UT04: Instalación y configuración de cortafuegos - 1) – Configuración cortafuegos firewall (router soho).

Nombre: Francisco Jesús García – Uceda Díaz - Albo

Curso: 2º ASIR.

Índice

Introducción

En esta práctica aprenderemos a configurar mediante emuladores y nuestro router de casa las distintas opciones que encontramos en los router SOHO las configuraciones de cortafuegos.

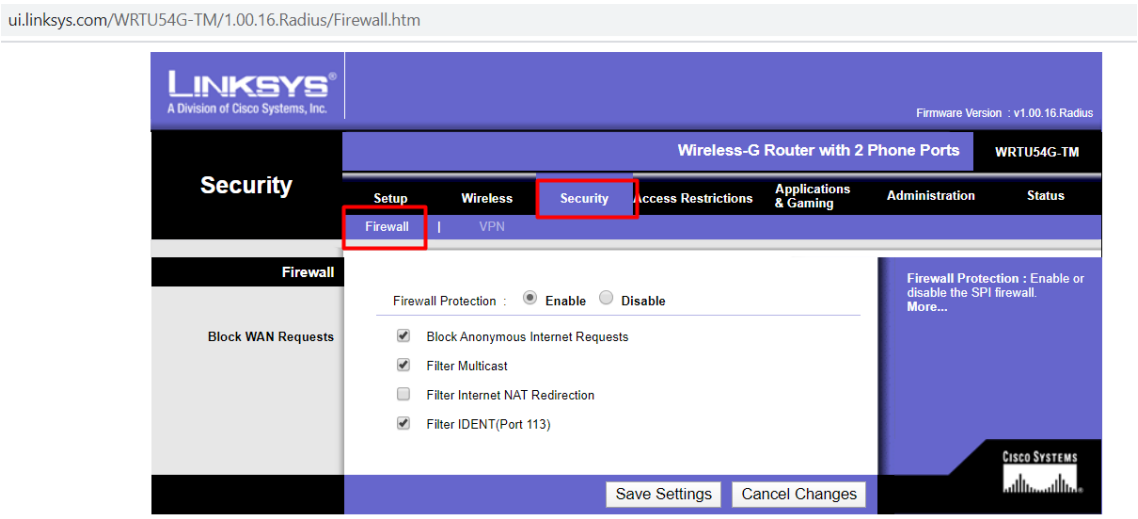
1. CONFIGURACIÓN CORTAFUEGOS "FIREWALL" (ROUTER SOHO).

I). Configura un router firewall utilizando los simuladores correspondientes:

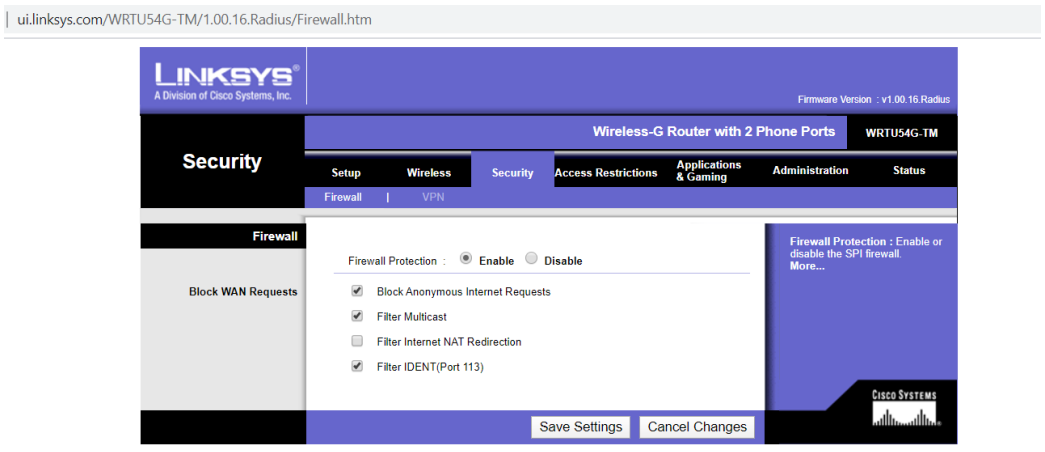
a) Router Linksys:

El escogido ha sido el DLINK de clase: Link.

Vamos a *Security* → *Firewall.*

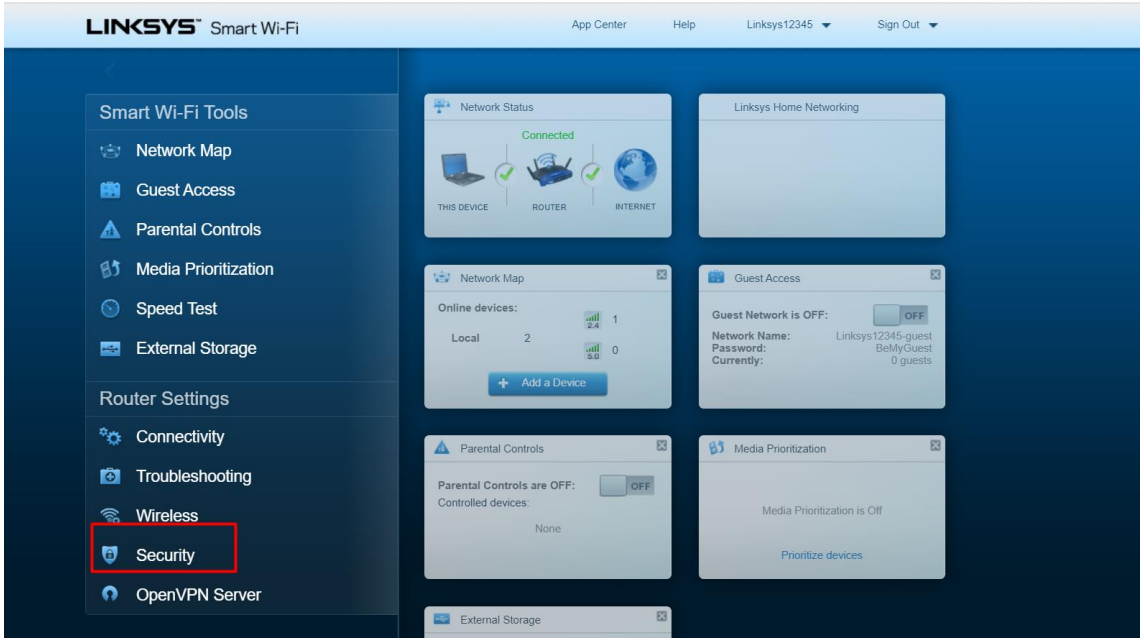


Podemos bloquear las respuestas anónimas, filtrar el multicast, la redirección NAT… No hay muchas opciones a escoger, por ello, cogeré uno más nuevo.

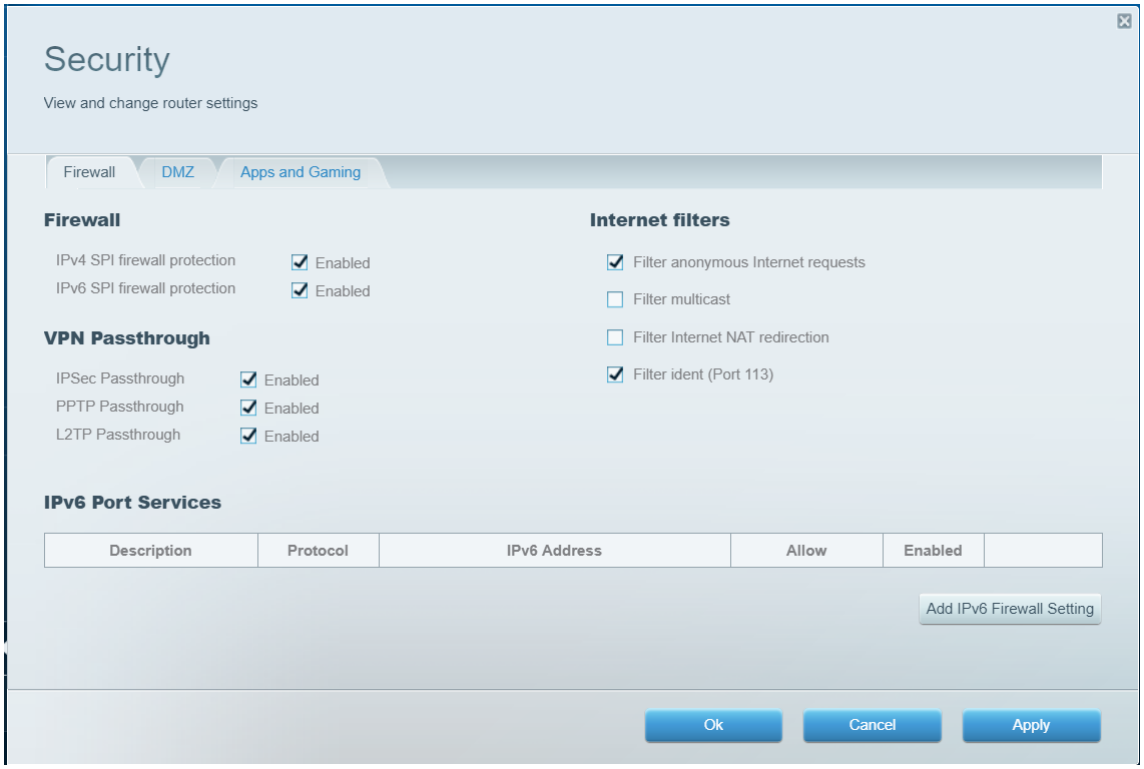


He escogido uno más nuevo como es el WRT1900AC: Link.

Vamos a *Security*.

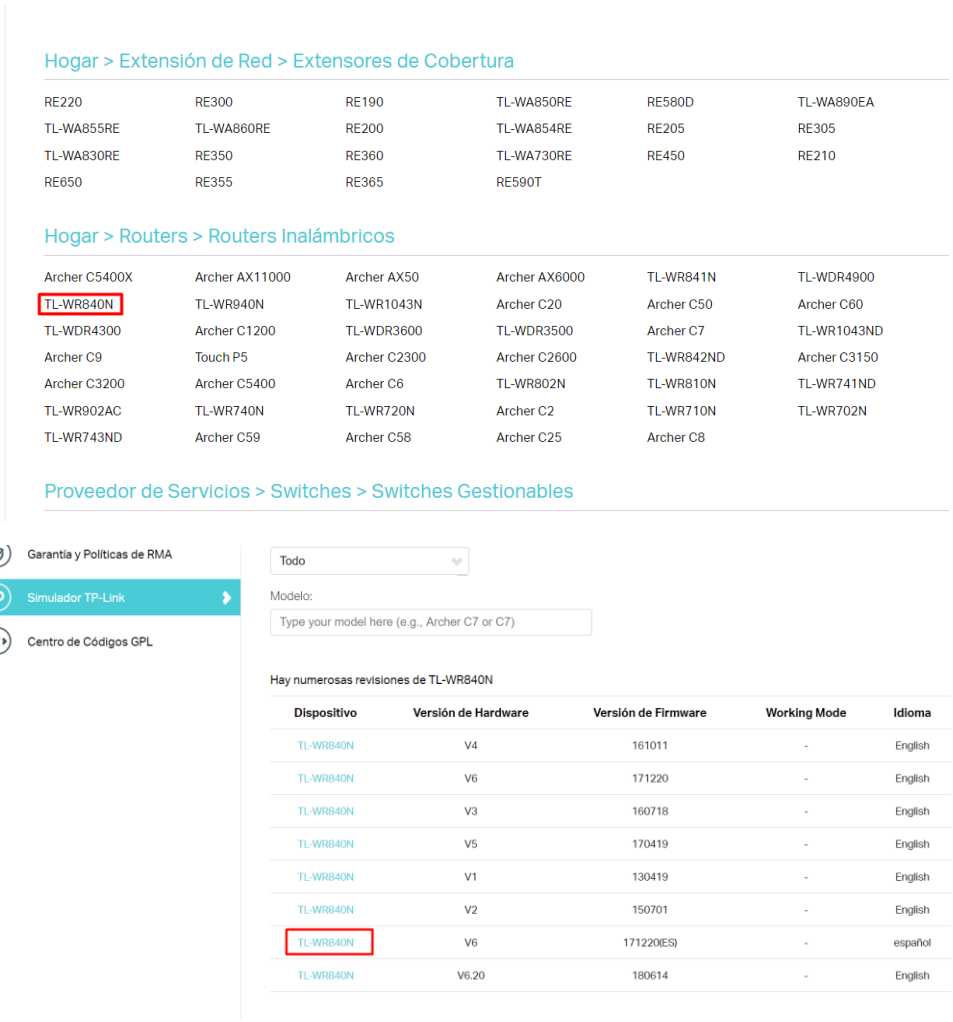


Podemos ver que las opciones no varían mucho, tenemos las mismas opciones como filtrar las respuestas anónimas, multicast, las redirecciones NAT o el ident… A diferencia del anterior podemos encontrar dos opciones más como es el IPv4 e IPv6 SPI Firewall. Podemos observar que en la misma pestaña tenemos las opciones de reenvío de puertos y DMZ como así las configuraciones de VPN Passthrough. Me ha gustado bastante esta interfaz más renovada y minimalista. Es bastante fácil de configurar.

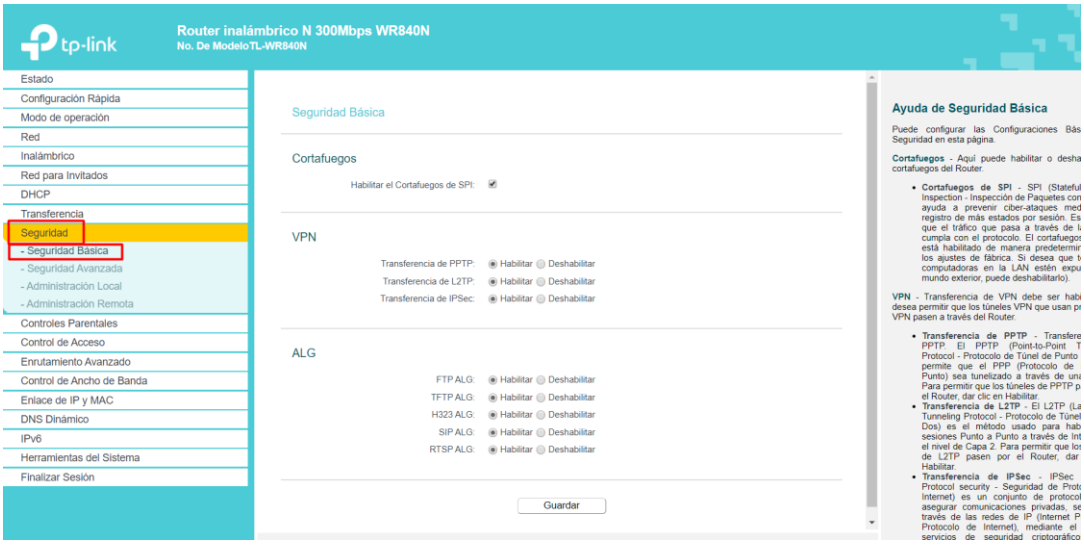


b) Router TP-LINL:

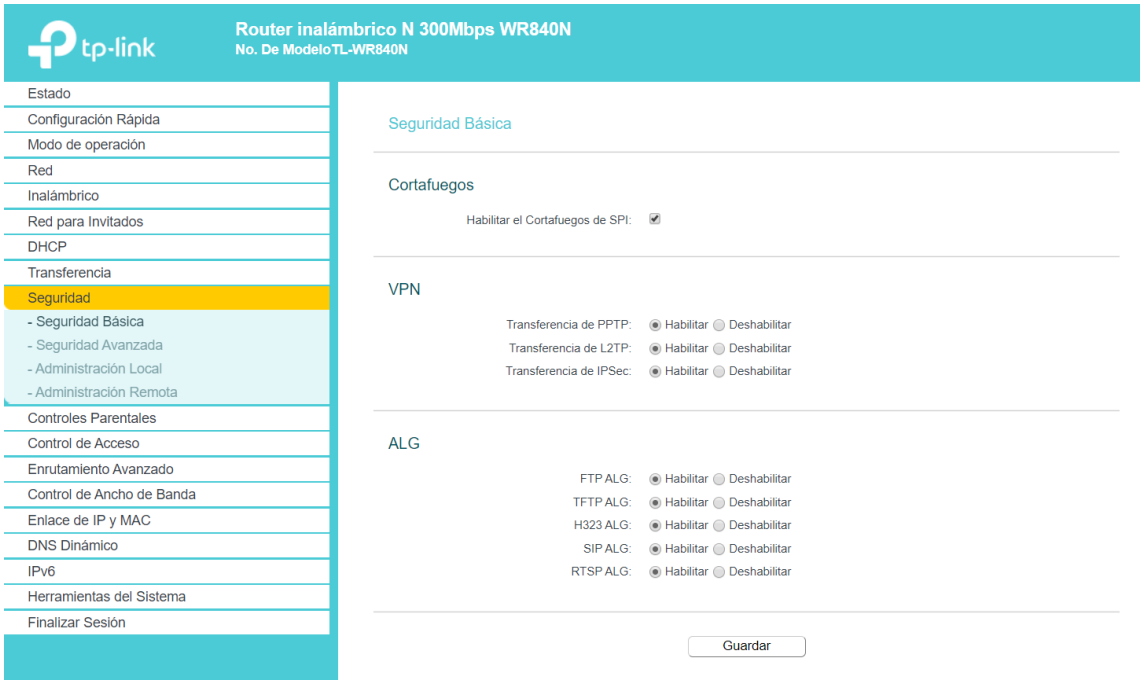
El escogido para este apartado ha sido el WR840N v6: [Link.](#)



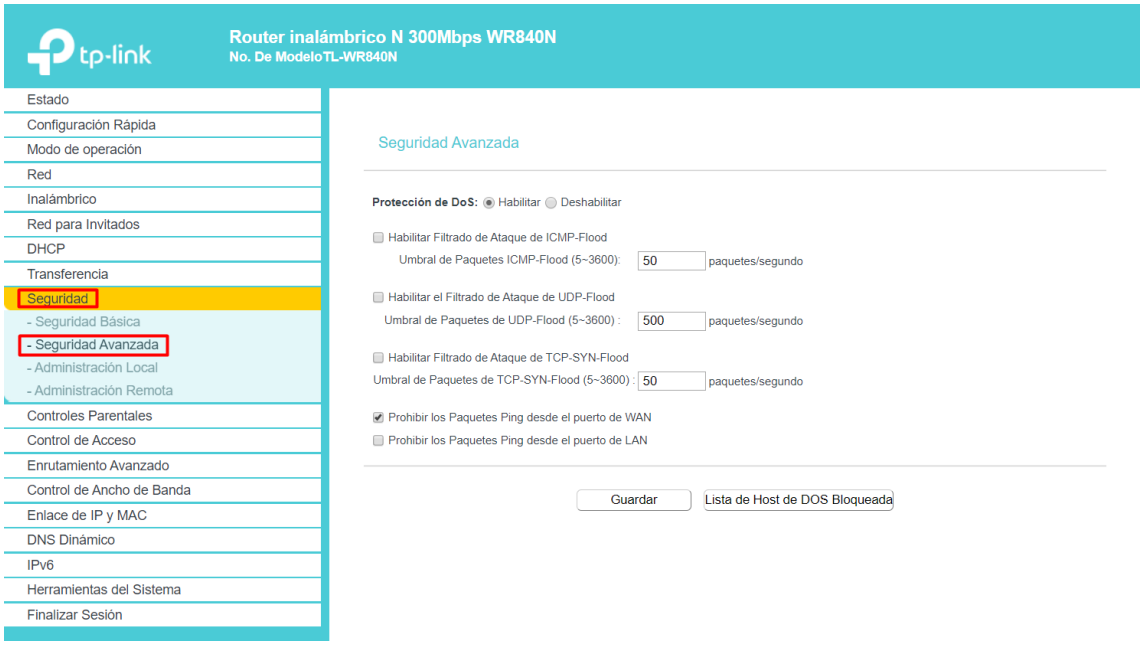
Vamos a *Seguridad* → *Seguridad Básica.*



Podemos ver que tenemos opciones para habilitar o deshabilitar el cortafuegos, las VPN o el ALG como estuvimos viendo. Por defecto todos están habilitado.

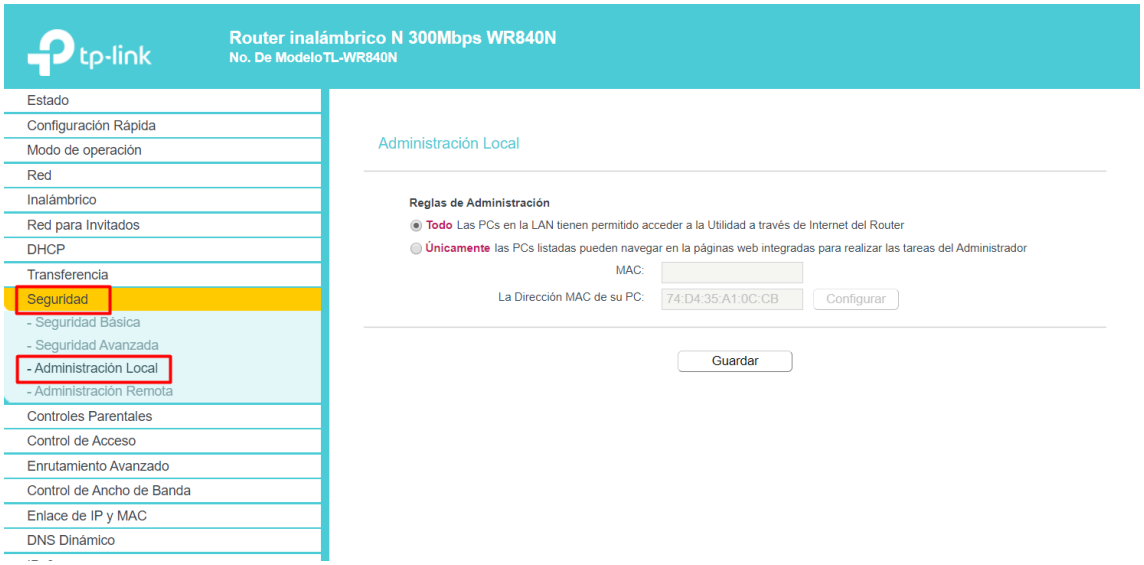


En *Seguridad* → *Seguridad Avanzada*, tenemos más opciones del Firewall para configurar. Podemos habilitar protección contra ataques DoS como ICMP Flood, TCP-SYN-Flood o UDP-Flood. También podemos habilitar protección contra la interfaz WAN para que esta no permita respuestas a los pings recibidos.

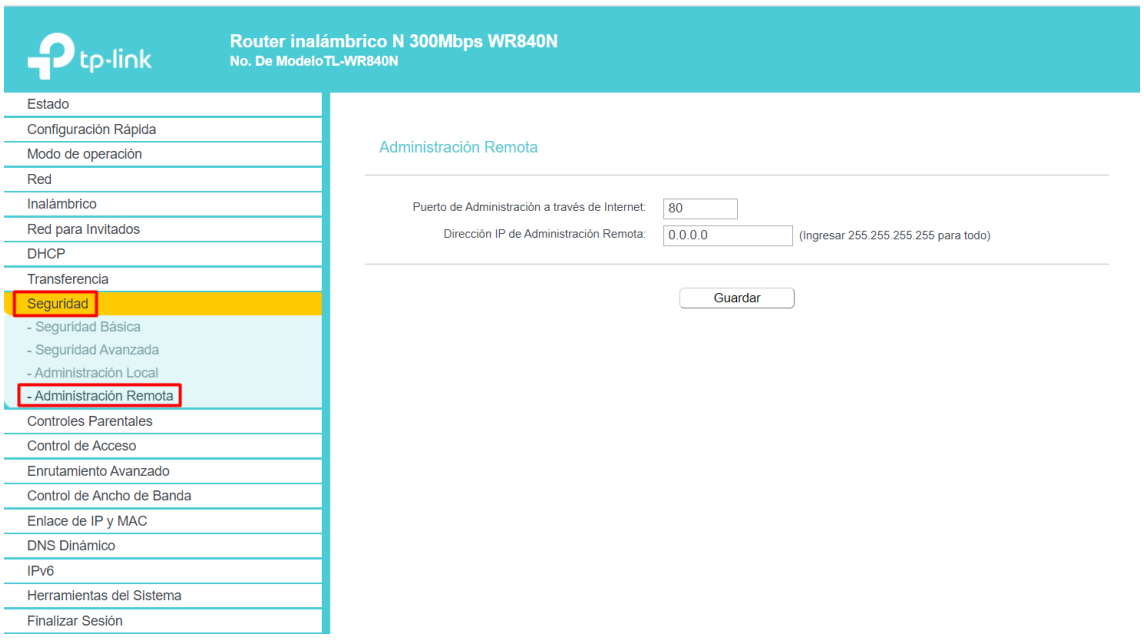


Ahora, vamos a *Seguridad → Administración Local.*

Podemos configurar la administración local, si habilitamos únicamente a un PC para administración local este PC será el único capaz de acceder a administrar el router en su configuración interna de forma local en la misma red.

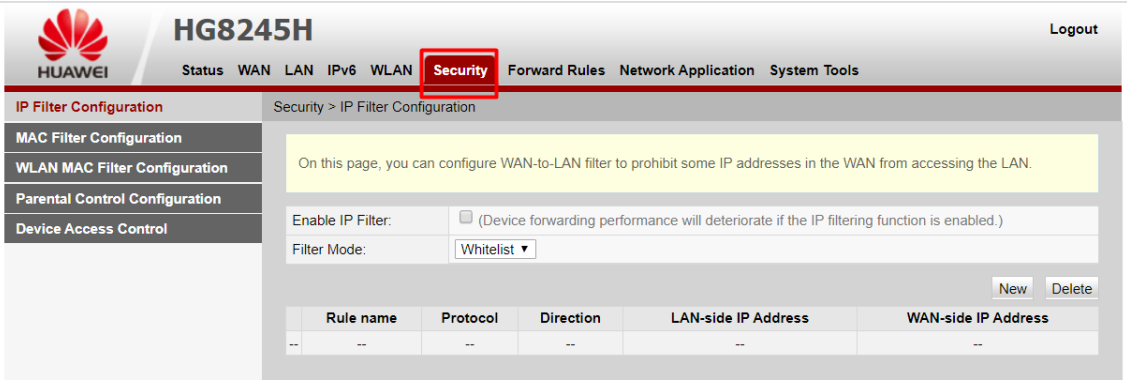


Por último, vamos a *Seguridad → Administración Remota.* Configurando esta opción podemos habilitar que equipos de fuera de la red (internet) puedan acceder al router a configurar el router.

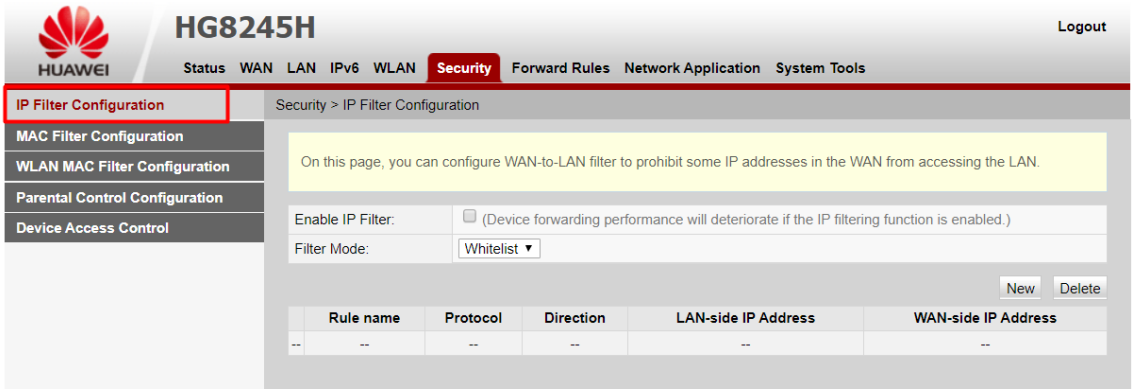


II) Elaborar un pequeño informe de las posibilidades que ofrece el firewall del router adsl que utilizas en CASA. Demuestra alguna de sus funcionalidades.

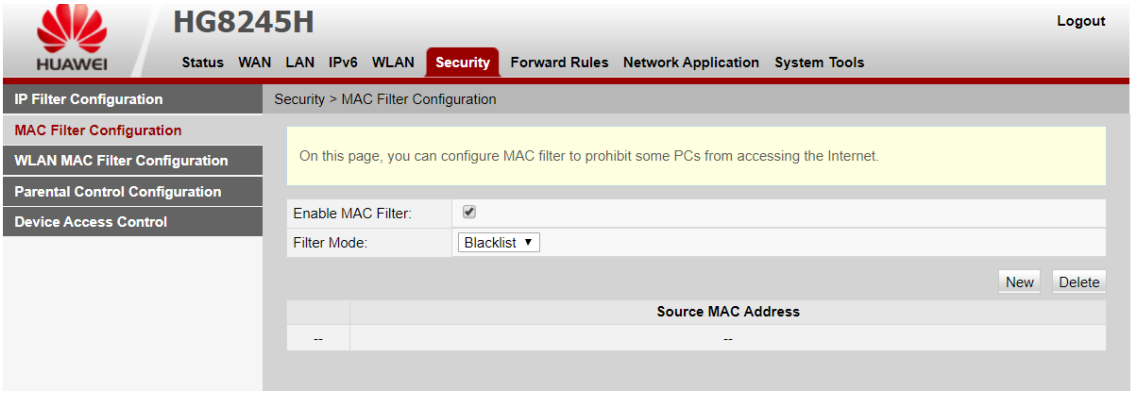
Mi router ofrece distintas configuraciones para cortafuegos. Vamos a la pestaña *Security.*



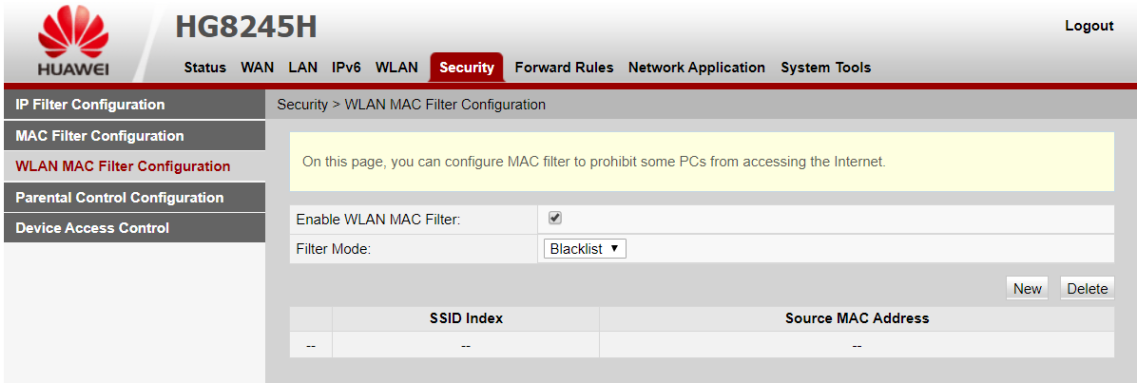
La primera pestaña de configuración de *Security* es *IP Filter Configuration.* Aquí podremos configurar para prohibir distintas IP dentro de la LAN.



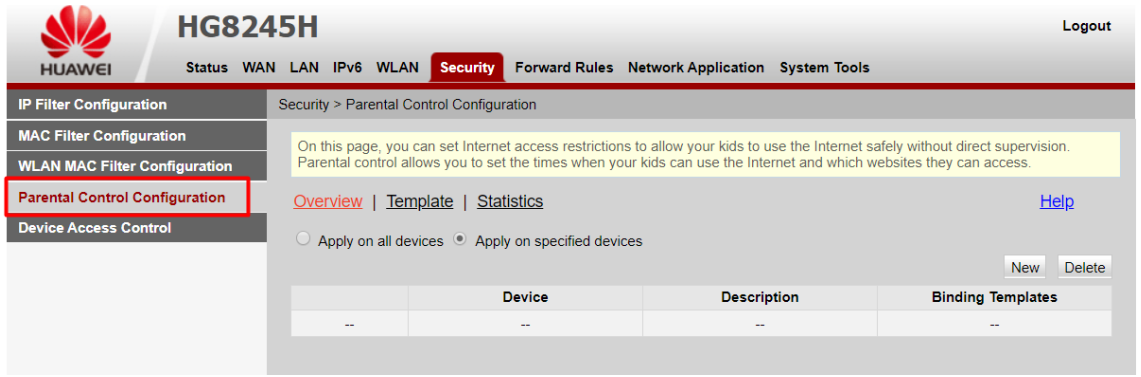
En *MAC Filter* podemos bloquear o permitir únicamente 'x' MAC Address.



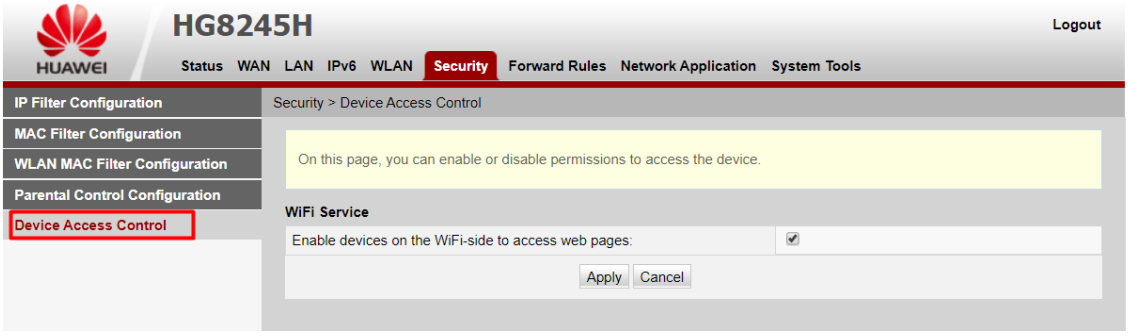
En *WLAN MAC Filter* es lo mismo que el anterior, pero para la red inalámbrica.



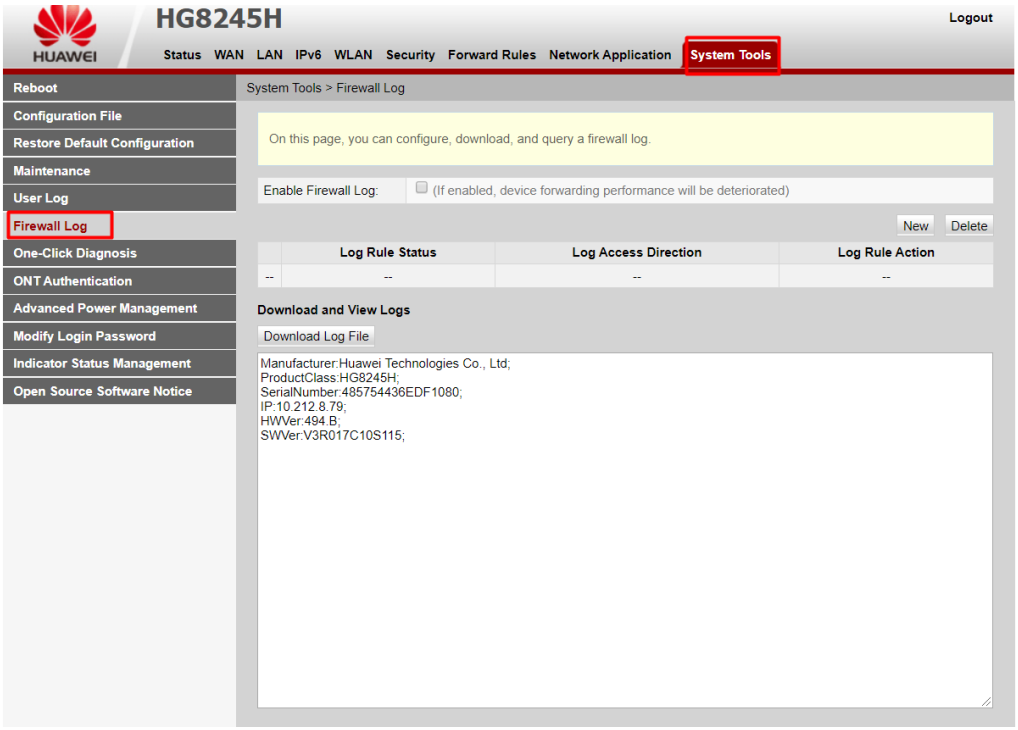
En *Parental Control Configuration* podremos configurar el control parental.



Podemos activar o desactivar que los equipos WIFI no accedan a las páginas con en *Devices Access Control.*



Mi router es un poco triste para esta configuración, no hay ni botón para activar o desactivar firewall ni otras opciones como hemos visto de protegerse contra ataques DOS. Lo que si he visto, podemos activar el log del Firewall en *System Tool* → *Firewall log.*



No hay ninguna configuración más en el router para configurar entorno a los cortafuegos, un poco triste la verdad.

Conclusión

La práctica ha sido útil para aprender sobre las distintas configuraciones que tienen los router en relación a los cortafuegos. No solo he podido ver como se configura el cortafuegos en un router Linksys o TP-LINK si no también en nuestro router de casa, aunque este sea muy escaso. La práctica como introducción al cortafuegos está bastante bien, que mejor que verlo en real y con emuladores para ver las distintas opciones que pueden ofrecer los router sobre esto.