

1 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...

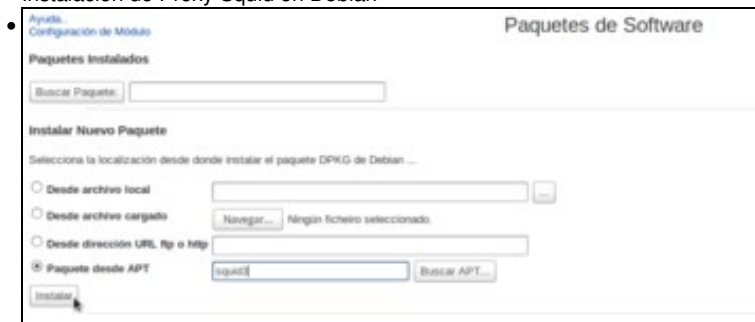
No apartado [Conceptos básicos de Enrutamento \(Routing\) e Proxy](#) podes revisar o funcionamento do servizo de proxy e as diferenzas deste co servizo de enrutamento.

1.1 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

1.2 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



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



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 multitude 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.



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.



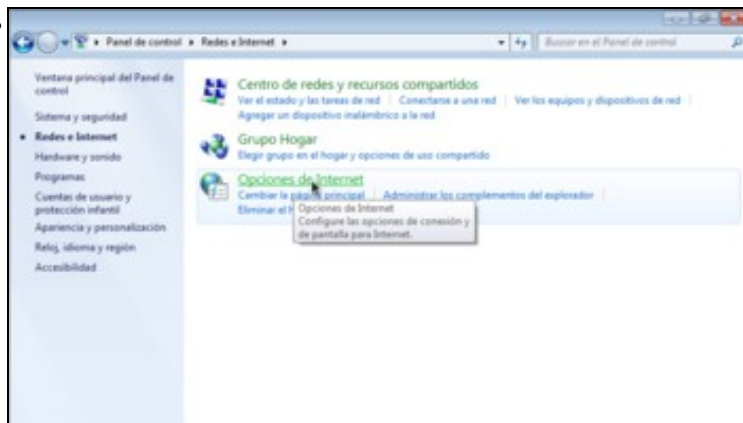
Trátase do porto no que escoita o servizo, que por defecto é o 3128. Neste caso deixaremos o parámetro como está, pero dependendo dos requisitos da rede podemos precisar cambialo, configurar o servizo para que escoite por máis de un porto ou para que funcione en modo de **proxy transparente** co obxectivo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

1.3 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.

1.3.1 Configuración de clientes Windows

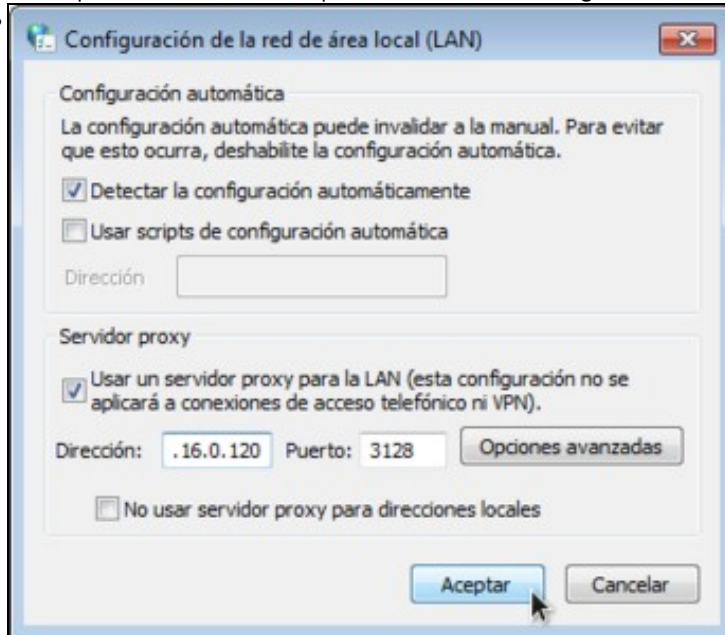
- Comezamos mostrando a configuración nun cliente Windows, utilizando como navegador Internet Explorer. Esta configuración tamén valería para Google Chrome, xa que toma os datos do proxy do sistema. En caso de usar Mozilla Firefox, seguiríamos os pasos que se explican para o cliente Linux.
- Configuración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



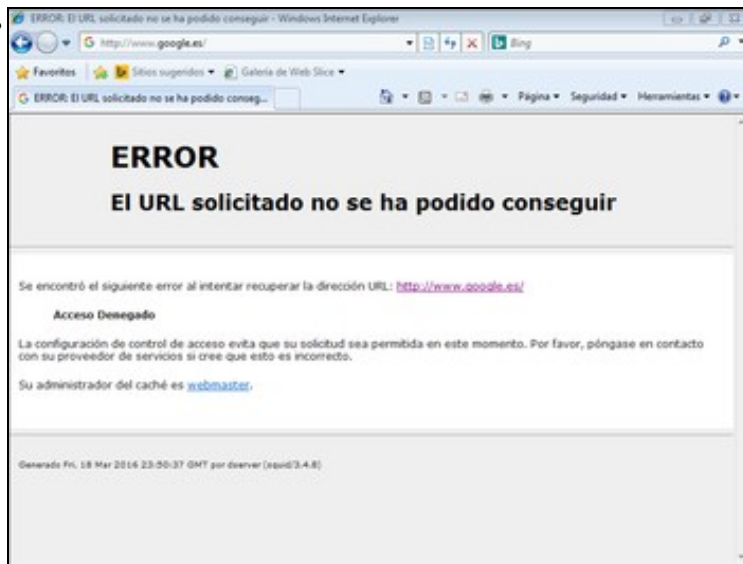
No Panel de Control de Windows, entramos no apartado de **Redes e Internet** e picamos en **Opciones de Internet**.



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



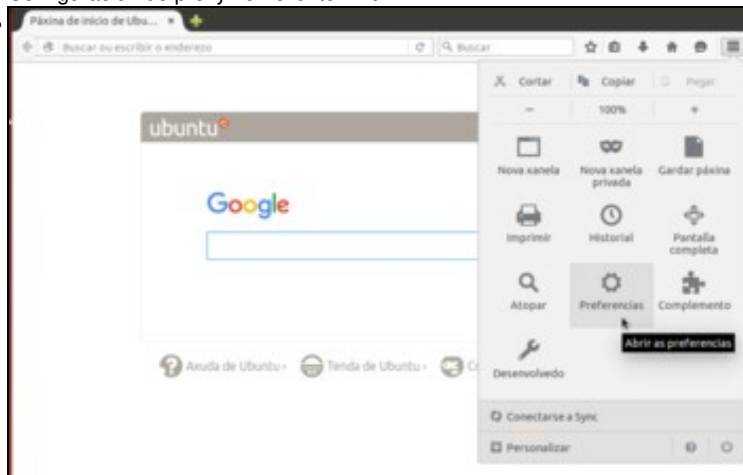
Activamos a opción de **Usar un servidor proxy para a LAN** e introducimos a dirección IP e porto do servidor proxy. Aceptamos.



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 permítenos comprobar que o navegador está usando o proxy para conectarse á páxina.

1.3.2 Configuración de clientes Linux

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



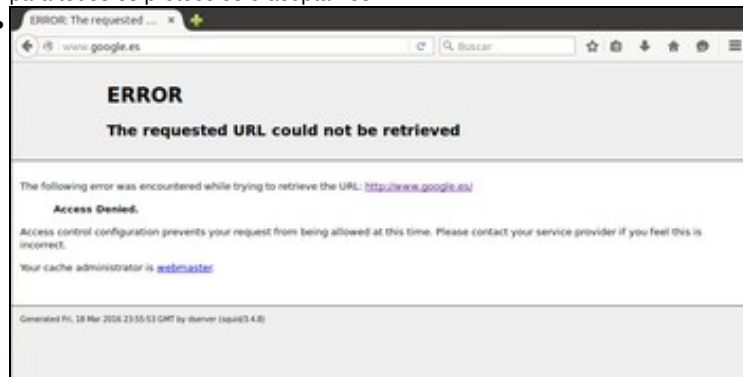
Imos á configuración das preferencias do navegador.



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.

1.4 Control de acceso segundo os equipos cliente

- Remataremos este apartado vendiendo 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.



Na primeira pestana de **Listas de control de acceso** podemos definir diversos criterios que logo poderemos utilizar para aplicar restricións

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**.

Indice de Módulo

Crear ACL

Dirección de Cliente ACL

Nombre ACL:

Desde IP: A IP: Máscara de Red:

URL de Fallo:

Almacenar ACL en archivo: ☒ Configuración Squid ☐ Separate file

☐ ¿Usar sólo contenidos existentes del archivo?

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

Podemos 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.

Indice de Módulo

Control de Acceso

Acción: [Regresar a índice squid](#)

Lista de control de Acceso: [Restricciones Proxy](#) | [Restricciones HTTP](#) | [Programas externos ACL](#) | [Reglas proxy restringidas](#)

Nombre	Tipo	Coincidiendo con...
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	25
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	255
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	468
Safe_ports	Puerto URL	561
Safe_ports	Puerto URL	1777
CONNECT	Método de Petición	CONNECT
LAN	Dirección de Cliente	172.16.0.0/16

[Regresar a índice squid](#)

Podemos ver ao final da táboa a ACL creada. Iremos agora á pestana de **Restriccións Proxy** para definir unha restricción sobre esta ACL.

Indice de Módulo

Control de Acceso

Acción: [Regresar a índice squid](#)

Lista de control de Acceso: [Restricciones Proxy](#) | [Restricciones HTTP](#) | [Programas externos ACL](#) | [Reglas proxy restringidas](#)

Nombre	ACL	Acción
Denegar	Safe_ports	Denegar
Denegar	CONNECT SSL_ports	Denegar
Denegar	localhost manager	Denegar
Denegar	localhost	Denegar
Denegar	all	Denegar

[Regresar a índice squid](#)

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

Indice de Módulo

Restricción de Proxy

Acción: ☒ Permitir ☐ Denegar

Coincidir con ACLs

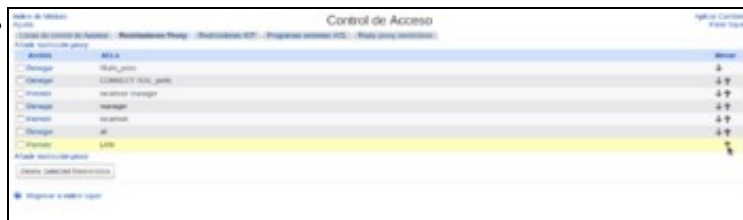
- all (1)
- SSL_ports (1)
- Safe_ports (1)
- CONNECT (1)
- LAN (0)**

No coincidir con ACLs

- all (1)
- SSL_ports (1)
- Safe_ports (1)
- CONNECT (1)
- LAN (0)

[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 restricción permitirá as conexións que coincidan coa ACL, o que ocorrerá se o equipo cliente ten unha dirección IP dentro da LAN. Gardamos a restricción.



E poderemos vela ao final da táboa. A orde das restricións dentro da táboa é moi importante, xa que ao recibir unha petición o proxy comezará dende o comezo da táboa comprobando se esa petición encaixa con cada unha das restricións. Cando a petición encaixe coa restrición, o proxy aplicará esa restrición e xa non mirará nas restricións 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.



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.