TEMA

Tema 10. Proxy

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 10: Proxy

¿Qué aprenderás?

- Cuál es la diferencia en Proxy y cortafuegos
- Pará qué se usa un Proxy
- Cómo se combina el Proxy y la VPN
- ¿Qué es la red TOR?

¿Sabías que…?

- Cada vez más usuarios prefieren navegar de manera anónima por la red.

9.1. INTRODUCCIÓN

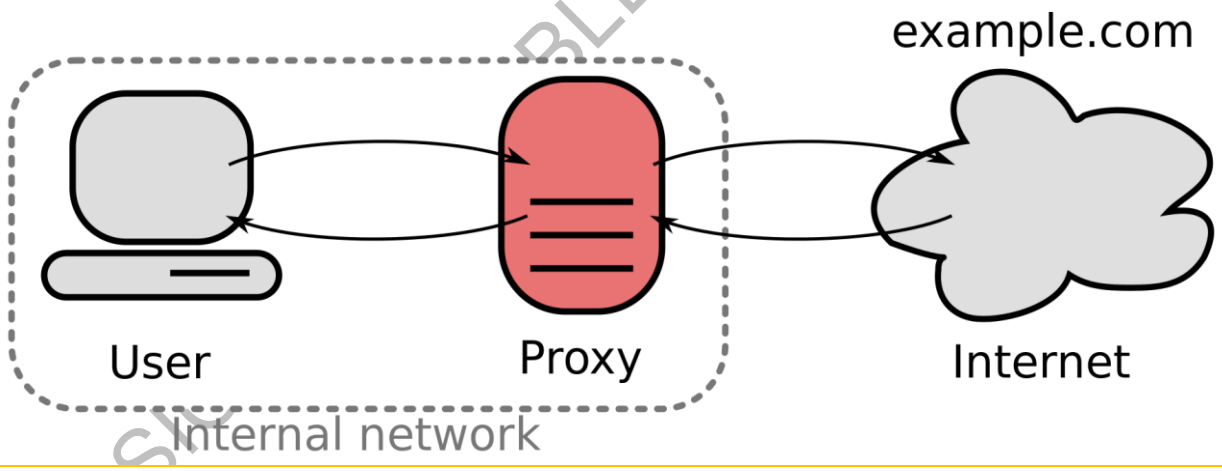
Continuamos con los elementos más importantes de la seguridad perimetral.

Vamos a tratar uno de los que más auge está teniendo en la actualidad, pero no con el uso que se le otorgó cuando se diseñó.

Hablaremos de un dispositivo que podría entrar dentro de la clasificación de cortafuegos, como hemos visto en el tema anterior, pero que como trabaja en un rango tan específico como es la capa de aplicación y realiza unas funciones que no se asignan al resto de cortafuegos, tiene su personalidad propia.

9.1.1. DEFINICIÓN

Un **Proxy** o servidor intermediario, actúa como un representante de otro programa. Me explico, el Proxy recibe la petición de un equipo de una red interna. La revisa, la acepta y este, en su nombre, realiza la petición a Internet. Desde Internet recibe la respuesta a la petición, pero sin saber que se la ha hecho el equipo de la red interna y la retransmite al equipo de la red interna.

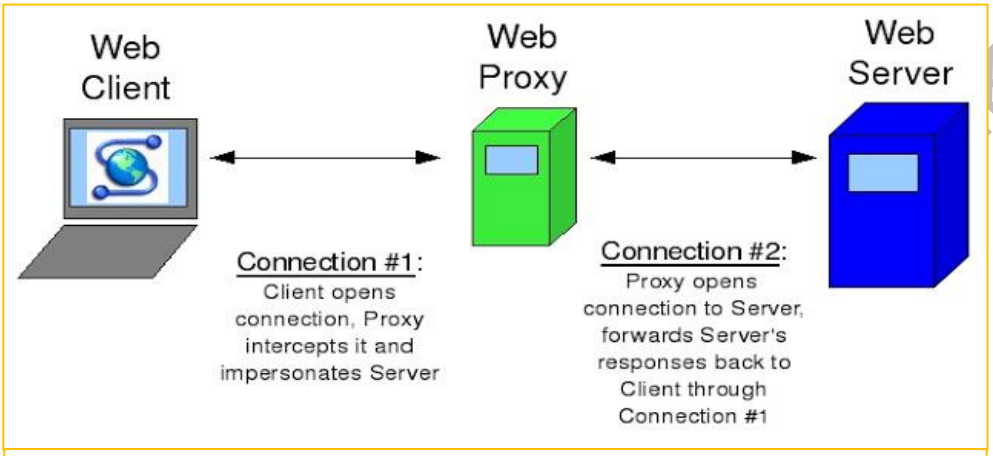


Un ejemplo de esto es un aula de una escuela donde solo tenemos un equipo conectado a Internet. Instalamos un servidor proxy en ese equipo y proporcionamos acceso a Internet a los equipos del aula.

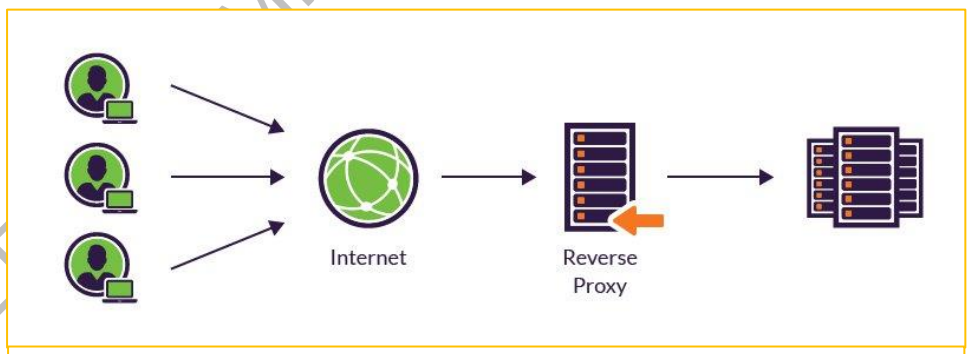
9.2. CLASIFICACIÓN DE PROXY

Clasificaremos los Proxy según su función en:

- **Caché** o Web: Este proxy almacena todas las páginas que se han visitado en su caché. Su objetivo es que cuando volvamos a visitarlas, no descargarlas otra vez, sino transmitir la que tiene almacenada. Esto nos permite un aumento importante de velocidad en la respuesta, además de un ahorro de tráfico. Lógicamente, tiene un sistema de actualización de los contenidos.



- **NAT**: Ofrece el Servicio NAT.
- **Transparente**: Este proxy es una combinación de Web más NAT
- **Anónimo**: Los veremos más adelante
- **Reverso o Inverso**: Este proxy se encarga de gestionar las peticiones que recibe nuestra red interna y que no son una respuesta a una petición que se ha realizado de esta



9.3. VENTAJAS DEL PROXY

- Los usuarios no se conectan al router sino al proxy, por lo que aumenta la seguridad
- Las páginas que se visitan se cachean en la memoria temporal, por lo que el acceso es más eficaz
- Permite crear una lista de URL's prohibidas
- Permite crear una lista de palabras prohibidas en las URL's
- Gestiona el acceso a subredes o equipos concretos
- Genera informes de todas las conexiones que hacen los usuarios
- Ante ataques externos el proxy hace de barrera
- Gestiona el acceso de los usuarios
- Se puede combinar perfectamente con un cortafuegos y con servidores web

9.4. INCONVENIENTES DEL PROXY

- Cada aplicación que tenga que conectarse a internet a través del proxy, deberá estar configurada para ello
- En caso de fallo en el proxy, toda la red se queda sin acceso a internet
- Ante un exceso de demanda, el proxy ralentizará el proceso o se colapsará
- El acceso a través de proxy no nos permite el control de puertos o protocolos
- El almacenamiento de las páginas puede incumplir la LOPD
- Puede ser utilizado para realizar ataques a redes

9.5. EL PROXY ANÓNIMO

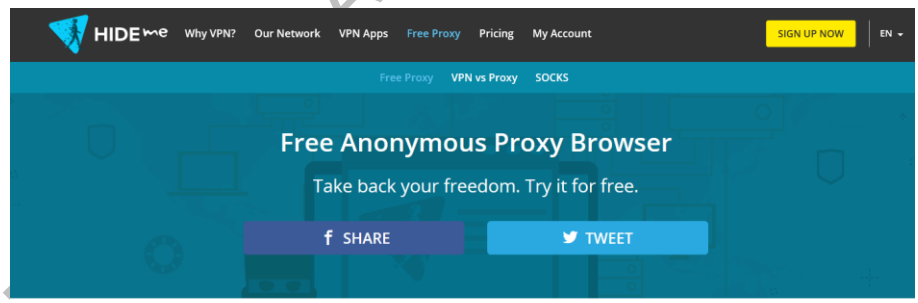
Vamos a realizar una reflexión. Todos los dispositivos que se conectan a Internet tienen una IP y un puerto. El proxy permite conectarnos a Internet a través de él, pero no con la IP que tenemos asignada en la red interna. Esa es su función original, pero ¿qué pasaría si en vez de conectarme a través de una IP de una red interna me conectase a través de una IP pública, la que me asigna la compañía de teléfono? Pues nada. El proxy haría su trabajo.

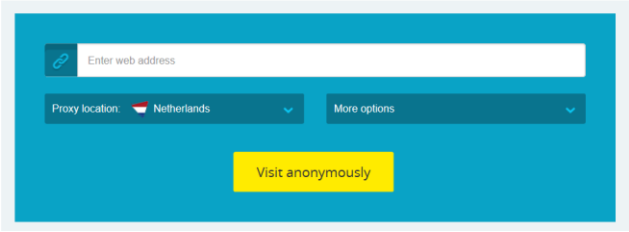
Con esta herramienta estamos consiguiente privacidad en la red, pues el destinatario no sabe desde qué parte del mundo nos estamos conectando.

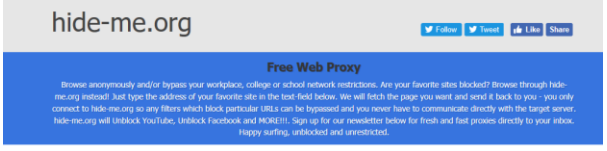
La clave estaba en conseguir un proxy que no estuviera en mi empresa, pues me podrían localizar. Pues los hay, y podemos acceder a ellos.

9.5.1. Los mejores proxy gratis

- Hidester
- Hide My Ass
- Hide Me
- Proxy Free
- Proxy Site
- VPN Book
- Cyberghost
- Kproxy
- Filter
- Hide
- Hideoxy
- Anonymouse
- Ninja
- New IP
- Web Proxy
- 4Ever
- Just Proxy
- Fast USA
- Site2
- Incloak
- UsWeb
- NNTime
- Uas
- Blew







- ChangeMyIP
- Don't Filter
- RX Proxy
- Bind
- You Hide
- Unblock
- Yellow

Dentro de este tipo de proxy anónimo nos encontramos con:

- **Públicos**: Son de "alguien" tan bueno tan bueno que nos permite utilizarlo. Pero claro, toda tu actividad quedará monitorizada sin que sepamos para qué
- **Semipúblicos**: Son Proxies públicos pero que utilizan un tipo limitado de usuarios. Son las que usan los SEO o particulares para acceder a servicios web de otros países y que requieren darse de alta
- **Privados**: Los que usas tú y nadie más. Se puede pagar por uno y no es caro

El siguiente paso es el nivel película de Hackers de alto nivel, enlazar Proxis para que sea más complicado localizarme.

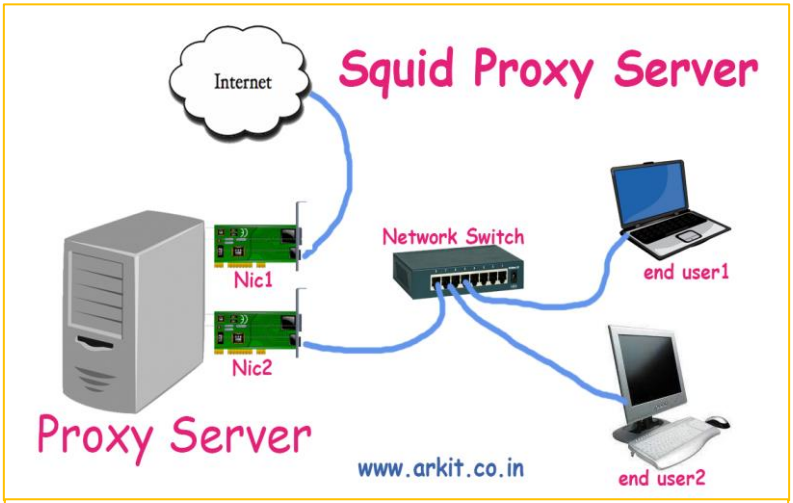
9.6. EL PROXY SQUID

Hablar de Proxy significa hablar de Squid.

Squid es un servidor intermediario de alto nivel que funciona en sistemas operativos GNU/Linux y desarrollado como software libre.

Puntos para tener en cuenta:

- Trabaja por defecto con el puerto 3128 (otros con los que se suele trabajar con 80, 8000 y 8080)
- No trabaja con SMTP, POP3, TELNET, SSH, IRC… solo con HTTP, HTTPS, FTP…
- Permite crear un árbol de servidores proxy
- Al soportar HTTPS permite la transmisión de comunicación encriptada
- Hace caché de peticiones DNS



9.6.1. INSTALACIÓN Y CONFIGURACIÓN

Como siempre, recomiendo revisar la documentación sobre cómo instalar la versión que se va a instalar (README o INSTALL), por si acaso.

1- Instalamos el paquete:

```
apt-get install squid
```

2- Arrancamos el proxy

```
/etc/init.d/squid start
```

3- Abrimos el fichero de configuracion:

```
sudo nano /etc/squid/squid.conf
```

Nos encontraremos con la siguiente estructura aproximadamente:

```
http_port
cache_mem
cache_dir
ftp_user
Listas de Control de Acceso (ACL)
....
```

Vamos revisar estos parámetros importantes:

http_port 3128	Este es el puerto de escucha por defecto. Lo podemos cambiar.
cache_mem 16 MB	Es la cantidad de memoria que utilizará para el tránsito de peticiones
cache_dir ufs /var/spool/squid 700 16 256	Memoria cache en el disco duro de 700 MB con una estructura de 16 directorios con 256 subdirectorios
ftp_user computer@gmail.com	Clave de acceso para conectarnos a ftp anónimo

9.6.2. Controles de Acceso (ACL)

Son equivalentes a las reglas de IPTABLE y gestionan el acceso a Squid.

Con los ejemplos siguientes entenderás mejor su funcionamiento.

- Con esta lista asocio todas las direcciones IP de una red a un nombre

```
acl redinterna1 src 192.168.100.0/255.255.255.0
```

Ahora añadiré las reglas que deben cumplir:

```
http_access allow redinterna1
```

- Ahora creo un archivo de texto que contenga las direcciones de esa red que quiero que no tengan acceso al proxy:

```
sudo nano /etc/squid/permitidos
```

Y escribo:

```
192.168.100.2
192.168.100.3
192.168.100.4
```

Y ahora genero una lista con la regla que les deniega el acceso

```
acl permitidos src "/etc/squid/permitidos"
http_access deny permitidos
```

- También podemos denegar acceso a varias acl's
-

```
http_access deny lista1 !lista2
```

Aquí tenéis un **ejemplo**:

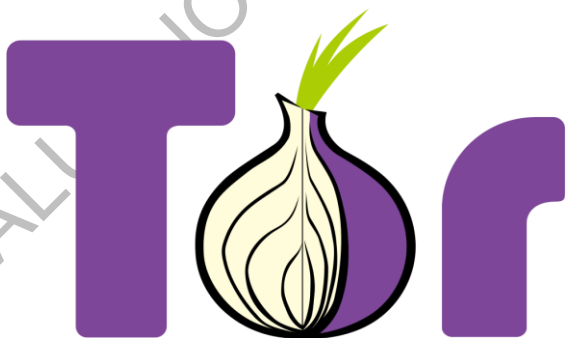
Deniega el acceso a Squid al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas. Para el resto de los equipos permitir el acceso sólo en horario de 10:00 a 14:00 horas. Se supone que los equipos pertenecen a la red 192.168.1.0 con máscara 255.255.255.0.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl red_local src 192.168.1.0/255.255.255.0.
acl equipo5 src 192.168.1.5
acl horario1 18:00-21:00
acl horario2 10:00-14:00
http_access deny equipo5 horario
http_access allow red_local horario
http_access deny all
```

9.6.3. Modos de autenticación en un proxy

- **Autenticación transparente:** Cuando un usuario realiza una petición para un sitio web, la misma se redirige automáticamente al proxy, que aplica las ACL. Si se permite el sitio, el sitio se muestra y sino, se muestra en el navegador un mensaje informativo. Para ello debe configurarse en el cortafuegos el reenvío
- **Autenticación manual**: Se usa junto a la transparente y consiste en configurar los navegadores para que el servicio se dirija directamente al proxy
- **Autenticación automática**: El cliente busca en el DNS o DHCP el fichero wpad.dat. Este fichero tiene toda la información para configurar el navegador

9.7. LA RED TOR



Esta foto de Autor desconocido está bajo

Tor (The Onion Router), es una herramienta excelente para navegar y realizar descargas de manera anónima, con o sin una VPN.

Tor crea una red totalmente cifrada de usuarios que comparten su ancho de banda y dirección IP unos con otros y contribuyen con su potencia computacional para mantener la totalidad de la red cifrada. Se modifican tanto la dirección IP de origen como la mac, ubicación, identidad, etc.

Se puede combinar con una VPN para ofrecer otra capa de privacidad y anonimato para consumir o publicar contenido sensible.

Para conectarse a esta red solo hay que descargarse el navegador web: **Tor Browser Bundle**.

9.7.1. ¿ES PELIGROSA LA RED TOR?

La red Tor por sí misma no es peligrosa, pues trabaja con los servidores web convencionales. Lo que hay que tener más cuidado dentro de Tor es con la Deep Web.

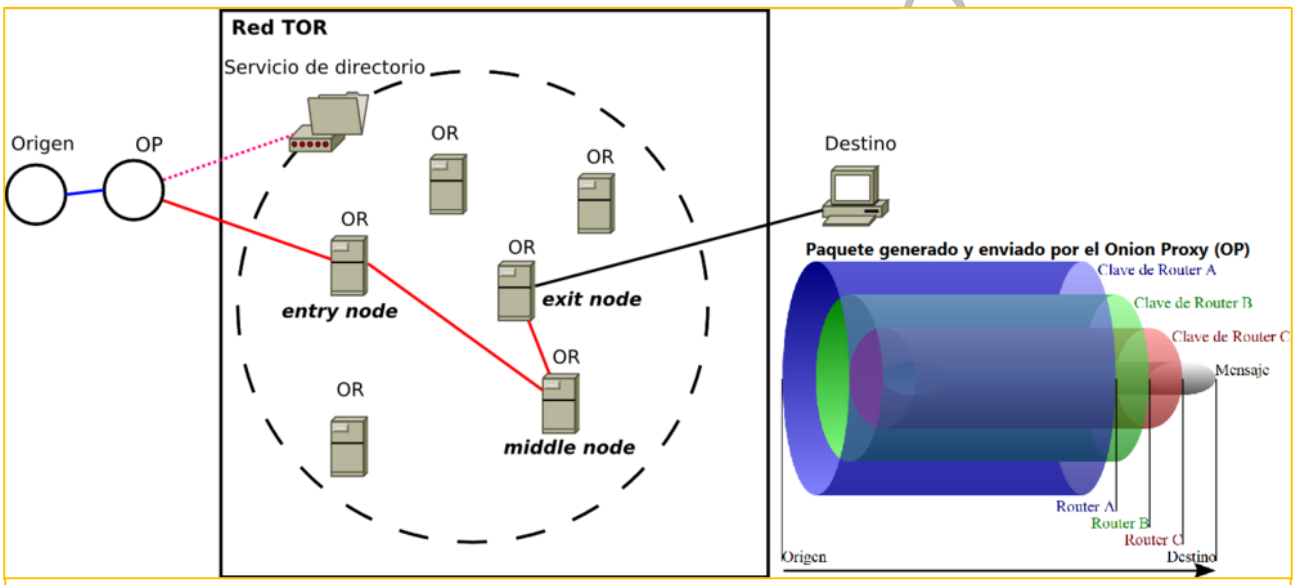
La **Deep Web (Web profunda**), es un conjunto de servidores que no aparecen en los buscadores y que los usuarios tienen memorizadas. Las URL están almacenadas de manera cifrada y solo se entra a través de la Red Tor.

9.7.2. ¿Cómo funciona esta Red Tor?

Imagina que eres el equipo A y quieres visitar una web de un servidor. La forma normal es ir directamente. Del equipo A a tu router, de ahí a ti ISP y directos al servidor web que almacena la página. Pero claro, todo este camino deja rastro, no es seguro y siempre estas localizado.

Pues nada, tengo un grupo de amigos que compartimos nuestros equipos y trabajamos con claves asimétricas. Cuando quiero visita una web voy al equipo B, después al equipo D, después al equipo BB, y así, aleatoriamente. En cada paso por un equipo, añado un cifrado simétrico con la clave pública de cada uno de ellos. Cuando llego al servidor web y responde, equipo a equipo, vamos desencriptando el paquete hasta que vuelve a mí.

Las información de esa red es claramente ilegal y solo entrar no solo nos puede infectar de cosas muy malas, sino que podemos estar inspeccionados por gobiernos u otras entidades.



Respondiendo a uno de los planteamientos iniciales, si quiero navegar de manera anónima por contenidos “legales”, el orden de elección sería: VPN, Proxy, TOR.

Recursos y enlaces

Servidor Cortafuegos-Proxy Linux. pfSense

Objetivo: En esta práctica vamos a instalar el servidor pfSense y realizamos una configuración del mismo.

La máquina dispone de dos tarjetas, una que se conecta a Internet y otra que se conecta la red Interna.

- https://youtu.be/rTM9M6WqxD8

- Proxy Squid http://www.squid-cache.org/

- Navegador TOR https://securityinabox.org/es/guide/torbrowser/windows/

- TOR Project https://www.torproject.org/

Test de autoevaluación

Quiero organizar un curso y que los alumnos naveguen por un listado de páginas web lo más rápidamente posible. ¿Qué tipo de Proxy me recomiendas?

a) Intermediario
b) Caché
c) NAT
d) Inverso

Resulta que en aula del curso me encuentro con único punto de acceso a internet. ¿Qué tipo de Proxy me recomiendas para que todos tengan acceso a Internet?

a) Intermediario
b) Caché
c) NAT
d) Inverso

He instalado en mi Ubuntu Server el proxy Squid. ¿Qué servicio podré filtrar?

a) Web
b) Correo
c) Telnet
d) IRC

Indica la ACL que permitirá a los ordenadores de mis alumnos conectarse a Internet de 8:00 a 14:00 h

e) acl alumnos src 192.168.100.0/255.255.255.0
f) acl horario 8:00 – 14:00
g) acl deny alumnos horario
h) acl allow alumnos horario

SOLUCIONARIOS

Test de autoevaluación tema 10

Quiero organizar un curso y que los alumnos naveguen por un listado de páginas web lo más rápidamente posible. ¿Qué tipo de Proxy me recomiendas?

a) Intermediario

b) Caché

c) NAT

d) Inverso

Resulta que en aula del curso me encuentro con único punto de acceso a internet. ¿Qué tipo de Proxy me recomiendas para que todos tengan acceso a Internet?

a) Intermediario

b) Caché

c) **NAT**

d) Inverso

He instalado en mi Ubuntu Server el proxy Squid. ¿Qué servicio podré filtrar?

a) **Web**

b) Correo

c) Telnet

d) IRC

Indica la ACL que permitirá a los ordenadores de mis alumnos conectarse a Internet de 8:00 a 14:00 h

a) acl alumnos src 192.168.100.0/255.255.255.0

b) acl horario 8:00 – 14:00

c) acl deny alumnos horario

d) acl allow alumnos horario