

LINUX

A UN CLIC



ANTES DE EMPEZAR

**“Cualquier tecnología suficientemente avanzada es
equivalente a la magia.”**

ARTHUR C. CLARKE



AGENDA

- CONCEPTUALIZACION: **PROXY**
- CONCEPTUALIZACION: **DENEGACION**
- CONCEPTUALIZACION: **DETECCION DE INTRUSOS**
- **RETO**



CONFIGURACION DE PROXY

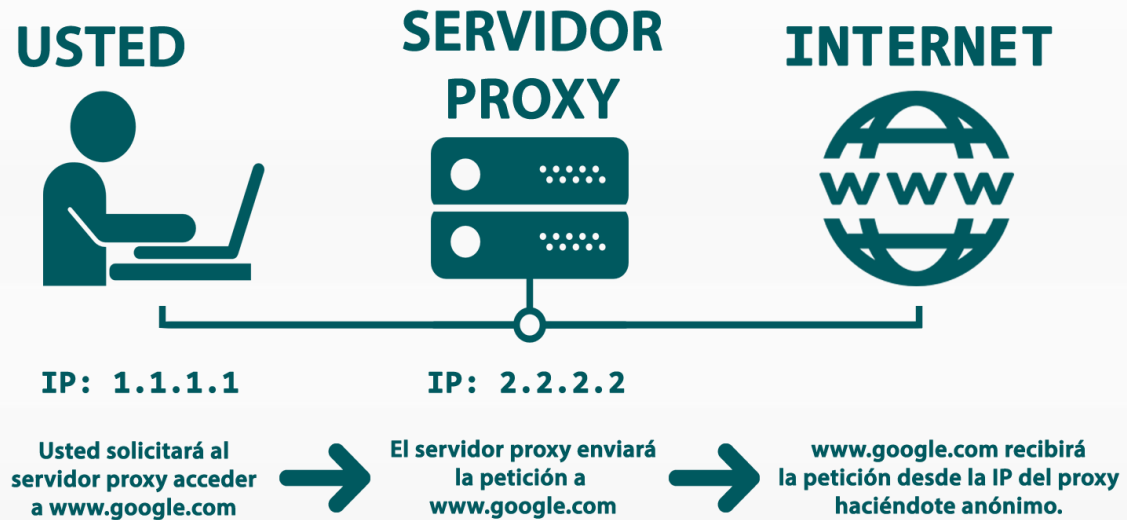
PROXY

Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).



CONFIGURACION DE PROXY

PROXY



CONFIGURACION DE PROXY

CARACTERISTICAS

- Comúnmente un servidor proxy, es un equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino.
- El más popular es el servidor proxy de web. Interviene en la navegación por la web, con distintos fines: seguridad, rendimiento, anonimato, etc.



CONFIGURACION DE PROXY

CARACTERISTICAS

- Existen proxys específicos para otros protocolos, como el proxy de FTP.
- El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.



CONFIGURACION DE PROXY

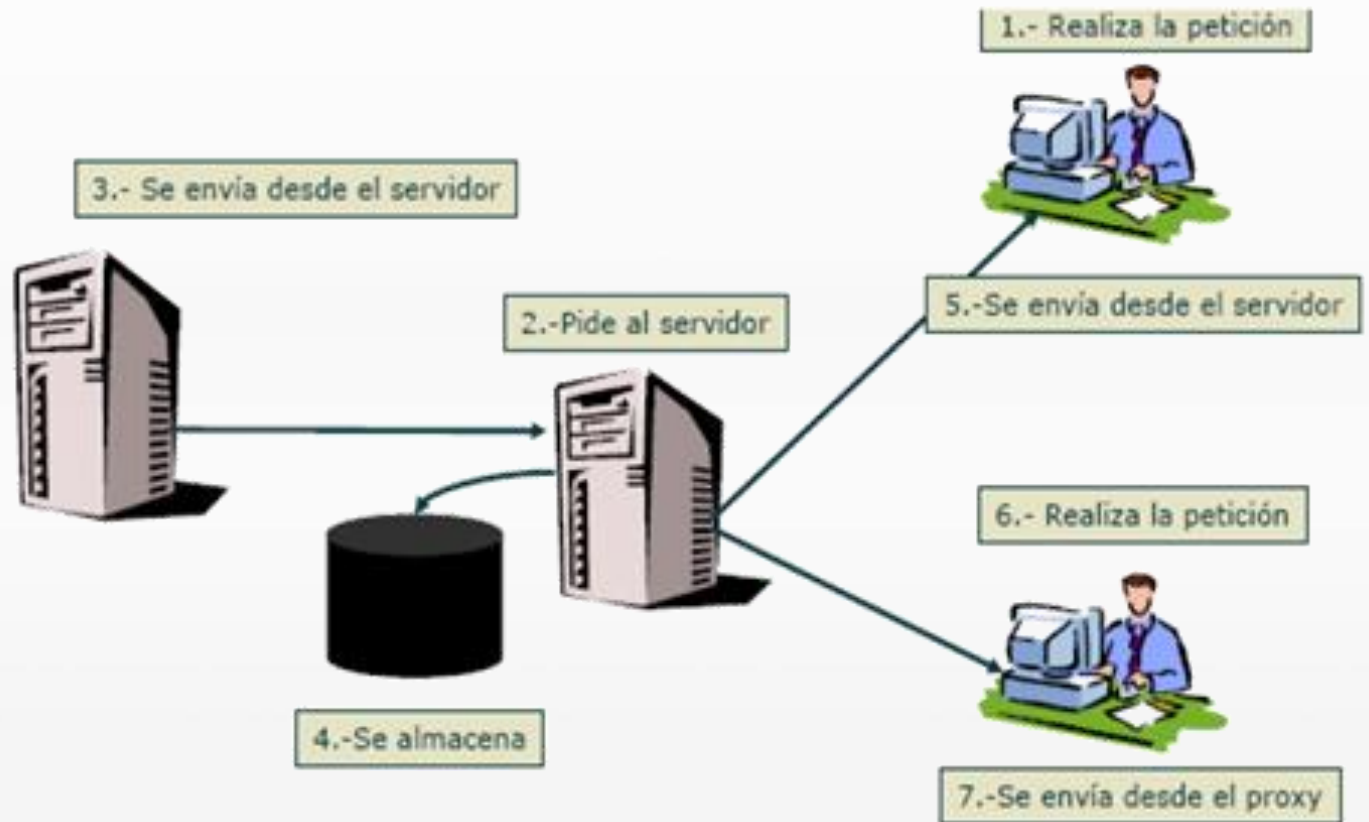
CARACTERISTICAS

- Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.
- Un componente hardware también puede actuar como intermediario para otros.



CONFIGURACION DE PROXY

CARACTERISTICAS



CONFIGURACION DE PROXY

TIPOS DE PROXY

- Proxy local
- Proxy de red o proxy externo



CONFIGURACION DE PROXY

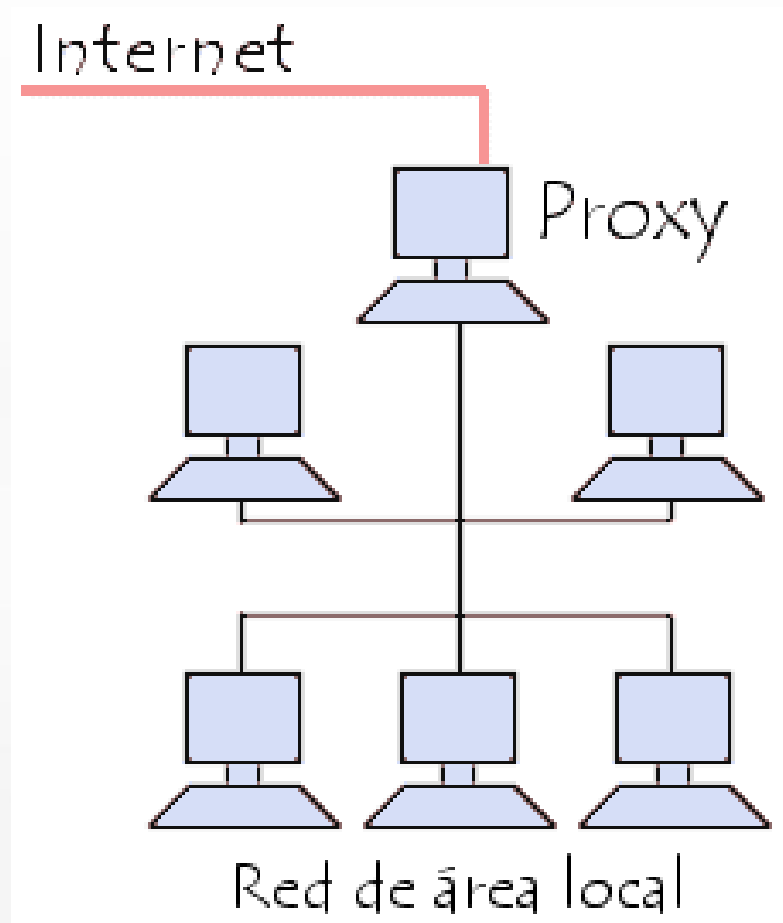
TIPOS DE PROXY

Proxy Local: En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).



CONFIGURACION DE PROXY

TIPOS DE PROXY



CONFIGURACION DE PROXY

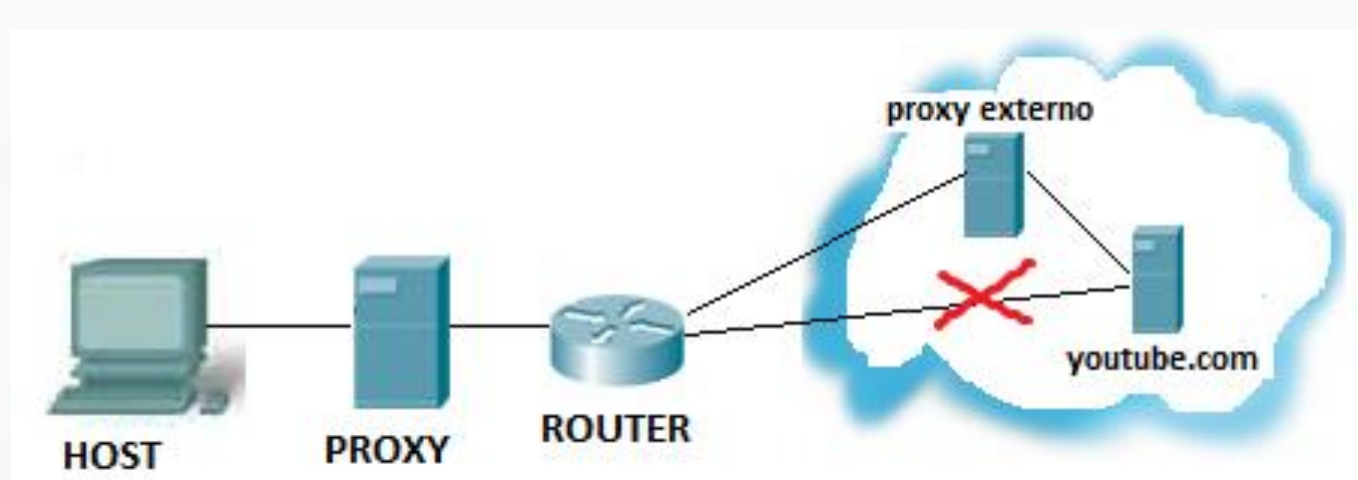
TIPOS DE PROXY

PROXY EXTERNO: El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc



CONFIGURACION DE PROXY

TIPOS DE PROXY



CONFIGURACION DE PROXY

VENTAJAS

- **CONTROL:** solamente el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos únicamente al servidor proxy.
- **AHORRO:** solamente uno de los usuarios (el proxy) ha de estar preparado para hacer el trabajo real. Con estar preparado significa que es el único que necesita los recursos necesarios para hacer esa funcionalidad. Ejemplos de recursos necesarios para hacer la función pueden ser la capacidad y lógica de la dirección de red externa (IP).



CONFIGURACION DE PROXY

VENTAJAS

- **VELOCIDAD:** si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: 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.



CONFIGURACION DE PROXY

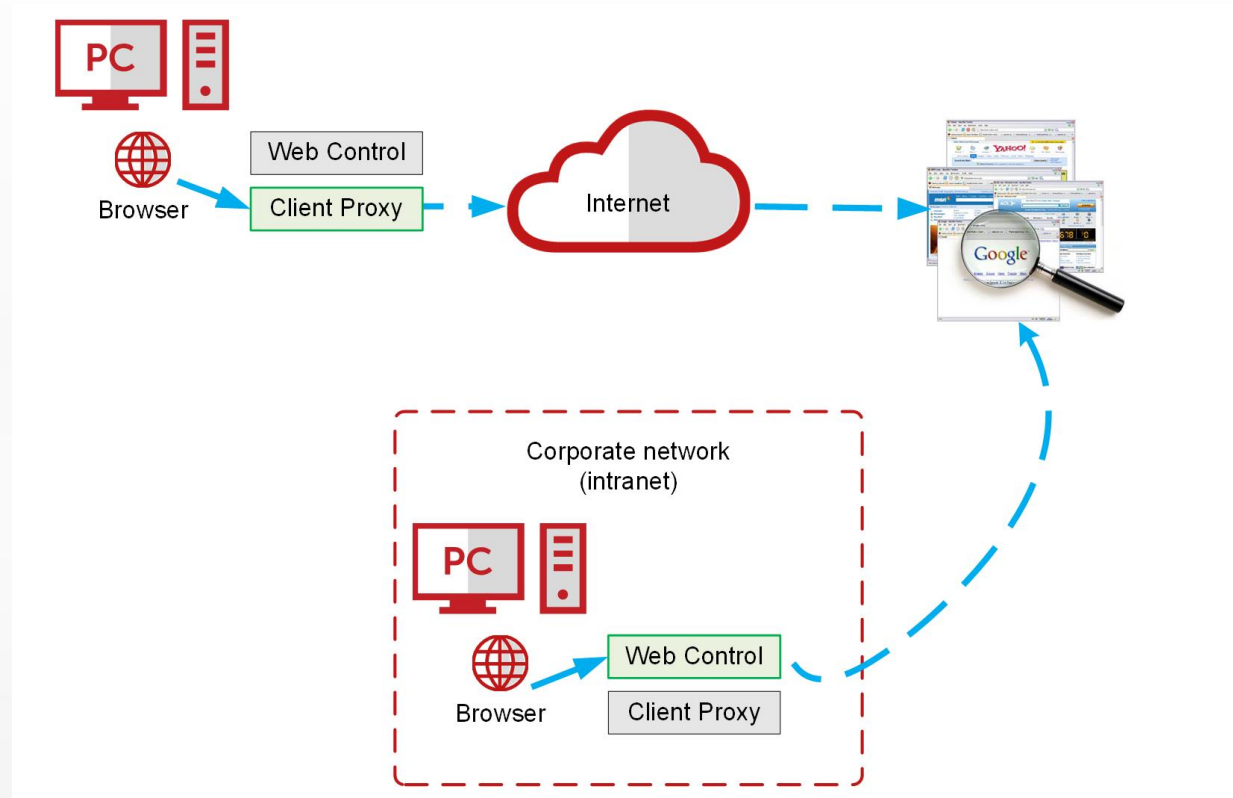
VENTAJAS

- **MODIFICACIÓN:** como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- **CONECTARTE** de forma segura sin dar tu IP.



CONFIGURACION DE PROXY

VENTAJAS



CONFIGURACION DE PROXY

DESVENTAJAS

ANONIMATO: si todos los usuarios se identifican como uno solo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

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.



CONFIGURACION DE PROXY

DESVENTAJAS

CARGA: un proxy tiene que 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.



CONFIGURACION DE PROXY

DESVENTAJAS

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).

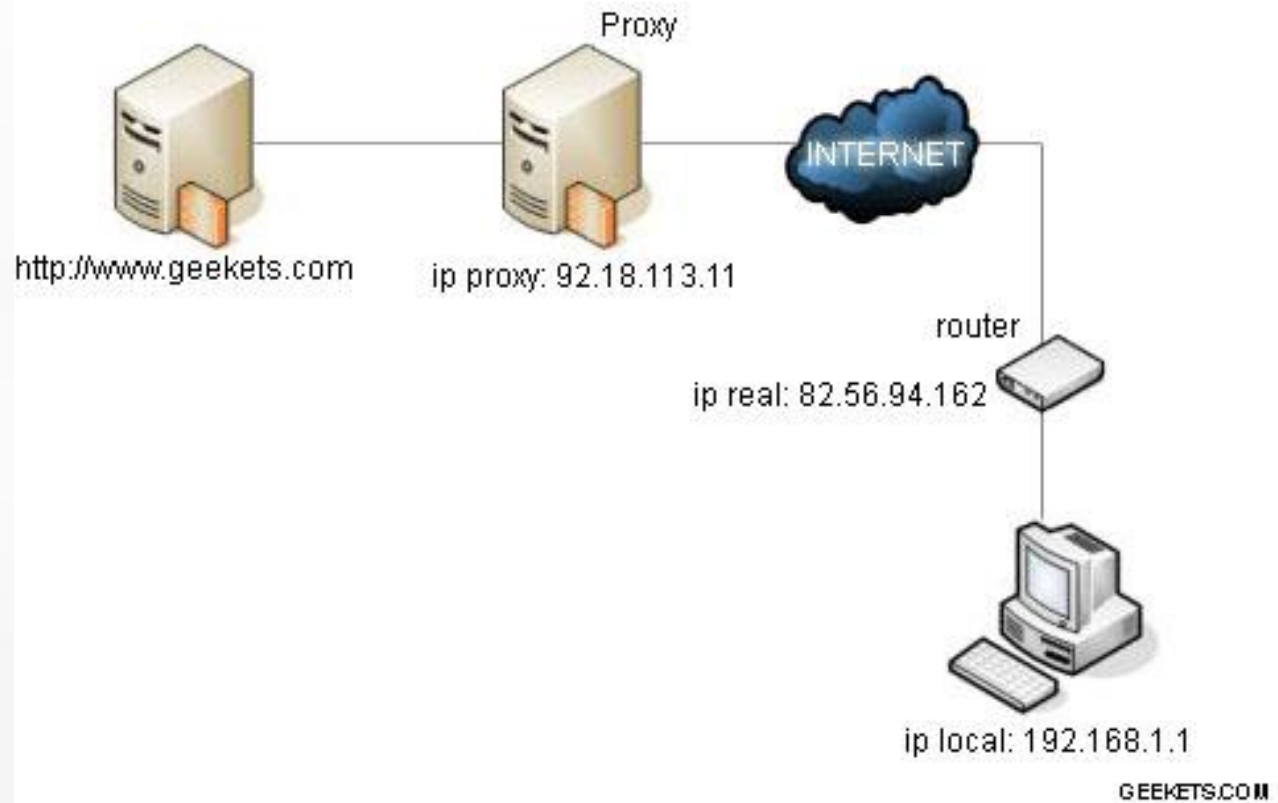
INCOHERENCIA: si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.



CONFIGURACION DE PROXY

DESVENTAJAS

CONEXION MEDIANTE PROXY



CONFIGURACION DE PROXY

APLICACION

- PROXY CACHE
- PROXY WEB



CONFIGURACION DE PROXY

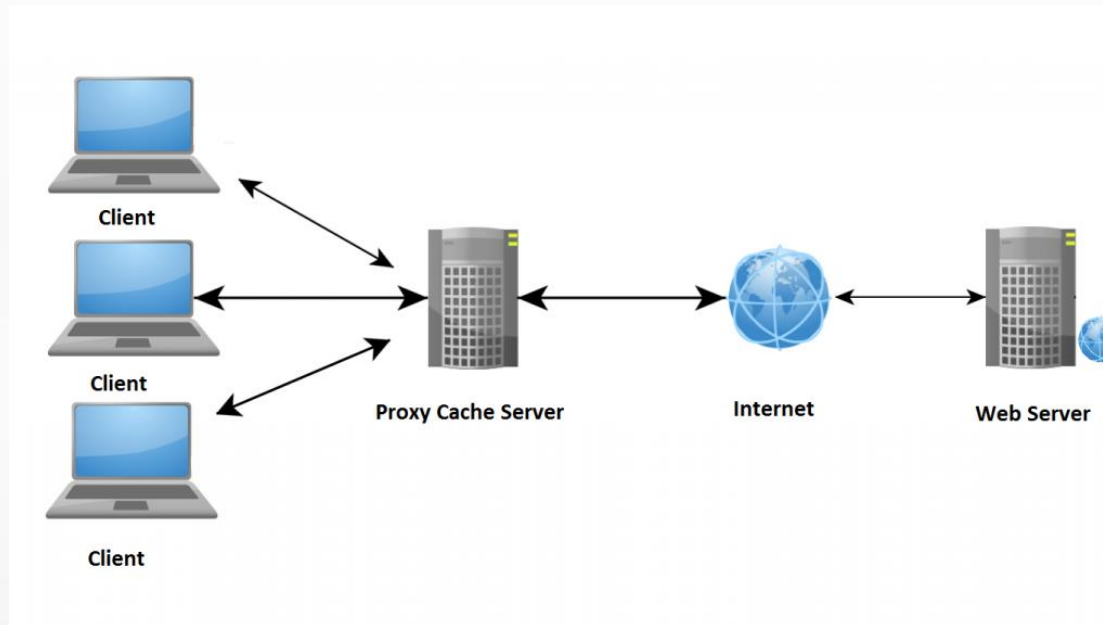
APLICACION

PROXY CACHE: Conserva el contenido solicitado por el usuario para acelerar la respuesta en futuras peticiones de la misma información de la misma máquina u otras. Habitualmente se trata de proxys HTTP/HTTPS accediendo a contenido web. Esta función es especialmente necesaria en redes con acceso precario a Internet, aunque los usuarios lo perciban a menudo como una intromisión que limita su privacidad frente a conexiones individuales directas.



CONFIGURACION DE PROXY

APLICACION



CONFIGURACION DE PROXY

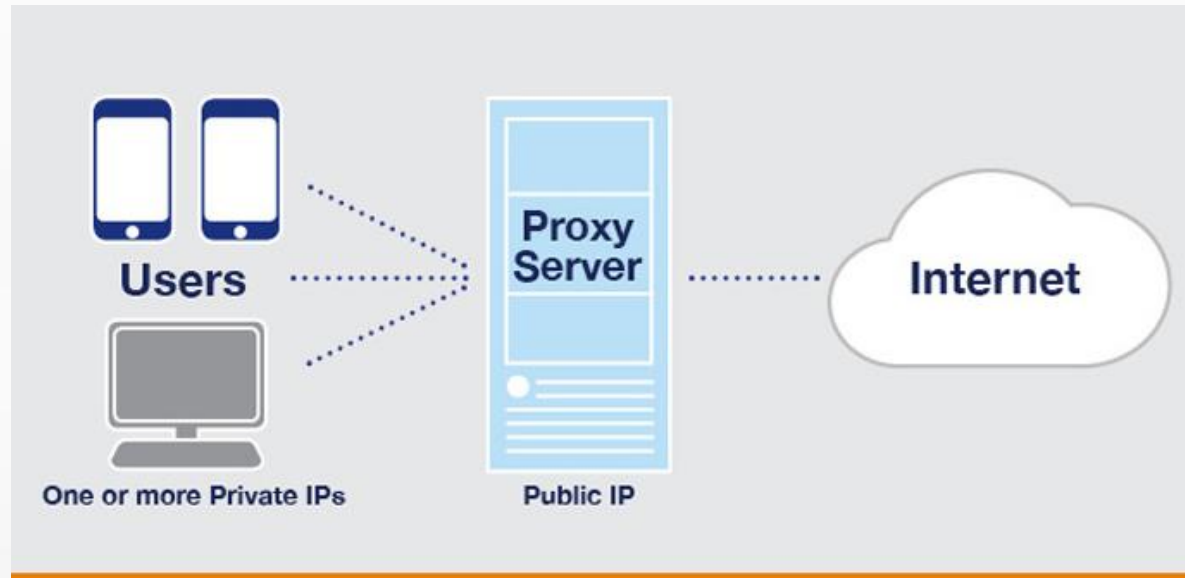
APLICACION

PROXY WEB: Se trata de un proxy para una aplicación específica: el acceso a la web con los protocolos HTTP y HTTPS, y accesoriamente FTP. Aparte de la utilidad general de un proxy puede proporcionar una caché compartida para las páginas web y contenidos descargados, actuando entonces como servidor proxy-caché. Esta caché es compartida por múltiples usuarios con la consiguiente mejora en los tiempos de acceso para consultas coincidentes y liberando de carga a los enlaces de acceso a Internet.



CONFIGURACION DE PROXY

APLICACION



CONFIGURACION DE PROXY

```
$ sudo apt update  
$ sudo apt install squid
```

```
http_port 3128
```

```
$ sudo service squid restart
```

```
/etc/squid/squid.conf
```

```
acl blocksite1 dstdomain yahoo.com  
acl blocksite2 dstdomain www.rediff.com  
http_access deny blocksite1  
http_access deny blocksite2
```



CONFIGURACION DE PROXY

RETO

**VALIDACION – CONFIGURACION E
IMPLEMENTACION DE UN PROXY**



SEGURIDAD KALI

DISTRIBUCION KALI

Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.



SEGURIDAD KALI

DISTRIBUCION KALI

<https://www.kali.org/downloads/>

<https://docs.kali.org/general-use/kali-linux-virtual-box-guest>



CONFIGURACION DE KALI

RETO

INTERACTUA EN KALI

“toor”



¿PREGUNTAS?



GRACIAS

