

Habilitar Firewall en HT2000W

Issue Col-001- Solution 20/11/2017

1. Objetivo

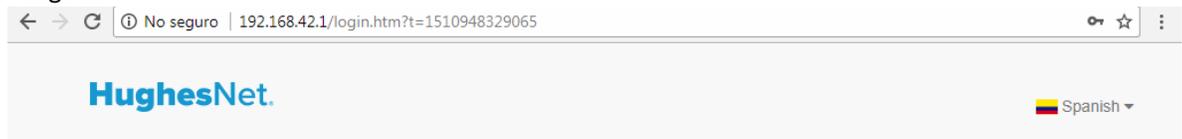
El modem Hughes HT2000W cuenta con un firewall integrado que permite el bloqueo de contenido por medio de URL.

En este manual explicaremos como habilitar esta función en módems con versión v0.09.24 o anteriores. Se debe tener en cuenta:

- a. Para habilitar esta función debe deshabilitar la función de IPv6.
- b. Se debe crear una regla para cada uno de los equipos a bloquear.
- c. Para los equipos que se conectan por cable y WIFI se debe crear una regla para cada uno.

Paso 1: ingrese al módulo administrador.

- En el navegador ingrese a <http://192.168.42.1>
- El password por defecto es "admin" (sin las comillas)
- Luego selecciona INICIAR SESIÓN.



Iniciar sesión

Contraseña Administrativa:

Por favor ingrese la contraseña correcta para el acceso del Administrador. Gracias.

©2017 HUGHES

Paso 2: ingrese a configuración avanzada y seleccione la opción Firewall.

192.168.42.1/advance.htm?t=1510948583840

Spanish Satélite Cerrar sesión

SAN: HCO2000000659 ESN: 12529518

Configuración Avanzada

El router soporta funciones avanzadas como Inspeccion del Estado de los Paquetes, detección de ataques de hackers, filtrado de contenidos, control de acceso, <--hosts virtuales DMZ -->, servidores virtuales y filtrado de clientes.

- Inicio
- Configuración Avanzada**
- INALÁMBRICO
- LAN
- DNS
- Firewall**
- NAT
- QoS

Paso 3: habilite la función de firewall haciendo check en la caja y selecciona grabar configuración.

Spanish Satélite Cerrar sesión

SAN: HCO2000000659 ESN: 12529518

Firewall

Características del Firewall

GRABAR CONFIGURACIÓN CANCELAR

Esta página le permite habilitar/deshabilitar las características del firewall en el router. El firewall protege al router de usuarios malintencionados en Internet.

- Inicio
- Configuración Avanzada
- INALÁMBRICO
- LAN
- DNS
- Firewall**
- Controles Parentales
- Bloqueo URL
- Detección de Intrusos

Paso 4: habilite la función de filtrado chequeando la caja, luego seleccione adicionar regla.

HughesNet

SAN: HCO200000659 ESN: 12529518

Controles Paternos

Función de Filtrado

Tabla de Filtrado Normal (hasta 10 computadores)

Dispositivo Cliente	Regla Habilitada	Servicio Cliente	Regla de Agendamiento	Configurar
pizarra-PC(64:5A:04:31:09:30)	yes	WWW with URL Blocking	Bloquear Siempre	Edit Delete
pizarra-PC(80:EE:73:73:34:FF)	yes	WWW with URL Blocking	Bloquear Siempre	Edit Delete

Adicionar Regla

GRABAR CONFIGURACIÓN CANCELAR

Esta página le permite adicionar reglas que el router usará para bloquear ciertos tipos de tráfico como aplicaciones específicas. Después de seleccionar "Adicionar Regla", puede darle un nombre a la regla y especificar el dispositivo LAN para el cual se debe aplicar la regla. Usted puede habilitar/deshabilitar ciertos servicios que están listados en la página o especificar protocolos particulares y/o rangos de puertos.

Paso 5: Seleccione regla habilitada SI, luego en client device ubique la MAC del equipo al que le aplicara el bloqueo para esto puede en Windows abrir el CMD (en buscar digite cmd y luego enter)

HughesNet

SAN: HCO200000659 ESN: 12529518

HT2000

Programas (1)

- cmd

Archivos (2)

- setup
- setup

Ver más resultados

cmd

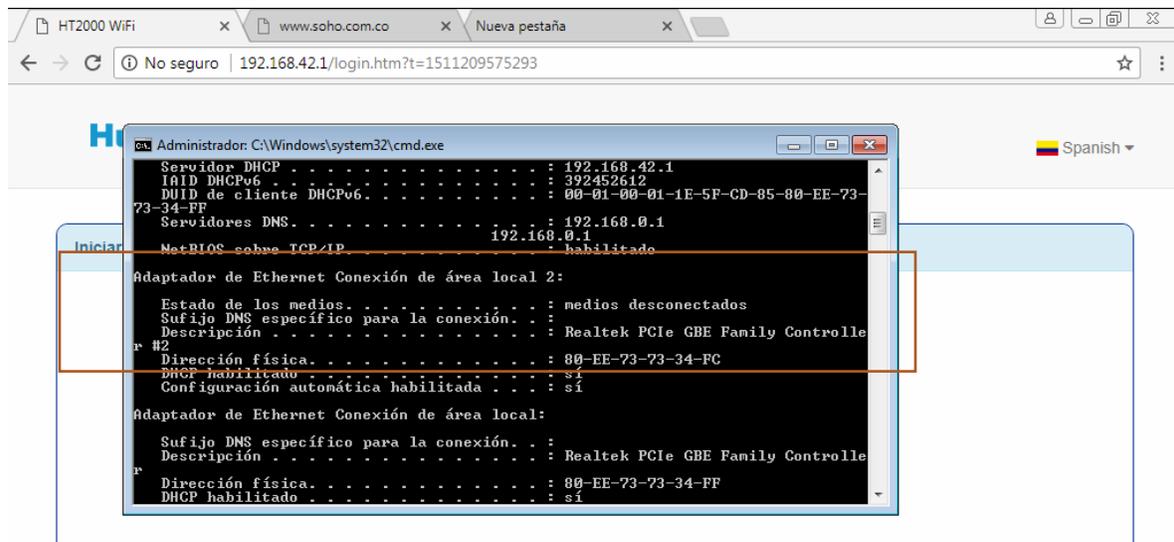
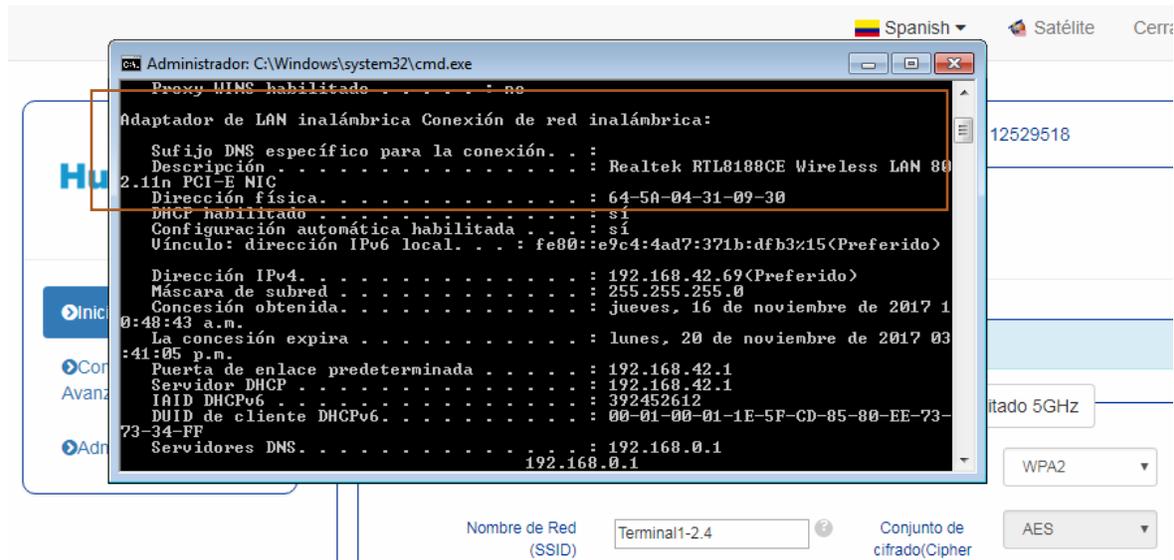
Apagar

GRABAR CONFIGURACIÓN CANCELAR

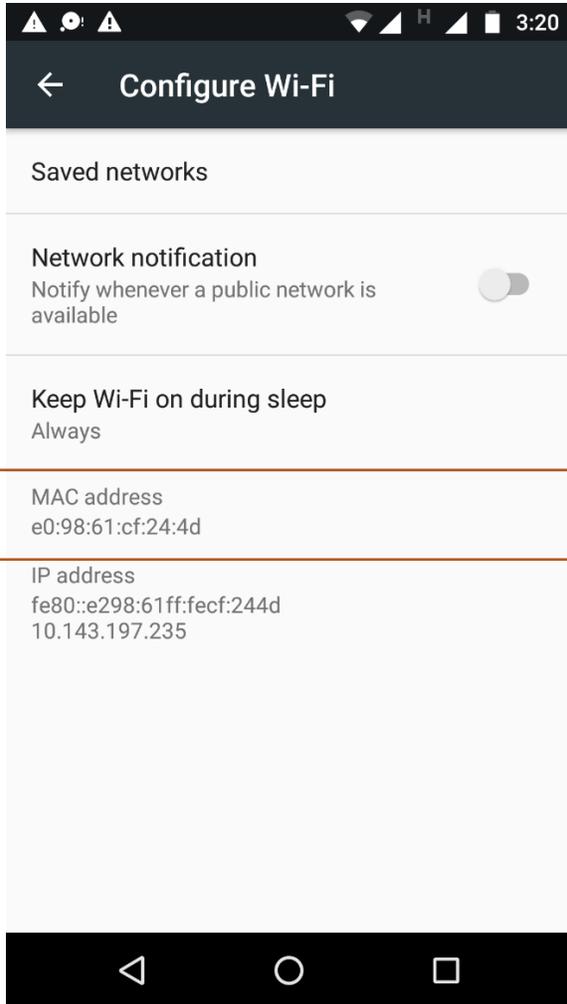
03:14 p.m. 20/11/2017

Una vez en el cmd digite el comando `ipconfig -all` y buscar la MAC o dirección física del adaptador de red.

- Si se conecta por WIFI buscar la dirección física del adaptador inalámbrico.
- Si se conecta por cable al modem buscar la conexión área local Ethernet.



En caso de bloquear un celular, ingrese a configuración -> WIFI -> ajustes



Una vez seleccionado el dispositivo a bloquear damos check en la casilla www with URL Blocking.

Spanish Satélite Cerrar sesión

SAN: HCO200000659 ESN: 12529518

Controles Paternos

Regla Habilitada si no

Client Device 54:C4:15:E1:55:54

Servicio Cliente

Nombre del Servicio	Descripción Detallada	Bloqueo
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

Paso 6: En la opción de agendamiento de Regla seleccionar “bloquear siempre” y luego Grabar la configuración.

Firewall

Controles Parentales

Bloqueo URL

Detección de Intrusos

DMZ

IPv6

NAT

QoS

Enrutamiento

IPv6

Administración

WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

Servicio Definido por el Usuario

Protocolo TCP UDP

Rango de puertos

BORRAR

Agendamiento de Regla

GRABAR CONFIGURACIÓN CANCELAR

Paso 7: Los pasos 5 y 6 se deben repetir por cada dispositivo al que se quiera aplicar el bloqueo. Si desea conectar dispositivos directamente al modem (por cable) deberá agregar una regla para cada MAC. Recuerde el paso 5 para obtener la MAC y crear la regla de control parental.

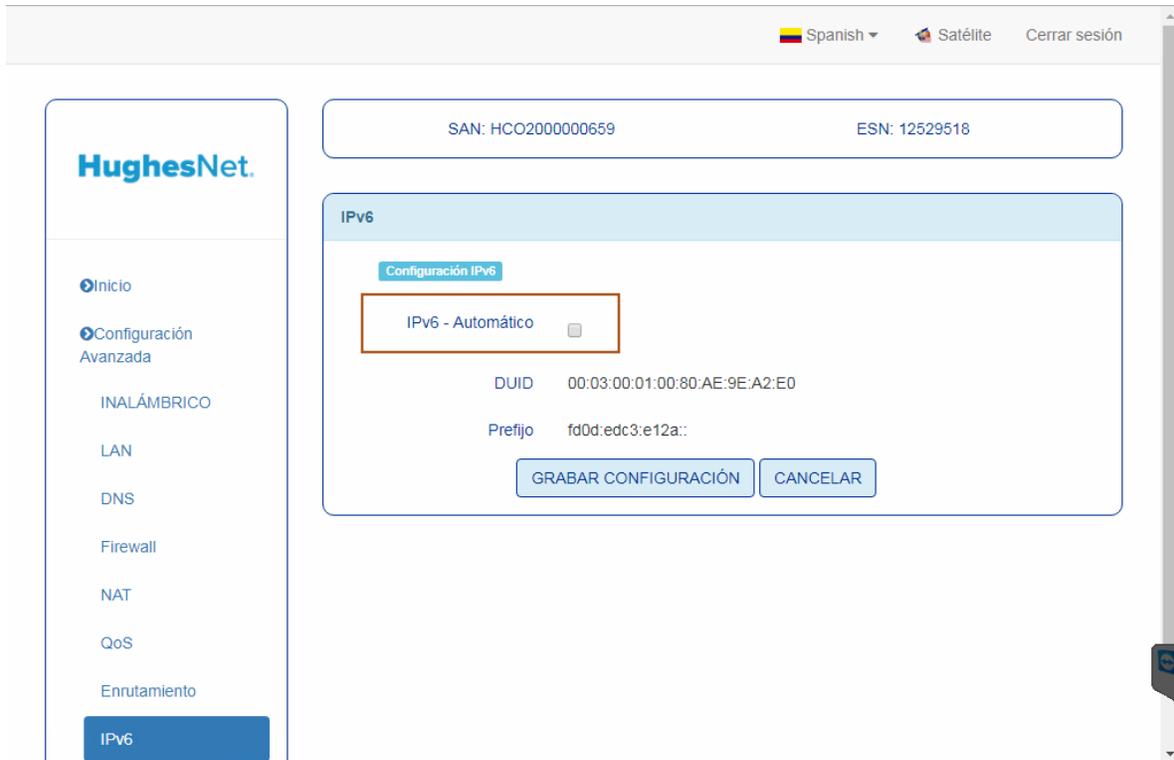
Paso 8: Verifique que las reglas creadas aparecen habilitadas.

Dispositivo Cliente	Regla Habilitada	Servicio Cliente	Regla de Agendamiento	Configurar
pizarra-PC(64:5A:04:31:09:30)	yes	WWW with URL Blocking	Bloquear Siempre	Edit Delete
pizarra-PC(80:EE:73:73:34:FF)	yes	WWW with URL Blocking	Bloquear Siempre	Edit Delete

Paso 9: en la opción de Bloqueo URL ingrese los nombres de dominios a bloquear (debe ser el dominio sin el www inicial), por ultimo grabar configuración.

No.	URL / Palabra clave
Sitio 1	eltiempo.com
Sitio 2	facebook.com
Sitio 3	soho.com.co
Sitio 4	
Sitio 5	
Sitio 6	
Sitio 7	
Sitio 8	
Sitio 9	
Sitio 10	

Paso 10: Por ultimo en configuración avanzada en la opción IPV6, asegúrese que la opción IPv6 – Automático esta deshabilitada y grabar la configuración.



The screenshot shows the HughesNet configuration interface. At the top right, there are options for 'Spanish', 'Satélite', and 'Cerrar sesión'. The main content area is divided into a left sidebar and a main panel. The sidebar contains the HughesNet logo and a list of configuration options: Inicio, Configuración Avanzada, INALÁMBRICO, LAN, DNS, Firewall, NAT, QoS, Enrutamiento, and IPv6 (which is highlighted). The main panel displays the IPv6 configuration settings. At the top, it shows 'SAN: HCO2000000659' and 'ESN: 12529518'. Below this, there is a section titled 'IPv6' with a sub-section 'Configuración IPv6'. In this section, the 'IPv6 - Automático' option is shown with an unchecked checkbox. Below the checkbox, the 'DUID' is '00:03:00:01:00:80:AE:9E:A2:E0' and the 'Prefijo' is 'fd0d:edc3:e12a::'. At the bottom of the configuration area, there are two buttons: 'GRABAR CONFIGURACIÓN' and 'CANCELAR'.

Con esta configuración al reiniciar el navegador los equipos que se indicaron en la regla no podrán ingresar a las páginas bloqueadas.