INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

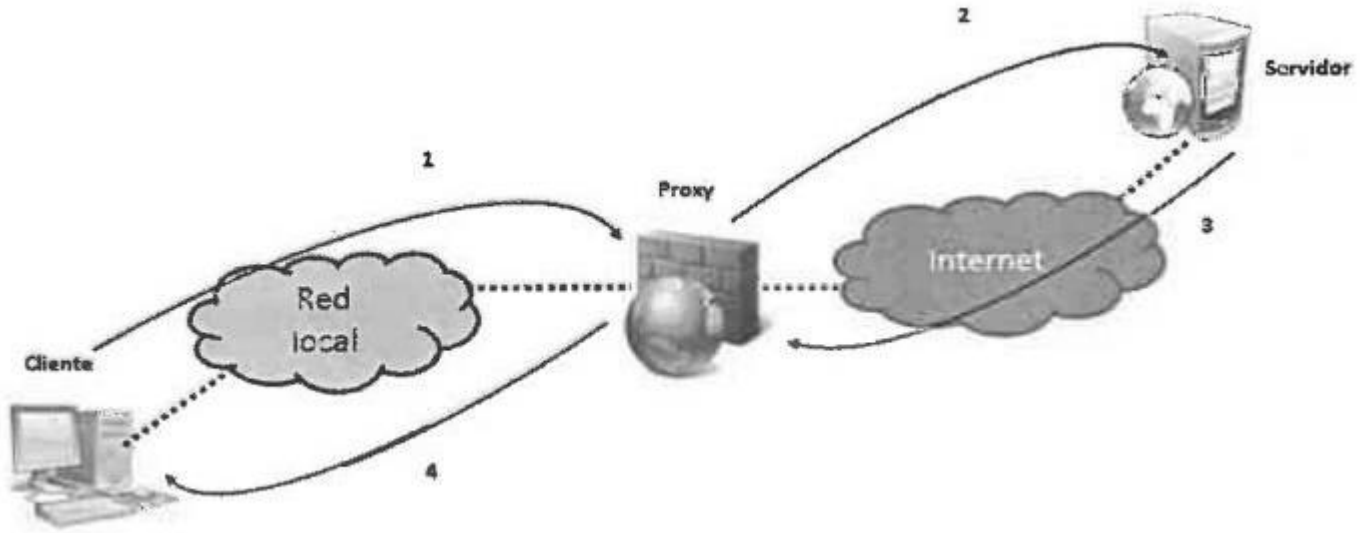
- Caracterización del servidor proxy
  - Es un software o dispositivo que realiza una función en nombre de otro sistema o aplicación que se denomina cliente proxy
  - Proxy transparente
  - Proxy no transparente
  - Aglutina todas las peticiones de los clientes de una red para impersonarse en nombre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

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- Caracterización del servidor proxy
  - 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

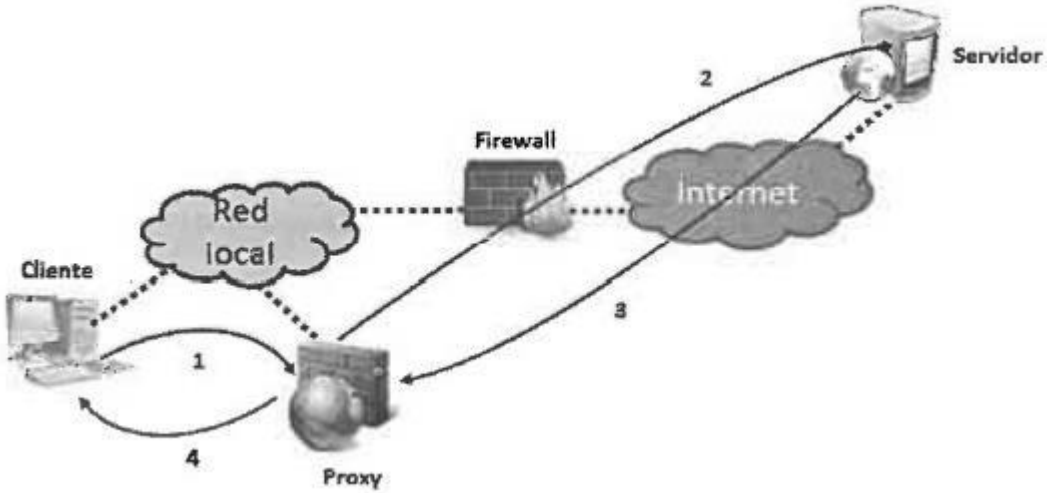
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

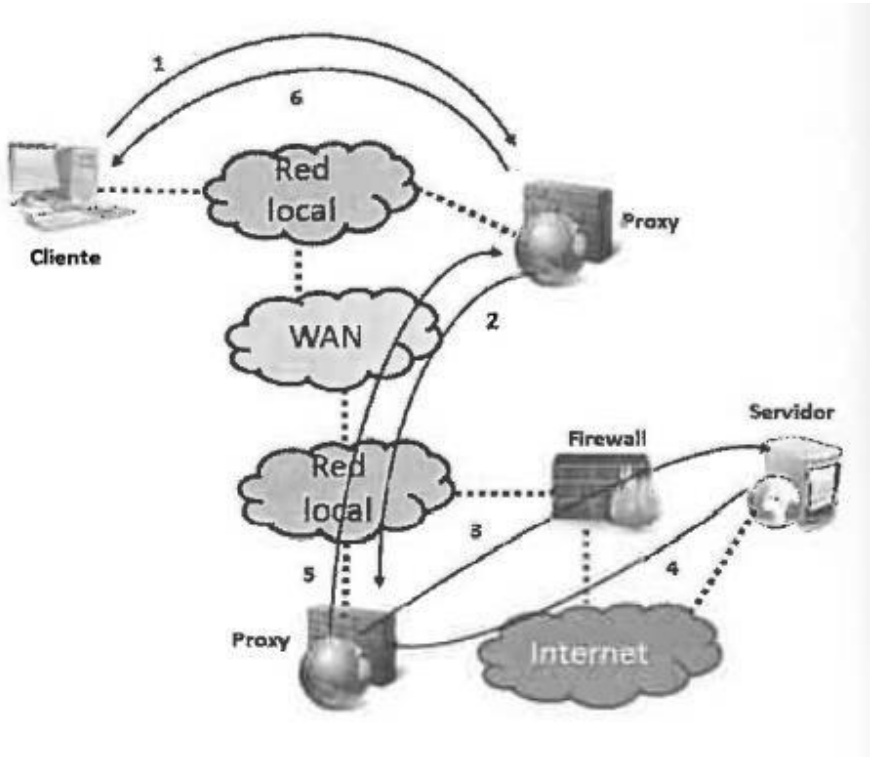
- Caracterización del servidor proxy
  - Fases a realizar en el entorno proxy para el acceso a un servicio remoto:



INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

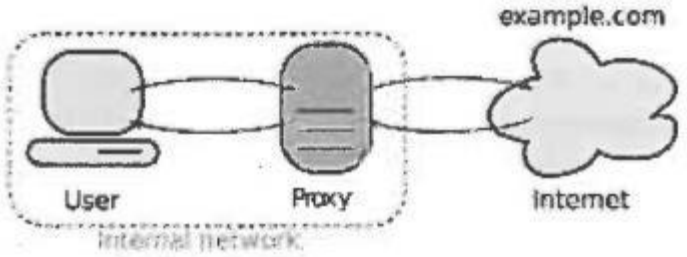
- Caracterización del servidor proxy
  - Los servidores proxy se pueden encadenar, esto aporta la ventaja de que en cada salto se pueden integrar nuevas funcionalidades de valor añadido, aunque presenta el problema de la latencia



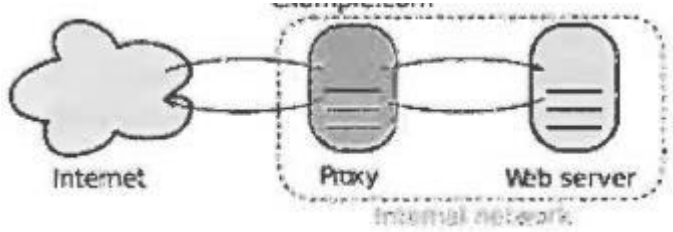


INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- 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



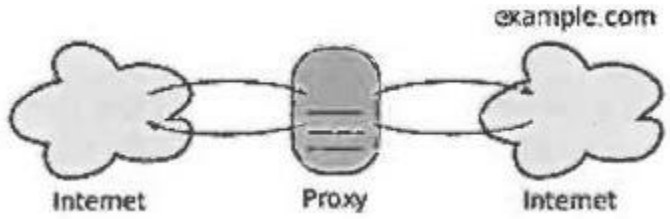
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- 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.

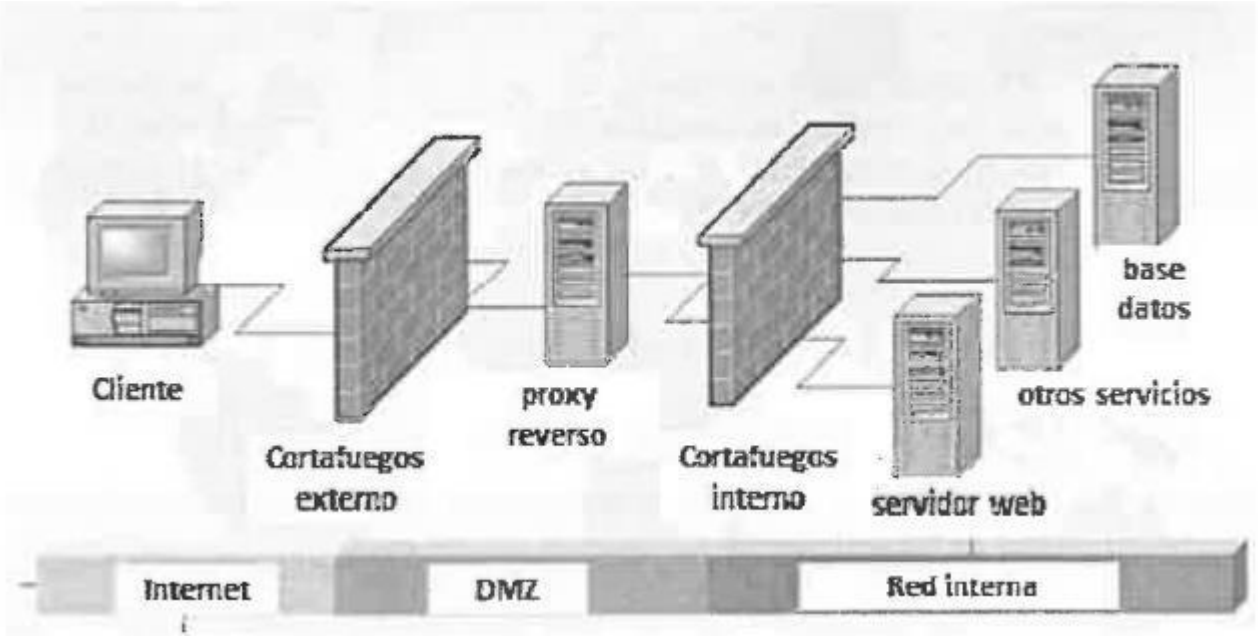
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

- 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

- 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 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

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

- 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
```