

Configuración dun proxy en Debian

- Neste apartado imos ver como configurar sobre unha máquina virtual con Debian o servizo de proxy usando o servidor **squid**.
- Explicaremos en primeiro lugar os pasos a seguir para instalar o servizo na máquina Debian e configurar as máquinas cliente para que fagan uso del para navegar por Internet, e a continuación como configurar o servidor proxy para permitir ou denegar o acceso en función da máquina que establece a conexión.



RECORDA QUE...

No apartado [Conceptos básicos de Enrutamiento \(Routing\) e Proxy](#) podes revisar o funcionamento do servizo de proxy e as diferenzas deste co servizo de enrutamento.

Sumario

- 1 Instalación do Proxy Squid en Debian
- 2 Configuración do equipo cliente
 - ◆ 2.1 Configuración de clientes Windows
 - ◆ 2.2 Configuración de clientes Linux
- 3 Control de acceso segundo os equipos cliente

Instalación do Proxy Squid en Debian

- Mostraremos a continuación os pasos que podemos seguir para instalar o servizo squid en Debian usando Webmin:

- Instalación do Proxy Squid en Debian

La captura muestra la sección 'Instalar Nuevo Paquete'. Se ha seleccionado la opción 'Paquete desde APT' y se ha ingresado 'squid' en el campo de búsqueda. El botón 'Instalar' está resaltado.

Usamos a ferramenta de **Paquetes de Software** para instalar usando *apt* o paquete **squid3**.

La captura muestra la sección 'Configuración del Servidor'. Se observan iconos para 'Máscara IP', 'Dominio de Cache', 'Programa de autenticación', 'Configuración del Proveedor de Proxies', 'Edit Configuration File', 'Cache Manager', 'Cache Manager Statistics' y 'Cache Manager Processes'.

Tras instalar o paquete e refrescar os módulos de Webmin, atoparemos o módulo de xestión do proxy dentro da categoría de **Servidores**. Dentro do módulo atopamos numerosos apartados de configuración do servizo, xa que se trata dun servizo moi potente con multitud de parámetros posibles dos que só veremos os máis representativos. Comezaremos pola inicialización da caché, que é unha carpeta na que o servidor proxy almacenará a información descargada para usala en futuros accesos reducindo o tráfico de rede.

A imaxe mostra o resultado da inicialización da caché, na que se crean unha serie de carpetas para almacenar os ficheiros temporais.

- The screenshot shows the Squid configuration interface with several tabs and icons:

 - Fuentes y Trabajos en Cache**: Includes icons for a blue folder and a yellow star.
 - Opciones de Cache**: Includes icons for a blue folder and a yellow star.
 - Programas de administración**: Includes icons for a blue folder and a yellow star.
 - Configuración del sistema y administración de usuarios**: Includes icons for a blue folder and a yellow star.
 - Otros Cachés**: Includes icons for a blue folder and a yellow star.
 - Programas de ayuda**: Includes icons for a blue folder and a yellow star.
 - Planes de trabajo**: Includes icons for a blue folder and a yellow star.
 - Configuración del sistema y administración de usuarios**: Includes icons for a blue folder and a yellow star.
 - Uso de Memoria**: Includes icons for a blue folder and a yellow star.
 - Datos de Acceso**: Includes icons for a blue folder and a yellow star.
 - Configuración del sistema y administración de usuarios**: Includes icons for a blue folder and a yellow star.
 - Cuentas de Acceso de Colaboradores**: Includes icons for a blue folder and a yellow star.
 - Administración de Cachés**: Includes icons for a blue folder and a yellow star.
 - Configuración del sistema y administración de usuarios**: Includes icons for a blue folder and a yellow star.
 - Sistema y Recursos Gerais**: Includes icons for a blue folder and a yellow star.
 - Sistema y Recursos Gerais**: Includes icons for a blue folder and a yellow star.

At the bottom, there are two buttons: **Abrir la Configuración** and **Cancelar**.

De novo no índice do módulo, comprobamos que a mensaxe de inicialización da caché xa non aparece. Aínda que con isto xa temos o servizo funcionando correctamente, imos entrar no apartado de **Portos e traballo en rede** para mostrar un parámetro de gran importancia, e que poderíamos querer modificar.

- | | |
|--|--|
| <p>Configuración de Puerto y Trabajo en Red</p> <p>Direcciones de Puerto y Trabajo en Red</p> <p>Direcciones a puertos de Proxy <input type="checkbox"/> Por defecto (puerto 8080) <input checked="" type="radio"/> Usar los mismos Puerto: <input type="text" value="8080"/> Número de máscara/cifrado IP: <input type="text" value="10.0.1.1"/> <input type="text" value="10.0.1.1"/> </p> <p>Direcciones y puertos ASA <input type="checkbox"/> Por defecto (puerto 443) <input checked="" type="radio"/> Usar los mismos Puerto: <input type="text" value="443"/> Número de máscara/cifrado IP: <input type="text" value="10.0.1.1"/> <input type="text" value="10.0.1.1"/> </p> <p>Dirección de IP de salida: <input type="text" value="10.0.1.1"/></p> <p>Dirección IP de entrada: <input type="text" value="10.0.1.1"/></p> <p>Dirección de enrutamiento: <input type="text" value=""/></p> <p>Variante Autenticación de SSL/TLS: <input type="radio"/> No <input type="radio"/> Sí <input type="checkbox"/> Utilizar desencriptación de tráfico SSL/TLS <input type="radio"/> Activado <input checked="" type="radio"/> Desactivado</p> <p>Otros: <input type="checkbox"/> Requerir a todos el uso de <input type="checkbox"/> B</p> | <p>Puertos y Trabajo en Red</p> <p>Dirección de salida: <input type="text" value="10.0.1.1"/> <input type="checkbox"/> Usar los mismos <input type="text" value="10.0.1.1"/></p> <p>Dirección de entrada: <input type="text" value="10.0.1.1"/> <input type="checkbox"/> Usar los mismos <input type="text" value="10.0.1.1"/></p> <p>Método de encriptación TCP: <input type="checkbox"/> Si es por defecto del ASA <input type="radio"/> No</p> <p>Otros: <input type="checkbox"/> Almacenar configuración de host/network <input type="radio"/> Sí <input type="radio"/> No</p> |
|--|--|

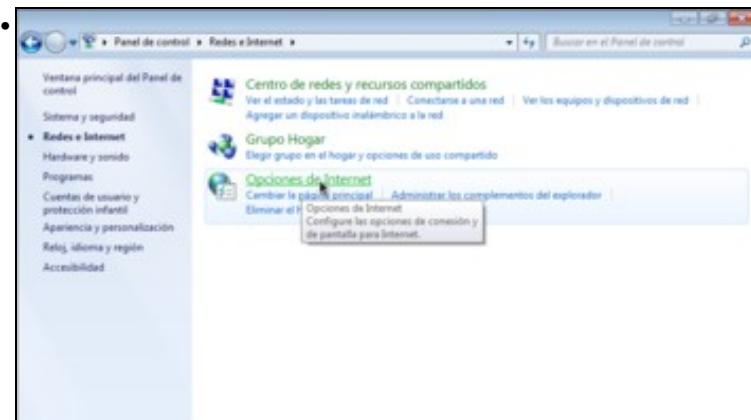
Trátase do porto no que escuta o servizo, que por defecto é o 3128. Neste caso deixaremos o parámetro como está, pero dependendo dos requisitos da rede podemos precisar cambialo, configurar o servizo para que escute por máis de un porto ou para que funcione en modo de proxy transparente co obxectivo de evitar ter que facer unha configuración explícita do proxy nos equipos cliente.

Configuración do equipo cliente

- Imos ver como debemos configurar os equipos cliente para que fagan uso do servidor proxy cando naveguen por Internet.
 - Tendo en conta que non imos usar o proxy en modo transparente, xa que isto non permitiría conexións HTTPS nin autenticación de usuarios, teremos que configurar o navegador no equipo cliente indicando cal é a dirección IP do proxy e o porto polo que escoita.

Configuración de clientes Windows

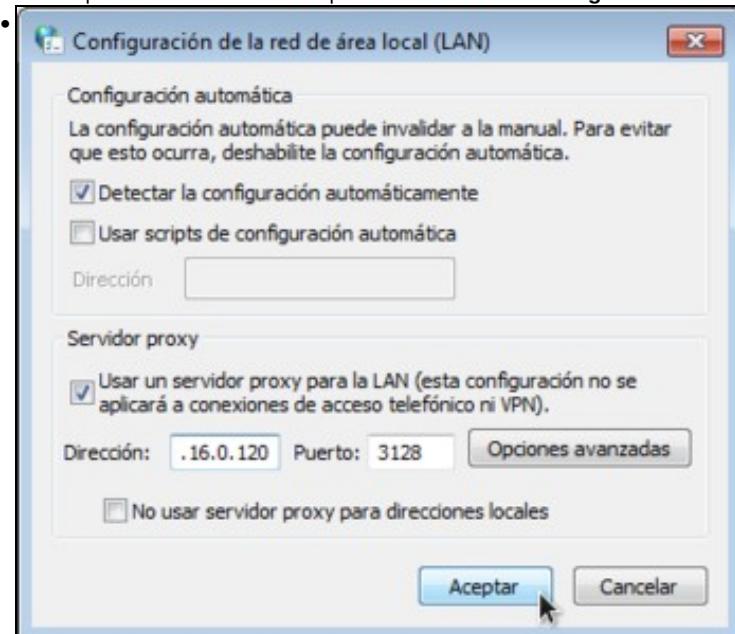
- Comezamos mostrando a configuración nun cliente Windows, utilizando como navegador Internet Explorer. Esta configuración tamén valería para Google Chrome, xa que toma os datos do proxy do sistema. En caso de usar Mozilla Firefox, seguiríamos os pasos que se explican para o cliente Linux.
 - Configuración do proxy nun cliente Windows



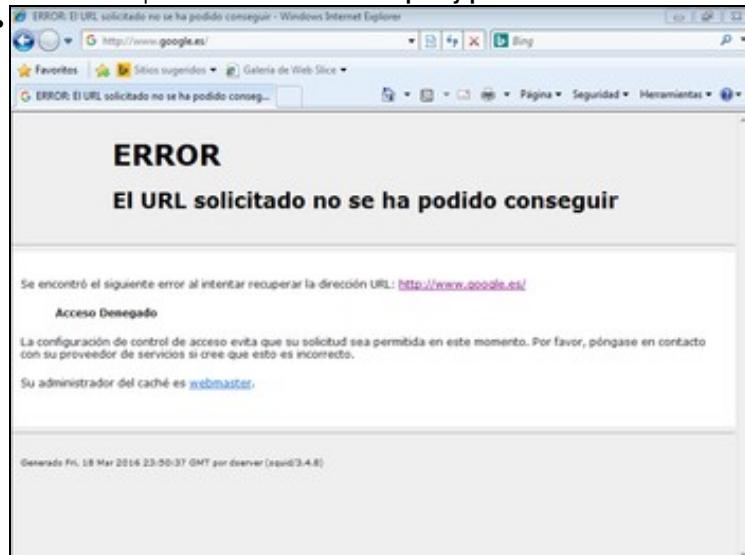
No Panel de Control de Windows, entramos no apartado de **Redes e Internet** e picamos en **Opciones de Internet**.



Imos á pestana de **Conexiones** e picamos no botón de **Configuración de LAN**.



Activamos a opción de **Usar un servidor proxy para a LAN** e introducimos a dirección IP e porto do servidor proxy. Aceptamos.

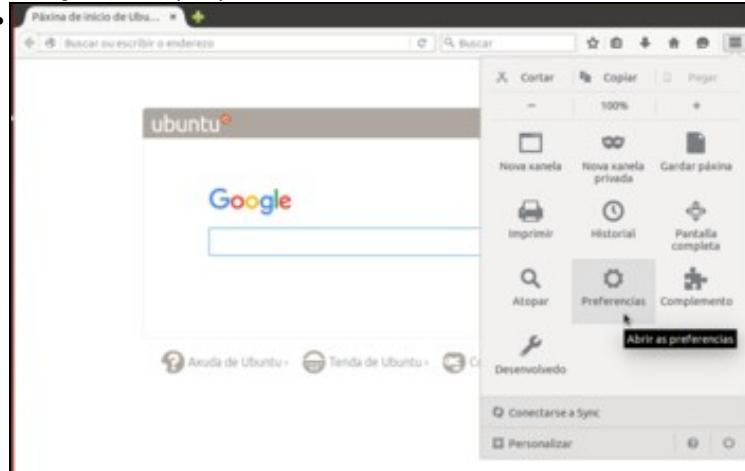


Podemos comprobar que se intentamos conectarnos a calquera web, aparece unha páxina indicando que o proxy denegou a conexión. Isto é debido á configuración por defecto do proxy, que de seguido cambiaremos, pero permítens comprobar que o navegador está usando o proxy para conectarse á páxina.

Configuración de clientes Linux

- Veremos agora como configurar o proxy nun cliente Ubuntu usando o navegador Mozilla Firefox:

- Configuración do proxy nun cliente Linux



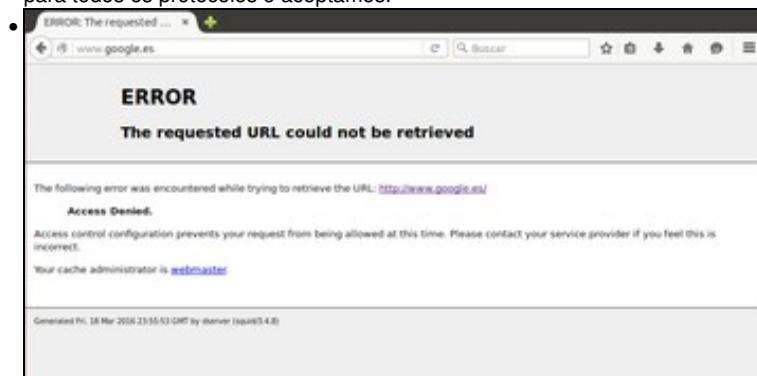
Imos á configuración das preferencias do navegador.



Entramos no apartado de **Opcións avanzadas** para na lapela de **Rede** picar na opción de **Configuración**.



Activamos a configuración manual do proxy para introducir a dirección IP e porto do proxy. Activamos a opción de usar este servidor proxy para todos os protocolos e aceptamos.



Igual que antes, observamos que o navegador usa o proxy para intentar conectarse ás páxinas web, e este denega o acceso.

Control de acceso segundo os equipos cliente

- Remataremos este apartado vendo como podemos configurar o proxy para que permita o acceso a Internet aos equipos que nos interese.

- Control de acceso por equipo cliente en squid



Entramos no apartado de **Control de acceso** do módulo de xestión do proxy.

| Control de Acceso | | Rango Control Pestañas |
|-------------------|------------------|---------------------------|
| Nombre | Tipo | Último acceso |
| Este punto | Punto (R) | 10:22 |
| Este punto | Punto (R) | 09:47 |
| Este punto | Punto (R) | 22 |
| Este punto | Punto (R) | 09:45 |
| Este punto | Punto (R) | 70 |
| Este punto | Punto (R) | 710 |
| Este punto | Punto (R) | 0204-0000 |
| Este punto | Punto (R) | 700 |
| Este punto | Punto (R) | 600 |
| Este punto | Punto (R) | 700 |
| Este punto | Punto (R) | 711 |
| CONSTRUCT | Método de Paseos | CONNECT |

Na primeira pestana de **Listas de control de acceso** podemos definir diversos criterios que logo poderemos utilizar para aplicar restricciones no proxy. Na lista podemos ver unha serie de ACLs que xa veñen configuradas por defecto en squid. Seleccionamos neste caso a opción de **Dirección de Cliente** e picamos en **Crear nova ACL**.

Índice de Módulo

Crear ACL

Dirección de Cliente ACL.

| | |
|---------------------------|--|
| Nombre ACL: | <input type="text" value="LAN"/> |
| Desde IP: | <input type="text" value="172.16.0.0"/> |
| A IP: | <input type="text"/> |
| Máscara de Red: | <input type="text" value="0.0.0.0"/> |
| URL de Fallo: | <input type="text"/> |
| Almacenar ACL en archivo: | <input checked="" type="radio"/> Configuración Squid <input type="radio"/> Separate file <input type="checkbox"/> Usar sólo contenidos existentes del archivo? |

Salvar

[Regresar a Lista ACL](#) | [Regresar a índice](#)

Poñemos un nome para a ACL (*LAN*) e teremos que indicar as direccións IP dos equipos cliente que queremos restrinxir. Podemos introducir un rango de direccións, pero neste caso imos permitir o acceso a todos os equipos da rede, introducindo a dirección da rede e a súa máscara. Gardamos a ACL.

| Control de Acceso | | | |
|-------------------------------|----------------------|---------------------|-------------------|
| Unidades de control de Acceso | | Restricciones proxy | Restricciones ICF |
| Nombre | Type | Coincidencia con... | |
| SSL_ports | Puerto URL | | 443 |
| Safe_ports | Puerto URL | | 80 |
| Safe_ports | Puerto URL | | 21 |
| Safe_ports | Puerto URL | | 443 |
| Safe_ports | Puerto URL | | 70 |
| Safe_ports | Puerto URL | | 238 |
| Safe_ports | Puerto URL | | 1325-65535 |
| Safe_ports | Puerto URL | | 280 |
| Safe_ports | Puerto URL | | 488 |
| Safe_ports | Puerto URL | | 993 |
| Safe_ports | Puerto URL | | 777 |
| CONNECT | Método de Petición | | CONNECT |
| LAN | Dirección de Cliente | | 172.16.0.938 |

Podemos ver ao final da táboa a ACL creada. Imos agora á pestana de **Restriccóns Proxy** para definir unha restrición sobre esta ACL.

| Control de Acceso | | Acción |
|---|-----------------------|--------|
| <input type="checkbox"/> Administrador de Redes | Administrador Proxy | |
| <input type="checkbox"/> Administrador de Redes | Administrador IPT | |
| <input type="checkbox"/> Administrador de Redes | Proprieta Interne PCI | |
| <input type="checkbox"/> Administrador de Redes | Ruta proxy heredada | |
| <input checked="" type="checkbox"/> Administrador | All rights | |
| <input type="checkbox"/> Orange | Sub-paths | - |
| <input type="checkbox"/> Orange | CONNECT_WLS_paths | - |
| <input type="checkbox"/> Orange | JaasAuth manager | - |
| <input type="checkbox"/> Orange | manager | - |
| <input type="checkbox"/> Orange | readattr | - |
| <input type="checkbox"/> Orange | rl | + |
| Modificar este perfil | | |
| Diseñar nuevo perfil | | |

Se nos fixamos nas restriccións definidas por defecto, só se permite acceder dende o propio equipo (*localhost*), e a última restrición denega todo o resto de conexións. Imos polo tanto a engadir unha restrición que permita as conexións dende os equipos da rede local.

- Índice de Módulo

Restricción de Proxy

Acción Permitir Denegar

| | |
|------------------------------|---|
| Coincidir con ACLs | all (1) SSL_ports (1) Safe_ports (1) CONNECT (1) LAN (0) |
| No coincidir con ACLs | all (1) SSL_ports (1) Safe_ports (1) CONNECT (1) LAN (0) |

Salvar

[← Regresar a Lista de ACL](#) | [Regresar a índice](#)

Seleccionamos como acción **Permitir** e na lista de **Coincidir con ACLs** seleccionamos a ACL que acabamos de crear. Desta maneira, a restrición permitirá as conexións que coincidan coa ACL, o que ocorrerá se o equipo cliente ten unha dirección IP dentro da LAN. Gardamos a restrición.

Control de Acceso

| Acción | ACLs | Mover |
|----------|--------------------|-------|
| Denegar | !Safe_ports | ↓ |
| Denegar | CONNECT !SSL_ports | ↓ ↑ |
| Denegar | localhost manager | ↓ ↑ |
| Denegar | manager | ↓ ↑ |
| Permitir | localhost | ↓ ↑ |
| Permitir | LAN | ↓ ↑ |
| Denegar | all | ↑ |

[Añadir restricción proxy](#)

[Delete Selected Restrictions](#)

[Aplicar Cambios](#) [Pasar Siguiente](#)

E poderemos vela ao final da táboa. A orde das restricciones dentro da táboa é moi importante, xa que ao recibir unha petición o proxy comenzará dende o comezo da táboa comprobando se esa petición encaixa con cada unha das restricciones. Cando a petición encaixe coa restrición, o proxy aplicará esa restrición e xa non mirará nas restricciones que haxa por debaixo. Por iso, se deixamos a restrición que creamos no final da lista, nunca se chegará a executar xa que a restrición anterior se aplica a calquera conexión. Picamos sobre a frecha cara arriba para subila dentro da táboa.

Control de Acceso

| Acción | ACLs | Mover |
|----------|--------------------|-------|
| Denegar | !Safe_ports | ↓ |
| Denegar | CONNECT !SSL_ports | ↓ ↑ |
| Denegar | localhost manager | ↓ ↑ |
| Denegar | manager | ↓ ↑ |
| Permitir | localhost | ↓ ↑ |
| Permitir | LAN | ↓ ↑ |
| Denegar | all | ↑ |

[Añadir restricción proxy](#)

[Delete Selected Restrictions](#)

[Regresar a Índice squid](#)

[Aplicar Cambios](#) [Pasar Siguiente](#)

Na imaxe vemos a restrición colocado no lugar axeitado. Picamos sobre **Aplicar Cambios** para activar a restrición introducida.



Podemos comprobar dende os equipos cliente que xa poden navegar por Internet usando o proxy.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez --