

1 Configuración de Zentyal como pasarela de acceso a Internet

1.1 Sumario

- 1 Características de Zentyal como pasarela de acceso a Internet
- 2 Instalación do módulo de Proxy HTTP
- 3 Configuración das interfaces de rede
- 4 Configuración do proxy en modo transparente
 - ◆ 4.1 Configuración do proxy no servidor Zentyal
 - ◆ 4.2 Configuración dos clientes da rede local
 - ◆ 4.3 Configuración do firewall no servidor Zentyal
- 5 Configuración do proxy en modo non transparente
 - ◆ 5.1 Configuración do proxy no servidor Zentyal
 - ◆ 5.2 Configuración dos clientes da rede local
 - ◆ 5.3 Configuración do firewall no servidor Zentyal

1.2 Características de Zentyal como pasarela de acceso a Internet

Zentyal inclúe dentro do módulo de *Gateway* distintos servizos para ofrecer todas as funcións necesarias para unha pasarela de acceso a Internet:

- O servizo de **firewall** (*cortafogos*), utilizando o subsistema **netfilter** do núcleo de Linux. Este servizo permitiranos configurar que conexións se permiten ou se rexeitan na nosa rede local.
- O servizo de enrutamento, utilizando o subsistema de encamiñamento do núcleo de Linux configurándoo con **iproute2**. Este servizo permitirá encamiñar todas as conexións que non sexan atendidas polo proxy (é dicir, que non usen protocolo HTTP ou HTTPS).
- O servizo de proxy mediante o servidor **squid**, e o filtro de contidos con **dansguardian**. Este servizo encamiñará todas as conexións á web dende a rede local.

Con estes servizos, teremos unha completa solución para cubrir co servidor Zentyal as necesidades que se requiren para a pasarela de acceso a Internet.

1.3 Instalación do módulo de Proxy HTTP

En primeiro lugar, teremos que instalar no servidor Zentyal o módulo de *Proxy HTTP*:

- Instalación do módulo de Proxy en Zentyal

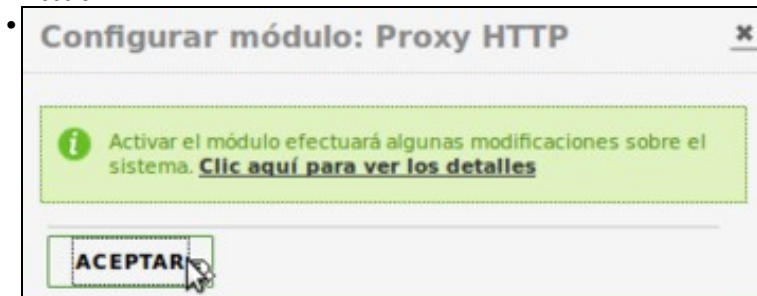


No apartado de **Xestión de software->Compoñentes de Zentyal**, seleccionamos o módulo de **HTTP Proxy**.

- Configuración del estado de los módulos**

Módulo	Depende	Estado
Mail		☒
Certificados	Mail	☒
Antivirus		☒
DBS	Mail	☒
Registros		☒
NTP		☒
Controlador de Servidor y Compartición de Recursos	Mail, DBS, NTP	☒
Proxy HTTP	Certificados, Controlador de Servidor y Compartición de Recursos	☐
Impresoras	Controlador de Servidor y Compartición de Recursos	☒

Despois de instalar o módulo, se imos ao apartado de **Estado dos módulos** podemos comprobar que o módulo está deshabilitado, e desta forma os cambios que fagamos coa ferramenta de administración de Zentyal non terán ningún efecto. Así que antes de nada activamos o módulo.



Aceptamos...



pero obtemos un erro, xa que Zentyal nos informa de que para poder activar este módulo hai que configurar cando menos unha interface de rede como externa. Iremos configurar as interfaces de rede do equipo para solventar este problema.

1.4 Configuración das interfaces de rede

Haberá que configurar as interfaces de rede da nosa pasarela, igual que o fixemos no caso do enrutamento en Windows. O máis habitual será que a pasarela de acceso a Internet conte con dúas interfaces de rede, se queremos que a rede local estea separada fisicamente da rede externa. No noso caso, poñerémolle á máquina dúas interfaces de rede, a primeira conectada á rede interna que será pola que se conecten os equipos da rede local e a segunda conectada por NAT que será pola que se terá o acceso a Internet:

- Configuración das interfaces de rede na pasarela

Interfaces de Red

eth0 eth1

Nombre
eth0

Método
Estático

☐ Externo (WAN)
Marque aquí si está usando Zentyal como gateway y este interfaz está conectado a su router a Internet

Dirección IP: 172.16.0.2 Máscara de red: 255.255.0.0

CAMBIAR

Configuramos a interface de rede conectada á rede interna (*eth0*) coa dirección 172.16.0.2. Esta interface non a marcaremos como externa, xa que así Zentyal saberá que esta será a interface conectada á rede local, e será por onde recibirá as peticións dos clientes para conectarse a Internet. Zentyal configurará automaticamente o servizo de firewall e o proxy atendendo a esta información.

Interfaces de Red

La operación solicitada hará que una de las puertas de enlace o rutas estáticas configuradas no sea accesible. Por favor, elimine antes si realmente desea hacer este cambio.

eth0 eth1

Nombre
eth0

Método
Estático

☐ Externo (WAN)
Marque aquí si está usando Zentyal como gateway y este interfaz está conectado a su router a Internet

Dirección IP: 192.168.1.120 Máscara de red: 255.255.255.0

CAMBIAR

Pero cando intentamos cambiar a configuración da interface, vemos unha mensaxe de erro que indica que este cambio faría que a dirección IP que está configurada como porta de enlace predeterminada (o equipo que permite saír a Internet) fora inaccesible dende o equipo, así que antes temos que eliminar esa porta de enlace. Iremos aló.

Configuración de Puertas de Enlace

Lista de Puertas de Enlace

Seleccionado	Nombre	Dirección IP	Interfaz	Porta	Predefinida	Acción
☒	router	192.168.3.1	eth0	1	☒	 Borrar

Proxy

Picamos no apartado de **Portas de enlace** e eliminamos a porta de enlace que temos configurada.

Interfaces de Red

eth0 eth1

Nombre
eth0

Método
Estático

☐ Externo (WAN)
Marque aquí si está usando Zentyal como gateway y este interfaz está conectado a su router a Internet

Dirección IP: 172.16.0.2 Máscara de red: 255.255.0.0

CAMBIAR

Volvemos ahora á configuración da interface para cambiar a dirección IP e a máscara.



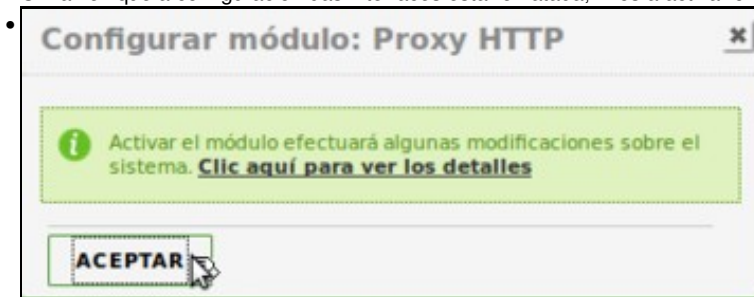
Aceptamos o aviso que nos informa de que estamos facendo cambios nas interfaces de rede do equipo.



Configuraremos a interface *eth1* (conectada por NAT) para que tome unha dirección IP de forma automática, e esta interfaz si debemos marcala como externa. Así Zentyal sabrá que esta interface é a que está conectada a Internet, e configurará o firewall e o proxy de acordo a iso.



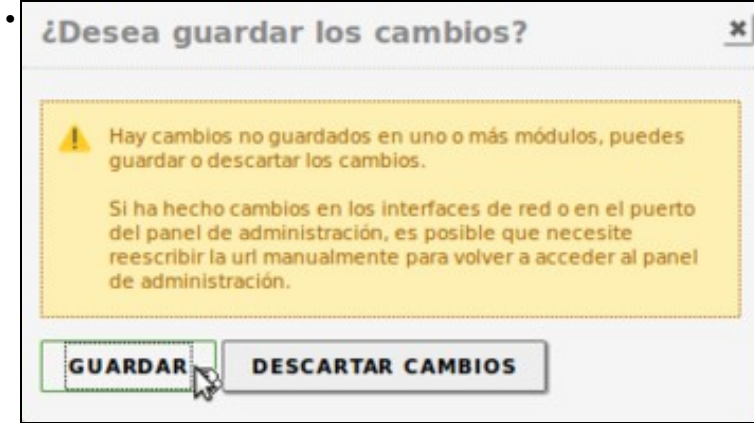
Unha vez que a configuración das interfaces está rematada, imos a activar o módulo de Proxy.



Aceptamos...



e gardamos os cambios.



Picamos en *Gardar*. Listo!!

1.5 Configuración do proxy en modo transparente

Imos ver en primeiro lugar os pasos para configurar un proxy transparente, xa que a configuración dos equipos cliente é máis simple deste xeito.

1.5.1 Configuración do proxy no servidor Zentyal

A configuración de Zentyal é moi simple, xa que só teremos que indicar que queremos habilitar o proxy transparente:

- Configuración do proxy transparente en Zentyal



Imos ao apartado de **Proxy HTTP->Configuración Xeral**, habilitamos a opción de proxy transparente e picamos no botón de **Cambiar**. Aquí vemos as opcións máis básicas do proxy, que son o porto no que escoita (por defecto o 3128), o bloqueo da publicidade nas páxinas web e o espazo en disco que se utilizará para almacenar temporalmente o contido descargado para evitar ter que descargalo de novo (caché).



Gardamos os cambios.

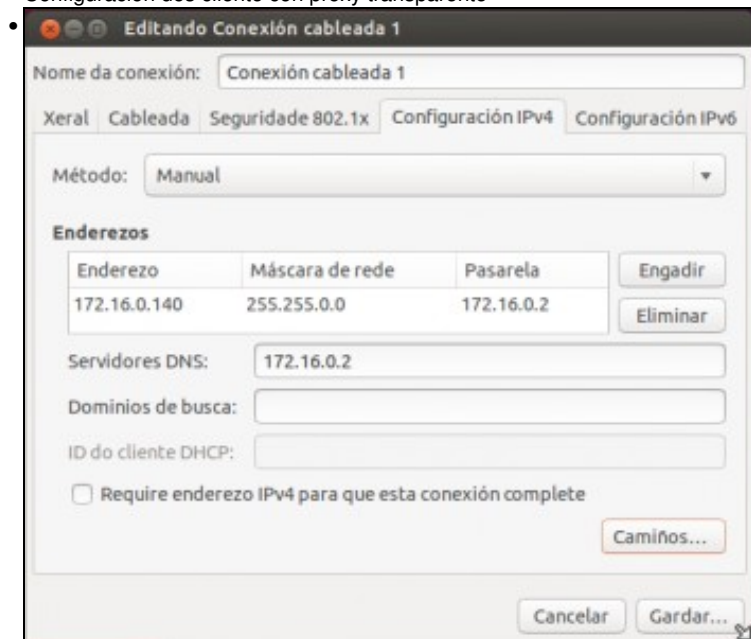
1.5.2 Configuración dos clientes da rede local

A configuración dos clientes co proxy transparente é moi sinxela, xa que simplemente teremos que poñer a dirección IP do servidor (a da interface interna coa que están conectados con unha tarxeta que tamén configuraremos conectada á rede interna) como porta de enlace predeterminada, igual que se fose un router.

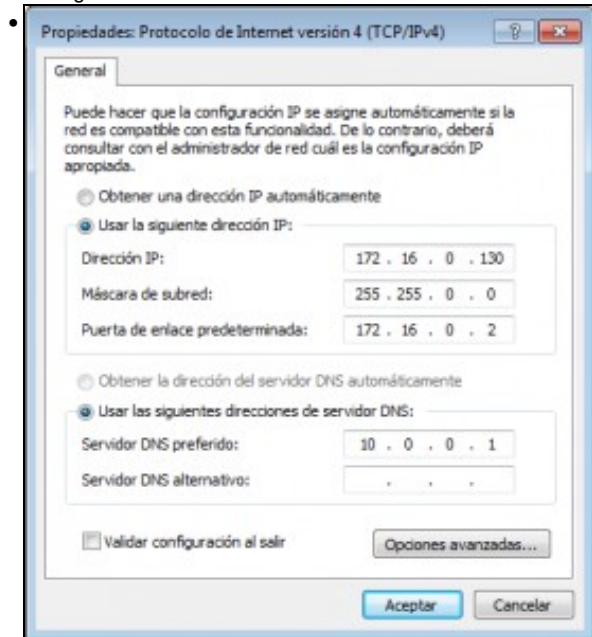
Con respecto á configuración do servidor de DNS nos clientes para poder conectarnos a Internet utilizando os nomes dos servidores (*www.google.es*, *www.xunta.es*, etc.), dado que o servizo de proxy en Zentyal obriga a activar o de *Controlador de dominio e compartición de ficheiros* e este require activar o de DNS, neste momento o noso servidor Zentyal xa pode actuar como servidor de DNS para estes equipos. Polo tanto, temos dúas posibilidades:

- Poñer a dirección IP do servidor Zentyal como servidor de DNS (como se ve na máquina Ubuntu).
- Poñer a dirección IP do servidor DNS que teñamos na nosa rede (como se pode ver na máquina Windows). Neste caso, cada quen terá que poñer as direccións dos servidores DNS que lle proporciona o seu *ISP* (Provedor de Servizo de Internet).

- Configuración dos cliente con proxy transparente



Configuración de cliente Ubuntu.

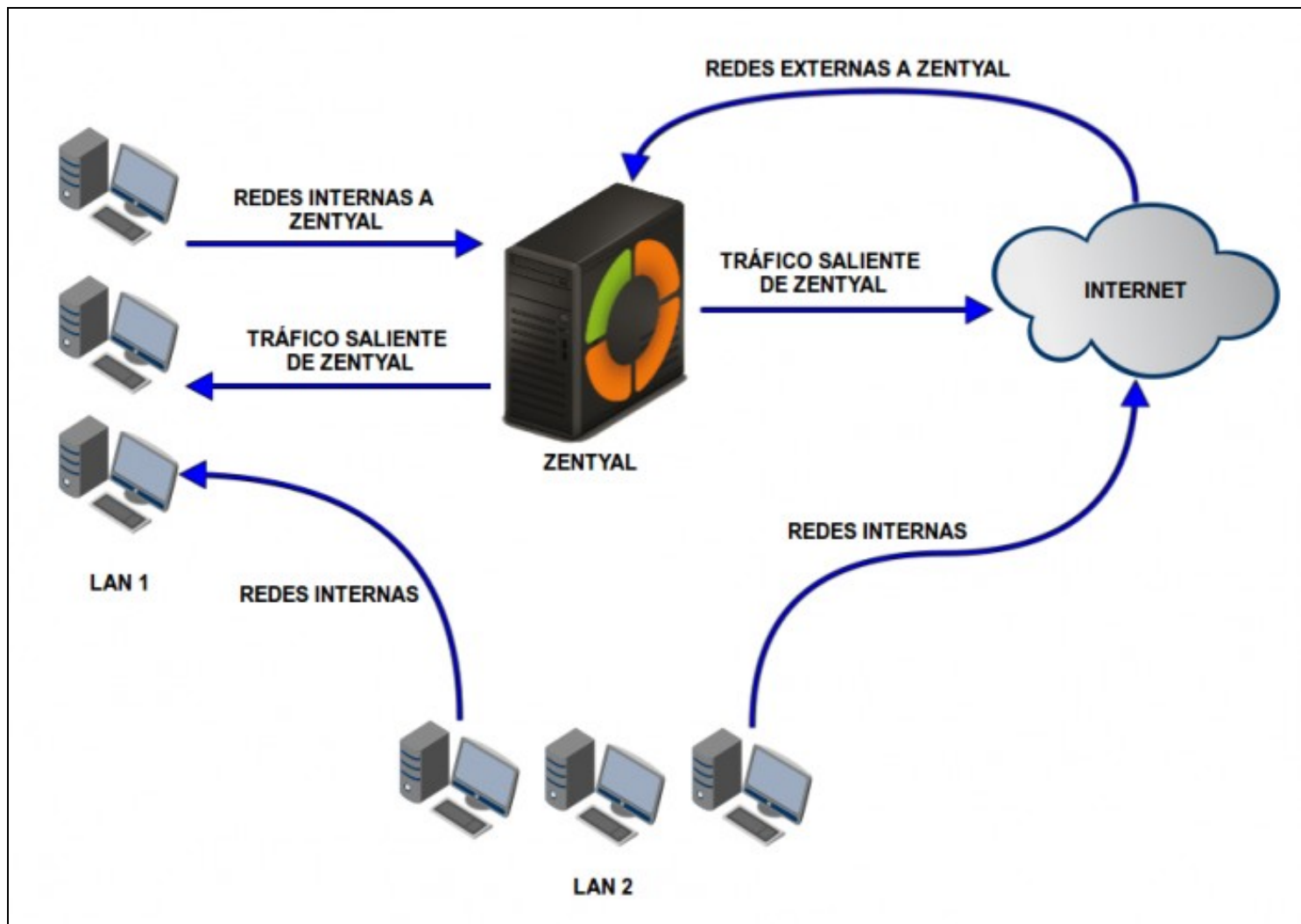


Configuración de cliente Windows.

1.5.3 Configuración do firewall no servidor Zentyal

A configuración do firewall é moi importante xa que vamos permitir configurar que conexións se permitirán e cales non daquelas que **non** son encamiñadas polo proxy, que serán todas as aquelas que non sexan do protocolo HTTP (téñase en conta que o proxy transparente tampouco captura as conexións HTTPS); como por exemplo conexións a servidores de correo, servidores DNS, polo protocolo HTTPS ou calquera outro protocolo.

Para facilitar a configuración do firewall, Zentyal agrupa as regras segundo os tipos de conexións que se poden dar, tendo en conta que interfaces de rede están marcadas como externas e cales non:



Esquema das regras do firewall en Zentyal (imaxe extraída da documentación de Zentyal)

Como se pode ver no diagrama, teremos as seguintes regras de filtrado no firewall:

- **Dende redes internas a Zentyal:** Englobará aquelas conexión que cheguen con destino á propia máquina dende un equipo conectado a algunha interface de rede non marcada como externa.
- **Para as redes internas:** Englobará todo o tráfico que se reciba dende un equipo conectado a algunha interface non marcada como externa que vai dirixido a outro equipo, xa sexa este último dunha rede interna ou externa.
- **Dende redes externas a Zentyal:** Englobará aquelas conexión que cheguen con destino á propia máquina dende un equipo conectado a algunha interface de rede marcada como externa. Normalmente deberemos ser bastante restritivos neste apartado.
- **Tráfico saínte de Zentyal:** Serán os paquetes enviados polo propio equipo.

Imos pois coa configuración do firewall:

- Configuración do firewall nun proxy transparente



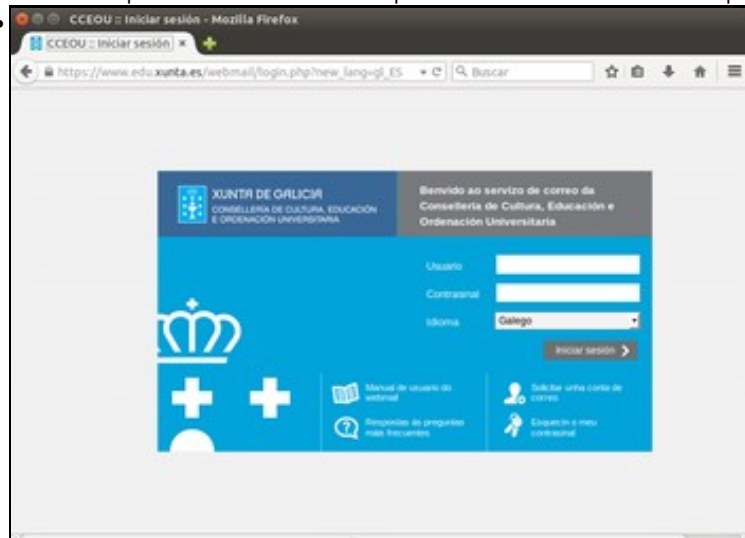
Imos ao apartado de **Cortafuegos->Filtrado de paquetes**, onde podemos ver os distintos tipos de regras que comentamos.



Imos agora ao apartado de regras para as redes internas, para ver a súa configuración.



Estanse aceptando todas as conexións que veñan das redes internas a calquera destino...



Comprobamos dende un equipo da rede interna que podemos establecer conexións HTTPS ¿pero non dixéramos que o proxy transparente non funciona coas conexións HTTPS??



Efectivamente, o que está pasando é que estas conexións non van dirixidas ao porto 80 (onde o proxy está capturando as conexións para redirixilas de forma transparente), senón que van ao porto 443 (que é o porto asociado a unha conexión https). O que pasa neste caso é que Zentyal encamiña estas conexións a nivel de rede co servizo de enrutamento, e como a regra do firewall establece que se acepten todas as conexións, déixanse pasar. Isto pode ser un problema porque hai programas como *Ultrasurf* que se saltan os proxys creando conexións HTTPS, así que imos ver como denegalas. Deberemos ter definido un servizo que identifique este tipo de conexións: Imos ao apartado de **Rede->Servizos** para ver os servizos definidos e atopamos que xa aparece o servizo HTTPS. Entramos na súa configuración



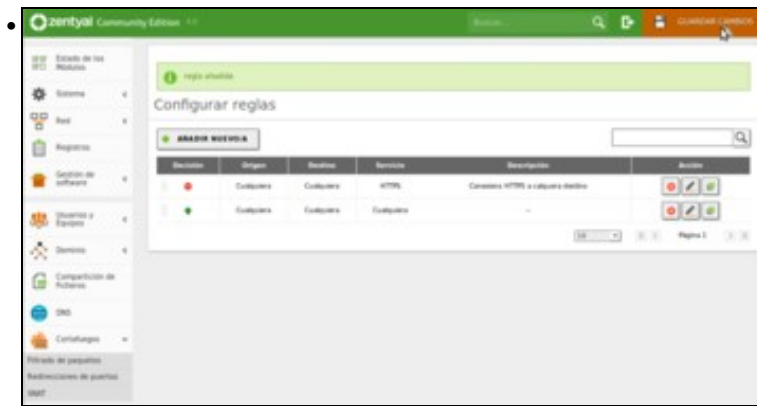
Vemos que o servizo se asocia a todos os paquetes que teñan como porto de destino o 443 (xusto o que precisabamos, en caso de que non estivera definido teríamos que definilo nós).



Agora volvemos ás regras do firewall para as redes internas, para engadir unha nova regra.



A regra indica que se deneguen as conexións que se correspondan co servizo HTTPS (que serán as que teñen como destino o porto 443).



Gardamos os cambios...



e comprobamos que xa non podemos acceder dende os equipos da rede interna a páxinas HTTPS. Na imaxe pódese ver que se está intentando cargar a páxina dende o cliente, pero non chega a recibir a resposta.

1.6 Configuración do proxy en modo non transparente

Imos ver agora como configuraríamos un proxy non transparente na nosa rede local, o cal vai implicar unha configuración explícita do servidor proxy nos equipos.

1.6.1 Configuración do proxy no servidor Zentyal

Realmente non é necesario facer ningún cambio na configuración do proxy para utilizar o proxy en modo non transparente, xa que podemos configurar o servidor proxy explicitamente nos equipos cliente e deixar igual a opción de proxy transparente activada. De feito, esta opción sería moi recomendable porque así os equipos que teñan o proxy configurado poden usalo para conexións HTTPS, pero os que non o teñan tamén poden usalo de forma transparente polo menos para as conexións HTTP.

De todas formas, imos desactivar a opción de proxy transparente para forzar neste caso a que os equipos da rede interna teñan que facer unha configuración explícita do proxy para poder ter acceso a Internet:

- Configuración do proxy en modo non transparente



Desactivamos a opción de proxy transparente...

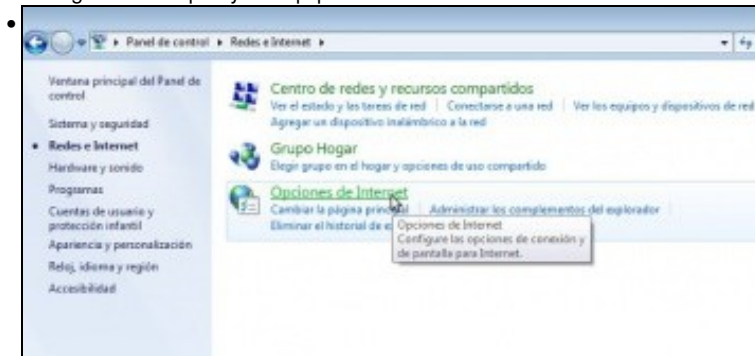


e gardamos os cambios.

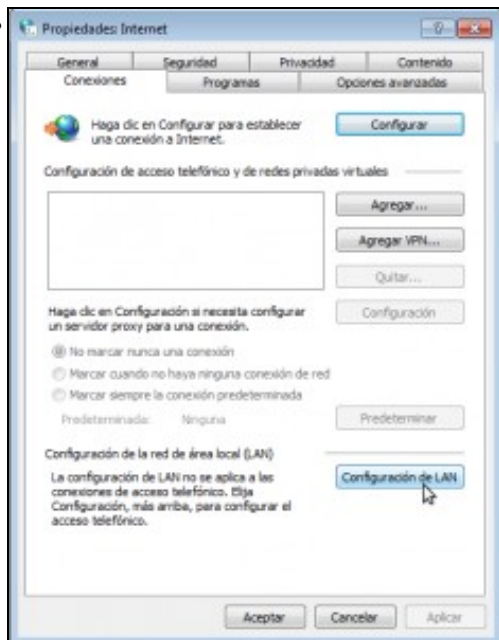
1.6.2 Configuración dos clientes da rede local

Nos clientes da rede local teremos que configurar o servidor proxy para que poidan conectarse a Internet. Imos ver como podemos facelo tanto en clientes Windows como Linux:

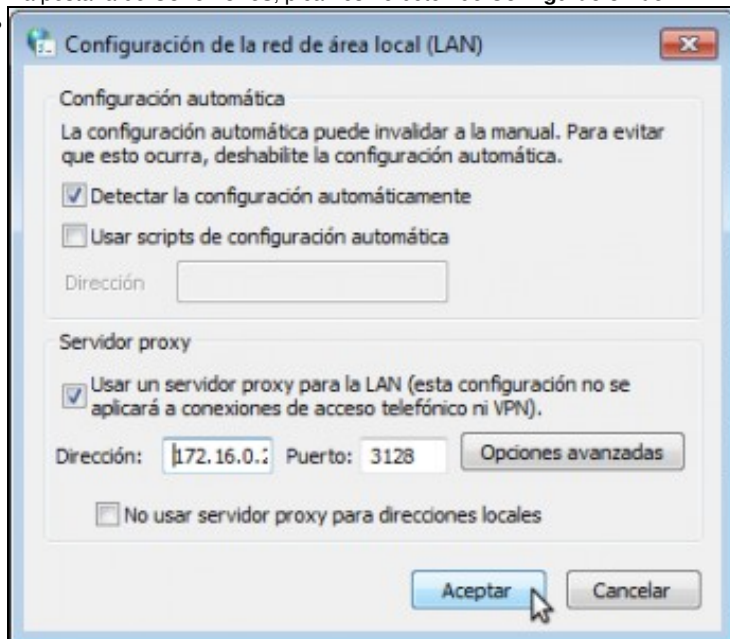
- Configuración do proxy en equipos cliente



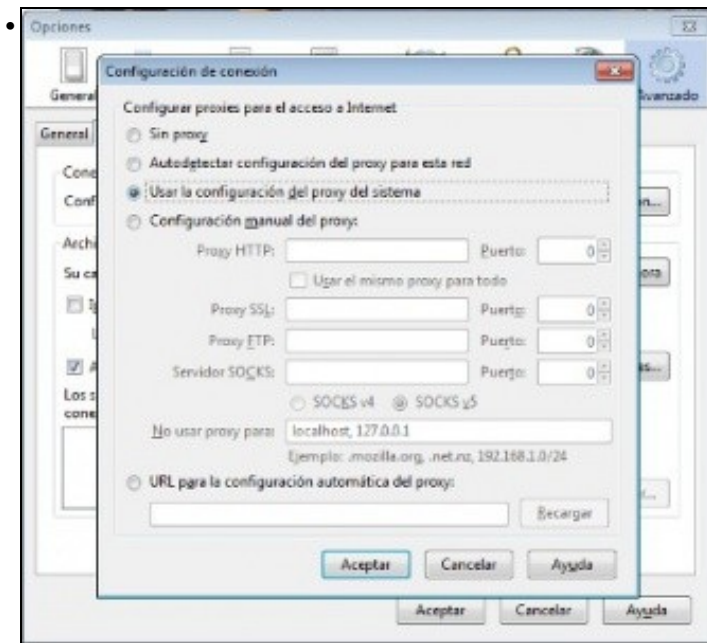
En Windows, entramos no apartado de **Redes e Internet** do **Panel de control** e picamos en **Opciones de Internet**.



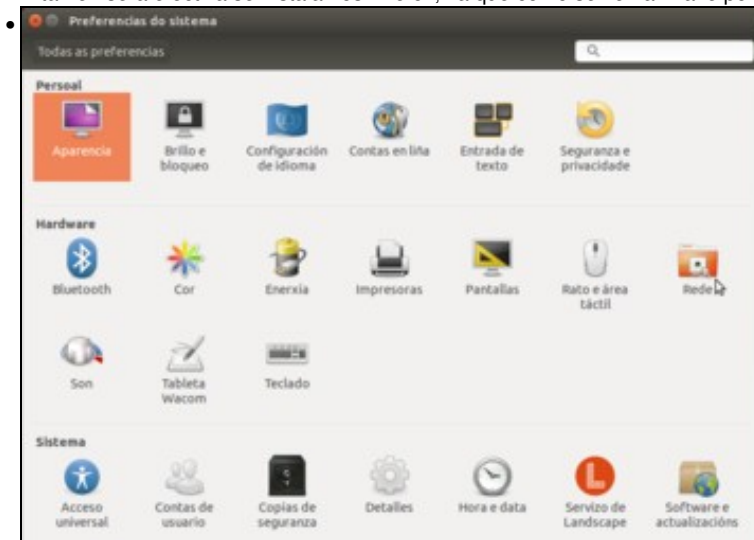
Na pestana de **Conexiones**, picamos no botón de **Configuración de LAN**.



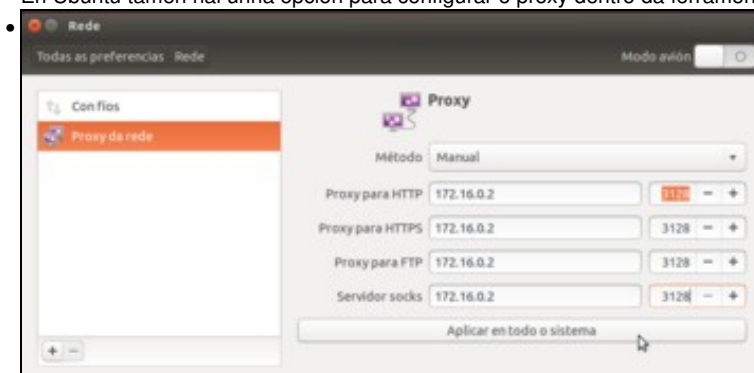
Activamos a opción de **Usar un servidor proxy** e indicamos a dirección IP e porto do servizo de proxy. Esta configuración xa afectará ao navegador Internet Explorer e ás aplicacións de Windows.



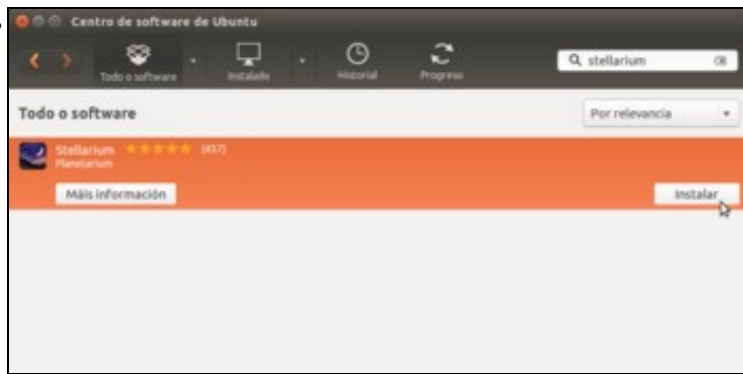
E tamén será efectiva se instalamos Firefox, xa que como se ve na imaxe por defecto toma a configuración proxy do sistema.



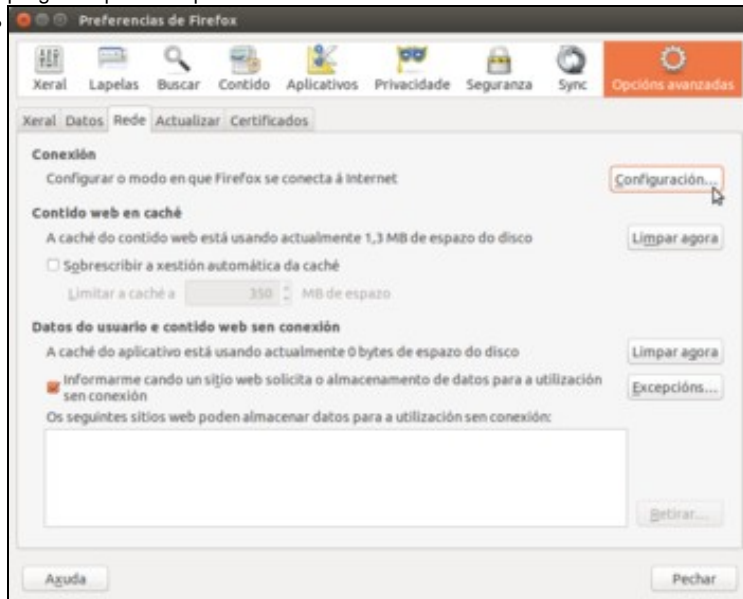
En Ubuntu tamén hai unha opción para configurar o proxy dentro da ferramenta de **Preferencias do sistema**, dentro do apartado de **Rede**.



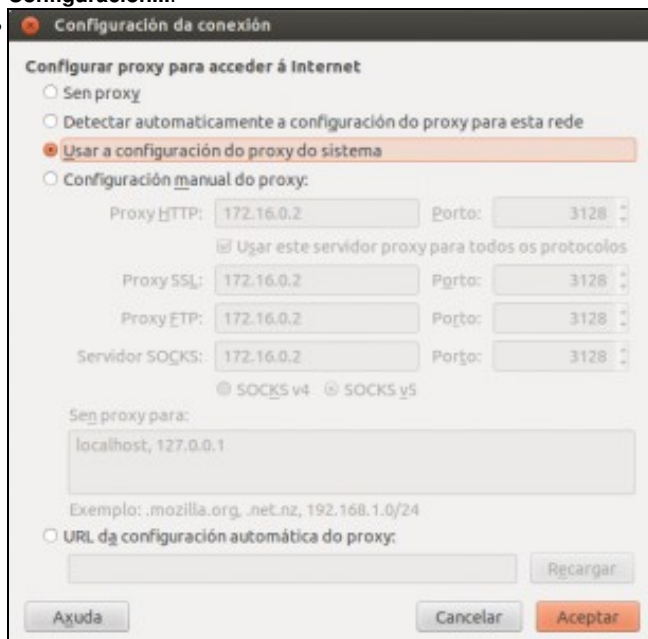
Seleccionamos o apartado de **Proxy de rede** e introducimos os datos do proxy. Picamos no botón de **Aplicar en todo o sistema**.



Desta maneira a configuración afecta a todas as aplicacións do sistema, como por exemplo Centro de software. Podemos instalar un novo programa para comprobalo.



O firefox tamén utilizará esta configuración se temos activada a opción de que tome a configuración do proxy do sistema. Para atopar esta opción, dentro das preferencias do programa imos ao apartado de **Opcións avanzadas** e na pestana de **Rede** picamos no botón de **Configuración....**

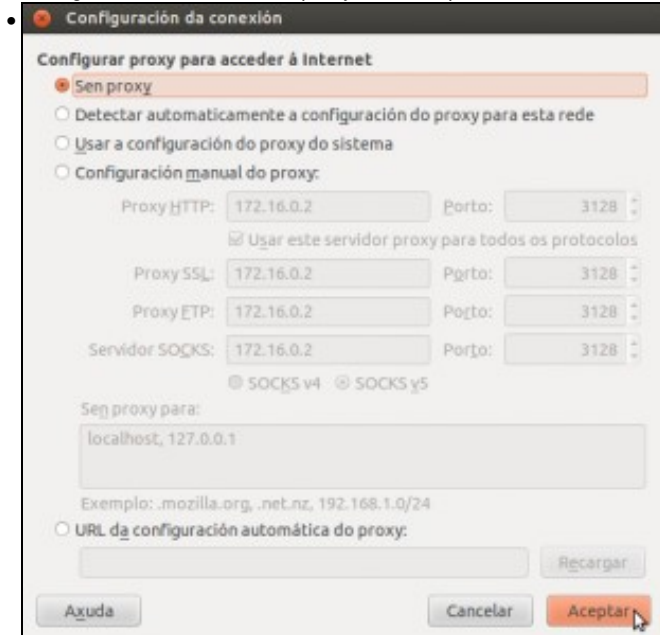


Aquí podemos indicar ao navegador que utilice a configuración do sistema, ou tamén se o queremos configurar o proxy de forma manual.

1.6.3 Configuración do firewall no servidor Zentyal

Configurando o proxy en modo non transparente, cómpre denegar as conexións HTTP (as que reciban polo porto 80) se queremos forzar aos clientes a que utilicen o proxy para saír a Internet.

- Configuración do firewall con proxy non transparente



Imos comprobar que pasa se un equipo cliente non configura o proxy para saír a Internet. Na configuración de firefoz, seleccionamos a opción de **Sen proxy** para que non faga caso da configuración do sistema e non use ningún tipo de proxy.



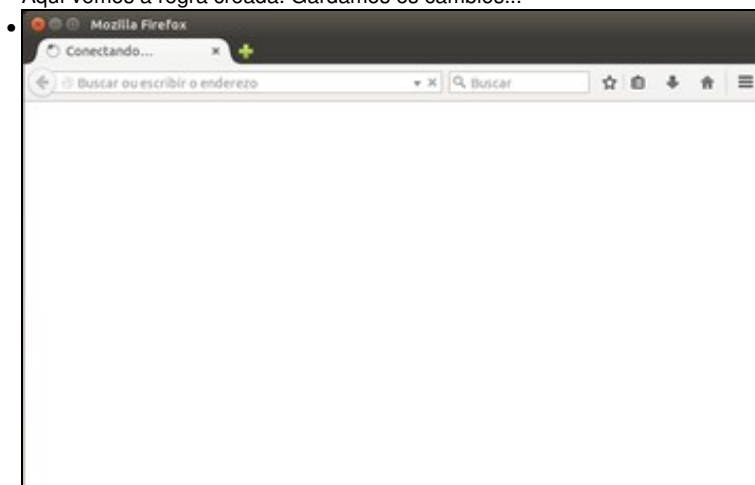
O navegador pode conectarse á web se problema ¿Como? Pois igual que pasou anteriormente coas conexións HTTPS, o servidor Zentyal está encamiñando os paquetes utilizando o servizo de enrutamento, e así os clientes poden *saltarse* o proxy.

-

Para evitalo, engadimos unha regra no firewall para as redes internas, denegando as peticións ao servizo HTTP. Neste caso o servizo xa existe, non temos que crealo, e está asociado ás peticións recibidas polo porto 80.

-

Aquí vemos a regra creada. Gardamos os cambios...



e comprobamos que agora o equipo cliente non pode conectarse á web se non o fai a través do servidor proxy.

Nota: A configuración do firewall que se mostra en calquera dos casos no servidor Zentyal é simplemente a modo de exemplo e para poder explicar o funcionamento básico do firewall en Zentyal, pero en cada caso particular esta configuración pode variar en función das conexións que se queiran permitir ou denegar na rede local. ¿Queremos adoptar unha política *permisiva* (permitir todas as conexións salvo algúns tipos de tráfico concreto, como neste caso) ou *restrictiva* (denegar todas as conexións salvo o tráfico que estea explicitamente autorizado)? ¿Que tipo de conexións queremos que se poidan establecer dende os equipos da rede local (POP, IMAP, FTP, SSH, etc.)? ¿A que ou dende que equipos? En función disto en cada caso teremos que introducir as regras correspondentes.



TAMÉN PODES VER

Os seguintes enlaces da documentación de Zentyal abordan a configuración do servizo de firewall, encamiñamento e proxy HTTP:

- O servizo de firewall en Zentyal
- O servizo de encamiñamento en Zentyal
- O servizo de proxy HTTP en Zentyal

-- Antonio de Andrés Lema e Carlos Carrión Álvarez -- (xan 2015).