

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

Nombre: Francisco Jesús García – Uceda Díaz - Albo

Curso: 2º ASIR.

Índice

Introducción	2
1. CONFIGURACIÓN CORTAFUEGOS “FIREWALL” (ROUTER SOHO).....	2
I). Configura un router firewall utilizando los simuladores correspondientes:	2
a) Router Linksys:.....	2
b) Router TP-LINL:.....	4
II) Elaborar un pequeño informe de las posibilidades que ofrece el firewall del router adsl que utilizas en CASA. Demuestra alguna de sus funcionalidades.	7
Conclusión	9

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.

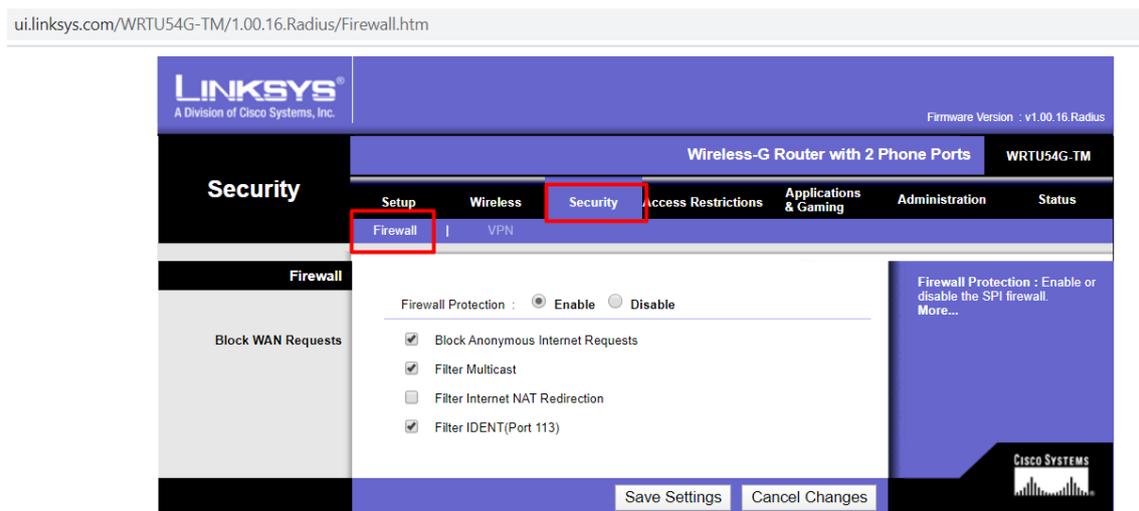
1. CONFIGURACIÓN CORTAFUEGOS “FIREWALL” (ROUTER SOHO).

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

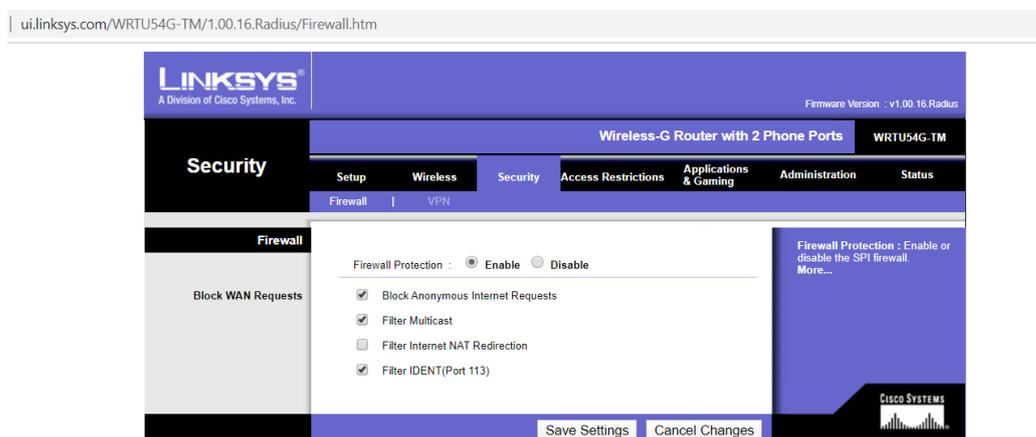
a) Router Linksys:

El escogido ha sido el DLINK de clase: [Link](#).

Vamos a *Security* → *Firewall*.

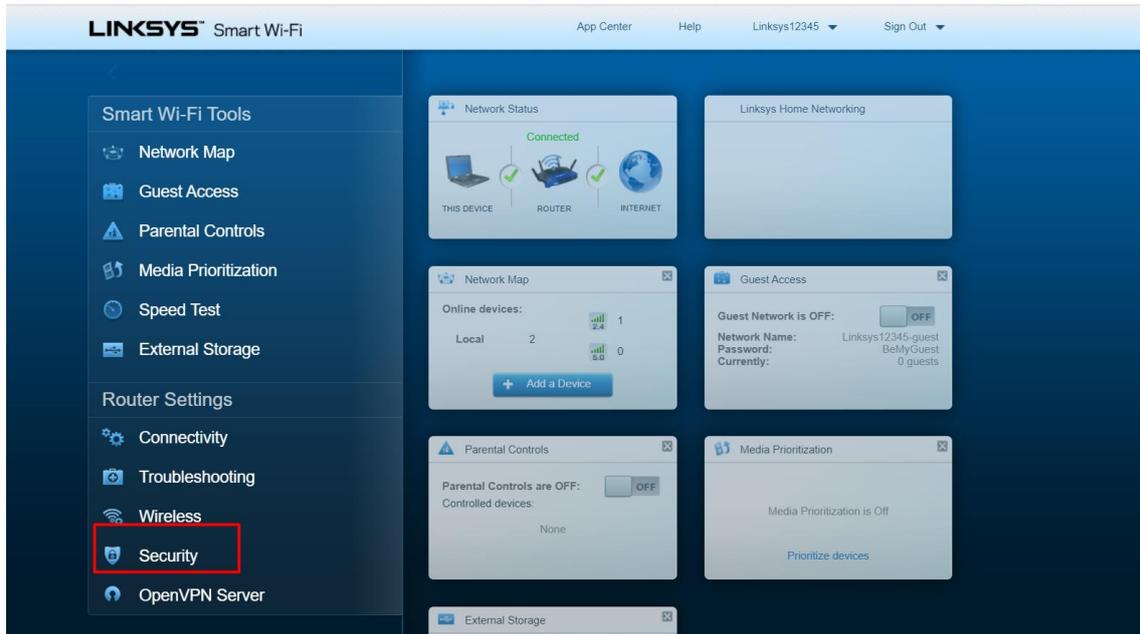


Podemos bloquear las respuestas anónimas, filtrar el multicast, la redirección NAT... No hay muchas opciones a escoger, por ello, cogeré uno más nuevo.

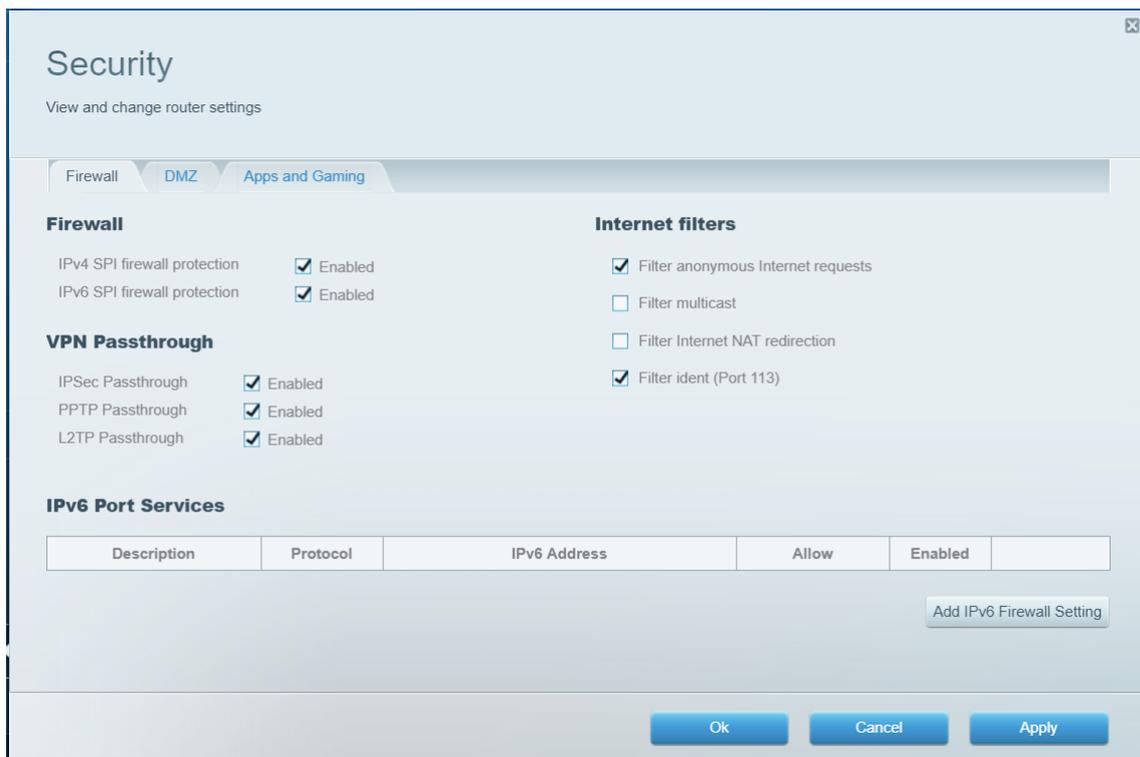


He escogido uno más nuevo como es el WRT1900AC: [Link](#).

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-LINK:

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

Hogar > Extensión de Red > Extensores de Cobertura

RE220	RE300	RE190	TL-WA850RE	RE580D	TL-WA890EA
TL-WA855RE	TL-WA860RE	RE200	TL-WA854RE	RE205	RE305
TL-WA830RE	RE350	RE360	TL-WA730RE	RE450	RE210
RE650	RE355	RE365	RE590T		

Hogar > Routers > Routers Inalámbricos

Archer C5400X	Archer AX11000	Archer AX50	Archer AX6000	TL-WR841N	TL-WDR4900
TL-WR840N	TL-WR940N	TL-WR1043N	Archer C20	Archer C50	Archer C60
TL-WDR4300	Archer C1200	TL-WDR3600	TL-WDR3500	Archer C7	TL-WR1043ND
Archer C9	Touch P5	Archer C2300	Archer C2600	TL-WR842ND	Archer C3150
Archer C3200	Archer C5400	Archer C6	TL-WR802N	TL-WR810N	TL-WR741ND
TL-WR902AC	TL-WR740N	TL-WR720N	Archer C2	TL-WR710N	TL-WR702N
TL-WR743ND	Archer C59	Archer C58	Archer C25	Archer C8	

Proveedor de Servicios > Switches > Switches Gestionables

- Garantía y Políticas de RMA
- Simulador TP-Link
- Centro de Códigos GPL

Modelo:
Type your model here (e.g., Archer C7 or C7)

Hay numerosas revisiones de TL-WR840N

Dispositivo	Versión de Hardware	Versión de Firmware	Working Mode	Idioma
TL-WR840N	V4	161011	-	English
TL-WR840N	V6	171220	-	English
TL-WR840N	V3	160718	-	English
TL-WR840N	V5	170419	-	English
TL-WR840N	V1	130419	-	English
TL-WR840N	V2	150701	-	English
TL-WR840N	V6	171220(ES)	-	español
TL-WR840N	V6.20	180614	-	English

Vamos a *Seguridad* → *Seguridad Básica*.

Router inalámbrico N 300Mbps WR840N
No. De Modelo TL-WR840N

Estado
Configuración Rápida
Modo de operación
Red
Inalámbrico
Red para Invitados
DHCP
Transferencia
Seguridad
- Seguridad Básica
- Seguridad Avanzada
- Administración Local
- Administración Remota
Controles Parentales
Control de Acceso
Enrutamiento Avanzado
Control de Ancho de Banda
Enlace de IP y MAC
DNS Dinámico
IPv6
Herramientas del Sistema
Finalizar Sesión

Seguridad Básica

Cortafuegos
Habilitar el Cortafuegos de SPI:

VPN
Transferencia de PPTP: Habilitar Deshabilitar
Transferencia de L2TP: Habilitar Deshabilitar
Transferencia de IPSec: Habilitar Deshabilitar

ALG
FTP ALG: Habilitar Deshabilitar
TFTP ALG: Habilitar Deshabilitar
H323 ALG: Habilitar Deshabilitar
SIP ALG: Habilitar Deshabilitar
RTSP ALG: Habilitar Deshabilitar

Ayuda de Seguridad Básica
Puede configurar las Configuraciones Básicas de Seguridad en esta página.
Cortafuegos - Aquí puede habilitar o deshabilitar los cortafuegos del Router.
• Cortafuegos de SPI - SPI (Stateful Inspection - Inspección de Paquetes con ayuda a prevenir ciberataques mediante registro de más estados por sesión. Es que el tráfico que pasa a través de él cumple con el protocolo. El cortafuegos está habilitado de manera predeterminada los ajustes de fábrica. Si desea que las computadoras en la LAN estén expuestas al mundo exterior, puede deshabilitarlo).
VPN - Transferencia de VPN debe ser habilitada para permitir que los túneles VPN que usan el protocolo PPTP pasen a través del Router.
• Transferencia de PPTP - Transferencia de PPTP. El PPTP (Point-to-Point Tunneling Protocol - Protocolo de Túnel de Punto a Punto) sea tunelizado a través de un router para permitir que los túneles de PPTP pasen a través del Router.
• Transferencia de L2TP - El L2TP (Layer 2 Tunneling Protocol - Protocolo de Túnel de Capa 2) es el método usado para habilitar sesiones Punto a Punto a través de Internet en el nivel de Capa 2. Para permitir que los túneles de L2TP pasen por el Router, dar clic en Habilitar.
• Transferencia de IPSec - IPSec (Internet Protocol Security - Seguridad de Protocolo de Internet) es un conjunto de protocolos para asegurar comunicaciones privadas, se habilita a través de las redes de IP (Internet Protocol - Protocolo de Internet), mediante el uso de servicios de seguridad criptográficos.

Guardar

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.

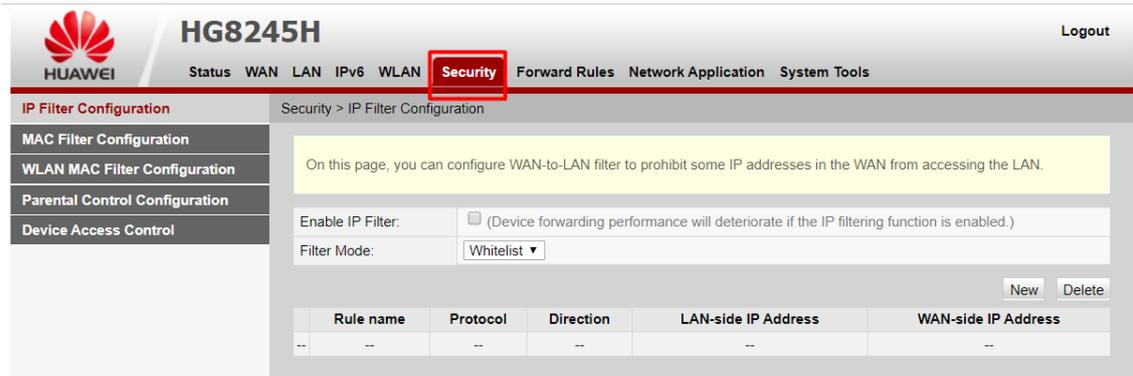
The screenshot shows the TP-Link router web interface for a 'Router inalámbrico N 300Mbps WR840N'. The left sidebar contains a menu with 'Seguridad' highlighted in yellow, and '- Administración Local' selected with a red box. The main content area is titled 'Administración Local' and features 'Reglas de Administración' with two radio button options: 'Todo' (selected) and 'Únicamente'. Below these are input fields for 'MAC' and 'La Dirección MAC de su PC' (containing '74:D4:35:A1:0C:CB'), and a 'Configurar' button. A 'Guardar' button is located at the bottom of the configuration area.

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.

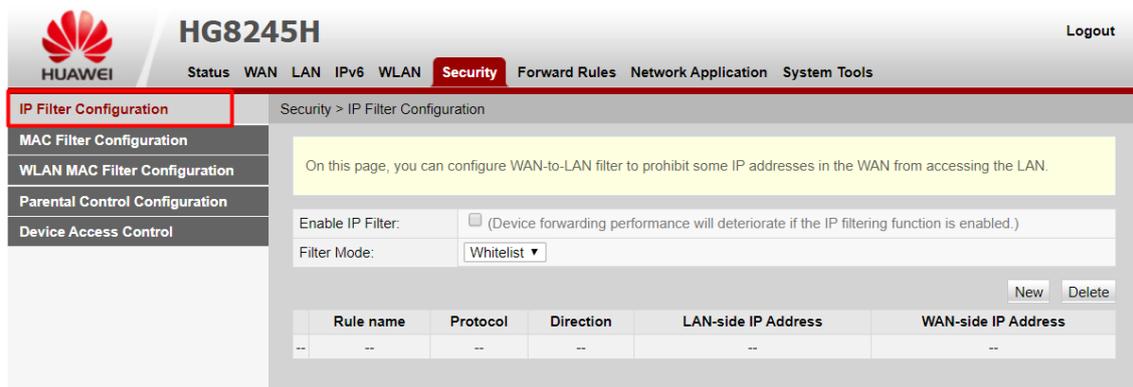
The screenshot shows the TP-Link router web interface for a 'Router inalámbrico N 300Mbps WR840N'. The left sidebar contains a menu with 'Seguridad' highlighted in yellow, and '- Administración Remota' selected with a red box. The main content area is titled 'Administración Remota' and features two input fields: 'Puerto de Administración a través de Internet' (set to '80') and 'Dirección IP de Administración Remota' (set to '0.0.0.0'). A note '(Ingresar 255.255.255.255 para todo)' is present next to the IP field. A 'Guardar' button is located at the bottom of the configuration area.

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

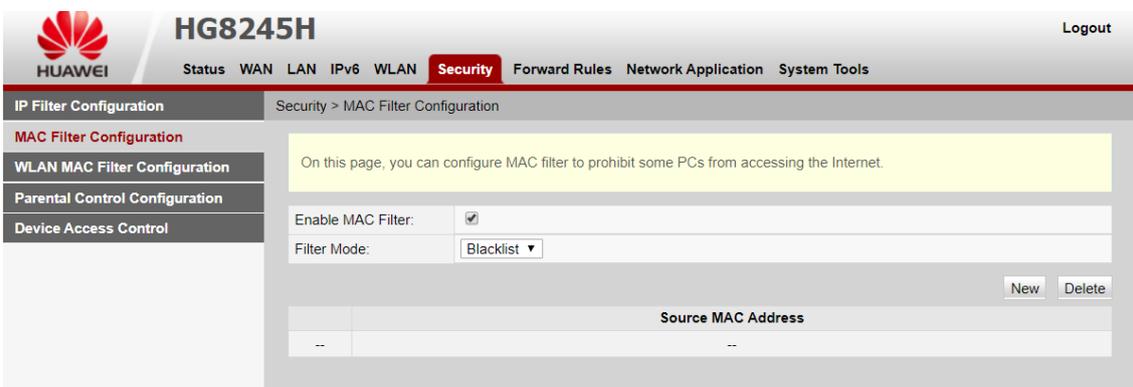
Mi router ofrece distintas configuraciones para cortafuegos. Vamos a la pestaña *Security*.



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.

HUAWEI **HG8245H** Logout

Status WAN LAN IPv6 WLAN **Security** Forward Rules Network Application System Tools

IP Filter Configuration Security > WLAN MAC Filter Configuration

MAC Filter Configuration

WLAN MAC Filter Configuration

Parental Control Configuration

Device Access Control

On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.

Enable WLAN MAC Filter:

Filter Mode: Blacklist

New Delete

SSID Index	Source MAC Address
--	--

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

HUAWEI **HG8245H** Logout

Status WAN LAN IPv6 WLAN **Security** Forward Rules Network Application System Tools

IP Filter Configuration Security > Parental Control Configuration

MAC Filter Configuration

WLAN MAC Filter Configuration

Parental Control Configuration

Device Access Control

On this page, you can set Internet access restrictions to allow your kids to use the Internet safely without direct supervision. Parental control allows you to set the times when your kids can use the Internet and which websites they can access.

[Overview](#) | [Template](#) | [Statistics](#) [Help](#)

Apply on all devices Apply on specified devices

New Delete

Device	Description	Binding Templates
--	--	--

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

HUAWEI **HG8245H** Logout

Status WAN LAN IPv6 WLAN **Security** Forward Rules Network Application System Tools

IP Filter Configuration Security > Device Access Control

MAC Filter Configuration

WLAN MAC Filter Configuration

Parental Control Configuration

Device Access Control

On this page, you can enable or disable permissions to access the device.

WiFi Service

Enable devices on the WiFi-side to access web pages:

Apply Cancel

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*.

The screenshot shows the Huawei HG8245H web interface. The top navigation bar includes 'Status', 'WAN', 'LAN', 'IPv6', 'WLAN', 'Security', 'Forward Rules', 'Network Application', and 'System Tools'. The 'System Tools' menu is highlighted. The left sidebar contains various system management options, with 'Firewall Log' selected. The main content area displays the 'Firewall Log' configuration page. It includes a yellow informational box, a checkbox for 'Enable Firewall Log' (disabled), and a table with columns for 'Log Rule Status', 'Log Access Direction', and 'Log Rule Action'. Below the table, there is a 'Download and View Logs' section with a 'Download Log File' button and a text area containing device information: Manufacturer: Huawei Technologies Co., Ltd; ProductClass: HG8245H; SerialNumber: 485754436EDF1080; IP: 10.212.8.79; HWVer: 494 B; SWVer: V3R017C10S115.

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.