Introducción a pfSense

pfSense es una distribución basada en FreeBSD, derivada de m0n0wall. Su objetivo es tener un cortafuegos (firewall) fácilmente configurable a través de una interfase web e instalable en cualquier PC, incluyendo los miniPC de una sola tarjeta.

Se trata, por tanto, de una solución muy completa, bajo licencia BSD y, por tanto, de libre distribución.

El cortafuegos forma parte del Kernel del sistema. De hecho, se trata del Packet Filter (PF) originario de OpenBSD, considerado com el sistema operativo más seguro del mundo.

Packet Filter (PF) está presente como estándar en FreeBSD desde noviembre de 2004. Incluye funcionalidades como el regulador de caudal ALTQ, que permite asignar prioridades por tipo de tráfico.

Los desarrolladores de pfSense escogieron FreeBSD en lugar de OpenBSD por su facilidad de instalación en el mundo de lps PCs y porqué ya existía BSD Installer, una versión muy, muy reducida de FreeBSD.

Todo ello da una gran flexibilidad a la solución pfSense, ya que se puede montar tanto en equipos miniPC (basados en una sola placa) que emplean como disco una Compact Flash como en PC estándar con disco duro. En este último caso se pueden añadir paquetes como Snort, Squid, Radius, etc.

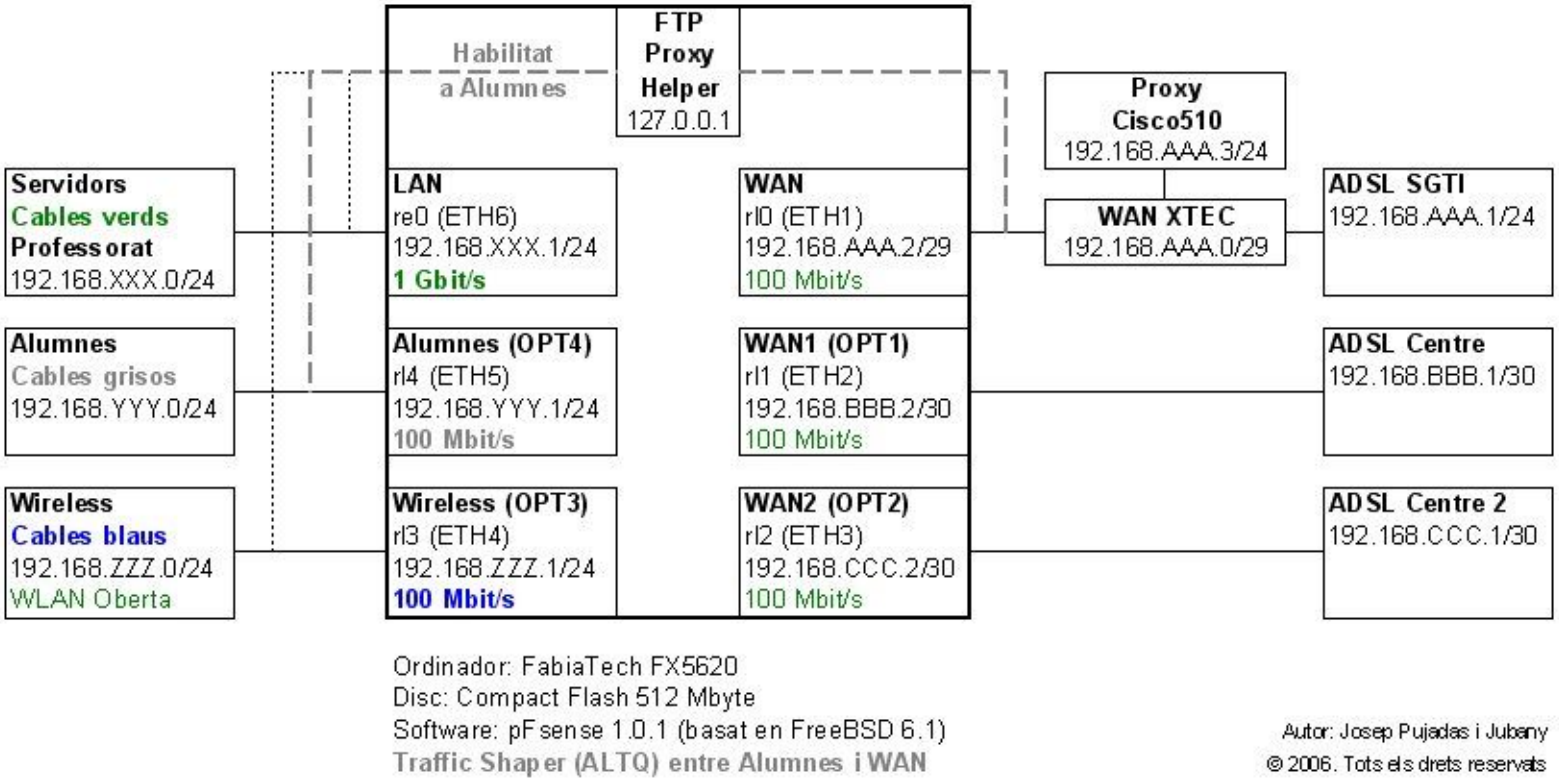
En esta web se explica cómo se ha configurado un pfSense 1.0.1 (octubre/noviembre 2006) que está en producción. En ningún caso es una web donde se tratan todas las posibilidades de este cortafuegos de código libre.

Caso-Estudio

Objetivos

- Aislar física y lógicamente las redes dedicadas a servidores, profesorado, alumnos i sin hilos (wireless). Seguridad **de dentro a dentro**.
- Regular las comunicaciones entre las distintas redes locales y de las redes locales a Internet. Seguridad **de dentro a dentro** y **de dentro a afuera**.
- Aprovechar el caudal de las tres ADSL de que se dispone, a poder ser de forma automática. Balanceo de carga.
- Aumentar la seguridad en los servicios que tenemos en Internet. Seguridad **de afuera a dentro**.
- Poder tener una red sin hilos (wireless) abierta.
- Utilizar una solución abierta, de código libre.
- Utilizar un hardware de tamaño reducido, integrable en el armario de comunicaciones.
- Utilizar un hardware no basado en disco duro, que no requiera protección con un SAI de apagado y puesta en marcha automáticos.
- Poder configurar todos los dispositivos de la red (ordenadores, impresoras, puntos de acceso, ...) mediante DHCP estático, es decir, asignándoles una dirección IP en función de su dirección MAC.
- Control del uso de aplicaciones P2P.
- Estandarizar y automatizar la configuración de los navegadores en lo que se refiere al uso de servidores intermediarios (proxy) y la configuración de red de todas las máquinas.

Esquemáticamente, el montaje ha quedado tal como muestra la figura (observa que tienen que haber seis redes diferenciadas AAA, BBB, CCC, XXX, YYY i ZZZ):



Prácticamente todos los objetivos han sido sobradamente logrados, fuera de algunas limitaciones que se han encontrado. pfSense tiene muchas funcionalidades, pero hay que tener en cuenta que algunas son incompatibles entre ellas. Y, por tanto, hay que escoger cuál es la mejor opción. Se explican a continuación las decisiones adoptadas.

Balanceo de carga de las ADSL

pfSense permite balanceo de carga con detección de fallo (fail-over), lo que resulta muy interesante si se tiene más de una ADSL. Esta prestación permite pues equilibrar las cargas de las ADSL y en caso de fallo de una de ellas redireccionar su tráfico hacia otra.

pfSense emplea para el balanceo el demonio (daemon) slbd. Como la mayoría de balanceadores, su intención es mejorar la navegación por Internet y no entiende las conexiones múltiples. Ello descarta su uso en accesos FTP. Por tanto, o se renuncia a balanceo o se renuncia a FTP. O bien se monta otro pfSense sólo para FTP. Se decidió renunciar al balanceo.

El balanceo se configura definiendo una pila (pool) donde se indica la IP pública de cada ADSL (IP a monitorizar) y la IP privada por la que se accede a la ADSL. Entonces pfSense comprueba periódicamente si la ADSL en cuestión está funcionando, haciéndole un ping. Se necesita, por tanto, que la IP pública de la ADSL conteste a estos ping internos. De lo contrario, pfSense no sabrá ver si la ADSL está activa.

Las comunicaciones peer-to-peer (P2P)

Otro de los quebraderos de cabeza de los administradores de red son las descargas indiscriminadas empleando programas como Emule o Ares: ocupación del ancho de banda, problemas de seguridad, ilegalidad, ...

Una solución drástica es hacer que las conexiones a Internet estén permitidas sólo hacia los puertos (servicios) más usuales (80, 443, 21, 53, 119, ...) En http://www.iana.org/assignments/port-numbers encontrarás la lista oficial de puertos.

La otra solución es emplear el regulador de caudal (traffic shaper) ALTQ que tiene pfSense y poner los accesos P2P en la cola de prioridades. Es una solución que requiere un cierto ajuste, pero es la más recomendable. Actualmente tiene la limitación que sólo se puede emplear ALTQ entre una de las LAN y una de las WAN del cortafuegos (es decir, ALTQ en pfSense no es multiWAN, pero se está trabajando para que lo sea ...)

En todo caso, tanto si se emplea una solución como otra, tiene que entrar en juego otra prestación de pfSense: FTP-Proxy Helper.

FTP-Proxy Helper

Se trata de una funcionalidad de Packet Filter (PF), que permite que la propia máquina (127.0.0.1) haga de intermediario (proxy) para las conexiones FTP. De esta manera queda obviado el problema de que un cliente FTP opere con el servidor no sólo por el puerto 21 si no también con un puerto dinámico, que está por encima del 1023 y que se confunde a la vez con un acceso P2P.

Desgraciadamente FTP-Proxy Helper tampoco es multiWAN, lo que se traduce en que siempre sale/entra por la puerta de enlace por defecto que tenga nuestro pfSense. Es por ello que en el esquema anterior se puede ver que sólo ha sido activado para la red Alumnes, al igual que ALTQ.

Si tienes más curiosidad a cerca de cómo funciona FTP-Proxy Helper visita http://www.openbsd.org/faq/pf/ftp.html#client

DMZ (zona desmilitarizada)

En el esquema de más arriba se puede ver que no hay una DMZ (zona desmilitarizada) propiamente dicha. Se ha renunciado a ella porqué implicaba un profundo cambio en la estructura de servidores, se necesitaba una séptima tarjeta de red en el cortafuegos y otro concentrador de red (switch) para la DMZ. A pesar de que no tener una DMZ no es una situación ideal, la adopción de pfSense con la estructura propuesta es, sin duda, un importante aumento de seguridad.

Estados y diagnósticos

pfSense tiene toda una serie de herramientas que permiten ver con todo detalle qué está pasando o qué ha pasado. Estado de las conexiones, gráficos del uso de cada interfase (históricos y en tiempo real), herramientas de diagnóstico, ... El administrador de red tiene pues con pfSense las herramientas necesarias para poder tomar decisiones sobre el tráfico de su red.

Instalación

Preparativos

Antes de la implantación definitiva de pfSense se tuvieron que hacer los siguientes cambios en la red:

- Dividir el cableado existente en seis redes físicas. Ello se hizo pasando algunos cables más del armario secundario al armario primario, instalando más concentradores (switch) en ambos armarios y cambiando el conexionado de equipos en los armarios. No hay más de dos concentradores encadenados (tal como estaba antes de los cambios).
- Adoptar DHCP en todos los ordenadores clientes. Ello se hizo activando provisionalmente DHCP en uno de los routers ADSL.
- Cambiar todos los procesos por lotes (archivos BAT y CMD en Windows, scripts de shell en máquinas Unix/Linux) que empleaban direcciones IP locales, poniendo su correspondiente nombre de máquina.
- Cambiar todos los puertos de impresora que estaban por dirección IP local, poniendo su correspondiente nombre de máquina.
- Asegurarse que el DNS local resuelve correctamente todos los nombres de máquina.
- Asegurarse que el archivo hosts de las máquinas sólo contiene la línea: 127.0.0.1 localhost. Es decir, que no se emplea para resolver nombres de máquina, excepto localhost.
- Cambiar la configuración proxy de los navegadores de Internet, poniendo la configuración automática

http://www.dominio.ejemplo/proxy.pac.

- Deshabilitar el acceso sin hilos de todas las impresoras que tienen esta funcionalidad, dejando sólo el acceso por red cableada.

Hardware utilizado

Se trata de un miniPC de FabiaTech, modelo FX5620.

El equipo tiene 5 puertos Ethernet de 100 Mbit/s y un sexto de 1 Gbit/s. Puede incorporar un disco duro de 2,5" (como los que llevan los portátiles) y una Compact Flash (que actúa como disco duro).

Se adquirió en Gran Bretaña, http://linitx.com/product_info.php?cPath=4&products_id=909. Pedido el domingo por la noche (pago con tarjeta de crédito) y el martes por la mañana ya llegaba (cerca de Barcelona) ...

Se compró también una tarjeta Compact Flash Kingston, de 512 MByte, a un proveedor local.

25-junio-2009
No adquirir el modelo FX5621. Sólo funciona correctamente si se deshabilita la primera boca de 1 Gbit/s (NIC número 5 en la BIOS): forum.pfsense.org/index.php/topic,17116.0.html

Descarga de pfSense

Se puede ir a la web oficial www.pfsense.org, pero hay otros repositorios con configuraciones ajustadas.

Así, en http://shopping.hacom.net/catalog/pub/pfsense/ se encuentran versiones preparadas según la unidad que reconoce pfSense para la Compact Flash y según su tamaño.

Notas importantes

Hay dos tipos de imágenes de pfSense:

- **Embedded**. Es la que se emplea para Compact Flash, tiene los acesos a disco minimizados y no admite instalación de paquetes. De esta forma se preserva la vida de la Compact Flash. Se presenta comprimida con gzip, con la extensión img. **No soporta ni teclado ni monitor, hay que conectar cable serie para acceder a la consola de pfSense y poder hacer la configuración inicial.**

- **LiveCD**. Es una imagen iso, también comprimida con gzip, para ser ejecutada desde el propio CD. Tiene una opción para instalar pfSense en disco duro y a partir de entonces se pueden instalar paquetes, muchos de ellos administrables desde la interfase web.

Últimas imágenes oficiales de pfSense (versión oficial con todos los parches que hayan salido):

- **Embedded**: http://snapshots.pfsense.org/FreeBSD6/RELENG_1_2/embedded

- **LiveCD**: http://snapshots.pfsense.org/FreeBSD6/RELENG_1_2/iso

Imágenes no-oficiales de Hacom:

Hacom es una empresa californiana que ofrece distintos tipos de cortafuegos, la mayoría de ellos basados en miniPC con tarjeta Compact Flash. Las imágenes **Embedded** en http://shopping.hacom.net/catalog/pub/pfsense se diferencian de las oficiales por:

- Usar el gestor de arranque grub en lugar del propio de FreeBSD.

- Soporte para teclado y monitor. **No se precisa cable serie para la configuración inicial.**

- Las imágenes que empiezan por **pfSense-releng_1_2-snapshot070424** corresponden a la versión 1.2 BETA de pfSense, con fecha 24-abril-2007. **Tengo esta versión funcionando satisfactoriamente desde el 25-abril-2007.**

FX5620 con pfSense nos reconoce la Compact Flash como la unidad **ad2** (tercer disco ATA en FreeBSD).

En uno de nuestros servidores FreeBSD hicimos:

```
mkdir pfSense
cd pfSense
vi fetch.sh
```

```
#!/bin/sh
fetch http://shopping.hacom.net/catalog/pub/pfsense/pfSense-1.0.1-512-ad2.img.gz.md5
fetch http://shopping.hacom.net/catalog/pub/pfsense/pfSense-1.0.1-512-ad2.img.gz

chmod +x fetch.sh
./fetch.sh
```

Nota: Me gusta tener un script llamado fetch.sh porqué así sé de donde he bajado los archivos ...

Comprobamos la firma del archivo:

```
md5 pfSense-1.0.1-512-ad2.img.gz
cat pfSense-1.0.1-512-ad2.img.gz.md5
```

Pasamos la aplicación a una máquina multimedia con Windows XP que tiene un frontal para insertar toda clase de tarjetas de memoria, con el fin de poder grabar la Compact Flash.

Como que tenemos Samba/CIFS en el servidor, copiamos los archivos del servidor desde la máquina Windows, por ejemplo, a una carpeta D:\CompactFlash

Nota: Si se bajan los archivos a través de Windows, para comprobar firmas se puede emplear **fsum**:
http://www.download.com/Fsum/3000-2248_4-10127195.html

Por ejemplo, se puede crear un archivo **comprueba.bat** que haga lo seguiente:

```
fsum -jm *.gz
type pfSense-1.0.1-512-ad2.img.gz.md5
```

Descarga de physdiskwrite

physdiskwrite es una pequeña utilidad que permite escribir imágenes de disco. Se la puede encontrar en:

http://m0n0.ch/wall/physdiskwrite.php

La descargamos en D:\CompactFlash y descomprimimos el archivo ZIP para obtener el EXE.

Grabación de la CompactFlash

Vamos a [Inicio] [Ejecutar ...] y ejecutamos **cmd** (intérprete de órdenes MS-DOS)

```
d:
cd /compactflash
```

Ejecutamos:

```
physdiskwrite.exe pfSense-1.0.1-512-ad2.img.gz
```

Obtendremos una respuesta similar a:

```
Searching for physical drives ...
Information for \\.\PhysicalDrive0:
...
...
Wich disk do you want to write <0..0>?
```

Cancelamos la ejecución mediante Ctl+C

Con ello hemos visto qué discos físicos tiene nuestra máquina.

Insertamos ahora la Compact Flash y volvemos a ejecutar:

```
physdiskwrite.exe pfSense-1.0.1-512-ad2.img.gz
```

Vemos que nos detecta un disco físico más y cambia la pregunta final:

```
Wich disk do you want to write <0..2>?
```

Indicamos pues el número de disco físico para la CompactFlash (en mi caso el 2).

El proceso de grabación empieza y dura un buen rato (media hora aproximadamente).

¡¡¡ Cuando se termina, hay que hacer el proceso de desconexión segura del dispositivo Compact Flash antes de extraerla de su ranura !!!

En muchas consolas de órdenes (Windows XP incluido) escribir los primeros caracteres de los archivos y darle al tabulador sirve para que aparezca en pantalla el nombre completo del archivo. Ello evita teclearlo todo.

En mi caso he creado un archivo de órdenes llamado `grabar.bat` que contiene la orden

```
physdiskwrite.exe pfSense-1.0.1-512-da0.img.gz
```

physdiskwrite controla automáticamente que no se puedan escribir discos de más de 2 GByte. De esta manera evita las confusiones entre el disco duro y la Compact Flash.

Configuración inicial de pfSense

Una vez instalada la Compact Flash en el FX5620 **(con el equipo sin alimentación)** lo ponemos en marcha con un monitor, teclado y cable de red conectados. El cable de red lo pondremos en ETH6 (interfase a 1 Gbit/s y que pfSense reconoce como re0).

Una vez en marcha el sistema, tenemos que indicar como mínimo la LAN y la WAN:

```
Do you want to set up VLANs now [y|n]? n
Enter the LAN interface name or 'a' for auto-detection: re0
Enter the WAN interface name or 'a' for auto-detection: rl0
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing is finished): _
```

Y confirmar la operación:

```
LAN -> re0
WAN -> rl0

Do you want to proceed [y|n]? y
```

El sistema carga su configuración por defecto y presenta al final la indicación de que la LAN es 192.168.1.1 y su menú de consola.

Seleccionaremos la opción `2)Set LAN IP address` de la consola para cambiar de 192.168.1.1 a 192.168.XXX.1

```
Enter the new LAN IP address: 192.168.XXX.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 8
Enter the new LAN subnet bit count: 24
Do you want to enable the DHCP server on LAN [y|n]? n
```

Confirmando la operación se nos informará de la nueva dirección.

A partir de aquí, normalmente emplearemos el configurador web, yendo a http://192.168.XXX.1

El acceso directo a la consola del cortafuegos tiene la pega de estar configurado con el teclado inglés. En caso de querer acceder al cortafuegos vía consola siempre será más cómodo hacerlo por SSH. Este acceso sí que nos reconocerá nuestro teclado (empleando, por ejemplo, el cliente PuTTY). En [Configuración base] explico cómo activar el acceso por SSH.

Configuración base

Acceso a la interfase web

Desde un navegador de páginas web iremos a la dirección IP que hayamos puesto (en la LAN del cortafuegos) durante la instalación:

http://192.168.XXX.1

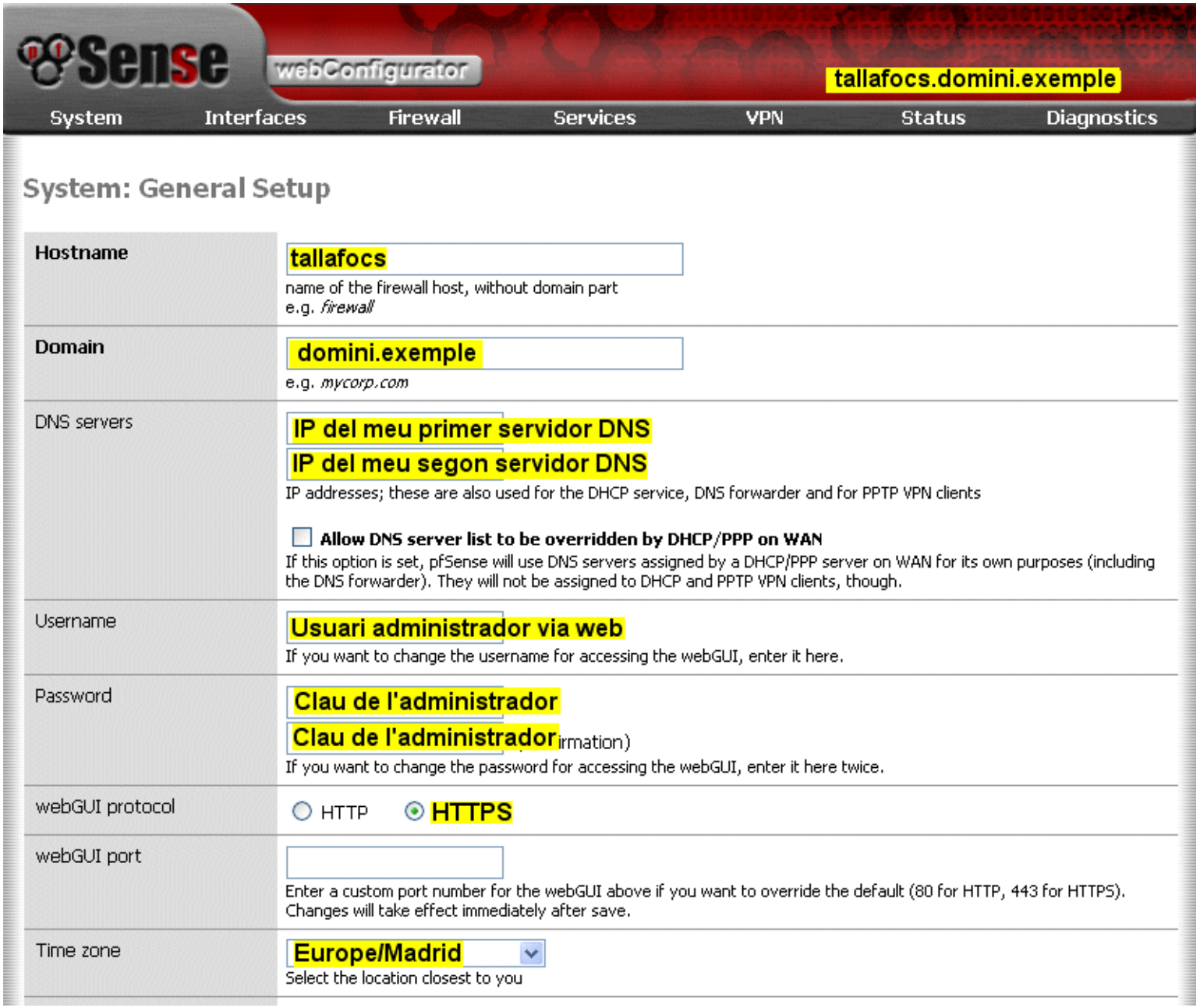
Y nos validaremos con el usuario **admin** y la contraseña **pfsense**.

Cuando se entra por primera vez aparece un asistente, pero se puede saltar haciendo clic sobre el logotipo de pfSense. Prefiero hacerlo así para ir familiarizándome con los menús ...

El configurador web está basado en un servidor web reducido llamado lighttpd. No sé si es un problema de este servidor o de su configuración pero, a veces, te ves obligado a refrescar la página para que se vea se vea bien o a repetir la acción de algún botón (por ejemplo el de descarga de la configuración del cortafuegos en formato XML). Resulta algo incómodo pero no tiene más importancia.

[System] [General Setup]

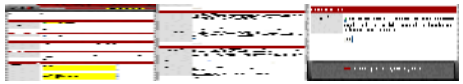
Iremos pues a [System] [General Setup] para ajustar la configuración básica de nuestro cortafuegos:


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
System: General Setup
Hostname
tallafocs
name of the firewall host, without domain part
e.g. firewall
Domain
domini.exemple
e.g. mycorp.com
DNS servers
IP del meu primer servidor DNS
IP del meu segon servidor DNS
IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients
Allow DNS server list to be overridden by DHCP/PPP on WAN
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.
Username
Usuari administrador via web
If you want to change the username for accessing the webGUI, enter it here.
Password
Clau de l'administrador
Clau de l'administrador
irmation)
If you want to change the password for accessing the webGUI, enter it here twice.
webGUI protocol
HTTP
HTTPS
webGUI port
Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).
Changes will take effect immediately after save.
Time zone
Europe/Madrid
Select the location closest to you

[System] [Advanced Functions]

A continuación, si queremos acceso a la consola por SSH y/o hacer servir HTTPS hay que ajustar cosas en [System] [Advanced functions]. El certificado de seguridad y la llave privada para el acceso web no son imprescindibles pero sí recomendables, sobretodo si queremos evitar el típico aviso sobre los certificados de cuando se entra en modo https. En www.eclectica.ca/howto/ssl-cert-howto.php hay un buen tutorial sobre certificados SSL.

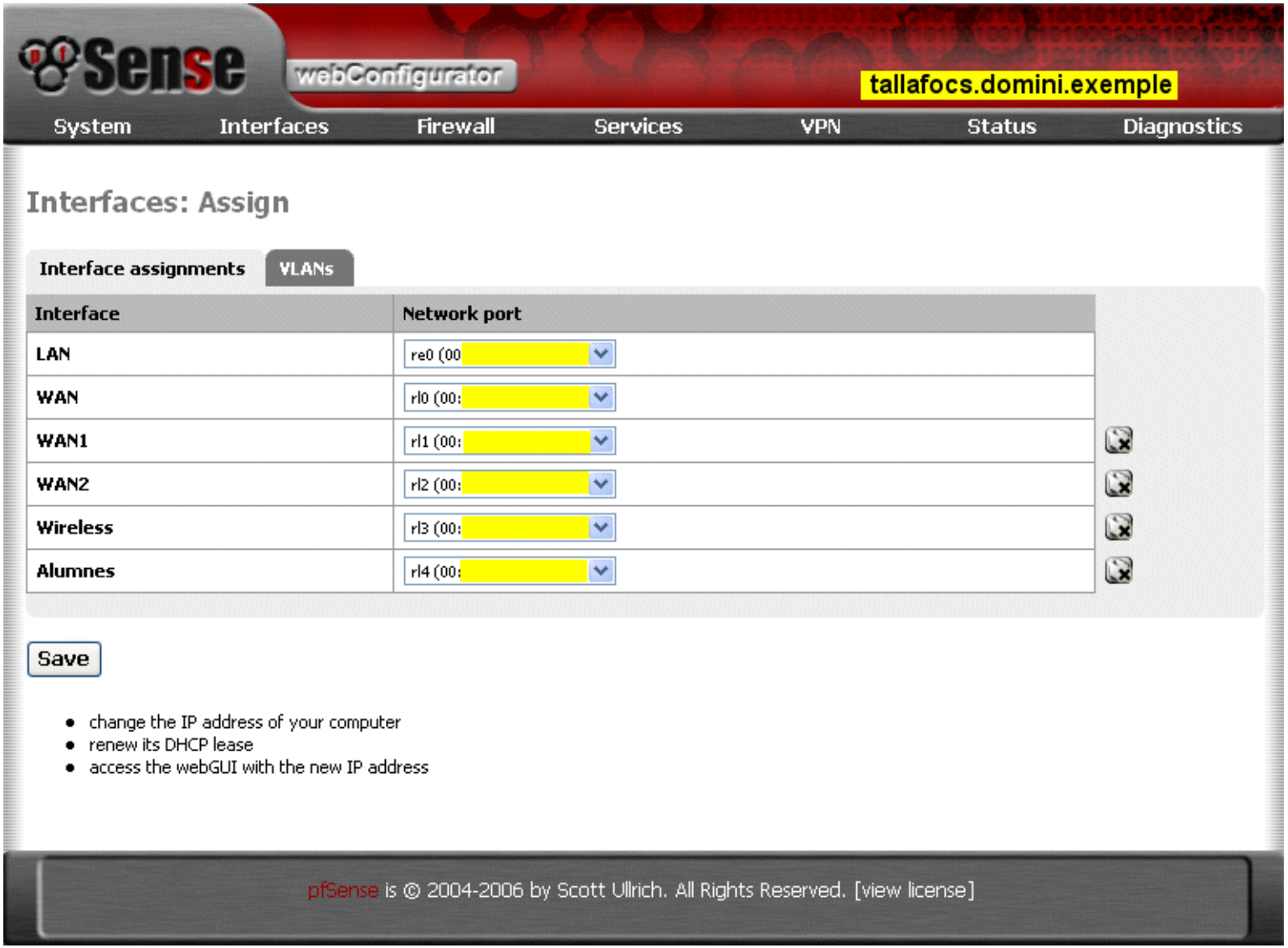
El usuario de acceso a la consola por SSH es siempre **admin**. El cambio del nombre del usuario administrador vía web no afecta el del administrador vía SSH. Por contra, el cambio de contraseña sí que afecta los dos modos de administración (SSH y web).



[Interfaces] [Assign]

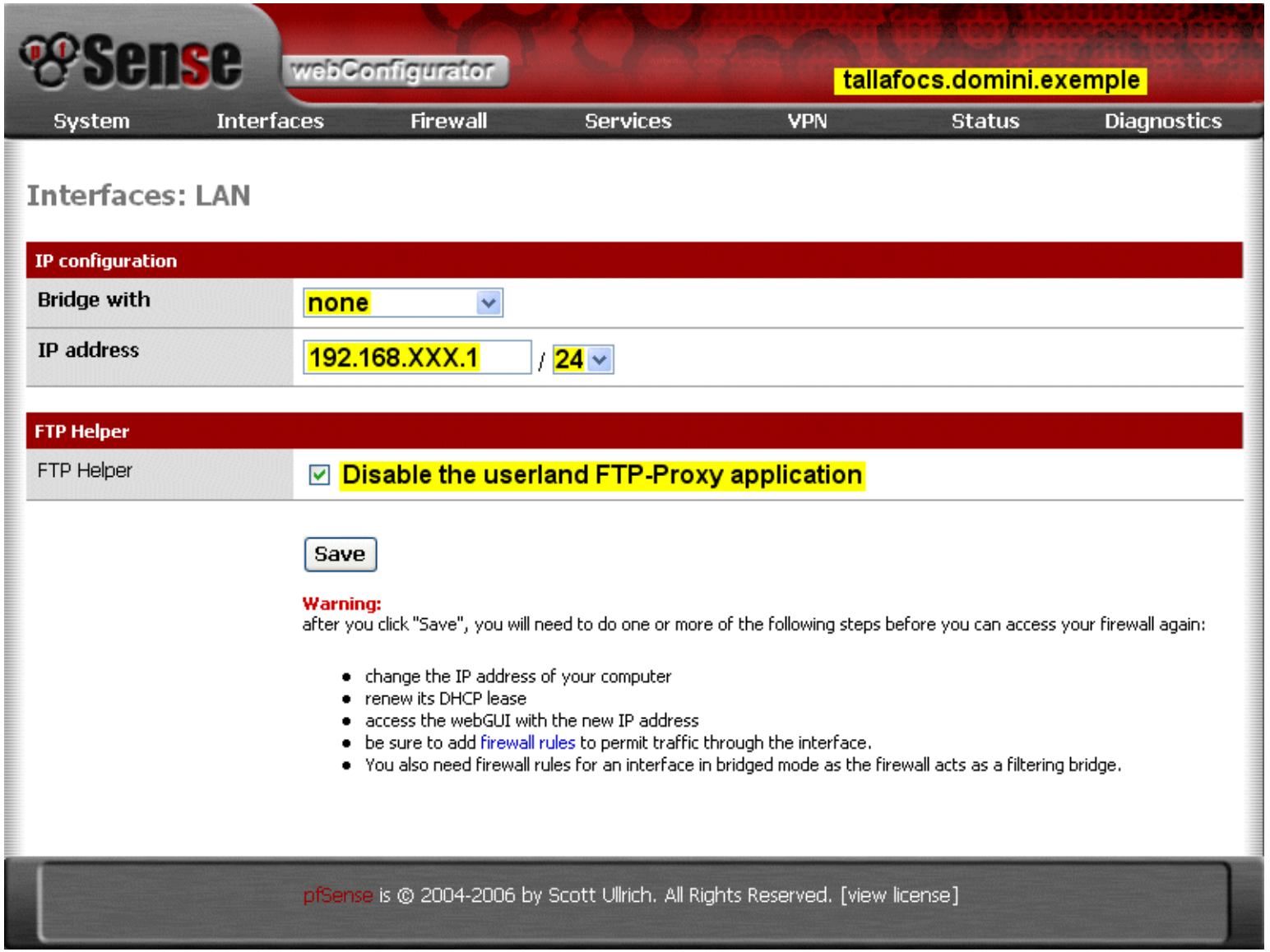
Habrá que ir también a [Interfaces] [Assign] con el fin de asignar el resto de interfases (recordemos que LAN y WAN ya se asignaron durante la instalación y configuración inicial). En un primer momento, el sistema va denominando las interfases que asignamos como Optional 1, Optional 2, Optional 3, Optional 4, ...

En los apartados que hay más adelante de configuración de cada una de las interfases podremos darles un nombre a nuestro gusto (WAN1, WAN2, Wireless i Alumnes). La pantalla que se muestra a continuación es ya la final de asignación de interfases:



[Interfaces] [LAN]

Terminamos por ajustar la configuración de la LAN asegurándonos que tenemos FTP-Proxy Helper desactivado:


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Interfaces: LAN
IP configuration
Bridge with
none
IP address
192.168.XXX.1
/ 24
FTP Helper
FTP Helper
Disable the userland FTP-Proxy application
Save
Warning:
after you click "Save", you will need to do one or more of the following steps before you can access your firewall again:
change the IP address of your computer
renew its DHCP lease
access the webGUI with the new IP address
be sure to add firewall rules to permit traffic through the interface.
You also need firewall rules for an interface in bridged mode as the firewall acts as a filtering bridge.
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]

[Interfaces] [WAN]

Asignaremos a la WAN (puerta de enlace por defecto de nuestro cortafuegos) una IP estática (192.168.AAA.2), indicaremos cuál es su puerta de salida (192.168.AAA.1, IP privada del router ADSL) y le desactivaremos FTP-Proxy Helper. Observemos que empleamos como máscara de esta red 29 bit (255.255.255.248), ya que tenemos un proxy en 192.168.AAA.3.

Interfaces: WAN

General configuration

Type	**Static**
MAC address	Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP configuration

IP address	**192.168.AAA.2** / **29**
Gateway	**192.168.AAA.1**

DHCP client configuration

Hostname	The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

Username	
Password	
Service name	Hint: this field can usually be left empty

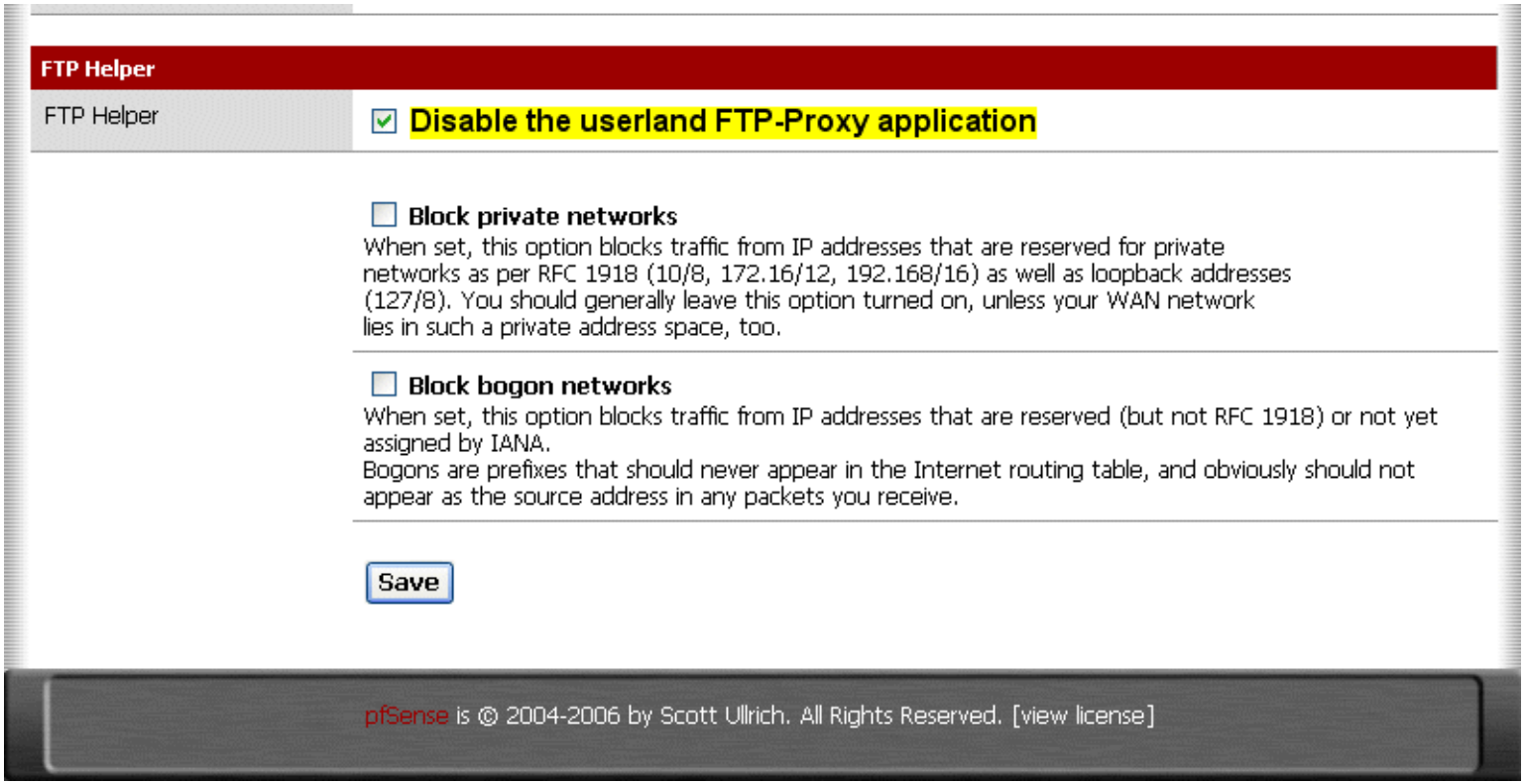
Dial on demand	☐ **Enable Dial-On-Demand mode** This option causes the interface to operate in dial-on-demand mode, allowing you to have a *virtual full time* connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
Idle timeout	seconds If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

PPTP configuration

Username	
Password	
Local IP address	/ 31
Remote IP address	
Dial on demand	☐ **Enable Dial-On-Demand mode** This option causes the interface to operate in dial-on-demand mode, allowing you to have a *virtual full time* connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
Idle timeout	seconds If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

BigPond Cable configuration

Username	
Password	
Authentication server	If this field is left empty, the default ("dce-server") is used.
Authentication domain	If this field is left empty, the domain name assigned via DHCP will be used. Note: the BigPond client implicitly sets the "Allow DNS server list to be overridden by DHCP/PPP on WAN" on the System: General setup page.
Min. heartbeat interval	seconds



[Interfaces] [WAN1]

Activamos la interfase opcional 1, le ponemos por nombre WAN1, le asignamos una IP estática (192.168.BBB.2), indicamos cuál es su puerta de salida (192.168.BBB.1, IP privada del router ADSL) y le desactivamos FTP-Proxy Helper. Observemos que empleamos como máscara de esta red 30 bit (255.255.255.252), de tal forma que entre esta interfase y el router ADSL es imposible poner nada más.

Interfaces: Optional 1 (WAN1)

Optional Interface Configuration

☑ Enable Optional 1 Interface

Description	WAN1 Enter a description (name) for the interface here.

General configuration

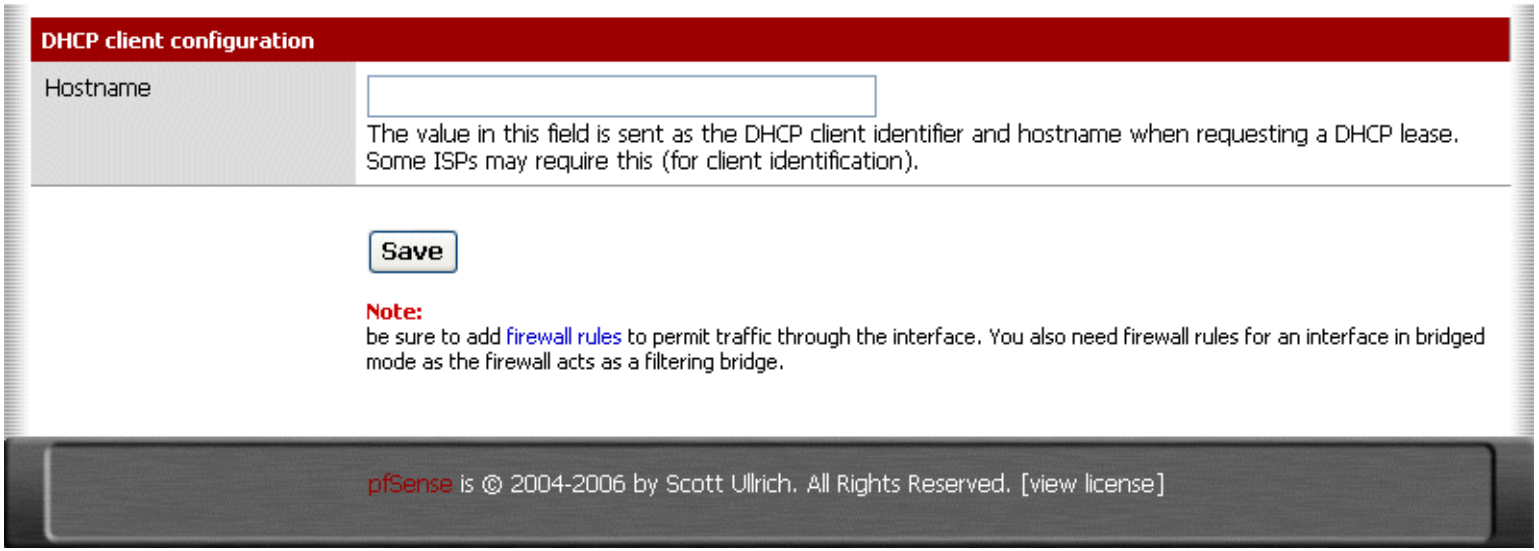
Type	Static
MAC address	Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

IP configuration

Bridge with	none
IP address	192.168.BBB.2 / 30
Gateway	192.168.BBB.1 If you have multiple WAN connections, enter the next hop gateway (router) IP address here. Otherwise, leave this option blank.

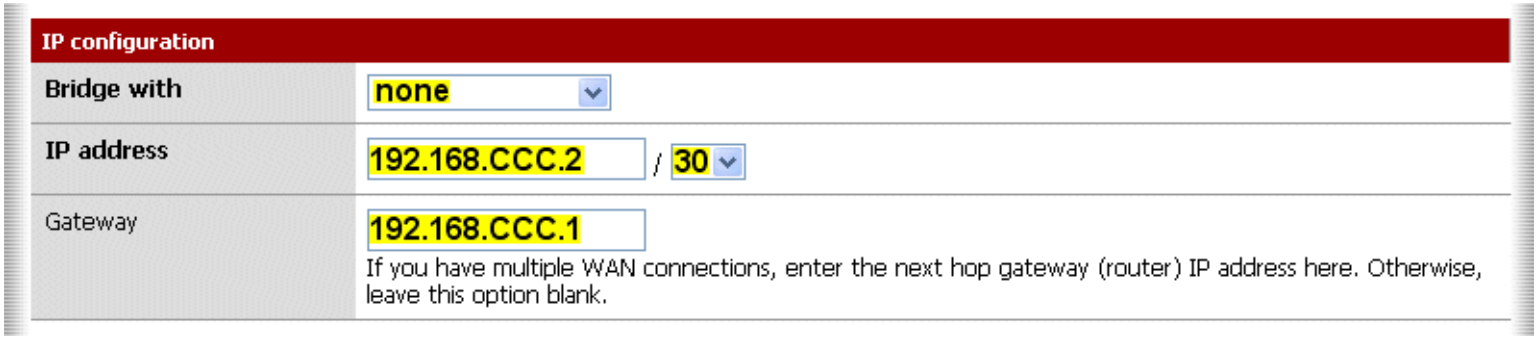
FTP Helper

FTP Helper	☑ Disable the userland FTP-Proxy application



[Interfaces] [WAN2]

Seguimos los mismos pasos (que para WAN1) para la interfase opcional 2, a la que llamaremos WAN2, le asignamos una IP estática (192.168.CCC.2), indicamos cuál es su puerta de salida (192.168.CCC.1, IP privada del router ADSL) y le desactivamos FTP-Proxy Helper.



[Interfaces] [Alumnes]

La interfase opcional 4 es la de la LAN de Alumnes. Le pondremos la dirección estática 192.168.YYY.1, con máscara de 24 bit (255.255.255.0). No le tenemos que poner una puerta de enlace, ya que son las reglas del cortafuegos las que definen a través de que WAN (WAN, WAN1 o WAN2) va el tráfico. Además, aquí dejaremos activado FTP-Proxy Helper.

Interfaces: Optional 4 (Alumnes)

Optional Interface Configuration

☑ Enable Optional 4 interface

Description	Alumnes Enter a description (name) for the interface here.

General configuration

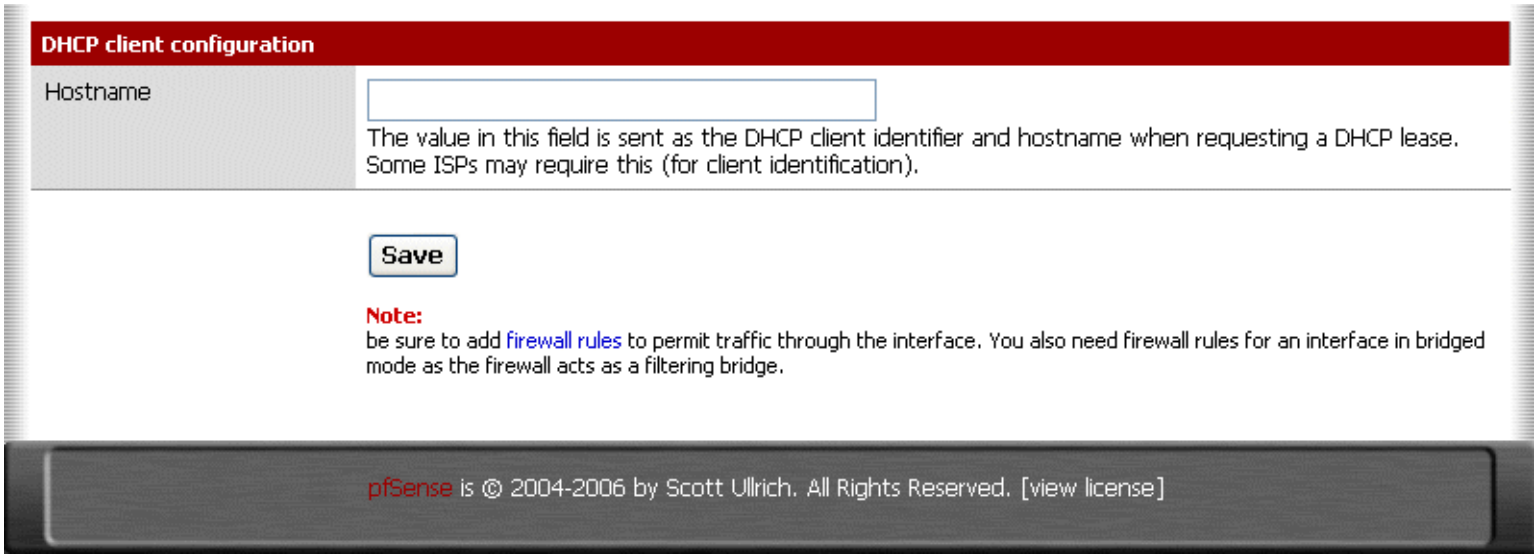
Type	Static
MAC address	Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

IP configuration

Bridge with	none
IP address	192.168.YYY.1 / 24
Gateway	If you have multiple WAN connections, enter the next hop gateway (router) IP address here. Otherwise, leave this option blank.

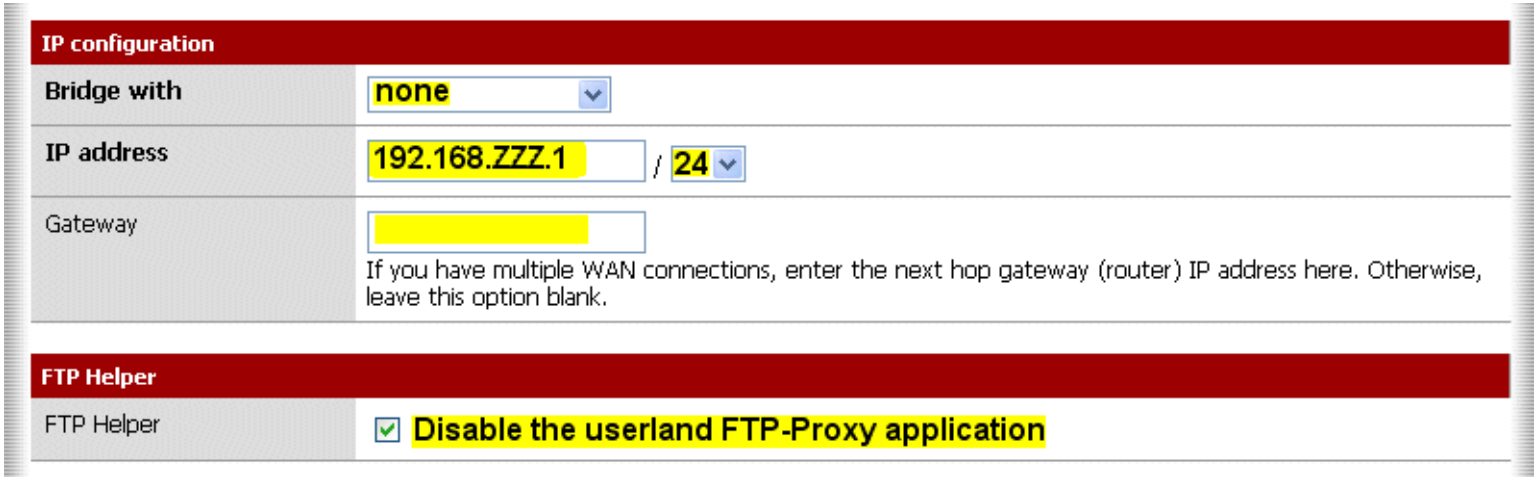
FTP Helper

FTP Helper	☐ Disable the userland FTP-Proxy application



[Interfaces] [Wireless]

Finalmente, la interfase opcional 3 la destinaremos a la red sin hilos (wireless), con FTP-Proxy Helper desactivado:



Guardar la configuración

Se aconseja ir a menudo a [Diagnostics][Backup/Restore][Remote] y guardar (download) la configuración. Genera un archivo XML a guardar. Además, el nombre de este archivo queda serializado con la fecha/hora, por lo que en caso de problemas puede ser muy útil recuperar la última configuración buena conocida.

Piensa que el archivo XML puede contener información delicada (llaves privadas SSL, contraseñas, estructura de nuestra red, ...) y conviene guardarlo en lugar seguro.

También hay que tener en cuenta que haciendo pruebas nos podemos encontrar con algunas configuraciones de comportamiento errático por lo que, ante la duda, más vale recuperar la configuración que sabemos que funcionaba correctamente.

Alias

[Firewall] [Aliases]

Puede ser un alias un puerto, un grupo de puertos, una dirección IP o un grupo de direcciones IP, toda una red o un grupo de redes.

Los alias no sólo ahorran escritura al configurar las reglas del cortafuegos. También permiten realizar cambios de forma mucho más fácil, al actuar como parámetros.

Un alias definido puede emplearse o no. Si un alias es empleado en alguna de las reglas del cortafuegos, pfSense no permite eliminarlo. A continuación se dan una serie de alias como ejemplo:

Firewall: Aliases

Name	Values	Description
WANnet	192.168.AAA.0/29	El configurador no té l'opció "WAN net"
XTEC	213.176.0.0/19, 82.151.192.0/19	Xarxa Telemàtica Educativa de Catalunya -NO UTILITZAT-
cb50	192.168.XXX.	
cisco510	192.168.AAA.3	Servidor Proxy Cisco510
correu	25, 995, 80, 443	TCP 25, 995, 80 i 443
estandard	80, 443, 22	TCP 80, 443 i 22
mail	192.168.XXX.	
microsoft	207.46.0.0/16, 64.4.0.0/18	Microsoft Corporation
panda	212.170.242.175, 212.170.238.83, 212.170.238.113	updates.pandasoftware.com, www.pandasoftware.es, www.pandasoftware.com -NO UTILITZAT-
s18	192.168.XXX.	
s204	192.168.XXX.	
s206	192.168.XXX.	
s207	192.168.XXX.	
samba	137, 138, 139, 445	UDP 137-138, TCP 139 i 445
servidors	192.168. , 192.168. , 192.168. , 192.168. , 192.168. , 192.168. , 192.168.	Ordinadors considerats servidors
www	192.168.XXX.	

Note:
Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

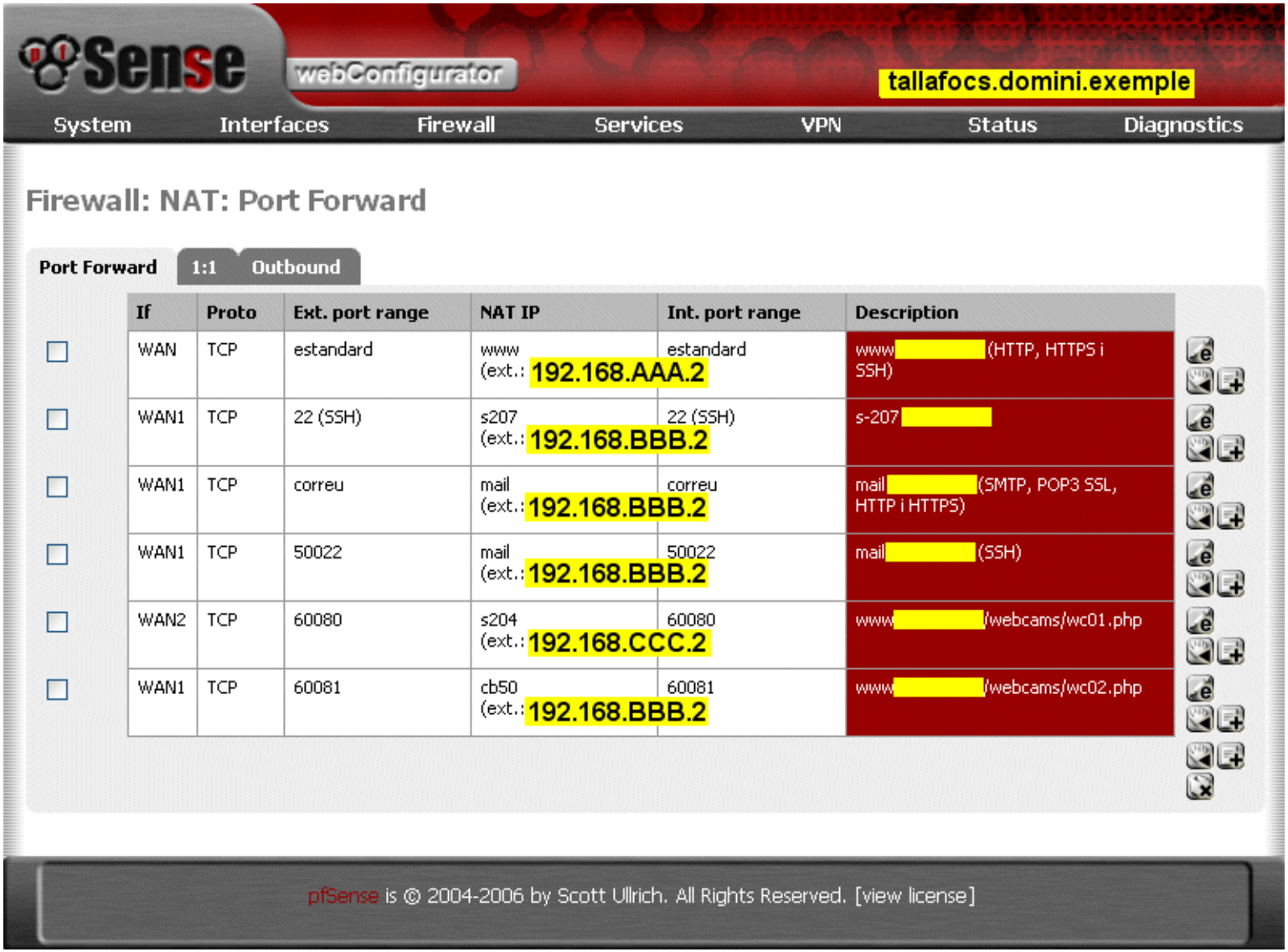
NAT (Network Address Translation)

Configuraremos NAT para las conexiones entrantes a nuestros servicios públicos y para les conexiones salientes ...

[Firewall] [NAT] [Port Forward]
[Firewall] [NAT] [Outbound]

[Firewall] [NAT] [Port Forward]

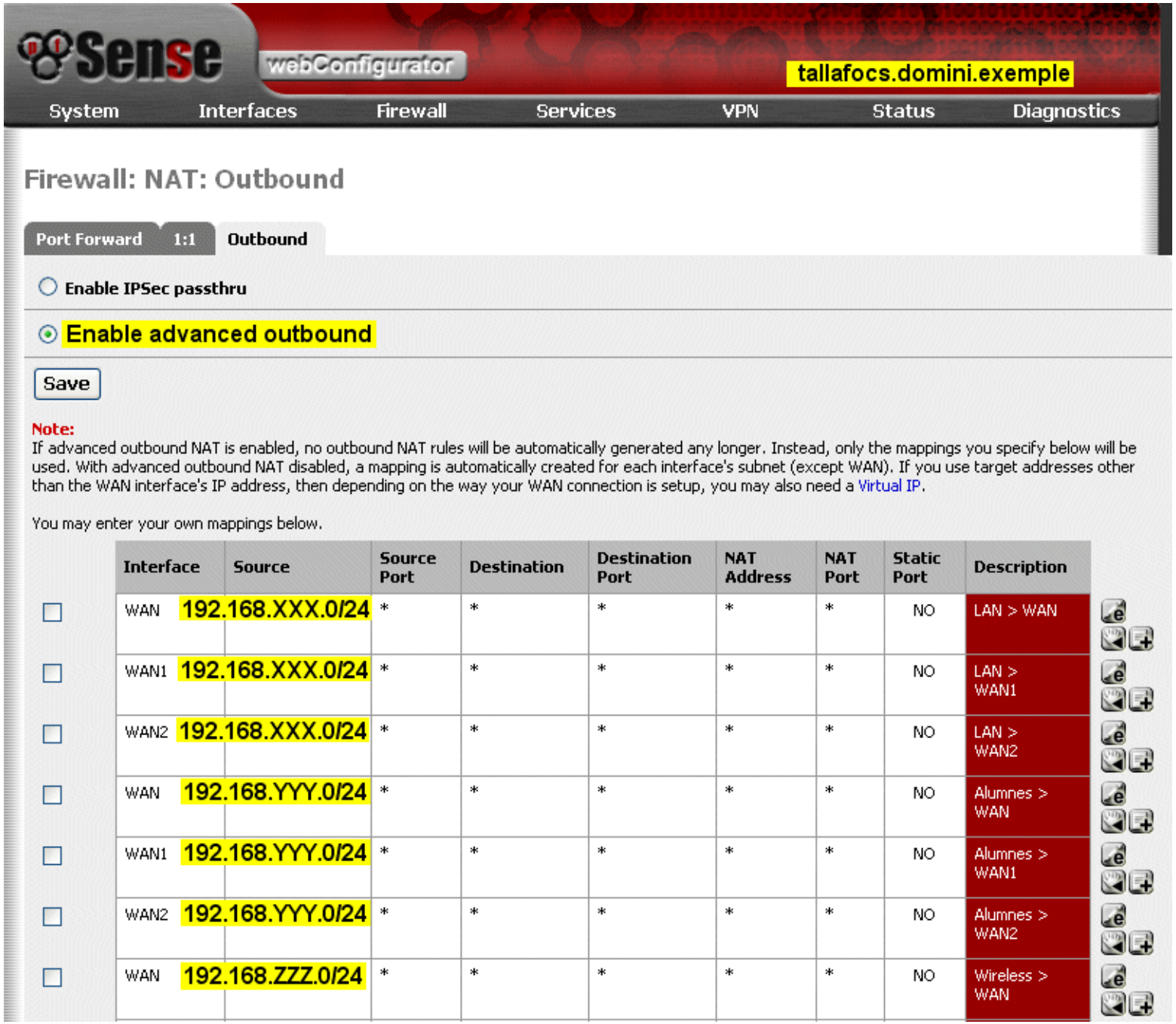
Aquí configuraremos el acceso a nuestros servidores desde el exterior (puertos y puerta de enlace). Es lo que popularmente se llama como "abrir puertos" ...

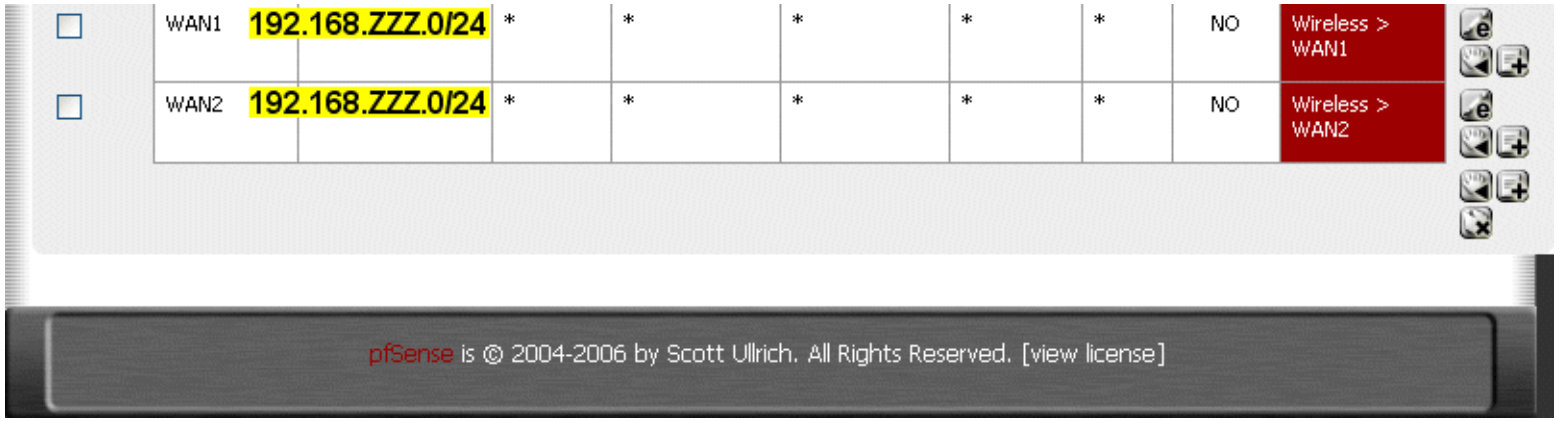

pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: NAT: Port Forward
Port Forward
1:1
Outbound
If
Proto
Ext. port range
NAT IP
Int. port range
Description
WAN
TCP
estandard
www
(ext.: 192.168.AAA.2
estandard
www (HTTP, HTTPS i SSH)
WAN1
TCP
22 (SSH)
s207
(ext.: 192.168.BBB.2
22 (SSH)
s-207
WAN1
TCP
correu
mail
(ext.: 192.168.BBB.2
correu
mail (SMTP, POP3 SSL, HTTP i HTTPS)
WAN1
TCP
50022
mail
(ext.: 192.168.BBB.2
50022
mail (SSH)
WAN2
TCP
60080
s204
(ext.: 192.168.CCC.2
60080
www /webcams/wc01.php
WAN1
TCP
60081
cb50
(ext.: 192.168.BBB.2
60081
www /webcams/wc02.php
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]

[Firewall] [NAT] [Outbound]

Aquí activaremos el NAT de salida avanzado (advanced outbound) para que pfSense no nos genere automáticamente reglas de NAT saliente. De esta forma tomamos un control total sobre el NAT saliente.

Definiremos todas las combinaciones posibles entre nuestras LAN (LAN, Alumnes i Wireless) y nuestras WAN (WAN, WAN1 i WAN2), tal como muestra la figura:


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: NAT: Outbound
Port Forward
1:1
Outbound
Enable IPSec passthru
Enable advanced outbound
Save
Note:
If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated any longer. Instead, only the mappings you specify below will be used. With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN). If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need a Virtual IP.
You may enter your own mappings below.
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description
WAN 192.168.XXX.0/24 * * * * * NO LAN > WAN
WAN1 192.168.XXX.0/24 * * * * * NO LAN > WAN1
WAN2 192.168.XXX.0/24 * * * * * NO LAN > WAN2
WAN 192.168.YYY.0/24 * * * * * NO Alumnes > WAN
WAN1 192.168.YYY.0/24 * * * * * NO Alumnes > WAN1
WAN2 192.168.YYY.0/24 * * * * * NO Alumnes > WAN2
WAN 192.168.ZZZ.0/24 * * * * * NO Wireless > WAN



Algunas de estas combinaciones no las emplearemos, debido a que las reglas de cortafuegos no permitirán el tráfico que aquí está previsto. Ponemos, pero, todas las combinaciones posibles para no tener problemas de NAT en el caso eventual de autorizar tráfico inicialmente no previsto.

Reglas del cortafuegos

Estamos ahora en el corazón del cortafuegos. Aquí se decide qué conexiones se permiten y cuáles no.

Tenemos que entender el cortafuegos como una caja con una serie de puertas de entrada. Se trata de dejar o no dejar entrar (paquetes de información) por cada una de las puertas que tenemos. Este concepto es muy importante, ya que si un paquete de información puede entrar por una puerta querrá decir que saldrá (en principio) por cualquier otra. Por tanto, en lo que se refiere a las salidas sólo nos ocuparemos de seleccionar cuál queremos. Nada más que esto.

Cada puerta tiene pues sus reglas, que se ejecutan según el orden en que están puestas. De la primera hacia la última de la lista. Digo "hacia la última" porque cuando un paquete de información cumple una de las reglas se hace la acción que dice la regla y ya no se miran las siguientes.

¿Y qué pasa si se llega a la última regla y ninguna de ellas se ajusta a nuestro paquete de información? Pues que el paquete no pasa. Si no hay regla, el paquete es bloqueado.

¿Y qué acciones puede hacer una regla? Pues tres: dejar pasar (pass), bloquear (block) y rechazar (reject). La diferencia entre bloquear y rechazar es importante. Si se bloquea, simplemente se ignora el paquete de información que se está recibiendo. Si se rechaza, se comunica al emisor que no se quiere el paquete. Por tanto, normalmente se bloquea. ¿Por qué? Pues porqué bloquear es silencioso, es

no hacer caso al emisor y nada más.

También podemos desactivar reglas. Las reglas desactivadas se ven "difuminadas" en la lista de reglas. Ello resulta especialmente interesante cuando se precisa de reglas ocasionales. Por ejemplo, para tareas de administración de la red.

Todos los ordenadores cliente emplean como configuración automática de proxy el archivo **www.dominio.ejemplo/proxy.pac** capaz de detectar si el proxy está disponible o no. En caso de no estar disponible, la navegación se hace de forma directa. El contenido del archivo proxy.pac es:

```
function FindProxyForURL(url, host) {

    // No emplear proxy desde 192.168.XXX/24
    // Hace obsoletas las regles 3 y 4 de la LAN
    isInNet(myIpAddress(), "192.168.XXX.0", "255.255.255.0") {return "DIRECT";}

    // No emplear proxy para nuestros dominios
    if (shExpMatch(url,"*.dominio.ejemplo/*"))              {return "DIRECT";}
    if (shExpMatch(url,"*.dominio.ejemplo:*"))              {return "DIRECT";}
    if (shExpMatch(url,"*.dominio.ejemplo2/*"))             {return "DIRECT";}
    if (shExpMatch(url,"*.dominio.ejemplo2:*"))             {return "DIRECT";}
    if (shExpMatch(url,"*/localhost/*"))                    {return "DIRECT";}
    if (shExpMatch(url,"*/localhost:*"))                    {return "DIRECT";}

  // No emplear proxy para microsoft
    if (isInNet(host, "207.46.0.0", "255.255.0.0"))         {return "DIRECT";}
    if (isInNet(host, "64.4.0.0", "255.255.192.0"))         {return "DIRECT";}

    // Emplear proxy en el resto de casos
    // Si el proxy falla o no se encuentra, va directo
    return "PROXY proxy.dominio.ejemplo:8080; DIRECT";

  }
```

Si se desea, se pueden configurar reglas destinadas a bloquear el acceso al proxy, con el fin de forzar las conexiones de determinados clientes de forma directa. Por tanto, no hay que perder de vista que **proxy.pac** y las reglas del cortafuegos actúan conjuntamente.

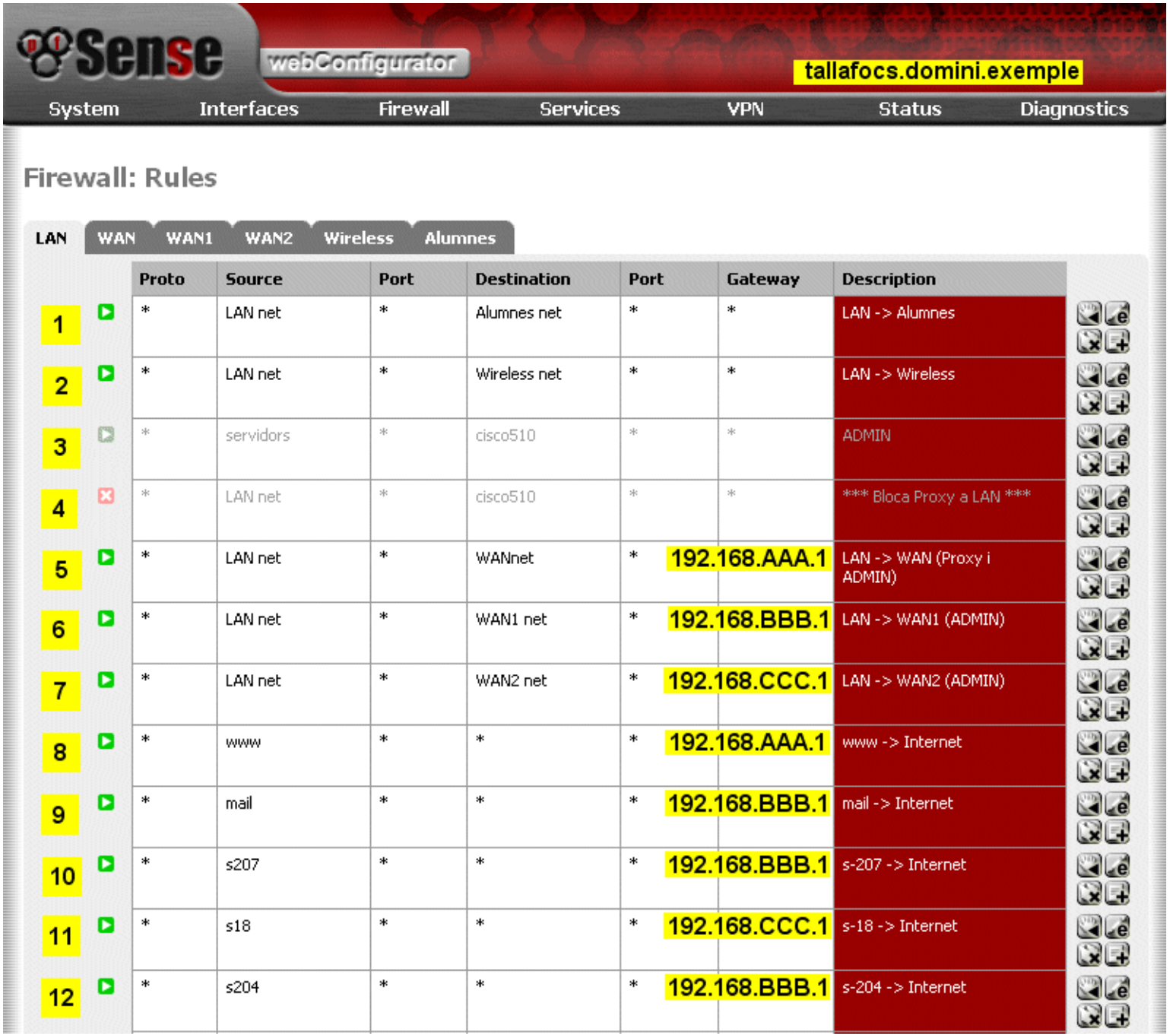
¡Vamos allá, pues! A las reglas de cada una de las seis interfases ...

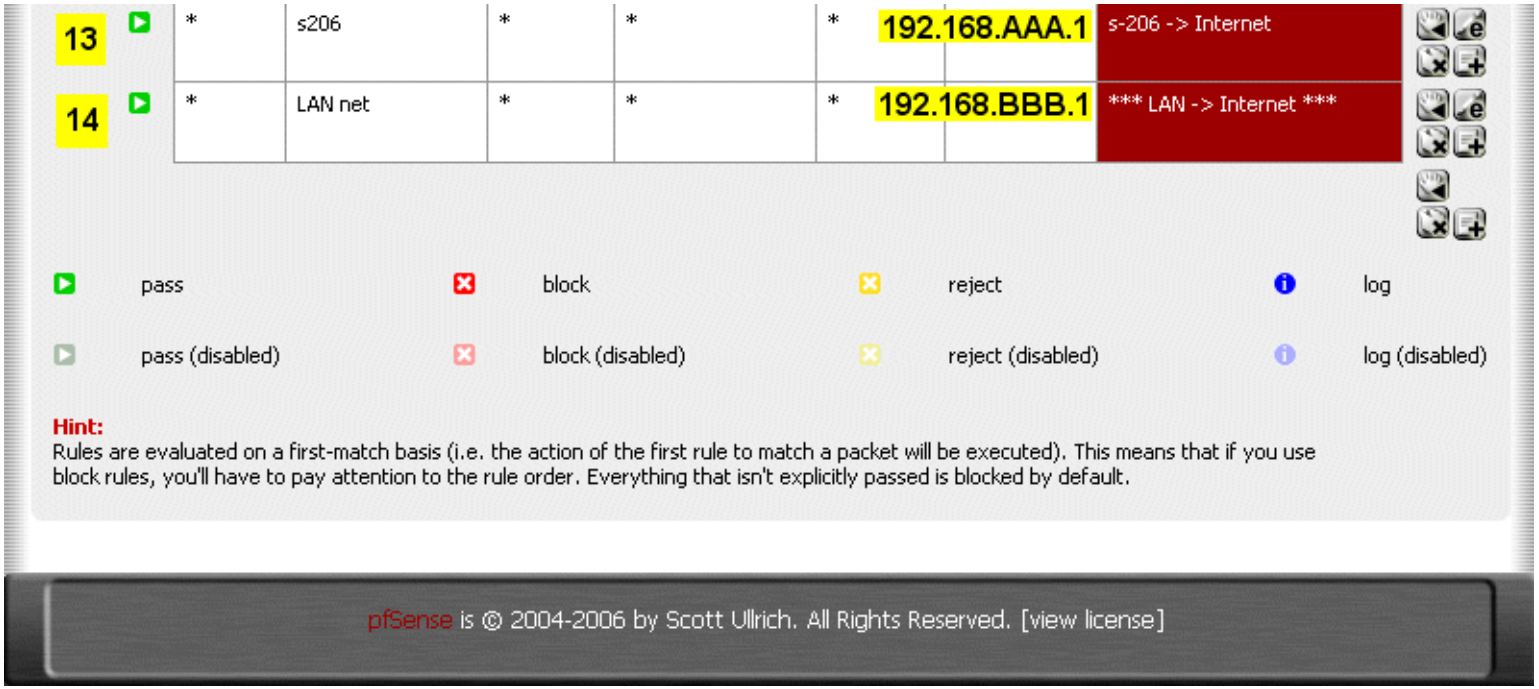
[Firewall] [Rules] [LAN]
[Firewall] [Rules] [WAN]
[Firewall] [Rules] [WAN1]
[Firewall] [Rules] [WAN2]
[Firewall] [Rules] [Alumnes]
[Firewall] [Rules] [Wireless]

[Firewall] [Rules] [LAN]

Explicación de las reglas:

1. Se permite cualquier acceso desde la red LAN a la red Alumnes.
2. Se permite cualquier acceso desde la red LAN a la red Wireless.
3. Se permite cualquier acceso desde los servidores (en la red LAN) al servidor proxy, situado en la red WAN (tareas de administración). Regla desactivada (obsoleta) porqué en proxy.pac ya se dice que la LAN va directa.
4. Se bloquea para el resto de ordenadores de la red LAN el acceso al servidor proxy (situado en la red WAN). De esta forma se fuerza la navegación directa, sin proxy (gracias a proxy.pac). Regla desactivada (obsoleta) porqué en proxy.pac ya se dice que la LAN va directa.
5. Cualquier ordenador de la red LAN puede ir a la red WAN, siendo la puerta de enlace la IP privada del router ADSL (192.168.AAA.1). En la práctica esto permite llegar al router ADSL (por ejemplo, para hacerle ping).
6. Lo mismo que 5, pero para WAN1. Permite administrar el router ADSL (192.168.BBB.1).
7. Lo mismo que 5 y 6, pero para WAN2. Permite administrar el router ADSL (192.168.CCC.1).
8. www de la red LAN accede a Internet empleando el router 192.168.AAA.1.
9. mail de la red LAN accede a Internet empleando el router 192.168.BBB.1.
10. s207 de la red LAN accede a Internet empleando el router 192.168.BBB.1.
11. s18 de la red LAN accede a Internet empleando el router 192.168.CCC.1.
12. s204 de la red LAN accede a Internet empleando el router 192.168.BBB.1.
13. s206 de la red LAN accede a Internet empleando el router 192.168.AAA.1.
14. El resto de tráfico de la red LAN saldrá hacia Internet empleando el router 192.168.AAA.1.

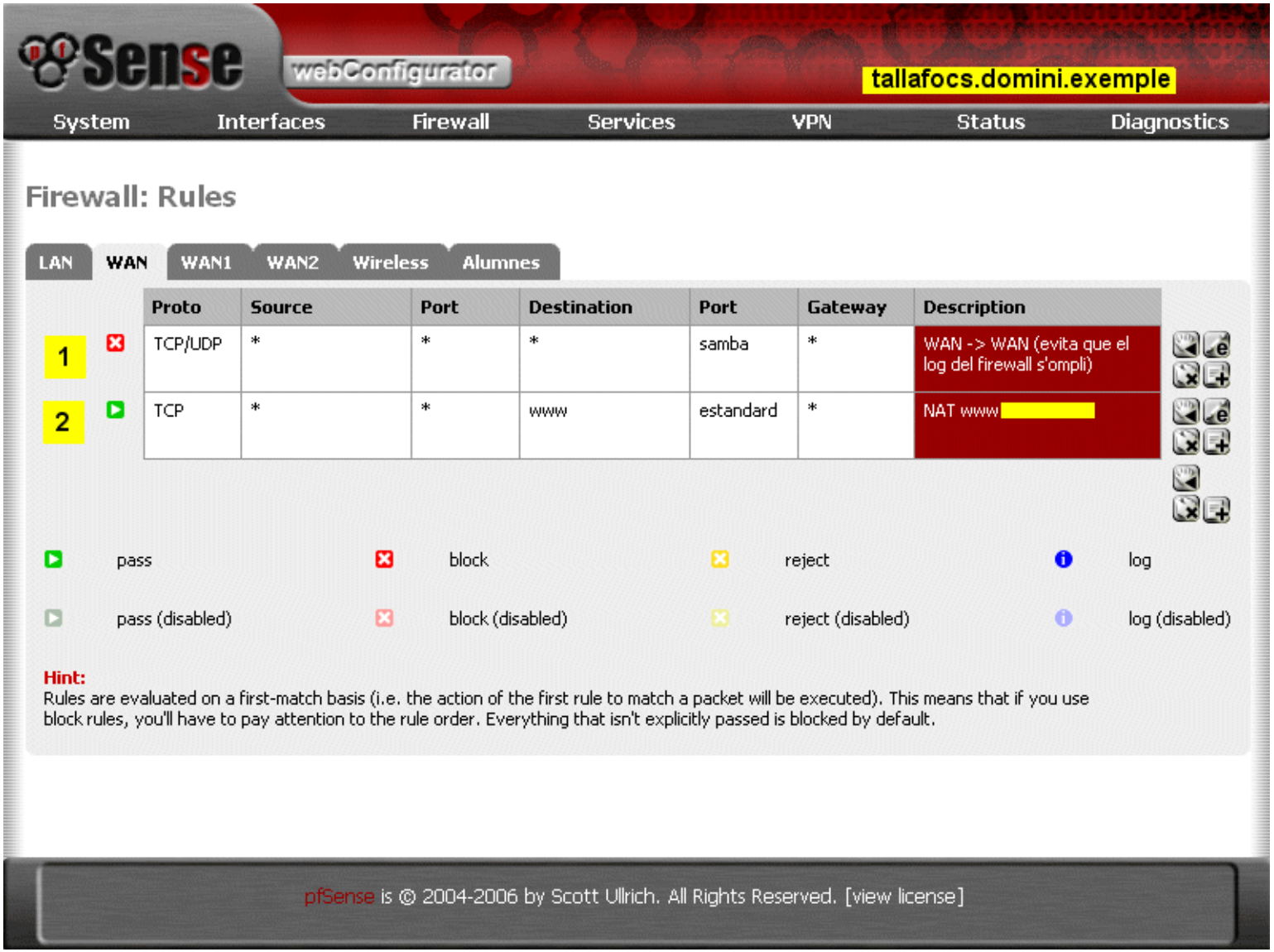

pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
LAN
WAN
WAN1
WAN2
Wireless
Alumnes
Proto
Source
Port
Destination
Port
Gateway
Description
1 * LAN net * Alumnes net * * LAN -> Alumnes
2 * LAN net * Wireless net * * LAN -> Wireless
3 * servidors * cisco510 * * ADMIN
4 * LAN net * cisco510 * * *** Bloca Proxy a LAN ***
5 * LAN net * WANnet * 192.168.AAA.1 LAN -> WAN (Proxy i ADMIN)
6 * LAN net * WAN1 net * 192.168.BBB.1 LAN -> WAN1 (ADMIN)
7 * LAN net * WAN2 net * 192.168.CCC.1 LAN -> WAN2 (ADMIN)
8 * www * * * 192.168.AAA.1 www -> Internet
9 * mail * * * 192.168.BBB.1 mail -> Internet
10 * s207 * * * 192.168.BBB.1 s-207 -> Internet
11 * s18 * * * 192.168.CCC.1 s-18 -> Internet
12 * s204 * * * 192.168.BBB.1 s-204 -> Internet



[Firewall] [Rules] [WAN]

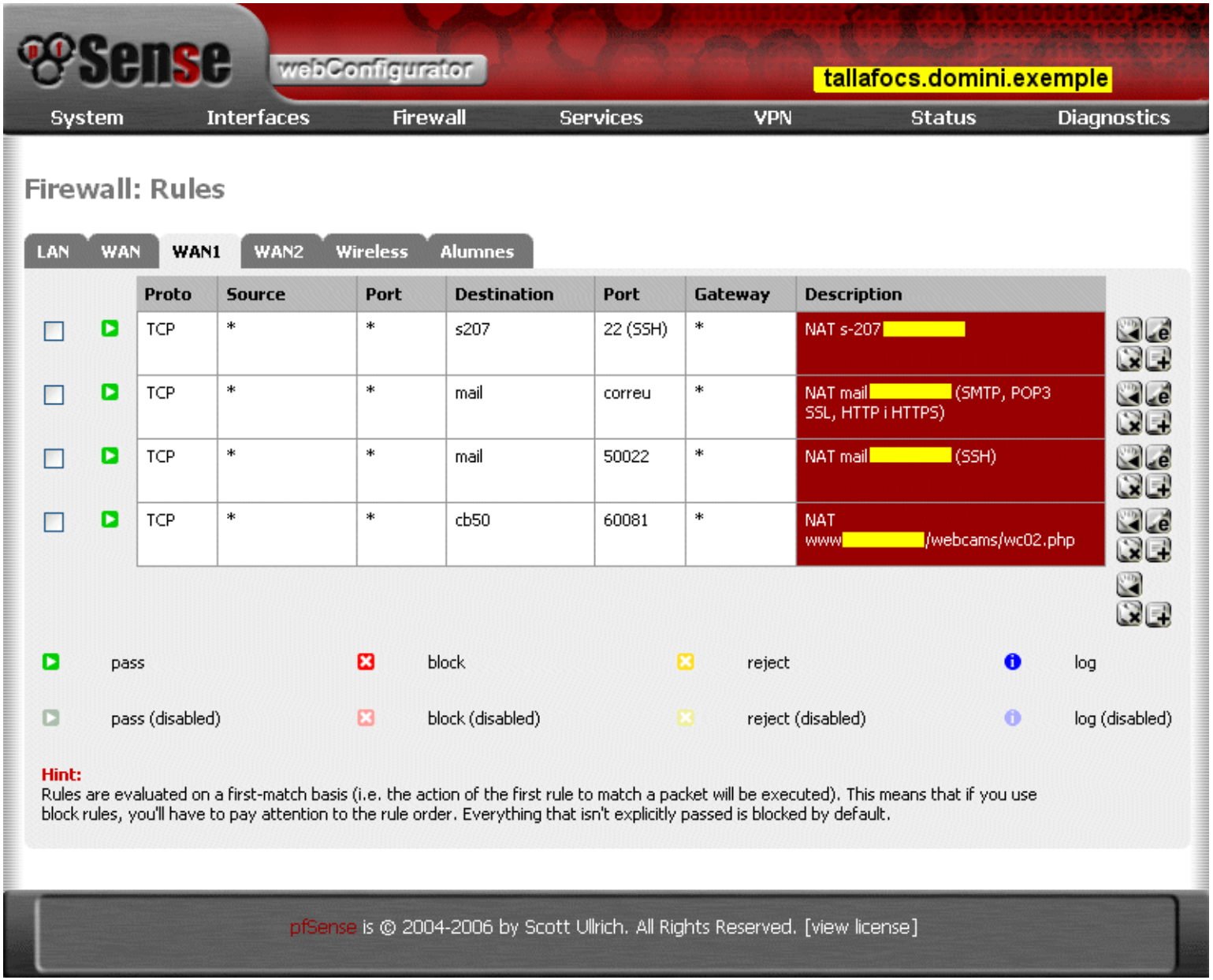
Explicación de las reglas:

1. La existencia de servidores Samba/CIFS (y, lo que es lo mismo, de servicios de archivos de Windows) en la red LAN origina paquetes del examinador de equipos que llegan a la puerta de enlace por defecto del cortafuegos. pfSense los bloquea automáticamente como medida de seguridad. Estos bloqueos quedan reflejados en el log del cortafuegos. Esta regla sólo tiene la finalidad de sustituir el comportamiento estándar de pfSense y evitar así los logs.
2. Se permite el acceso (desde la red WAN) a www de la LAN en protocolo TCP y para los puertos estandard (HTTP, HTTPS y SSH). Esta regla se complementa con el NAT Port Forward definido para www.


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
LAN
WAN
WAN1
WAN2
Wireless
Alumnes
Proto
Source
Port
Destination
Port
Gateway
Description
1
TCP/UDP
*
*
*
samba
*
WAN -> WAN (evita que el log del firewall s'ompli)
2
TCP
*
*
www
estandard
*
NAT www
pass
block
reject
log
pass (disabled)
block (disabled)
reject (disabled)
log (disabled)
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]

[Firewall] [Rules] [WAN1]

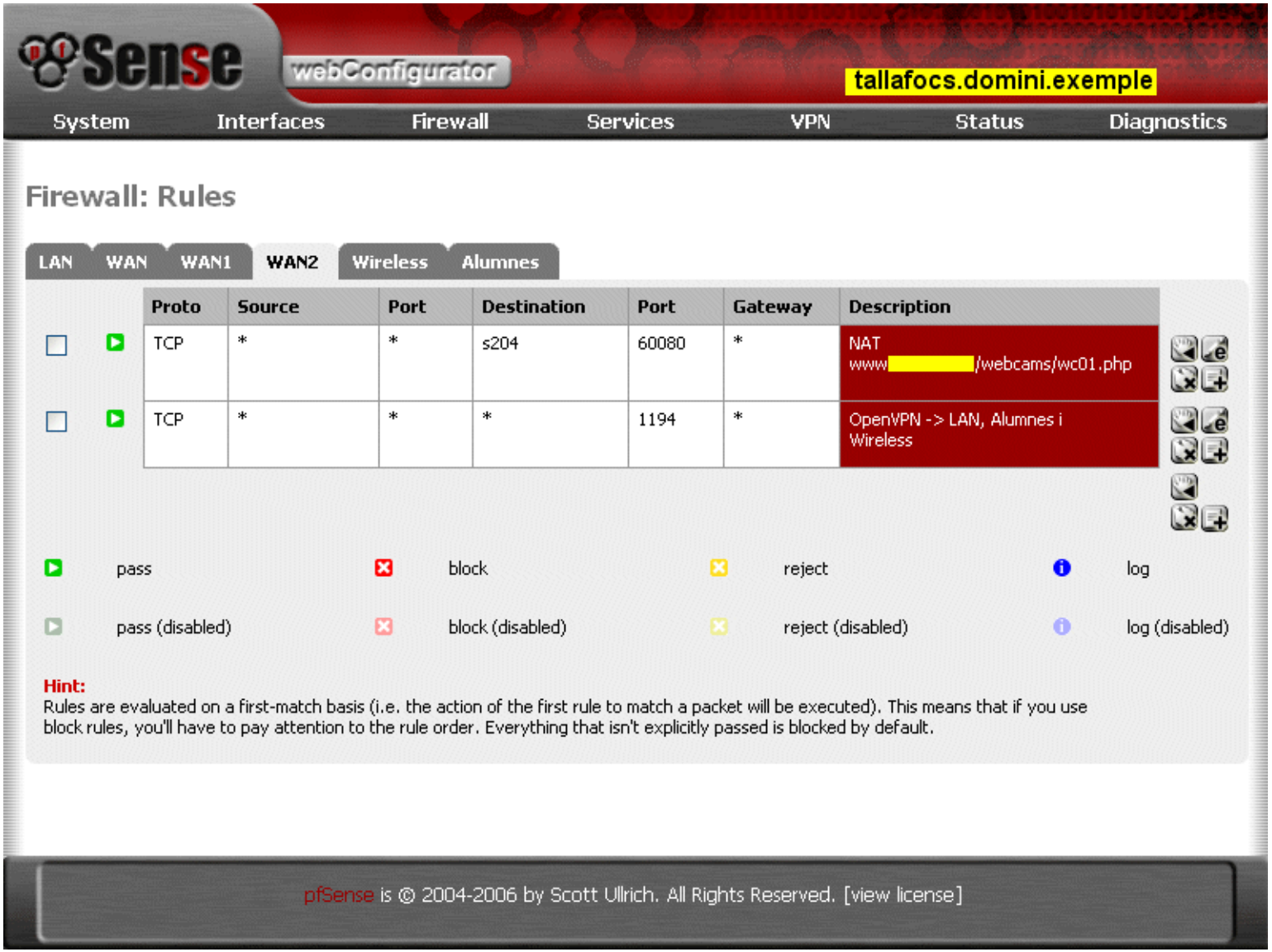
Las reglas corresponden a la autorización del tráfico (desde la red WAN1) para los NAT Port Forward anteriormente definidos ...


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
LAN
WAN
WAN1
WAN2
Wireless
Alumnes
Proto
Source
Port
Destination
Port
Gateway
Description
TCP * * s207 22 (SSH) * NAT s-207 [redacted]
TCP * * mail correu * NAT mail [redacted] (SMTP, POP3 SSL, HTTP i HTTPS)
TCP * * mail 50022 * NAT mail [redacted] (SSH)
TCP * * cb50 60081 * NAT www[redacted]/webcams/wc02.php
pass
block
reject
log
pass (disabled)
block (disabled)
reject (disabled)
log (disabled)
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]

[Firewall] [Rules] [WAN2]

Las reglas corresponden a:

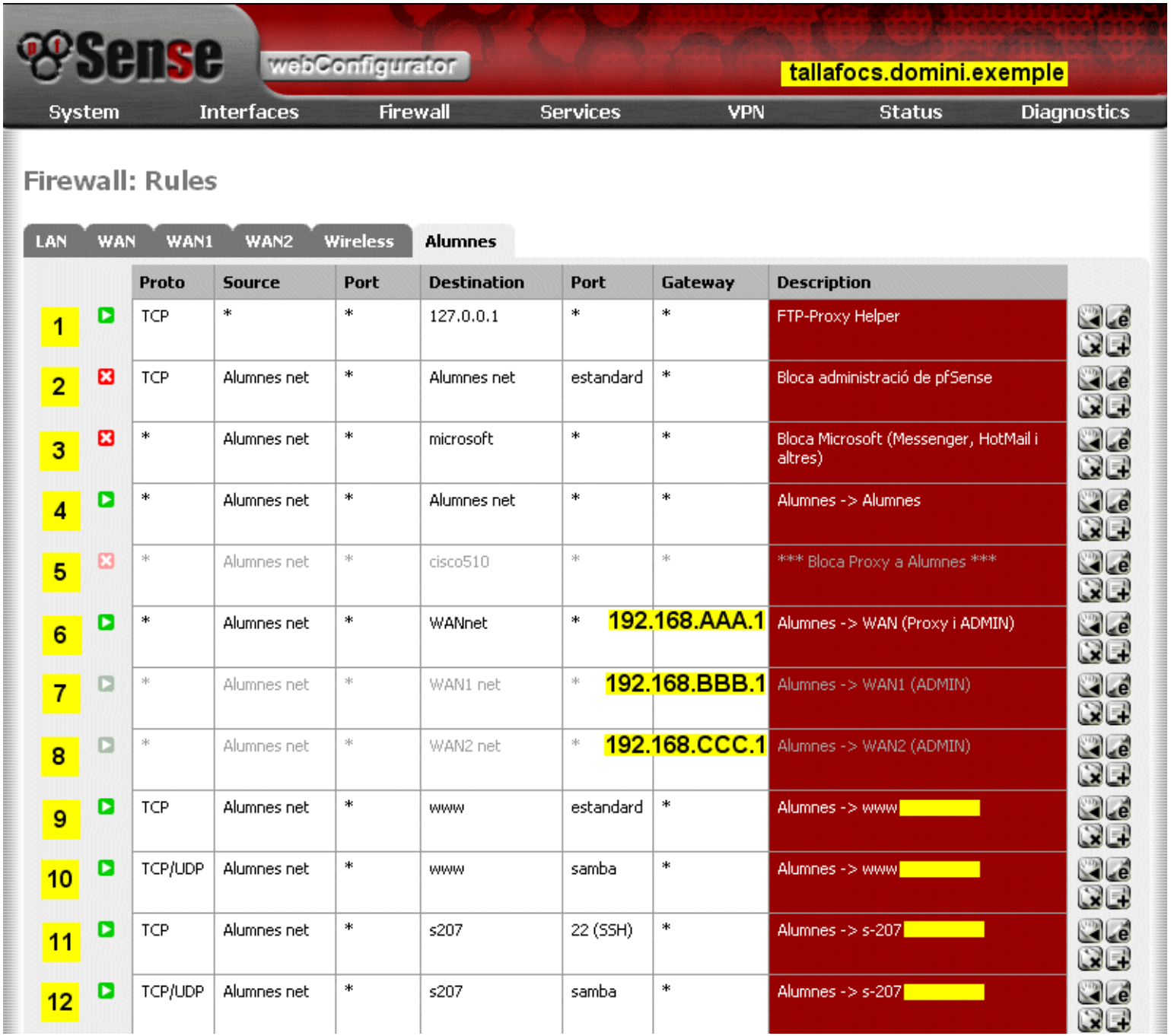
- La autorización del tráfico (desde la red WAN2) del NAT Port Forward anteriormente definido para s204.
- La autorización del tráfico (desde la red WAN2) para el port 1194, que emplea OpenVPN. pfSense incorpora el servidor OpenVPN, que permite montar accesos VPN. Por ejemplo, podremos conectarnos desde casa, con una IP dinámica, y ser una máquina más de las redes gestionadas por pfSense. Todo ello garantizando nuestra autentificación y estableciendo un túnel encriptado a través de Internet. Para más detalles sobre la configuración de OpenVPN, ir a la página [OpenVPN] de esta web.

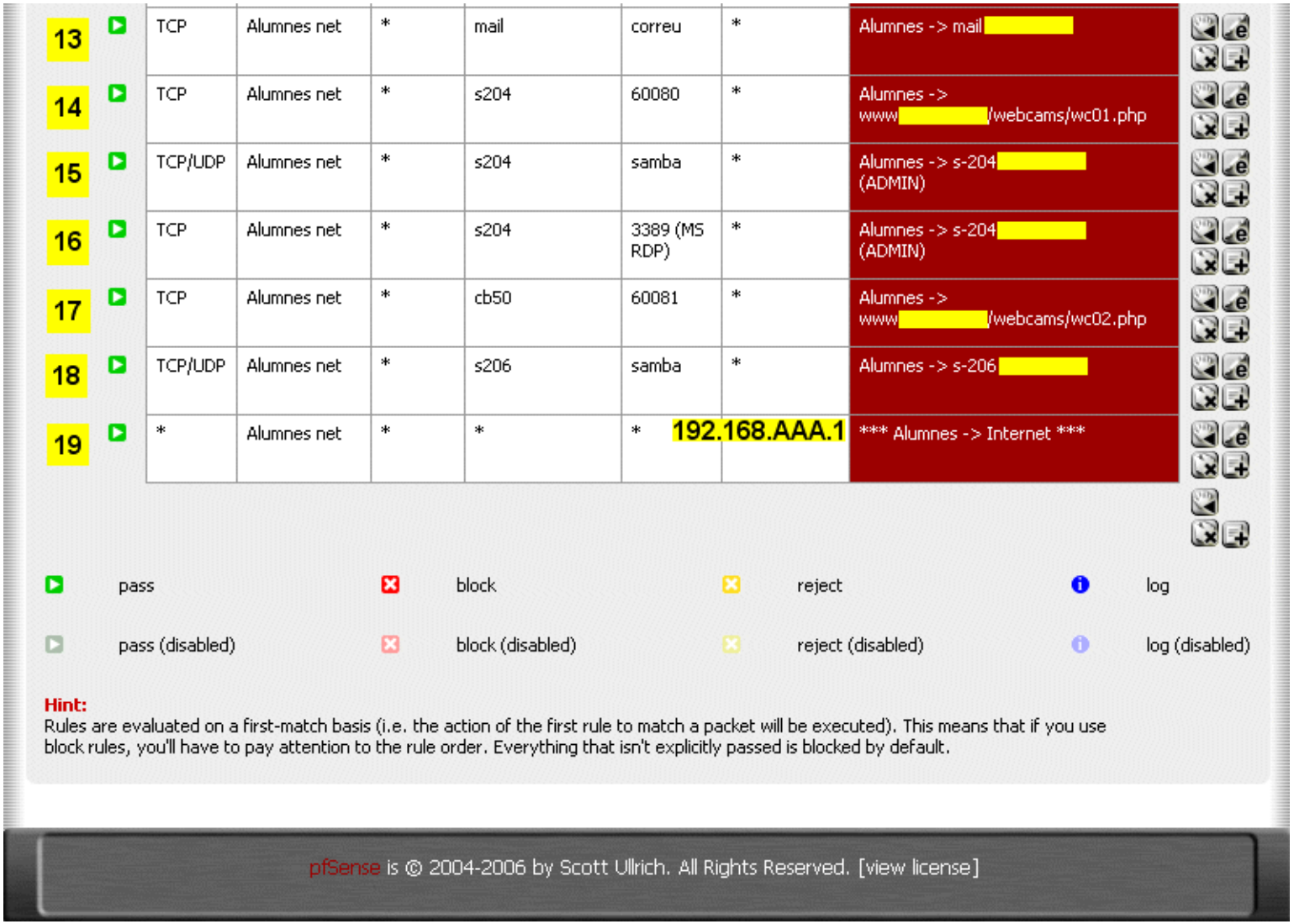

pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
LAN
WAN
WAN1
WAN2
Wireless
Alumnes
Proto
Source
Port
Destination
Port
Gateway
Description
TCP
*
*
s204
60080
*
NAT
www [redacted] /webcams/wc01.php
TCP
*
*
*
1194
*
OpenVPN -> LAN, Alumnes i Wireless
pass
block
reject
log
pass (disabled)
block (disabled)
reject (disabled)
log (disabled)
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]

[Firewall] [Rules] [Alumnes]

Explicación de les reglas:

1. Se permite el tráfico hacia FTP-Proxy Helper, que reside en localhost (127.0.0.1).
2. Se bloquea el acceso a la administración de pfSense desde la red Alumnes.
3. Se bloquea el acceso a servicios de Microsoft desde la red Alumnes. Este bloqueo funciona sólo si no se pasa por el proxy que hay en la WAN. Por ello, en proxy.pac hay una regla para ir directo en el caso de Microsoft.
4. En contraposición a la regla 2, se permiten el resto de accesos de Alumnes a Alumnes. Esta regla es necesaria porqué la red Alumnes ve la IP de pfSense como servidor DHCP, DNS y puerta de enlace predeterminada.
5. Regla desactivada. Si se la activa sirve para bloquear el acceso al servidor proxy situado en la red WAN.
6. Permite el acceso a la red WAN desde la red Alumnes. Regla necesaria para poder acceder al servidor proxy de la WAN.
7. Regla desactivada. Si se la activa permite el acceso a la red WAN1 desde la red Alumnes.
8. Regla desactivada. Si se la activa permite el acceso a la red WAN2 desde la red Alumnes.
9. Permite el acceso desde la red Alumnes a www por los puertos estandard (HTTP, HTTPS y SSH).
10. Permite el acceso desde la red Alumnes a www por los puertos samba (servidor Samba/CIFS).
11. Permite el acceso SSH desde la red Alumnes a s207.
12. Permite el acceso desde la red Alumnes a s207 por los puertos samba (servidor Samba/CIFS).
13. Permite el acceso desde la red Alumnes a mail por los puertos correu (SMTP, POP3 SSL, HTTP y HTTPS).
14. Permite el acceso desde la red Alumnes a s204 por el puerto 60080 (webcam).
15. Permite el acceso desde la red Alumnes a s204 por los puertos samba (servidor Samba/CIFS).
16. Permet el acceso por RDP desde la red Alumnes a s204.
17. Permite el acceso desde la red Alumnes a cb50 por el puerto 60081 (webcam).
18. Permite el acceso desde la red Alumnes a s206 por los puertos samba (servidor Samba/CIFS).
19. El resto de tráfico de la red Alumnes saldrá hacia Internet por el router ADSL 192.168.AAA.1.


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
LAN
WAN
WAN1
WAN2
Wireless
Alumnes
Proto
Source
Port
Destination
Port
Gateway
Description
1 TCP * * 127.0.0.1 * * FTP-Proxy Helper
2 TCP Alumnes net * Alumnes net estandard * Bloca administració de pfSense
3 * Alumnes net * microsoft * * Bloca Microsoft (Messenger, HotMail i altres)
4 * Alumnes net * Alumnes net * * Alumnes -> Alumnes
5 * Alumnes net * cisco510 * * *** Bloca Proxy a Alumnes ***
6 * Alumnes net * WANnet * 192.168.AAA.1 Alumnes -> WAN (Proxy i ADMIN)
7 * Alumnes net * WAN1 net * 192.168.BBB.1 Alumnes -> WAN1 (ADMIN)
8 * Alumnes net * WAN2 net * 192.168.CCC.1 Alumnes -> WAN2 (ADMIN)
9 TCP Alumnes net * www estandard * Alumnes -> www
10 TCP/UDP Alumnes net * www samba * Alumnes -> www
11 TCP Alumnes net * s207 22 (SSH) * Alumnes -> s-207
12 TCP/UDP Alumnes net * s207 samba * Alumnes -> s-207



13	▶	TCP	Alumnes net	*	mail	correu	*	Alumnes -> mail [redacted]
14	▶	TCP	Alumnes net	*	s204	60080	*	Alumnes -> www [redacted] /webcams/wc01.php
15	▶	TCP/UDP	Alumnes net	*	s204	samba	*	Alumnes -> s-204 [redacted] (ADMIN)
16	▶	TCP	Alumnes net	*	s204	3389 (MS RDP)	*	Alumnes -> s-204 [redacted] (ADMIN)
17	▶	TCP	Alumnes net	*	cb50	60081	*	Alumnes -> www [redacted] /webcams/wc02.php
18	▶	TCP/UDP	Alumnes net	*	s206	samba	*	Alumnes -> s-206 [redacted]
19	▶	*	Alumnes net	*	*	*	192.168.AAA.1	*** Alumnes -> Internet ***

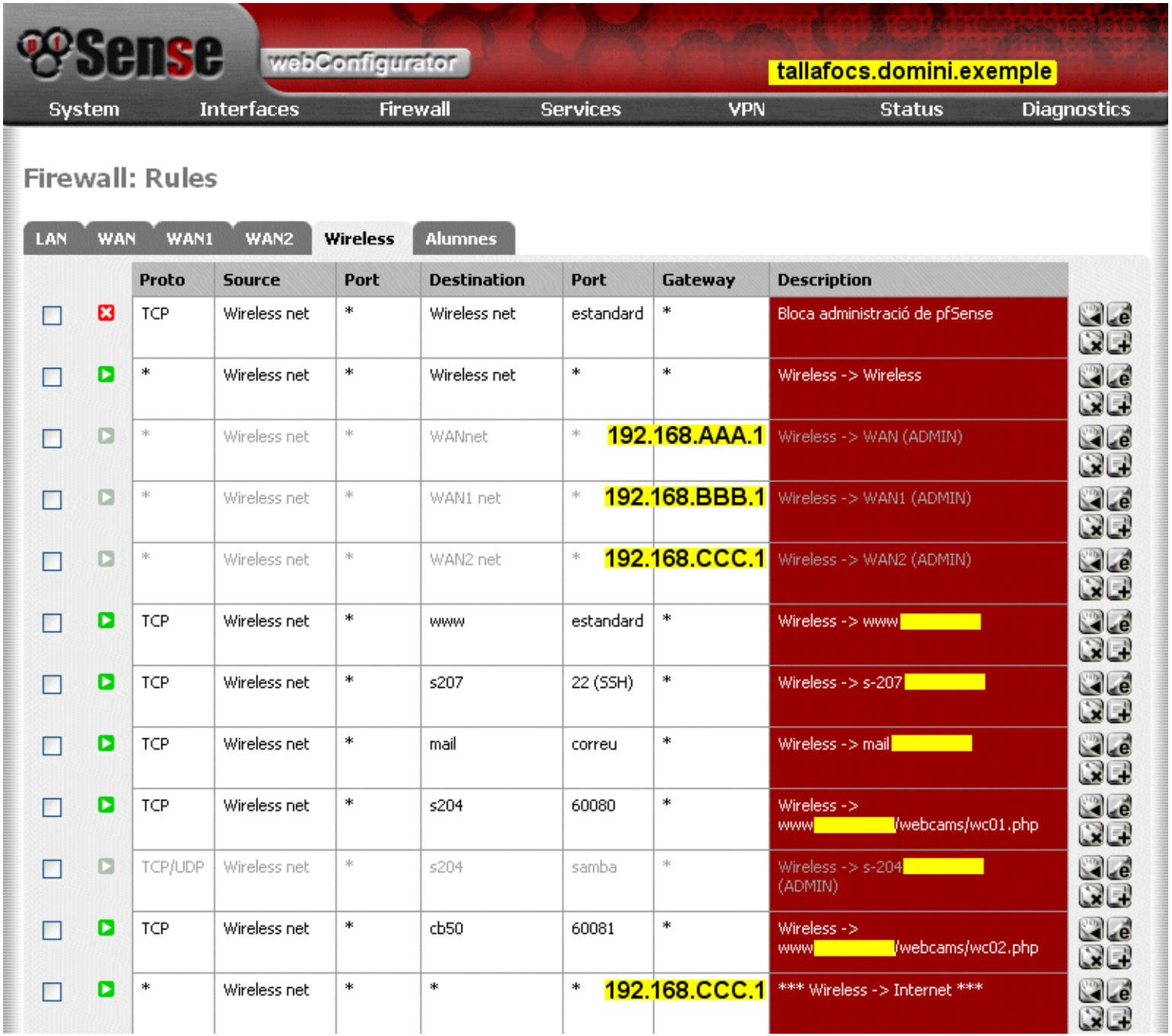
▶	pass	✖	block	✖	reject	ℹ	log
▶	pass (disabled)	✖	block (disabled)	✖	reject (disabled)	ℹ	log (disabled)

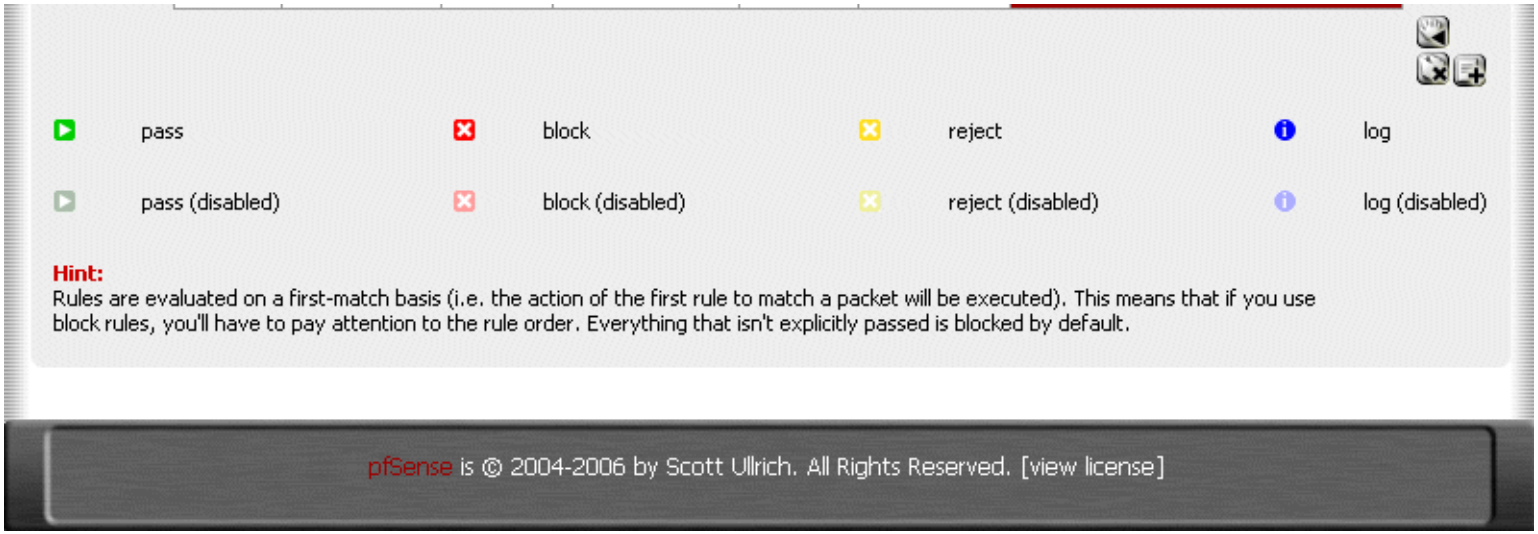
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

[Firewall] [Rules] [Wireless]

Vistas las reglas de la red Alumnes (sin duda la más compleja), las de la red Wireless se explican por si mismas ...

Las diferencias son que para la Wireless sólo se autorizan los servicios locales que se tendrían si se accediese desde Internet (web, SSH, correo y webcams) y que la conexión a Internet se hace por el router ADSL 192.168.CCC.1.


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
LAN
WAN
WAN1
WAN2
Wireless
Alumnes
Proto
Source
Port
Destination
Port
Gateway
Description
TCP
Wireless net
*
Wireless net
estandard
*
Bloca administració de pfSense
*
Wireless net
*
Wireless net
*
*
Wireless -> Wireless
*
Wireless net
*
WANnet
*
192.168.AAA.1
Wireless -> WAN (ADMIN)
*
Wireless net
*
WAN1 net
*
192.168.BBB.1
Wireless -> WAN1 (ADMIN)
*
Wireless net
*
WAN2 net
*
192.168.CCC.1
Wireless -> WAN2 (ADMIN)
TCP
Wireless net
*
www
estandard
*
Wireless -> www
TCP
Wireless net
*
s207
22 (SSH)
*
Wireless -> s-207
TCP
Wireless net
*
mail
correu
*
Wireless -> mail
TCP
Wireless net
*
s204
60080
*
Wireless -> www /webcams/wc01.php
TCP/UDP
Wireless net
*
s204
samba
*
Wireless -> s-204 (ADMIN)
TCP
Wireless net
*
cb50
60081
*
Wireless -> www /webcams/wc02.php
*
Wireless net
*
*
*
192.168.CCC.1
*** Wireless -> Internet ***



DNS (Domain Name Server)

Yendo a [Services] [DNS forwarder] activaremos el DNS (servidor de nombres) que incorpora pfSense y, además, le diremos que haga uso de las asignaciones que realice el DHCP de pfSense, tal como muestran las dos primeras casillas de verificación de la pantalla que figura al final de esta página.

A pesar de que FreeBSD lleva como DNS el conocido BIND, pfSense emplea como DNS y DHCP el demonio (daemon) dnsmasq, ideal para cortafuegos.

Es un servidor de nombres limitado pero muy rápido, que recurrirá a los servidores de nombres especificados en la configuración básica del cortafuegos cuando no pueda resolver un nombre.

Al emplear el DHCP de pfSense, las máquinas verán el cortafuegos como su servidor de nombres y su puerta de enlace.

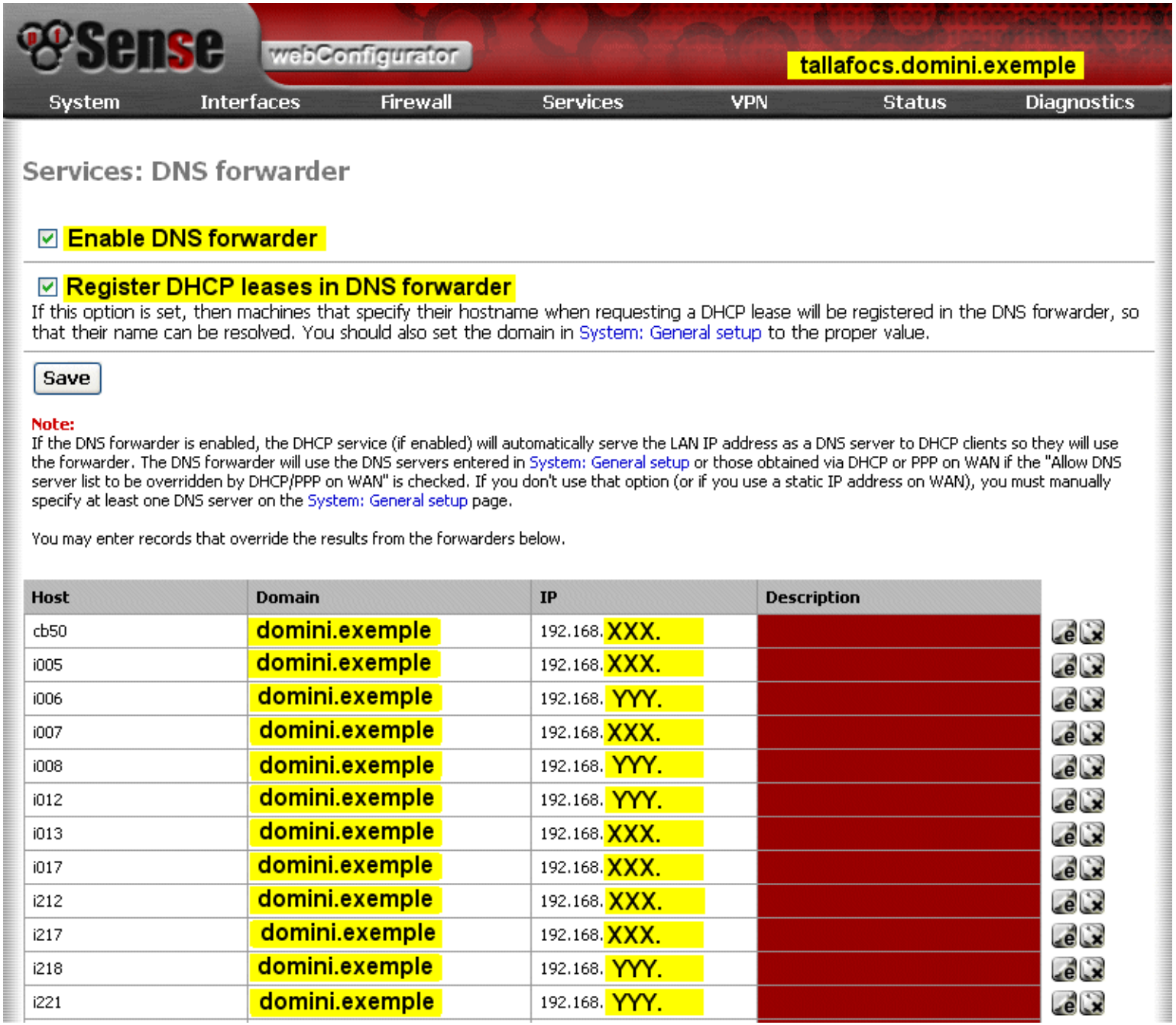
Además, podemos indicar nombres de máquinas (incluido su dominio) para forzar la resolución del nombre de máquina hacia una determinada IP. Ello nos permite asignar IP locales a nombres de máquina del tipo **nombremaquina.dominio.ejemplo**, con lo que los usuarios podrán ver un servicio (web, correo) con el mismo nombre tanto si están en la red local como si se conectan desde Internet (desde casa, desde una biblioteca, desde un ciber, ...)

Resulta ideal poner en esta lista de nombres de máquina (que puedes ver en la figura de más abajo) todas las máquinas que den

servicios a la red (servidores e impresoras). De esta forma la resolución de nombres para los servicios será altamente eficaz.

Eventualmente también se puede emplear esta asignación para bloquear/redireccionar el acceso a alguna dirección de Internet que no interese que esté disponible. No conviene, pero, abusar de esta funcionalidad. Si lo que pretendemos es filtrar contenidos más vale pensar en un servidor proxy como, por ejemplo, Squid.

[Services] [DNS forwarder]


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Services: DNS forwarder
Enable DNS forwarder
Register DHCP leases in DNS forwarder
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
Save
Note:
If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in System: General setup or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the System: General setup page.
You may enter records that override the results from the forwarders below.
Host
Domain
IP
Description
cb50 domini.exemple 192.168.XXX.
i005 domini.exemple 192.168.XXX.
i006 domini.exemple 192.168.YYY.
i007 domini.exemple 192.168.XXX.
i008 domini.exemple 192.168.YYY.
i012 domini.exemple 192.168.YYY.
i013 domini.exemple 192.168.XXX.
i017 domini.exemple 192.168.XXX.
i212 domini.exemple 192.168.XXX.
i217 domini.exemple 192.168.XXX.
i218 domini.exemple 192.168.YYY.
i221 domini.exemple 192.168.YYY.

i223	domini.exemple	192.168. YYY.	
i224	domini.exemple	192.168. YYY.	
i240	domini.exemple	192.168. XXX.	
i241	domini.exemple	192.168. YYY.	
i242	domini.exemple	192.168. YYY.	
i243	domini.exemple	192.168. YYY.	
i245	domini.exemple	192.168. XXX.	
mail	domini.exemple	192.168. XXX.	
mail	domini.exemple	192.168. XXX.	Compatibilitat amb el ja no usat .org
proxy	domini.exemple	192.168. AAA.3	
s-18	domini.exemple	192.168. XXX.	
s-204	domini.exemple	192.168. XXX.	
s-206	domini.exemple	192.168. XXX.	
s-207	domini.exemple	192.168. XXX.	
www	domini.exemple	192.168. XXX.	

Below you can override an entire domain by specifying an authoritative dns server to be queried for that domain.

Domain	IP	Description

DNS (Domain Name Server)

Yendo a [Services] [DNS forwarder] activaremos el DNS (servidor de nombres) que incorpora pfSense y, además, le diremos que haga uso de las asignaciones que realice el DHCP de pfSense, tal como muestran las dos primeras casillas de verificación de la pantalla que figura al final de esta página.

A pesar de que FreeBSD lleva como DNS el conocido BIND, pfSense emplea como DNS y DHCP el demonio (daemon) dnsmasq, ideal para cortafuegos.

Es un servidor de nombres limitado pero muy rápido, que recurrirá a los servidores de nombres especificados en la configuración básica del cortafuegos cuando no pueda resolver un nombre.

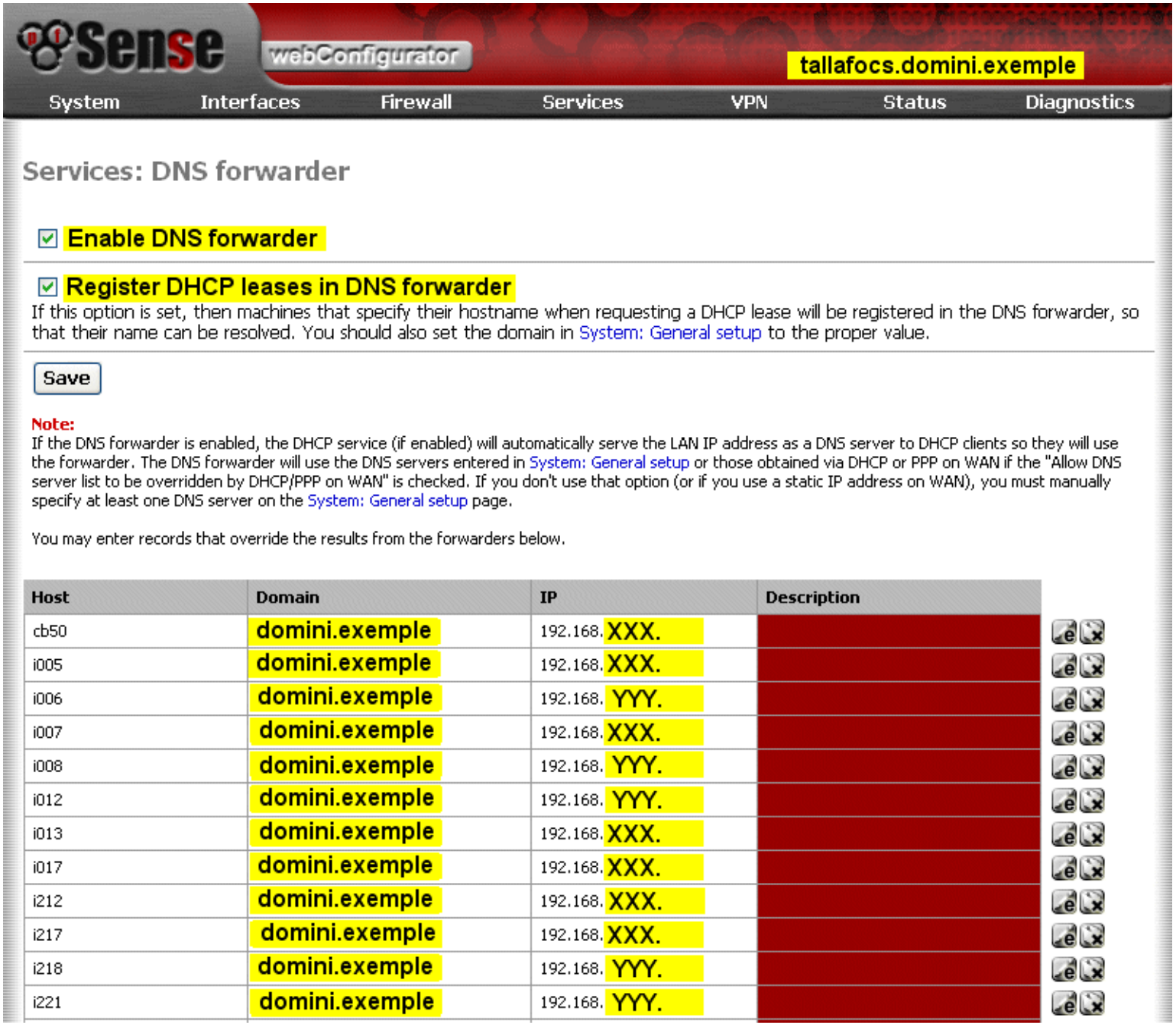
Al emplear el DHCP de pfSense, las máquinas verán el cortafuegos como su servidor de nombres y su puerta de enlace.

Además, podemos indicar nombres de máquinas (incluido su dominio) para forzar la resolución del nombre de máquina hacia una determinada IP. Ello nos permite asignar IP locales a nombres de máquina del tipo **nombremaquina.dominio.ejemplo**, con lo que los usuarios podrán ver un servicio (web, correo) con el mismo nombre tanto si están en la red local como si se conectan desde Internet (desde casa, desde una biblioteca, desde un ciber, ...)

Resulta ideal poner en esta lista de nombres de máquina (que puedes ver en la figura de más abajo) todas las máquinas que den servicios a la red (servidores e impresoras). De esta forma la resolución de nombres para los servicios será altamente eficaz.

Eventualmente también se puede emplear esta asignación para bloquear/redireccionar el acceso a alguna dirección de Internet que no interese que esté disponible. No conviene, pero, abusar de esta funcionalidad. Si lo que pretendemos es filtrar contenidos más vale pensar en un servidor proxy como, por ejemplo, Squid.

[Services] [DNS forwarder]


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Services: DNS forwarder
Enable DNS forwarder
Register DHCP leases in DNS forwarder
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
Save
Note:
If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in System: General setup or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the System: General setup page.
You may enter records that override the results from the forwarders below.
Host
Domain
IP
Description
cb50 domini.exemple 192.168.XXX.
i005 domini.exemple 192.168.XXX.
i006 domini.exemple 192.168.YYY.
i007 domini.exemple 192.168.XXX.
i008 domini.exemple 192.168.YYY.
i012 domini.exemple 192.168.YYY.
i013 domini.exemple 192.168.XXX.
i017 domini.exemple 192.168.XXX.
i212 domini.exemple 192.168.XXX.
i217 domini.exemple 192.168.XXX.
i218 domini.exemple 192.168.YYY.
i221 domini.exemple 192.168.YYY.

i223	domini.exemple	192.168. YYY.	
i224	domini.exemple	192.168. YYY.	
i240	domini.exemple	192.168. XXX.	
i241	domini.exemple	192.168. YYY.	
i242	domini.exemple	192.168. YYY.	
i243	domini.exemple	192.168. YYY.	
i245	domini.exemple	192.168. XXX.	
mail	domini.exemple	192.168. XXX.	
mail	domini.exemple	192.168. XXX.	Compatibilitat amb el ja no usat .org
proxy	domini.exemple	192.168. AAA.3	
s-18	domini.exemple	192.168. XXX.	
s-204	domini.exemple	192.168. XXX.	
s-206	domini.exemple	192.168. XXX.	
s-207	domini.exemple	192.168. XXX.	
www	domini.exemple	192.168. XXX.	

Below you can override an entire domain by specifying an authoritative dns server to be queried for that domain.

Domain	IP	Description

DHCP (Dynamic Host Configuration Protocol)

Emplearemos DHCP en las tres LAN (LAN, Alumnes i Wireless), mientras que en las WAN (WAN, WAN1 y WAN2) las direcciones IP estarán configuradas de forma totalmente estática.

He tardado años en decidirme por DHCP, pero con las funcionalidades que ofrece el DHCP de pfSense (basado en dnsmasq) he apostado por él incluso en los puntos de acceso de la red sin hilos y las impresoras de red.

¿Qué me ha hecho decidir? Pues:

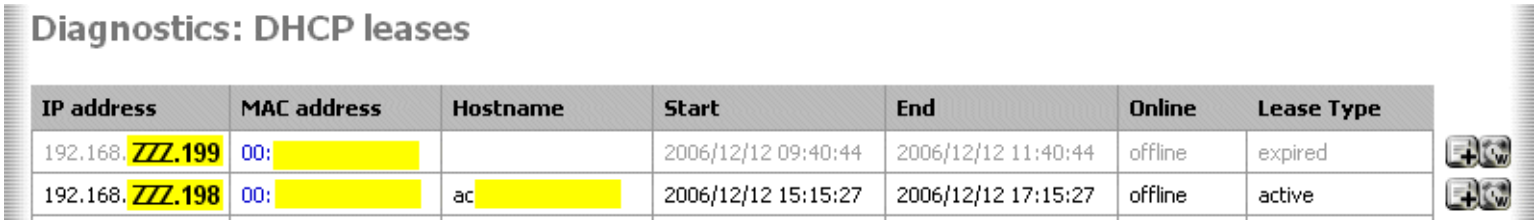
- La posibilidad de asignar direcciones IP "estáticas" en función de la dirección MAC del dispositivo.
- La posibilidad de "capturar" fácilmente las direcciones MAC, sin tener que introducirlas manualmente.
- La posibilidad de "cerrar" la lista de direcciones MAC, impidiendo la conexión de dispositivos "no conocidos".
- Poder "despertar" (wake-up) dispositivos de la red para tareas de mantenimiento remoto.
- Tener una pantalla donde tienes relacionados todos los equipos de una red.
- Eventual movilidad de equipos entre redes.
- Y, evidentemente, lo que supone intrínsecamente el uso de DHCP: olvidarme de una vez por todas de configurar las conexiones de red de cada dispositivo (ordenador, punto de acceso, impresora, ...) ¡Lástima que esto no pueda incluir el nombre de máquina!

[Services] [DHCP Server] [LAN]
[Services] [DHCP Server] [Alumnes]
[Services] [DHCP Server] [Wireless]

[Services] [DHCP Server] [LAN]

Activaremos pues la casilla [Enable DHCP server on LAN interface]. Indicaremos el rango de IP que queremos que el servidor asigne en las casillas [Range] y guardaremos los cambios. Con ello ya tendremos DHCP activado para la interfase.

Después haremos que cada máquina tome una dirección IP determinada (fuera del rango) en función de su dirección MAC. De esta forma cada máquina tendrá siempre la misma dirección IP (DHCP estático). Para ello necesitamos llenar la tabla [MAC address][IP address] [Description], pero no lo haremos (en principio) desde esta pantalla, si no que iremos al menú [Status] [DHCP Leases] del cortafuegos:



Diagnostics: DHCP leases

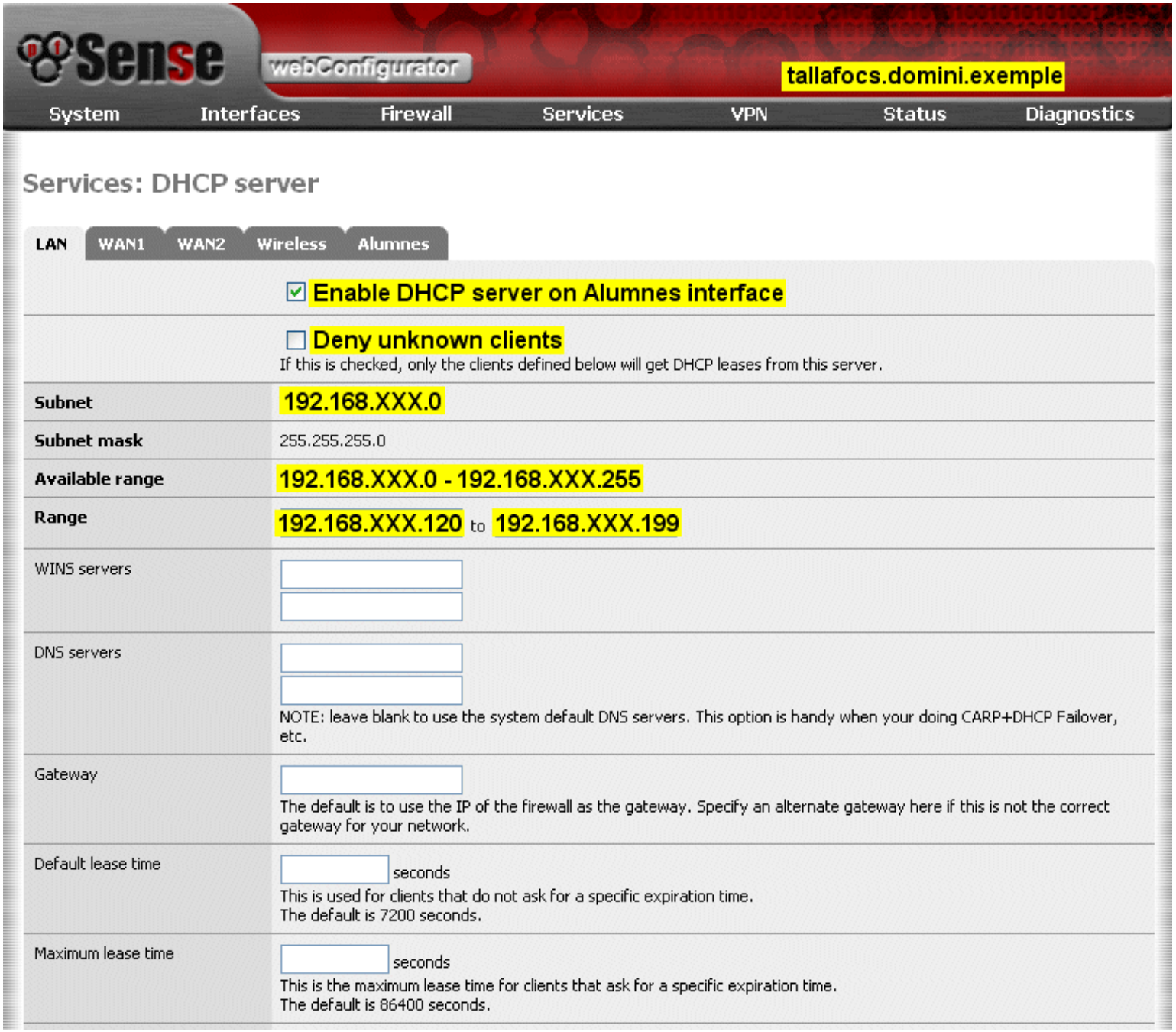
IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.ZZZ.199	00:		2006/12/12 09:40:44	2006/12/12 11:40:44	offline	expired
192.168.ZZZ.198	00:	ac	2006/12/12 15:15:27	2006/12/12 17:15:27	offline	active

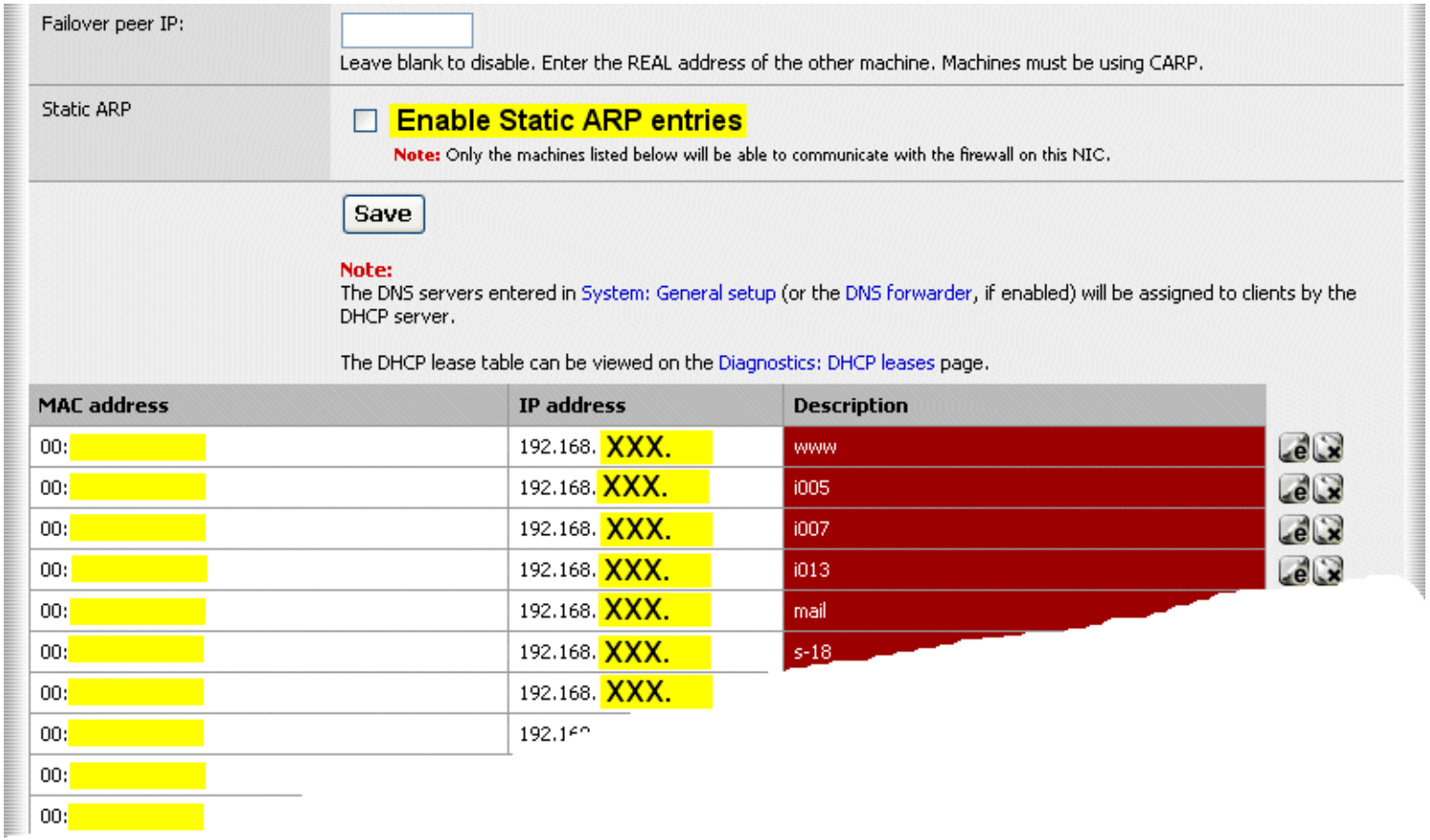
Allí podremos emplear el botón para "capturar" la dirección MAC, asignarle una dirección IP y modificar el comentario (inicialmente es el nombre de máquina). A partir de aquí se asignará siempre la misma dirección IP para la máquina en cuestión. Hay que tener presente que esta dirección IP no puede estar, naturalmente, dentro del rango de direcciones automáticas de DHCP. La "captura" se puede hacer mientras la máquina esté en la lista [DHCP leases]. Estará en ella mientras esté conectada o no haya pasado demasiado tiempo desde su desconexión.

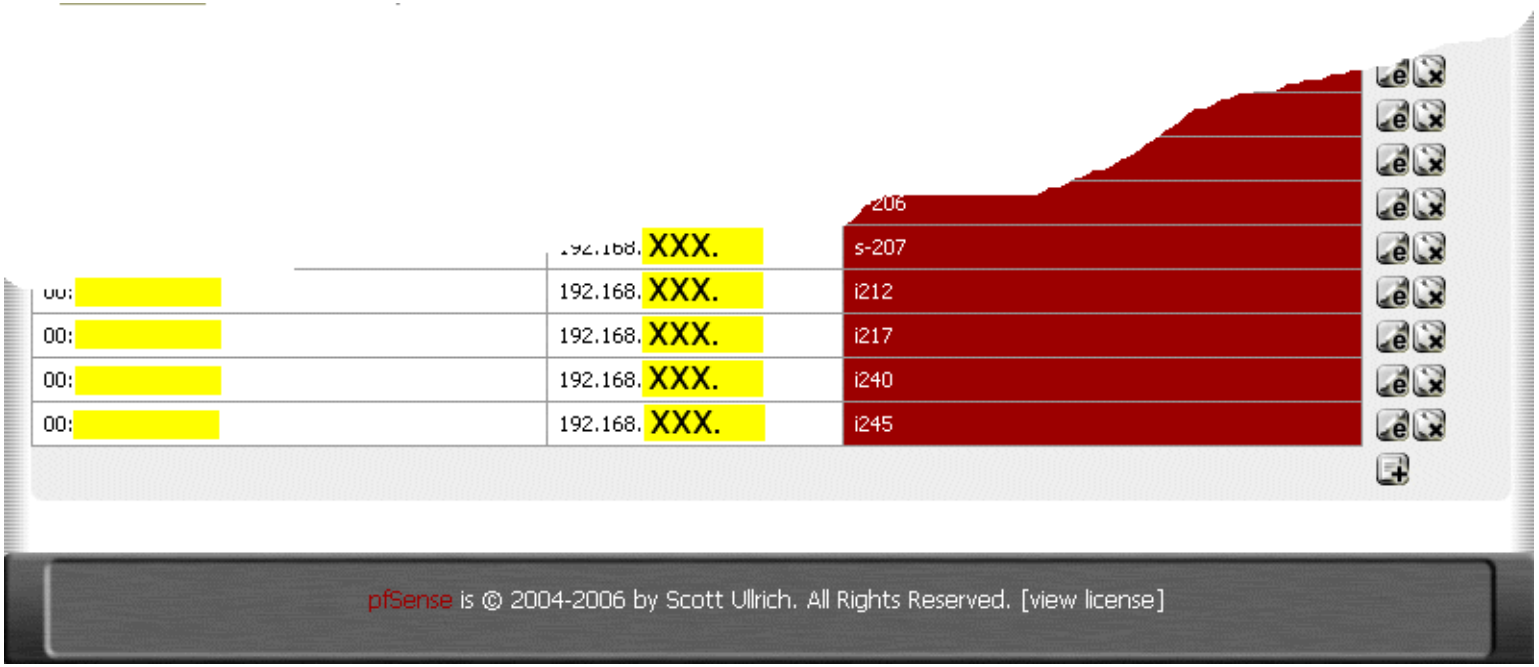
Si queremos "cerrar" la red a nuevas máquinas habrá que activar una de estas dos casillas de verificación:

- Deny unknown clients. En este caso sólo se asignan direcciones IP para las máquinas que figuran en la lista de direcciones MAC que hay al final de la pantalla. Se permite el resto de comunicaciones con el cortafuegos.
- Enable static ARP entries. Sólo las máquinas que figuren en la lista de direcciones MAC podrán comunicarse con el cortafuegos. A pesar de que un hacker podría llegar a falsear una dirección MAC esta opción es mucho más segura que la anterior.

¡Cuidado con "cerrar" las redes si no se han incluido todas las máquinas! Si hay máquinas que no funcionan por DHCP habrá que mirar su dirección MAC (orden **ipconfig /all** en Windows y **ifconfig** en Unix/Linux) y entrarlas manualmente en la lista.

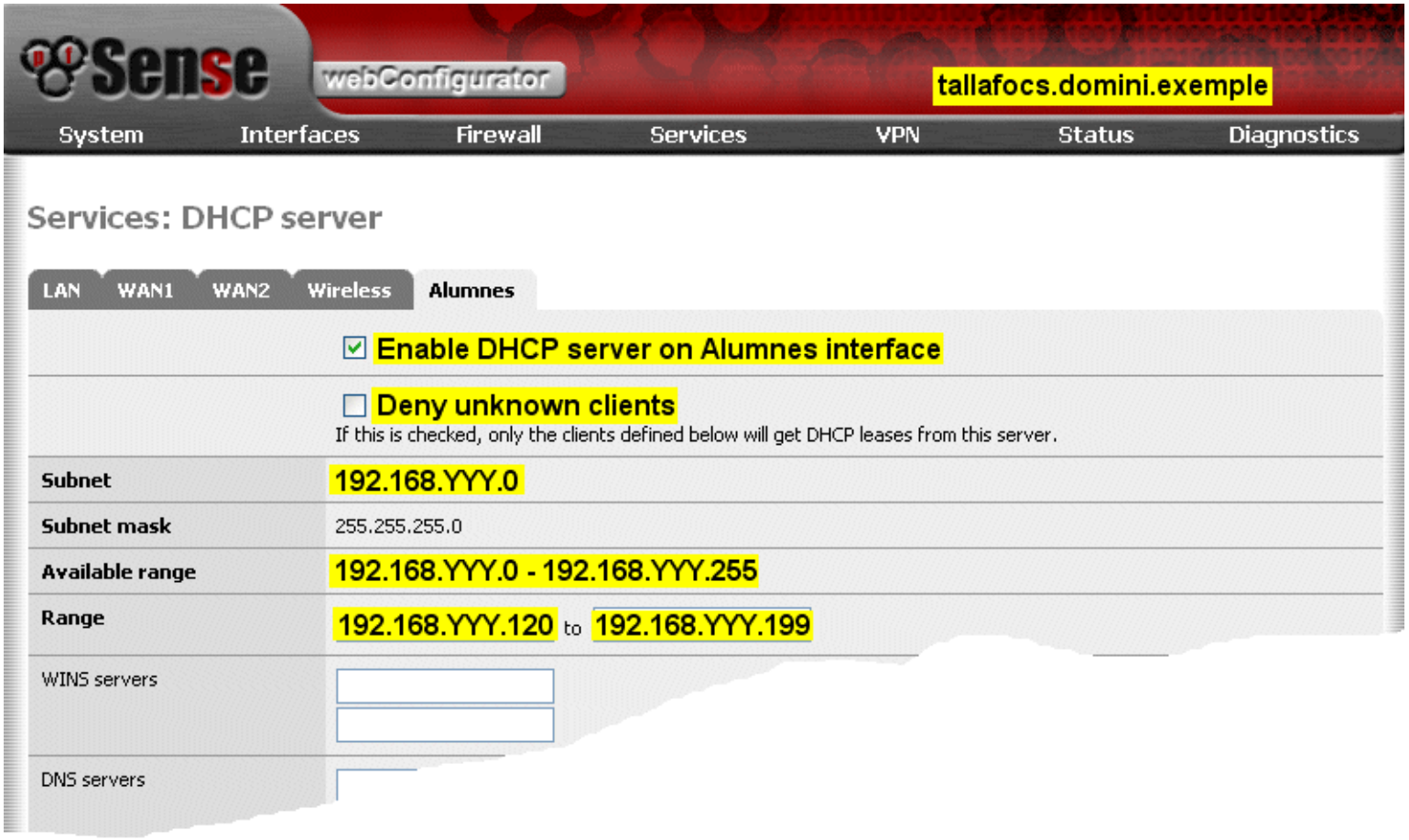

pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Services: DHCP server
LAN
WAN1
WAN2
Wireless
Alumnes
Enable DHCP server on Alumnes interface
Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.
Subnet
192.168.XXX.0
Subnet mask
255.255.255.0
Available range
192.168.XXX.0 - 192.168.XXX.255
Range
192.168.XXX.120 to 192.168.XXX.199
WINS servers
DNS servers
NOTE: leave blank to use the system default DNS servers. This option is handy when your doing CARP+DHCP Failover, etc.
Gateway
The default is to use the IP of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.
Default lease time
seconds
This is used for clients that do not ask for a specific expiration time.
The default is 7200 seconds.
Maximum lease time
seconds
This is the maximum lease time for clients that ask for a specific expiration time.
The default is 86400 seconds.


Failover peer IP:
Leave blank to disable. Enter the REAL address of the other machine. Machines must be using CARP.
Static ARP
Enable Static ARP entries
Note: Only the machines listed below will be able to communicate with the firewall on this NIC.
Save
Note:
The DNS servers entered in System: General setup (or the DNS forwarder, if enabled) will be assigned to clients by the DHCP server.
The DHCP lease table can be viewed on the Diagnostics: DHCP leases page.
MAC address
IP address
Description
00:
192.168. XXX.
www
i005
i007
i013
mail
s-18



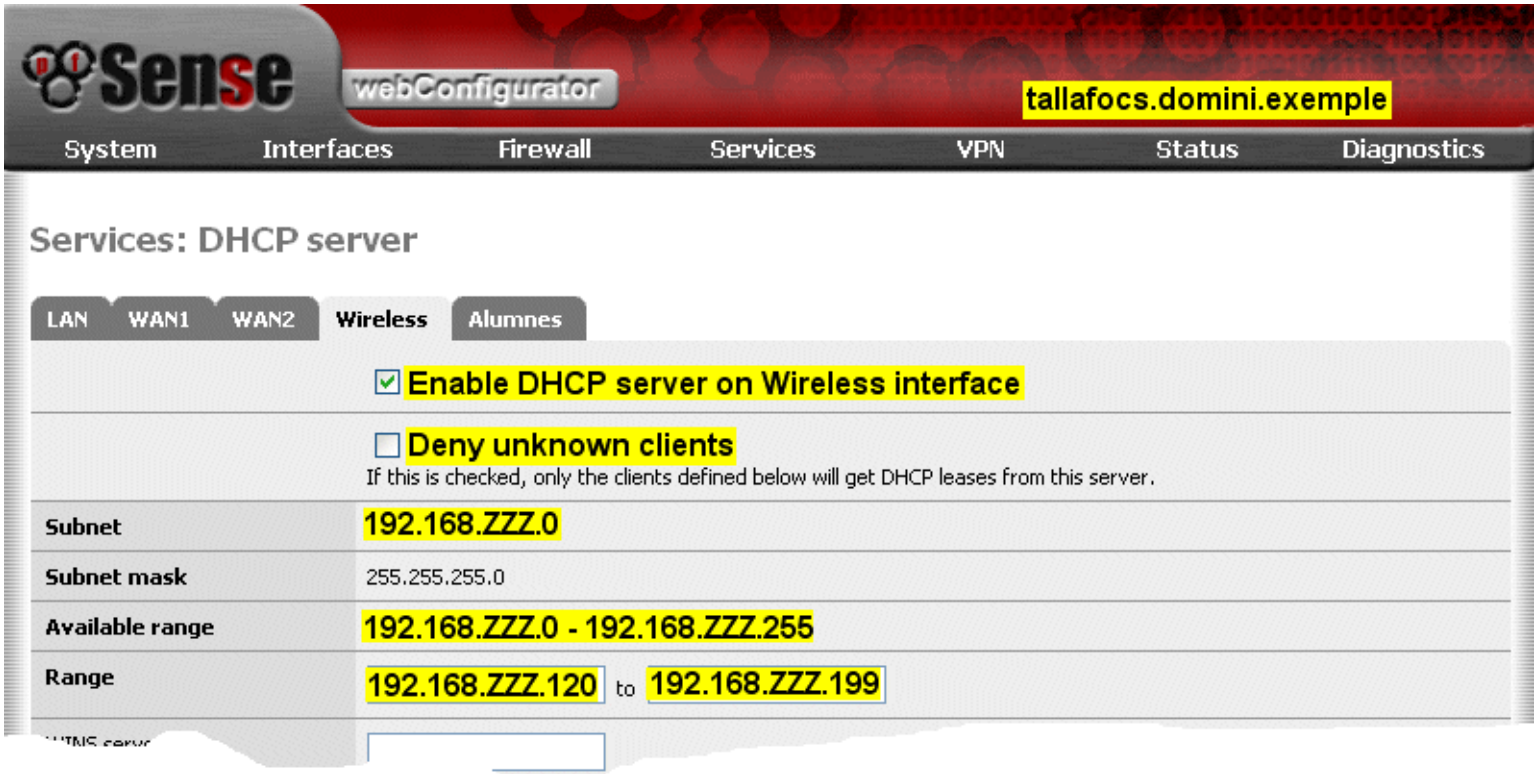
[Services] [DHCP Server] [Alumnes]

De forma similar a la red LAN, activaremos DHCP en la red Alumnes y "capturaremos" sus direcciones MAC para que cada máquina trabaje siempre con la misma dirección IP.



[Services] [DHCP Server] [Wireless]

Tal como hemos hecho en las redes LAN y Alumnes, activaremos DHCP en la red Wireless y "capturaremos" las direcciones MAC de los puntos de acceso y de los ordenadores que tengan tarjeta sin hilos (wireless) para que siempre trabajen con la misma dirección IP.



Regulador de caudal ALTQ

El regulador de caudal ALTQ (Alternate Queuing) forma parte de Packet Filter (PF), originario de OpenBSD. Packet Filter (PF) está presente como estándar en FreeBSD desde noviembre del 2004. pfSense es una distribución basada en FreeBSD.

ALTQ es un conjunto de herramientas de calidad de servicio (QoS) que permiten montar colas de tráfico, asignando caudales y prioridades. ALTQ dispone de distintos modelos de funcionamiento.

pfSense emplea colas HFSC (Hierarchical Fair Service Curve) con funcionalidades ACK, RED (Random Early Detection) y ECN (Explicit Congestion Notification).

Cada cola HFSC (Hierarchical Fair Service Curve) tiene los siguientes parámetros encargados de garantizar su caudal:

- **UpperLimit**: Caudal máximo para la cola. Nunca tendrá más tráfico que el indicado.
- **RealTime**: Caudal mínimo para la cola. Independientemente del tráfico que se tenga en la interfase se garantiza este caudal.
- **LinkShare**: HFSC calcula el caudal sobrante en la interfase teniendo en cuenta que se cumplan los caudales mínimos (**RealTime**) de cada cola. Este sobrante de caudal se reparte entonces entre las colas, en función de su valor **LinkShare**. Por ejemplo, si se tienen dos colas con un 50% en **LinkShare** y se satura la conexión, ambas colas presentarán el mismo exceso de tráfico. Por contra, si una de las dos colas no necesita caudal sobrante, la otra lo cogerá todo.
- **m1**: Caudal inicial a tener en **d** milisegundos.
- **d**: Milisegundos que se tardará en tener el caudal **m1**.
- **m2**: Caudal final a tener. Los parámetros **m1**, **d** y **m2** modelan la curva (arranque) de la cola.
- **BandWidth**: Por comodidad, se indica este parámetro que, de hecho, corresponde al valor **m2** de **LinkShare**. Si ponemos un valor en **m2** de **LinkShare** el que esté en **BandWidth** no sirve para nada. Se recomienda no hacerlo.

En las ventanas que pfSense tiene para las colas estos parámetros se presentan en forma de tabla, excepto BandWidth que figura como primer parámetro de la cola:

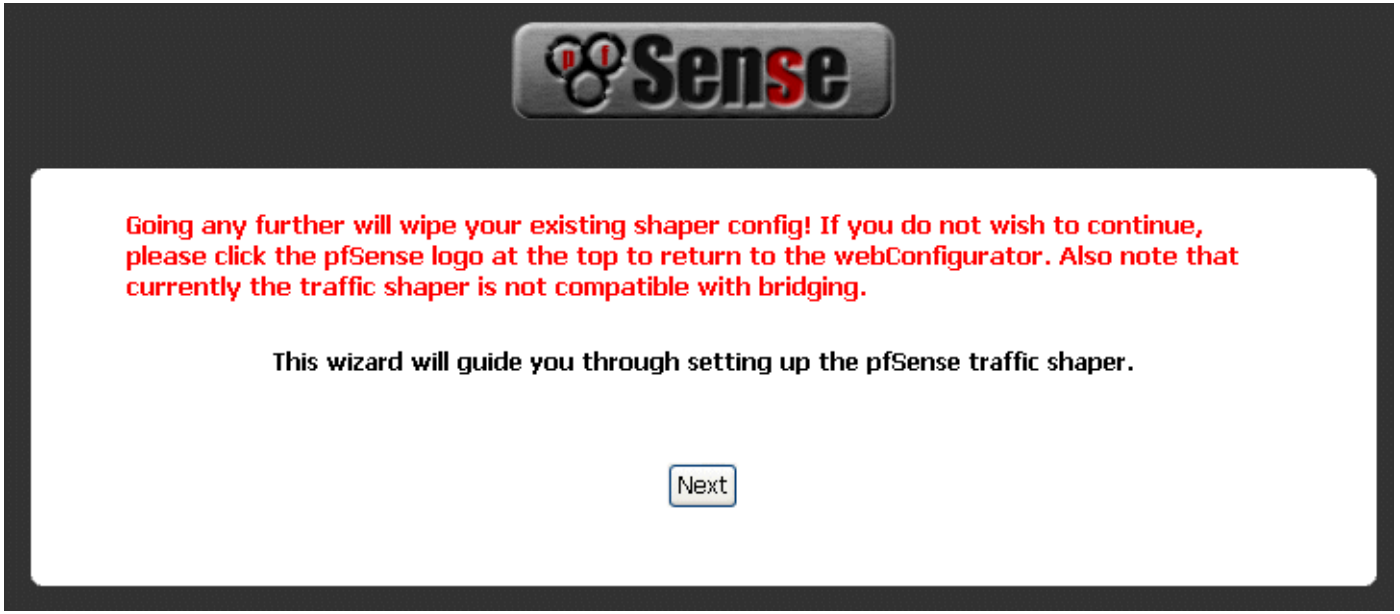
	m1	**d**	**m2**
UpperLimit			
RealTime			
LinkShare			

ALTQ es algo complejo de configurar y ajustar, por lo que pfSense incorpora un asistente y herramientas de monitorización de las colas.

[Firewall] [Traffic Shaper] [Wizard]
Colas creadas por el asistente
Ajuste del regulador de caudal
La otra solución para controlar P2P

[Firewall] [Traffic Shaper] [Wizard]

La primera vez que entramos aquí se ejecutará el asistente ...



¡Atención! Cuando ya tengamos configurado Traffic Shaper la simple entrada al asistente desmonta toda la configuración de Traffic Shaper. Si hacemos clic sobre el logotipo de pfSense se cancela la acción.

Hacemos clic sobre el botón 

para continuar con el asistente ...

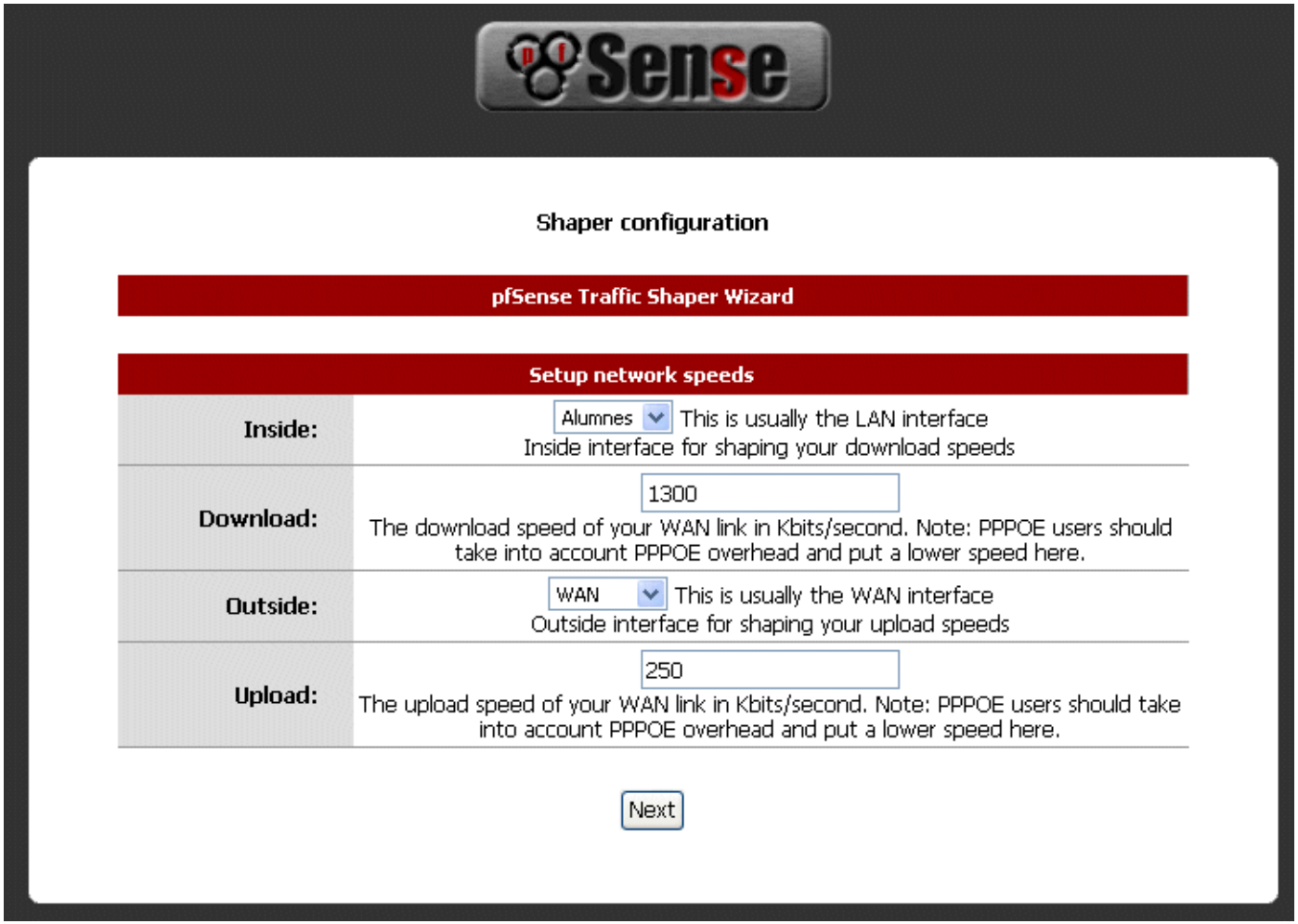
Ahora tendremos que indicar:

- La interfase de dentro (inside) y la velocidad de bajada (download) de la ADSL en kbit/s.
- La interfase de fuera (outside) y la velocidad de subida (upload) de la ADSL en kbit/s.

Si se puede medir la ADSL empleando una herramienta como MRTG, mejor. En el caso expuesto se ha podido comprobar con MRTG que "la cosa" no da para más de 1.300/250 kbit/s.

Hacemos 

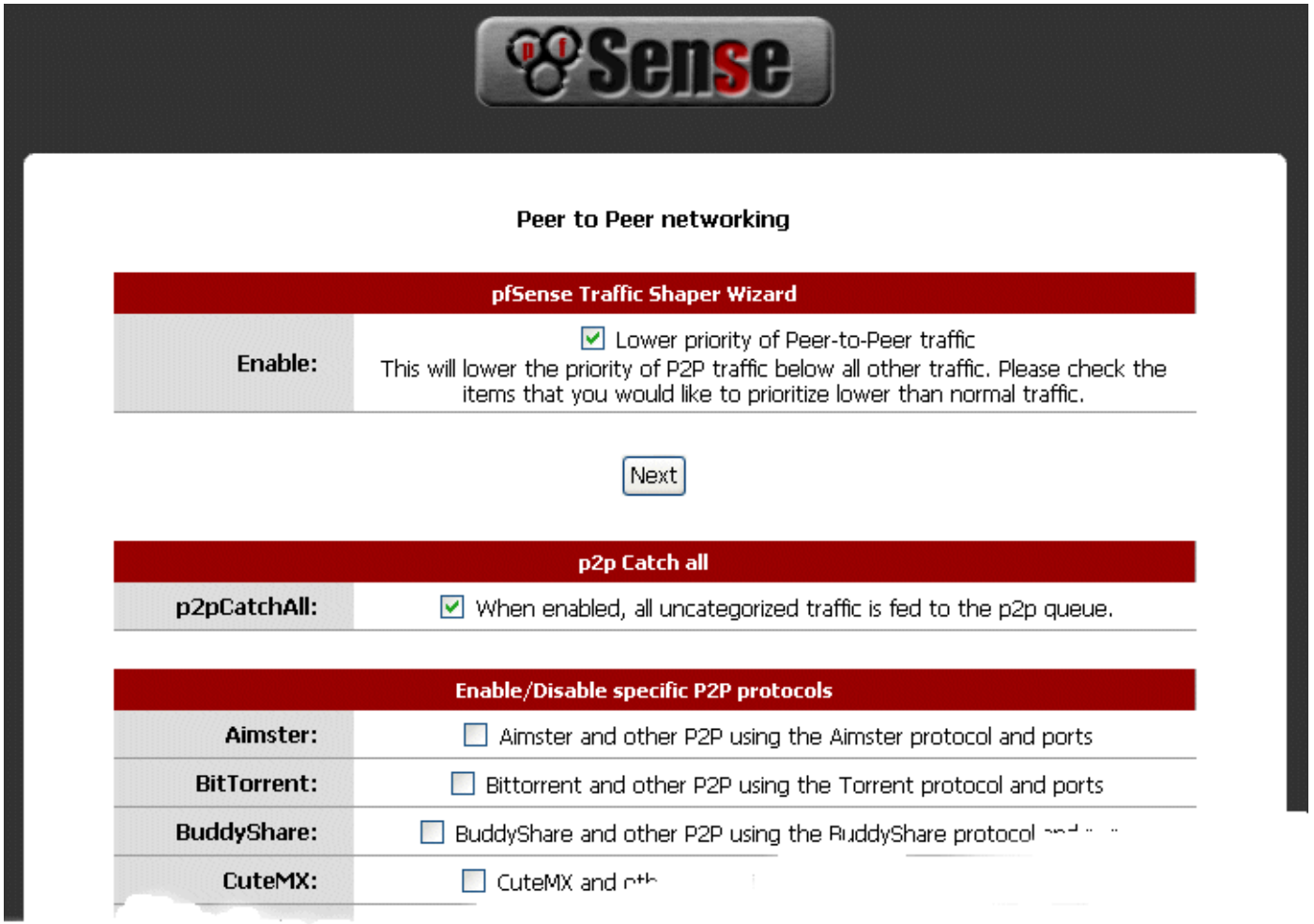
...



A continuación se nos pide si queremos un tratamiento especial para comunicaciones de voz sobre IP. Como que no es nuestro caso, nos saltamos la pantalla con 

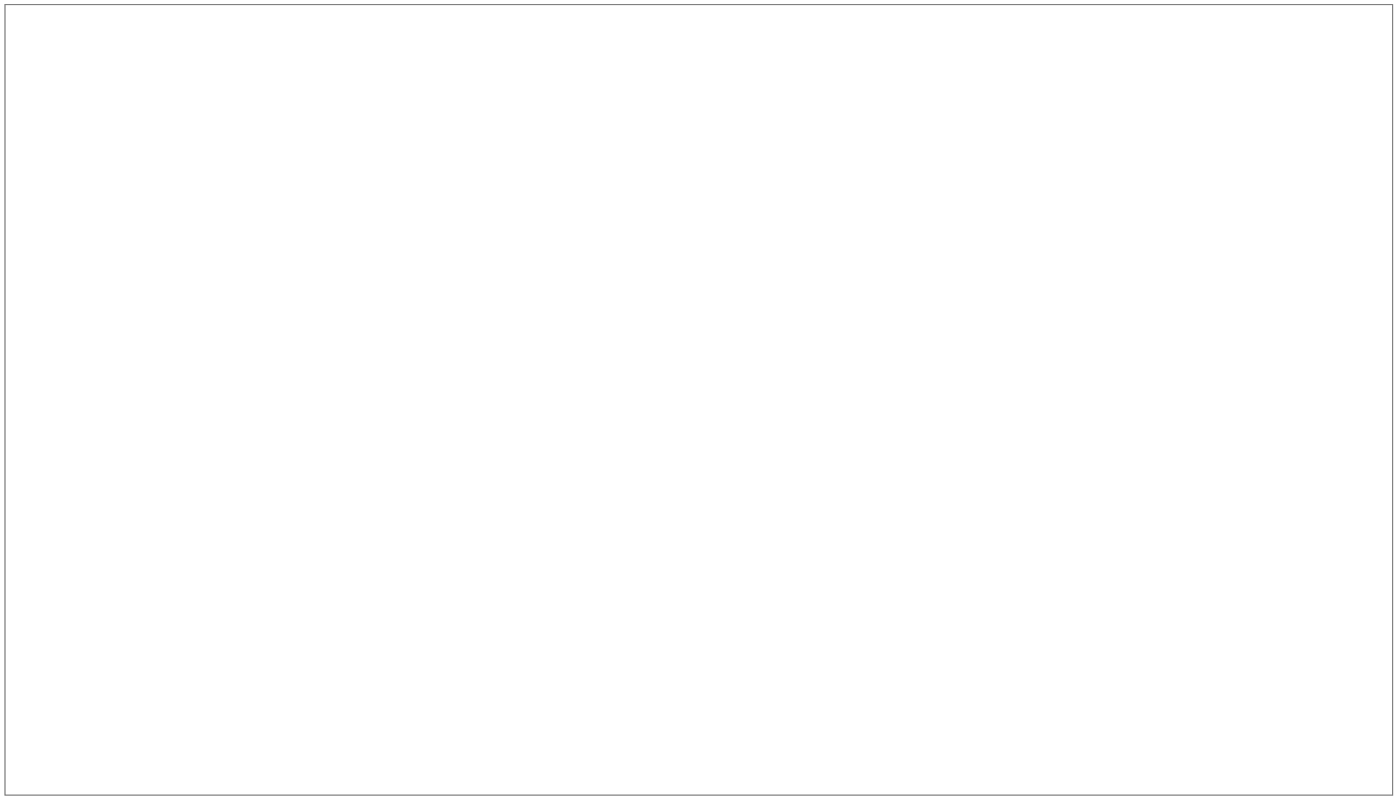
...

Ahora es el momento de ocuparse de las conexiones P2P. Marcamos aquí las dos primeras casillas, la de habilitar un tráfico menor para las aplicaciones P2P (Enable) y la de considerar P2P todo aquello que no esté previsto (p2pCatchAll):



Le damos a Next para continuar ..

La siguiente pantalla del asistente permite otorgar tráfico prioritario a varios juegos. Hacemos Next de nuevo ...



Ahora se nos pedirá si deseamos activar el control de prioridades para el resto de tráfico. Lo activamos, con lo que todos los tipos de tráfico configurables (en esta ventana) tomarán la prioridad por defecto (Default priority). Una vez hecho esto le damos de nuevo a

...

Raise or lower other Applications

pfSense Traffic Shaper Wizard	
Enable:	☑ Other networking protocols This will help raise or lower the priority of other protocols higher than most traffic.

Next

Remote Service / Terminal emulation	
MSRDP:	Default priority Microsoft Remote Desktop Protocol
VNC:	Default priority Virtual Network Computing
AppleRemoteDesktop:	Default priority Apple Remote Desktop
PCAnywhere:	Default priority Symantec PC Anywhere

Messengers	
IRC:	Default priority Internet Relay Chat
Jabber:	Default priority Jabber instant messanger
ICQ:	Default priority ICQ
AIM:	Default priority AOL Instant Messenger
MSN:	Default priority MSN Messenger
Teamspeak:	Default priority TeamSpeak

VPN	
PPTP:	Default priority Microsoft Point to Point tunneling protocol

IPSEC:	Default priority IPSEC VPN traffic

Multimedia/Streaming	
StreamingMP3:	Default priority Streaming Media
RTSP:	Default priority RealTime streaming protocol

Web	
HTTP:	Default priority HTTP and HTTPS aka Web Traffic

Mail	
SMTP:	Default priority Mail Protocol
POP3:	Default priority POP3 Protocol
IMAP:	Default priority IMAP Protocol
LotusNotes:	Default priority Lotus Notes

Miscellaneous	
DNS:	Default priority Domain Name Services
ICMP:	Default priority ICMP Protocol
SMB:	Default priority Microsoft SMB Protocol and friends
SNMP:	Default priority Simple Network Management Protocol
MySQLServer:	Default priority MySQL Server
NNTP:	Default priority Internet News
CVSUP:	Default priority CVSUP

Next

Y tendremos la pantalla final del asistente ...

Aquí se dice simplemente que la activación de las colas afectará sólo a las nuevas conexiones y que si se quiere que se aplique a todas habrá que reiniciar la tabla de estados (con posible pérdida de conexiones), yendo a [Diagnostics] [States] [Reset States].

Una vez hayamos hecho clic en el botón Finish veremos cómo se recargan las reglas (ahora hay muchas y toman su tiempo):

Y cuando termina se ofrece la posibilidad de ir directamente a ver el estado de las colas creadas (Queue Status):

Colas creadas por el asistente

El asistente habrá creado las siguientes colas, con los siguientes caudales, prioridades y curvas de tráfico:

Colas-hijas de **qwanRoot** (Cola-madre de WAN)		Colas-hijas de **qAlumnesRoot** (Cola-madre de Alumnes)

	Caudal	Prioridad	Curva			Caudal	Prioridad	Curva
qwandef es la cola por defecto (la mayoría del tráfico).	**1 %**	**1** 1%			**qAlumnesdef** es la cola por defecto (la mayoría del tráfico).	**1 %**	**1** 1%	
qwanacks es la cola de acuse de recibo (ACK). No puede haber pérdidas (drops), ya que ello cortaría/ralentizaría las conexiones.	**25 %**	**7** 10%			**qAlumnesacks** es la cola de acuse de recibo (ACK). No puede haber pérdidas (drops), ya que ello cortaría/ralentizaría las conexiones.	**25 %**	**7** 10%	
qP2PUp es la cola de subida a Internet empleando aplicaciones P2P (Emule, Ares, ...)	**1 %**	**1** 1kb			**qP2PDown** es la cola de bajada de Internet empleando aplicaciones P2P (Emule, Ares, ...)	**1 %**	**1** 1kb	
qOthersUpH es la cola de otras subidas a Internet con prioridad alta (High). **¡No la necesitamos!**	**25 %**	**4** 1kb			**qOthersDownH** es la cola de otras bajadas de Internet con prioridad alta (High). **¡No la necesitamos!**	**25 %**	**4** 1kb	
qOthersUpL es la cola de otras subidas a Internet con prioridad baja (Low). **¡No la necesitamos!**	**1 %**	**2** 1kb			**qOthersDownL** es la cola de otras bajadas de Internet con prioridad baja (Low). **¡No la necesitamos!**	**1 %**	**2** 1kb	

Podremos ver con más detalle qué ha hecho el asistente yendo a [Firewall][Trafic Shaper] y mirando:

- [Queues], que son las colas creadas.
- [Rules], que son las reglas que determinan a qué cola va a parar un determinado tipo de tráfico.

Observemos que las colas qOthers no las necesitamos porqué hemos dejado todos los protocolos que no son P2P en Default priority, con lo que van todos por qwandef y qAlumnesdef.

Ajuste del regulador de caudal

Yendo a [Status][Queues] del cortafuegos podremos ver gráficos en tiempo real (pfSense utiliza RRDtool como herramienta estadística) y estadísticas que nos dicen:

- **pps**, paquetes por segundo.
- **b/s** o **kb/s** (bits por segundo o quilobits por segundo).
- **borrows**, paquetes (ancho de banda) tomados de la cola-madre. No aplicable en nuestro caso, ya que sólo existe una madre para todas las colas de subida o de bajada.
- **suspends**, paquetes cancelados (¿?). No he visto ninguno aún y no sé demasiado que son. No he encontrado una documentación clara sobre este aspecto.
- **drops**, paquetes descartados. Es lo que interesa que haya en las colas de menos prioridad y que no debe estar nunca en las colas ACK.

Status: Traffic shaper: Queues

Queue	Statistics			
qwanRoot 0/pps	0 b/s	0 borrows	0 suspends	0 drops
qwandef 4/pps	6.57Kb/s	0 borrows	0 suspends	13 drops
qwanacks 50/pps	22.21Kb/s	0 borrows	0 suspends	0 drops
qP2PUp 1/pps	752 b/s	0 borrows	0 suspends	2226 drops
qAlumnesRoot 0/pps	0 b/s	0 borrows	0 suspends	0 drops
qAlumnesdef 93/pps	475.74Kb/s	0 borrows	0 suspends	84 drops
qAlumnesacks 6/pps	2.90Kb/s	0 borrows	0 suspends	0 drops
qP2PDown 0/pps	2.39Kb/s	0 borrows	0 suspends	207 drops

Note:
Queue graphs take 5 seconds to sample data.

Yendo a [Firewall] [Traffic Shaper] [Queues] dejamos las colas de la siguiente forma, después de bastantes pruebas:

Colas-hijas de **qwanRoot** (Cola-madre de WAN)					Colas-hijas de **qAlumnesRoot** (Cola-madre de Alumnes)			
	Caudal	Prioridad	Curva			Caudal	Prioridad	Curva
qwandef	**79 %**	**3** (35%)			**qAlumnesdef**	**84 %**	**3** (60%)	
qwanacks	**20 %**	**7** (10%)			**qAlumnesacks**	**15 %**	**7** (10%)	
qP2PUp	**1 kb/s**	**1** (1kb, 5000, 1kb)			**qP2PDown**	**1 kb/s**	**1** (1kb, 5000, 1kb)	

Los cambios hechos son suficientes para garantizar que no hay pérdidas de paquetes en ninguna cola, salvo en las de P2P, que es lo que nos interesa.

La otra solución para controlar los accesos P2P

La otra solución para evitar las conexiones P2P es adoptar reglas de cortafuegos y no usar ALTQ.

Para hacer esto desactivaremos **Traffic Shaper** en [Firewall][Traffic Shaper] y definiremos primero los siguientes alias:

internetTCP	80, 443, 21, 53, 119	HTTP, HTTPS, FTP, DNS, NNTP
internetUDP	53, 119	DNS, NNTP

Y a continuación, en la interfase de Alumnes, donde nuestra última regla es:

19	*	Alumnes net	*	*	*	192.168.AAA.1	*** Alumnes -> Internet ***

cambiaremos esta regla por las siguientes:

	TCP	Alumnes net	*	*	internetTCP	192.168.AAA.1	*** Alumnes -> Internet ***
	TCP	Alumnes net	*	*	8000 - 8100	192.168.AAA.1	*** Alumnes -> Internet ***
	UDP	Alumnes net	*	*	internetUDP	192.168.AAA.1	*** Alumnes -> Internet ***
	ICMP	Alumnes net	*	*	*	192.168.AAA.1	*** Alumnes -> Internet ***

Con esto autorizaremos sólo la navegación por Internet, FTP, la actualización de la fecha/hora de los ordenadores de la red y las herramientas ICMP (PING y otras). Los puertos de 8000 a 8100 son empleados normalmente para streaming (audio y/o vídeo) o como puertos alternativos en servidores web.

Evidentemente esta solución es más segura que emplear ALTQ pero también es mucho más restrictiva.

OpenVPN (Virtual Private Network)

pfSense incorpora el paquete OpenVPN que permite crear redes privadas virtuales (VPN).

Con OpenVPN podremos extender nuestra red a cualquier lugar del mundo, haciendo que la identificación y la comunicación sean

seguras.

Antes de tener pfSense el administrador de la red se conectaba al escritorio de uno de los servidores Windows de su red por RDP, desde una IP fija. Al usar una IP fija se podía controlar con las reglas de uno de los routers ADSL el acceso a este servicio.

Ahora, con OpenVPN el administrador entra directamente en la red local, sin necesidad de que ningún ordenador le haga de puente. Y lo hace desde una IP dinámica, autentificándose en base a certificados SSL.

Instalación de OpenVPN en Windows XP

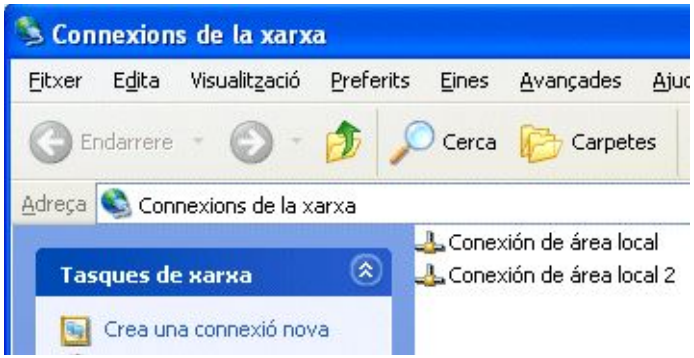
El OpenVPN para Windows es incompatible con la mayoría de cortafuegos de terceros para Windows XP SP2. Para más información mira la página openvpn.se/xpsp2_problem.html. En nuestro caso empleamos Panda Antivirus, por lo que tendremos que instalar la versión sin cortafuegos y, en todo caso, dejar activado el cortafuegos propio de Windows XP. Hay que hacer estos cambios antes de hacer la instalación de OpenVPN para Windows.

Descargamos de openvpn.se la última versión de OpenVPN para Windows (es de código libre) con el driver TAP de tarjeta de red virtual incluido:

http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

Instalamos la aplicación con sus opciones por defecto.

Vamos ahora a nuestras conexiones de red, donde encontraremos una nueva tarjeta de red:



Le cambiamos el nombre que tiene por defecto, por el de TUN (podemos aprovechar también para ponerle, a la tarjeta real, el nombre de LAN):

Vamos a la carpeta C:\Archivos de programa\OpenVPN\config y creamos un archivo de texto que se diga **dominio.ejemplo.ovpn** con el siguiente contenido (siendo RRR.RRR.RRR.RRR la IP pública del sitio al que queremos connectarnos):

```
float
port 1194
dev tun
dev-node TAP
proto tcp-client
remote RRR.RRR.RRR.RRR 1194
ping 10
persist-tun
persist-key
```

```
tls-client
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
#comp-lzo
pull
verb 4
```

La línea comp-lzo está comentada (símbolo #) para poder hacer las primeras pruebas sin compresión en las comunicaciones.

Ahora, para podernos conectar sólo nos queda la generación de los certificados y llaves SSL.

Generación de llaves y certificados (entidad certificadora, servidor y cliente)

En un ordenador Windows que tengamos instalado OpenVPN y que sea de acceso seguro ...

Abrimos una ventana de órdenes MS-DOS ([Inicio] [Ejecutar ...] cmd) y tecleamos:

cd "c:\Archivos de programa\OpenVPN\easy-rsa"
init-config
edit vars.bat

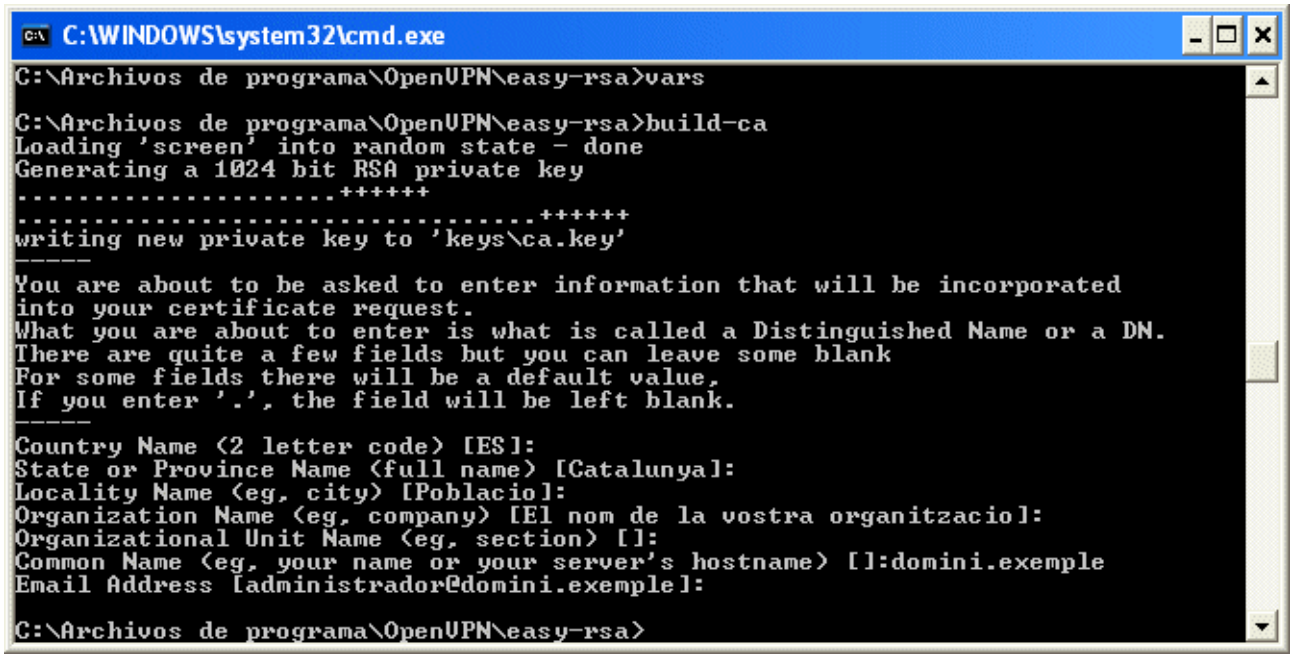
Editamos ahora vars.bat, poniendo nuestros datos en las últimas líneas:

```
set KEY_COUNTRY=ES
set KEY_PROVINCE=Provincia
set KEY_CITY=Población
set KEY_ORG=El nombre de vuestra organización
set KEY_EMAIL=administrador@dominio.ejemplo
```

De nuevo en el intérprete de órdenes MS-DOS, hacemos:

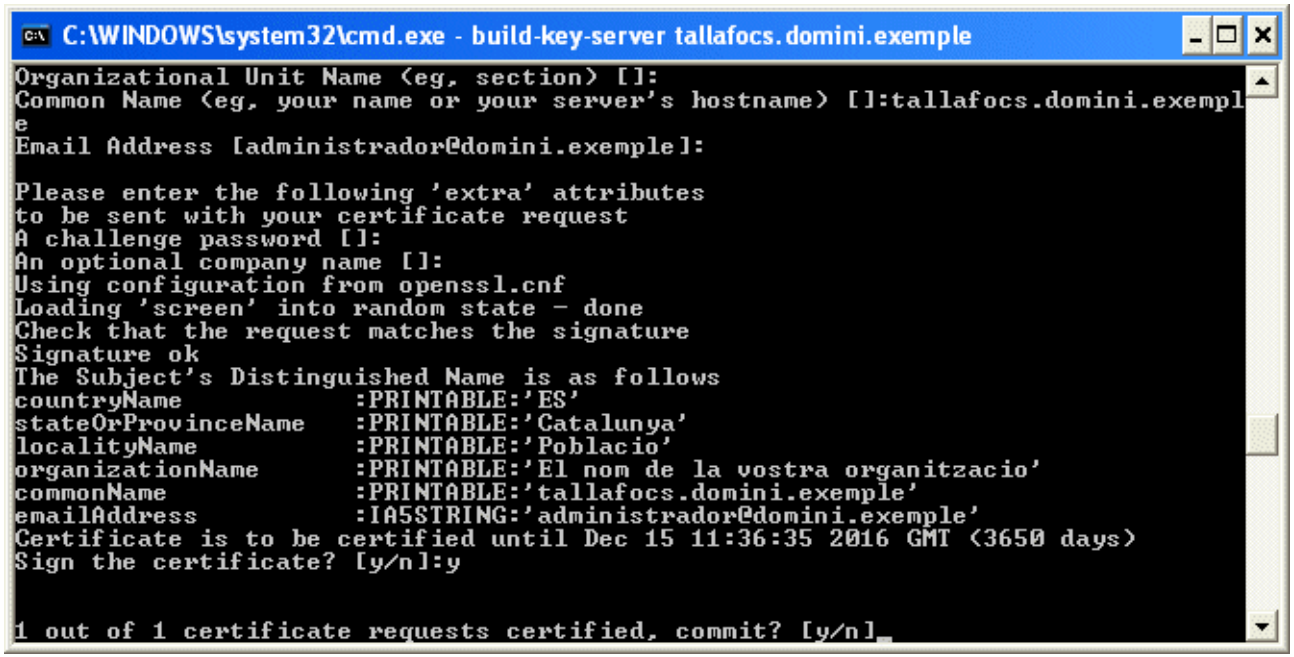
vars
clean-all
build-ca

Se nos presentarán los datos por defecto, los cuales sólo tendremos que confirmar. En el nombre del servidor tendremos que poner **dominio.ejemplo** ya que este proceso nos generará **ca.key** (llave privada de la entidad certificadora, para el servidor) y **ca.crt** (certificado-raíz de la entidad certificadora, para el servidor y para todos los clientes):



build-key-server server

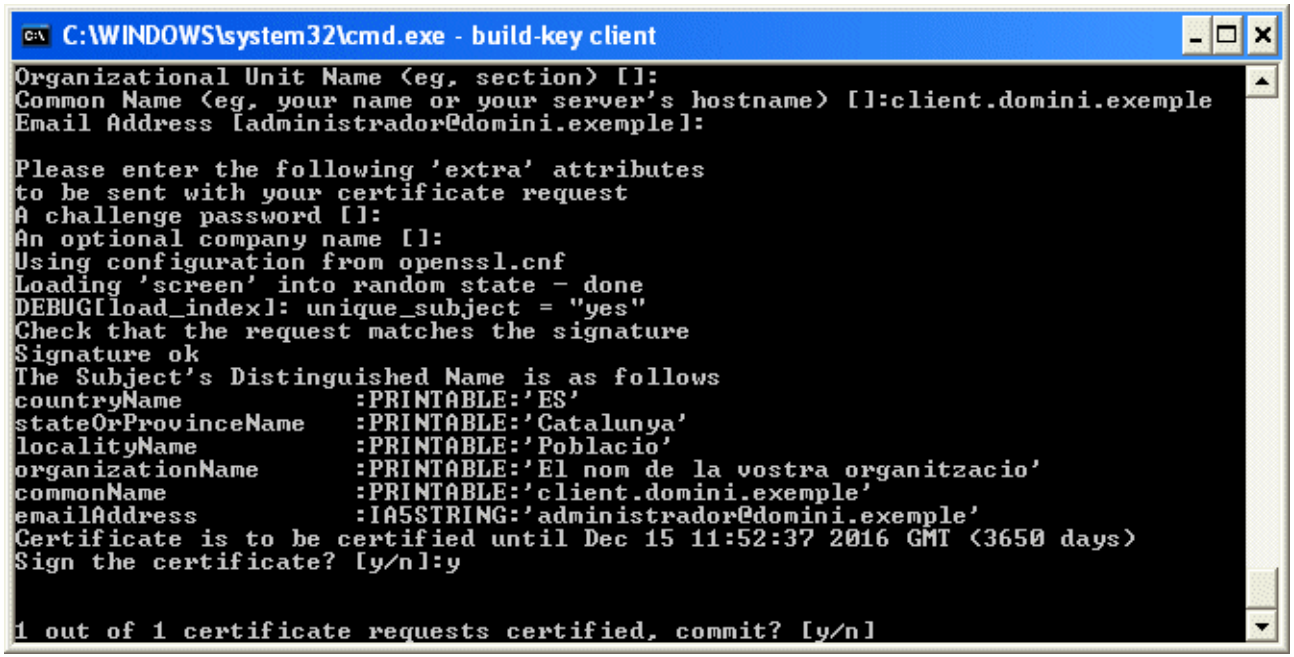
Este proceso genera la llave privada y el certificado (**server.key** i **server.crt**) para un servidor OpenVPN. Aquí tendremos que indicar **cortafuegos.dominio.ejemplo** como nombre de nuestra máquina:



A las dos preguntas finales de confirmación sólo tenemos que contestar mediante **y** (yes).

build-key client

Este proceso genera la llave privada y el certificado (**client.key** i **client.crt**) para un cliente OpenVPN. Indicamos como nombre de máquina **cliente.dominio.ejemplo**:

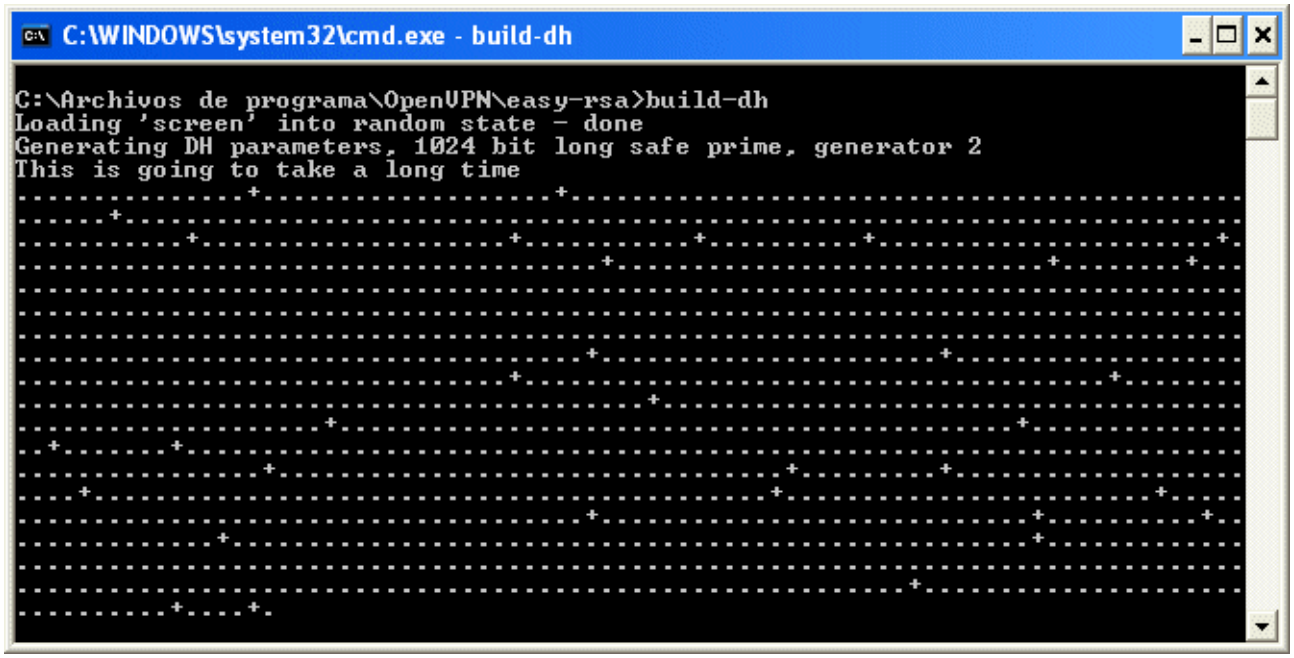


A las dos preguntas finales de confirmación sólo tenemos que contestar por **y** (yes).

En caso de conectar más de un cliente cada uno de ellos tiene que tener su propia llave y certificado de cliente. Los certificados de cliente pueden ser revocados y de esta manera un cliente deja de estar autorizado para conectarse.

build-dh

Como paso final tenemos que generar los parámetros Diffie Helman para nuestro servidor OpenVPN, lo que requiere un cierto tiempo de máquina:



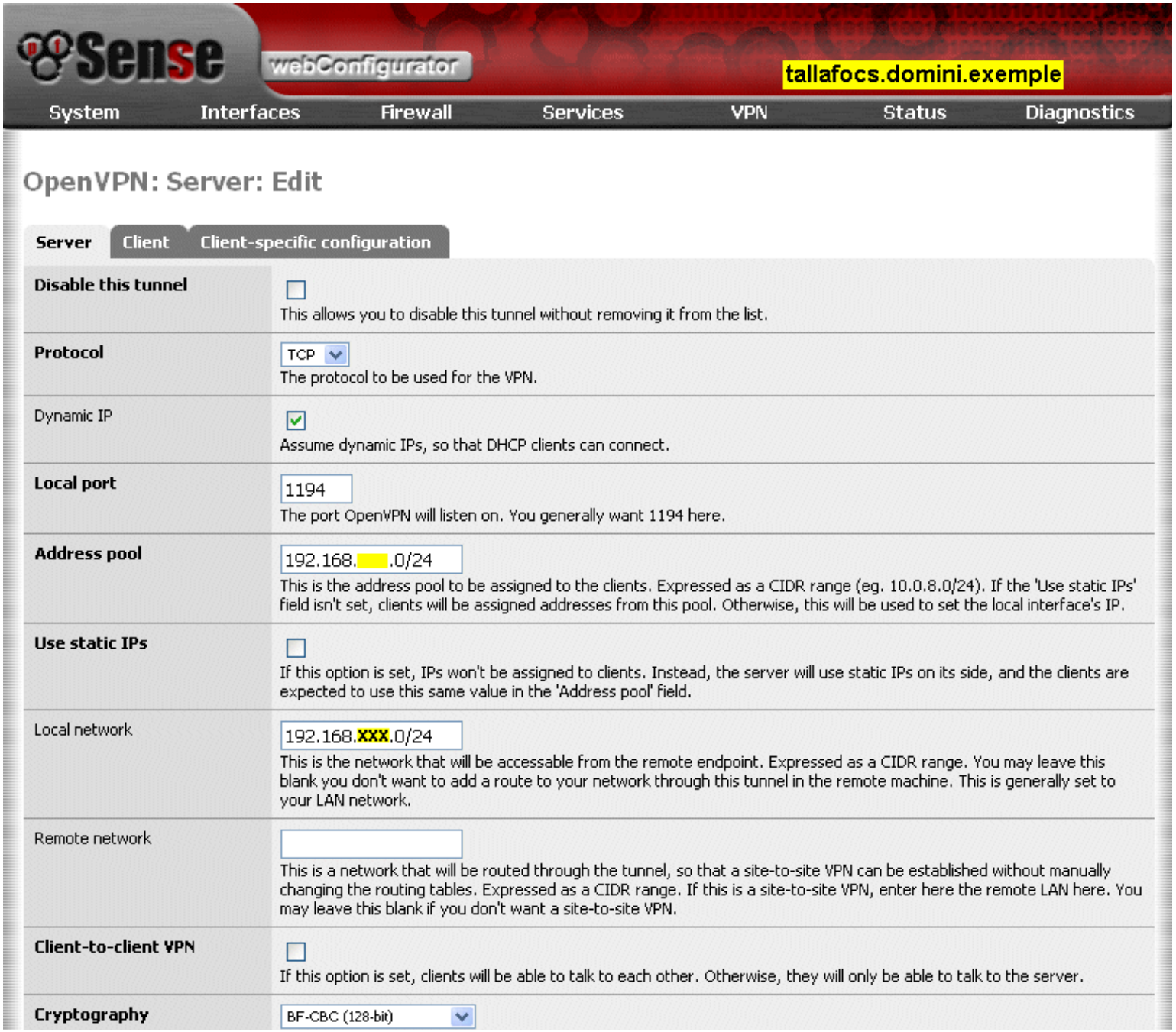
Obtendremos con ello un archivo para el servidor llamado **dh1024.pem**.

Instalación de la llave y de los certificados en el cliente Windows XP

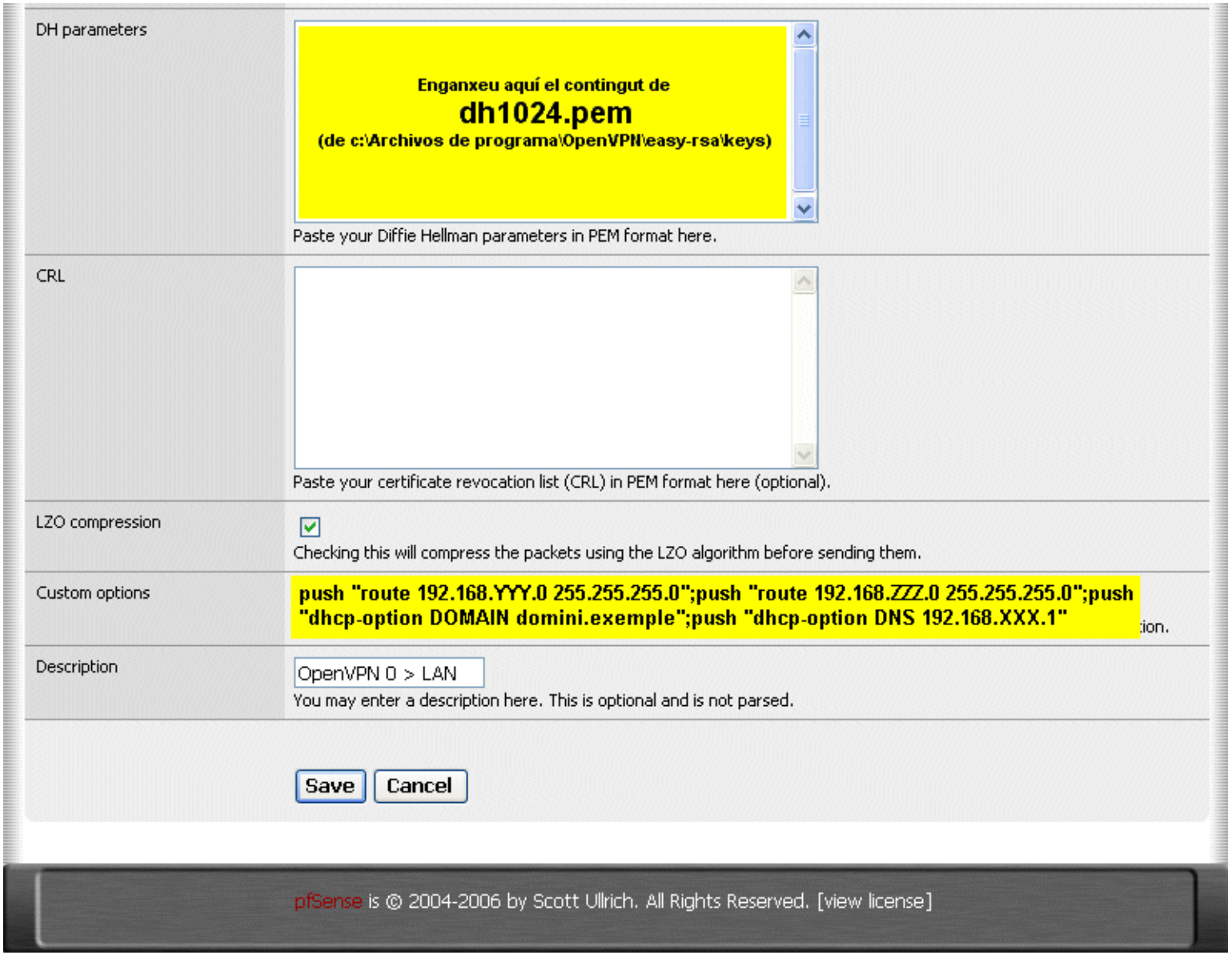
Copiamos los archivos **ca.crt**, **client.key** i **client.crt** que tenemos en c:\Archivos de programa\OpenVPN\easy-rsa\keys (generados en el apartado anterior) a c:\Archivos de programa\OpenVPN\config del ordenador cliente.

Configuración de OpenVPN en pfSense

Vamos a [VPN] [OpenVPN] [Servers] y añadimos un servidor VPN ...


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
OpenVPN: Server: Edit
Server
Client
Client-specific configuration
Disable this tunnel
This allows you to disable this tunnel without removing it from the list.
Protocol
TCP
The protocol to be used for the VPN.
Dynamic IP
Assume dynamic IPs, so that DHCP clients can connect.
Local port
1194
The port OpenVPN will listen on. You generally want 1194 here.
Address pool
192.168.[redacted].0/24
This is the address pool to be assigned to the clients. Expressed as a CIDR range (eg. 10.0.8.0/24). If the 'Use static IPs' field isn't set, clients will be assigned addresses from this pool. Otherwise, this will be used to set the local interface's IP.
Use static IPs
If this option is set, IPs won't be assigned to clients. Instead, the server will use static IPs on its side, and the clients are expected to use this same value in the 'Address pool' field.
Local network
192.168.XXX.0/24
This is the network that will be accessable from the remote endpoint. Expressed as a CIDR range. You may leave this blank you don't want to add a route to your network through this tunnel in the remote machine. This is generally set to your LAN network.
Remote network
This is a network that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a CIDR range. If this is a site-to-site VPN, enter here the remote LAN here. You may leave this blank if you don't want a site-to-site VPN.
Client-to-client VPN
If this option is set, clients will be able to talk to each other. Otherwise, they will only be able to talk to the server.
Cryptography
BF-CBC (128-bit)

	Here you can choose the cryptography algorithm to be used.
Authentication method	PKI (Public Key Infrastructure) The authentication method to be used.
Shared key	Paste your shared key here.
CA certificate	**Enganxeu aquí el contingut de** **ca.crt** **(de c:\Archivos de programa\OpenVPN\easy-rsa\keys)** Paste your CA certificate in X.509 format here.
Server certificate	**Enganxeu aquí el contingut de** **server.crt** **(de c:\Archivos de programa\OpenVPN\easy-rsa\keys)** Paste your server certificate in X.509 format here.
Server key	**Enganxeu aquí el contingut de** **server.key** **(de c:\Archivos de programa\OpenVPN\easy-rsa\keys)** Paste your server key in RSA format here.



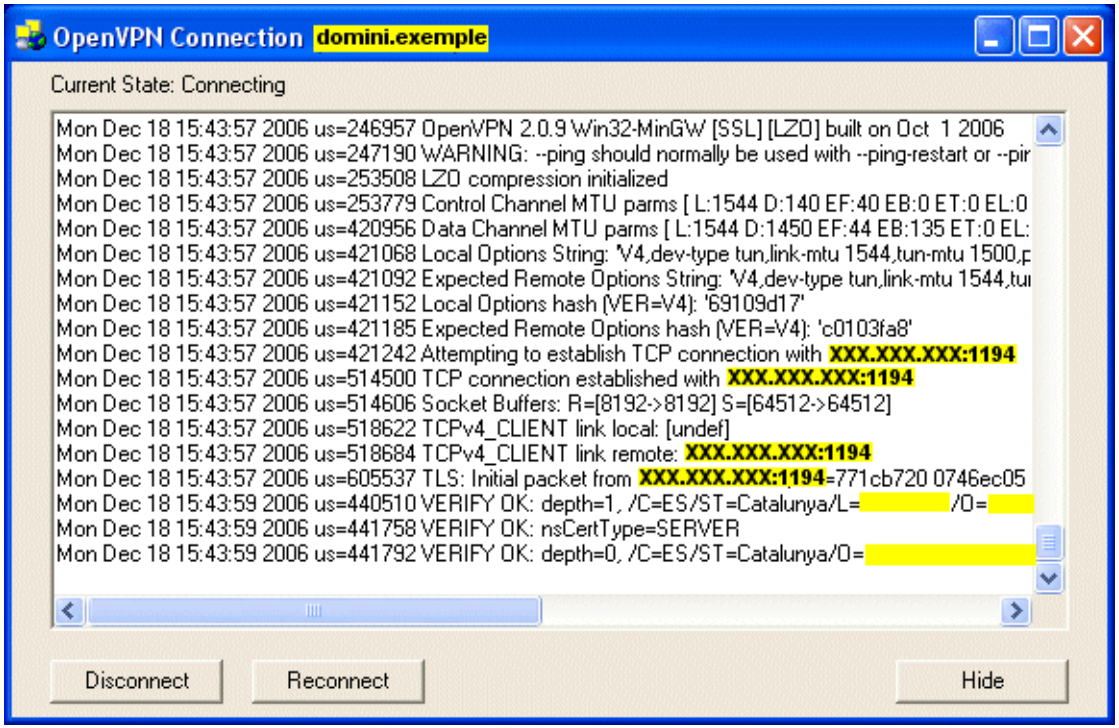
En **Address pool** tendremos que poner una red que no coincida con ninguna de las que tenemos (AAA, BBB, CCC, XXX, YYY, ZZZ).

Es recomendable probar primero la conexión sin compresión LZO (LZO compression) y después la activamos, tanto a nivel cliente como a nivel servidor.

Conectando ...

Ya está todo a punto para la primera conexión. En la barra de tarea tenemos dos nuevos iconos, el de OpenVPN GUI (interfase gráfica) y el de TAP, que nos dice que está desconectada:

Si hacemos doble clic sobre el icono de OpenVPN GUI veremos una ventana como la siguiente:



donde se nos informa de los pasos que hace la conexión. Si todo ha ido bien, esta ventana se cerrará y veremos que el icono de TAP cambia:

Con ello estaremos en nuestra red gestionada por pfSense como una máquina más ... Probamos si podemos acceder pues a recursos que estén en las redes 192.168.XXX.0, 192.168.YYY.0 y 192.168.ZZZ.0. Por ejemplo, a la propia administración web de pfSense.

Recordad que si hemos hecho las primeras pruebas sin compresión LZO hay que activarla, tanto en el servidor como en el cliente (ya comentado anteriormente).

Conexión automática

Si deseamos que cuando se ponga en marcha nuestro cliente Windows se realice la conexión de forma automática, tendremos que seguir los siguientes pasos:

Eliminamos del registro de Windows el arranque de OpenVPN GUI

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"openvpn-gui"="C:\\Archivos de programa\\OpenVPN\\bin\\openvpn-gui.exe"
```

Vamos al [Panel de Control] [Herramientas Administrativas] [Servicios] y buscamos OpenVPN Service. Veremos que está en modo manual. Lo ponemos en Automático y con OpenVPN GUI ya parado, ponemos en marcha el servicio.

Veremos como al cabo de unos segundos nuestra tarjeta TAP ya tiene conexión, de forma silenciosa.

OpenVPN sin DHCP

Al cabo de un mes de funcionar, la conexión empezó a fallar ocasionalmente, sin motivo aparente. A veces reiniciando el ordenador se arreglaba el error de conexión. Finalmente se desechó la conexión automática, volviendo a OpenVPN GUI, hasta que volvieron a aparecer fallos. Al final pareció que el problema era la velocidad de conexión entre las dos ADSL, por lo que se pasó a configurar OpenVPN sin asignación automática de direcciones IP (DHCP).

Por ello se ha confeccionado una página específica (en este tutorial) sobre cómo configurar [OpenVPN sin DHCP] ...

Problemas de estabilidad

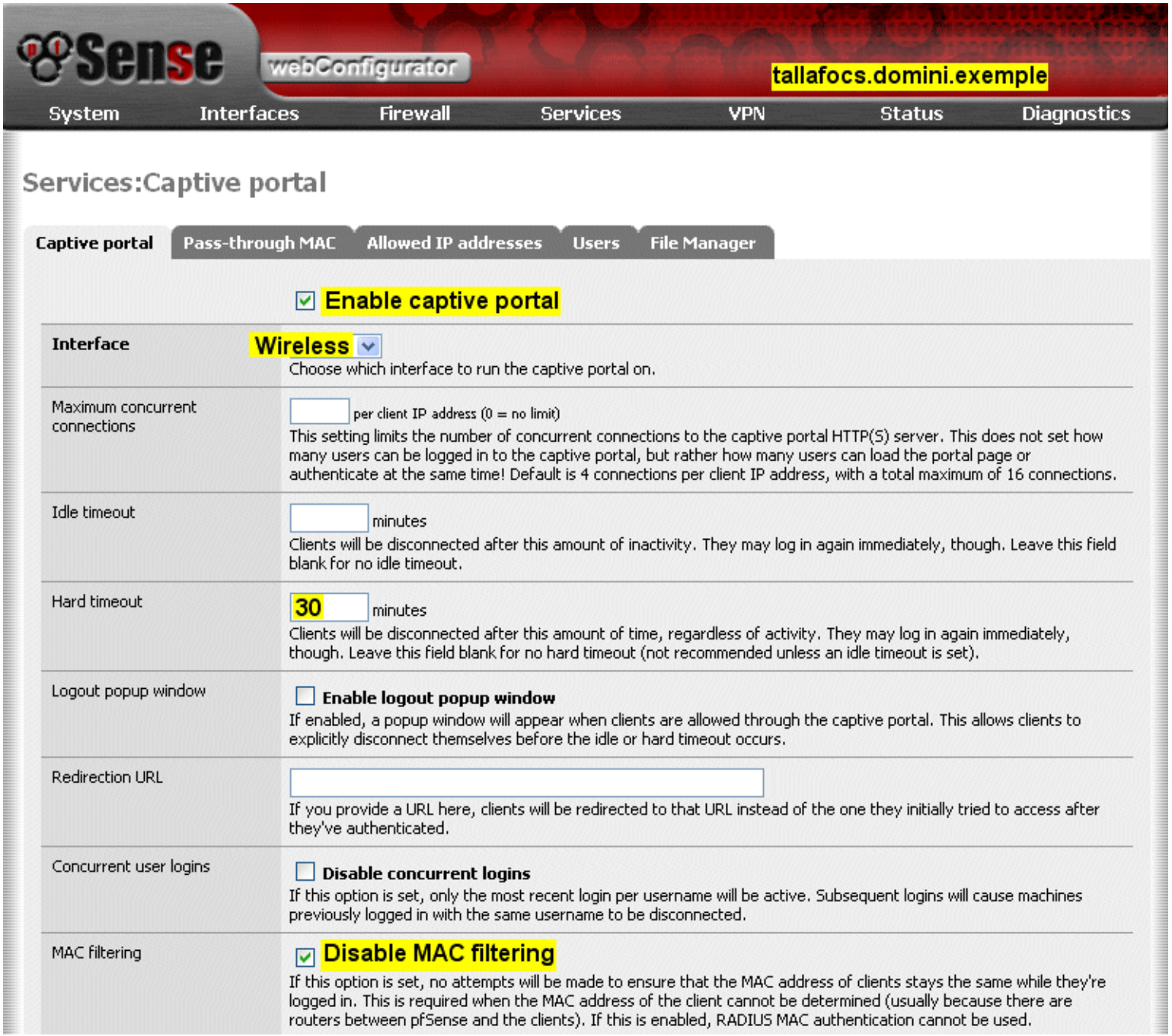
A pesar de haber dejado OpenVPN sin DHCP (véase el apartado anterior), seguí teniendo problemas con la conexión. Los desarrolladores de pfSense me recomendaron migrar a la última versión parcheada de pfSense. El 25-abril-2007 migré el cortafuegos a la versión 1.2 BETA de pfSense y desde entonces funciona sin problemas.

Portal cautivo

Yendo a [Services] [Captive portal] podemos configurar la forma en que los usuarios de una red entran a navegar por Internet. A esta prestación se le llama portal cautivo.

El portal cautivo admite desde sencillas configuraciones donde sólo aparece una página de información al usuario hasta distintos sistemas de validación.

Se muestra aquí cómo habilitar el portal cautivo para la red sin hilos (wireless) con una página de información al usuario, sin autentificación y con un tiempo máximo de conexión de 30 minutos.


pfSense
webConfigurator
tallafocs.domini.exemple
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Services:Captive portal
Captive portal
Pass-through MAC
Allowed IP addresses
Users
File Manager
Enable captive portal
Interface
Wireless
Choose which interface to run the captive portal on.
Maximum concurrent connections
per client IP address (0 = no limit)
This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.
Idle timeout
minutes
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout
30
minutes
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Logout popup window
Enable logout popup window
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Redirection URL
If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.
Concurrent user logins
Disable concurrent logins
If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.
MAC filtering
Disable MAC filtering
If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Authentication

- (•) **No authentication**
- ( ) Local user manager
- ( ) RADIUS authentication

Primary RADIUS server

IP address	Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.
Port	Leave this field blank to use the default port (1812).
Shared secret	Leave this field blank to not use a RADIUS shared secret (not recommended).

Secondary RADIUS server

IP address	If you have a second RADIUS server, you can activate it by entering its IP address here.
Port	
Shared secret	

Accounting

	[ ] **send RADIUS accounting packets** If this is enabled, RADIUS accounting packets will be sent to the primary RADIUS server.
Accounting port	Leave blank to use the default port (1813).

Reauthentication

	[ ] **Reauthenticate connected users every minute** If reauthentication is enabled, Access-Requests will be sent to the RADIUS server for each user that is logged in every minute. If an Access-Reject is received for a user, that user is disconnected from the captive portal immediately.
Accounting updates	(•) no accounting updates ( ) stop/start accounting ( ) interim update

RADIUS MAC authentication

Enable RADIUS MAC authentication
If this option is enabled, the captive portal will try to authenticate users by sending their MAC address as the username and the password entered below to the RADIUS server.

Shared secret

RADIUS options

Type: default
If RADIUS type is set to Cisco, in Access-Requests the value of Calling-Station-Id will be set to the client's IP address and the Called-Station-Id to the client's MAC address. Default behaviour is Calling-Station-Id = client's MAC address and Called-Station-Id = pfSense's WAN IP address.

HTTPS login

Enable HTTPS login
If enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name, certificate and matching private key must also be specified below.

HTTPS server name

This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS.

HTTPS certificate

Paste a signed certificate in X.509 PEM format here.

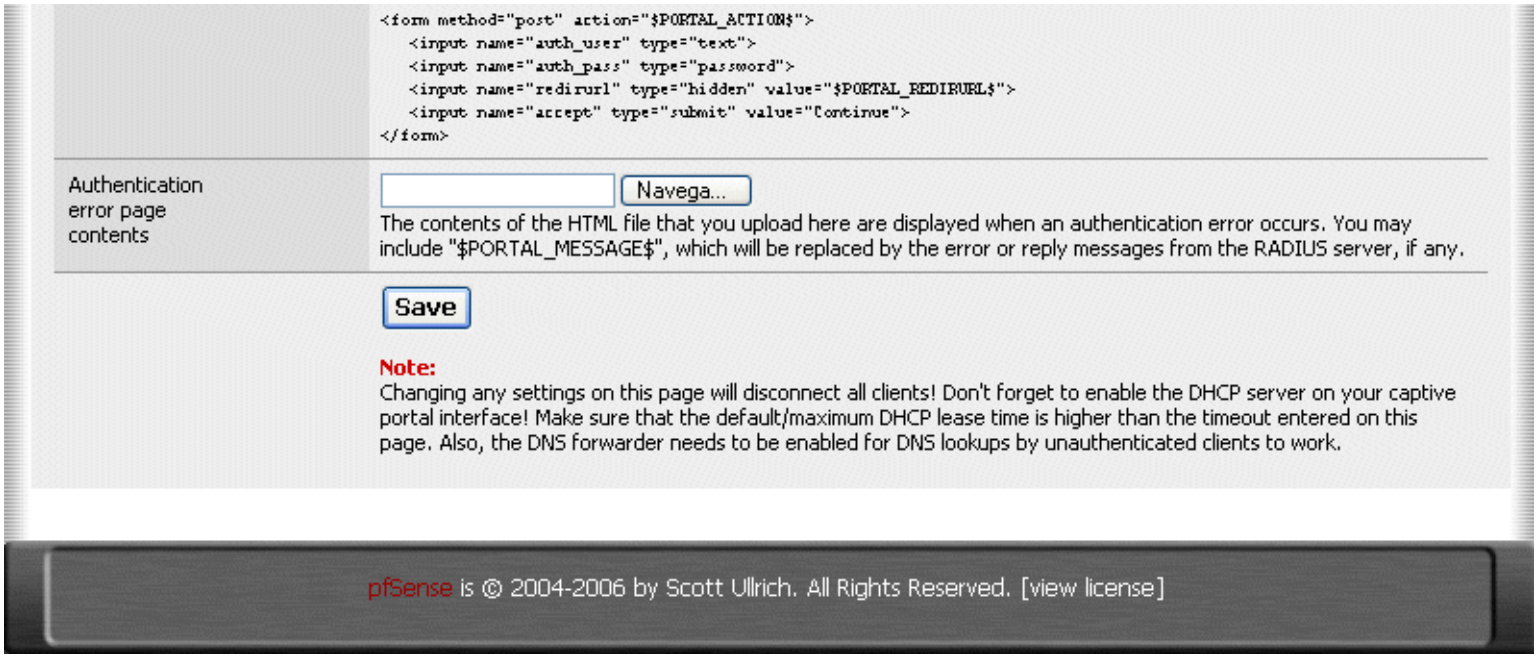
HTTPS private key

Paste an RSA private key in PEM format here.

Portal page contents

Navega...
View current page

Upload an HTML file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "$PORTAL_ACTION$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="$PORTAL_REDIRURL$". Include the "auth_user" and "auth_pass" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:

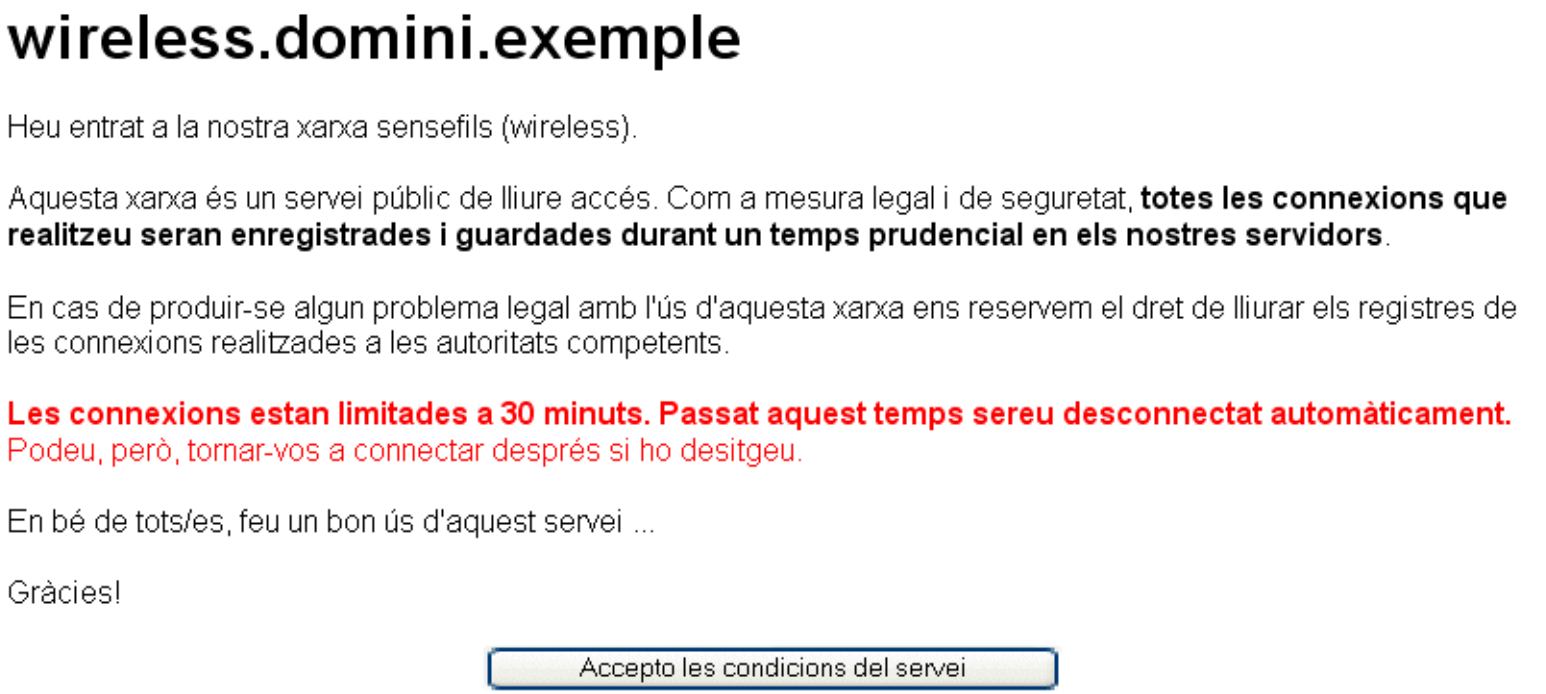


El código HTML cargado en **Portal page contents** es:

```
<html>

<head>
<title>wireless.dominio.ejemplo</title>
</head>

<body>

<h1><font face="Arial">wireless.dominio.ejemplo</font></h1>

<p><font face="Arial">Has entrado en nuestra red sin hilos (wireless).</font></p>

<p><font face="Arial">Esta red es un servicio público de libre acceso. Como medida legal y de seguridad, <b>todas las conexiones que realices serán registradas y guardadas durante un tiempo prudencial en nuestros servidores</b>.</font></p>
```

```
<p><font face="Arial">En caso de producirse algún problema legal con el uso de esta red nos
reservamos el derecho de entregar los registros de las conexiones realizadas a las autoridades
competentes.</font></p>

<p><font face="Arial"><b><font color="#FF0000">Las conexiones están limitadas a 30 minutos. Pasado
este tiempo serás desconectado automáticamente.</b> Puedes, no obstante, volver a conectarte después
si lo deseas.</font></p>

<p><font face="Arial">En bien de todos/as, haz un buen uso de este servicio ...</font></p>

<p><font face="Arial">¡Gracias!</font></p>

<form method="post" action="$PORTAL_ACTION$">
<p align="center"><font face="Arial">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="accept" type="submit" value="Acepto las condiciones del servicio">
</font>
</form>

</body>

</html>
```

es decir, que lo que ve el usuario cuando entra por primera vez a su navegador es:



OpenVPN sin DHCP

Para poder comprender bien lo que se explica en esta página hay que estar al corriente de lo explicado en [OpenVPN] ...

Cuando las comunicaciones son un tanto difíciles conviene sacarle trabajo al servidor OpenVPN que incorpora pfSense. Se trata por tanto de que el cliente se conecte empleando una dirección estática y, mejor aún, estableciendo él mismo las rutas, el servidor DNS, el servidor WINS (si hace falta), etc.

¿Y cómo le decimos los DNS? ¿Y los WINS?

Cambios en la configuración del cliente Windows XP

Modificamos nuestro archivo **dominio.ejemplo.ovpn** de la carpeta C:\Archivos de programa\OpenVPN\config dejándolo de la siguiente forma:

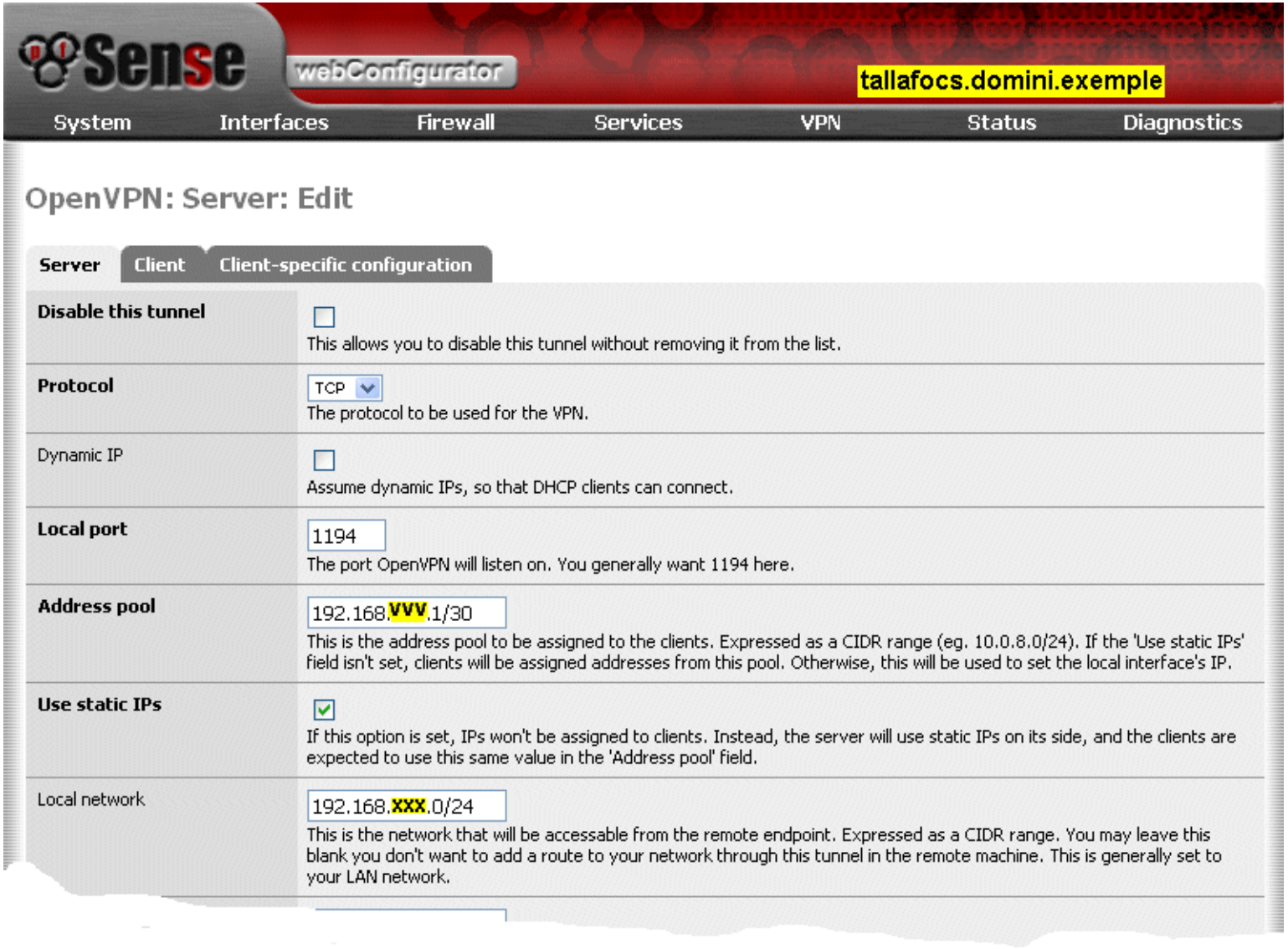
```
dev tun
dev-node TAP
proto tcp-client
nobind

ifconfig 192.168.VVV.2 192.168.VVV.1
route 192.168.XXX.0 255.255.255.0
route 192.168.YYY.0 255.255.255.0
route 192.168.ZZZ.0 255.255.255.0

remote RRR.RRR.RRR.RRR 1194
keepalive 10 60

tls-client
ca ca.crt
cert client.crt
key client.key
ns-cert-type server

comp-lzo

verb 4
```

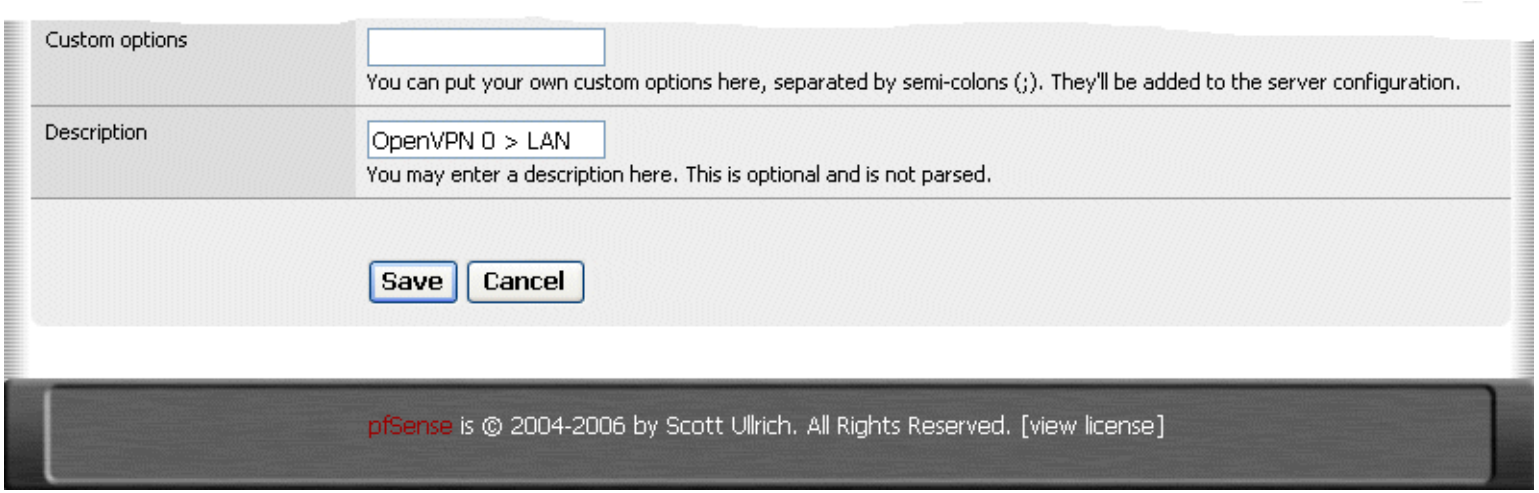
Siendo 192.168.VVV.0/30 la VPN que sólo contendrá la IP del servidor (VVV.1) y la del cliente (VVV.2) que emplea el administrador de las redes.

El uso de **tls-client** en lugar de **client** (que implica **pull** y **tls-client**) hace que el servidor no transmita ninguna orden de cómo configurarse al cliente (no pull). Por tanto, el servidor no enviará ni la ruta para la red 192.168.XXX.0/24 y habrá que ponerla en la configuración. Per a más detalles visítese http://openvpn.net/man.html.

Cambios en la configuración del servidor OpenVPN

En el lado del servidor habrá que ...





Obsérvese que:

- Hemos deshabilitado la casilla [Dynamic IP].
- Que el cajetín [Address pool] contiene la IP del servidor OpenVPN que definimos, que a su vez es la puerta de enlace de la interfase TAP de nuestro cliente Windows.
- Que activamos la casilla [Use static IPs].
- Que el cajetín [Local network] no debe servir para nada. No lo tocamos ...
- Que el cajetín [Custom options] no contiene nada.

Desgraciadamente parece que hay un error en la versión 1.0.1 de pfSense y el servidor OpenVPN no se reinicia de forma limpia, por lo que habrá que reiniciar todo el cortafuegos una vez cambiada la configuración.

¿Y cómo le decimos los DNS? ¿Y los WINS?

Resulta que el cliente Windows de OpenVPN no tiene forma de configurar servidores DNS y/o WINS si no se emplea DHCP desde el servidor OpenVPN.

Por tanto, habrá que decirle a nuestra interfase de red virtual (que hemos llamado TAP) estos datos. Iremos pues a las propiedades de red y las rellenaremos a nuestro gusto. Incluso tendremos que introducirle la IP 192.168.VVV.2, ya que Windows no nos dejará guardar la configuración sin una IP.

Si en nuestro cliente ejecutamos **ipconfig /all** veremos algo como (incluso sin habernos conectado):

```
Servidores DNS . . . . . . . . . . .: 192.168.XXX.1
                                      192.168.XXX.2
                                      DDD.DDD.DDD.DDD
                                      DDD.DDD.DDD.DDD

Adaptador Ethernet TAP :

Sufijo de conexión específica DNS : dominio.ejemplo
Descripción. . . . . . . . . . . .  : TAP-Win32 Adapter V8
Dirección física. . . . . . . . . . : 00-FF-D5-A4-3F-FC
DHCP habilitado. . . . . . . . . .  : No
Dirección IP. . . . . . . . . . . . : 192.168.VVV.2
Máscara de subred . . . . . . . . . : 255.255.255.252
Puerta de enlace predeterminada . : 192.168.VVV.1
Servidores DNS . . . . . . . . . . .: 192.168.XXX.1
                                      192.168.XXX.2
Servidor WINS principal . . . . . : 192.168.XXX.2
```

Obsérvese que hemos configurado, tanto en la tarjeta física (la primera, llamada LAN) como en la virtual (la segunda, llamada TAP) los servidores DNS que tenemos en la red 192.168.XXX.0/24. De esta forma evitaremos problemas de resolución de nombres al administrar nuestra red.

Otro aspecto importante es que al estar trabajando con subredes es aconsejable disponer de un servidor WINS para los clientes Windows, el cual también hemos indicado (192.168.XXX.2) y que en nuestro caso está en la misma máquina que el segundo DNS.

Con todo esto podremos acceder a nuestras máquinas por IP, nombre en el dominio y nombre NetBIOS. Por ejemplo 192.168.XXX.70, Pc70.dominio.ejemplo o Pc70.