Guía rápida
Arris TG862

1. Introducción

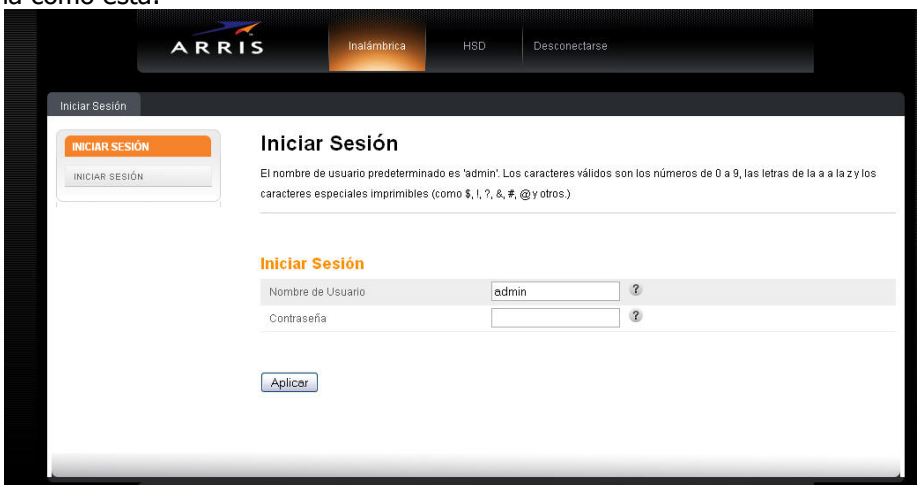
El nuevo cable módem router Arris TG862 introduce nuevas funcionalidades que hasta ahora ningún equipo doméstico era capaz de hacer. Esta guía pretende servir para configurar su enrutador y para describir estas nuevas funcionalidades de manera concisa pero clara.

2. Configuración de la conexión inalámbrica

El nuevo cable módem router Arris TG862, dispone de la última tecnología WIFI, por lo que si su dispositivo inalámbrico tiene una tarjeta WIFI 802.11n puede conectarse hasta a 300mbps.

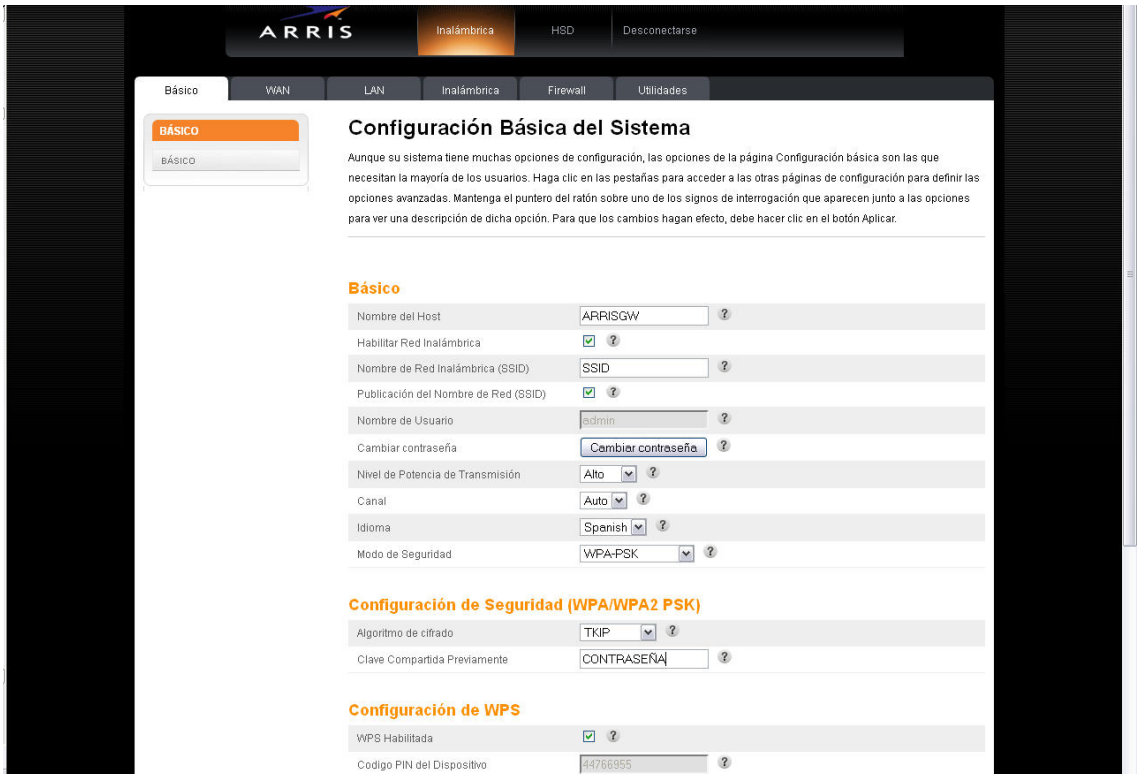
Para configurar su router, en primer lugar, debe abrir un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1.

A continuación se mostrará una página donde se le solicita nombre de usuario y contraseña como ésta:



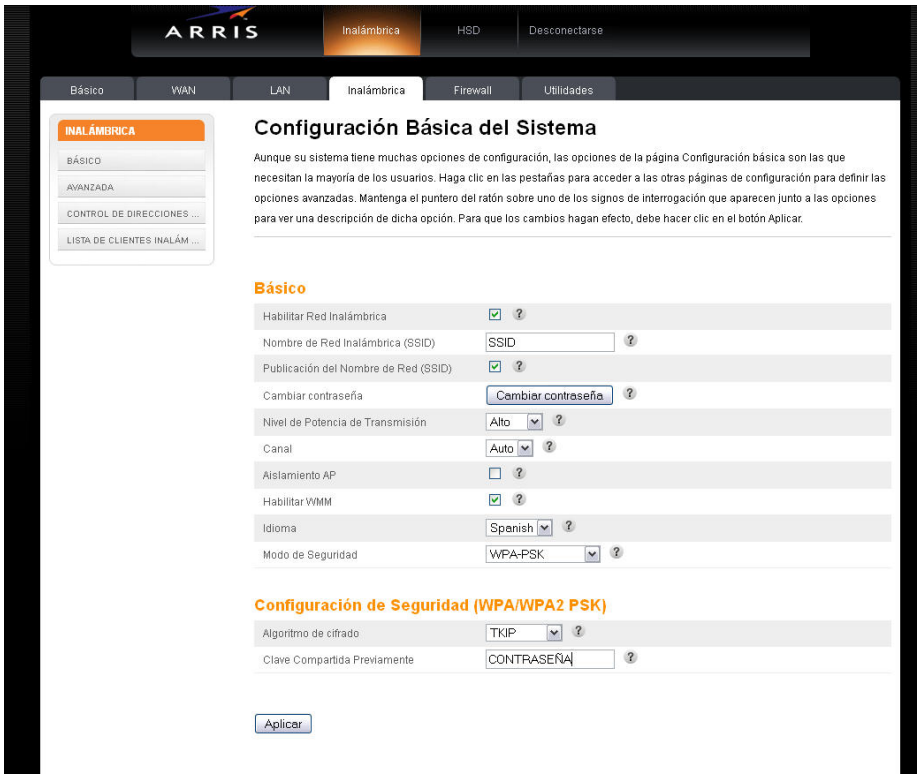
Las credenciales de acceso son:
Username: admin
Password: password

Una vez introducidas las credenciales, hacemos click en el botón "Aplicar". Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:



Desde esta pantalla se pueden configurar rápidamente los aspectos básicos de nuestro router, tales como el nombre de nuestra red inalámbrica, la contraseña de la misma, el canal de emisión, el nivel de transmisión de la red WIFI el idioma del sistema o la contraseña para acceder al router.

Si deseamos una configuración más minuciosa, debemos picar en la pestaña "Inalámbrica", situada en la parte superior del menú. Se nos mostrará la siguiente pantalla:



Desde la pestaña "Básico" tenemos las siguientes opciones:

- Habilitar Red Inalámbrica: si deseamos desactivar la conexión inalámbrica tan solo tenemos que deshabilitarla desde esta opción.
- Nombre de Red Inalámbrica (SSID): el nombre de nuestra red WIFI.
- Publicación del Nombre de Red (SSID): desmarque esta opción si no desea que su red WIFI sea visible.
- Nivel de Potencia de Transmisión: nivel de potencia de transmisión de su red WIFI, puede definirse como "Baja", "Media" y "Alta".
- Canal: define el canal de emisión de su router. Se recomienda usar los canales 1, 6 ó 11. Si detecta bajo rendimiento en su conexión WIFI, esto puede deberse a la proximidad de otro router WIFI que está provocando interferencias, pruebe a cambiar el canal hasta que el rendimiento mejore.
- Aislamiento AP: si desea que los dispositivos conectado por WIFI no puedan comunicarse con los dispositivos conectados por cable, marque esta opción.
- Habilitar WMM: aplica opciones de calidad de servicio para la transmisión de multimedia a través de WIFI.
- Idioma: Idioma del sistema.
- Modo de seguridad: las opciones son: **Open**, sin ningún tipo de seguridad; **WEP**, encriptación débil, se recomienda no usar a no ser que su equipo inalámbrico no soporte WPA; **WPA-PSK**, el método de encriptación más seguro; **WPA2-PSK**, evolución de la anterior, más segura pero menos compatible con tarjetas inalámbricas antiguas; **WPA/WPA2-PSK**, modo mixto, se recomienda su uso.
- Algoritmo de cifrado: método de cifrado de la clave de su WIFI. Si se desea usar toda la potencia del router, se debe seleccionar como método de cifrado "AES". Si experimentase algún tipo de problema con su conexión inalámbrica, se recomienda utilizar el algoritmo TKIP.
- Clave Compartida Previamente: contraseña de acceso a su red WIFI.

Aunque las opciones básicas son suficientes para un usuario medio, pasamos a describir someramente las opciones de configuración "Avanzada". Se recomienda encarecidamente no modificar estas opciones a no ser que se sea plenamente consciente de qué se modifica:

- Modo inalámbrico: define la evolución de la tecnología inalámbrica a usar, 802.11b (hasta 11 mbs), 802.11g (hasta 54 mbs), 802.11n (hasta 300mbs) o los modos mixtos. Se recomienda la opción "B/G/N mixed".
- Protección BG: si dispone de dispositivos 802.11b y tiene problemas, seleccione esta opción.
- Intervalo de Baliza: tiempo que pasa en milisegundos entre las transmisiones "baliza" entre el router y los dispositivos. Se recomienda no modificar.
- Intervalo DTIM: define el intervalo de mensaje indicativo del tráfico de entrega. Se recomienda no modificar.
- Umbral RTS: define el límite de tamaño de paquete.
- Umbral de fragmentación: este umbral debe definirse como igual al tamaño máximo permitido del marco Ethernet en el enlace. Se recomienda no modificar.
- Frame Burst: el Frame Burst es una modalidad que permite maximizar el rendimiento de su conexión WIFI, y mejora la transmisión en redes mixtas.
- Modo de Ahorro de Energía WMM: método de gestión de energía más eficaz que el antiguo sondeo.
- Modo de Funcionamiento: si sus dispositivos inalámbricos son todos 802.11n seleccione el modo "Greenfield", de lo contrario no modifique esta opción.
- Ancho de Banda del Canal: define el ancho de banda del canal 802.11n.
- Intervalo de protección: espacio entre la transmisión de símbolos en nanosegundos.
- MCS: Define el esquema de codificación y modulación 802.11n que se va a utilizar.

En la pestaña "Control de direcciones…" se nos permite aplicar filtros por direcciones MAC.

En la pestaña "Lista de clientes inalám…" se nos muestra los equipos conectados a través de nuestra conexión WIFI.

Gestión del cortafuegos

La gestión de un cortafuegos es una tarea muy compleja, pues este elemento es el responsable de controlar los intentos de intrusión en los equipos que hay conectados al router, por lo que cualquier modificación ha de ser hecha sabiendo muy bien qué deseamos hacer, para sí no comprometer la seguridad.

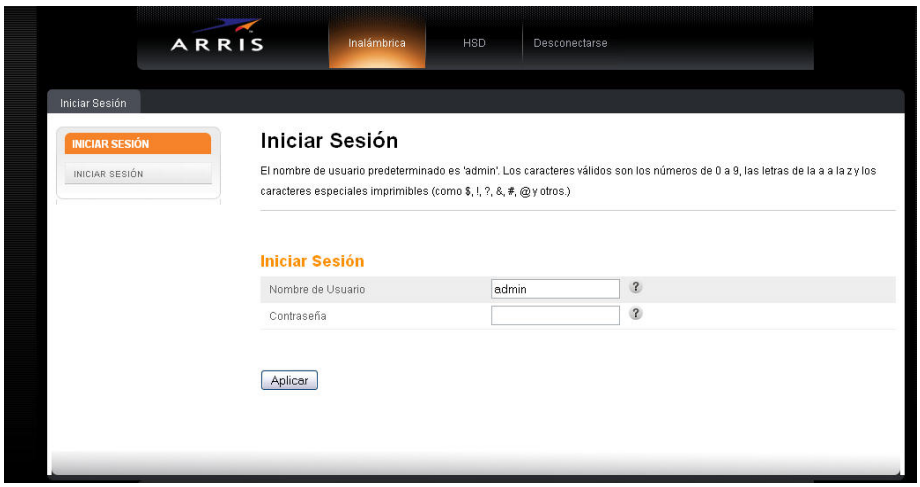
Con este espíritu, tan sólo vamos a explicar en este apartado cómo abrir los puertos para un determinado programa, y como crear una DMZ para un equipo que necesita muchos puertos abiertos, como por ejemplo una consola de videojuegos.

2.1 Abrir un puerto o un rango de puertos

Si tenemos una aplicación instalada en nuestro ordenador que necesita tener un puerto o un rango de puertos, ya sea TCP o UDP abiertos (por favor, consulta la ayuda de tus aplicaciones para conocer este dato), vamos a pasar a explicar cómo realizar esta tarea.

En primer lugar debe abrir un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1

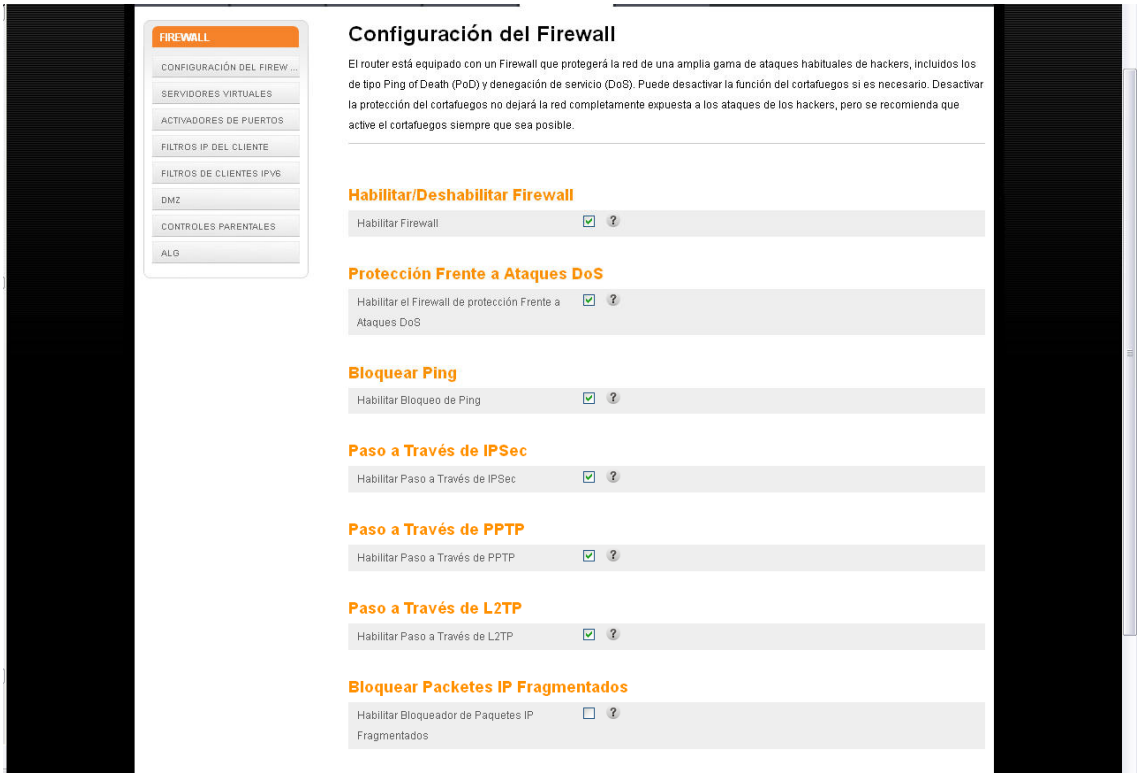
A continuación le saldrá una página donde se le solicita nombre de usuario y contraseña como ésta:



Las credenciales de acceso son:
Username: admin
Password: password

Una vez introducidas las credenciales, hacemos click en el botón "Aplicar". Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:

Una vez hemos accedido al router, en el menú de la superior seleccionamos la opción "Firewall", accederemos a la siguiente página:



Estas son las opciones básicas de bloqueo de ataques al router. Si por necesidades especiales, desea que su router sea accesible a Ping desde otra conexión a Internet, debe deshabilitar la opción "Bloquear Ping".

Para abrir un puerto o un rango de puertos haga click en la pestaña "Servidores Virtuales". Debe aparecer una Web como esta:

Haga Click en el botón "Agregar":

Pasamos a explicar brevemente cada una de las opciones:

- Descripción: nombre de la aplicación, una simple etiqueta para reconocer el programa al que hemos abierto el o los puertos.
- Puerto de entrada: rango público de puertos. Rango de puertos que la aplicación necesita tener abiertos. Si tan sólo es un puerto, se rellenarán ambos campos con el mismo, si es un rango de puertos se pondrá en el primer campo el primer puerto del rango y en el segundo campo el último campo.
- Formato: protocolo que usará el puerto o los puertos, TCP/UDP/Ambos.
- Dirección IP privada: dirección IP del ordenador en el que se desea tener los puertos abiertos.
- Puerto Local: rango privado de puertos. Puertos configurados en el ordenador para el servicio configurado, normalmente se usan los mismos valores que en el "Puerto de entrada".

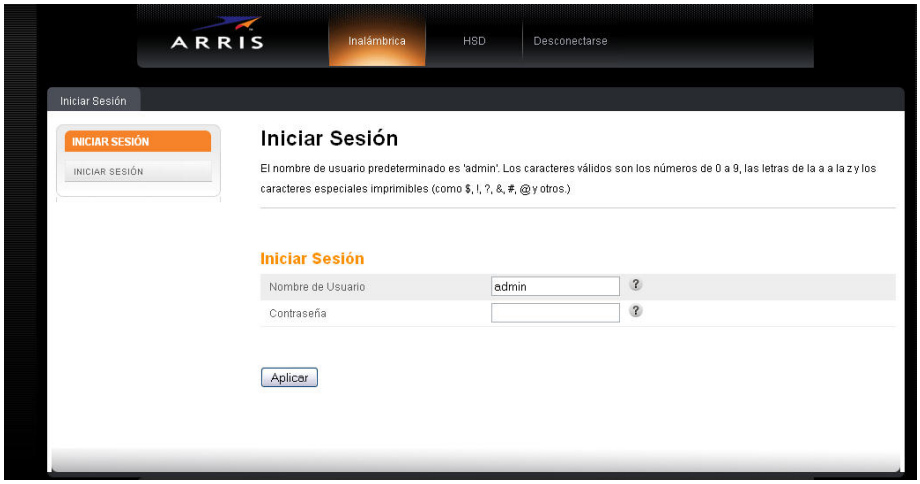
Una vez cumplimentados todos los campos pulsamos el botón "Agregar Servidor Virtual" y se salvarán los datos.

2.2 Crear una DMZ

En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. El motivo por el cual creamos una DMZ es para que un equipo no tenga ninguna limitación en cuanto a apertura de puertos. Un ejemplo de equipos ideales para estar en una DMZ son un segundo router o una consola de videojuegos. Es poco aconsejable poner un PC en una DMZ, pues será vulnerable a ataques e intentos de intrusión.

En primer lugar debe abrir un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1

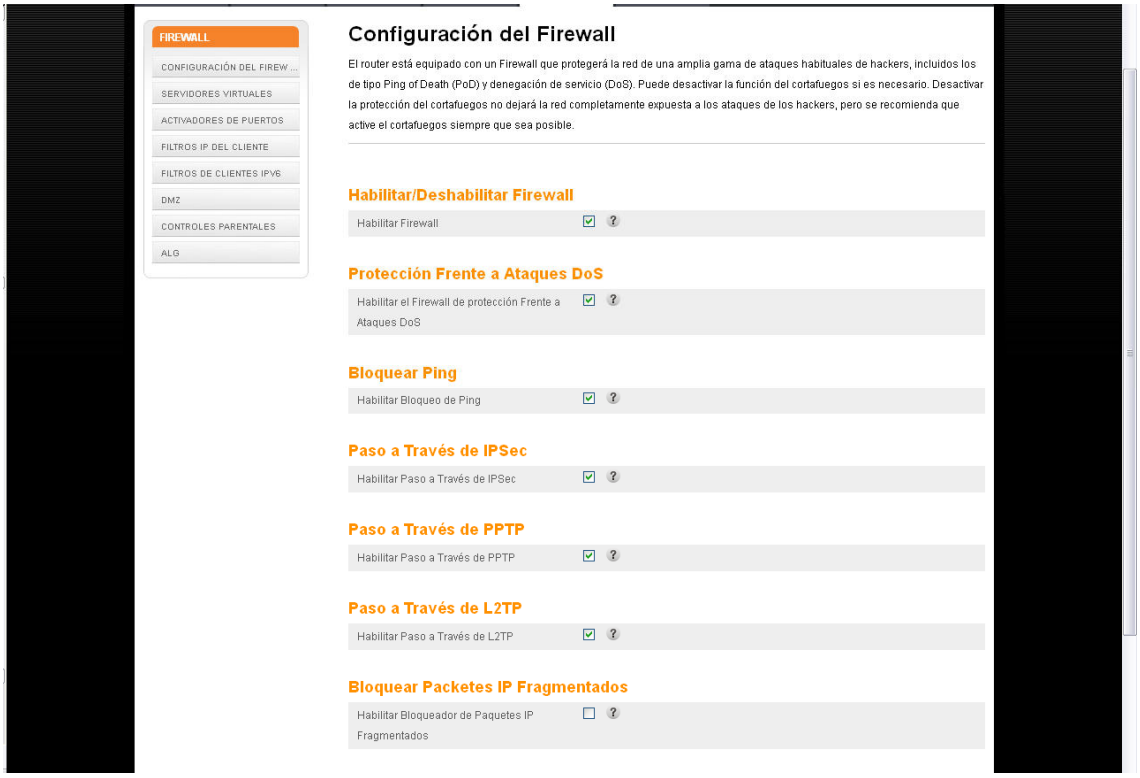
A continuación le saldrá una página donde se le solicita nombre de usuario y contraseña como ésta:



Las credenciales de acceso son:
Username: admin
Password: password

Una vez introducidas las credenciales, hacemos click en el botón "Aplicar". Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:

Una vez hemos accedido al router, en el menú de la superior seleccionamos la opción "Firewall", accederemos a la siguiente página:



Hacemos click en la pestaña "DMZ" que nos dará acceso a la siguiente página:

Aquí marcaremos la casilla "Habilitar DMZ" y en el campo "IP Privada" pondremos la dirección IP del equipo que deseamos incluir en la DMZ. Tan sólo podemos incluir un equipo en la DMZ. Recomendamos que el equipo incluido en la DMZ no esté configurado con DHCP, si no que tenga fijada una IP del rango privado del router.

Anexo

SSID:_____

Contraseña:_____