Servizo Proxy Caché Squid: Tipos de ACLs

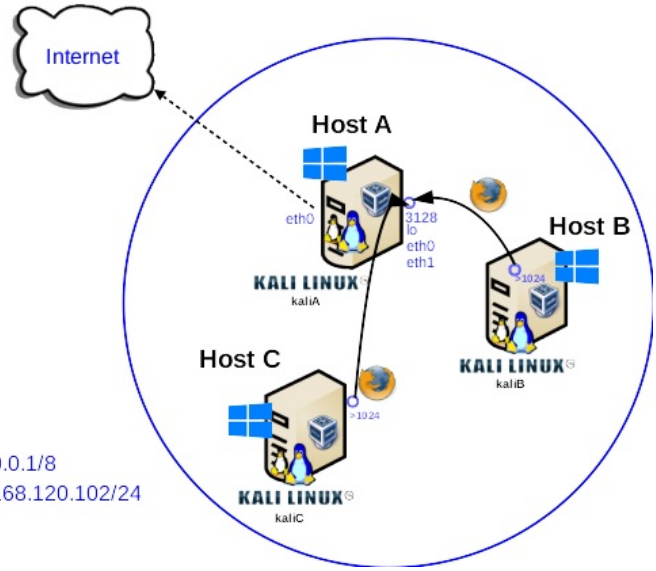
ESCENARIO

Máquinas virtuais:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
ISO: Kali Live amd64
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
Cliente Web: Navegador (firefox)

Máquina virtual A (kaliA)
loopback (lo) → 127.0.0.1/8
Rede (eth0): NAT → 10.0.2.15/24
Rede (eth1): Interna → 192.168.120.100/24
Servidor Proxy Caché Squid → Porto TCP 3128

Máquina virtual B (kaliB)
loopback (lo) → 127.0.0.1/8
Rede (eth0): Interna → 192.168.120.101/24

Máquina virtual C (kaliC)
loopback (lo) → 127.0.0.1/8
Rede (eth0): Interna → 192.168.120.102/24



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTA: URLs de interese

- **Práctica SI Squid**
- **Reference (Directivas)**

Resumo Prácticas Exemplos

- No **Exemplo1. ACL: Orixe MAC Address (OSI - Capa 2)**, veremos como poder permitir/denegar o acceso a Internet según a Mac Address de orixe da solicitude.
- No **Exemplo2. ACL: Orixe IP (OSI - Capa 3)**, veremos como poder permitir/denegar o acceso a Internet según a IP de orixe da solicitude.
- No **Exemplo3. ACL: Orixe Rede (OSI - Capa 3)**, veremos como poder permitir/denegar o acceso a Internet según a rede de orixe da solicitude.
- No **Exemplo4. ACL: Listas brancas e negras de dominios (OSI - Capa 7)** veremos como poder permitir/denegar o acceso a Internet según o dominio destino da solicitude.
- No **Exemplo5. ACL: Control de acceso mediante HTTP Basic (OSI - Capa 7)** imos tratar a autentificación http basic.

  HTTP proporciona un método de autenticación básico de usuarios: basic. Este método ante unha petición do cliente(navegador web) ao servidor cando se solicita unha URL amosará un diálogo pedindo usuario e contrasinal. Unha vez autenticado o usuario, o cliente volverá facer a petición ao servidor pero agora enviando o usuario e contrasinal, en texto claro (sen cifrar) proporcionados no diálogo. É recomendable entón se se emprega este método que se faga combinado con conexión SSL (HTTPS).

Configuración máquina virtual A: Kali amd64
(lo -> loopback -> 127.0.0.1/8)
(eth0 -> NAT -> 10.0.2.15/24)
(eth1 -> Rede Interna -> 192.168.120.100/24)

1. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal **abc123.** (Ollo que o contrasinal ten un caracter punto final).

2. Cambiar hostname da máquina virtual A. Por kaliA como hostname:
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
      root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.
      root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
      root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
      root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

3. Configurar a rede:
   Na contorna gráfica abrir un terminal e executar:

   kali@kaliA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
      root@kaliA:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
      root@kaliA:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
      root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), NAT(eth0) e interna(eth1).
      root@kaliA:~# ip addr add 192.168.120.100/24 dev eth1 #Configurar a tarxeta de rede interna eth1, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.
      root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), NAT(eth0) e interna(eth1).
      root@kaliA:~# ip route #Amosar a táboa de rutas do sistema.
      root@kaliA:~# cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.
      root@kaliA:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth1
      root@kaliA:~# ping -c4 www.google.es #Comprobar mediante o comando ping a conectividade co dominio www.google.es
      root@kaliA:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
      root@kaliA:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A

4. Activar Servidor Proxy Caché Squid:
      root@kaliA:~# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
      root@kaliA:~# apt search squid #Buscar calquera paquete que coincida co patrón de búsqueda squid
      root@kaliA:~# apt -y install squid #Instalar o paquete squid, é dicir, instalar o servidor proxy caché squid. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
      root@kaliA:~# /etc/init.d/squid status #Comprobar o estado do servidor proxy caché Squid.
      root@kaliA:~# /etc/init.d/squid start #Iniciar o servidor proxy caché Squid.
      root@kaliA:~# /etc/init.d/squid status #Comprobar o estado do servidor proxy caché Squid.
      root@kaliA:~# nc -vz 192.168.120.100 3128 #Mediante o comando nc(netcat) comprobar se o porto 3128 do servidor proxy caché Squid está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 3128 é o porto TCP a escanear.

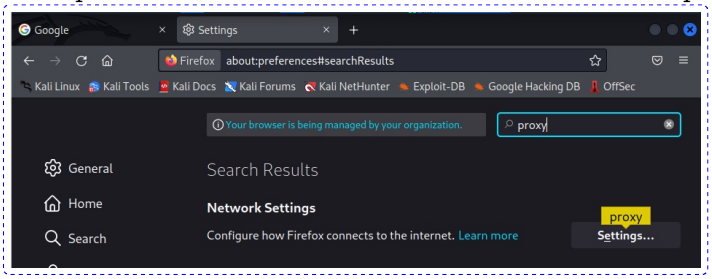
Configuración máquina virtual B: Kali amd64
(lo -> loopback -> 127.0.0.1/8)
(eth0 -> Rede Interna -> 192.168.120.101/24)

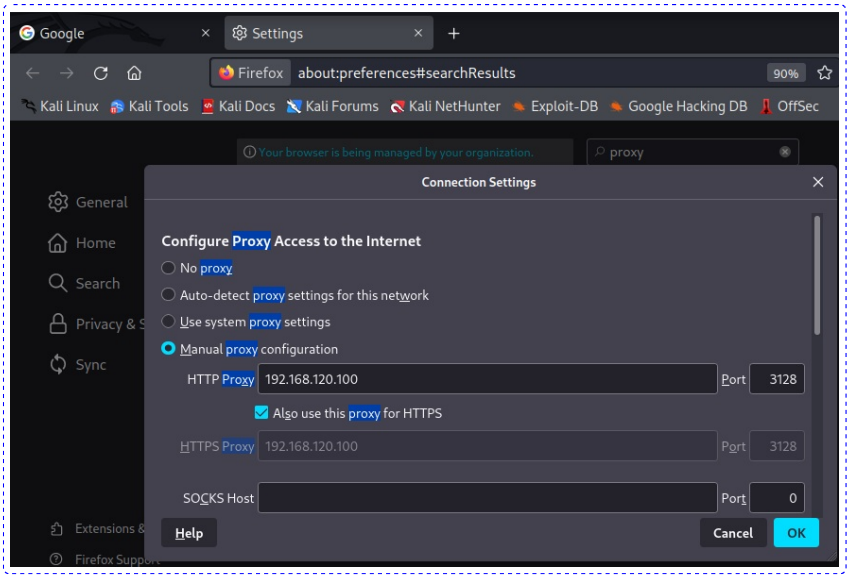
5. Configuración da rede. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
   root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kali:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kali:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
   root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
   root@kali:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
   root@kali:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
   root@kali:~# cat /sys/class/net/eth0/address #Amosar o valor da MAC Address da NIC eth0.

6. Cambiar hostname da máquina virtual B. Por kaliB como hostname:
   root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
   root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
   root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

7. Na máquina virtual B (kaliB) configurar o navegador firefox:
   A. Para que non posúa caché e así as páxinas non sexan gardadas na caché do navegador:

   B. Para que o acceso a Internet sexa a través do servidor proxy caché 192.168.120.100(kaliA) no porto TCP 3128:





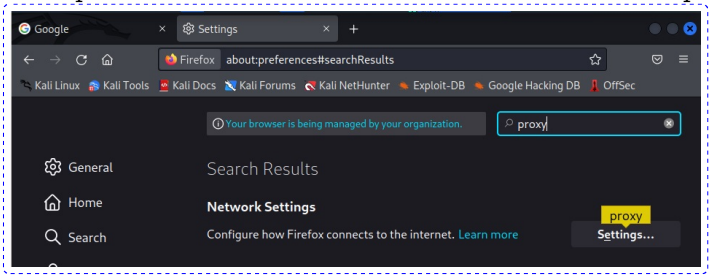
Configuración máquina virtual C: Kali amd64
(lo -> loopback -> 127.0.0.1/8)
(eth0 -> Rede Interna -> 192.168.120.102/24)

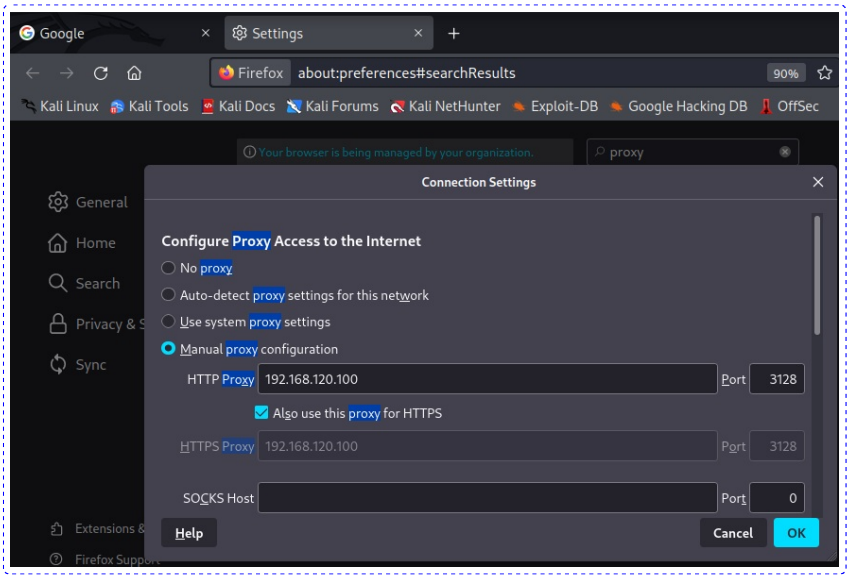
8. Configuración da rede. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
   root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kali:~# ip addr add 192.168.120.102/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.102 e máscara de subrede: 255.255.255.0.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kali:~# ping -c4 192.168.120.102 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
   root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
   root@kali:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
   root@kali:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
   root@kali:~# cat /sys/class/net/eth0/address #Amosar o valor da MAC Address da NIC eth0.

9. Cambiar hostname da máquina virtual C. Por kaliC como hostname:
   root@kali:~# echo 'kaliC' > /etc/hostname #Indicar ao sistema o valor do hostname.
   root@kali:~# echo 'kernel.hostname=kaliC' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
   root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

10. Na máquina virtual C (kaliC) configurar o navegador firefox:
    A. Para que non posúa caché e así as páxinas non sexan gardadas na caché do navegador:

    B. Para que o acceso a Internet sexa a través do servidor proxy caché 192.168.120.100(kaliA) no porto TCP 3128:





Exemplos:

11. **Exemplo1. ACL: Orixe MAC Address (OSI - Capa 2) (acl name arp mac-address).**

> Sustituir 01:02:03:04:05:06 pola mac-address correspondente á NIC eth0 de kaliB e kaliC según corresponda.
> Lembrar que podedes recoller os valores desas mac-address executando en kaliB e kaliC o seguinte comando:
> $ cat /sys/class/net/eth0/address

Executar en kaliA:

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kaliA:~# echo -e 'acl arpOK arp 01:02:03:04:05:06\nhttp_access allow arpOK' > /etc/squid/conf.d/arpsOK.conf
#Xerar un novo ficheiro de configuración, /etc/squid/conf.d/arpsOK.conf, que contén unha acl de nome arpOK, á cal se lle permite o acceso a Internet, é dicir, se lle permite o acceso a Internet a kaliB.
root@kaliA:~# echo -e 'acl arpKO arp 01:02:03:04:05:06\nhttp_access deny arpKO' > /etc/squid/conf.d/arpsKO.conf
#Xerar un novo ficheiro de configuración, /etc/squid/conf.d/arpsKO.conf, que contén unha acl de nome arpKO, á cal se lle denega o acceso a Internet, é dicir, se lle denega o acceso a Internet a kaliC.
root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta as acls definidas: arpOK e arpKO.
```

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar a URL http://book.hacktricks.xyz

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar a URL http://book.hacktricks.xyz

   Que acontece? Por que?

12. **Exemplo2. ACL: Orixe IP (OSI - Capa 3) (acl name src IP).**

Executar en kaliA:

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kaliA:~# rm -f /etc/squid/conf.d/arpsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsOK.conf xerado no Exemplo1.
root@kaliA:~# rm -f /etc/squid/conf.d/arpsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsKO.conf xerado no Exemplo1.
root@kaliA:~# echo -e 'acl ipOK src 192.168.120.101\nhttp_access allow ipOK' > /etc/squid/conf.d/ipsOK.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/ipsOK.conf, que contén unha acl de nome ipOK, á cal se lle permite o acceso a Internet, é dicir, se lle permite o acceso a Internet a kaliB.
root@kaliA:~# echo -e 'acl ipKO src 192.168.120.102\nhttp_access deny ipKO' > /etc/squid/conf.d/ipsKO.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/ipsKO.conf, que contén unha acl de nome ipKO, á cal se lle denega o acceso a Internet, é dicir, se lle denega o acceso a Internet a kaliC.
root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta as acls definidas: ipOK e ipKO.
```

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar a URL http://www.google.es

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar a URL http://www.google.es

   Que acontece? Por que?

13. **Exemplo3. ACL: Orixe Rede (OSI - Capa 3) (acl name src Rede).**

    Executar en kaliA:

kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kaliA:~# rm -f /etc/squid/conf.d/arpsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsOK.conf xerado no Exemplo1.
root@kaliA:~# rm -f /etc/squid/conf.d/arpsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsKO.conf xerado no Exemplo1.
root@kaliA:~# rm -f /etc/squid/conf.d/ipsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsOK.conf xerado no Exemplo2.
root@kaliA:~# rm -f /etc/squid/conf.d/ipsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsKO.conf xerado no Exemplo2.
root@kaliA:~# echo -e 'acl redeOK src 192.168.120.0/24\nhttp_access allow redeOK' > /etc/squid/conf.d/redes.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/redes.conf, que contén unha acl de nome redeOK, á cal se lle permite o acceso a Internet, é dicir, se lle permite o acceso a Internet a kaliB e kaliC.
root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta a acl definida: redeOK.

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar a URL http://github.com

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar a URL http://github.com

   Que acontece? Por que?

root@kaliA:~# echo -e 'acl redeKO src 192.168.120.0/24\nhttp_access deny redeKO' > /etc/squid/conf.d/redes.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/redes.conf, que contén unha acl de nome redeKO, á cal se lle denega o acceso a Internet, é dicir, se lle denega o acceso a Internet a kaliB e kaliC.

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar a URL http://github.com

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar a URL http://github.com

   Que acontece? Por que?

14. **Exemplo4. ACL: Listas brancas e negras de dominios (OSI - Capa 7) (acl name dstdomain dominio).**

Executar en kaliA:

kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

root@kaliA:~# rm -f /etc/squid/conf.d/arpsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsOK.conf xerado no Exemplo1.

root@kaliA:~# rm -f /etc/squid/conf.d/arpsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsKO.conf xerado no Exemplo1.

root@kaliA:~# rm -f /etc/squid/conf.d/ipsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsKO.conf xerado no Exemplo2.

root@kaliA:~# rm -f /etc/squid/conf.d/ipsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsOK.conf xerado no Exemplo2.

root@kaliA:~# rm -f /etc/squid/conf.d/redes.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsOK.conf xerado no Exemplo3.

root@kaliA:~# echo -e 'acl whitelist dstdomain .edu.xunta.gal .youtube.com\nhttp_access allow whitelist' > /etc/squid/conf.d/whitelist.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/whitelist.conf, que contén unha acl de nome whitelist, á cal se lle permite o acceso a Internet, é dicir, se lle permite no acceso a Internet visitar os dominios e subdominios pertencentes a edu.xunta.gal e youtube.com en kaliB e kaliC.

root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta a acl definida: whitelist.

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar as URL http://edu.xunta.gal e http://youtube.com

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar as URL http://edu.xunta.gal e http://youtube.com

   Que acontece? Por que?

root@kaliA:~# echo -e 'acl blacklist dstdomain .marca.com .mundodeportivo.com\nhttp_access deny blacklist' > /etc/squid/conf.d/blacklist.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/blacklist.conf, que contén unha acl de nome blacklist, á cal se lle denega o acceso a Internet, é dicir, se lle denega no acceso a Internet visitar os dominios e subdominios pertencentes a marca.com e mundodeportivo.com en kaliB e kaliC.

root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta a acl definida: whitelist.

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar as URLs http://marca.com e http://mundodeportivo.com

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar as URLs http://marca.com e http://mundodeportivo.com

   Que acontece? Por que?

15. **Exemplo5. ACL: Control de acceso mediant HTTP Basic (OSI - Capa 7) (acl name dstdomain dominio).**

$ tail +$(grep -n 'OPTIONS FOR AUTHENTICATION' /etc/squid/squid.conf | cut -d ':' -f1) /etc/squid/squid.conf | less #Ver información sobre como configurar a autenticación en squid. Aquí atoparemos a seguinte ligazón: **AddonHelpers** pero está "rota", sendo as URLs de interese para atopar información sobre os distintos tipos de autenticación as seguintes:

- **Authentication**
- **Squid helpers**

Tamén podemos atopar información sobre o tipo de autenciación HTTP Basic a través das páxinas do manual co comando:
$ man basic_ncsa_auth

Executar en kaliA:

kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kaliA:~# rm -f /etc/squid/conf.d/arpsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsOK.conf xerado no Exemplo1.
root@kaliA:~# rm -f /etc/squid/conf.d/arpsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/arpsKO.conf xerado no Exemplo1.
root@kaliA:~# rm -f /etc/squid/conf.d/ipsKO.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsKO.conf xerado no Exemplo2.
root@kaliA:~# rm -f /etc/squid/conf.d/ipsOK.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsOK.conf xerado no Exemplo2.
root@kaliA:~# rm -f /etc/squid/conf.d/redes.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/ipsOK.conf xerado no Exemplo3.
root@kaliA:~# rm -f /etc/squid/conf.d/whitelist.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/whitelist.conf xerado no Exemplo4.
root@kaliA:~# rm -f /etc/squid/conf.d/blacklist.conf #Eliminar o ficheiro de configuración, /etc/squid/conf.d/blacklist.conf xerado no Exemplo4.
root@kaliA:~# echo 'auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/squid.htpasswd' > /etc/squid/conf.d/users.conf #Xerar un novo ficheiro de configuración, /etc/squid/conf.d/users.conf, que permite o tipo de autenticación HTTP Basic para permitir o acceso a Internet, é dicir, permitir o acceso a Internet según usuarios coas credenciais definidas no arquivo /etc/squid/squid.htpasswd
root@kaliA:~# echo -e 'acl allowUsers proxy_auth REQUIRED\nhttp_access allow allowUsers' >> /etc/squid/conf.d/users.conf #Modificar o ficheiro de configuración, /etc/squid/conf.d/users.conf, para engadirlle unha acl de nome allowusers, á cal se lle permite o acceso a Internet, é dicir, permitir o acceso a Internet según usuarios coas credenciais definidas no arquivo /etc/squid/squid.htpasswd.
root@kaliA:~# htpasswd -c /etc/squid/squid.htpasswd ana #Crear o contrasinal para o usuario ana no ficheiro de contrasinais /etc/squid/squid.htpasswd. Pór **123456** como contrasinal do usuario *ana*
root@kaliA:~# htpasswd /etc/squid/squid.htpasswd brais Crear o contrasinal para o usuario brais no ficheiro de contrasinais /etc/squid/squid.htpasswd. Pór **654321** como contrasinal do usuario *brais*
root@kaliA:~# chmod 600 /etc/squid/squid.htpasswd && chown proxy /etc/squid/squid.htpasswd #Configurar os permisos ugo(600=rw- --- ---) e a pertenza do usuario propietario ao arquivo de credenciais HTTP Basic /etc/squid/squid.htpasswd
root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta a autenticación HTTP Basic, e así permitir que soamente os usuarios ana e brais poidan acceder a Internet.

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar a URL http://www.hackthebox.com

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar a URL http://www.hackthebox.com

   Que acontece? Por que?

root@kaliA:~# sed -i 's/http_access allow allowUsers/http_access deny allowUsers/' /etc/squid/conf.d/users.conf #Modificar no ficheiro de configuración, /etc/squid/conf.d/users.conf, a acl de nome allowusers, para denegar o acceso a Internet, é dicir, denegar o acceso a Internet aos usuarios coas credenciais definidas no arquivo /etc/squid/squid.htpasswd.
root@kaliA:~# /etc/init.d/squid reload #Recargar a configuración do Servidor Web Squid para ter en conta a acl definida: whitelist.

A. Lanzar na máquina virtual B (kaliB) o navegador firefox e visitar a URL http://picoctf.org

   Que acontece? Por que?

B. Lanzar na máquina virtual C (kaliC) o navegador firefox e visitar a URL http://picoctf.org

   Que acontece? Por que?

Ricardo Feijoo Costa