PFSENSE,
INSTALACIÓN CONFIGURACIÓN Y ADMINISTRACIÓN

Profesor Pedro Enrique Guerrero Zuluaga

Christian Camilo Gaviria Castro.
Estudiante de Telecomunicaciones

Noviembre 17 de 2016.

Instituto Tecnológico Metropolitano.
Facultad de Ingenierías.
Medellín.

Abstract

Los servidores son una parte muy importante de una infraestructura de redes ya que estos se encargan de proveer servicios a los clientes tales como almacenamiento de archivos, distribución de algunas aplicaciones, seguridad, alta escalabilidad, centralización de la red, entre otras muchas ventajas, todo esto con el propósito de satisfacer al usuario final. Los servidores deben tener ciertas características físicas para poder cumplir con requisitos de rendimiento y disponibilidad. El software y el hardware de un servidor son generalmente muy determinantes, un hardware regular de un computador personal no puede servir a cierta cantidad de clientes y no podría soportar la escalabilidad por parte de usuarios y demás máquinas debido al alto requerimiento de rendimiento, hay otro factor que influye en esta parte, es la de infraestructura física, de nada sirve tener un servidor con excelentes características si tenemos una infraestructura de red deficiente, lenta e inestable, se debe garantizar una velocidad apta, redundancia en la red y se recomienda al menos cableado de fibra óptica para garantizar una alta velocidad en la transmisión de datos, buen ancho de banda y el ofrecimiento óptimo de los servicios hacia los usuarios finales.

En las próximas páginas de este pequeño anexo se desarrollará la configuración de diferentes servidores para propósitos que se explicarán más adelante.

Tabla de Contenidos

Capítulo 1

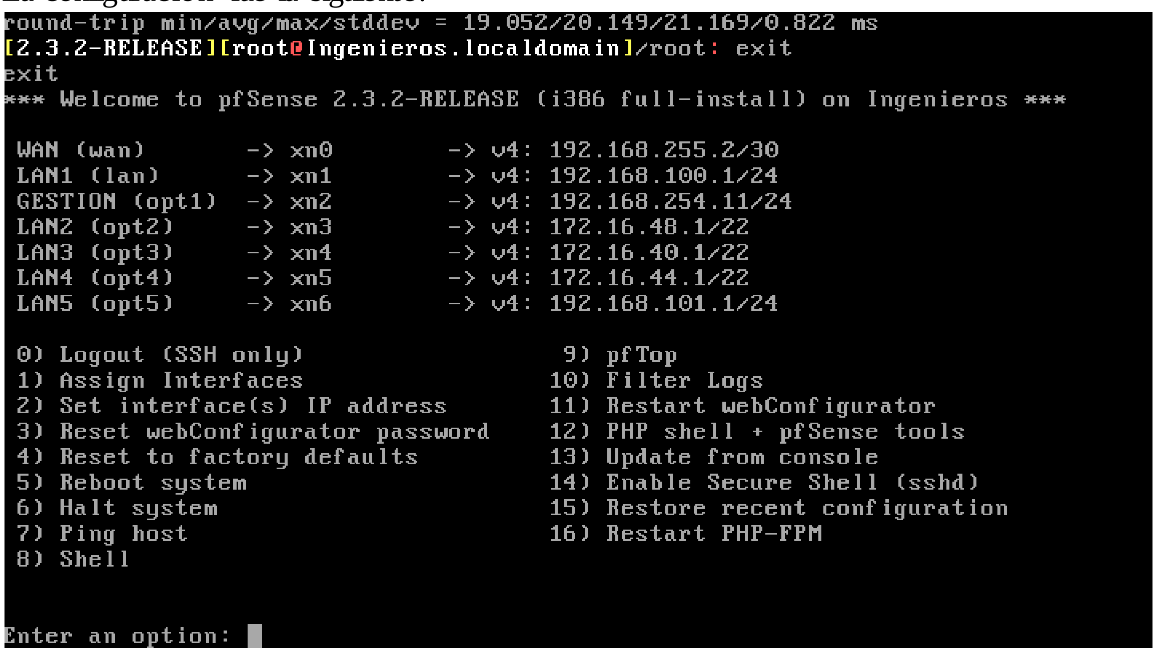
Desarrollo de contenidos

Junto con el profesor Pedro guerrero, asesor de nuestro trabajo de grado y cabeza del semillero de redes, se ha instalado, configurado y administrado una serie de servidores para cubrir las diferentes necesidades de los usuarios y resolver varios problemas que se presentan en las diferentes infraestructuras.

En el laboratorio de radiopropagación ubicado en el sexto piso remotamente accedimos a un servidor ubicado en el departamento de Putumayo para realizar la instalación de un servidor proxy transparente para así mejorar un poco la seguridad de la red, mejorar la velocidad de navegación de los usuarios, mejorar la calidad del servicio en la navegación en internet, disminuir notoriamente el ancho de banda y la latencia y tener una administración centralizada de la misma.

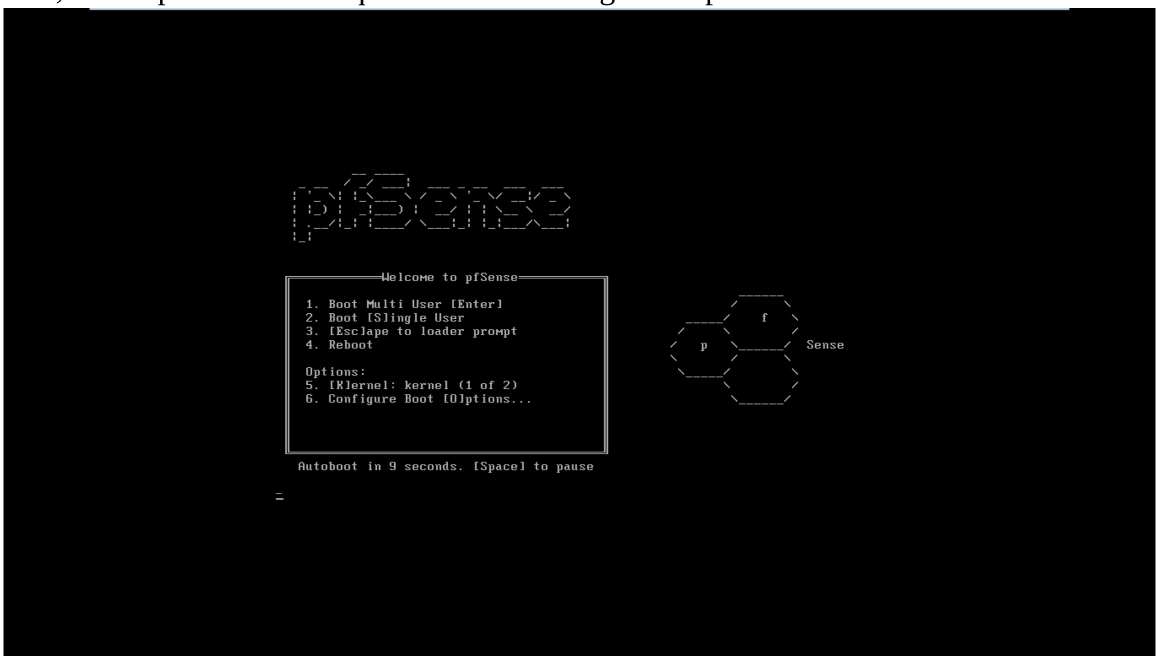
Link de descarga Pfsense: https://pfsense.org/download/

La configuración fue la siguiente:

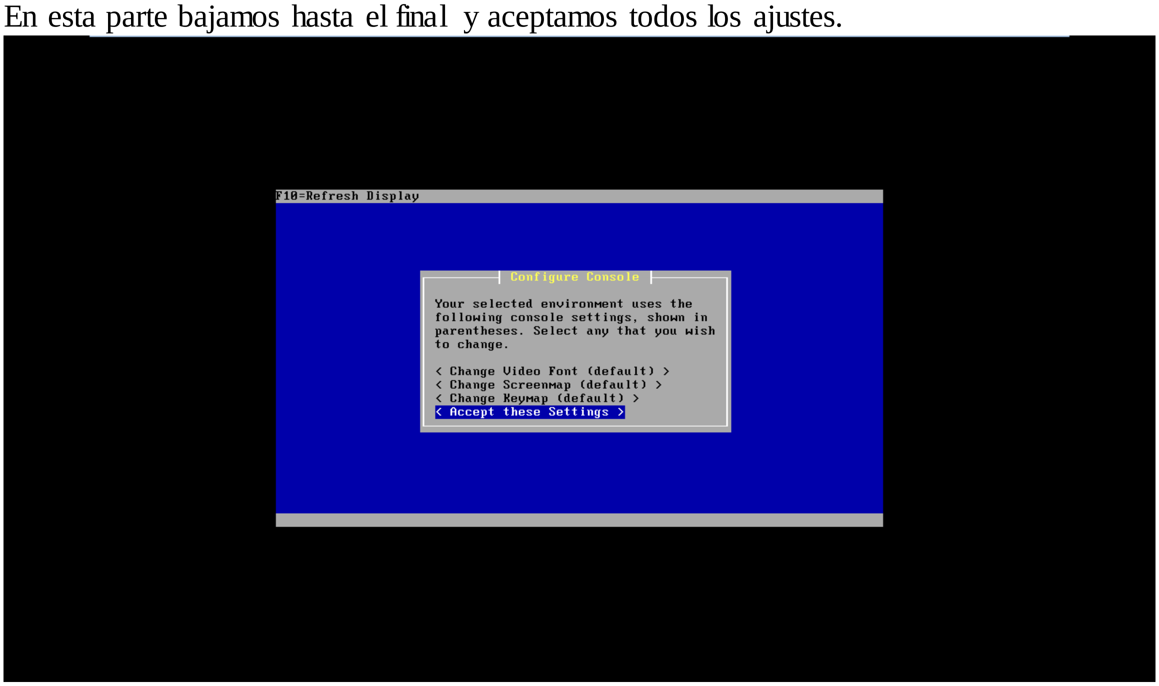


Para llevar a cabo esto instalamos una máquina virtual en el hipervisor XenServer, el sistema operativo implementado fue Pfsense. A continuación se mostrará paso por paso la instalación, configuración y administración.

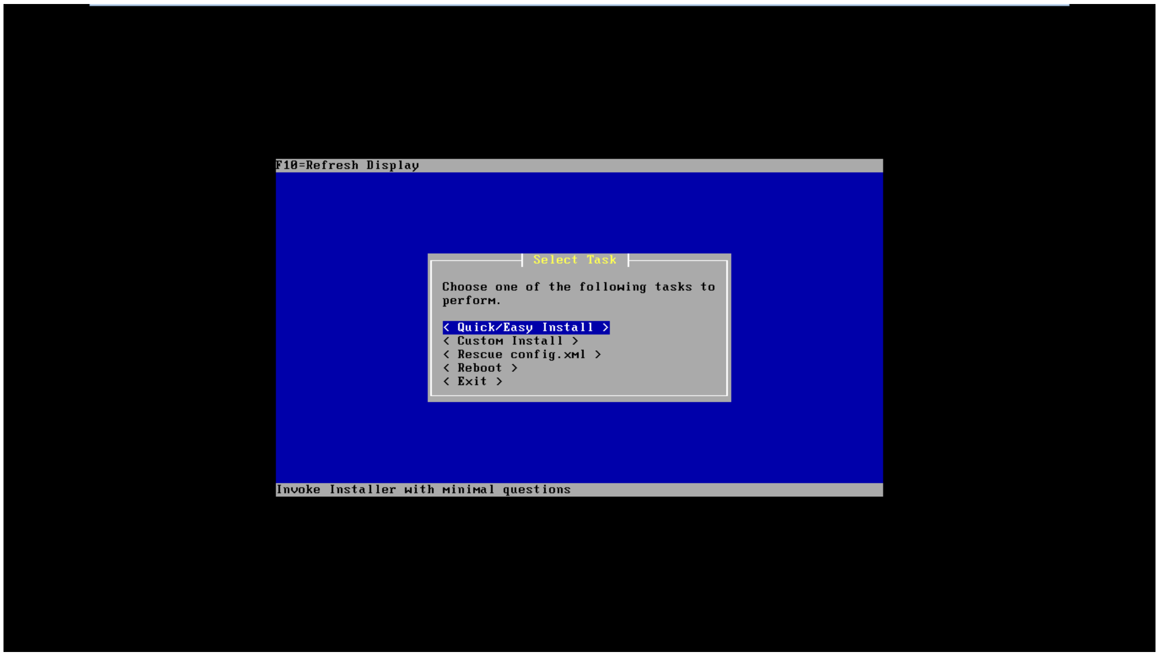
Esta es la pantalla con la que nos encontraremos la primera vez que iniciemos desde el ISO, solo esperamos hasta que entremos a la siguiente pantalla.



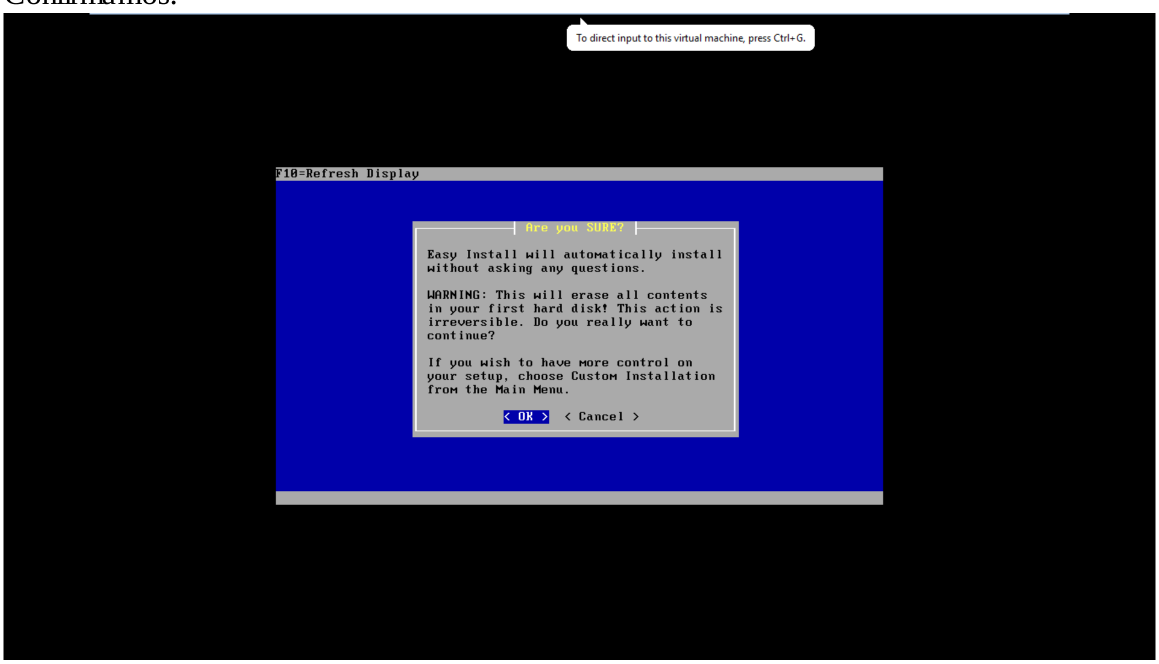
En esta parte bajamos hasta el final y aceptamos todos los ajustes.



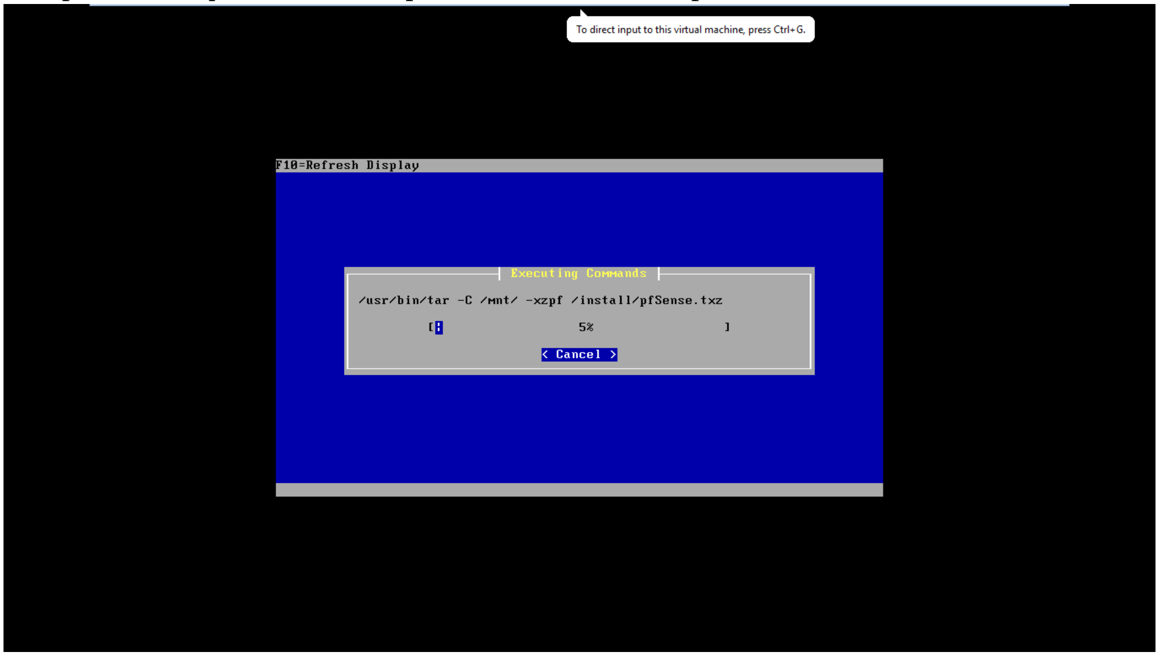
Seleccionamos la instalación fácil.



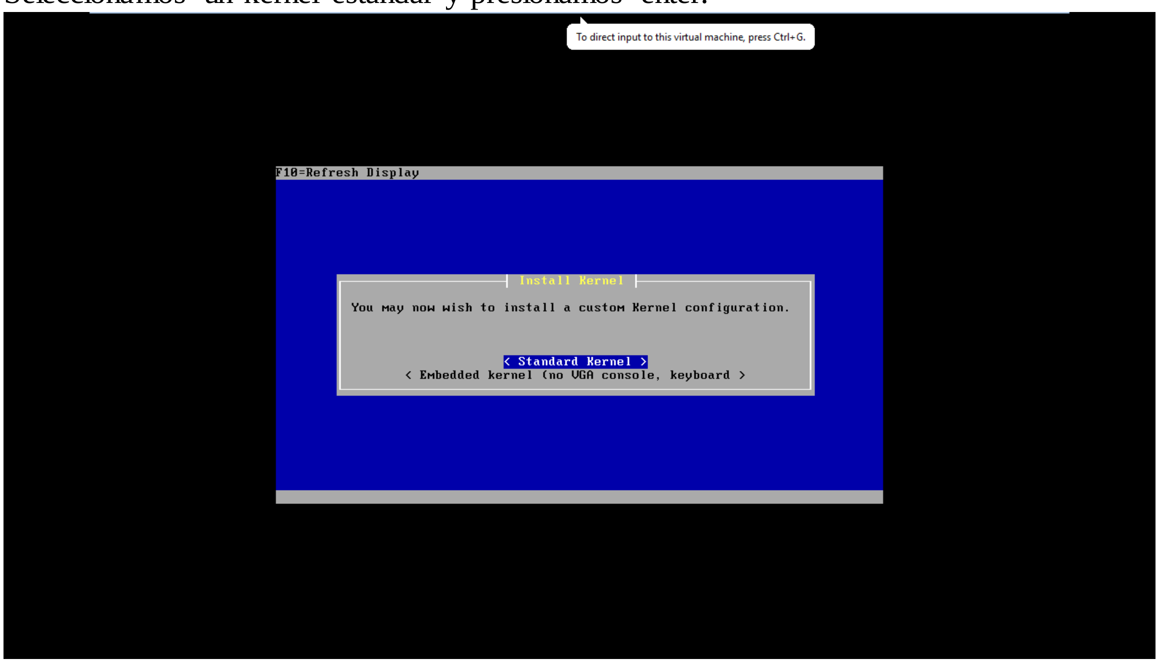
Confirmamos.



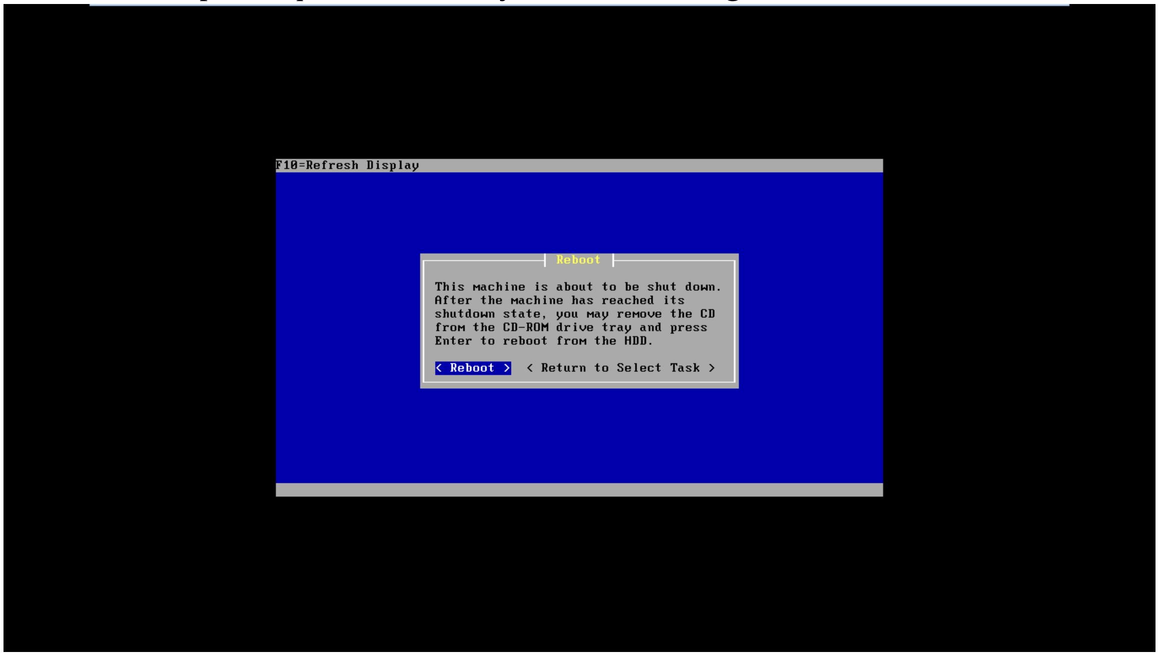
Y esperamos a que el sistema operativo realice las respectivas instalaciones.



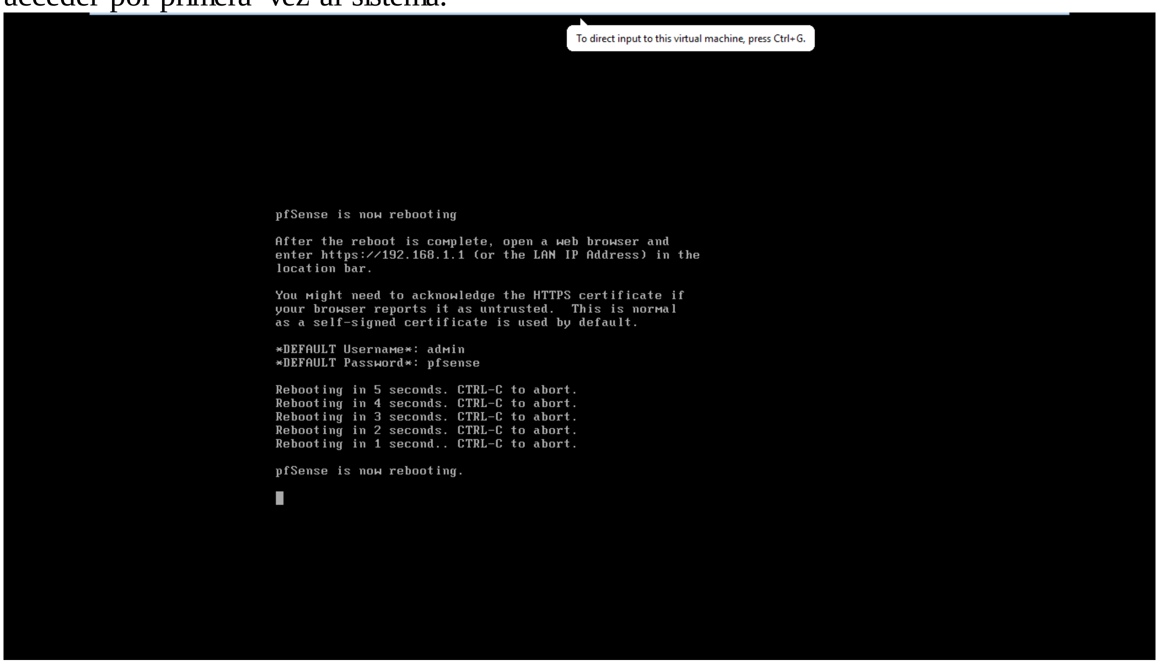
Seleccionamos un kernel estándar y presionamos enter.



Por último nos pedirá que reiniciemos y retiramos la imagen ISO.

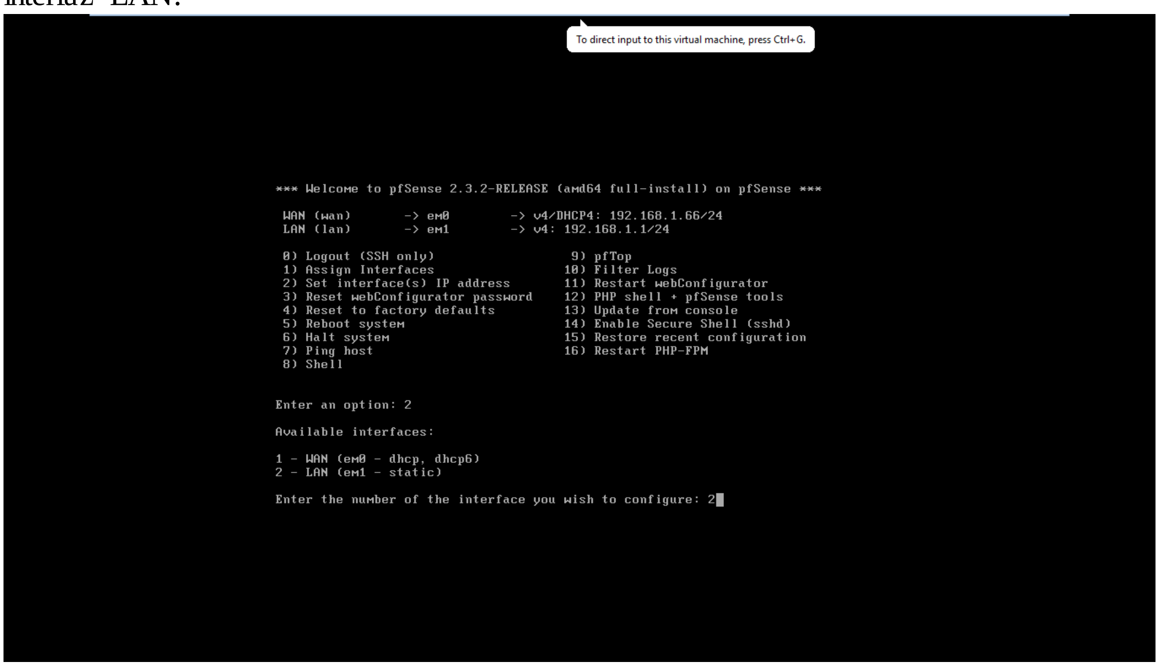


En esta pantalla nos muestra como son las credenciales de usuario con las que podemos acceder por primera vez al sistema.

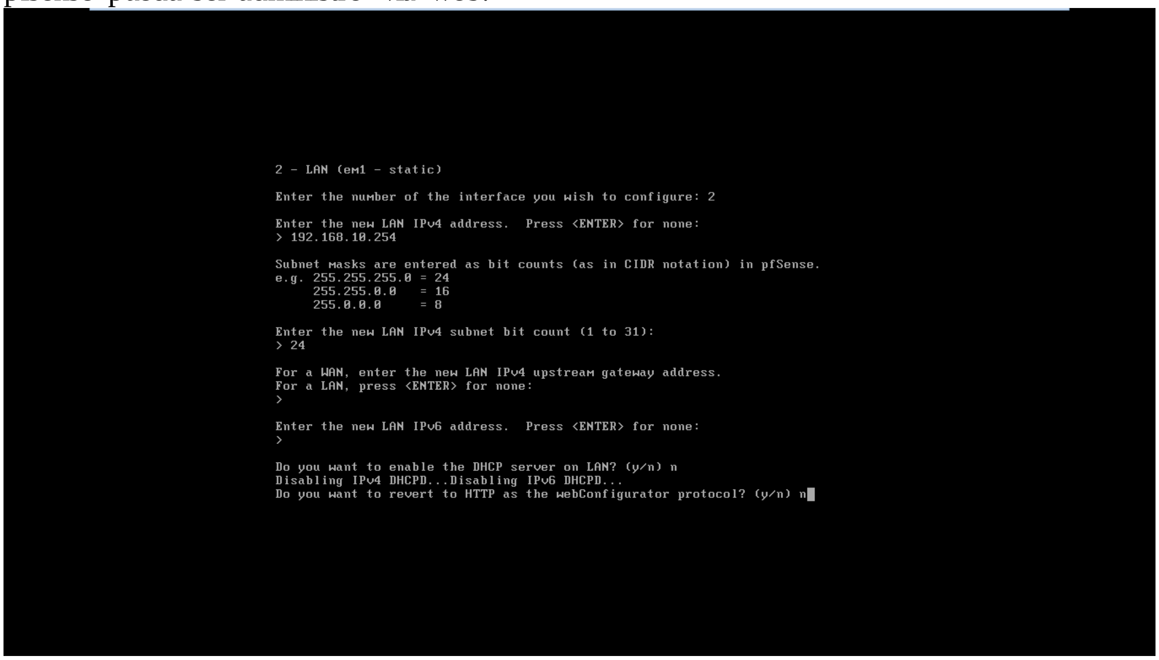


En algunas ocasiones nuestro servidor nos configurará IPs automáticamente, de no ser así se puede configurar seleccionando la opción número 2.

Nos mostrará esta opción y podremos configurar nuestras redes como deseemos.
Nota: Por defecto pfsense solo permite acceder a la configuración web solo por su interfaz LAN.

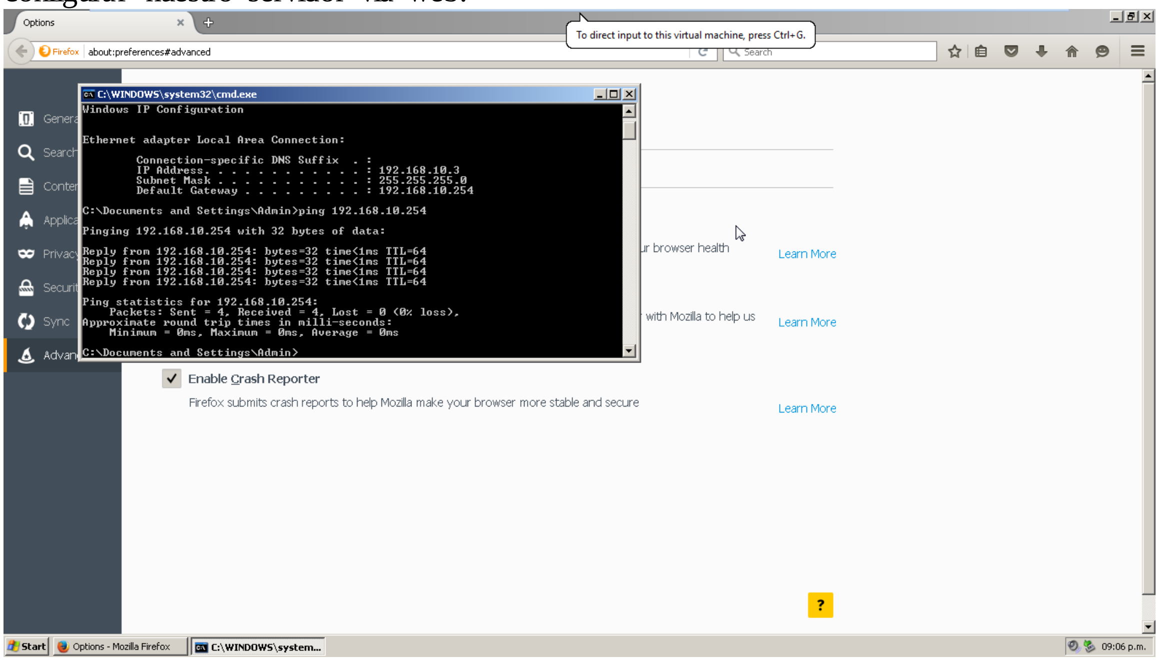


Seguiremos los pasos y al final nuestra nueva red quedará lista para que nuestro servidor pfsense pueda ser administro vía web.

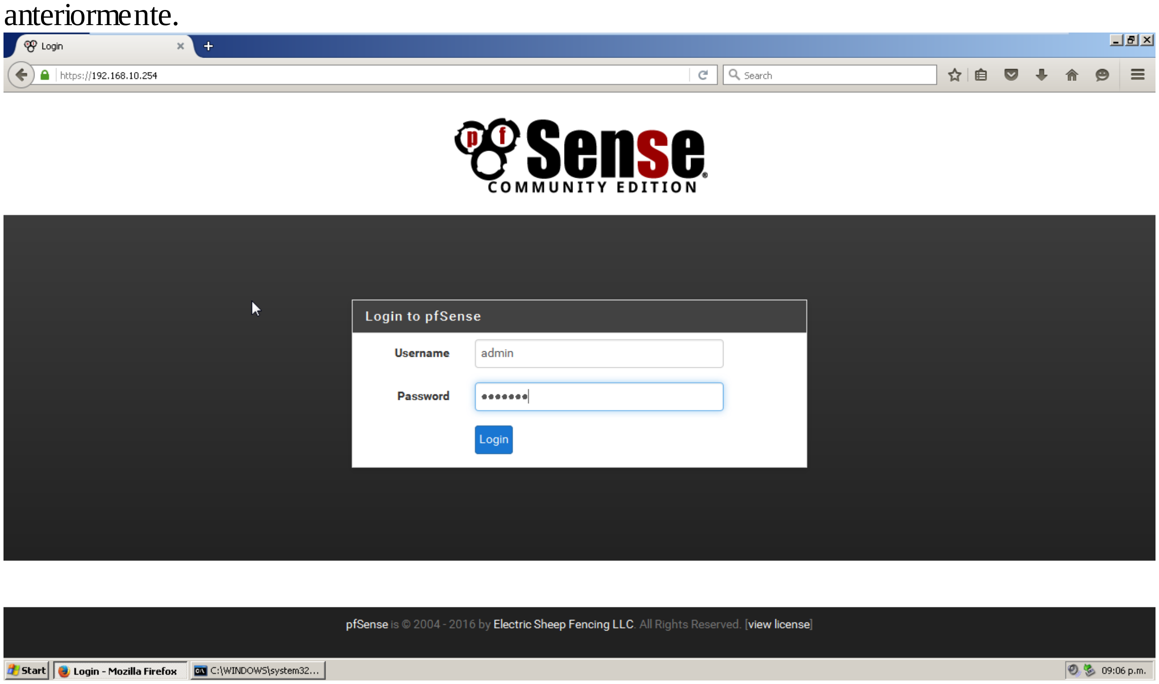


Con la dirección que se nos indica accederemos para configurar el servidor por primera vez.

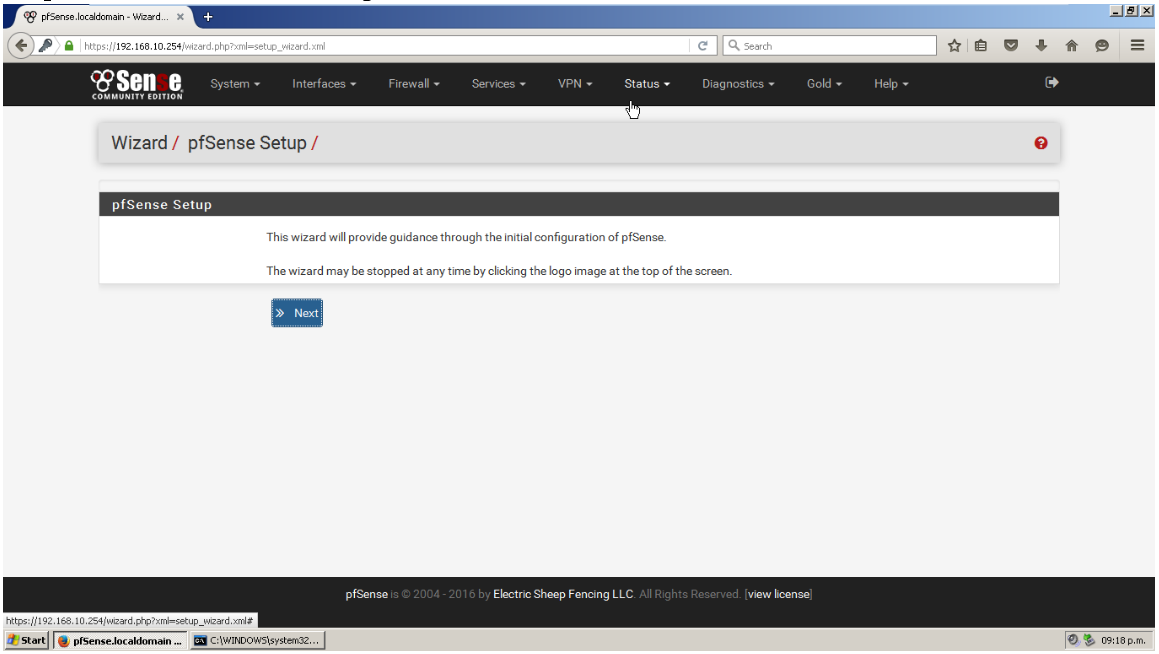
En un PC cliente agregamos una IP en el mismo segmente de red para poder acceder a configurar nuestro servidor vía web.



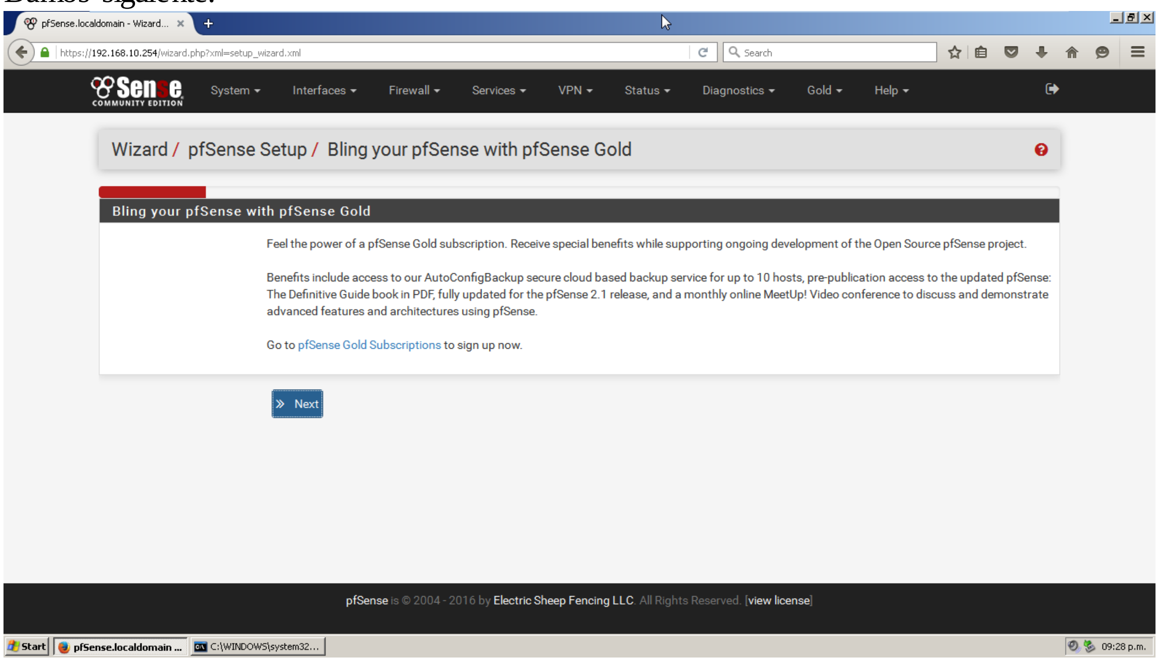
Esta es la página que nos encontraremos, accedemos con las credenciales descritas anteriormente.



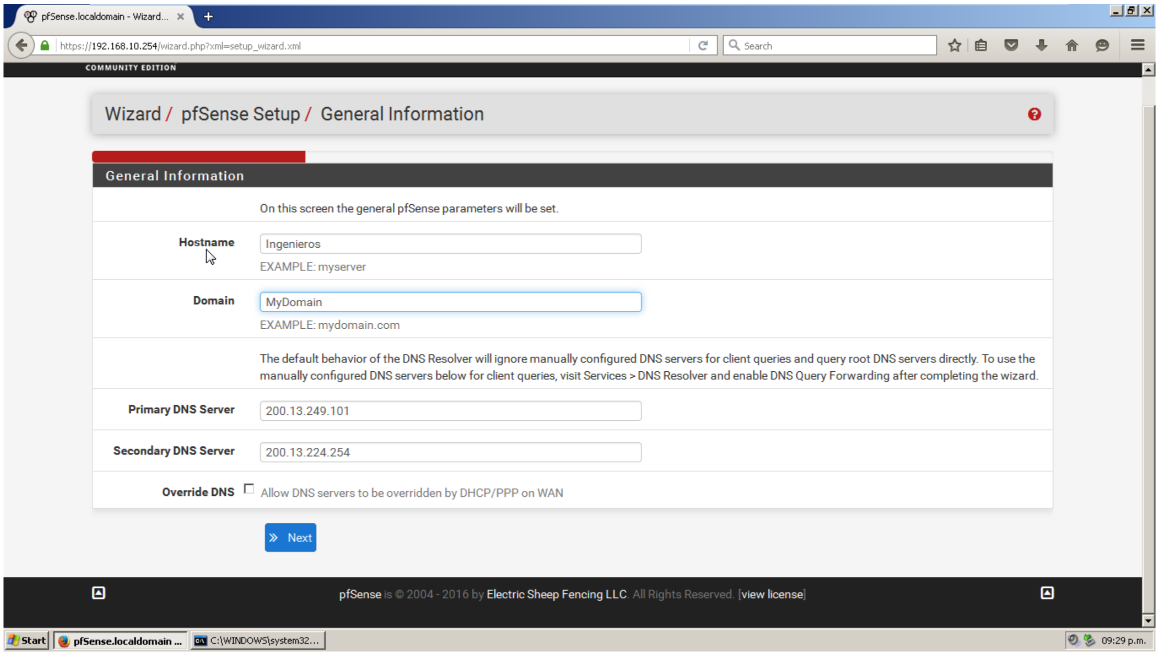
Empezaremos con una configuración básica, daremos next.



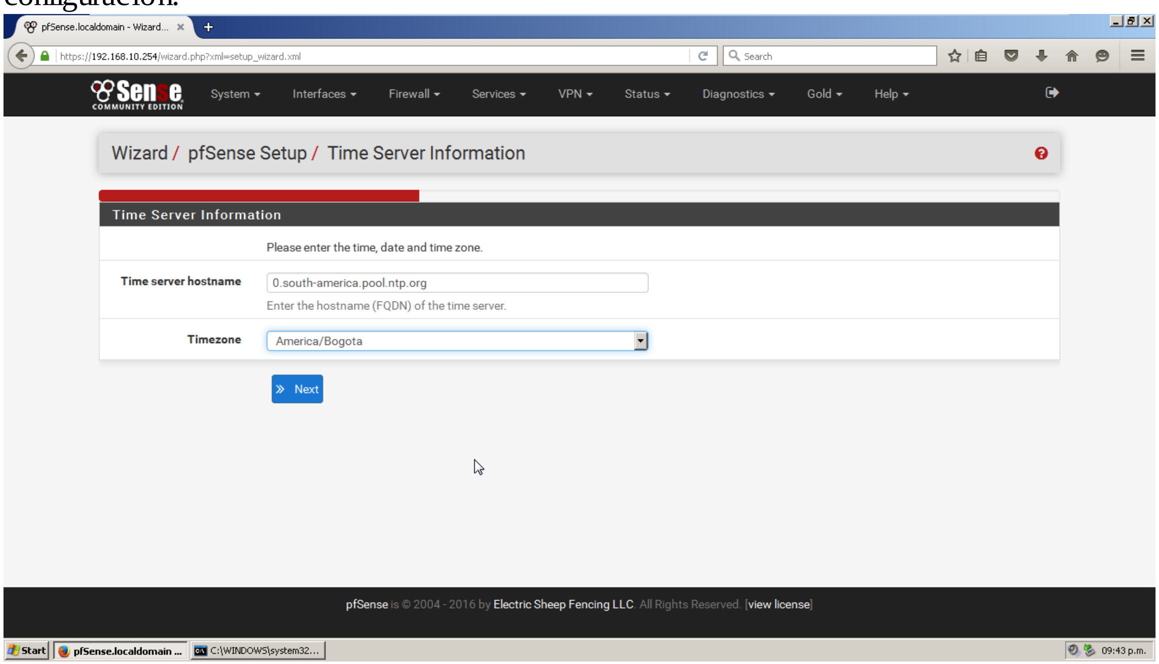
Damos siguiente.



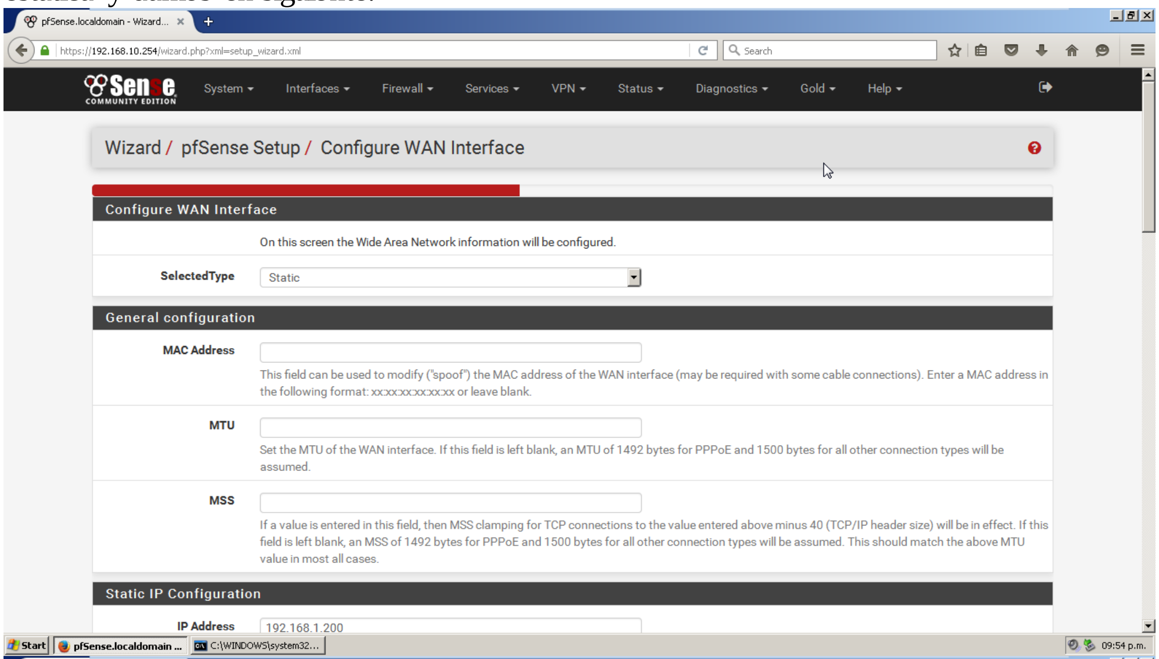
En este paso pondremos nombre a nuestro servidor, dominio si tenemos, DNS primeros y secundarios y deshabilitamos la opción de que nos entregue DNS por DHCP en la red WAN.

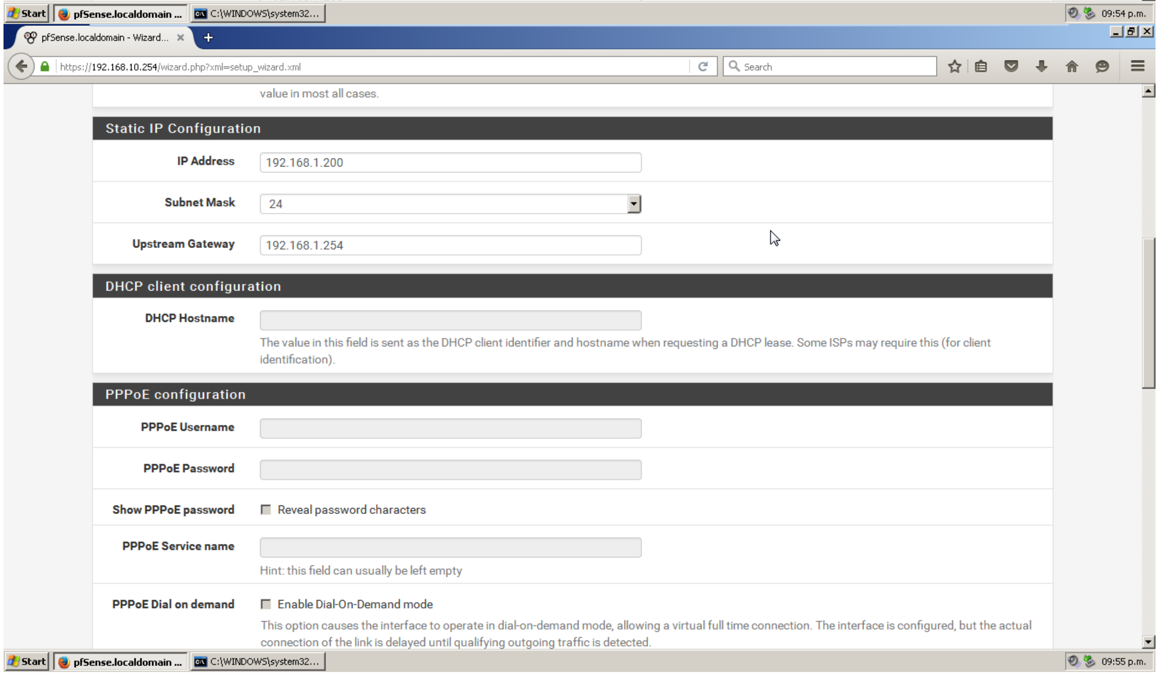


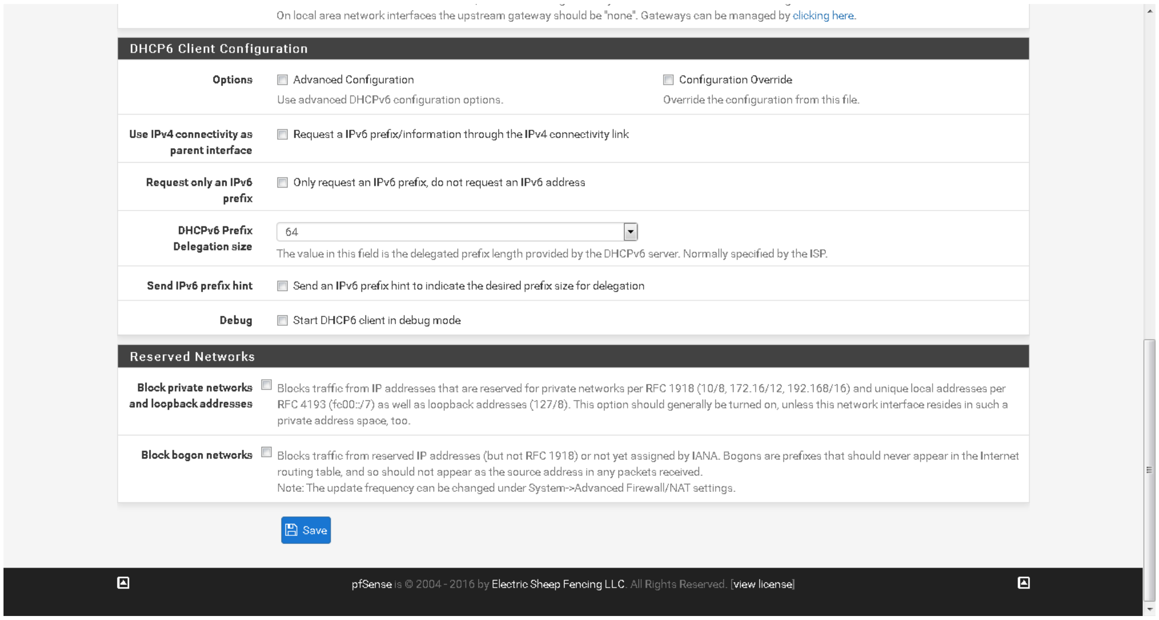
Seleccionamos nuestra zona horaria y el respectivo servidor NTP y continuamos con la configuración.



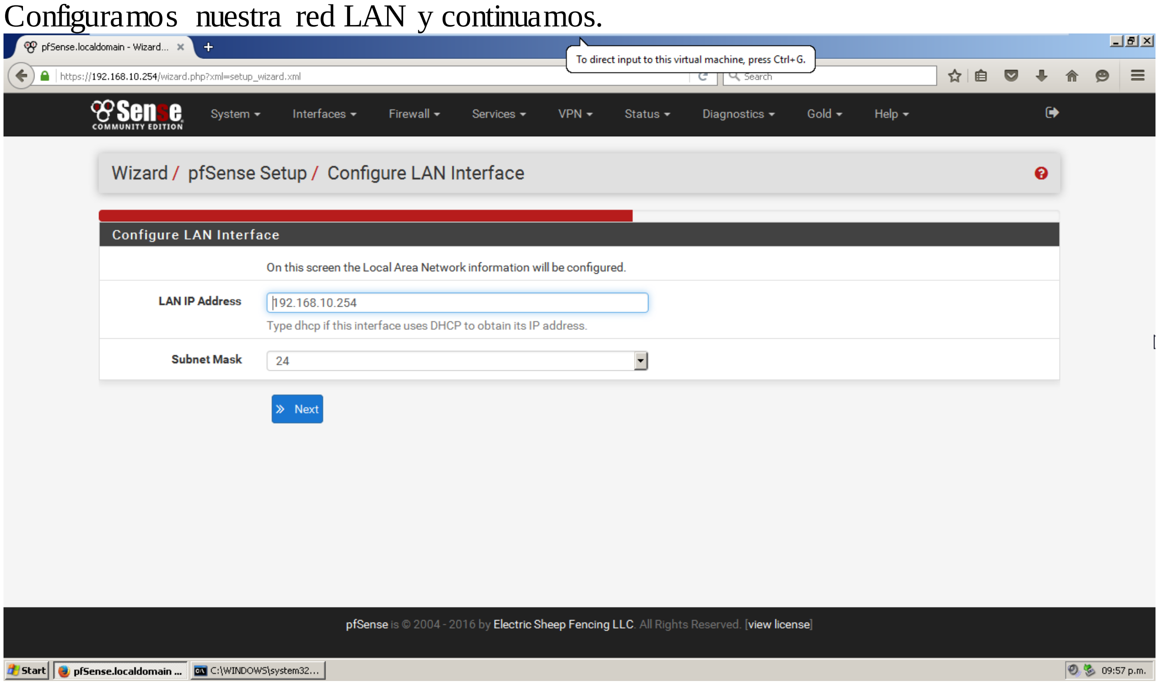
En esta parte configuraremos nuestra red WAN, en este caso la configuraremos con IP estática y damos en siguiente.



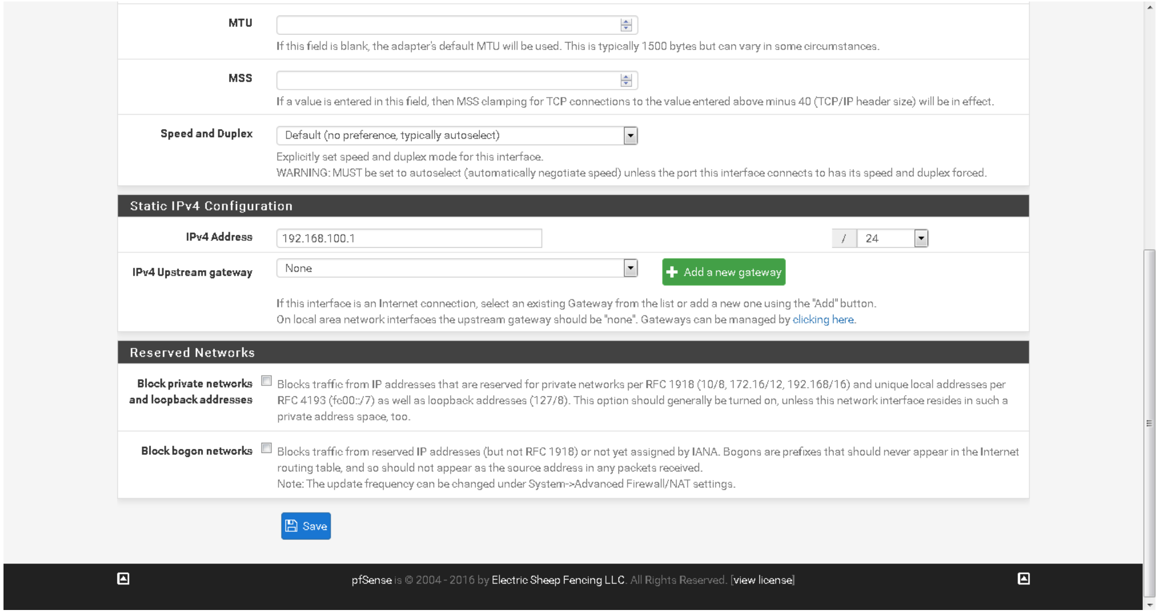




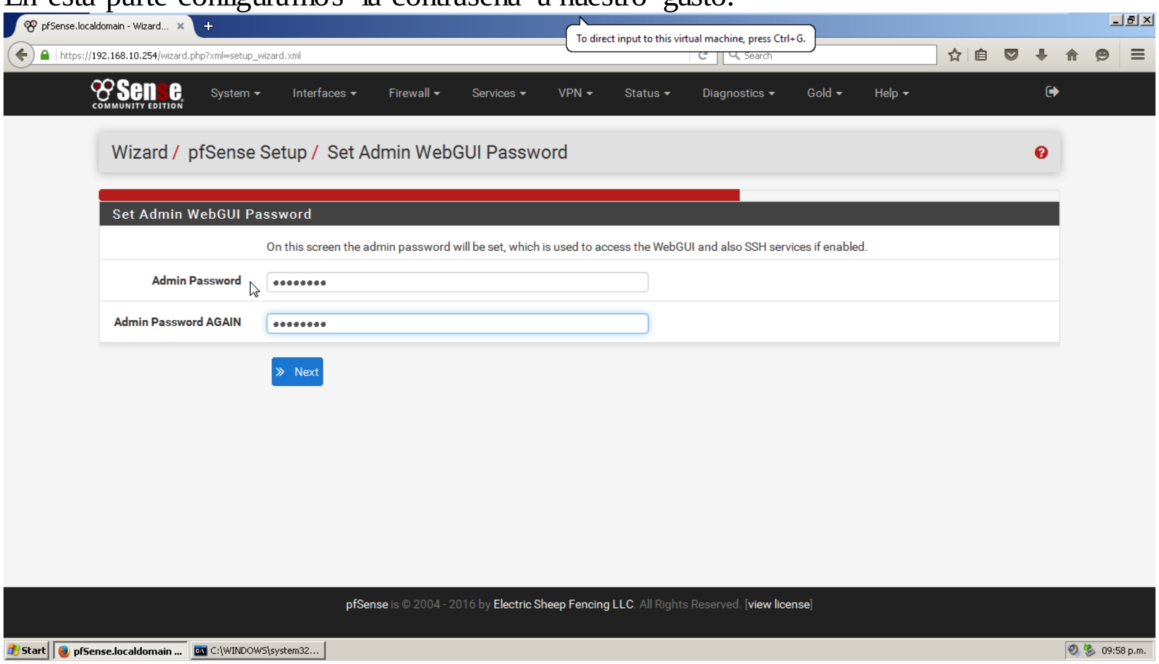
Configuramos nuestra red LAN y continuamos.



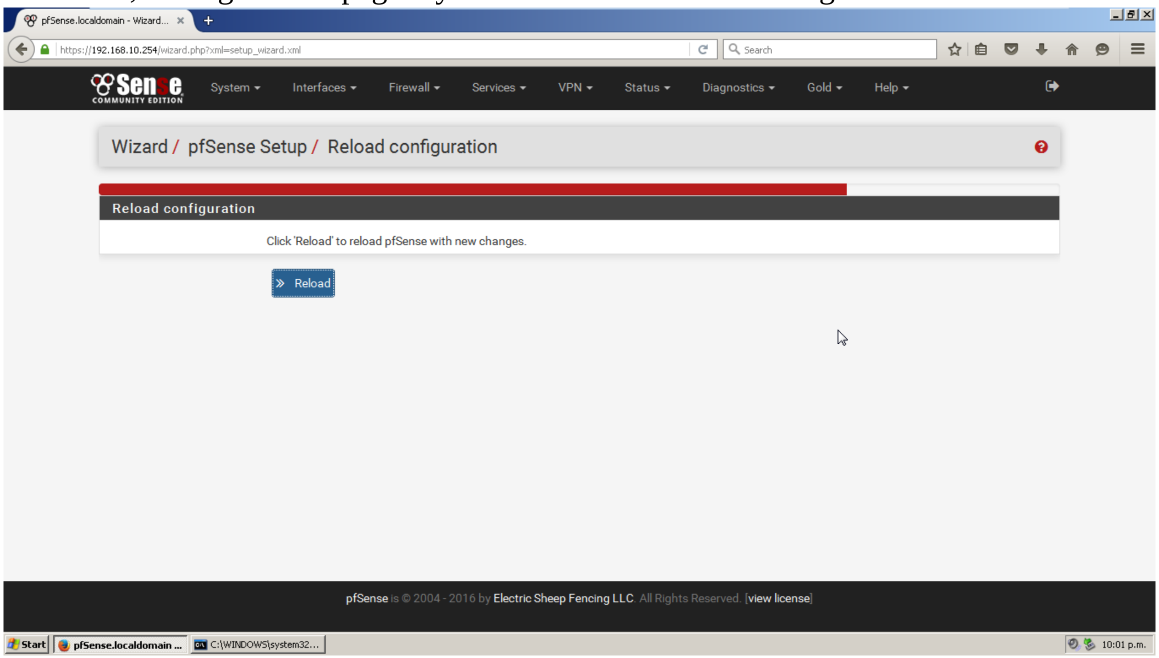
Las demás interfaces de red locales se configuran de manera similar.



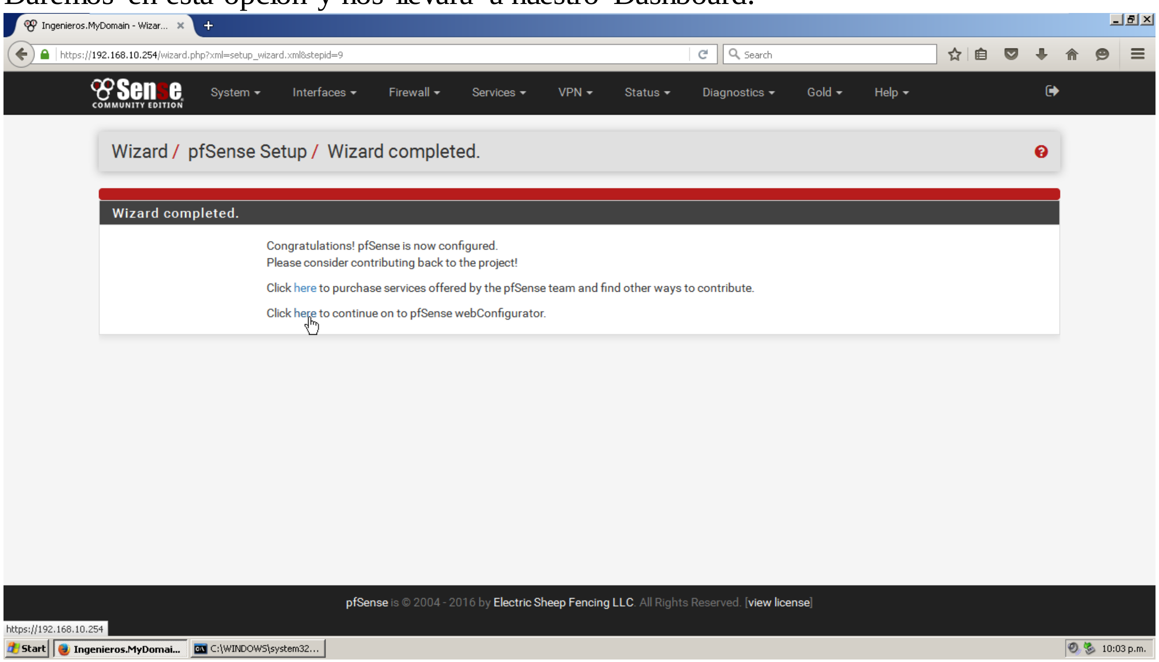
En esta parte configuramos la contraseña a nuestro gusto.



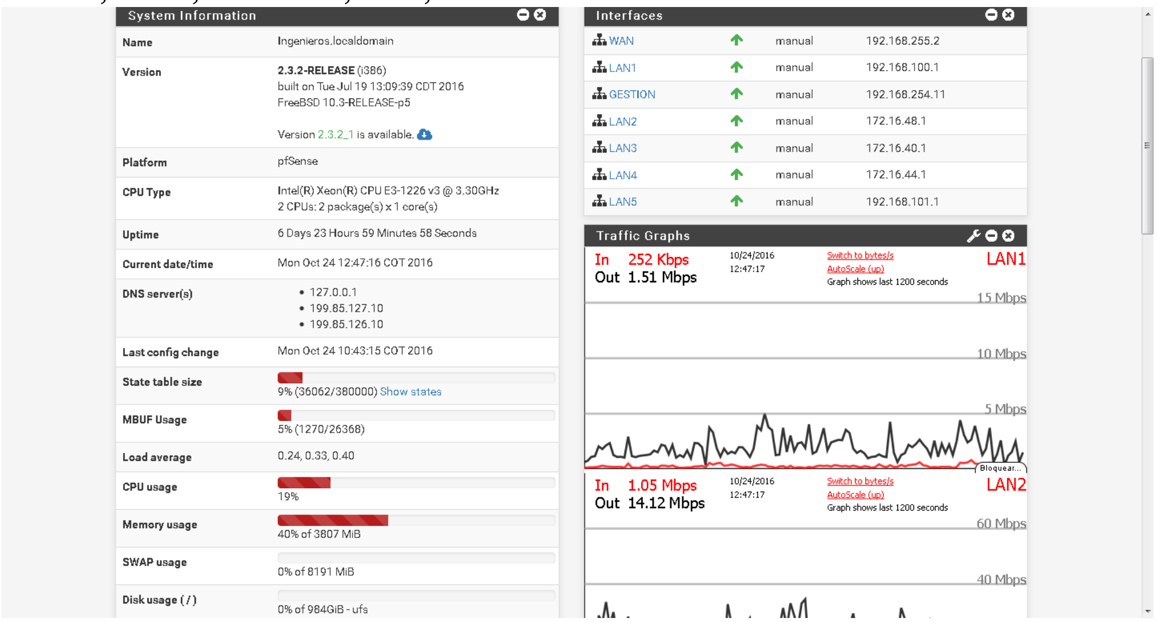
Por último, recargamos la página y estará casi lista nuestra configuración básica.



Daremos en esta opción y nos llevara a nuestro Dashboard.

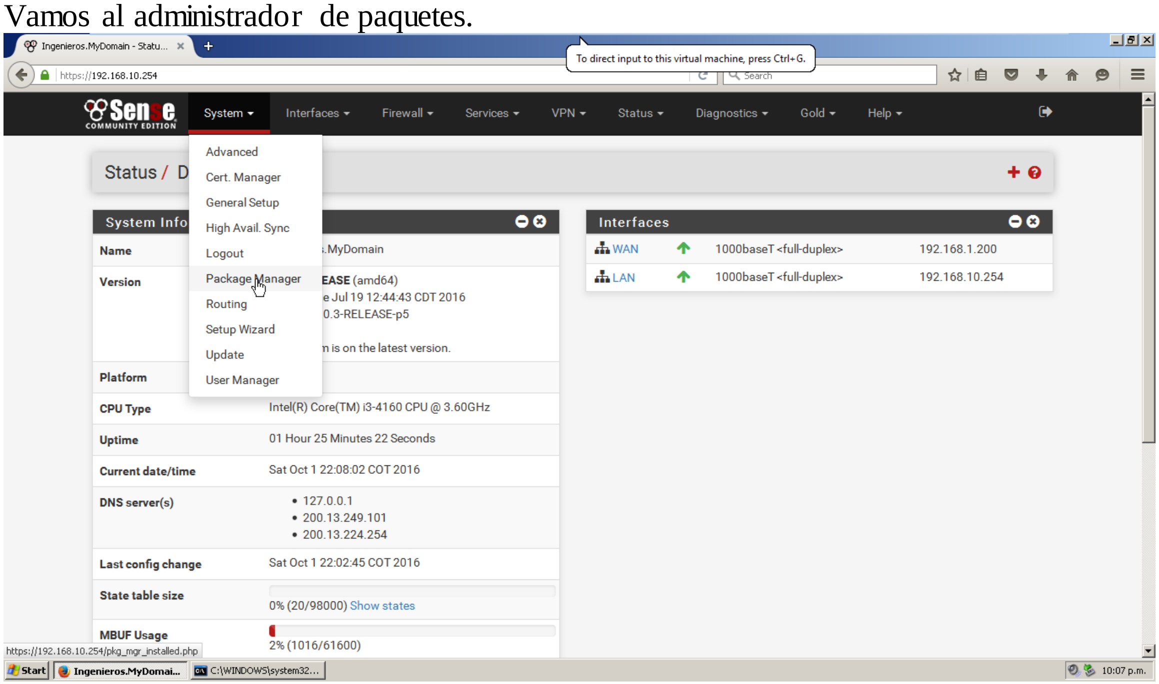


Este es nuestro Dashboard, desde aquí podemos monitorear lo que sucede con nuestro servidor, RAM, disco duro, CPU, etc.

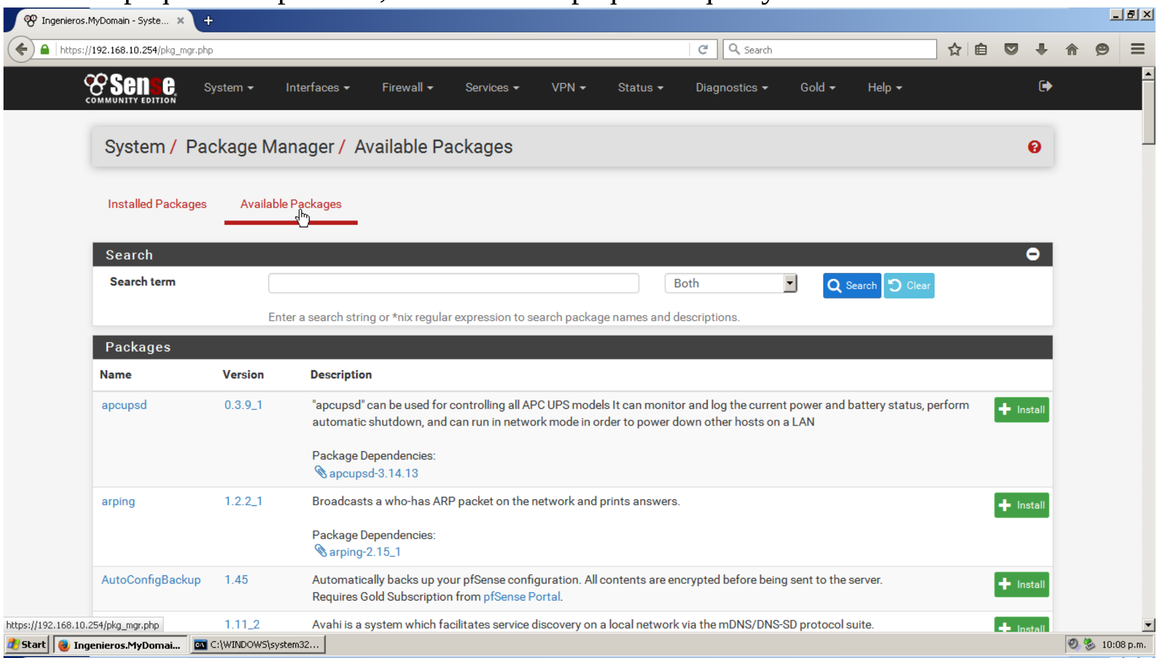


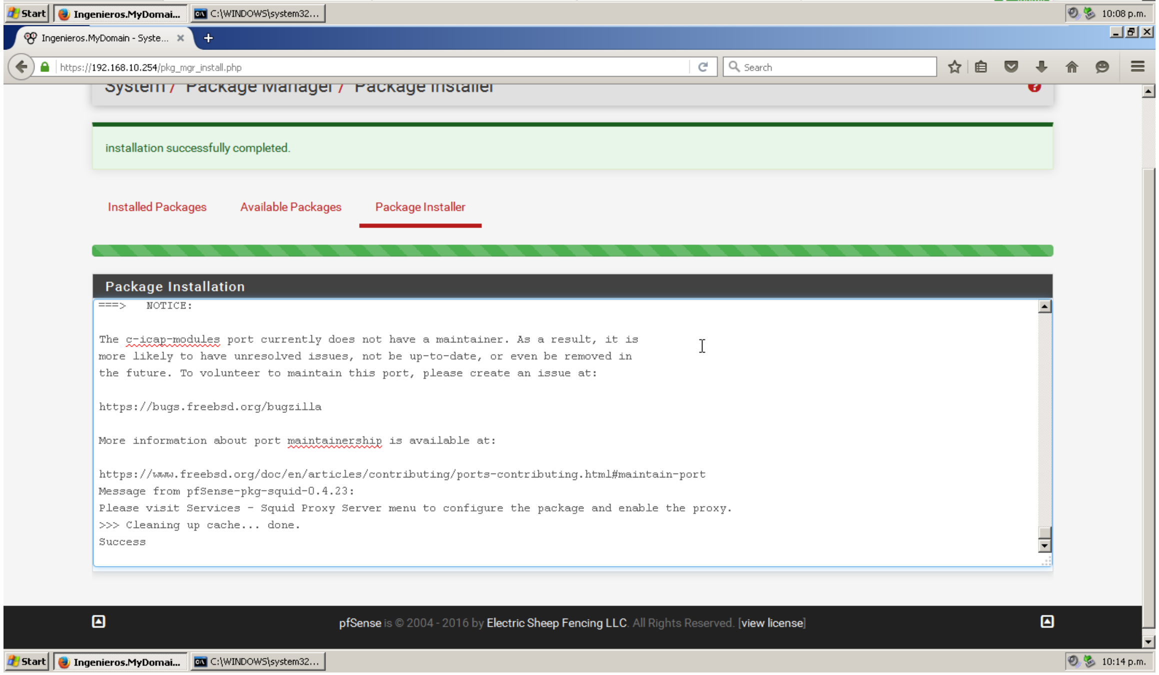
A partir de este momento instalaremos y configuraremos nuestro servidor como proxy transparente:

Vamos al administrador de paquetes.

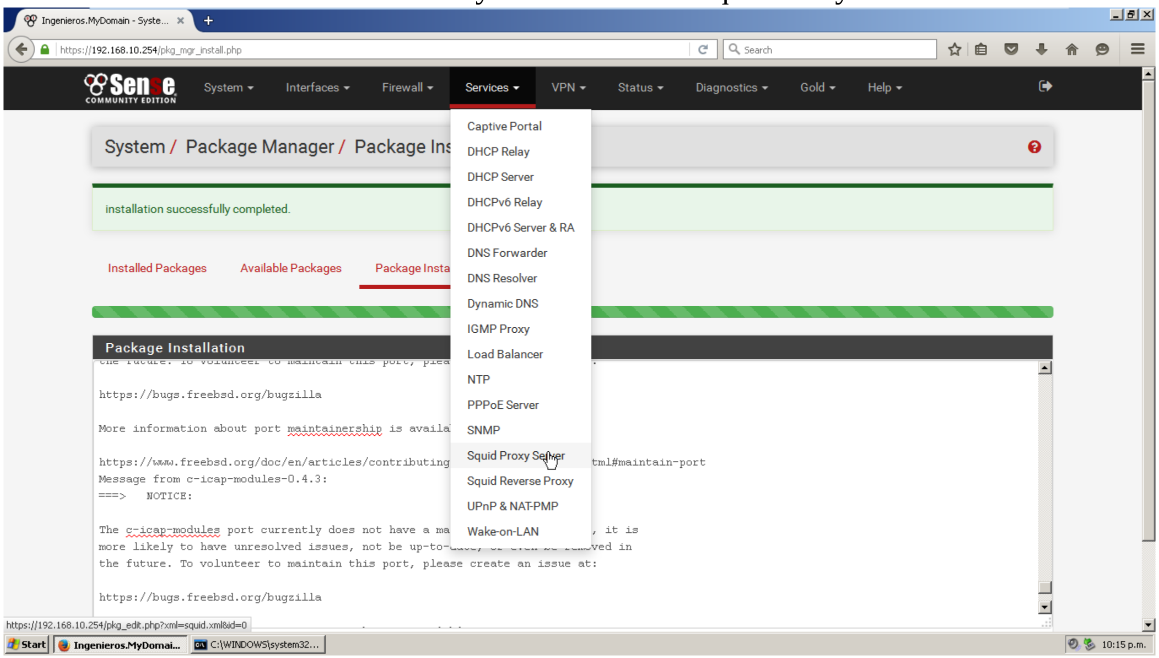


Vamos a paquetes disponibles, buscamos el paquete Squid y lo instalamos.

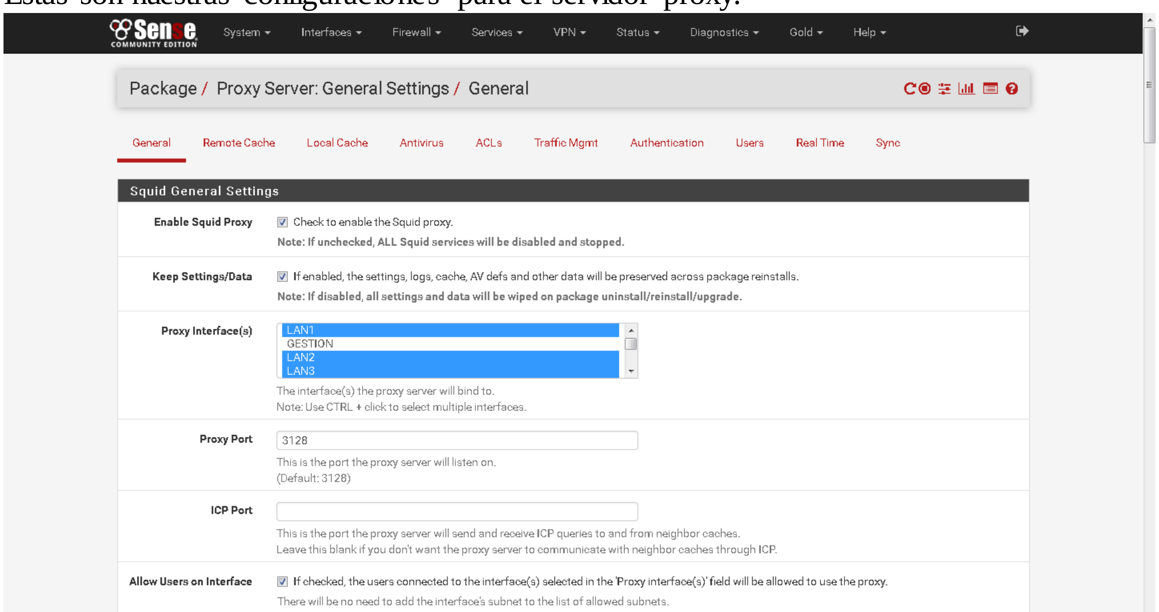




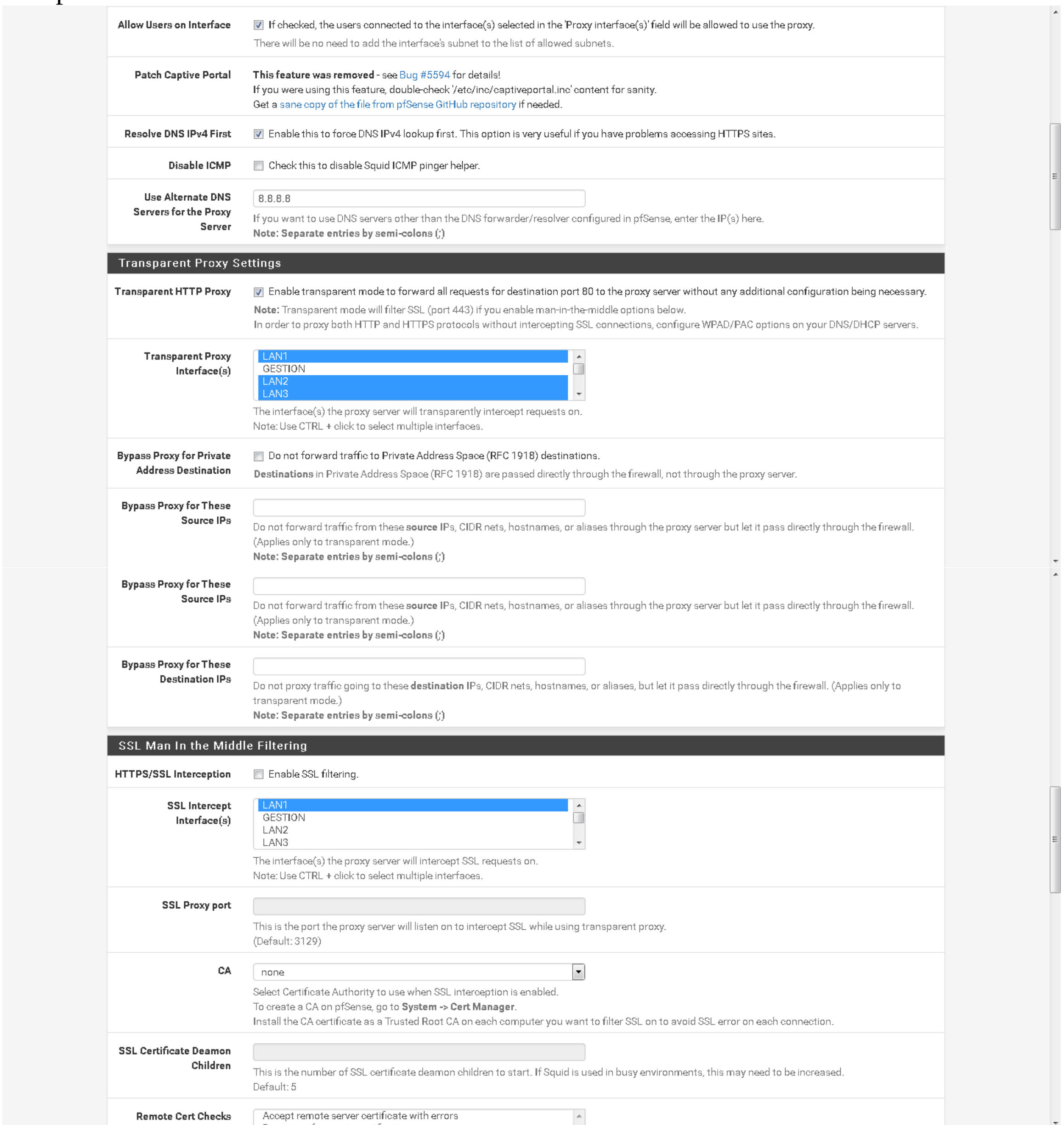
Una vez instalado vamos a servicios y seleccionamos Squid Proxy Server.

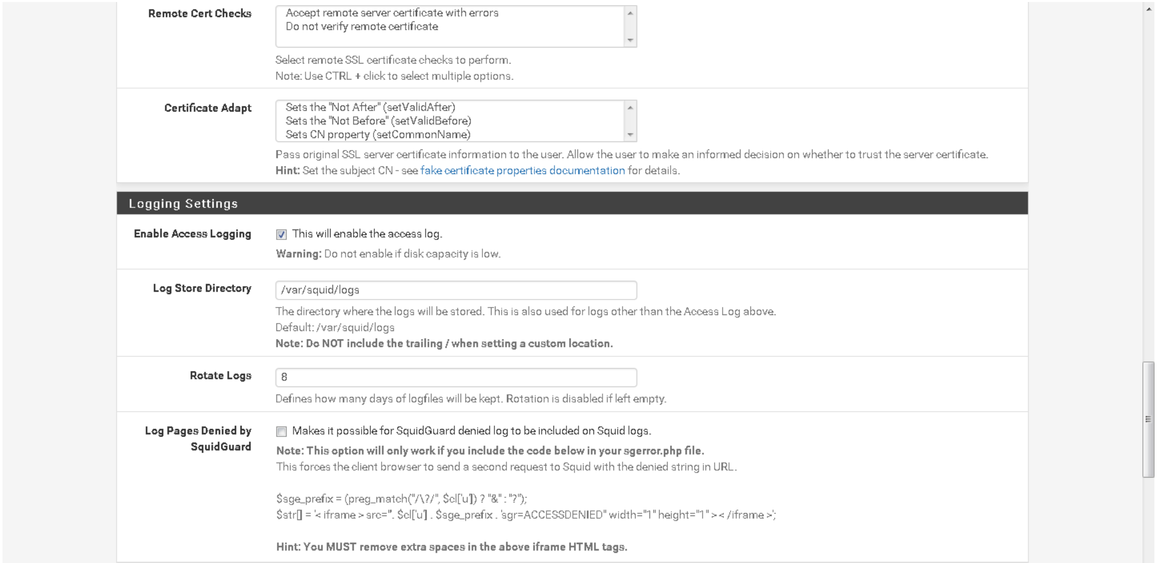


Estas son nuestras configuraciones para el servidor proxy.

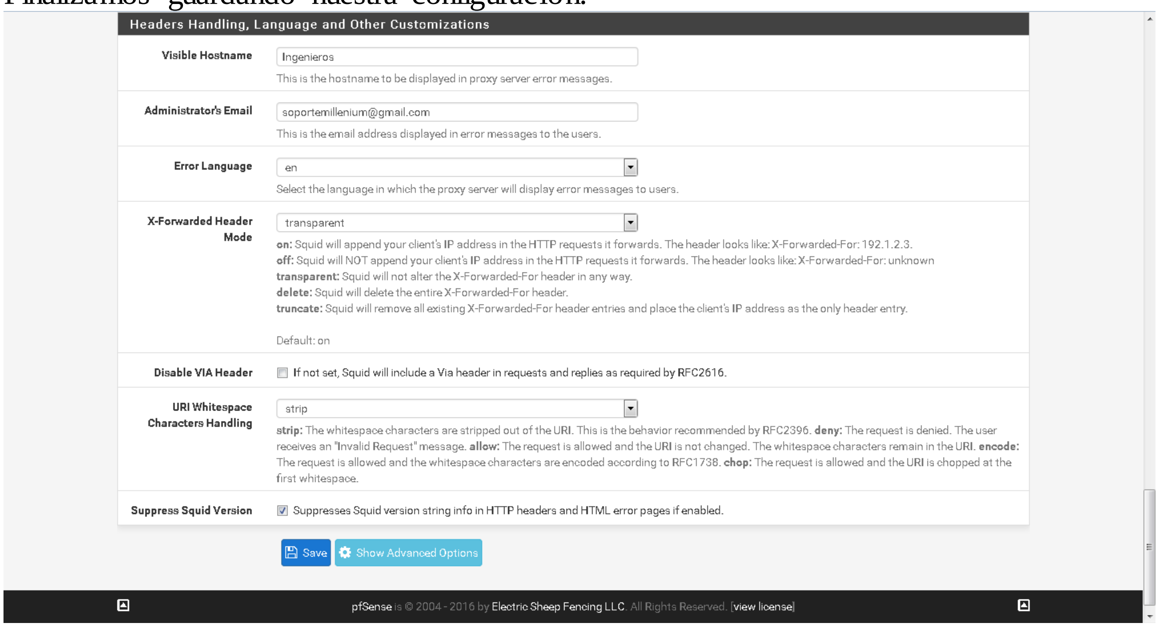


Haremos las siguientes configuraciones para establecer nuestro servidor como proxy transparente:

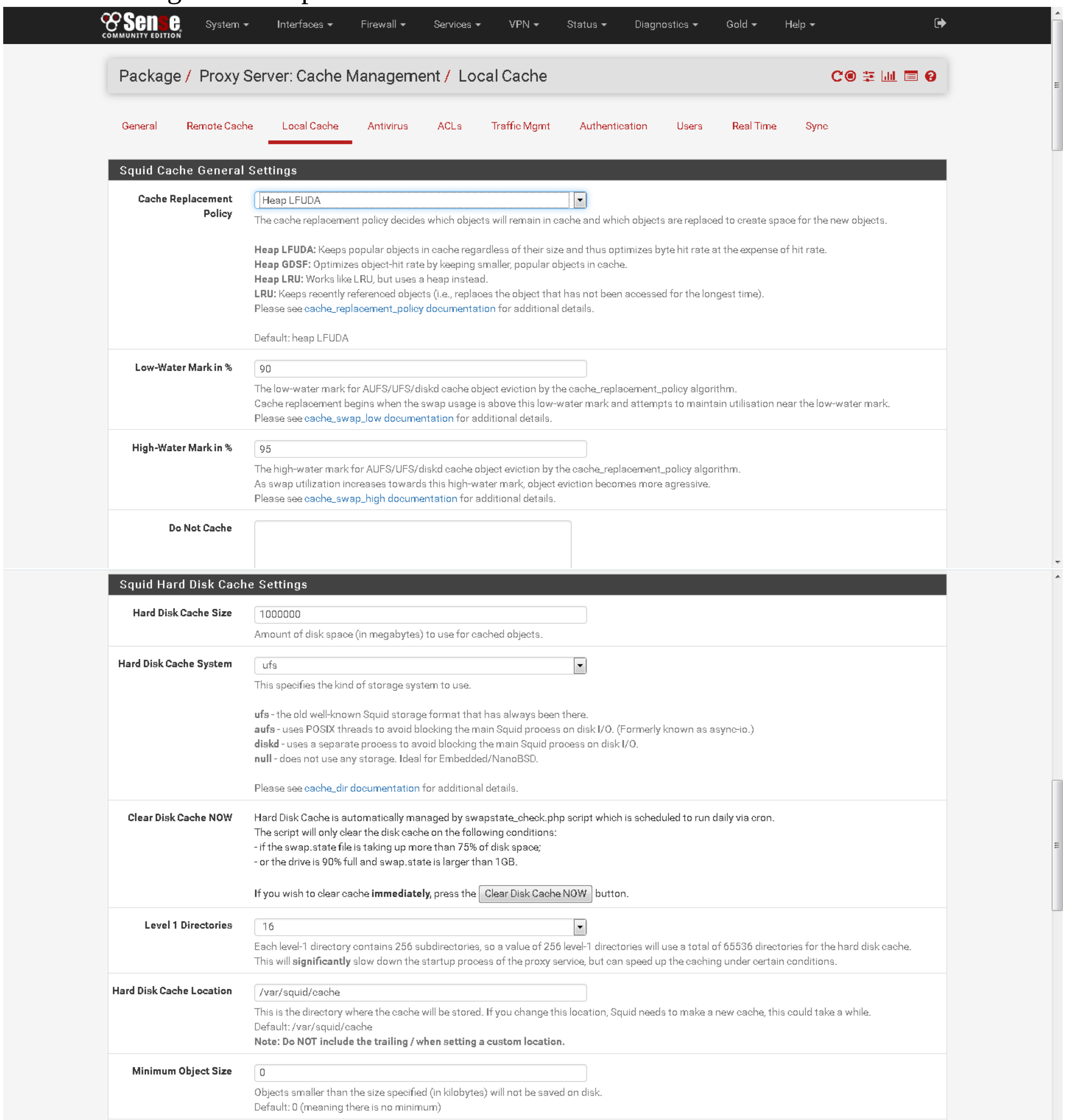


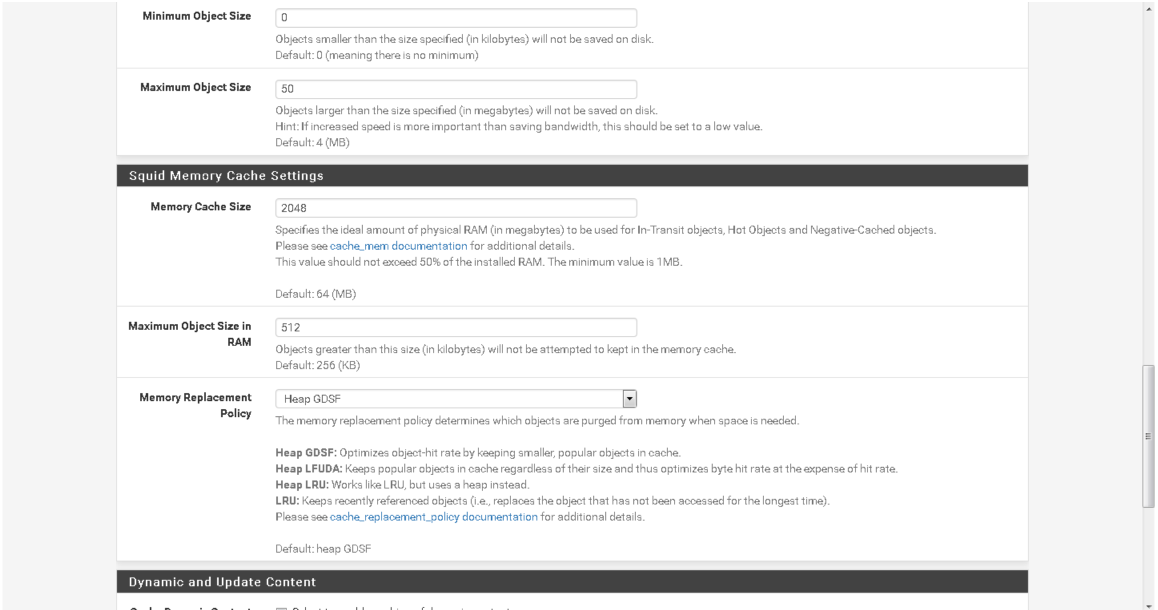


Finalizamos guardando nuestra configuración.

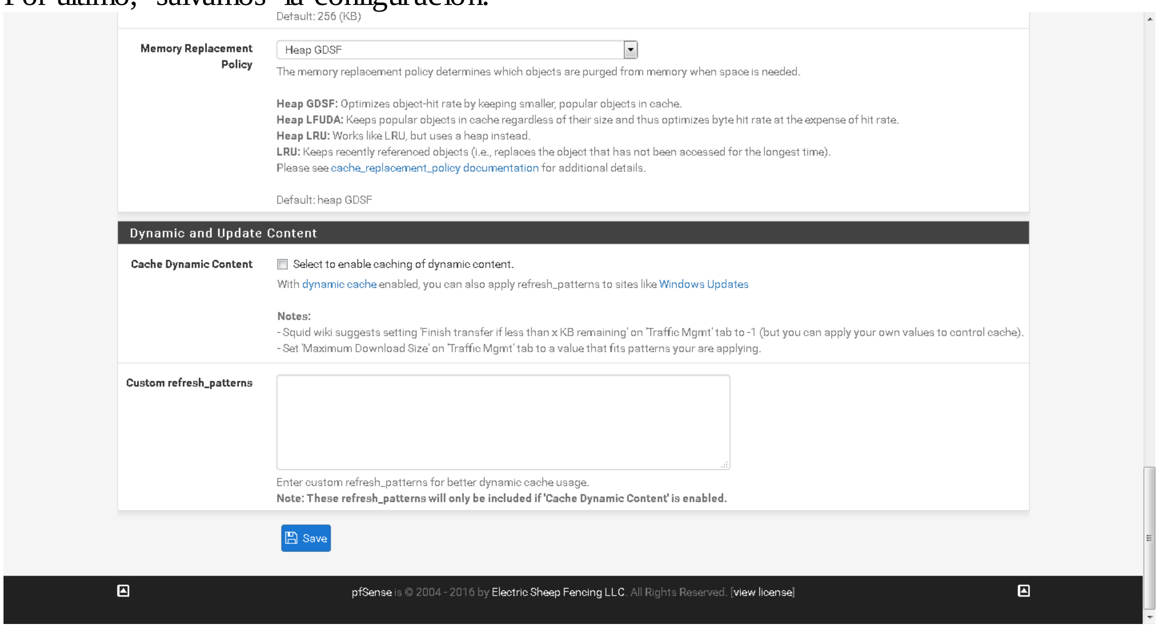


Ahora nos dirigimos a la pestaña de local cache.

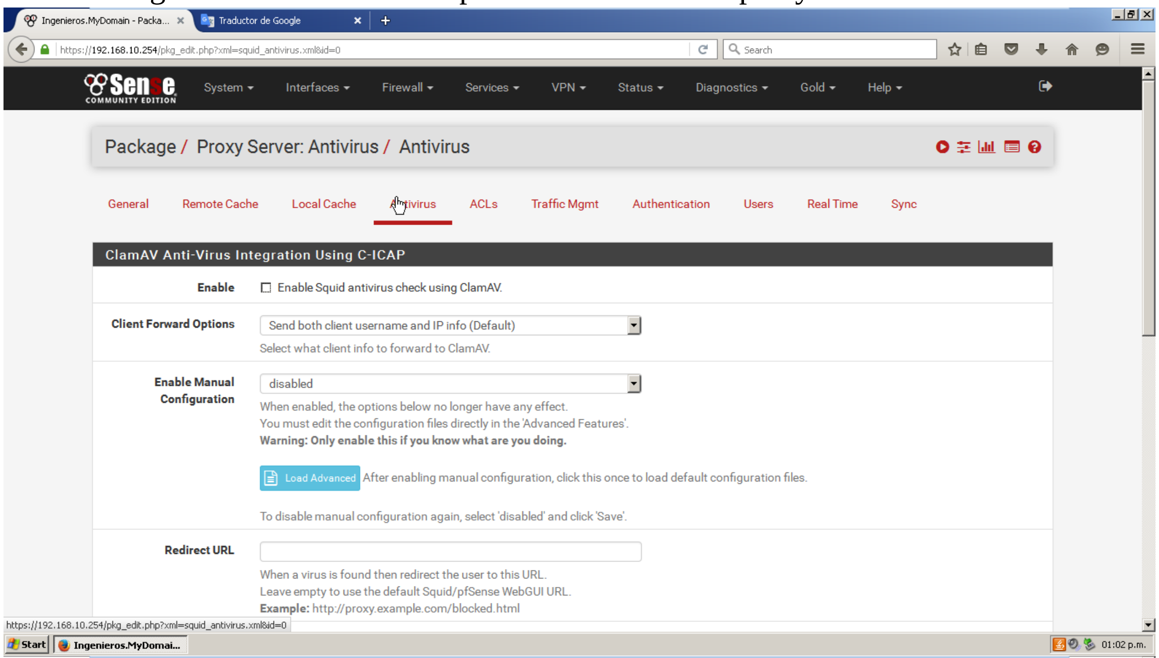


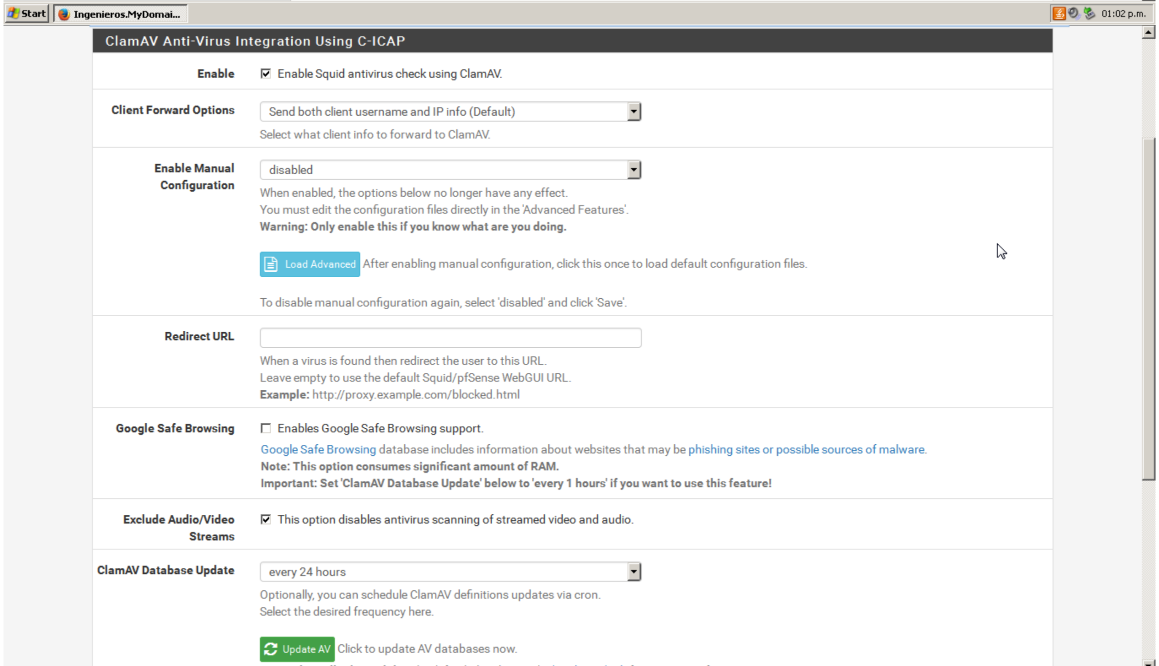


Por último, salvamos la configuración.

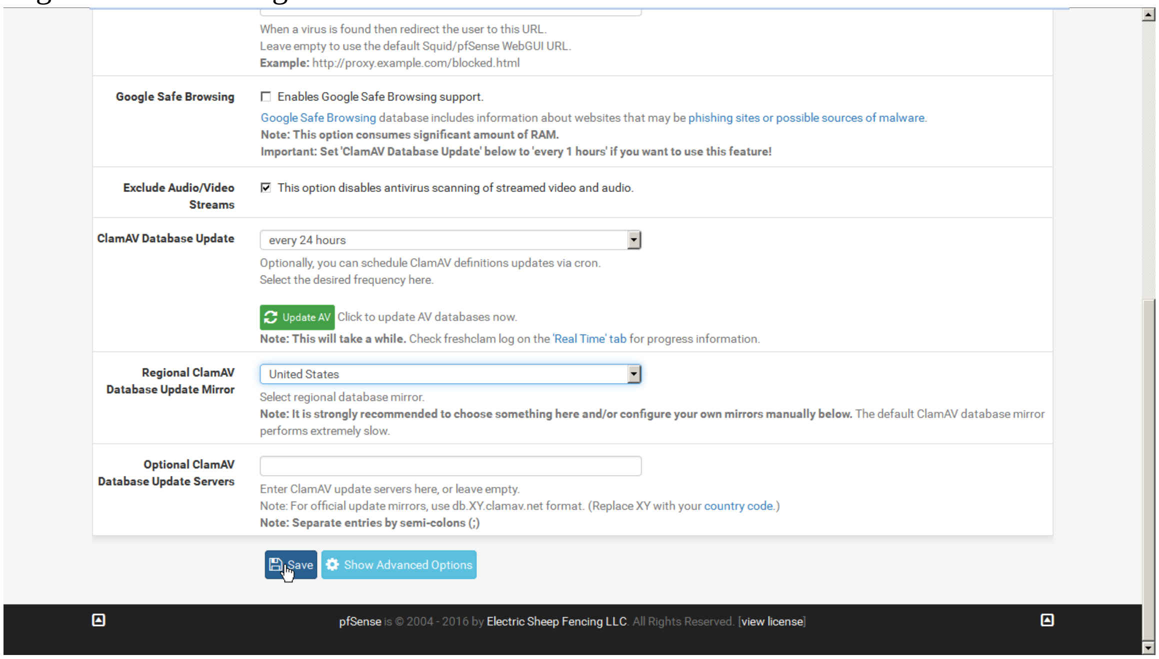


Ahora configuraremos un antivirus para nuestro servidor proxy.

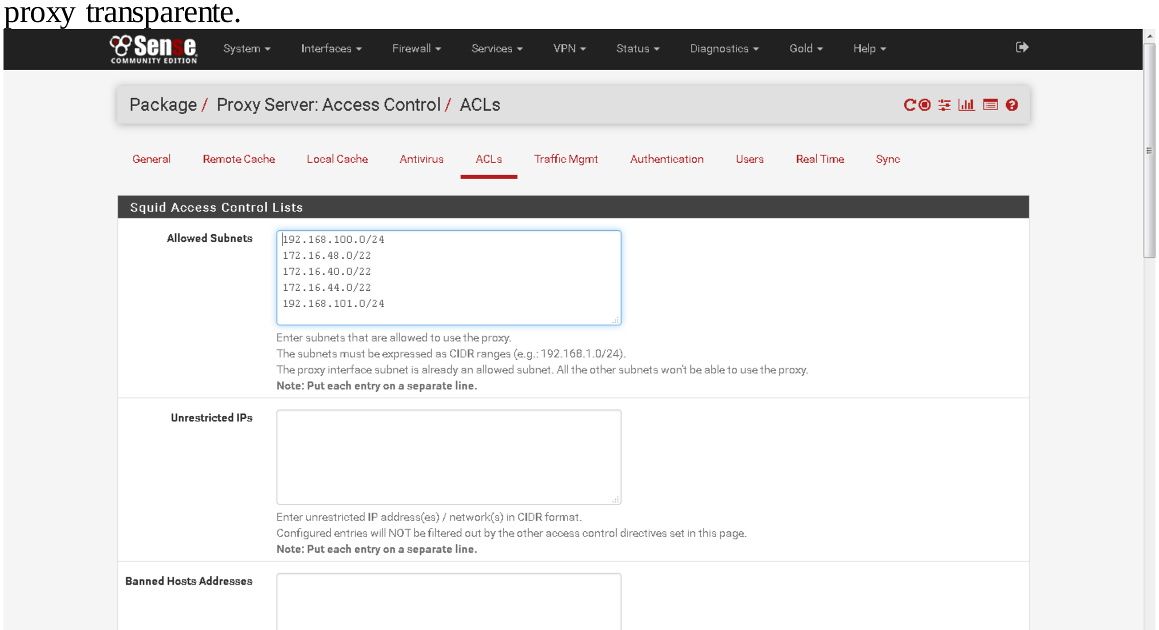




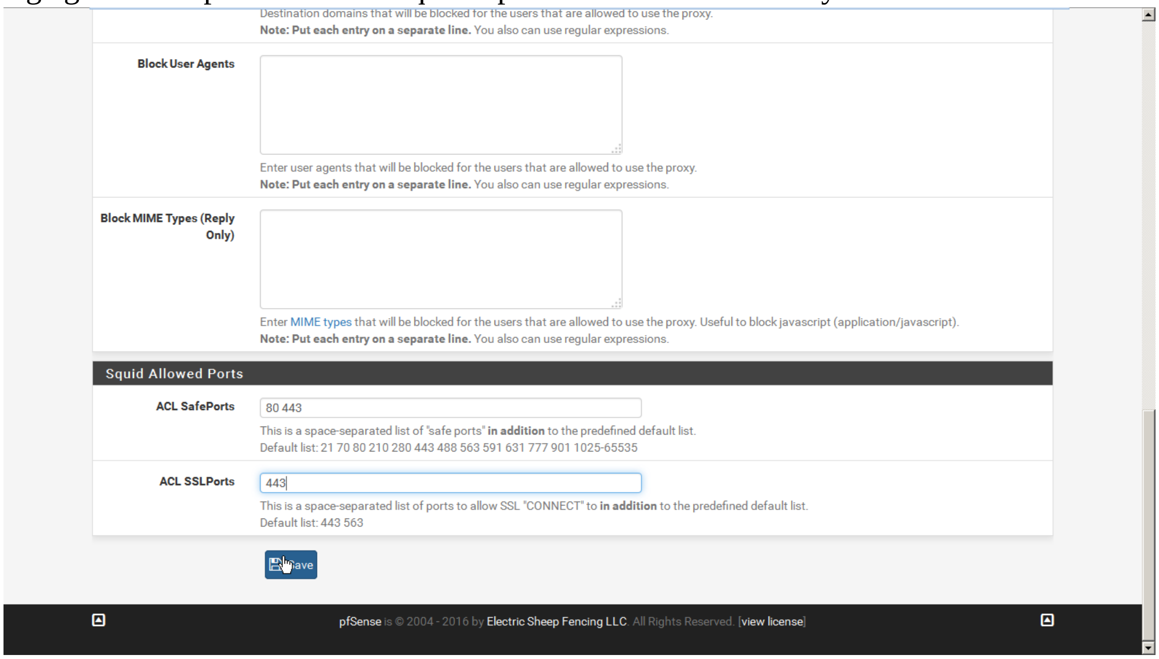
Y guardamos la configuración.



Vamos a la pestaña de ACLs y permitimos las subredes en donde aplicaremos nuestro proxy transparente.

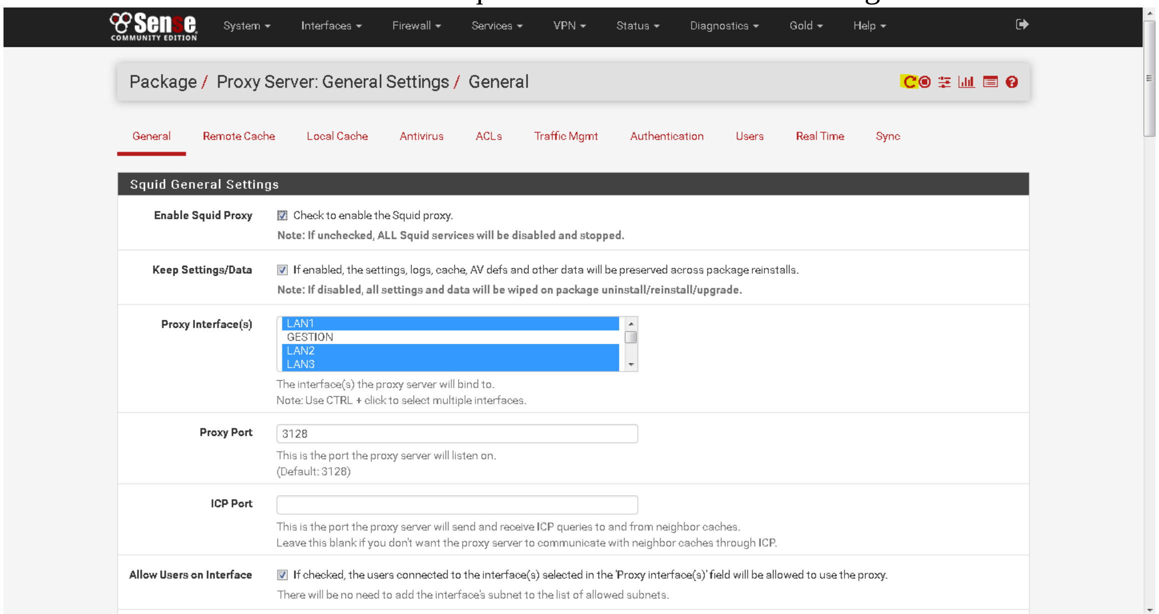


Agregamos los puertos básicos que se permitirán en el servidor y salvamos los cambios.

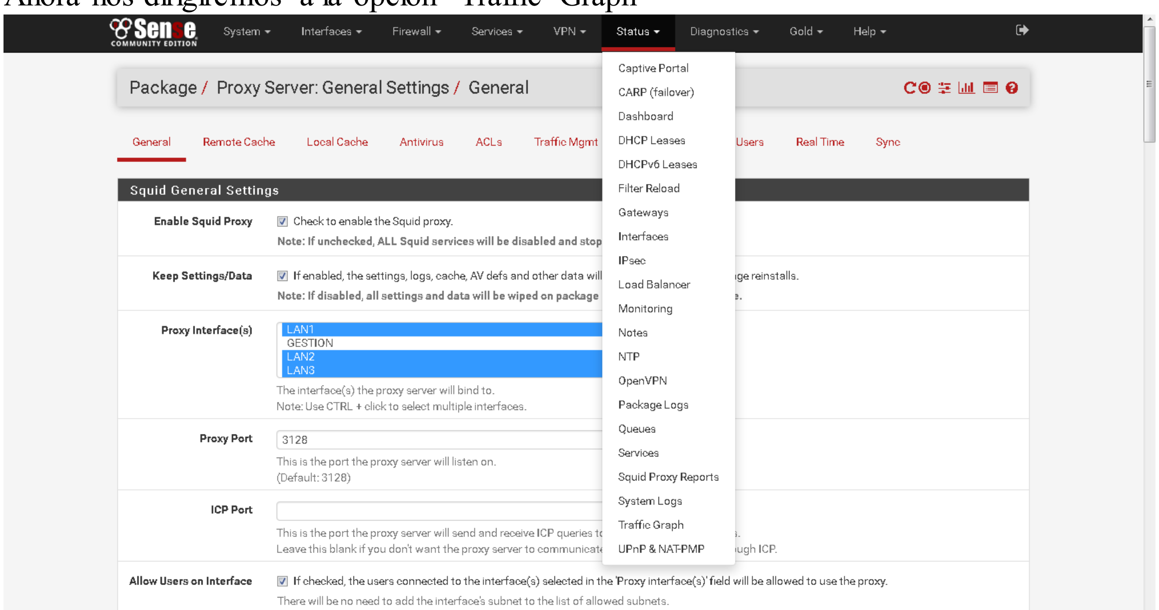


Con esta configuración los usuarios ya deberían poder navegar en internet, para verificar esto nos iremos a la pestaña "Real time", desde acá podemos administrar y observar a qué tipo de páginas están accediendo los diferentes usuarios

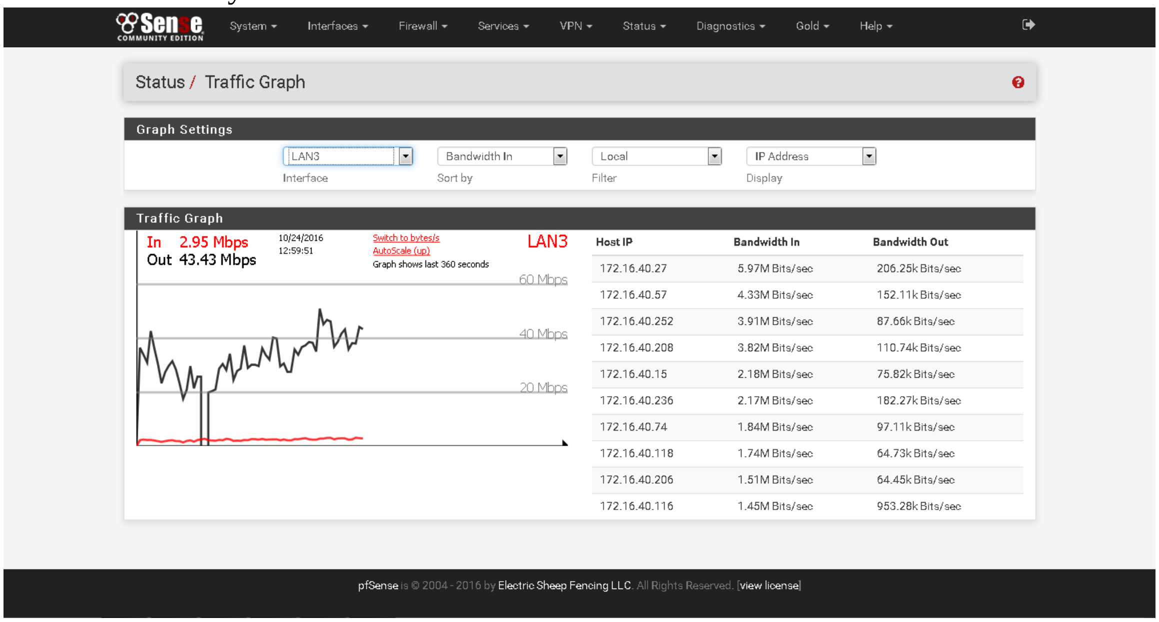
Se recomienda reiniciar el servicio squid una vez finalizada la configuración.



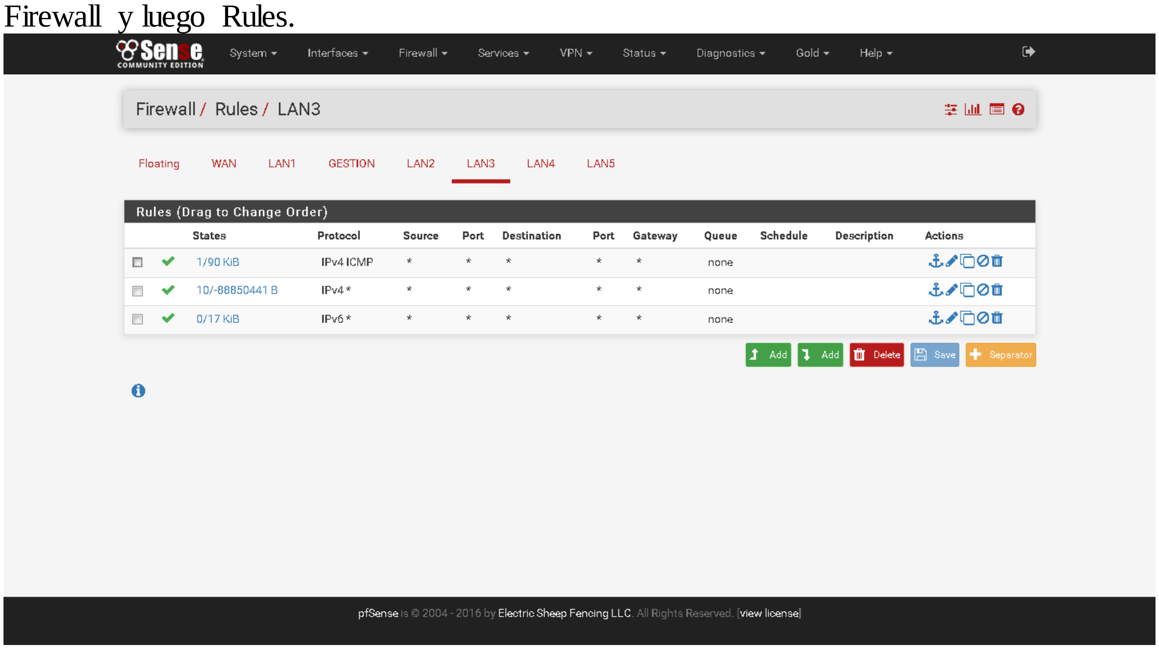
Ahora nos dirigiremos a la opción "Traffic Graph"



En esta sección nos encontraremos con tablas en donde podemos analizar los diferentes usuarios que están accediendo por las diferentes redes, además de analizar anchos de banda de entrada y salida.



Ahora nos iremos para el apartado de Firewall, en donde observaremos las reglas básicas para permitir tráfico y navegación en las diferentes redes, para hacer esto iremos a Firewall y luego Rules.



Significados en Pfsense

Se destacan en el proxy transparente pfsense las opciones más importantes, su respectiva traducción y explicación, las demás opciones no se destacan ya que son opciones por defecto:

- Enable Squid Proxy: Marcar para habilitar el squid proxy, si no se marca, todos los servicios de squid estarán deshabilitados y detenidos.
- Keep Settings/Data: Si se marca, los ajustes, registros, caché, antivirus y otros datos serán preservados a través de la reinstalación de paquetes, si está desactivada, todos los ajustes y los datos serán eliminados en el paquete de desinstalación / reinstalación / actualización.
- ICP Port: Este es el puerto del servidor proxy enviará y recibirá las consultas ICP hacia y desde cachés vecinas, dejar en blanco si no desea que el servidor proxy se comunique con cachés vecinas mediante ICP.
- Allow Users on Interface: Si se selecciona, los usuarios conectados a la interfaz seleccionada en el campo de “Proxy interface(s)” se permitirán para usar el proxy, no habrá necesidad de añadir la subred de interfaces a la lista de subredes permitidas.
- Resolve DNS IPv4 First: habilitar esto para forzar la búsqueda de DNS IPv4 primero, esta opción es muy útil si tienes problemas accediendo a sitios HTTPS.
- Disable ICMP: Activar esto para desactivar la ayuda de ping ICMP squid.

- Bypass Proxy for Private Address Destination: No reenviar el tráfico a destino de espacio a direcciones privadas (RFC 1918), destinos en espacio de direcciones privadas son pasadas directamente a través del firewall, no a través del servidor proxy.
- Enable Access Logging: Esto permitirá el acceso al registro, advertencia: no activar si la capacidad del disco es baja.
- Rotate Logs: define cuantos días de los archivos de registro se mantendrán. La rotación se desactiva si se deja vacío.
- Error Language: Seleccione el idioma en el que el servidor proxy mostrará los mensajes de error a los usuarios.
- X-Forwarded Header Mode:

  On: Squid anexará la dirección IP en la solicitud reenviar HTTP. El encabezado parece: X-Forwarded-For: 192.1.2.3.

  Off: Squid no anexará la dirección IP del cliente en la solicitud reenviar HTTP. El encabezado parece: X-Forwarded-For: unknown

  Transparent: Squid no alterará el encabezado de ninguna manera.

  Delete: Squid eliminará todo el encabezado.

  Truncate: Squid eliminará todas las entradas de encabezado existentes X-Forwarded-For y coloca la dirección IP como la única entrada de encabezado.
- URI Whitespace Characters Handling: Identificador uniforme de recursos (URI), es una cadena corta de caracteres que identifica inequívocamente un recurso (servicio, página, documento, dirección de correo electrónico, enciclopedia, etc).

Normalmente estos recursos son accesibles en una red o sistema basado en el Protocolo IP.

Strip: Los espacios en blanco son despojados de la URI. Este es el comportamiento recomendado por RFC 2396.

Deny: La solicitud es denegada. El usuario recibe un mensaje de "solicitud inválida".

Allow: Se deja que la solicitud y la URI no se cambie. Los espacios en blanco permanecen en el URI.

Encode: e permite que la petición y los espacios en blanco estén codificados de acuerdo con RFC 1738.

Chop: Se permite que la solicitud y la URI se corte en el primer espacio en blanco.

- Cache Replacement Policy: La política de sustitución de caché decide qué objetos permanecerán en la memoria caché y qué objetos se sustituyen para crear espacio para los nuevos objetos.

  Heap LFUDA: Mantiene los objetos populares en la memoria caché, independientemente de su tamaño y por lo tanto optimiza la tasa de éxito de bytes a expensas de la tasa de éxito.

  Heap GDSF: Permite optimizar el índice de aciertos a objetos manteniendo los objetos más pequeños, objetos populares en la memoria caché.

  Heap LRU: Funciona como LRU, pero utiliza un montón en su lugar.

LRU: Mantiene recientemente objetos referenciados (es decir, sustituye el objeto que no ha sido visitado por más tiempo).

- Do Not Cache: Introduzca dominio (s) y / o dirección IP (es) que nunca deben ser almacenados en caché.
- Hard Disk Cache Size: Cantidad de espacio en disco (en megabytes) que se utilizará para los objetos almacenados en caché (no usar más del 50% de la memoria total de nuestro servidor ya que squid siempre en su momento puede usar mas).
- Hard Disk Cache System: Esto especifica el tipo de sistema de almacenamiento de usar.

  ufs: El viejo conocido formato de almacenamiento de squid que siempre ha estado allí.
- Minimum Object Size: Los objetos más pequeños que el tamaño especificado (en kilobytes) no se guardarán en el disco, por defecto: 0 (es decir, no hay un mínimo).
- Memory Cache Size: Especifica la cantidad ideal de RAM física (en megabytes) que se utilizará para los objetos en tránsito, objetos calientes y objetos en caché negativo, este valor no debe exceder de 50% de la RAM instalada. El valor mínimo es de 1 MB.
- Maximum Object Size in RAM: Objetos mayores que este tamaño (en kilobytes) no se intentarán de mantener en la memoria caché, por defecto: 256 (KB).

- Memory Replacement Policy: La política de sustitución de memoria determina qué objetos se limpian de la memoria cuando se necesita espacio.

  Heap GDSF: Permite optimizar el índice de aciertos a objetos manteniendo los objetos más pequeños, objetos populares en la memoria caché.

  Heap LFUDA: Mantiene los objetos populares en la memoria caché, independientemente de su tamaño y por lo tanto optimiza la tasa de byte de éxito a expensas de la tasa de éxito.

  Heap LRU: Funciona como LRU, pero utiliza un montón en su lugar.

  LRU: Mantiene recientemente objetos referenciados (es decir, sustituye el objeto que no ha sido visitado por más tiempo). La política de sustitución de memoria determina qué objetos se limpian de la memoria cuando se necesita espacio.

Título 2

Usa los subtítulos consistentemente. Revisando constantemente el espaciado, mayúsculas y puntuación.

Título 3. El uso de estilos es de ayuda a la hora de generar una tabla de contenidos. Este documento de ejemplo usa los títulos, subtítulos y demás estilos para generar automáticamente la tabla de contenido, lista de tablas y lista de figuras. Este documento está configurado para seguir las normas APA.

Título 3. Acá puede ir otra idea del documento.

Capítulo 2

Usuarios y contraseñas

Nombre-Sistema Operativo	Usuario	Contraseña
Vmware ESXi-Vmware ESXi 5.5		
Proxy Pfsense-Pfsense 2.3.2		