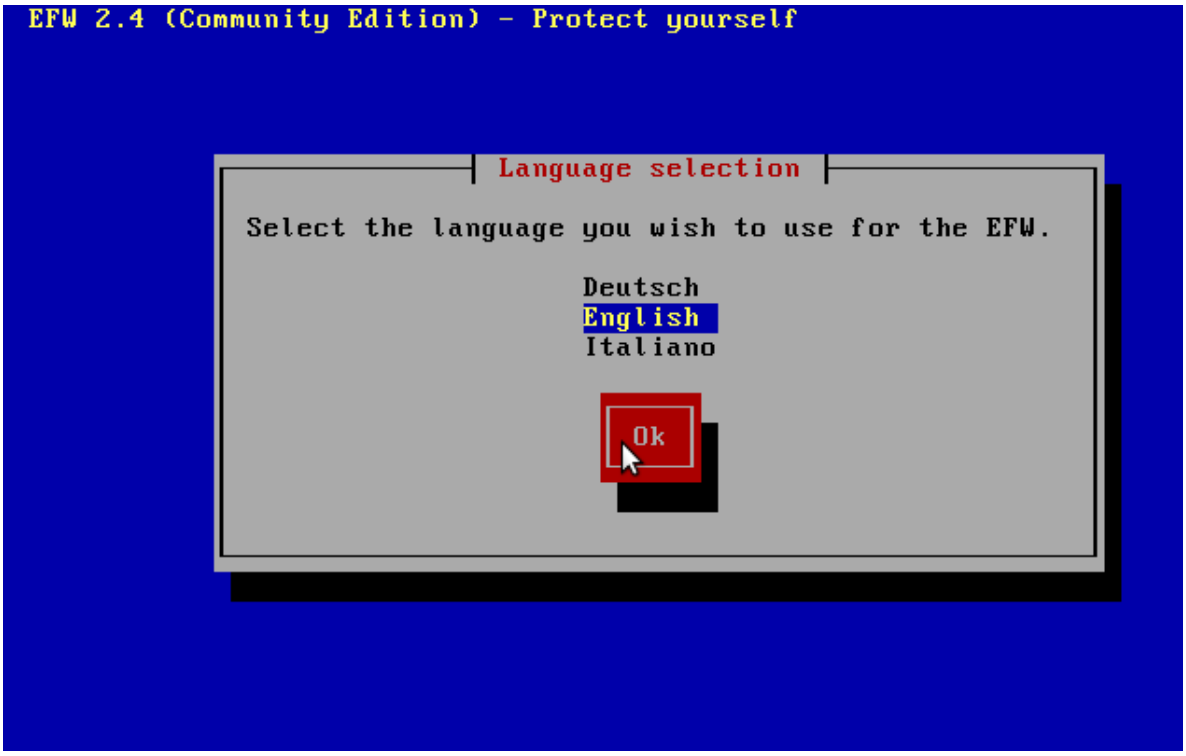
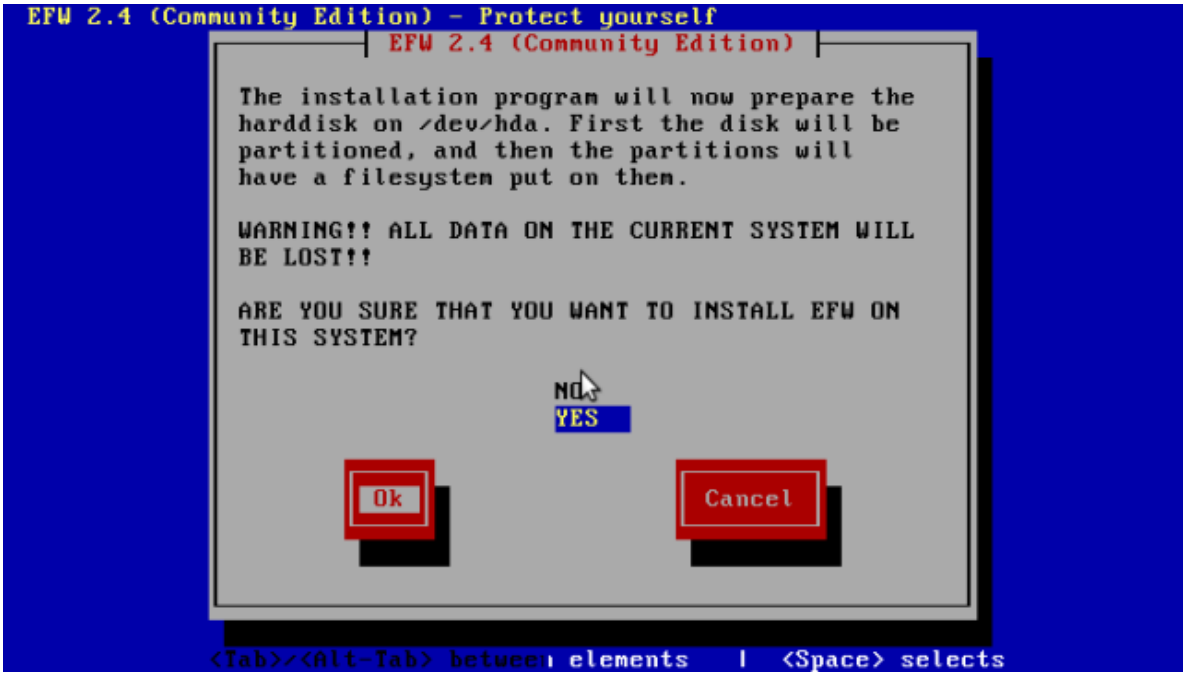
instalación de Endian

Comenzamos la instalación, podemos dar enter directamente o esperar unos segundos para que arranque el wizard de instalación. después de este nos salta una imagen donde elegimos el idioma.

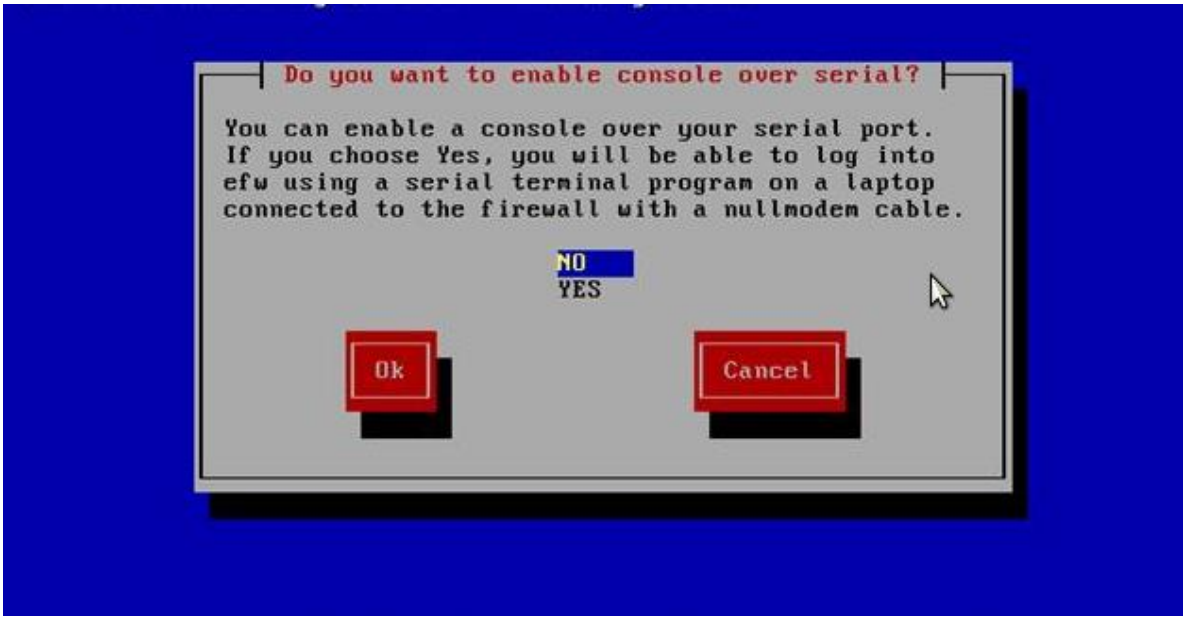


A continuación, nos mostrara un mensaje de bienvenida para la instalación de Endian

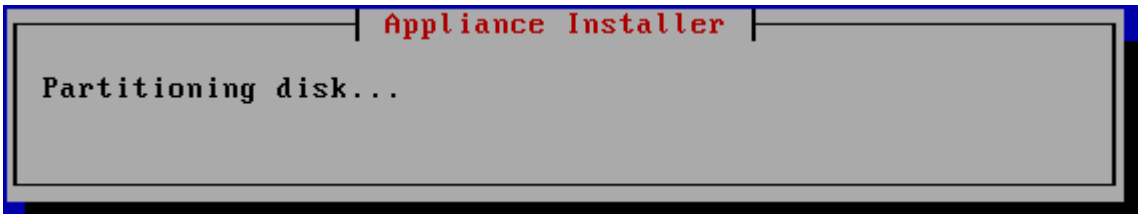
después nos aparece una advertencia, la cual especifica que proceso de instalación borrara todos los datos que contenga el disco duro, si deseamos continuar seleccionamos YES

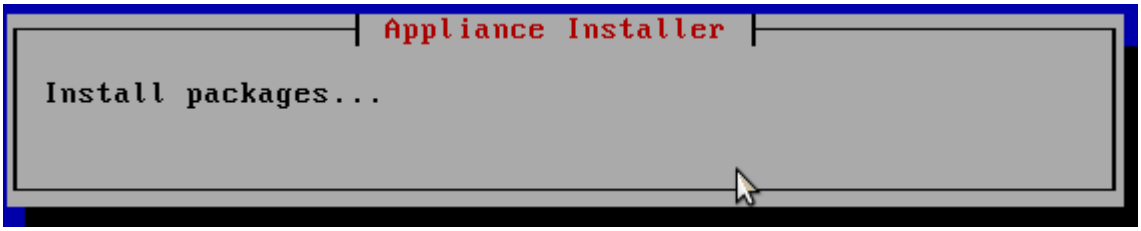


La siguiente pantalla nos ofrece la posibilidad de activar el servicio de Consola, esta opción la debemos elegir según nuestras necesidades.

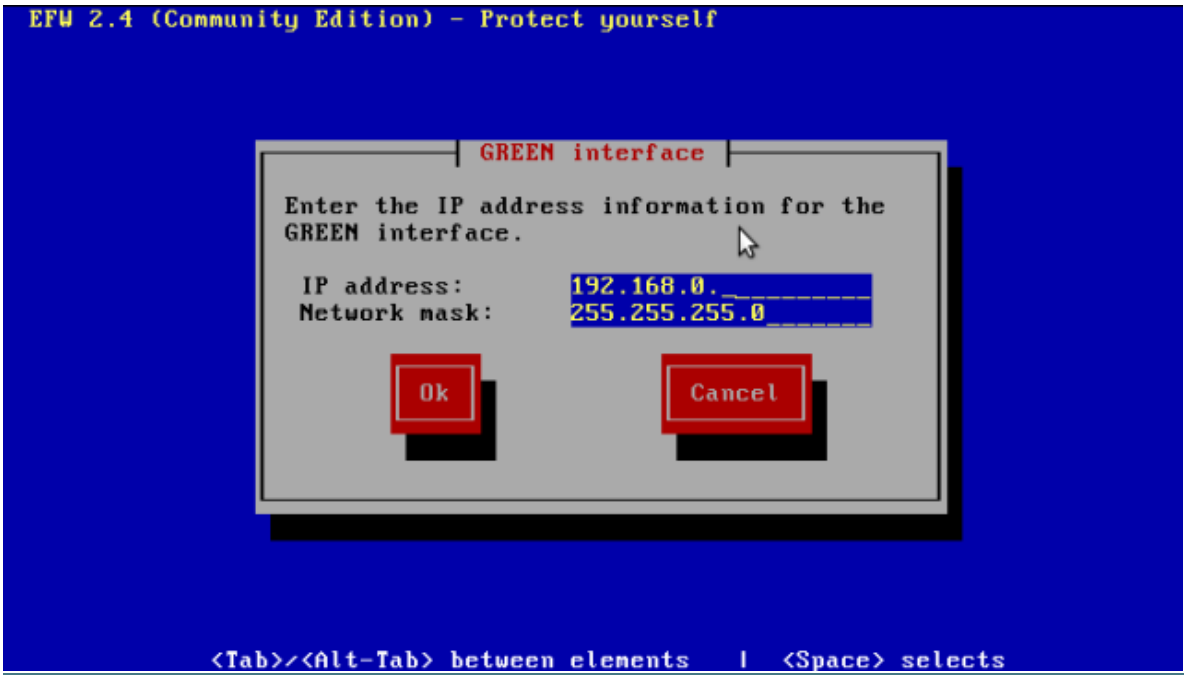


Ahora Endian comenzara a instalarse en nuestro disco duro, y podemos ver que nos irán saliendo mensajes como los siguientes.

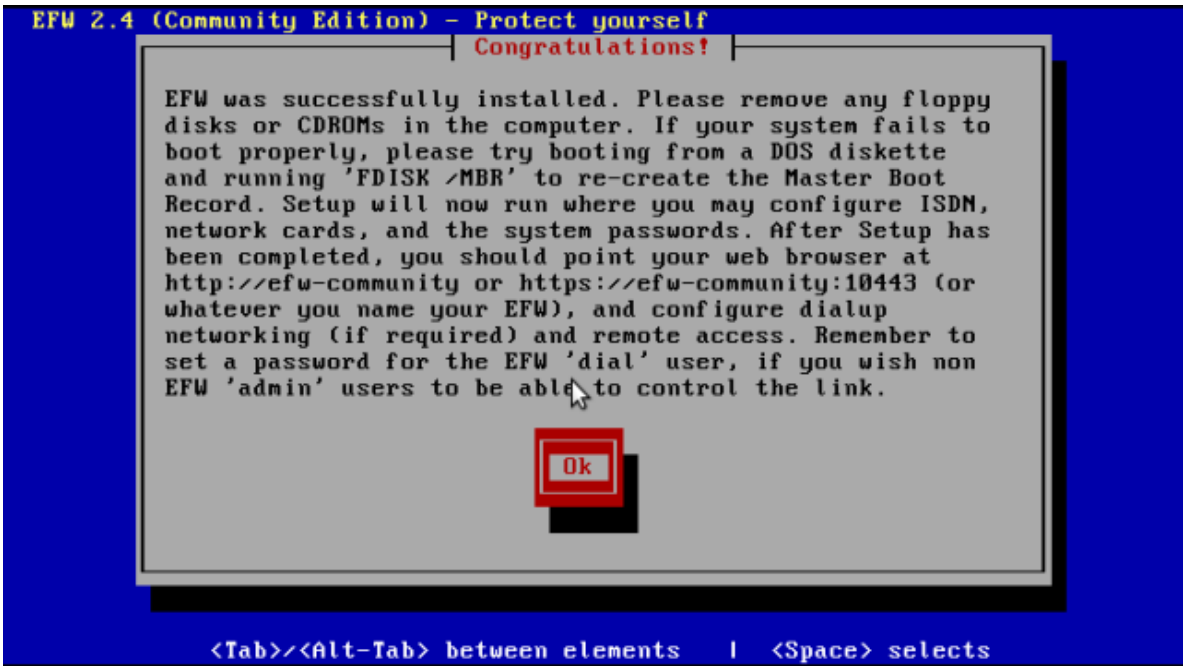




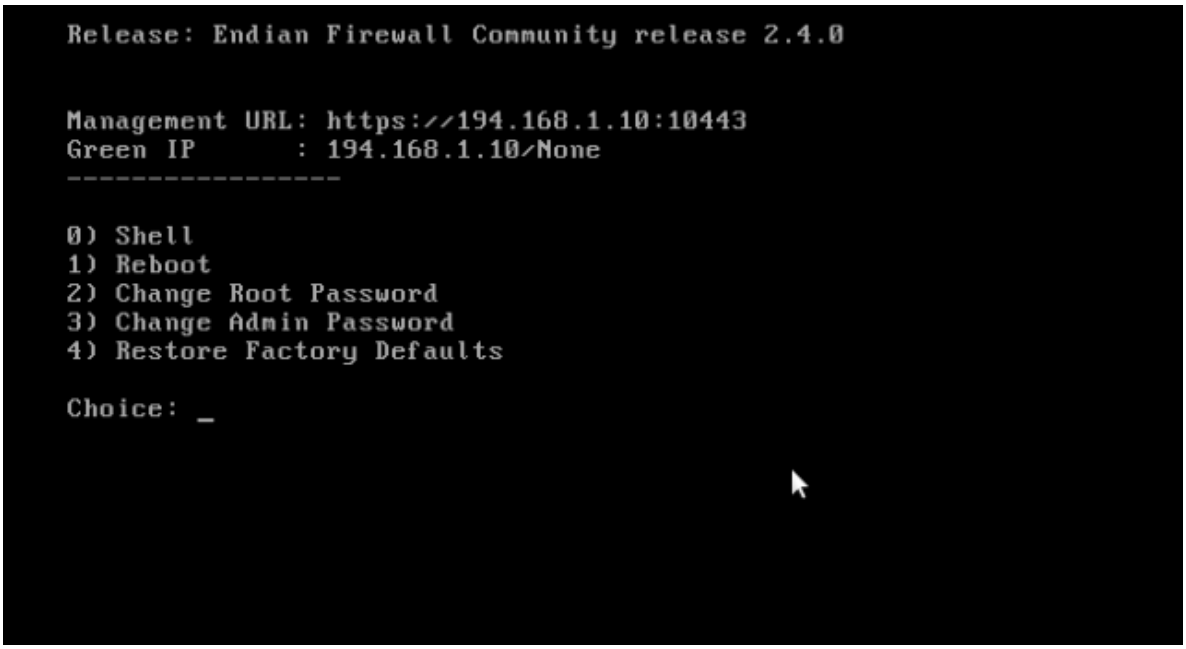
después del proceso de instalación, nos aparece una pantalla en la cual debemos de configurar la dirección IP de la interfaz de red local (GREEN) para posteriores configuraciones de Endian mediante el navegador web.



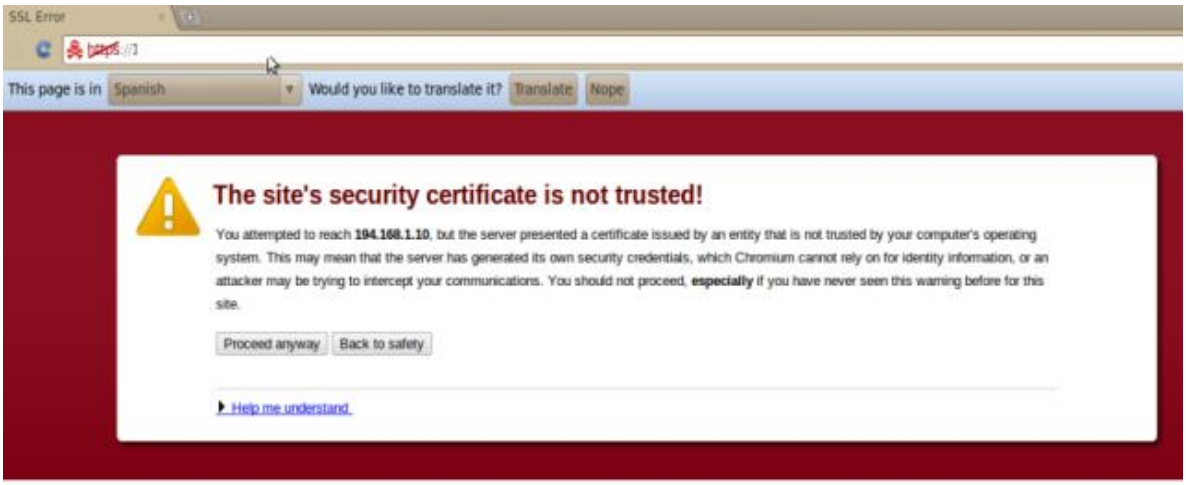
Para finalizar el proceso de instalación, se nos recomienda quitar cualquier diskette o CD-ROM que aún se encuentre insertado, damos OK para que el sistema se reinicie



después de que Endian se reinicie por completo nos aparece la siguiente pantalla en la cual podemos elegir las diferentes opciones según nuestro criterio.
Nota: la contraseña del root es endian.

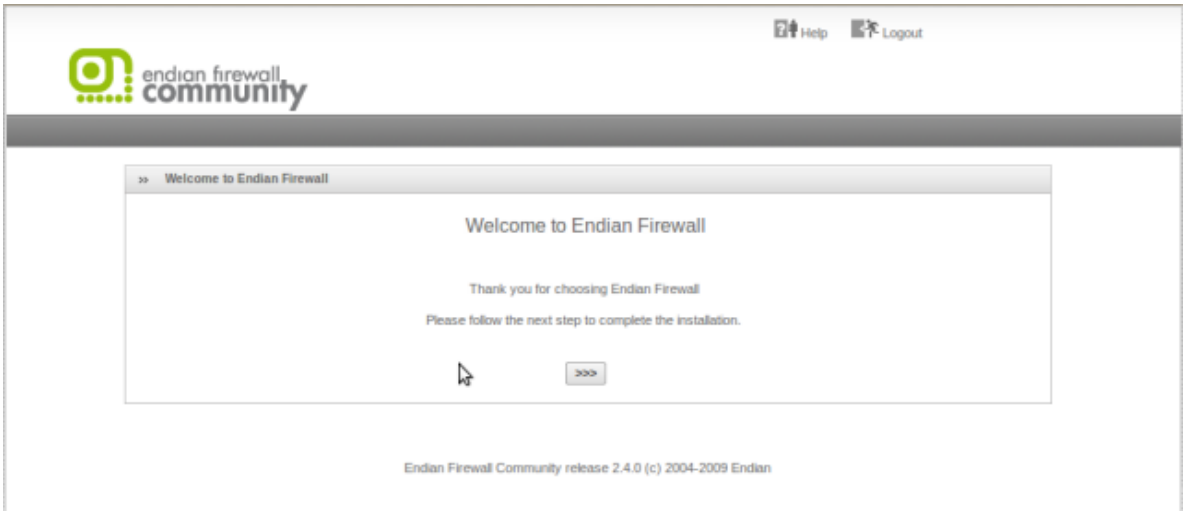


Con un PC que se encuentre dentro del mismo rango de direcciones, abrimos un navegador web y escribimos la dirección IP que le asignamos al servidor Endian.

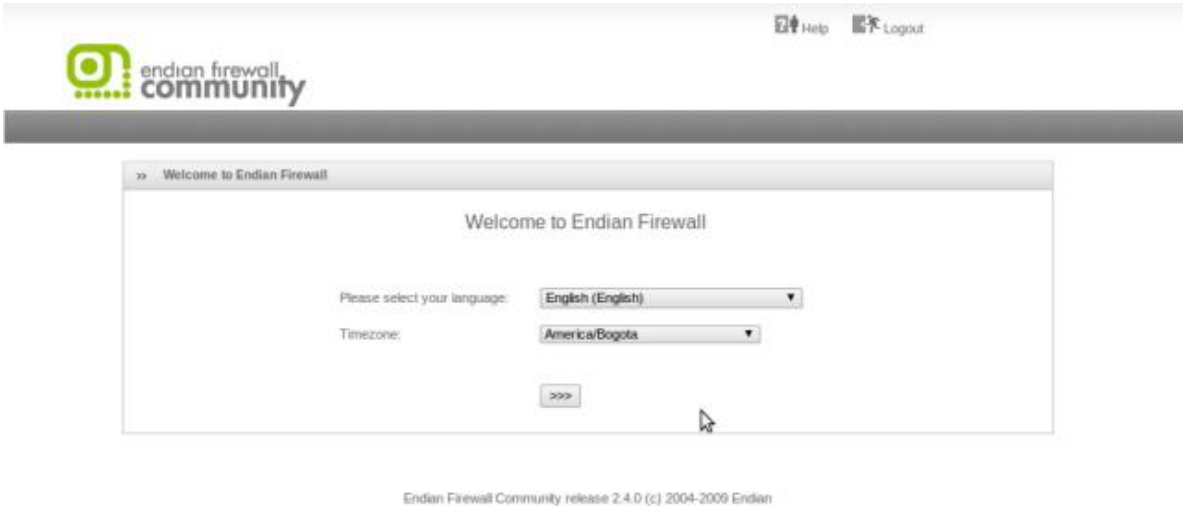


Aceptamos la validacion del certificado de la interfaz web de Endian, para que podamos acceder a la configuracion basica de Endian.

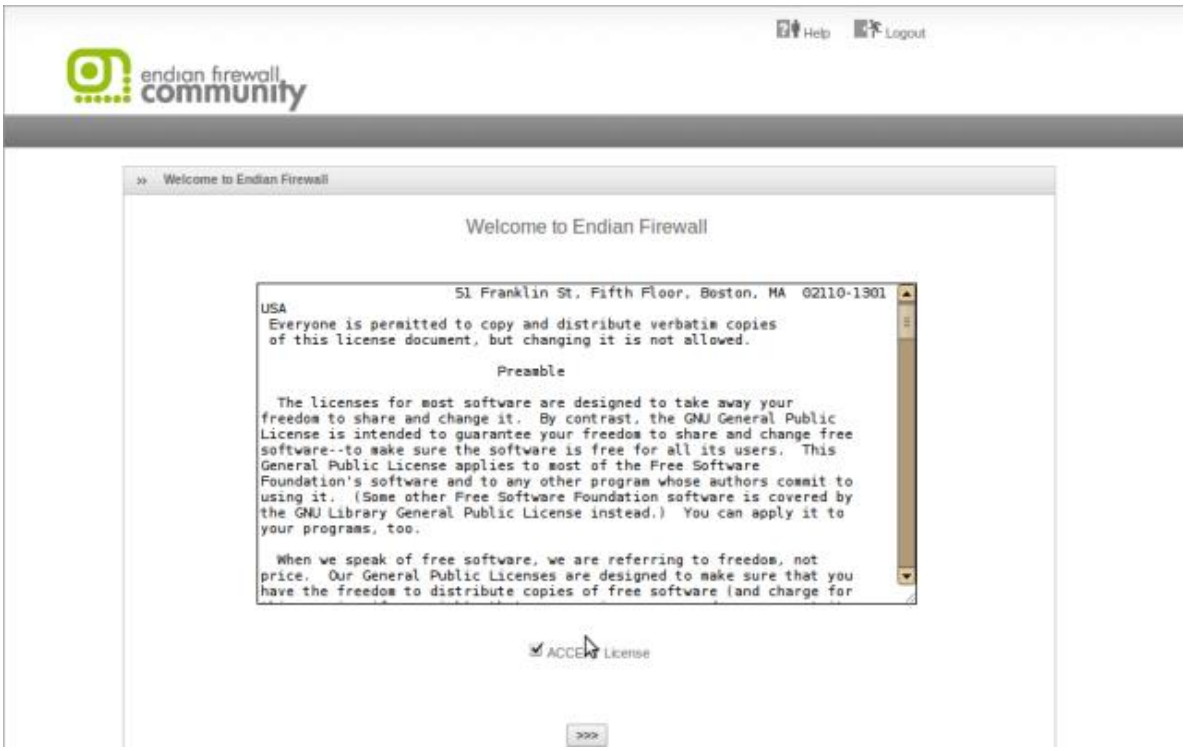
Acontinuacion aparecera la bienvenida a la configuracion de Endian. para continuar damos clic en >>>



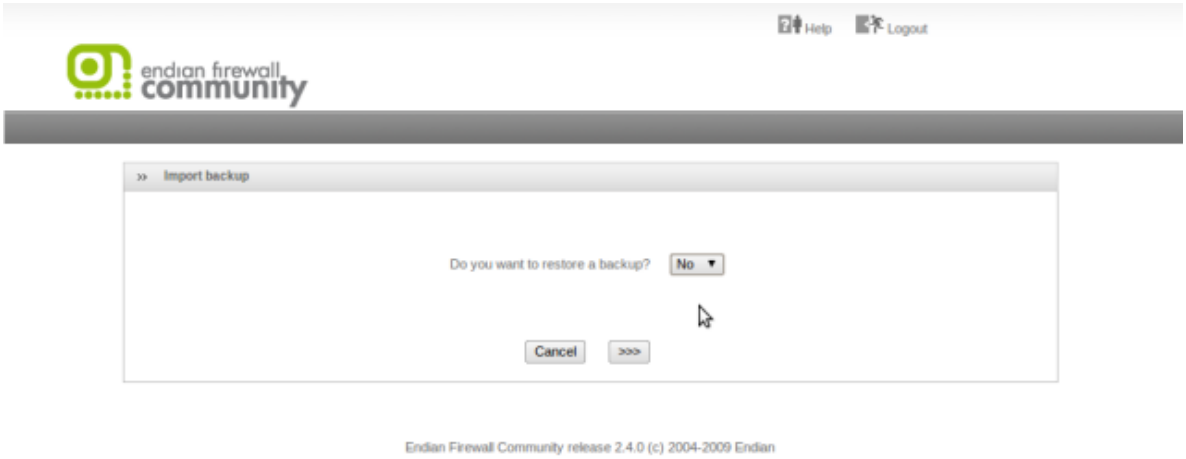
Ahora vamos a escoger el idioma con el cual queremos configurar Endian, tambien tenemos la opcion de configurar la zona horaria segun nuestra ubicacion.



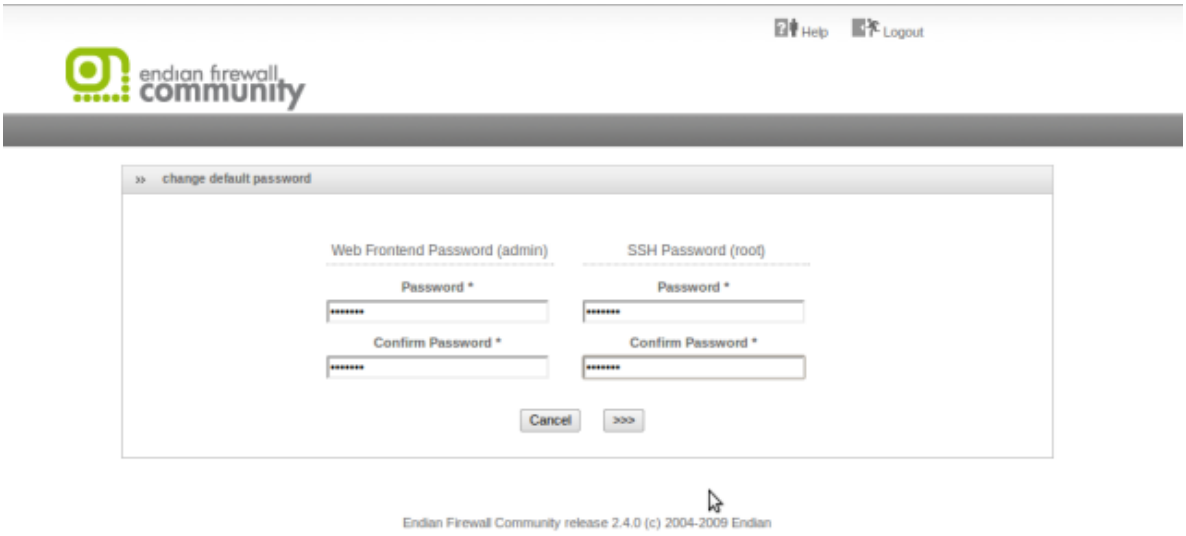
Aceptamos el acuerdo de licencia sobre el uso de Endian



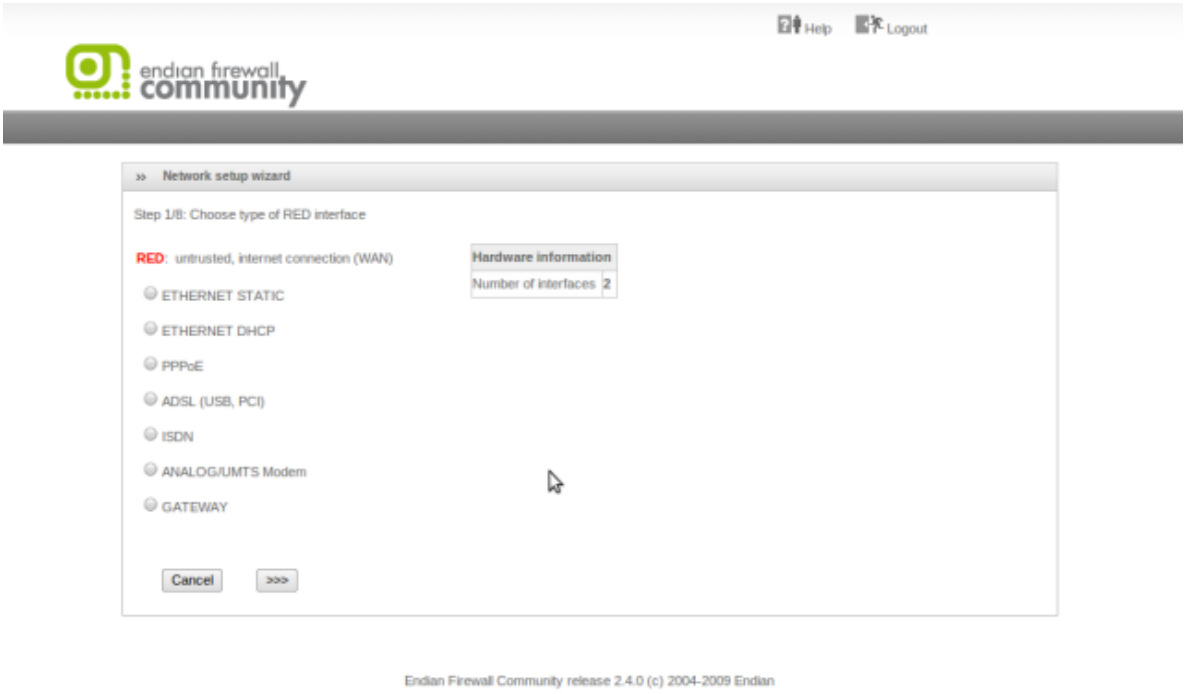
Endian ahora nos pregunta que si queremos restablecer la configuracion desde un archivo de respaldo o backup, pero como es primera vez que lo instalamos entonces dejemos la opcion no y continuamos.



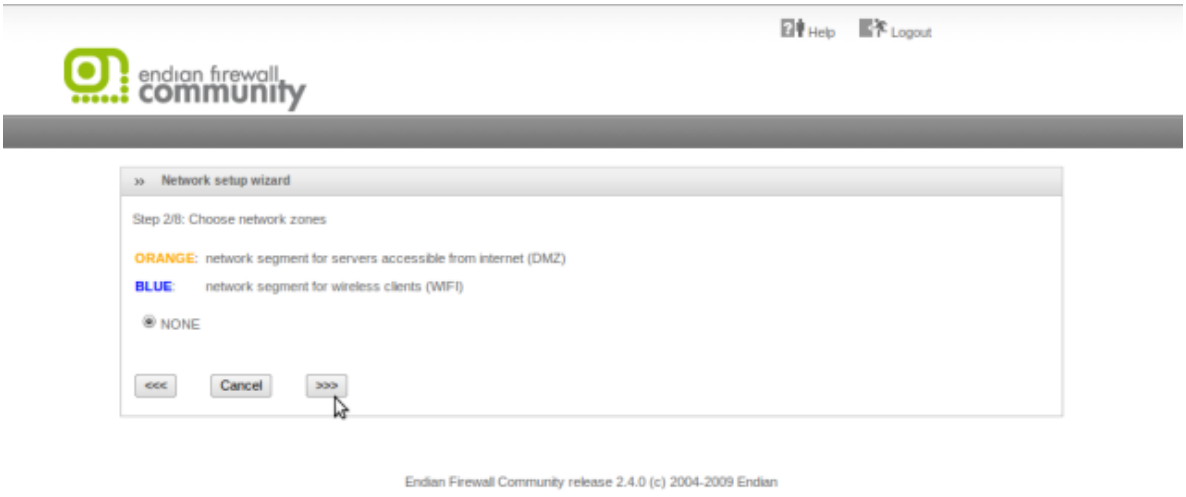
En la siguiente pantalla debemos configurar las contraseñas para la administracion de la interfaz web y del usuario root, cabe recalcar que entre mas seguras sea nuestra contraseñas mas dificil le hacemos el trabajo al atacante.



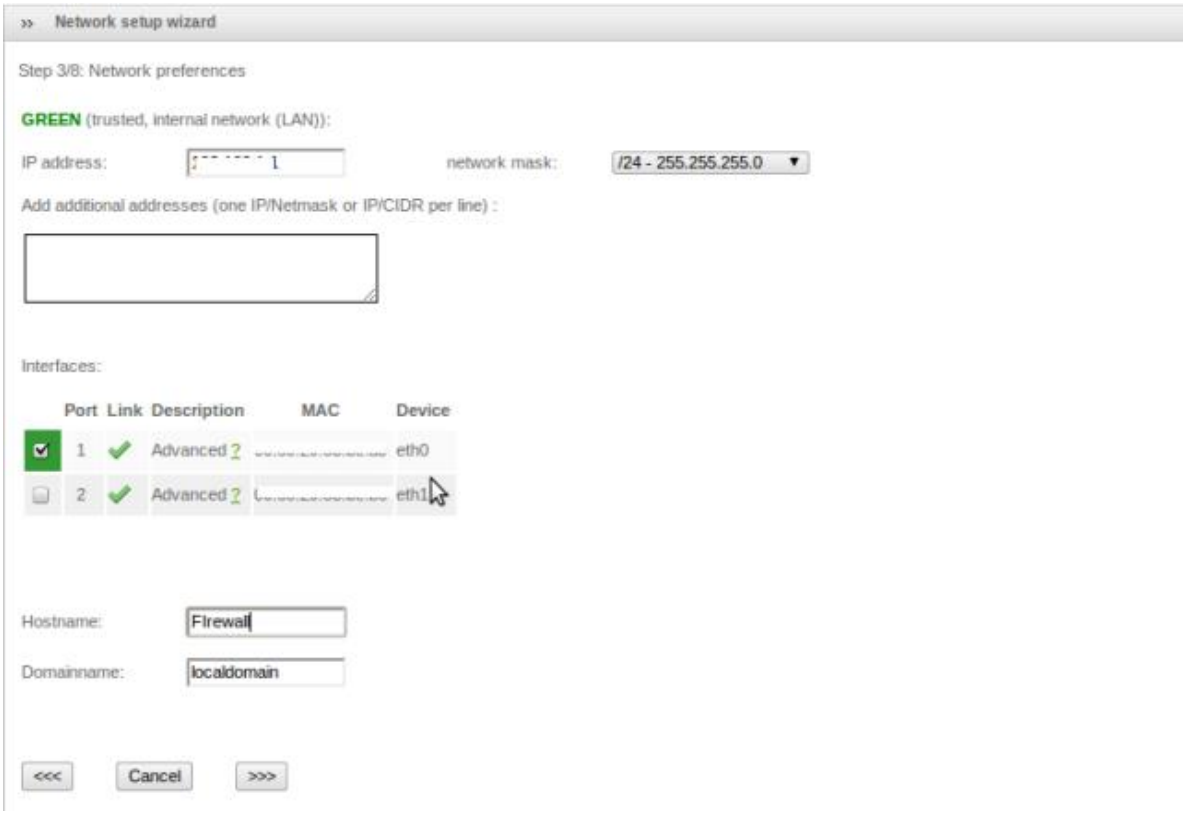
Ahora vamos a configurar el tipo de conexión que tendrá la interfaz o tarjeta de red que va a estar conectada hacia el cable modem. (internet), en el diagrama de la red podemos ver que estamos utilizando 2 tarjetas de red, la primera esta conectada a nuestra LAN (GREEN) y fue la que configuramos antes (recordemos que la configuramos en la instalacion de Endian), la segunda es la que vamos a configurar en este momento (RED), seleccionamos la opcion que mas se ajuste a nuestras necesidades. en este caso escogemos ETHERNET STATIC, al seleccionar esta opcion quiere decir que mas adelante vamos a colocarle una direccion IP a esta interfaz (RED)



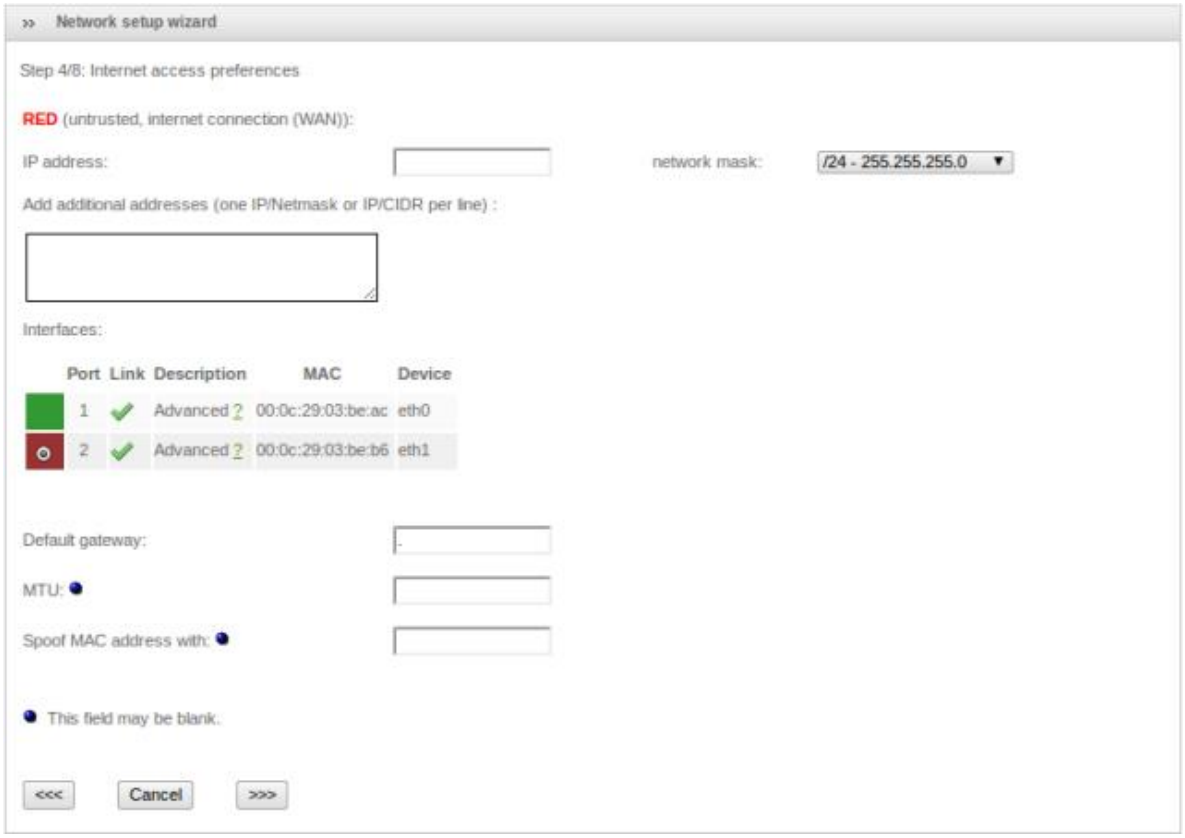
Como nosotros no tenemos mas tarjetas de red, entonces verificamos que este selecionada la opcion NONE y continuamos



En esta pantalla tenemos la opcion de cambiar la direccion IP de la interfaz (GREEN), asignar el direccionamiento a una interfaz de red especifica. asignarle el nombre al servidor y el dominio al cual pertenece.



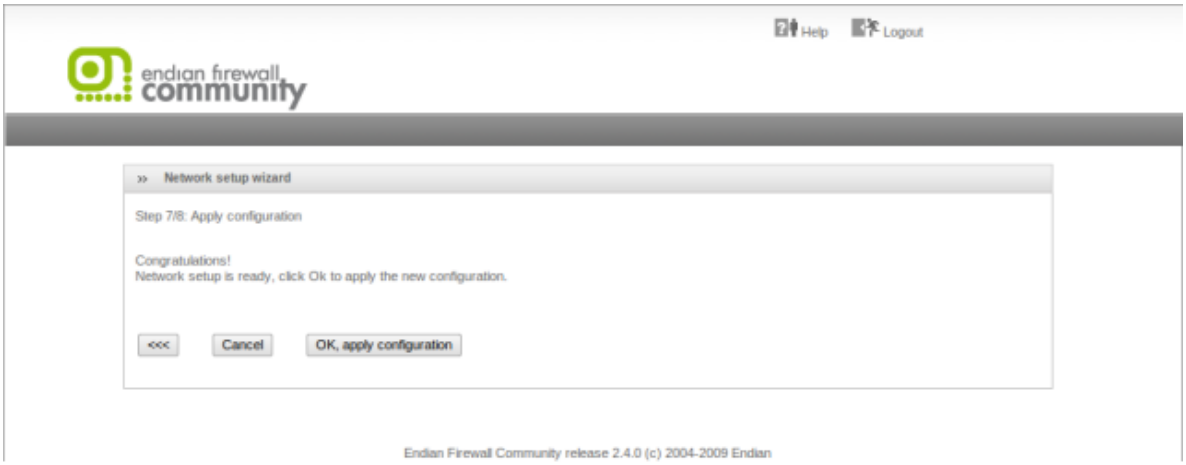
Acontinuacion vemos una imagen similar a la anterior pero en este caso solo vamos a configurar la interfaz de red que da hacia internet (RED), tambien configuramos una direccion IP a la interfaz seleccionada, direccion IP del gateway entre otras opciones.



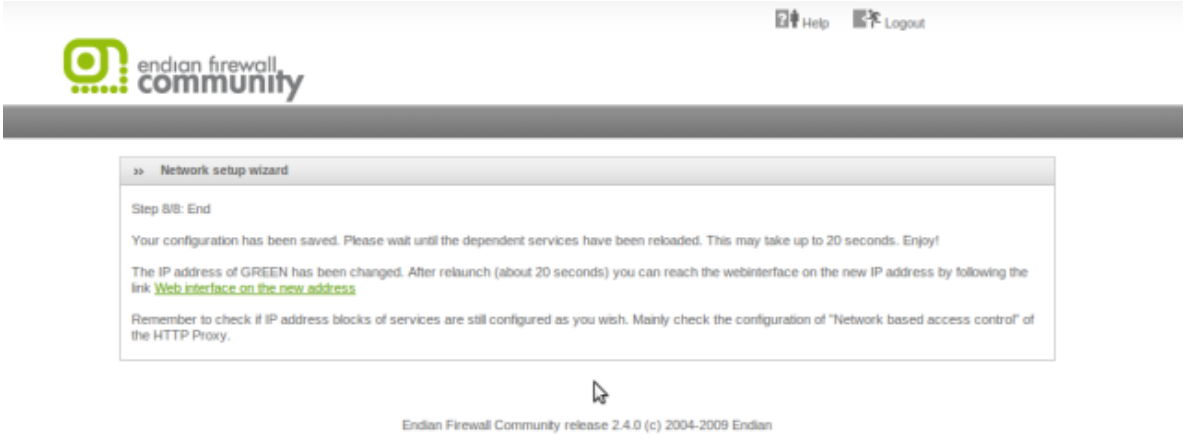
Ahora escribimos las direcciones IP de nuestros servidores DNS en el caso de que contemos con ellos de los contrario debemos colocar unos externos

Despues Endian nos pedira alguna informacion acerca del administrador, con el fin, de enviar por correo alarmas y reestablecer contraseñas

Ya en este paso Endia va a aplicar y grabar los cambios y/o configuraciones previamente hechas para esto damos clic en OK

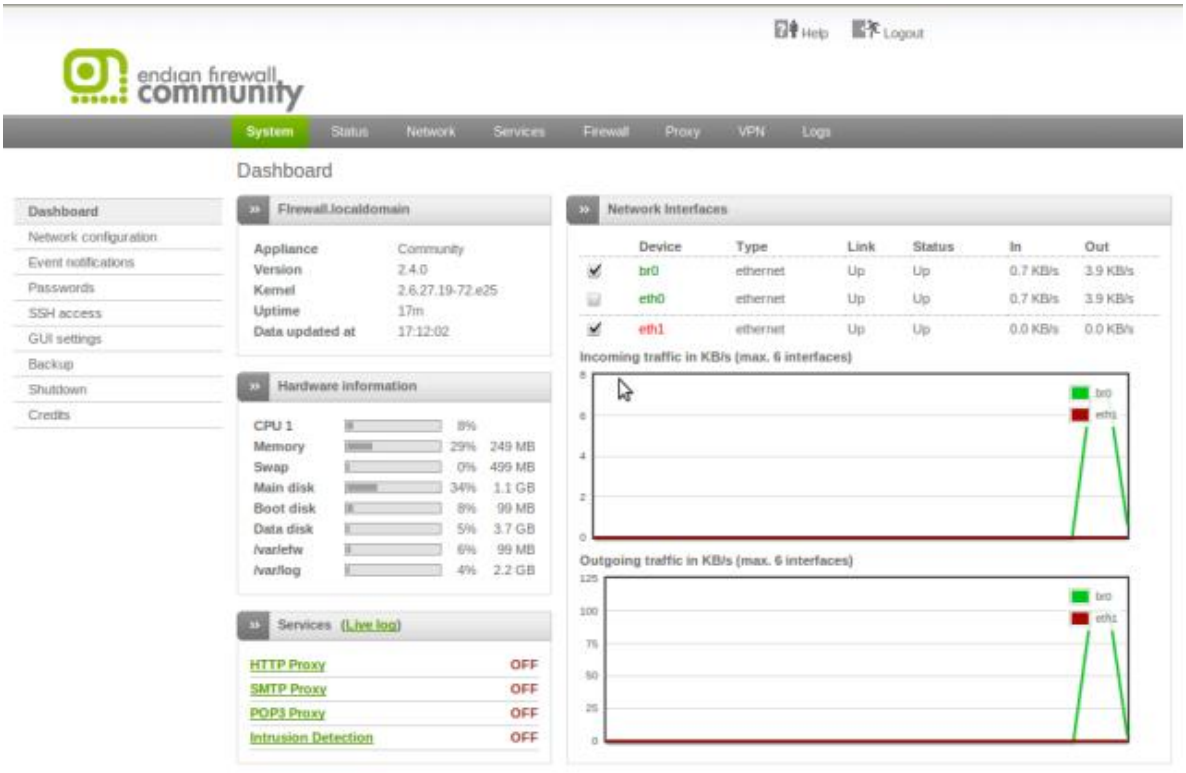


Despues de haber aplicado todas las configuracion previamente hecha, nuestro servidor se reiniciara automaticamente esto tarda unos minutos.



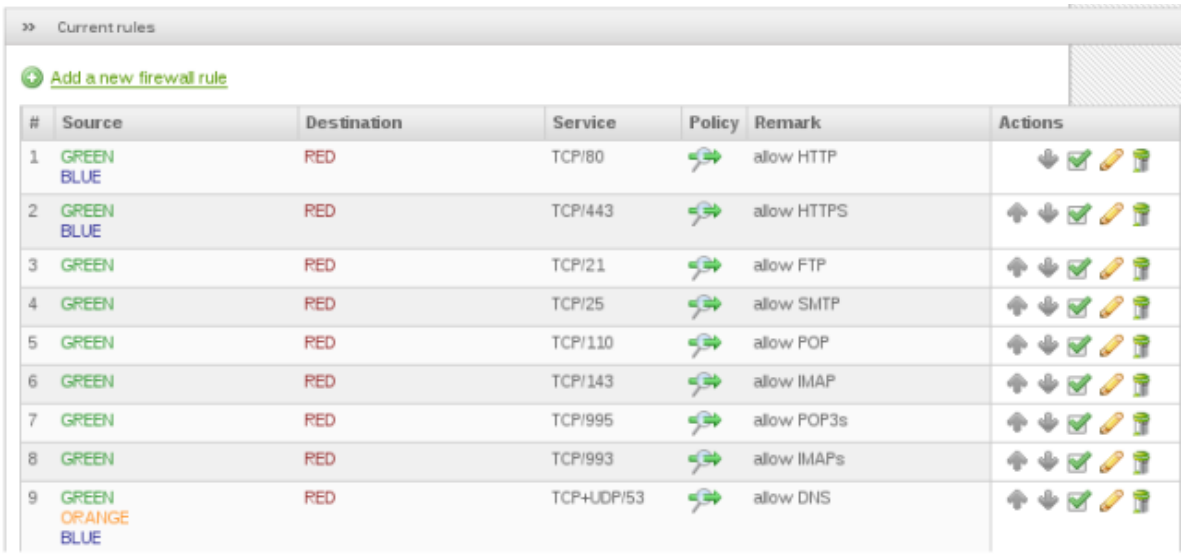
Ya reiniciado nuestro servidor volvemos a entrar la direccion IP de nuestro servidor via web y como podemos ver en la pantalla nos esta pidiendo una autenticacion, el usuario es admin y la contraseña que nosotros escogimos para este usuario.

Podemos ver que ingresamos a la consola de administracion de Endian, recordemos que podemos configurar todos los aspectos que estan nombrados en las caracteristicas mencionadas anteriormente



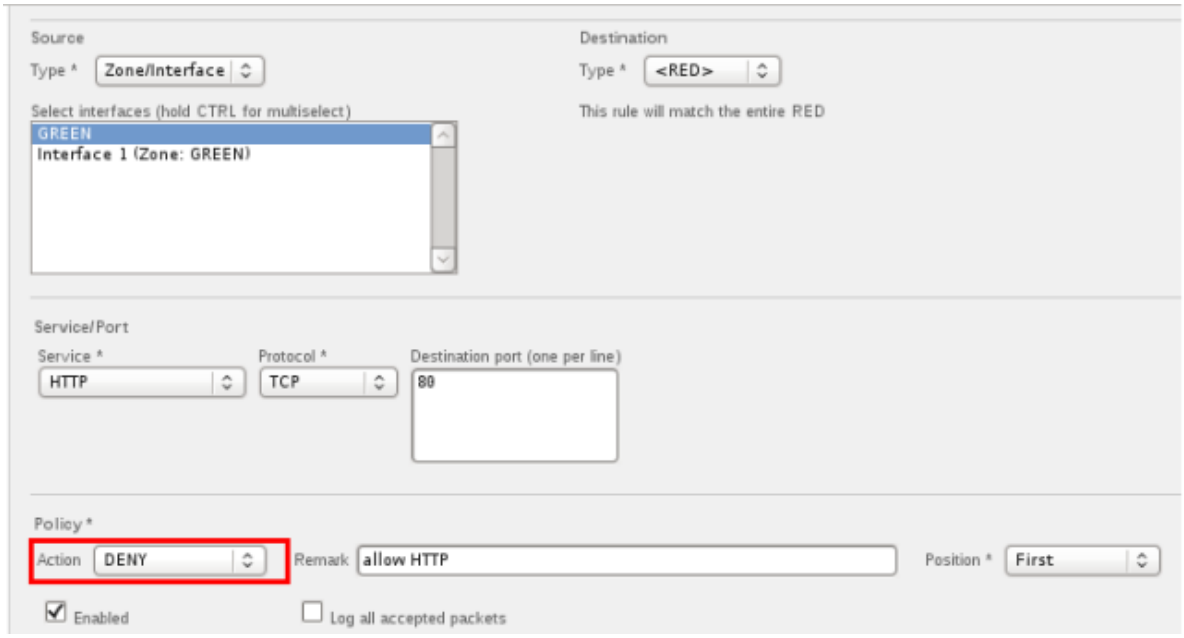
Ahora voy hacer unas pruebas poniendo una maquina virtual y simulando estar en la red interna, por defecto en el firewall Endian esta permitido todo el trafico, verificamos que esto sea correcto, entonces navegamos hacia nuestro gran amigo.

Acontinuacion vamos a dar clic en la pestaña firewall y en la opcion de trafico saliente podemos ver la reglas por defecto que trae el firewall.

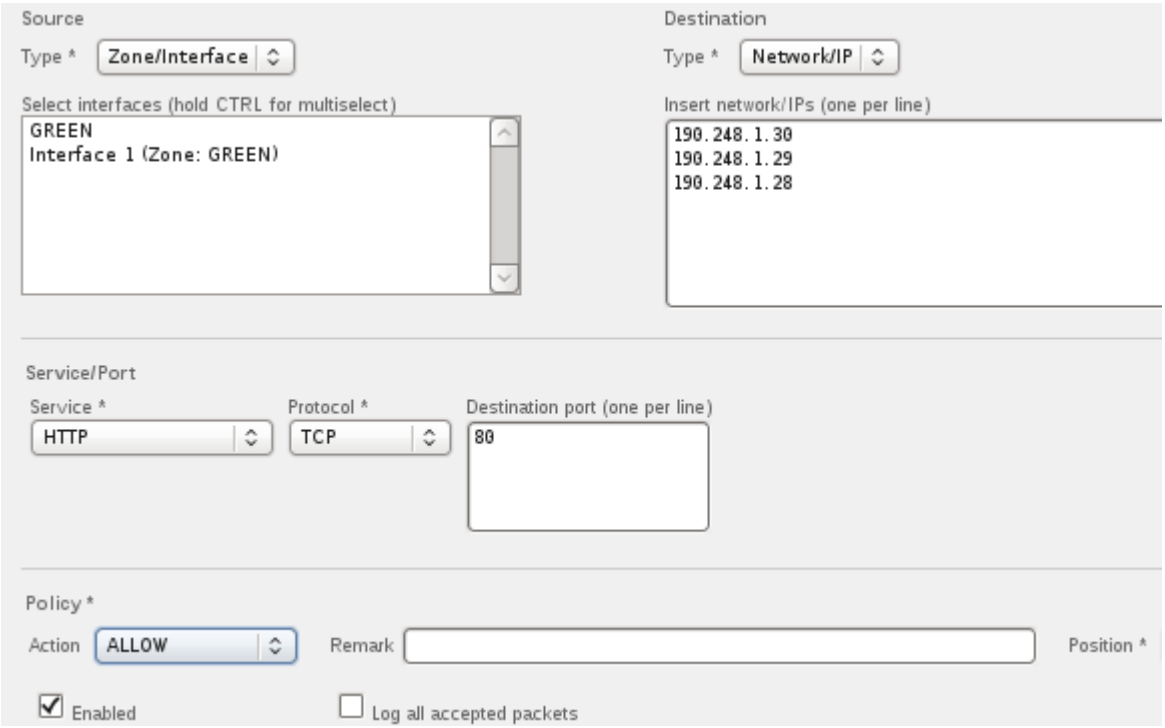


Voy a cambiar la regla primera regla de la lista, esta me permite navegar desde mi red local hacia internet, se va a denegar todo por defecto y despues creamos una regla que me permita ingresar donde nuestro gran amigo.

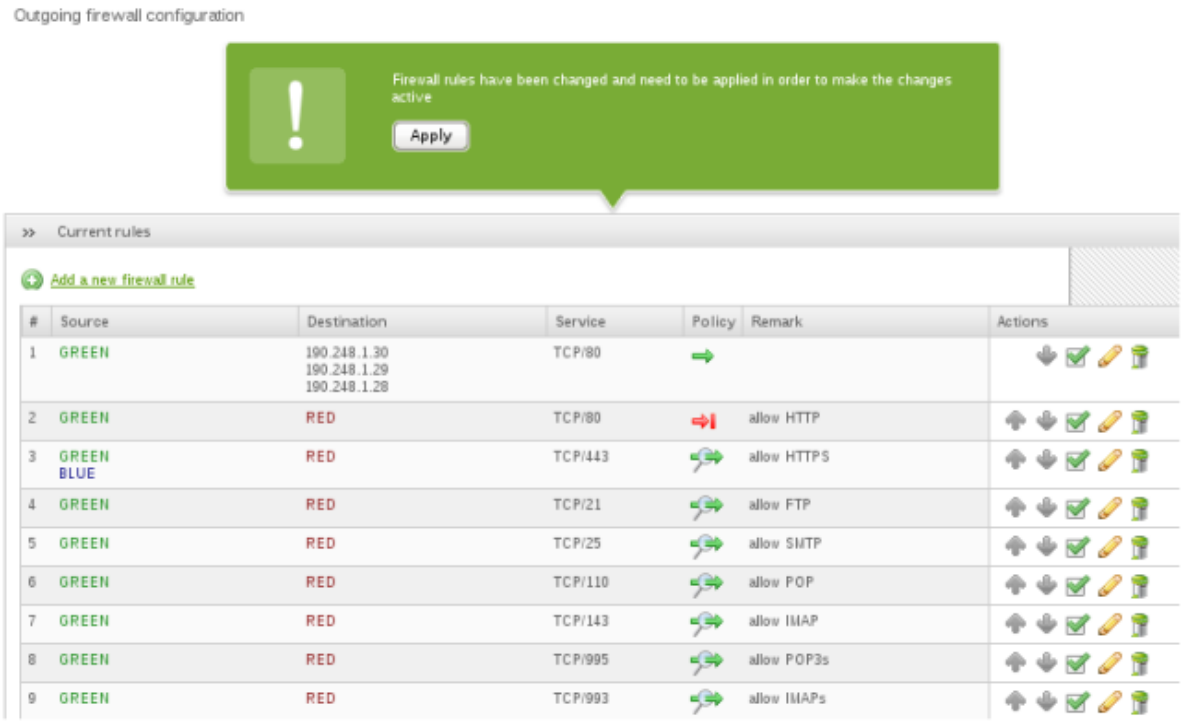
Para poder editar la regla debemos hacer clic encima del lapiz que se encuentra al final de cada regla, dentro de esta regla solo vamos a editar solo la parte de la accion (recuadro rojo) y la cambiamos por deny que es denegar todo el trafico hacia internet.



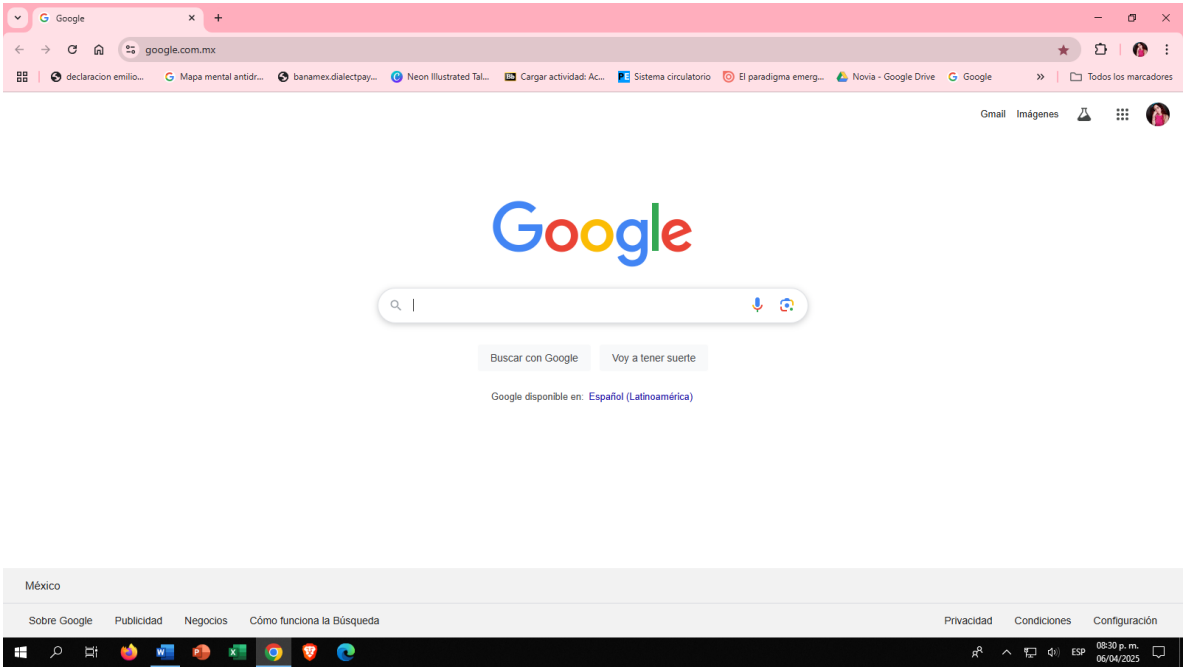
Ahora voy a crear un regla que me permita el ingreso solo a google por parte de nuestra red interna, damos clic en añadir regla y acontinuacion nos aparecera lo siguiente, source debemos poner de donde se originan lo paquetes en este caso desde la zona GREEN que es la LAN, Destination debemos poner los lugares hacia donde llega el trafico en este caso coloque 3 direcciones de servidores de google. service y protocolo colocamos http y protocolo tcp, por ultimo en accion colocamos allow para que nos permita todo el trafico http con protocolo tcp hacia los servidores de google desde nuestra red.



En la imagen podemos ver que nuestra nueva regla a quedado creada satisfactoriamente y la segunda regla a quedado modificada. solo hace falta dar el clic en apply para que nuestras reglas se actualicen

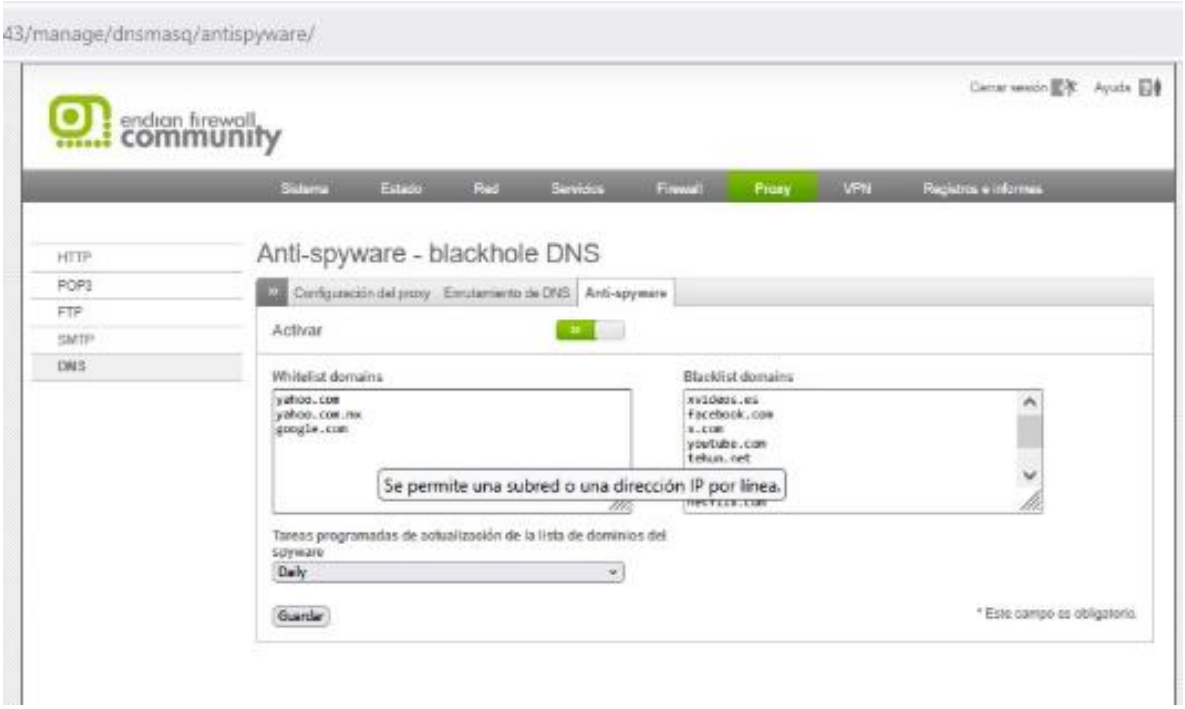


Volvemos hacer la prueba.



página web que se pueden bloquear por dns dominio. blackhole dns

anti-spyware



Black list dominios
instagram.com
facebook.com
x.com
youtube.com
msn.com
netflix.com
spotify.com

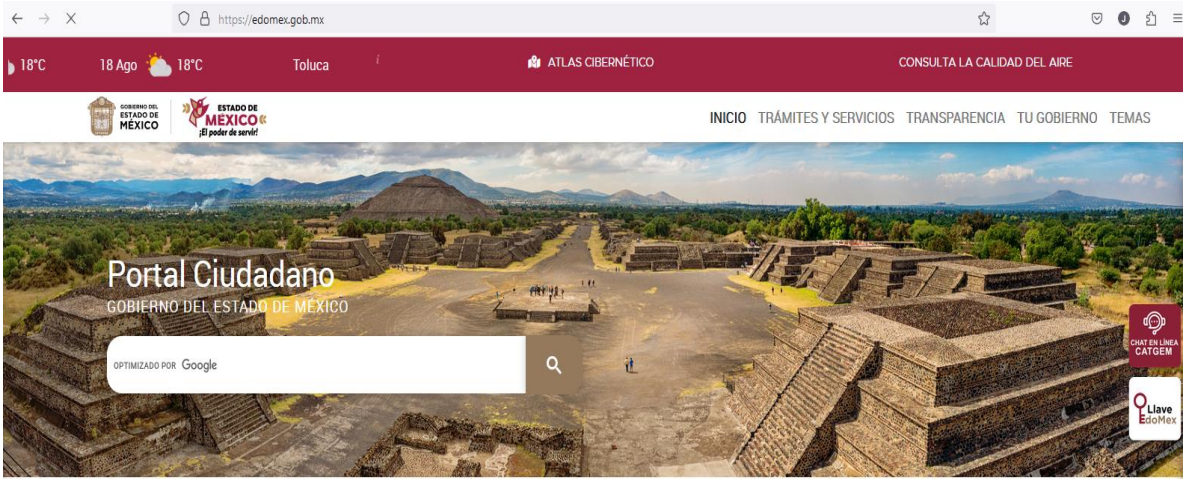
En Endian Firewall, el Blackhole DNS es una técnica para bloquear el acceso a sitios maliciosos, de spyware o no permitidos a nivel de resolución de nombres (DNS), antes de que el navegador siquiera intente conectarse.

Páginas web Bloqueadas por este método, que es muy seguro y con mayores ventajas.

💡 Ventajas:

- Bloquea el tráfico **antes** de que se establezca la conexión.
- Consume menos recursos que inspeccionar todo el tráfico con un proxy o IDS/IPS.
- Funciona incluso con HTTPS, ya que corta el acceso por nombre, sin importar el cifrado.

Página web con acceso permitido por DNS dominio.



Lista blanca de dominios
Permitidos.
edomex.gob.mx
g2g.edomex.gob.mx
mail.edomex.gob.mx
siser.secogem.gob.mx

Ejemplo de dominio dns dominio bloqueado.