone segura.
    - Pueden distribuir la carga (load balancing) entre varios servidores equivalentes en la misma LAN de servidores.
    - Aligeran la carga del servidor mediante técnicas de caching.
    - Optimizan las comunicaciones mediante técnicas de compresión ahorrando ancho de banda.

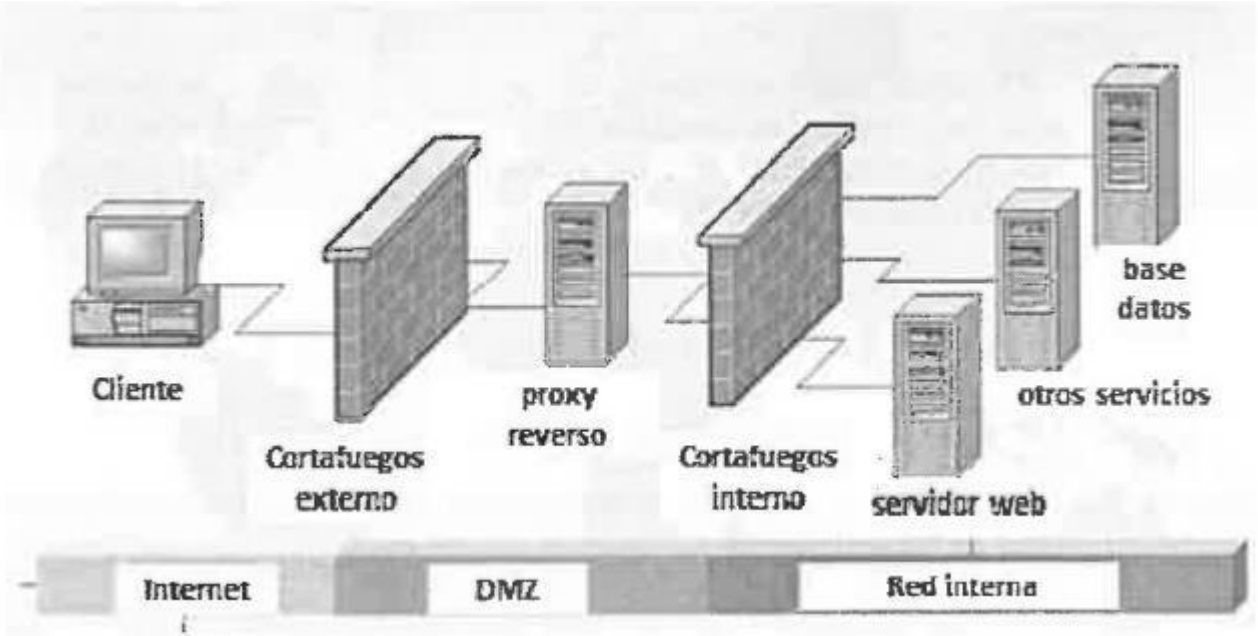
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Tipos de servidores proxy por la relación con sus clientes:
    - Forward abierto: es un proxi de tipo directo que es accesible por cualquier desde cualquier lugar de la red. Suelen utilizarse como proxy anónimos



INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Ejemplo de reverse proxy en DMZ fuertemente protegida



INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Proxy transparente, intercepting proxy o forced proxy
    - Requiere que el equipo cliente tenga dirigida su ruta por defecto hacia él y examinará el tráfico y capturará las peticiones de los clientes
    - La puerta de enlace por defecto del equipo cliente debe apuntar al proxy transparente
    - Es frecuente que el proxy tenga habilitado el protocolo NAT para la traducción de direcciones IP internas en las IP externas del proxy
    - El cliente ignora que sus peticiones son desviadas o capturadas por lo que no tiene que hacer ninguna operación de configuración adicional. Por este motivo es muy utilizado por los ISP (Internet Service Providers)

    - Tiene algunos inconvenientes:
      - Problemas de autenticación ya que los protocolos que admiten no siempre permiten gestionar autenticación de cliente
      - Permite ocultar las actividades de los usuarios de redes de navegación anónima

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - Tipos de servidores proxy por las aplicaciones que impersonan
    - Los servidores proxy ofrecen servicios dedicados que son específicos de la aplicación o protocolo que impersonan
    - Se habla por tanto de proxy de aplicación
    - Es habitual por tanto que sobre un mismo sistema se configuren varios proxies de aplicación cada uno dedicado a servir peticiones de un protocolo o aplicación específica (un proxy para http, otro para https, SMTP, IMAP,…)

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

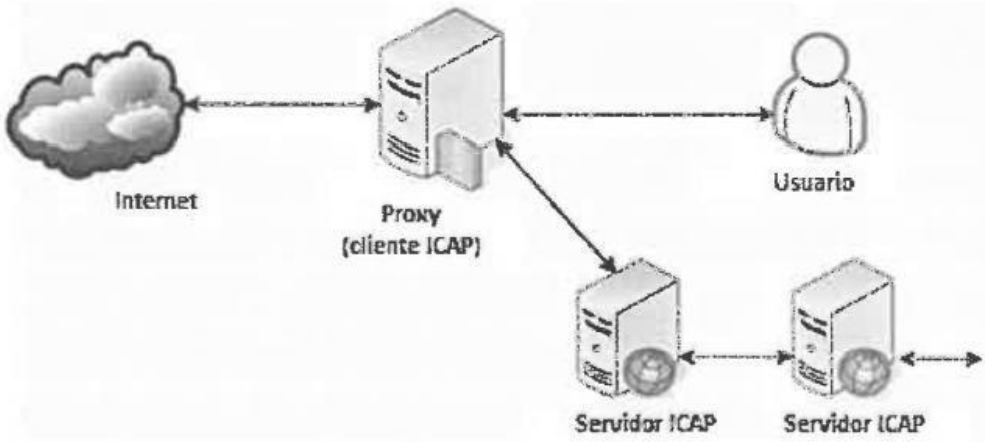
- Integración del proxy con otras aplicaciones
  - Aunque la funcionalidad del proxy es muy específica su implementación puede integrar otras funcionalidades (antivirus, cortafuegos, filtrado de contenidos, …)
  - El software específico que añade la función se inserta entre la acción de interceptación de la petición del cliente proxy y la nueva petición del servidor proxy hacia el servidor remoto.
  - En estos casos el nombre del proxy se toma de la función que añaden, así podemos tener:
    - Proxy de caché: gestiona una caché de forma que la información solicitada por la primera petición de un cliente queda almacenada por si un segundo cliente vuelve a solicitar la misma información
    - Proxy de filtrado de contenidos: realiza el filtrado de contenidos en función de unas reglas previamente configuradas
    - Proxy de antivirus: escanea malware mediante la búsqueda de patrones
    - Proxy de registro de actividad: registra en ficheros log la actividad de los usuarios

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Proxy ICAP (Internet Content Adaptation Protocol) e inspección de contenidos
  - ICAP es un protocolo de adaptación de contenidos que permite la transformación de contenidos y su filtrado. Fue creado en 1999 y estandarizado en 2003
  - Permite el uso de antivirus, filtrado de contenidos, traducción dinámica de páginas, inserción automática de anuncios, compresión de HTML, etc.
  - El cliente ICAP es un dispositivo de la seguridad de red que recoge la petición, por ejemplo servidor proxy

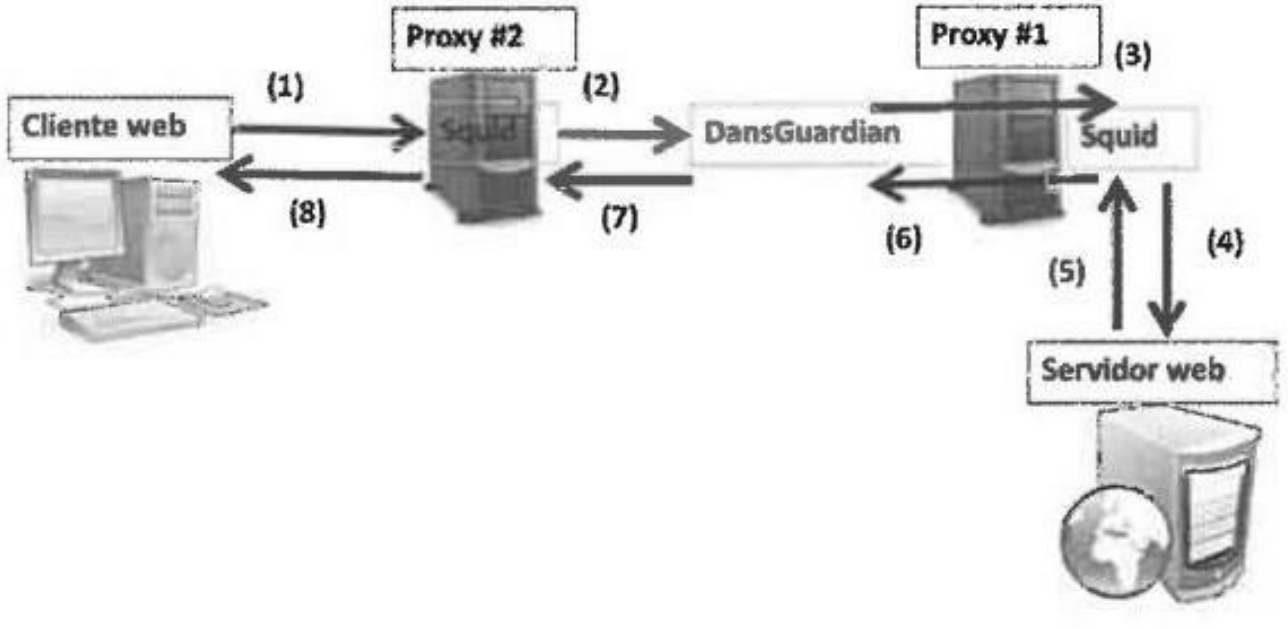
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Proxy ICAP e inspección de contenidos
  - Los servicios basados en ICAP tienen dos posibilidades de implantación:
    - Modo solicitud (request): la redirección al servidor de filtrado se realiza inmediatamente después de la solicitud del cliente → Para el filtrado de acceso, el cliente ICAP primero comprueba la petición de usuario pasándola a la cadena de servidores IPCAP y si la petición es aceptada accede a los servidores para recuperar el contenido
    - Modo de respuesta (response): la redirección se realiza después de la respuesta del servidor de destino → para el filtrado de contenido, el cliente ICAP primero recupera los contenidos de Internet y posteriormente los pasa a la cadena de servidores IPCAP para validar al respuesta



INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Proxy ICAP e inspección de contenidos
  - Otra posibilidad para el filtrado de contenidos es la utilización de DansGuardian como servidor de gestión de contenidos con un servidor proxy (como por ejemplo Squid). DansGuardian también puede hacer al función de cliente ICAP



INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Copfilter sobre IPCop
  - IPCop es una distribución Linux que implementa un cortafuegos (firewall):
    - Sencillo, con pocos requerimientos hardware → Orientado a usuarios domésticos o pequeñas empresas (SOHO)
    - Proporciona una simple interfaz web de administración
    - Integra un servidor proxy Squid
    - La comunidad de Copfilter ha desarrollado un add-in que permite operaciones de filtrado (antivirus, antispam, filtrado de contenidos)

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Proxy socks
  - Opera a nivel de circuito y no depende de la aplicación utilizada por el usuario
  - No hace las peticiones en nombre del cliente, sólo las traspasa
  - Requiere que la aplicación esté preparada para poder dialogar con el proxy
  - Pueden funcionar de una forma genérica dando soporte a múltiples protocolos, como pueden ser: FTP, HTTP/s , POP3, SMTP, DNS, etc. Esto supone una gran ventaja frente a los proxy de aplicación que sólo soportan un único protocolo. Esto es debido a que no interpretan el tráfico de datos, simplemente lo enrutan a través de una conexión TCP
  - Se trata de una solución adecuada para proteger la red interna de las intrusiones mediante el uso de firewall sin tener que limitar excesivamente a los usuarios en sus accesos a la red externa
  - Sin embargo puede presentar problemas al administrador de seguridad ya que permite a los usuarios saltarse limitaciones que el administrador haya implementado basándose en aplicación, como puede ser limitación de navegación web, mediante el uso de proxy socks (que no limitaría a nivel de aplicación)

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Instalación y configuración de Squid
  - Es uno de los servidores proxy de código libre más utilizados. Ha sido desarrollado en origen para Linux, pero hay versiones para UNIX y Windows

  - Características:
    - Proxy para http, https, ftp y gopher
    - Es compatible con SSL
    - Gestiona una caché con niveles de jerarquía y arrays de caché mediante protocolo WCCP (Web Cache Control Protocol)
    - Se puede configurar como proxy transparente
    - Ofrece control de acceso
    - Es compatible con protocolo de gestión SNMP
    - Dispone de caché de resolución de DNS

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Instalación y configuración básica de Squid

La instalación de Squid sobre un sistema Ubuntu (o Debian) se puede hacer desde los repositorios oficiales de la distribución con la orden:

sudo apt-get install squid3 squid3-client squid3-cgi resolvconf

en donde se han instalado también algunos componentes adicionales que pueden ser útiles como resolvconf. La instalación crea automáticamente en el sistema un usuario y un grupo específico con el que se ejecutará el proceso. Podemos validar la creación de este usuario y grupo con la orden:

grep proxy /etc/{passwd,group}

que presentará una salida semejante a:

/etc/passwd:proxy:x:13:13:proxy:/bin:/bin/sh

/etc/group:proxy:x:13:

En donde se ve que efectivamente hay una cuenta y un grupo con el nombre "proxy". El fichero de configuración de Squid se llama /etc/squid3/squid.conf

El usuario que ejecute el servicio tendrá que tener derechos sobre todos los ficheros de squid, así como sobre la caché, que por defecto se instalará sobre /var/spool/squid3.

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Instalación y configuración básica de Squid

Así sobre el fichero de configuración, basta con que squid tenga derechos de lectura, mientras que sobre la caché tendrá que tener todos los derechos:

ls -l /etc/squid3/squid.conf

-rw-r--r-- 1 root root 158453 2010-02-26 17:45 /etc/squid3/squid.conf

ls -ld /var/spool/squid3

drwxr-xr-x 19 proxy proxy 4096 2010-03-03 08:30 /var/spool/squid3

Por seguridad, nunca debe ejecutarse Squid con los privilegios de la cuenta root.

El fichero de configuración (/etc/squid3/squid.conf) es un fichero de texto repleto de comentarios (líneas que comienzan con #) y de directivas que se pueden configurar. Aunque por seguridad conviene hacer una copia de seguridad del fichero de configuración original, cuando se modifica este fichero se puede analizar la validez de su sintaxis, lo que nos previene de posibles errores en la edición, con la orden:

squid3 -k parse

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Instalación y configuración básica de Squid

A continuación, estudiaremos algunas de las directivas más utilizadas con un ejemplo para cada una de ellas y especificando su significado concreto:

- **http_port 3128**. Abre todas las direcciones IP del sistema por el puerto 3128 para escucha de http. Por defecto, Squid escucha las peticiones procedentes de los clientes proxy por el puerto 3128.
- **http_port 192.168.221.254:3128**. Abre únicamente la IP de referencia (no todas), por el puerto especificado.
- **visible_hostname fwproxy.example.com**. Define el nombre de host con el que el proxy se anunciará a los clientes (por ejemplo, en las páginas de error).
- **dns_nameservers 192.168.221.253 192.168.221.252**. Squid utiliza los DNS de /etc/resolv.conf, pero si se configura esta directiva consultará los DNS que se especifiquen en ella.

Las páginas de error que presenta Squid a los clientes proxy son archivos de texto plano en formato HTML, por lo que se pueden editar para su personalización. La directiva que asigna la ruta al directorio que contiene las páginas de error es:

error_directory /usr/share/squid3/errors/Spanish

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Instalación y configuración básica de Squid

En cuanto al servicio de sistema, que es el soporte para el servidor Squid, se puede gestionar como cualquier otro servicio del sistema. Por ejemplo, para iniciar el servicio squid ejecutaremos como superusuario:

/etc/init.d/squid3 start

Este script ejecuta el programa /usr/sbin/squid3 en segundo plano usando las opciones definidas en la variable SQUID_ARGS, que por defecto son: -D –s y -C. La opción -D deshabilita los chequeos DNS iniciales, la opción -s habilita el registro de eventos al syslog, y la opción -C gestiona las señales de error fatales.

Si se modifica algún ACL en el fichero de configuración y se desea que el proxy tome la nueva configuración sin tener que reiniciar el servicio se puede ejecutar una validación de la configuración y posteriormente una reconfiguración con las dos órdenes siguientes:

squid3 -k parse

squid3 -k reconfigure

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Instalación y configuración básica de Squid

Una vez que está arrancado el servicio se puede parar como cualquier otro servicio. Se recomienda parar el proxy siempre que los cambios de configuración sean pronunciadamente significativos. La orden de parada es:

/etc/init.d/squid3 stop

Aunque también se puede parar y arrancar inmediatamente con:

/etc/init.d/squid3 restart

Para automatizar el inicio del Squid con el arranque del sistema se puede ejecutar la orden siguiente que creará los enlaces simbólicos necesarios para el arranque automático:

update-rc.d squid3 defaults

Por último, si deseamos remover este automatismo procederemos a ejecutar la orden inversa a la anterior, que es:

update-rc.d -f squid3 remove

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de caché y log de Squid
  - Squid no sólo es un proxy web, también integra un servidor de caché para almacenar las páginas web

El fichero de configuración de Squid también incluye algunas directivas para la gestión de la caché. Algunas de ellas son las siguientes:

- **cache_effective_user proxy**. Define el usuario con el que Squid operará en la caché.
- **cache_mgr proxy@example.com**. Define la dirección de correo electrónico utilizada en las páginas de error. Si Squid fracasa, se envía un mail a esta dirección avisando al administrador.
- **cache_mem 32 MB**. Memoria asignada para caché en RAM.
- **cache_dir Type Directory-Name Mbytes Level1 Level2 [options].** El tipo define el sistema de almacenamiento: ufs, aufs, etc. Directory-Name es el directorio de la caché. Por defecto, en Ubuntu está en /var/spool/squid3. Mbytes son los Mbytes que se reservan para el caché. Level1 es el número de directorios de primer nivel. Por defecto es 16. Level 2 es el número de subdirectorios de segundo nivel. Por defecto es 256. Se pueden habilitar varias cachés en distintas ubicaciones escribiendo más de una directiva.
- **maximum_object_size 4096 KB**. Define el tamaño máximo de los objetos que serán guardados en caché.

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de caché y log de Squid

Squid permite registrar todas las conexiones que se le hagan de modo que el administrador pueda conocer en cada momento qué ocurre en su sistema. La configuración de la información que se registrará en los ficheros de log se lleva a cabo también en el fichero de configuración de Squid mediante directivas. Las más utilizadas son las siguientes:

logformat <name> <format specification>. Name es una etiqueta que identificará el formato especificado posterior. Format specification es una cadena de caracteres con la especificación del formato del registro log. Este formato se puede consultar en la documentación de Squid, aunque un resumen lo podemos encontrar en la

- **Tabla 5.1**. Por ejemplo una línea válida sería: **logformat squid %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt**
- **access_log /var/log/squid3/access.log squid.** Ruta del archivo de log con la actividad de clientes y el formato en que se registrará (en este caso, formato Squid). El usuario squid debe tener derechos de escritura sobre este fichero de log. Si no se desea log: el argumento debe ser none.
- **cache_store_log /var/log/squid3/store.log.** Ruta del log de la caché.
- **logfile_rotate 7.** Número de ficheros logs que se guardarán.

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de caché y log de Squid

Código	Descripción
>a	Dirección IP del cliente en origen
>A	FQDN del cliente
<A	Dirección IP del servidor
la	Dirección IP local
lp	Número de puerto local
ts	Tiempo en segundos
tu	Tiempo en milisegundos
tl	Hora local
tg	Hora GMT
tr	Tiempo de respuesta en milisegundos
>h	Cabecera de petición

Código	Descripción
<h	Cabecera de respuesta
un	Nombre de usuario
ul	Login de usuario
ui	Identidad del usuario
Hs	HTTP status code
Ss	Squid request status
Sh	Squid hierarchy status
mt	Tipo MIME
rm	Método de request (GET/POST, etc.)
ru	URL solicitada
rv	Versión de protocolo de petición

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de caché y log de Squid

Código	Descripción
et	Valor devuelto por un ACL externo
ea	Literal devuelto por un ACL externo
<st	Tamaño de la respuesta, incluidas las cabeceras
<sS	Tamaño del objeto de subida
%	Carácter literal

- Para más detalle consultar: http://www.squid-cache.org/Doc/config/logformat/

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - El filtrado de conexiones se realiza en Squid mediante la inclusión de 2 componentes diferentes (pero que están relacionados) que se incluyen en el fichero de configuración de Squid:
    - Los elementos de ACL (Access Control List o Lista de Control de Acceso) → es una declaración en la que se relacionan varios elementos (los que la componen) en base a origen, destino, usuario, horario, … del tráfico que se somete a filtrado
    - La lista de acceso, es la que permite o niega el acceso al servicio → También denominadas reglas de acceso
  - El filtrado se produce por la concurrencia de ambos elementos

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - Se confeccionan unas Listas de Control de Acceso que designan grupos de máquinas o redes para especificar posteriormente qué tienen permitido. Cada una de ellas tendrá asociada unas Reglas de Control que regulará la actividad. Es decir, definimos unas listas, por una parte y establecemos unas reglas específicas ellas

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - La estructura de una ACL tiene uno de los siguientes formatos:
    - acl nombreacl tipoacl [-i] valor1 valor 2 … → valores separados por espacios
    - acl nombreacl tipoacl [-i] "identificador archivo" → sólo admite un archivo con lista de valores
  - La estructura de una regla:
    - access_list <allow|deny> nombreacl1 nombreacl2 …
  - Ejemplo de uso:

    acl loc_subnet src 192.168.221.0/24 → Elemento de ACL

    …..

    http_access allow loc_subnet → Regla

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - ACL
    - Sus elementos pueden ser (hace referencia al tipoacl):
      - De tipo origen:
        - src: es la dirección IP del cliente, puede ser una IP o un rango de ellas
        - proxy_auth: autenticación de usuario a través de un proceso externo
        - browser: user agent del navegador que realiza la petición
      - De tipo destino:
        - dstdomain: nombre de domino(s) de destino solicitados por el cliente
        - url_regex: permite comprobar expresiones regulares para URLs solicitadas por el cliente
        - urlpath_regex: permite comprobar expresiones regulares para URLs solicitadas por el cliente, sin considerar el protocolo y el hostname de la misma
        - port: define uno o más números de puerto de destino solicitados por el cliente

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - ACL
    - Sus elementos pueden ser (hace referencia al tipoacl):
      - De otros tipos:
        - method: define el método utilizado por el cliente para realizar la petición HTTP (GET, POST)
        - proto: especifica el protocolo usado
        - req_mime_type: permite comprobar expresiones regulares para tipo de contenido en peticiones
        - rep_mime_type: permite comprobar expresiones regulares para tipo de contenido en respuestas
        - time: hora del día y día de la semana

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - ACL
    - Las ACL son sensibles a mayúsculas y minúsculas, aunque se pueden definir para que no lo sean, usando el parámetro –i detrás del tipoacl
    - Cuando la lista de elementos (valores) es grande se recomienda escribir todos los valores en un fichero y construir la ACL mediante una referencia al fichero

    - Los nombres de las ACL pueden ser cualquiera siempre que cumplan:
      - Dos ACL no pueden tener el mismo nombre
      - No se pueden utilizar espacios en el nombre de la ACL
      - Los nombres deben tener menos de 31 caracteres y no pueden incluir símbolos
      - Sí pueden usarse “_” y “-” para facilitar la lectura / escritura

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - Reglas / listas de acceso
    - Una vez definidas las ACL se pueden construir reglas de acceso basadas en ellas. Estas reglas concederán el acceso o lo denegarán a las peticiones que cumplan las ACL asociadas a la regla
    - Existen múltiples reglas de control, algunas de ellas:
      - **http_access**
      - http_reply_access
      - reply_body_max
      - icp_access
      - always_direct
      - never_direct

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - Reglas / listas de acceso
    - Las reglas se evalúan en el orden en que están escritas en el fichero de configuración y se dejan de verificar en cuanto la regla coincida
    - Se hace un OR entre cada línea (entre cada regla)
    - Si una regla tiene más de una ACL se hace un AND entre cada una de ellas
    - Si después de evaluar todas las reglas de acceso no se encuentra una regla que coincida con la petición se ejecuta la acción definida por la última regla de la lista, por lo que se recomienda usar el ACL “all” tal como se indica en el ejemplo siguiente

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - Reglas / listas de acceso

http_access allow|deny acl1 acl2...

http_access allow|deny acl3 acl4...

...

http_access deny all

las reglas deben interpretarse con la siguiente lógica:

http_access allow|deny acl1 AND acl2 AND ...

OR

http_access allow|deny acl3 AND acl4 AND ...

OR

...

http_access deny all

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Configuración de filtros mediante reglas y ACL en Squid
  - Ejemplo

Ejemplo: Declaración de reglas con ACL de puertos, métodos y direcciones IP.

```
# Elementos de ACL:
...
# Declaración del localhost
acl localhost src 127.0.0.1/32
# Declaración de puertos considerados seguros
acl Safe_ports port 80 21 443 563 70 210 1025-65535
# Declaración de puertos SSL
acl SSL_ports port 443
# Declaración de métodos de tipo CONNECT
acl CONNECT method CONNECT
# Declaración de la subred local
acl loc_subnet src 192.168.221.0/24
# Declaración de direcciones IP que no podrán navegar
acl ip_sin_internet src "/etc/squid3/ip_sin_internet.acl"
```

```
# Reglas de acceso:
...
# Se deniega el acceso por todos los puertos que NO sean seguros.
http_access deny !Safe_ports
# Se deniega el acceso mediante CONNECT a los puertos que no estén en SSL_ports
http_access deny CONNECT !SSL_ports
# Se permite el acceso al localhost
http_access allow localhost
# Se deniega el acceso a las direcciones IP incluidas en la ACL ip_sin_internet
http_access deny ip_sin_internet
# Se permite el acceso al resto de nodos de la subred
http_access allow loc_subnet
# Se deniega el acceso para cualquier otra condición
http_access deny all
```

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy
  - En el acceso a través de un proxy web puede ser interesante restringir el acceso en función de parámetros no estáticos del sistema (como son p.e. las IPs) sino examinando el usuario que hace la petición.
  - En estos casos se requiere un proceso de autenticación

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Cuando se configura un proxy con soporte de autenticación, los navegadores web envían las credenciales del usuario codificadas en la petición http usando la cabecera "authorization" (del protocolo HTTP), de esta forma si al proxy llega una petición con esta cabecera decodifica el usuario y la contraseña para validar el usuario
  - La autenticación puede utilizar diferentes protocolos

Módulo	Descripción
NCSA	Usa un archivo de usuarios y contraseñas de tipo NCSA
LDAP	Usa el protocolo Lightweight Directory Access Protocol
MSNT	Usa un dominio de autenticación Windows NT
PAM	Usa los módulos de autenticación PAM para autenticación local
SMB	Usa un servidor SMB de tipo Windows o Samba
getpwam	Usa el primitivo archivo de contraseñas Unix
SASL	Usa las bibliotecas de autenticación SASL
NTLM	Usa la autenticación y negociación de autenticación

Tabla 5.2. Módulos de autenticación de usuarios disponibles en Squid.

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Squid soporta autenticación basada en NCSA (entre otras) que usa un archivo en el que se mantiene una lista de usuarios y contraseñas codificadas
  - Este método es el más sencillo de usar, aunque no el más seguro y flexible

  - La autenticación se hace utilizando la directiva auth_param para introducir la configuración adecuada en el fichero de configuración de squid para establecer entre otros el fichero de usuarios y contraseñas

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid3/users-passwd
auth_param basic children 10
auth_param basic realm Servidor Proxy Squid Corporativo
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
```

  - El fichero de usuarios y contraseñas deberá ser creado y editado con htpasswd

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Adicionalmente se debe proceder a la creación de ACLs y reglas de autenticación en Squid

  - Por ejemplo para permitir el acceso a todos los usuarios autenticados independientemente de quiénes sean:

    acl usuarios_NCSA proxy_auth REQUIRED

    http_access allow usuarios_NCSA

  - Para permitir el acceso a unos usuarios concretos habría que especificar unas reglas más estrictas:

    acl usuarios_permitidos proxy_auth usuario1 usuario2 usuario3

    http_access allow usuarios_permitidos

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Ejemplo

Ejemplo: Discriminación en el acceso de diversos usuarios

```
# Tomado de la web oficial de Squid.
# Declaración de una lista blanca de dominios
acl whitelist dstdomain .whitelist.com .goodsite.com .partnerssite.com
# Declaración del protocol de navegación
acl http proto http
# Declaración de los puertos de navegación inseguros
acl port_80 port 80
# Declaración de los puertos de navegación seguros
acl port_443 port 443
# Declaración de los métodos http que podrán crear túneles SSL
acl CONNECT method CONNECT
# Los usuarios tendrán que autenticarse y pasarán a formar parte de autenticated_users
acl authenticated_users proxy_auth REQUIRED
```

```
# Reglas para usuarios que no han sido autenticados correctamente
# Se permite el acceso por el puerto 80 hacia la lista blanca de dominios
http_access allow http port_80 whitelist
# Se permite la creación de túneles SSL solo para el puerto 443 hacia la lista blanca
http_access allow CONNECT port_443 whitelist
#
# Reglas solo para usuarios autenticados
# Pueden navegar por el Puerto 80 hacia cualquier destino, no solo hacia la lista blanca
http_access allow http port_80 authenticated_users
# Pueden crear túneles SSL por el Puerto 443 hacia cualquier destino
http_access allow CONNECT port_443 authenticated_users
```

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 1
    - Crear las entradas para un archivo de configuración para denegar el acceso a todos los equipos a la dirección www.google.es
  - Actividad 2
    - Crear las entradas para un archivo de configuración para denegar el acceso a todos los equipos a las direcciones www.google.es y www.pruebax.com
  - Actividad 3
    - Crear las entradas para un archivo de configuración para denegar el acceso a todos los equipos a las direcciones www.google.es, http://es.yahoo.com/ y http://es.msn.com/

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 1
    - Crear las entradas para un archivo de configuración para denegar el acceso a todos los equipos a la dirección www.google.es

```
acl no_permitido1 dstdomain www.google.es
http_access deny no_permitido1
```

  - Actividad 2
    - Crear las entradas para un archivo de configuración para denegar el acceso a todos los equipos a las direcciones www.google.es y www.pruebax.com

```
acl no_permitido1 dstdomain www.google.es www.pruebax.com
http_access deny no_permitido1
```

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 3
    - Crear las entradas para un archivo de configuración para denegar el acceso a todos los equipos a las direcciones www.google.es, http://es.yahoo.com/ y http://es.msn.com/

Crear en la carpeta personal un archivo llamado no_permitidos que contenga las direcciones de los tres siguientes dominios:

www.google.es
http://es.yahoo.com/
http://es.msn.com/

Incluir en el fichero de configuración:

acl no_permitido1 url_regex "/home/usuario/no_permitidos"

http_access deny no_permitido1

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 4
    - Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Crear las entradas en el archivo de configuración squid.conf que permita el acceso a Squid a todos los ordenadores de la red y no lo permita a los restantes.
  - Actividad 5
    - Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Se desea permitir el acceso a Squid a los ordenadores con las IP que están comprendidas en el rango 192.168.1.1 y 192.168.1.10 (ambas incluidas). Crear las entradas en el archivo de configuración squid.conf que permita el acceso a Squid de acuerdo a lo indicado.

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 4
    - Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Crear las entradas en el archivo de configuración squid.conf que permita el acceso a Squid a todos los ordenadores de la red y no lo permita a los restantes.

```
acl todalared src 192.168.1.0/255.255.255.0
http_access allow todalared
http_access deny all
```

  - Actividad 5
    - Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Se desea permitir el acceso a Squid a los ordenadores con las IP que están comprendidas en el rango 192.168.1.1 y 192.168.1.10 (ambas incluidas). Crear las entradas en el archivo de configuración squid.conf que permita el acceso a Squid de acuerdo a lo indicado.

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 5
    - Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Se desea permitir el acceso a Squid a los ordenadores con las IP que están comprendidas en el rango 192.168.1.1 y 192.168.1.10 (ambas incluidas). Crear las entradas en el archivo de configuración squid.conf que permita el acceso a Squid de acuerdo a lo indicado.

      Crea en el directorio personal un fichero llamado ip_permitidas que tenga estas direcciones (cada dirección en una línea diferente)

      acl red_local src "/home/nombre_usuario/ip_permitidas"
      http_access allow red_local
      http_access deny all

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 6
    - Crear las entradas en el archivo de configuración squid.conf que denieguen las conexiones a todos los equipos en horario de 18:00 a 21:00 horas
  - Actividad 7
    - Crear las entradas en el archivo de configuración squid.conf que denieguen las conexiones a todos los equipos en horario de 18:00 a 21:00 horas, pero sólo los lunes, martes y miércoles

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 6
    - Crear las entradas en el archivo de configuración squid.conf que denieguen las conexiones a todos los equipos en horario de 18:00 a 21:00 horas

```
acl horario time 18:00-21:00
http_access deny horario
```

  - Actividad 7
    - Crear las entradas en el archivo de configuración squid.conf que denieguen las conexiones a todos los equipos en horario de 18:00 a 21:00 horas, pero sólo los lunes, martes y miércoles

```
acl horario time MTW 18:00-21:00
http_access deny horario
```

  - NOTA: Los días de la semana se definen con letras, las cuales corresponden a la primera letra del nombre en inglés: S – Domingo, M – Lunes, T – Martes, W – Miércoles, H – Jueves, F – Viernes, A - Sábado

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 8
    - Crear las entradas en el archivo de configuración squid.conf que denieguen las conexiones al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Métodos de autenticación en un proxy Squid
  - Actividad 8
    - Crear las entradas en el archivo de configuración squid.conf que denieguen las conexiones al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas

```
acl equipo5 src 192.168.1.5
acl horario 18:00-21:00
http_access deny equipo5 horario
```

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Herramientas y gestión de logs
  - Es importante que el administrador revise los ficheros de log que generan todos los dispositivos de seguridad para conocer el estado de la red
  - Una dificultad que se encuentra el administrador es que esta información suele estar muy dispersa (distribuida por todos los nodos de la red)
  - Un segundo problema que tiene que resolver es que la cantidad de información a evaluar es inmensa y, dependiendo del análisis a realizar, deberá discriminar los eventos más significativos separando los de menor relevancia
  - Las herramientas de gestión de logs pueden ayudar al administrador en esta tarea de revisión
    - En Squid se dispone de Sarg (Squid Analysis Report Generator), que es una aplicación que construye informes de uso del Squid de una red. Genera informes en formato HTML con gran cantidad de información (usuarios, direcciones IP, bytes transmitidos, sitios web visitados, tiempos…)
    - Requiere configuración en base a las necesidades del administrador
    - Los informes Sarg se visualizan como una página web, por lo que precisa de un servidor web