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 qu utilizas en CASA. Demuestra alguna de sus funcionalidades	ue . 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).

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

a) Router Linksys:

El escogido ha sido el DLINK de clase: Link.

Vamos a Security \rightarrow Firewall.

ui.linksys.com/WRTU54G-TM/1.00.16.Radius/Firewall.htm

LINKSYS® A Division of Cisco Systems, Inc.						Firmware Ver	sion : v1.00.16.Radius
				Wireles	ss-G Router with 2	Phone Ports	WRTU54G-TM
Security	Setup	Wireless	Security	Access Restrict	Applications ions & Gaming	Administration	Status
	Firewall	I VPN					
Firewall						Firewall Prot	tection : Enable or
	Firew	all Protection :	Enable 🔘	Disable		disable the S More	PI firewall.
Block WAN Requests	•	Block Anonymous I	nternet Reques	ts			
		Filter Multicast					
		Filter Internet NAT	Redirection				
		Filter IDENT(Port 1	13)				
							CISCO SYSTEMS
			5	Save Settings	Cancel Changes		ավիստուլիստ

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

ui.linksys.com/WRTU54G-TM/1.00.16.Radius/Fi	rewall.htm						
A Division of Cisco Systems, Inc.						Firmware Ve	ersion : v1.00.16.Radius
				Wireless-G	Router with 2	Phone Ports	WRTU54G-TM
Security	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status
	Firewall	VPN					
Firewall						Firewall Pro	otection : Enable or
	Firev	vall Protection : 🦲	Enable 🔘	Disable		More	or i mewan.
Block WAN Requests	1	Block Anonymous Ir	nternet Reques	its			
	4	Filter Multicast					
		Filter Internet NAT F	Redirection				
		Filter IDENT(Port 11	3)				
							CISCO SYSTEMS
				Save Settings Ca	incel Changes		hiiiiih

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

vallios a security.	Vamos	а	Security.
---------------------	-------	---	-----------

LINKSYS [®] Smart Wi-Fi	App Center Help Linksys12345 👻 Sign Out 👻
Smart Wi-Fi Tools	The Network Status Linksys Home Networking
া Network Map	Connected
Guest Access	
A Parental Controls	
Media Prioritization	😨 Network Map 📓 💼 Guest Access 📓
Speed Test	Online devices: Guest Network is OFF: OFF
External Storage	Local 2 Network Name: Linksys12345-guest all 0 Password: BeMyGuest Currently: 0 Quests
Router Settings	+ Add a Device
Connectivity	A Parental Controls
Troubleshooting	Parental Controls are OFF: OFF
S Wireless	Controlled devices: Media Prioritization is Off
🗑 Security	Prioritize devices
OpenVPN Server	
	External Storage

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.

Firewall DMZ	Apps and Gaming				
irewall		Internet filters			
IPv4 SPI firewall protect	tion Z Enabled	Filter anonymo	ous Internet requests		
IPv6 SPI firewall protect	tion I Enabled	Filter multicast			
PN Passthrough		Filter Internet I	NAT redirection		
IPSec Passthrough	Enabled	✓ Filter ident (Page)	ort 113)		
PPTP Passthrough	Enabled				
L2TP Passthrough	Enabled				
Pv6 Port Service	S				
Description	Protocol	IPv6 Address	Allow	Enabled	
				Add ID.	C Firewell Cottine
				Add IPv6	3 Firewall Setting

Página 3|9

b) Router TP-LINL:

El escogido para este apartado ha sido el WR840N v6: Link.

	Hogar > Exten	sión de Red > l	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 > Route	rs > Routers In	alámbricos				
	Archer C5400X	Archer AX11000	Archer AX50	Archer AX6000	TL-WR841N	TL-WDR4900	I
	TL-WR840N	TL-WR940N	TL-WR1043N	Archer C20	Archer C50	Archer C60	
	TL-WDR4300	Archer C1200	TL-WDR3600	TL-WDR3500	Archer C7	TL-WR1043N	D
	Archer C9	Touch P5	Archer C2300	Archer C2600	TL-WR842ND	Archer C3150	0
	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		
(©) (•) (•)	Garantia y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Mode	lo elo: be your model here (e.g., / numerosas revisiones de	Archer C7 or C7)			
(a) (c) (c)	Garantía y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Too Modd Typ Hay r	lo elo: uumerosas revisiones de Dispositivo Ve	Archer C7 or C7) TL-WR840N rsión de Hardware V	ersión de Firmware	Working Mode	Idioma
(8) (1) (1) (1)	Garantía y Politicas de RMA Simulador TP-Link Centro de Códigos GPL	Toc Mode Typ	lo elo: humerosas revisiones de Dispositivo Ve TL-WR840N	Archer C7 or C7) TL-WR840N rsión de Hardware V V4	ersión de Firmware 161011	Working Mode	Idioma English
	Garantia y Politicas de RMA Simulador TP-Link Centro de Códigos GPL	Toc Mode Typ Hay I	lo slo: e your model here (e.g., , numerosas revisiones de Dispositivo Ve TL-WR840N TL-WR840N	Archer C7 or C7) TL-WR840N V4 V6 V6	ersión de Firmware 161011 171220	Working Mode - -	Idioma English English
	Garantía y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Toc Modd Typ Hay t	lo elo: e your model here (e.g., / numerosas revisiones de Dispositivo Ve TL-WR840N TL-WR840N	Archer C7 or C7) TL-WRB40N V4 V4 V6 V3	ersión de Firmware 161011 171220 160718	Working Mode - - -	Idioma English English English
	Garantía y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Nodd	lo elo: numerosas revisiones de Dispositivo Ve TL-WR840N TL-WR840N TL-WR840N TL-WR840N	Archer C7 or C7) TL-WR840N V4 V6 V3 V5 V5	ersión de Firmware 161011 171220 160718 170419	Working Mode - - - -	Idioma English English English English
	Garantía y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Mode	lo slo: ee your model here (e.g., / numerosas revisiones de Dispositivo Ve TL-WR840N TL-WR840N TL-WR840N TL-WR840N	Archer C7 or C7) TL-WR840N v6 v3 v5 v1	ersión de Firmware 161011 171220 160718 170419 130419	Working Mode - - - - -	Idioma English English English English English
 (a) (b) (c) (c)	Garantía y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Toc Modd Typ	lo elo: e your model here (e.g., / humerosas revisiones de Dispositivo Ve TL-WR840N TL-WR840N TL-WR840N TL-WR840N TL-WR840N	V V V4 V V3 V5 V1 V2	ersión de Firmware 161011 171220 160718 170419 130419 150701	Working Mode - - - - - - - -	Idioma English English English English English English
8 (4) (4)	Garantía y Políticas de RMA Simulador TP-Link Centro de Códigos GPL	Toc Modd Typ Hay t	lo elo: elo: umerosas revisiones de Dispositivo Ve TL-WR840N TL-WR840N TL-WR840N TL-WR840N TL-WR840N TL-WR840N TL-WR840N TL-WR840N	V V v4 V v3 v5 v1 v2 v6 v3	ersión de Firmware 161011 171220 160718 170419 130419 150701 150701 171220(ES)	Working Mode - - - - - - - - - - - -	Idioma English English English English English English english

Vamos a Seguridad \rightarrow Seguridad Básica.

Ptp-link	Router inalá No. De ModeloT	mbrico N 300Mbps WR840N L-WR840N		
Estado				
Configuración Rápida		Operation (D) (since		 Avuda de Seguridad Básica
Modo de operación		Segundad Basica		 Ruda confaurar las Confauraciones Rás
Red				 Seguridad en esta página.
Inalámbrico		Cortafuegos		 Cortafuegos - Aqui puede habilitar o desha
Red para Invitados		Habilitar el Cortafuence de SPI-		 contatuegos del Router.
DHCP		masiliar el contaidegus de Seri.	that a second	 Contatuegos de SPI - SPI (Statetul Inspection - Inspección de Paquetes con
Transferencia Seguridad - Seguridad Básica	_	VPN		 ayuda a prevenir ciber-ataques med registro de más estados por sesión. Es que el tráfico que pasa a través de la cumpla con el protocolo. El cortafuegor está habilitado de manera predetermir los ajustes de fábrica. Si desea que h
- Seguridad Avanzada		Transferencia de PPTP:	 Habilitar 	 computadoras en la LAN estén expu
- Administración Local		Transferencia de L2TP:	Habilitar Deshabilitar	 VPN - Transferencia de VPN debe ser babi
- Administración Remota		Transferencia de IP/Sec.	 Habiitar U Deshabiitar 	 desea permitir que los túneles VPN que usan pr
Controles Parentales				 vern pasen a traves del Router.
Control de Acceso		ALC		 PPTP. EI PPTP (Point-to-Point T
Enrutamiento Avanzado		ALG		 permite que el PPP (Protocolo de
Control de Ancho de Banda		FTP ALG:	 Habilitar Deshabilitar 	 Punto) sea tunelizado a través de una Para permitir que los túneles de PPTP p
Enlace de IP y MAC		TFTP ALG:	 Habilitar Deshabilitar 	 el Router, dar clic en Habilitar. Transferencia de L2TP - El L2TP (La
DNS Dinámico		H323 ALG:	Habilitar Deshabilitar	 Tunneling Protocol - Protocolo de Túnel Dos) es el método usado para hab
IPv6		SIP ALG:	Habilitar Deshabilitar	 sesiones Punto a Punto a través de Int el nivel de Cana 2. Para permitir que los
Herramientas del Sistema		RISPALS:	 Habiitar U Deshabiitar 	 de L2TP pasen por el Router, dar
Finalizar Sesión				 Transferencia de IPSec - IPSec Protocol security Securidad de Prote
			Guardar	Internet) es un conjunto de protocio asegurar comunicaciones privadas, se través de las redes de IP (internet P Protocolo de Internet), mediante el servicios de securidad cristocráfico
				Página 4

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

Ptp-link Router in No. De Moo	alámbrico N 300Mbps WR840N eloTL-WR840N
Estado	
Configuración Rápida	Seguridad Básica
Modo de operación	
Red	Outstan
Inalámbrico	Cortatuegos
Red para Invitados	Habilitar el Cortafuegos de SPI:
DHCP	
Transferencia	
Seguridad	VPN
- Seguridad Básica	Transferencia de PPTP: Habilitar Deshabilitar
- Seguridad Avanzada	Transferencia de L2TP: Habilitar Deshabilitar
- Administración Local	Transferencia de IPSec: 💿 Habilitar 🔘 Deshabilitar
- Administración Remota	
Controles Parentales	
Control de Acceso	ALG
Enrutamiento Avanzado	ETP ALG:
Control de Ancho de Banda	TETP ALG: Habilitar TETP ALG:
Enlace de IP y MAC	H323 ALG: Habilitar Deshabilitar
DNS Dinámico	SIP ALG:
IPv6	RTSP ALG:
Herramientas del Sistema	1
Finalizar Sesión	
	Guardar

En Seguridad \rightarrow 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.

Estado Configuración Rápida Modo de operación Red Inalámbrico Inalámbrico DHCP Transferencia Seguridad Básica • Seguridad Básica • Seguridad Avanzada • Administración Local • Administración Local Control de Acceso Enrutamiento Avanzado Control de Ancho de Banda Ence de IP y MAC DNS Dinàmico IPvé Haramientas del Sistema Finalizar Sesión		Router inalámbrico N 300Mbps WR840N No. De ModeloTL-WR840N
Configuración Ràpida Modo de operación Red Inalámbrico Red para Invitados DHCP Transferencia Seguridad Básica - Seguridad Avanzada - Administración Local - Administración Renota Control de Acceso Control de Acceso Enrutamiento Avanzado Control de Ancho de Banda Enciac de IP y MAC DNS Dinàmico IPré6 Herramientas del Sistema Finalizar Sesión	Estado	
Modo de operación Seguridad Avanzada Red Inalámbrico Red para Invitados Protección de DoS: @ Habilitar @ Deshabilitar DHCP Inhalitar Filtrado de Ataque de ICMP-Flood Transferencia Inhalitar Elitrado de Ataque de UDP-Flood Seguridad Básica Inhalitar el Filtrado de Ataque de UDP-Flood (Umbral de Paquetes/degundo) - Seguridad Avanzada Inhalitar Elitrado de Ataque de UDP-Flood (Umbral de Paquetes/degundo) - Administración Local Inhalitar Elitrado de Ataque de TCP-SYN-Flood (5-3800): 500 paquetes/segundo - Administración Remota Prohibir los Paquetes Ping desde el puerto de WAN Control de Ancho de Banda Prohibir los Paquetes Ping desde el puerto de UAN Enricace de IP y MAC Guardar DNS Dinàmico Ipví6 Herramientas del Sistema Finalizar Sesión	Configuración Rápida	
Red Inalambrico Red para Invitados DHCP Transferencia Seguridad Basica - Seguridad Manzada - Administración Local - Administración Remota Controles Parentales Control de Ancho de Banda Enlace de IP y MAC DNS Dnamico IPv6 Herramlentas del Sistema Finalizar Sesión	Modo de operación	Seguridad Avanzada
Inaliambrico Protección de DoS: @ Habilitar © Deshabilitar Red para Invitados Habilitar Filtrado de Ataque de ICMP-Flood Umbral de Paquetes ICMP-Flood (5-3600); 50 paquetes/segundo Seguridad Basica Seguridad Avanzada Administración Local Administración Remota Controles Parentales Control de Acceso Prohibir los Paquetes Ping desde el puerto de LAN Prohibir los Paquetes Ping desde el puerto de LAN Guardar Lista de Host de DOS Bioqueada Itada de Host de DOS Bioqueada Finalizar Sesión	Red	
Red para Invitados Habilitar Filtrado de Ataque de ICMP-Flood DHCP Umbral de Paquetes ICMP-Flood (5-3600); 50 paquetes/segundo Transferencia Habilitar el Filtrado de Ataque de UDP-Flood - Seguridad Básica Umbral de Paquetes de UDP-Flood (5-3600); 500 paquetes/segundo - Seguridad Avanzada Habilitar Filtrado de Ataque de TCP-SYN-Flood - Administración Local Habilitar Filtrado de Ataque de TCP-SYN-Flood - Administración Remota Prohibir los Paquetes de TCP-SYN-Flood Controles Parentales Prohibir los Paquetes Ping desde el puerto de WAN Control de Ancho de Banda Prohibir los Paquetes Ping desde el puerto de LAN Entace de IP y MAC Guardar Lista de Host de DOS Bioqueada DNS Dinámico IPv6 Finalizar Sesión Finalizar Sesión	Inalámbrico	Protección de DoS: Habilitar Deshabilitar
DHCP Indianial Finiadua de Praquetes (CMP-Flood (5-3600): 60 paquetes/segundo Transferencia Umbral de Paquetes (CMP-Flood (5-3600): 60 paquetes/segundo - Seguridad Básica Umbral de Paquetes de UDP-Flood (5-3600): 500 paquetes/segundo - Seguridad Vanazada - Administración Local - Habilitar Filtrado de Ataque de TCP-SYN-Flood - Material Filtrado de Ataque de TCP-SYN-Flood - Administración Remota Imbral de Paquetes de UDP-Sinod (5-3600): 50 paquetes/segundo Controles Parentales Imbral de Paquetes de UDP-Sinod (5-3600): 50 paquetes/segundo Control de Acceso Imbral de Paquetes Ping desde el puerto de UAN Prohibir los Paquetes Ping desde el puerto de LAN Entace de IP y MAC Guardar Lista de Host de DOS Bioqueada DNS Dinámico IPv6 Finalizar Sesión Finalizar Sesión Finalizar Sesión Finalizar Sesión	Red para Invitados	Habilitar Elitrado de Ataque de ICNIP Elood
Transferencia Image: Control de Acaque de UDP-Flood Seguridad Basica Imabilitar el Filtrado de Ataque de UDP-Flood Seguridad Avanzada Imabilitar el Filtrado de Ataque de UDP-Slood (5-3600): 500 paquetes/segundo - Administración Local Imabilitar Filtrado de Ataque de TCP-SYN-Flood - Administración Remota Imabilitar Filtrado de Ataque de TCP-SYN-Flood Control de Acceso Imabilitar Filtrado de Ataque de TCP-SYN-Flood (5-3600): 500 paquetes/segundo Enrutamiento Avanzado Imabilitar Plitrado de Ataque de TCP-SYN-Flood (5-3600): 500 paquetes/segundo Control de Acceso Imabilitar Plitrado de Ataque de TCP-SYN-Flood (5-3600): 500 paquetes/segundo Enrutamiento Avanzado Imabilitar Plitrado de Ataque de Ipuerto de WAN Control de Ancho de Banda Imabilitar Plitrado de Ataque de Ipuerto de LAN Intramiento Guardar Lista de Host de DOS Bioqueada Invo6 Imabilitar Sistema Imabilitar Sistema Finalizar Sesión Imabilitar Sistema Imabilitar Sistema	DHCP	Umbried in adduce de comercia in tod
Seguridad Habilitar el Filtrado de Ataque de UDP-Flood - Seguridad Bàsica Umbral de Paquetes de UDP-Flood (5-3600): 500 paquetes/segundo - Administración Cocal Habilitar Filtrado de Ataque de TCP-SYN-Flood - Administración Remota Controles Parentales Control de Acceso Prohibir los Paquetes Ping desde el puerto de UAN Enrutamiento Avanzado Control de Ancho de Banda Enlace de IP y MAC DNS Dinámico IPv6 Herramientas del Sistema Finalizar Sesión Finalizar Sesión	Transferencia	harden en e
- Seguridad Básica Umbral de Paquetes de UDP-Flood (5~3600): 500 paquetes/segundo - Administración Local Habilitar Filtrado de Ataque de TCP-SYN-Flood Umbral de Paquetes de UCP-SYN-Flood (5~3600): 50 paquetes/segundo - Administración Local Whoral de Paquetes de TCP-SYN-Flood (5~3600): 50 paquetes/segundo - Administración Local Prohibir los Paquetes de TCP-SYN-Flood (5~3600): 50 paquetes/segundo - Administración Local Prohibir los Paquetes de TCP-SYN-Flood (5~3600): 50 paquetes/segundo - Control de Anceso Prohibir los Paquetes Ping desde el puerto de WAN Prohibir los Paquetes Ping desde el puerto de LAN - Control de Ancho de Banda Prohibir los Paquetes Ping desde el puerto de LAN Guardar Lista de Host de DOS Bloqueada - IPv6 IPv6 Ista de Host de DOS Bloqueada Ista de Host de DOS Bloqueada Ista de Host de DOS Bloqueada	Seguridad	Habilitar el Filtrado de Ataque de UDP-Flood
• Seguridad Avanzada - Administración Local • Administración Local - Maministración Exercisa • Administración Remota I Habilitar Filtrado de Ataque de TCP-SYN-Flood Controles Parentales Prohibir los Paquetes de TCP-SYN-Flood (5-3600): 50 paquetes/segundo Control de Acceso Prohibir los Paquetes Ping desde el puerto de WAN Enrutamiento Avanzado Prohibir los Paquetes Ping desde el puerto de LAN Control de Ancho de Banda Guardar Lista de Host de DOS Bloqueada IPvo6 Herramientas del Sistema Finalizar Sesión	- Seguridad Básica	Umbral de Paquetes de UDP-Flood (5~3600) : 500 paquetes/segundo
- Administración Local Industrat instactó e Vital de Calueto e Interiore - Administración Local Umbral de Paquetes de TCP-SYN-Flood (5-3600) Controles Parentales Imbral de Paquetes de TCP-SYN-Flood (5-3600) Control de Acceso Imbral de Paquetes Ping desde el puerto de WAN Enrutamiento Avanzado Imbral de Paquetes Ping desde el puerto de LAN Control de Ancho de Banda Imbral de Paquetes Ping desde el puerto de LAN Enlace de IP y MAC Imbral de Paquetes Ping desde el puerto de LAN DNS Dinámico Imbral de Sistema Finalizar Sesión Imbral de Sistema	- Seguridad Avanzada	Habilitar Eiltrado de Ataque de TCP.SVN.Elood
- Administración Remota Sinistración Remota Controles Parentales Image: Control de Acceso Control de Acceso Prohibir los Paquetes Ping desde el puerto de WAN Prohibir los Paquetes Ping desde el puerto de UAN Control de Ancho de Banda Enlace de IP y MAC DNS Dinámico IPv6 Herramientas del Sistema Finalizar Sesión	- Administración Local	I initial initial de maguela de l'of services
Controles Parentales Prohibir los Paquetes Ping desde el puerto de WAN	- Administración Remota	
Control de Acceso Prohibir los Paquetes Ping desde el puerto de LAN Enrutamiento Avanzado Control de Ancho de Banda Control de Ancho de Banda Guardar Lista de Host de DOS Bioqueada Ista de Host de DOS Bioqueada DNS Dinàmico IPv6 Herramientas del Sistema Finalizar Sesión	Controles Parentales	✓ Prohibir los Paquetes Ping desde el puerto de WAN
Enrutamiento Avanzado Control de Ancho de Banda Enlace de IP y MAC DNS Dinámico IPv6 Herramientas del Sistema Finalizar Sesión	Control de Acceso	Prohibir los Paquetes Ping desde el puerto de LAN
Control de Ancho de Banda Enlace de IP y MAC DNS Dinámico IPv6 Herramientas del Sistema Finalizar Sesión	Enrutamiento Avanzado	
Enlace de IP y MAC DNS Dinámico IPv6 Herramientas del Sistema Finalizar Sesión	Control de Ancho de Banda	Guardar Lista de Host de DOS Bloqueada
DNS Dinámico IPv6 Herramientas del Sistema Finalizar Sesión	Enlace de IP y MAC	
IPv6 Herramientas del Sistema Finalizar Sesión	DNS Dinámico	
Herramientas del Sistema Finalizar Sesión	IPv6	
Finalizar Sesión	Herramientas del Sistema	
	Finalizar Sesión	

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.

Ptp-link No. De M	inalambrico N 300Mbps WR840N lodelo TL-WR840N
Estado	
Configuración Rápida	-
Modo de operación	Administración Local
Red	
Inalámbrico	Beglas de Administración
Red para Invitados	 Todo Las PCs en la LAN tienen permitido acceder a la Utilidad a través de Internet del Router
DHCP	Únicamente las PCs listadas pueden navegar en la páginas web integradas para realizar las tareas del Administrador
Transferencia	MAC:
Seguridad	La Dirección MAC de su PC: 74:D4:35:A1:0C:CB Configurar
- Seguridad Básica	
- Seguridad Avanzada	
- Administración Local	Guardar
- Administración Remota	
Controles Parentales	
Control de Acceso	
Enrutamiento Avanzado	
Control de Ancho de Banda	
Enlace de IP y MAC	
DNS Dinámico	

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

Rout	er inalámbrico N 300Mbps WR840N
	Modelo TL-WR840N
Estado	
Configuración Rápida	
Modo de operación	Administracion Remota
Red	
Inalámbrico	Puerto de Administración a través de Internet: 80
Red para Invitados	Dirección IP de Administración Remota: 0.0.0.0 (Ingresar 255.255.255.255 para todo)
DHCP	
Transferencia	
Seguridad	Guardar
- 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	

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

₩ HG8245H										
HUAWEI Status WA	N LAN IPV6 WLAN S	ecurity Forward Rules	Network Application System Tools	i						
IP Filter Configuration	Security > IP Filter Configu	ration								
MAC Filter Configuration										
WLAN MAC Filter Configuration	WLAN MAC Filter Configuration On this page, you can configure WAN-to-LAN filter to prohibit some IP addresses in the WAN from accessing the LAN.									
Parental Control Configuration										
Device Access Control	Enable IP Filter:	(Device forwarding perf	ormance will deteriorate if the IP filteri	ng function is enabled.)						
	Filter Mode:	Whitelist 🔻								
				New Delete						
	Rule name	Protocol Direction	LAN-side IP Address	WAN-side IP Address						

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.

HG82	45H										
HUAWEI Status WA	AN LAN IPv6 WLAN S	ecurity Forward Rules	Network Application System Tools	i							
IP Filter Configuration	Security > IP Filter Configu	ration									
MAC Filter Configuration											
WLAN MAC Filter Configuration	On this page, you can o	configure WAN-to-LAN filter to	prohibit some IP addresses in the W	AN from accessing the LAN.							
Parental Control Configuration											
Device Access Control	Enable IP Filter:	(Device forwarding performance)	ormance will deteriorate if the IP filteri	ng function is enabled.)							
	Filter Mode:	Whitelist T									
				New Delete							
	Rule name	Protocol Direction	LAN-side IP Address	WAN-side IP Address							

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

HG824	5H				Logout
HUAWEI Status WAN	LAN IPv6 WLAN	ecurity Forward Rules	Network Application	System Tools	
IP Filter Configuration	Security > MAC Filter Config	guration			
MAC Filter Configuration					
WLAN MAC Filter Configuration	On this page, you can c	onfigure MAC filter to proh	ibit some PCs from acce	essing the Internet.	
Parental Control Configuration					
Device Access Control	Enable MAC Filter:				
	Filter Mode:	Blacklist V			
					New Delete
			Source MAC Ad	dress	

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

W HG824	15H		Logout
HUAWEI Status WAN	N LAN IPv6 WLAN Security For	ward Rules Network Application System Tools	
IP Filter Configuration	Security > WLAN MAC Filter Configuration	1	
MAC Filter Configuration			
WLAN MAC Filter Configuration	On this page, you can configure MAC	filter to prohibit some PCs from accessing the Internet.	
Parental Control Configuration			
Device Access Control	Enable WLAN MAC Filter:		
	Filter Mode:	Blacklist V	
			New Delete
	SSID Index	Source MAC Address	

En Parental Control Configuration podremos configurar el control parental.

HG824	ISH			Logout
HUAWEI Status WAI	N LAN IPv6 WLA	N Security Forward Rules Ne	etwork Application System Tools	
IP Filter Configuration	Security > Parental (Control Configuration		
MAC Filter Configuration	On this page, you	can set Internet access restrictions to	o allow your kids to use the Internet s	afely without direct supervision.
WLAN MAC Filter Configuration	Parental control a	allows you to set the times when your	kids can use the Internet and which w	ebsites they can access.
Parental Control Configuration	Overview Ter	mplate Statistics		<u>Help</u>
Device Access Control	Apply on all dependence	evices 💿 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.*

	HG82	245	45H									Logout
HUAWEI	Status V	WAN I	LAN	IPv6	WLAN	Security	Forward Rules	Network Appl	ication	System Tools		
IP Filter Configuration	'n	Se	ecurity	> Devic	ce Acce	ss Control						
MAC Filter Configura	ation											
WLAN MAC Filter Co		On this page, you can enable or disable permissions to access the device.										
Parental Control Configuration WiFi Service												
Device Access Control			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* \rightarrow *Firewall log*.

	HG8	324 !	5H												Logout
HUAWEI	Status	WAN	LAN	IPv6	WLAN	Security	Forward	Rules	Network	Applicatio	on Sy	stem Tool	ls		
Reboot		5	System	Tools >	 Firewall 	Log									
Configuration File															
Restore Default Con	figuration		On	this pag	ge, you ca	an configu	ire, downlo	ad, and	query a fir	ewall log.					
Maintenance															
User Log			Enal	ble Fire	wall Log:	U ((If enabled,	device	forwarding	performan	ce will t	be deteriora	ated)		
Firewall Log														New	Delete
One-Click Diagnosis	;				Log Ru	ile Status	;		Log	Access Di	rection			Log Rule Action	
ONT Authentication															
Advanced Power Ma	nagement		Dowr	nload a	nd View L	Logs									
Modify Login Passw	ord		Dow	nload L	og File										
Indicator Status Man	agement		Manu	ufacture	r:Huawei	Technolo	gies Co., L	td;							
Open Source Softwa	ire Notice		Seria IP:10 HWV SWV	IINumbo .212.8 (er:494. (er:V3R	er:485754 79; B; 017C10S	436EDF1	1080;								

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.