

1 Filtrado de páxinas web

Neste apartado imos ver como podemos filtrar as páxinas web ás que se acceden a través do proxy de Zentyal en base a diferentes criterios, que van dende a presenza de virus ata a a extensión do ficheiro ao que se accede.

1.1 Sumario

- 1 Tipos de filtro de contidos no proxy en Zentyal
- 2 Configuración do filtrado no proxy
 - ◆ 2.1 Filtro de virus
 - ◆ 2.2 Filtro de contido
 - ◆ 2.3 Filtro de dominios
 - ◆ 2.4 Filtros de tipos MIME e extensións de ficheiros

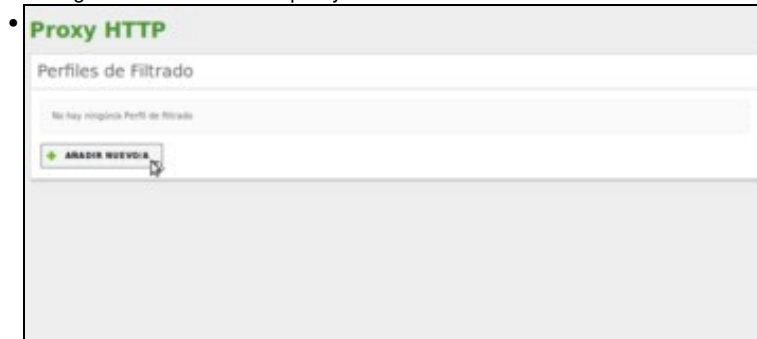
1.2 Tipos de filtro de contidos no proxy en Zentyal

O proxy de Zentyal inclúe varios filtros de contidos que poden ser combinados para restrinxir o acceso á rede externa da forma que desexemos. Os filtros incluídos son:

- **Filtro de virus:** Utilizando o antivirus **clamav**, permite bloquear o acceso a páxinas que conteñan código detectado como virus.
- **Filtro de contido:** Permite filtrar páxinas polo seu contido usando diversas listas de palabras. Hai que ter en conta que este filtro pode bloquear páxinas ás que en realidade si queremos acceder, polo que pode ser configurado en distintos niveis de intensidade que van dende *moi permisivo* ata *moi estrito*. Tamén podemos incluír unha páxina nunha lista branca se queremos garantir que se permita o acceso á mesma independentemente do seu contido.
- **Filtro de dominios:** Permite filtrar páxinas polo dominio de DNS do servidor no que residen (*google.es*, *xunta.es*, etc.).
- **Filtro de tipos MIME:** Permite restrinxir certos obxectos MIME de elementos incrustados nas páxinas, como obxectos flash, java, activeX, etc.
- **Filtro de extensión de ficheiros:** Permite restrinxir a descarga de ficheiros que teñan unha extensión determinada.

1.3 Configuración do filtrado no proxy

- Configuración do filtrado no proxy



Dentro da configuración do *Proxy HTTP*, imos ir ao apartado de **Perfiles de filtrado**. Como vemos, non hai creado ningún perfil, así que a única opción que temos dispoñible é a de crear un novo.



Só temos que introducir o nome para o perfil, neste caso **filtro**.



Vemos o perfil xa creado, e poderíamos crear diferentes perfís de filtrado para actuar de forma distinta sobre distintos equipos da rede ou grupos de usuarios. Picamos no botón de **Configuración** do perfil.

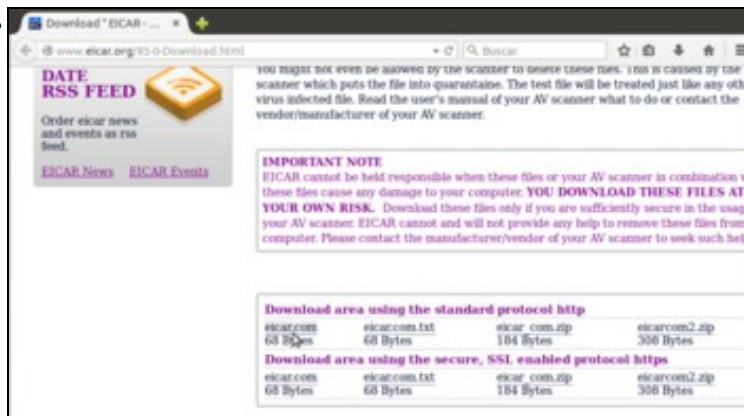


Nesta páxina podemos configurar os distintos filtros do perfil. Como xa temos instalado o módulo de antivirus, a opción de activar este filtro xa está dispoñible dentro da pestana de *Configuración*, e como podemos ver xa está activada por defecto (se non estivera, activámola). Desta forma, xa temos o filtro de antivirus funcionando.

1.3.1 Filtro de virus

Imos neste apartado a comprobar o funcionamento do filtro de virus:

- Filtro de virus



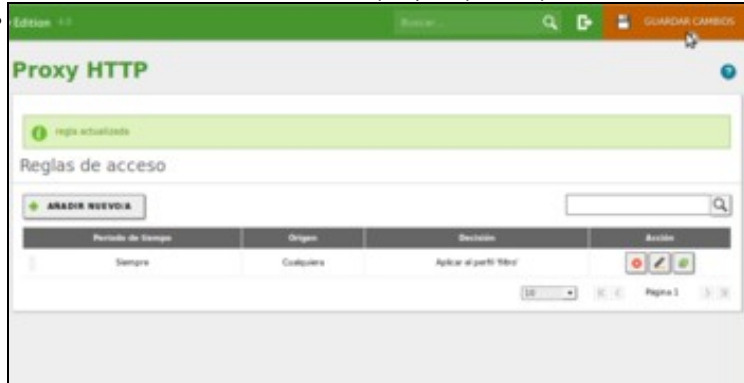
Para probar o seu funcionamento, dende un cliente imos á páxina <http://www.eicar.org/85-0-Download.html>, e picamos nun enlace ao ficheiro **eicar.com** que contén un virus inofensivo. Pero a pesar de ter o filtro de virus activado, vemos que o proxy non impide que nos descarguemos este ficheiro ¿Por que?



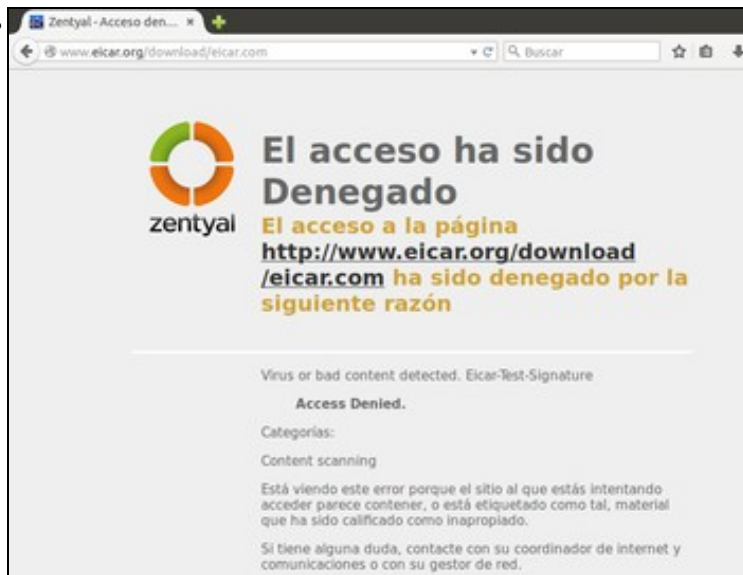
O que pasa é que o perfil de filtrado *filtro* non se está aplicando. Imos a entrar na ferramenta de administración de Zentyal no apartado de **Reglas de acceso** dentro da configuración do **Proxy HTTP**. As regras de acceso permítenos configurar como queremos que se comporte o proxy ante os distintos tipos de conexións (en función da súa orixe e/ou de cando se produzan). Comprobamos que a única regra de acceso definida establece que sempre se permiten todo tipo de conexións, así que imos editar esta regra.



Cambiamos a decisión de *Permitir siempre* por *Aplicar o perfil de filtrado "filtro"*, e picamos en **Cambiar**.



Agora segundo a regra de acceso que ten configurada o proxy aplicará para todas as conexións o perfil de filtrado. Gardamos os cambios.



Comprobamos que o proxy agora bloquea o acceso a este ficheiro.

1.3.2 Filtro de contido

Como xa comentamos, este filtro restrinxirá o acceso a páxinas que conteñan unha serie de palabras, en distintos idiomas. Téñase en conta que este filtro pode impedir o acceso a páxinas que si poden ser do noso interese:

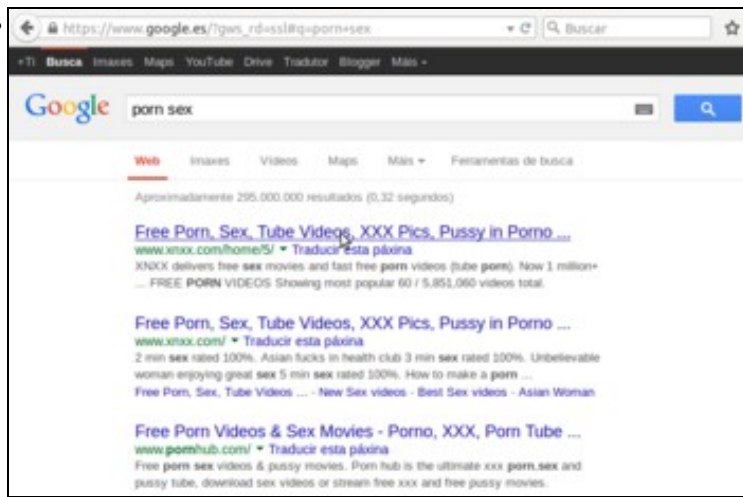
- Configuración do filtro de contido



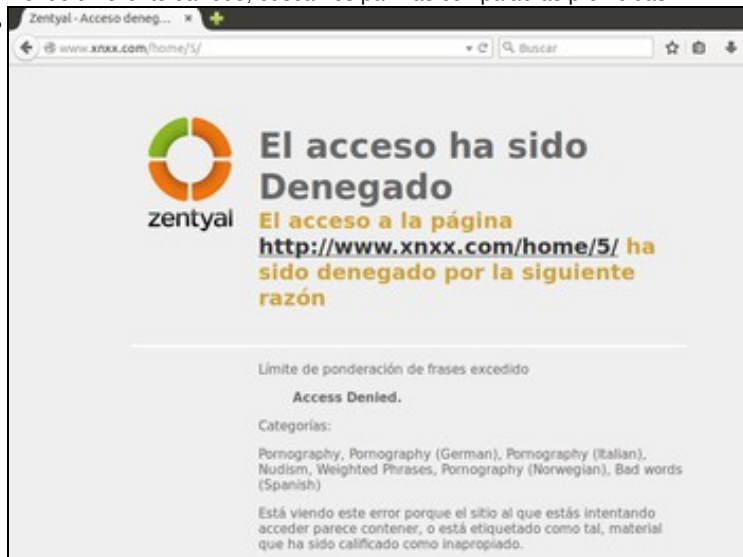
Cambiamos o umbral do filtro de contidos a **Moi estrito** para facilitar o bloqueo de páxinas.



Gardamos os cambios.



Dende un cliente da rede, buscamos páxinas con palabras prohibidas.



Comprobamos que o proxy impide o acceso a estas páxinas.

1.3.3 Filtro de dominios

Este filtro permitirá introducir unha serie de dominios ou URLs que poderán ser permitidos ou denegados polo proxy:

- Configuración do filtro de dominios



Dentro da configuración do perfil de filtrado, imos á pestana de **Reglas de dominios e URLs**. Vemos que non hai ningunha regra de dominio creada, así que picamos no botón de **Engadir novo**.



Introducimos un nome de dominio que queremos denegar (*minijuegos.com*).



Vemos o dominio engadido na lista, e poderíamos incluír tantos dominios como quixéramos. Gardamos os cambios.



Comprobamos que dende o cliente non se pode acceder ao dominio.



A opción de **Bloquear sitios especificados sólo como IP** pode ser interesante para evitar que dende os clientes se intente acceder a dominios non permitidos introducindo no enderezo do navegador a dirección IP do servidor en lugar do seu nome de DNS.

1.3.4 Filtros de tipos MIME e extensións de ficheiros

Estes filtros permiten rexeitar a descarga de elementos dun **tipo MIME** determinado ou de ficheiros que teñan unha extensión concreta:

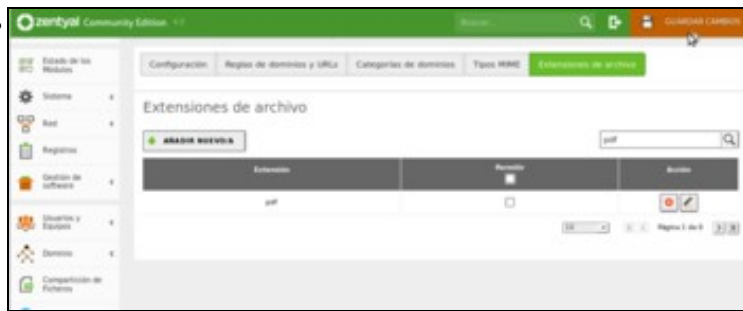
- Configuración dos filtros de tipos MIME e extensións de ficheiros



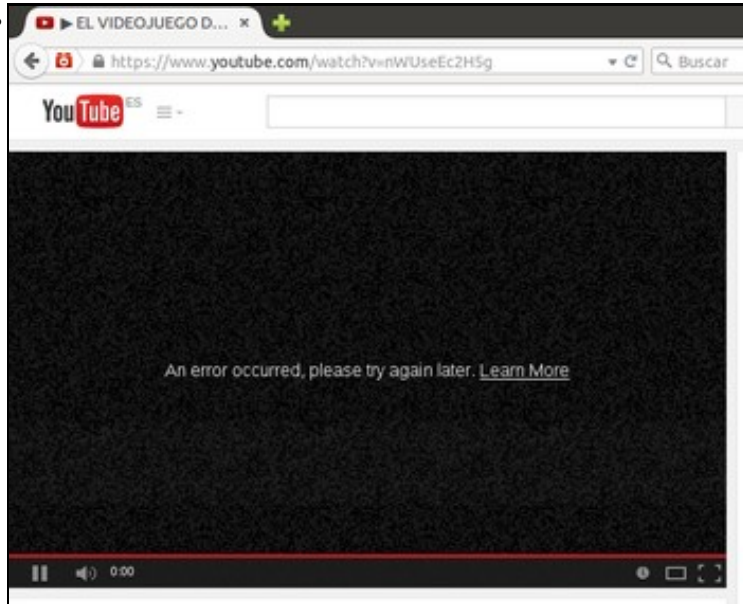
No filtro de tipos MIME, desactivamos o de flash, de forma non se permitirá a descarga de animacións en flash.



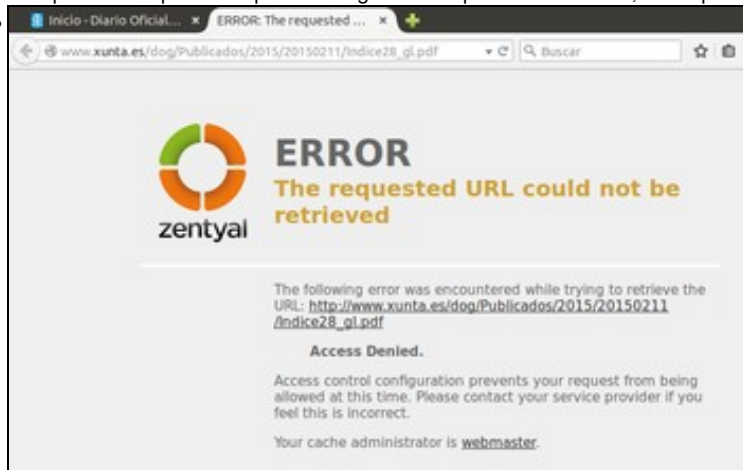
E no filtro de extensións impedimos o acceso a ficheiros coa extensión pdf.



Gardamos os cambios.



Comprobamos que non é posible cargar os compoñentes de flash, como por exemplo os vídeos de *youtube*.



Tampouco podemos descargar un documento *.pdf*.

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