

Control de acceso a servicios: Proxy



Prof. Manuel Castillo

Administración de Redes

Escuela Profesional de Ciencia de la Computación

Facultad de Ciencias

Universidad Nacional de Ingeniería

Introducción



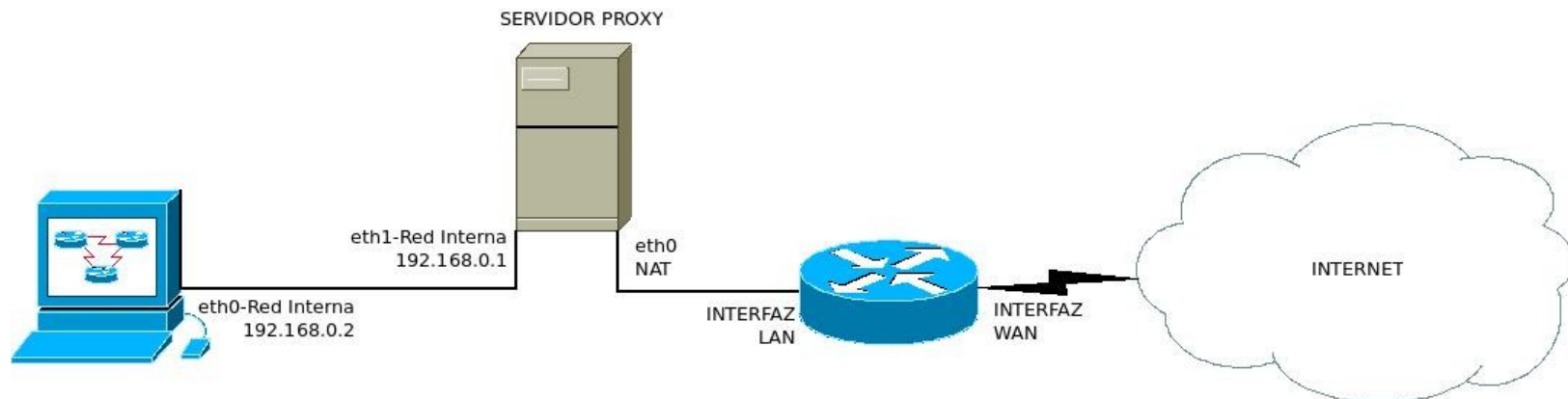
- Aplicaciones especializadas que actúan de intermediarios entre servidores y clientes.
- También se conocen como servicios delegados o apoderados (tiene el poder sobre otro).
- Cada servicio requiere un proxy diferente.
- Pasarela de aplicación: máquina que ejecuta un proxy.
- Componentes:
 - Servidor real. Ofrece un servicio (WWW, FTP...).
 - Cliente proxy. Versión especial del cliente estándar. Se conecta a través del servidor proxy.
 - Servidor proxy. Es el intermediario.
- El cliente cree estar conectado al servidor real.
- El servidor real cree que el servidor proxy es el cliente.



Definición



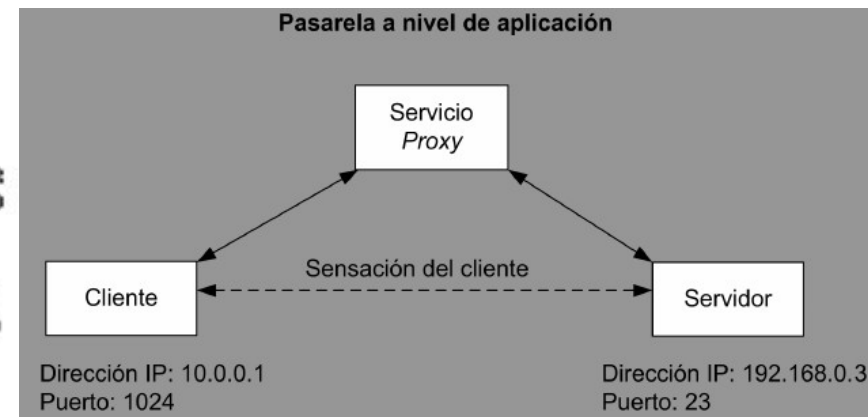
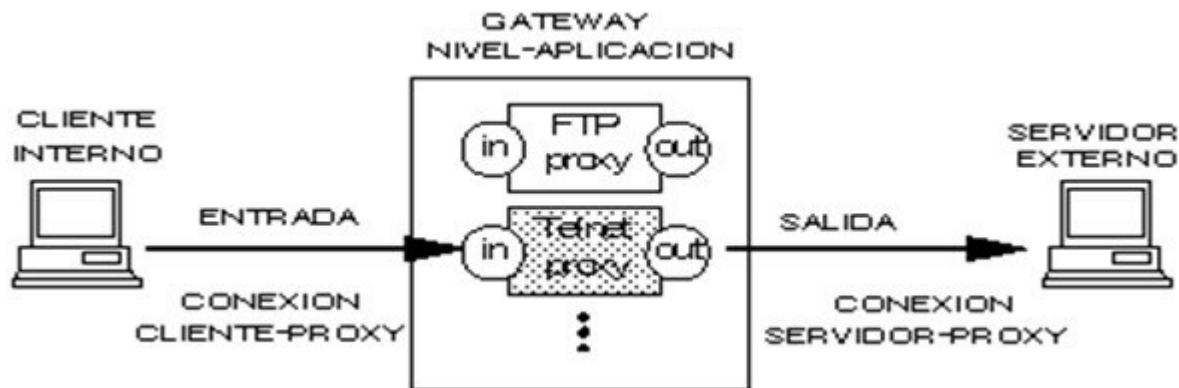
- Servicio de red que permite a los clientes realizar conexiones de red indirectas hacia otros servicios.
- Proceso de conexión:
 - Cliente se conecta hacia el Proxy.
 - Cliente solicita una conexión, archivo o recurso hacia un destino distinto de él mismo.
 - Proxy proporciona el recurso: (i) dado desde su caché; o (ii) conectándose hacia el servidor y devolver el recurso al cliente.



Funciones (Ventajas)



- Filtrado y firewalling.
 - Permite denegar el acceso a algunos dominios
 - Estudia el contenido de los paquetes, trabajando a nivel de aplicación.
 - Puede modificar el contenido de los paquetes.
- Compartir conexión a Internet.
- Servicio de caché
 - En servicios (como web) mantiene una caché de contenidos.
 - Puede mejorar el ancho de banda de la red.



Desventajas



- Se requiere adaptación de los clientes para usar proxy.
- Elevada carga de trabajo → potencial cuello de botella.
 - Su efectividad depende del patrón de tráfico en la organización.
 - Peor de los casos: los clientes visitan páginas que no están relacionadas entre sí. Entonces el Proxy no es más que una sobrecarga.
 - No son de gran utilidad con páginas web de generación dinámica.
- Los servidores no pueden distinguir a sus usuarios por IP si están detrás de un Proxy.

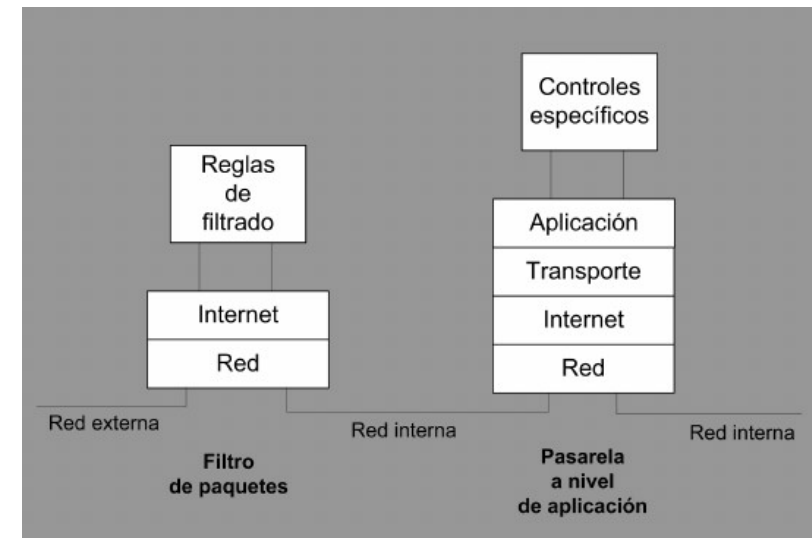
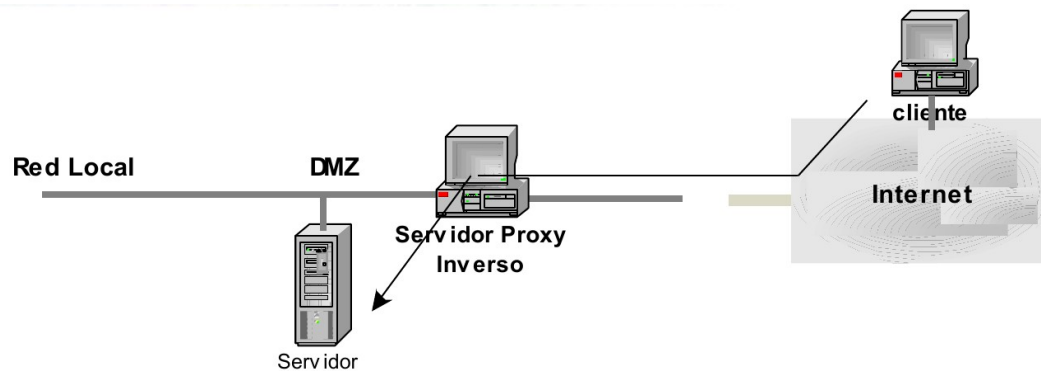


TIPOS DE PROXY

Proxy saliente/entrante



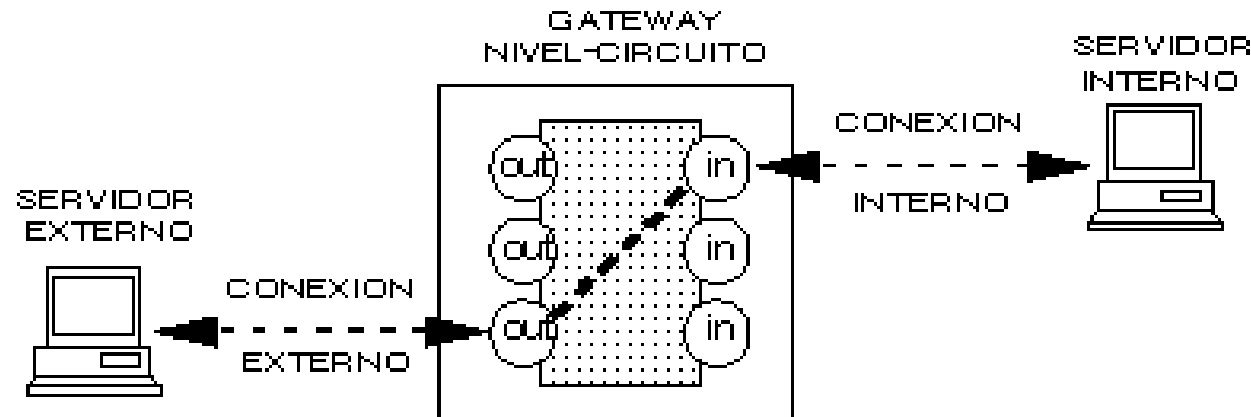
- Proxy saliente
 - Un cliente interno accede a un servidor externo.
 - Se identifica al cliente interno (ej.- por IP).
 - Se registra la actividad y traduce dirección y puerto: PAT.
- Proxy entrante o inverso
 - Un cliente externo accede a un servicio interno.
 - Se registra la actividad y traduce dirección y puerto: NAT.
 - Ofrece seguridad puesto que es el único punto de entrada.
 - Los ataques se centran en el proxy.
 - Enmascara las direcciones internas.



Pasarela a nivel de circuito



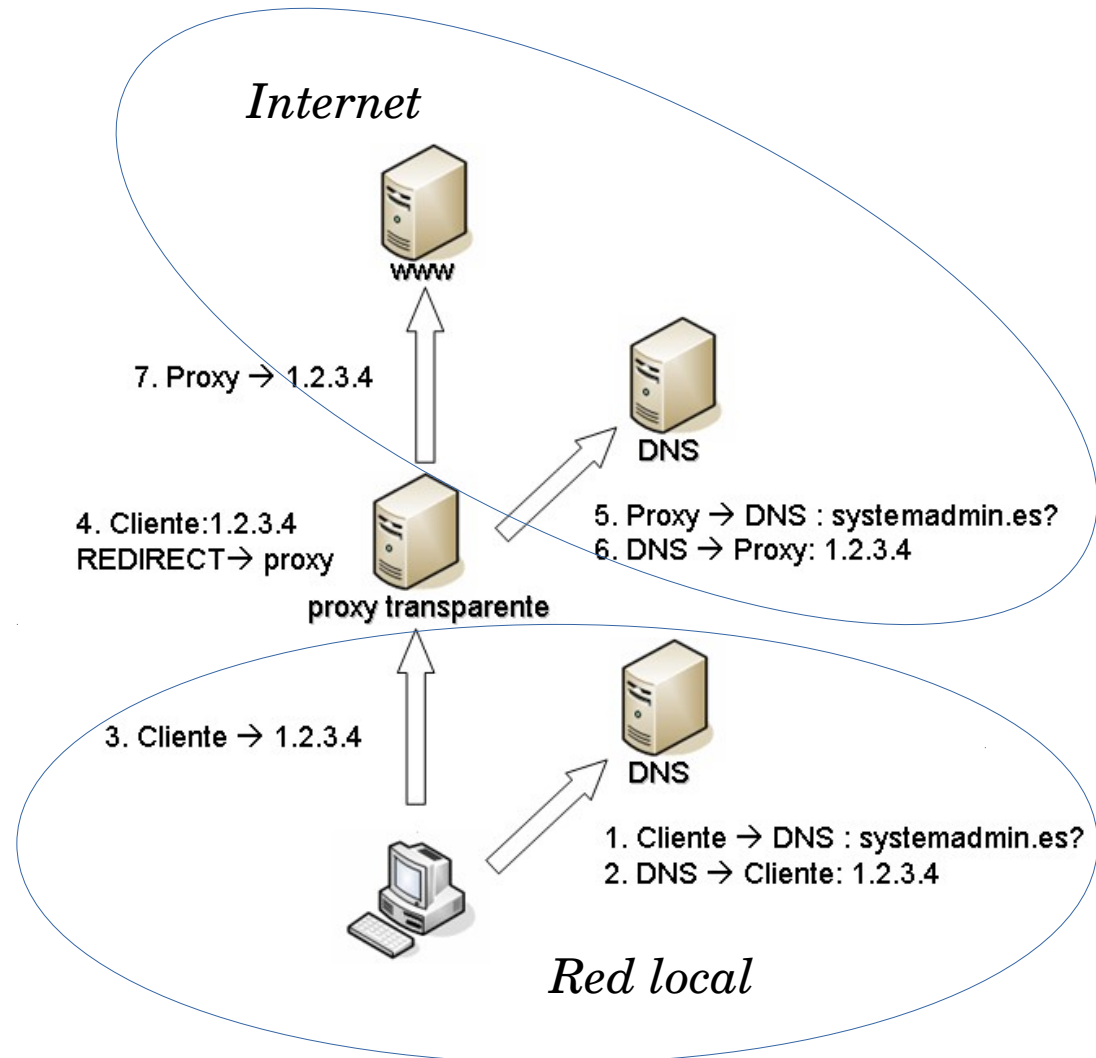
- Capaces de redirigir conexiones TCP (reenviando tramas).
- Se limitan a autenticar al usuario antes de establecer un circuito virtual entre sistemas.
 - No procesan o filtran paquetes en base al protocolo de nivel de aplicación.
- Sí traduce direcciones, por lo que enmascara direcciones.
- El host puede configurarse como pasarela "híbrida":
 - Servicios Proxy (nivel aplicación) en conexiones de entrada.
 - Funciones de nivel-circuito para conexiones de salida.



Proxy transparente



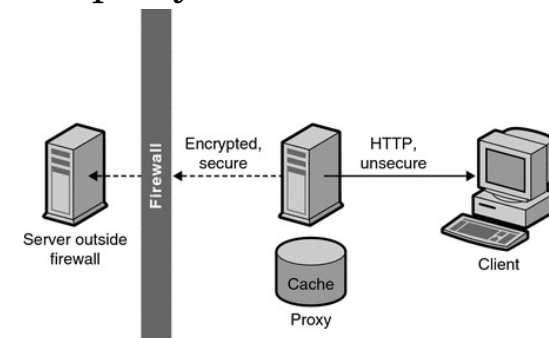
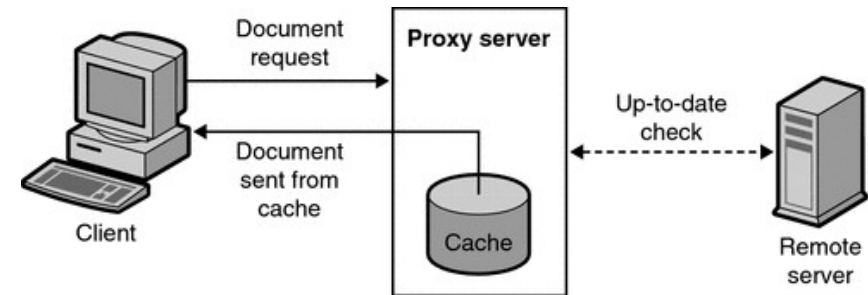
- No requiere clientes modificados para trabajar con proxies.
- Detecta que hay una petición a Internet y “la captura”.
- Es entonces el proxy el que se conecta e intercede.



Proxy caché



- Almacena la información durante un tiempo determinado para ofrecerla a un cliente que la solicite.
 - Si lo dispone en caché lo devuelve; si no dispone de ella o ha caducado, la solicita al servidor.
- Tiene sentido para servicios como web o FTP.
- Objetivos: Intentan mejorar la conectividad con el servicio:
 - Reducir la carga del servidor web
 - Reducir tráfico en la red
 - Reducir los tiempos de respuesta
- Diferencias con caché de cliente:
 - Se ubica en la red y es utilizada por múltiples usuarios.
 - Es necesario mantener consistencia entre caché local y caché del proxy. En web enviando un GET condicional
- Es posible crear jerarquías de proxies:
 - Crea múltiples capas de caché.





CONFIGURACIONES PROXY

Configuración del proxy en navegadores

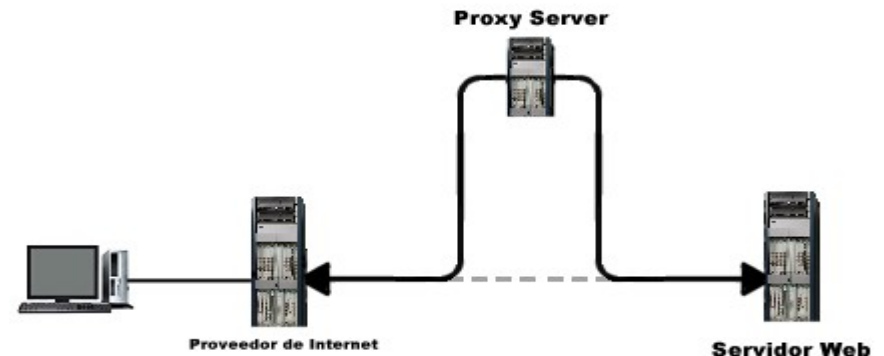


- Se indicará si se usa proxy o no.
- Se indicará si se detecta automáticamente o no.
- Se especifica la dirección IP y puerto del Proxy.
- Se suele usar un único puerto Proxy para todos los servicios:
 - No existe un puerto estándar. Los más usuales: 8000 y 8080.
- Configuración automática del Proxy:
 - Se usa un fichero de configuración con código JavaScript.
 - El fichero está en el servidor Proxy o en un servidor web.
 - Se especifica la URL de dicho fichero.
 - Ej: <http://proxy.uni.edu.pe>

Salida



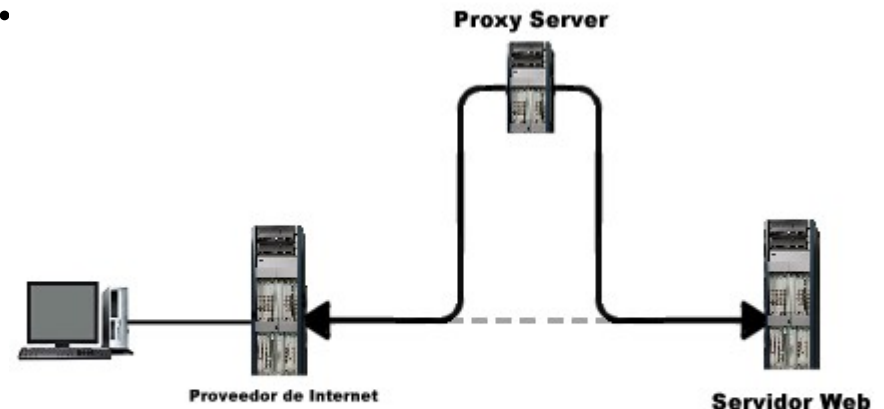
- El Proxy proporciona seguridad baja en conexiones salientes.
- Un host puede salir sin usar el Proxy.
- El router se encarga de la traducción de direcciones.
- El Proxy sólo sirve como caché.



Entrada



- El Proxy actúa como Proxy inverso.
- El router reenvía todas las conexiones entrantes al proxy.
- El Proxy realiza filtrado de paquetes.
- El Proxy actúa como caché.



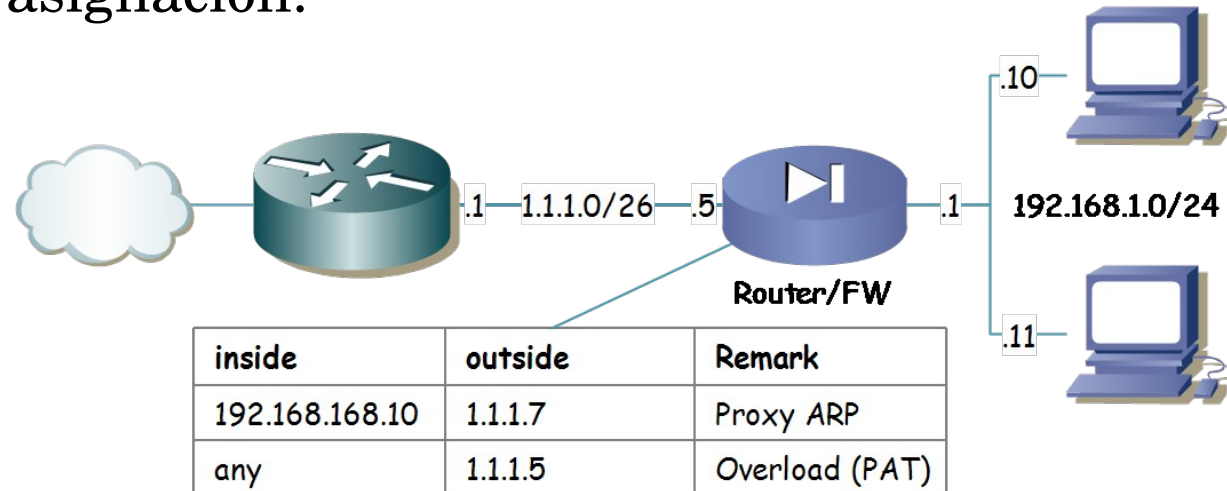


MASQUERADING EN PROXY

PAT



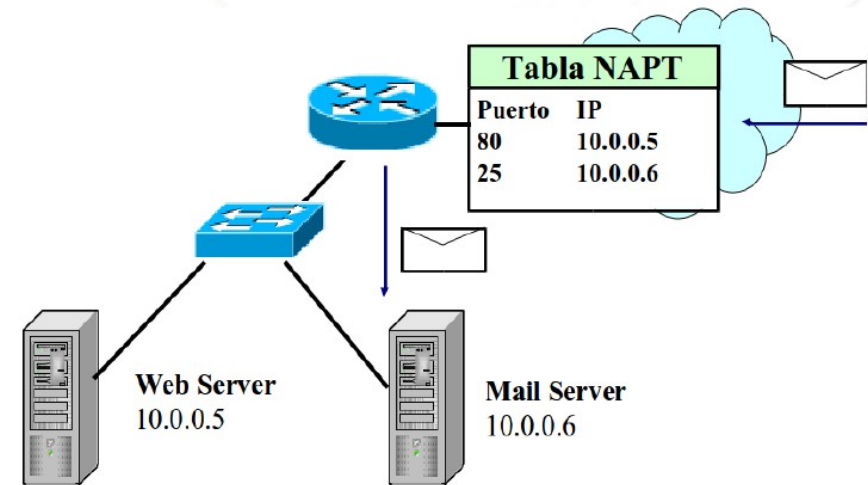
- Port Address Translation.
- Se mantiene una tabla de asignación:
 - IP original del paquete
 - IP traducida del paquete
 - IP destino
 - Puerto original del paquete
 - Puerto traducido
 - Puerto destino
 - Protocolo de transporte
 - Indicador de FIN
 - Temporizador
- Este proceso de traducción implica un alto rendimiento del router.



NAPT o IP masquerading



- También se le llama NAT inverso.
- Asociar un puerto de una IP pública con una IP privada.
- Tiene algunas asignaciones estáticas
 - Puerto 21 → redirige a servidor FTP interno
 - Puerto 80 → redirige a servidor WWW interno
- Funcionamiento (igual que PAT):
 - Paquete de salida:
 - Cambia la IP interna por IP oficial
 - Cambia puerto interno por puerto no usado del NAT
 - Paquete de entrada
 - Mira el puerto, si coincide con uno de la tabla:
 - Cambia IP oficial por IP interna
 - Cambia puerto NAT por puerto interno
 - Si no coincide: se rechaza la conexión



NAT Vs. Proxy



- La idea del NAT surge con el uso de los primeros Proxys.
- Un Proxy es una solución software que recibe peticiones del cliente solicitando información, se obtiene esa información y se le envía al cliente.
- Un Proxy puede ofertar servicios de navegación por Internet, así como también controlar los contenidos de navegación.
- Por otro lado el Proxy suele realizar también tareas de caché para facilitar el acceso a los contenidos.



SQUID

Definición



- Programa principal como servidor desarrollado para GNU/Linux confiable, robusto y versátil.
- Funciona como Servidor intermediario y caché de contenido de red.
- Squid versión 4.
 - Paquete: *squid*
 - Servicio: *service squid [action]*



Notas importantes



- Evitar dejar espacios en lugares indebidos.

```
# Opción incorrectamente habilitada.  
http_port 8080
```

```
# Opción correctamente habilitada.  
http_port 8080
```

- Archivo de configuración:
 - */etc/squid/squid.conf*
- Recomendaciones de configuración:
 - Al menos una Lista de Control de Acceso
 - Al menos una Regla de Control de Acceso
 - *http_port*
 - *cache_dir*
 - *error_directory*, sólo si va a personalizar mensajes de error.

Listas de control de acceso (ACL)



- Permite controlar el tráfico de los clientes hacia Internet
- Definen una red o bien ciertos anfitriones en particular.
- A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.


- Sintaxis:

- *acl [nombre de la lista] src [lo que compone a la lista]*

- Ejemplos:

- Determinada Red: *acl localnet src 172.16.100.0/28*

- Archivo ACL: *acl permitidos src "/etc/squid/listas/permitidos"*



```
172.16.100.1
172.16.100.2
172.16.100.3
172.16.100.15
172.16.100.16
172.16.100.20
172.16.100.40
```

Reglas de control de acceso



- Permite o deniega acceso hacia Squid.
- Deben colocarse en la sección de reglas de control de acceso definidas, a partir de:

```
#  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
#
```

- Sintaxis:
 - *http_access [deny o allow] [lista de control de acceso]*
- Para desactivar la configuración predeterminada y utilizar una diferente:

```
# Example rule allowing access from your local networks.  
# Adapt localnet in the ACL section to list your (internal) IP networks  
# from where browsing should be allowed  
# http_access allow localnet  
http_access allow localhost
```

- Regla que establece acceso permitido a la Lista de Control de Acceso denominada “permitidos”: `http_access allow permitidos`



Ejemplos

Reglas de control de acceso. Caso 1.



- Definir la red *172.16.100.0/28* como red local.

```
acl localnet src 172.16.100.0/28
```

- Listas de Control de Acceso: definición de una red local completa

```
# Recommended minimum configuration:  
acl all src 0.0.0.0/0  
acl manager proto cache_object  
acl localhost src 127.0.0.1/8  
acl localnet src 172.16.100.0/28
```

- Aplicar la regla de control de acceso:

```
http_access allow localnet
```

- Reglas de control de acceso: Acceso a una Lista de Control de Acceso.

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
#  
http_access allow localhost  
http_access allow localnet  
http_access deny all
```

Reglas de control de acceso. Caso 1.



- La regla *http_access allow localnet* permite el acceso a Squid a la Lista de Control de Acceso denominada *localnet*.
- En el siguiente ejemplo, está conformada por *172.16.100.0/28*.
- Cualquier anfitrión desde *172.16.100.1* hasta *172.16.100.14* podrá acceder a Squid.

Reglas de control de acceso. Caso 2.



- Archivo `/etc/squid/listas/localnet` que permitirá acceso a Squid a ciertas direcciones IP.

```
172.16.100.1
172.16.100.2
172.16.100.3
172.16.100.4
172.16.100.5
172.16.100.6
172.16.100.7
```

- Denominaremos a esta lista de control de acceso como *localnet*:

```
acl localnet src "/etc/squid/listas/localnet"
```

- Listas de Control de Acceso: definición de una red local completa

```
# Recommended minimum configuration:
acl all src 0.0.0.0/0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl localnet src "/etc/squid/listas/localnet"
```

- Aplicar la regla de control de acceso:

```
http_access allow localnet
```

- Reglas de control de acceso: Acceso a una Lista de Control de Acceso.

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow localnet
http_access deny all
```

Reglas de control de acceso. Caso 2.



- La regla *http_access allow localnet* permite el acceso a Squid a la Lista de Control de Acceso denominada localnet
- Está conformada por las direcciones IP especificadas en el archivo */etc/squid/listas/localnet*.
- Esto significa que cualquier anfitrión excluido del archivo */etc/squid/listas/localnet* se le denegará el acceso a Squid.



Algunas opciones importantes

Opción *cache_mgr*



- Enviará un mensaje de aviso a la cuenta webmaster del servidor.

```
cache_mgr joseperez@midominio.net
```

Opción *http_port*



- Indica el puerto a través del cual escuchará peticiones Squid. El valor predeterminado es 3128, es decir, Squid escuchará peticiones a través del puerto *3128/tcp*. `http_port 3128`
- El puerto estándar designado para servidores de caché de Internet (webcache) es el puerto 8080. `http_port 8080`
- La opción permite establecer también si se quiere utilizar una dirección IP en particular. Esto añade mayor seguridad al servicio, pues si se tienen dos tarjetas de red, una con una dirección IP pública y otra con una dirección IP privada, se puede establecer que Squid sólo permita conexiones desde la dirección IP privada.
`http_port 192.168.80.1:8080`
- Si se necesita configurar un servidor proxy en modo transparente, sólo es necesario añadir la opción ***intercept***, misma que desde la versión 3.1 de Squid reemplaza a la opción ***transparent***. `http_port 192.168.80.1:8080 intercept`

Opción *cache_dir*



- Establece que tamaño se desea que utilice Squid para almacenamiento de caché en el disco duro.

Predeterminado, crea en el directorio */var/spool/squid* un caché de 100 MB, dividido en jerarquías de 16 directorios subordinados, hasta 256 niveles cada uno:

```
cache_dir ufs /var/spool/squid 100 16 256
```

- Incrementar el tamaño del caché hasta donde lo desee el administrador. Más objetos se almacenarán en éste y por lo tanto se consumirá menos el ancho de banda.

2GB por ejemplo:

```
cache_dir ufs /var/spool/squid 2048 16 256
```


Opción

maximum_object_size



- Define el tamaño máximo de los objetos en el caché.
- Se recomienda establecerla en escenarios con alta carga de trabajo
 - Evita desperdiciar recursos de sistema almacenando en el caché objetos de gran tamaño que probablemente sólo sean aprovechados por unos pocos usuarios
 - Optimizando el uso del caché con objetos pequeños.

```
maximum_object_size 48 MB
```



Restricción de accesos

Por expresiones regulares (I)



- Se debe crear un archivo donde se definirá la lista de expresiones regulares en un fichero. Por ejemplo en *“/etc/squid/listas/expreg-denegadas”*.

- Ejemplo de lista:

```
adult
celebri
mp3
otrositioindeseable.com
playstation
porn
sex
sitioindeseable.com
taringa
torrent
warez
wii
```

- Añadir en */etc/squid/squid.conf* la lista anterior

```
acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"
```

Por expresiones regulares



- Siempre se tiene que crear un fichero, ya sean dominios, extensiones de archivos, expresiones, etc; y/o simplemente para permitir o denegar
- Se debe crear un archivo donde se definirá la lista de expresiones regulares en un fichero. Por ejemplo en “*/etc/squid/listas/expreg-denegadas*”.

- Ejemplo de lista:

```
adult
celebri
mp3
otrositioindeseable.com
playstation
porn
sex
sitioindeseable.com
taringa
torrent
warez
wii
```

- Añadir en */etc/squid/squid.conf* la lista anterior

```
acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"
```