Net-LAN

Guía rápida de Firewall en sedes Net-LAN

Índice

1. INTRODUCCIÓN

El servicio de Firewall en Sedes Net-LAN es una funcionalidad adicional de las Sedes del Servicio Solución Net-LAN en sus dos modalidades, Estándar y Avanzada.

Mediante este servicio, contratable por sede, se ofrece a las Sedes del Servicio Net-LAN la posibilidad de filtrar la entrada y salida del tráfico de sus sedes, haciendo más segura la misma y además controlando de esta manera el uso del ancho de banda.

El servicio se implementará con un nuevo equipo, Zywall 35 de Zyxel que actúa como Firewall. A su vez el nuevo equipamiento (FW-LAN a partir de ahora) sirve para soportar el servicio de Cifrado.

La gestión de los niveles de seguridad se realizará a través del portal de gestión Net-LAN, que incluirá adicionalmente los informes de servicio.

Existen diferentes niveles seguridad (Nulo, Bajo, Medio y Alto) prefijados para cada pareja de zonas (LAN-WAN, WAN-LAN, DMZ-LAN, LAN-DMZ, WAN-DMZ y DMZ-WAN), así como la también existe la opción de realizar una configuración personalizada de las reglas de filtrado y también una opción de activar y desactivar por completo el Firewall.

2. FUNCIONALIDADES

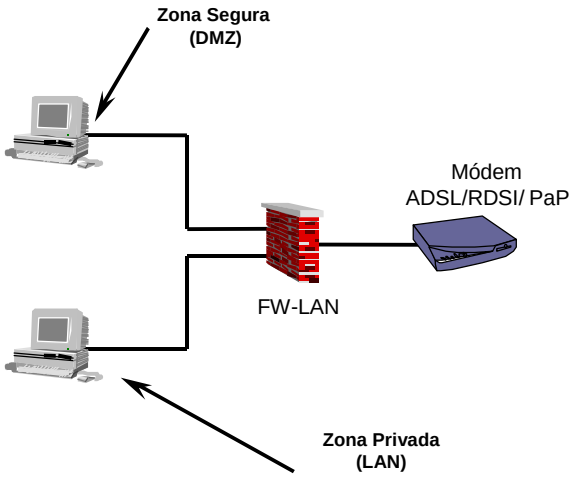
2.1 Introducción:

Como ocurre en la mayoría de los Firewall basados en un equipo hardware, el FW-LAN dispone de tres zonas: WAN, LAN y DMZ. Así se pueden tener diferenciadas dos zonas dentro de la Sede de la RPV (LAN y DMZ). La otra zona, la WAN, será la que represente el exterior de la sede y estará directamente conectada con el router (EDC).

El nivel de seguridad de estas zonas es configurado a través del portal de gestión del servicio, en www.movistar.es/negocios/netlan. Estas zonas se definen habitualmente como:

- Zona Segura (DMZ): esta zona no debe contener datos de tipo crítico sin copia de seguridad. En definitiva, esta zona estará destinada a información que pueda ser reemplazada de forma rápida y fácil. Con esta arquitectura, permitimos que el servidor sea accesible por usuarios de la propia RPV, de tal forma que si es atacado y se accede a él, la red local sigue protegida por el Firewall.

- Zona Privada (LAN): esta zona esta destinada a máquinas que contengan servidores críticos y equipos de usuarios que queremos mantener completamente seguros.



Dentro de cada zona, se podrán definir distintos niveles de seguridad prefijados según la zona origen y destino. Además se permitirá una configuración personalizada a la medida del cliente.

Para la configuración de las distintas posibilidades del servicio de Firewall, tiene a su disposición un área específica dentro del Portal del Servicio Net-LAN donde puede elegir entre las siguientes funcionalidades:

- Gestión de Configuración de su Firewall, disponible en la pestaña de Gestión Avanzada de su RPV-IP.
- Informes de tráfico en cuanto a paquetes válidos y filtrados en cada interfaz, y número de reglas activadas, desactivadas, etc. Dicha documentación será accesible desde el apartado de Informes del Portal de Gestión del Servicio Net-LAN.

En el apartado de "Gestión de Configuración de su Firewall" aparece un listado con las Sedes de la RPV que tengan contratado el servicio de Firewall identificadas por el número de teléfono. La gestión se realizará sede a sede, por lo que deberá seleccionarse una sede para modificar la configuración de la misma.

La configuración por defecto del servicio Firewall es nivel bajo de seguridad. Este nivel de configuración por defecto aplica a todas las subredes del servicio Firewall (WAN, LAN y DMZ).

2.2 Habilitación/deshablitación del Firewall

En la pantalla de Gestión de Configuración de su Firewall existe la posibilidad de habilitar y deshabilitar el Firewall. Esta funcionalidad no debe considerarse como un nivel de configuración ya que deshabilita toda la seguridad implementada en el Firewall.

Se recomienda un uso limitado de esta opción de desactivación, únicamente para realizar pruebas de conectividad y de comprobación del filtrado de la sede. La principal ventaja que tiene esta funcionalidad es que no se pierden las reglas que el Firewall tuviera configuradas. Esta opción no debe confundirse con el nivel de seguridad Nulo que se presentará a continuación en el siguiente apartado.

2.3 Niveles de Seguridad

Dentro del portal de configuración del Servicio, se tiene la posibilidad de elegir entre los niveles de seguridad Alto, Medio, Bajo, Nulo y Personalizado. Dichos niveles se aplican a las parejas de zonas y quedan definidos según:

- **Nivel Alto**

- LAN-WAN, DMZ-WAN, LAN-DMZ: se permite el tráfico DNS, FTP, HTTP, HTTPS, SMTP, POP3, IMAP e IMAPS.

- WAN-LAN, DMZ-LAN, WAN-DMZ: se deniega todo el tráfico.

- **Nivel Medio**

- LAN-WAN, DMZ-WAN, LAN-DMZ: se permite todo el tráfico.

- WAN-LAN, DMZ-LAN, WAN-DMZ: se deniega todo el tráfico.

- **Nivel Bajo** (por defecto):

- LAN-WAN, DMZ-WAN, LAN-DMZ: se permite todo el tráfico.

- WAN-LAN, DMZ-LAN, WAN-DMZ: se permite el tráfico NETBIOS, DNS, FTP, HTTP, HTTPS, SMTP, POP3, IMAP e IMAPS.

Es decir, si se sitúan todas las zonas en **nivel alto** se permitirá únicamente tráfico DNS, FTP, HTTP, HTTPS, SMTP, POP3, IMAP e IMAPS con origen las zonas de la sede (DMZ y LAN) y destino cualquier otra dirección y se deniega el resto. Si se configuran con **nivel medio** todas las parejas de zonas se permite todo el tráfico IP con origen en la Sede y destino cualquier otra dirección,

denegándose el resto. Y en caso de que todas las parejas se configuren con **nivel bajo** se permite todo el tráfico IP con origen las zonas de la sede y destino cualquier otra dirección y se permite el trafico NETBIOS, DNS, FTP, HTTP, HTTPS, SMTP, POP3, IMAP e IMAPS destinado a las zonas del cliente.

Existe también otro nivel adicional para cada pareja de zonas denominado **Nulo**. Este nivel elimina todas las reglas y permite el paso de todo el tráfico entre las zonas definidas en la pareja. Por ejemplo si se configura nivel nulo para la pareja LAN-DMZ, se permitirá todo el tráfico de la LAN a la DMZ.

2.4 Nivel de Seguridad Personalizado. Configuración de reglas:

Este nivel de seguridad se obtendrá modificando las reglas correspondientes a un nivel prefijado (alto, medio, bajo y nulo). Para ello deberá accederse al enlace de configuración de reglas del Firewall.

Recordar en este punto que los niveles prefijados se configuran sobre las parejas de zonas y que no es necesario que todas las parejas tengan el mismo nivel de seguridad. De hecho puede haber niveles personalizados en unas y prefijados en otras.

Las reglas de filtrado se pueden crear, modificar, eliminar y activar y desactivar. De esta forma, podemos tener una lista amplia de reglas y activar/desactivar y eliminar cuando lo deseemos. Para que los cambios de configuración entre en servicio se deberá salvar la configuración.

Los datos necesarios para configurar una regla son: direcciones de origen y destino, pareja de zonas que indica la zona origen y destino, protocolo de transporte y puerto.

Para facilitar la configuración de las reglas, se ha habilitado la posibilidad de configurar macros de direcciones IP y aplicaciones. Esta funcionalidad permite poner un nombre a una dirección (bien sea una dirección IP, una subred o un rango) y utilizarlo en la configuración de reglas. De modo similar, las aplicaciones pueden también nombrarse para facilitar su uso en la configuración.

Así, a la hora de configurar una regla en el firewall, deberá aportarse la siguiente información:

- Nombre de regla: servirá para identificar la regla en la consulta de las mismas. Será un campo alfanumérico.
- Número prioridad de regla: las reglas se irán aplicando en el ámbito de una pareja de zonas (por ejemplo LAN-WAN) según el número de prioridad que tengan, de menor a mayor. En caso de que un paquete cumpla las condiciones de una regla, se realizará la acción que

indique dicha regla (dejar pasar o bloquear) y no se comprobarán más reglas, pasándose a analizar el siguiente paquete.

- Dirección IP de origen y destino: deberá seleccionarse el origen y destino del tráfico. Podrá seleccionarse una dirección IP, una subred (con su máscara) o un rango. Por su puesto se permitirá el uso de una macro de direcciones IP o un conjunto de ellas.
- Zona de origen y destino: se seleccionará el origen y destino a través de la zona. Esto se realizará mediante la elección de la pareja de zonas (LAN-WAN, WAN-LAN, LAN-DMZ, DMZ-LAN, DMZ-WAN ó WAN-DMZ), donde se indica la zona origen en primer lugar y la destino en el segundo.
- Protocolo: podrá seleccionar entre UDP, TCP, ICMP o IP.
- Puertos origen y destino: se podrá elegir un único puerto, un rango de puertos o una aplicación o conjunto de aplicaciones definido anteriormente.
- Acción a realizar: se indicará aquí la acción a realizar con el tráfico definido en la regla. Las opciones serán las siguientes: permitir (no hace nada con el tráfico, lo deja pasar), o tirar (se prohíbe el acceso y no se anuncia nada, el remitente no sabe qué ha ocurrido exactamente).
- Activa/inactiva: al configurar la regla se deberá seleccionar si inicialmente estará activa o no.

Durante la modificación de una regla se podrán variar cualquiera de estos parámetros. Tras la modificación de reglas deberá confirmarse y enviarse los cambios para que estos tengan efecto.

Los cambios no se enviarán y confirmarán hasta que no se pulse el botón correspondiente. Existe la posibilidad de activar y desactivar varias reglas al mismo tiempo. En caso de que no estén activas todas las reglas definidas, el orden de aplicación se seguirá realizando por su número.

Cuando se tenga un nivel de seguridad nulo, bajo, normal o alto y decida pasar a nivel personalizado, las reglas definidas serán las del nivel de seguridad que se tuviera. Es decir, si un usuario pasa de nivel de seguridad bajo a personalizado, cuando acceda a la configuración de reglas, las que le aparezcan serán las de nivel bajo, las cuales podrá modificar a su gusto.

A su vez si se tiene un nivel de seguridad personalizado y se desea pasar a nivel bajo, medio, alto o nulo, se perderán las reglas definidas y se quedará únicamente con las de dicho nivel.

Por último y como ya se ha adelantado, cuando se accede a la página principal de gestión de Firewall de una sede, aparecerá una indicación de si el firewall está o no activado. En ese caso podrá activar y desactivar el firewall cuando lo desee. Al ser una funcionalidad que deja sin servicio se recomienda un uso limitado y sólo en caso de querer probar si el filtrado es correcto.

2.5 Informes del Servicio

Los informes de estos dos servicios en el Portal del Servicio serán comunes para todos los usuarios independientemente de si la sede es Avanzada o Estándar.

Dentro de la zona de Informes del servicio Firewall, se puede consultar información relativa a:

- Rendimiento: CPU, memoria
- Tráfico y errores de las interfaces
- Informe de tráfico filtrado y conmutado, por interfaz de red
- Informe de Evolución temporal de Instalación de nuevas políticas.
- Informe de ataques. Éstos nos informarán de un intento de conexión, tanto si se trata de una conexión exterior, como de otro equipo perteneciente a nuestra RPV-IP.

2.6 Opciones adicionales del Servicio

El servicio Firewall en sedes Net-LAN está incluido dentro del servicio de Mantenimiento Seguridad Integral 12h, 8h y 6 h, sin coste adicional.

Además el equipamiento Zywall está incluido en el servicio de Firewall en LAN y en caso de avería del mismo será sustituido sin desembolso por parte del cliente.

Se ofrece la posibilidad de contratación del servicio sin equipamiento, sólo en aquellos casos en que el Cliente disponga de uno compatible con el servicio tanto en modelo como en versión de firmware.

Junto a las modificaciones propias del servicio Net-LAN, se permite la modificación de los parámetros de la subred DMZ (dirección IP LAN DMZ, dirección IP subred DMZ, máscara subred DMZ) facilitada en el momento de la contratación del Servicio Firewall.

3. DESCRIPCIÓN DEL PORTAL DE CONFIGURACIÓN

3.1 Acceso al Portal de Solución Net-LAN

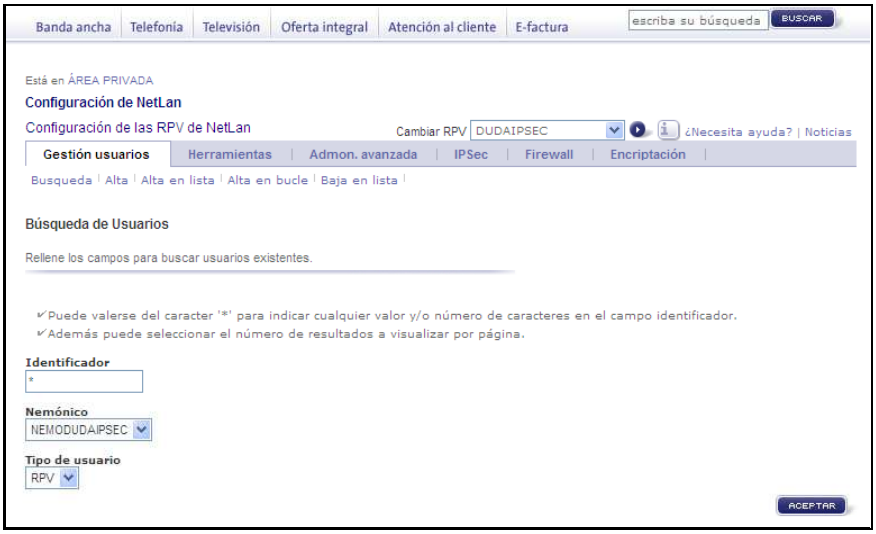
Para acceder al portal del servicio, tendremos que teclear en el navegador la dirección http://www.movistar.es/negocios/netlan

Una vez en una dirección, se deberá pinchar en el enlace, "Gestione online la Solución ADSL Net-LAN", donde se nos pedirán el Nombre de Usuario, así como la Contraseña.

Una vez validados, accederemos al Portal del Servicio, nos encontraremos ante una pantalla como la que sigue:

En el caso de tener más de una RPV-IP contratada, se le pedirá elegir la RPV que quiere gestionar. La elección será mediante un menú desplegable.

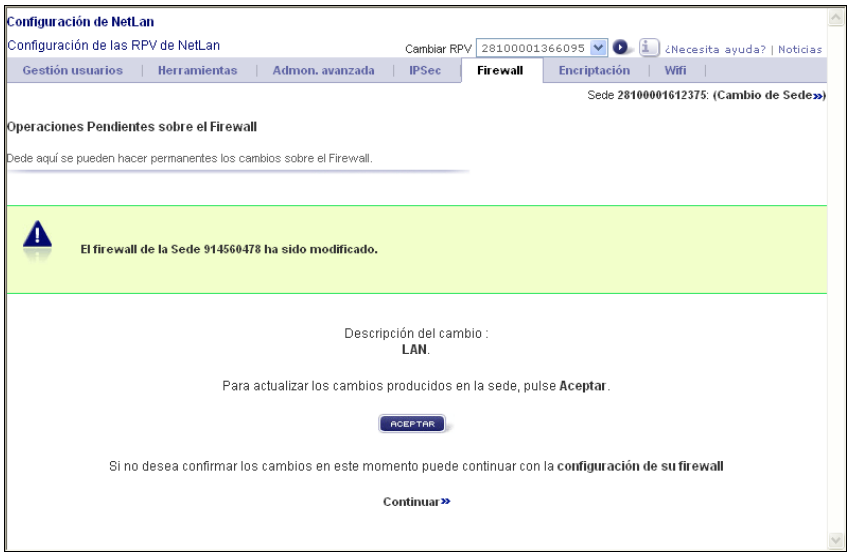
Esta es la página de entrada al sistema. En ella se muestran algunos datos del administrador como su nombre. Aparece también una lista de menús de primer nivel con las posibles opciones del usuario en función de lo que tenga contratado. También verá la RPV elegida así como la opción de cambiar de RPV en cualquier momento dando a la flecha existente al lado del desplegable.



Pestañas en la parte superior permitirán salir de la navegación del portal Net-LAN hacia otros apartados de TOL sin perder la sesión.

En el menú principal aparecerán dos pestañas de Firewall y Cifrado, tal y como se muestra en la figura anterior. En caso de que se tenga contratado el servicio en alguna sede, al pinchar sobre la pestaña correspondiente se permitirá elegir la sede a configurar el Firewall o el Cifrado respectivamente.

Al seleccionar la opción de Firewall para una sede determinada mediante su número de teléfono, el sistema comprobará si existen operaciones pendientes y las realizará, mostrando el resultado.



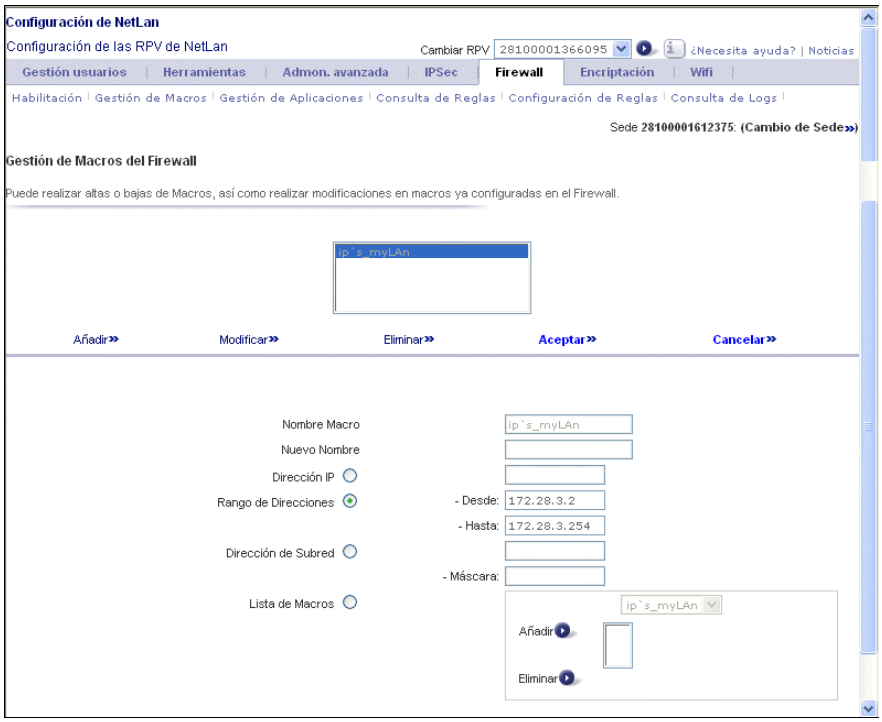
Si no existieran operaciones pendientes o se pincha en el enlace de menú Firewall, entonces se mostraría el siguiente menú:

Desde este menú principal se puede ver el estado del Firewall, pudiendo estar HABILITADO o DESHABILITADO existiendo la posibilidad de realizar la acción contraria.

La finalidad de la gestión del Firewall es la de creación de Reglas, para ello existen las facilidades de la gestión de Macros (filtrado por IP o segmentos de IPs) y de Aplicaciones (puerto y protocolos) que facilitan en gran medida la gestión de las reglas.

3.2 Gestión de Macros

Esta pantalla permitirá una gestión completa de las Macros. En primer lugar se tendrá una lista de las macros existentes con las opciones de eliminación, modificación o de añadir nuevas macros. Cada una de estas acciones se completará al dar a Aceptar, o en el caso contrario, se cancelará pulsando en Cancelar.



Si se desea añadir una nueva Macro, se deberá pulsar en Añadir, entonces se deshabilitará la lista y se mostrará activo el campo Nombre Macro, así como una de las posibles opciones de la que se compone una Macro:

- Dirección IP
- Rango de direcciones IP
- Dirección de Rango, con máscara
- Lista de Macros: Ya que una macro puede constar de varias macros, por lo que aparecerá de nuevo la lista con la posibilidad de añadir las que el usuario desee.

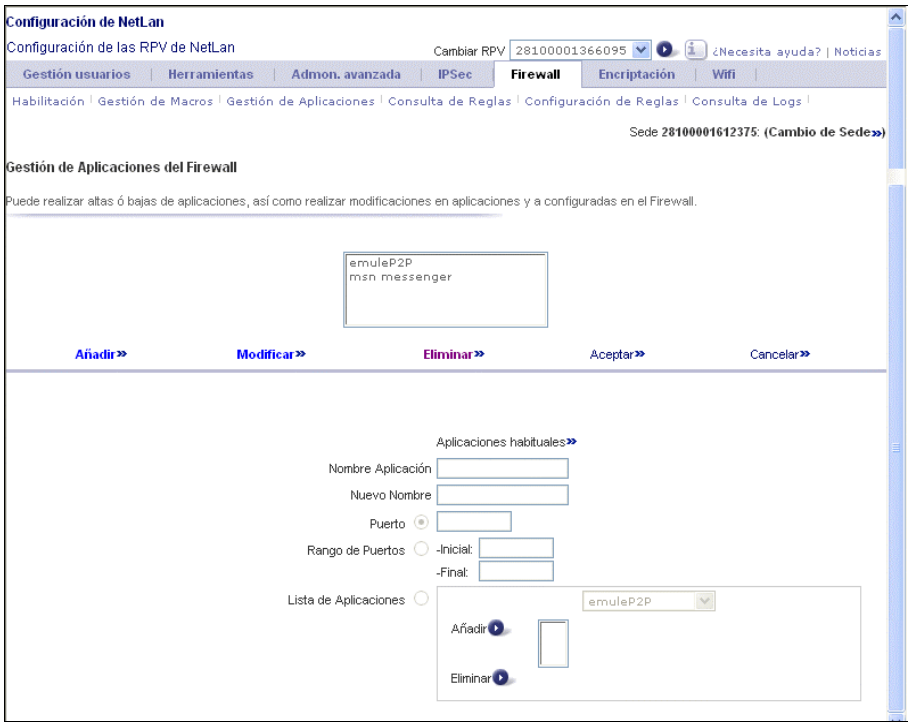
Si lo que se pretende es modificar, pulsando en Modificar se copiarán las características de la macro en los campos correspondientes, permitiéndose modificar el nombre así como sus parámetros.

Las dos acciones anteriores se completan con los links de Aceptar y Cancelar para la aceptación o cancelación de las acciones de alta y/o modificación.

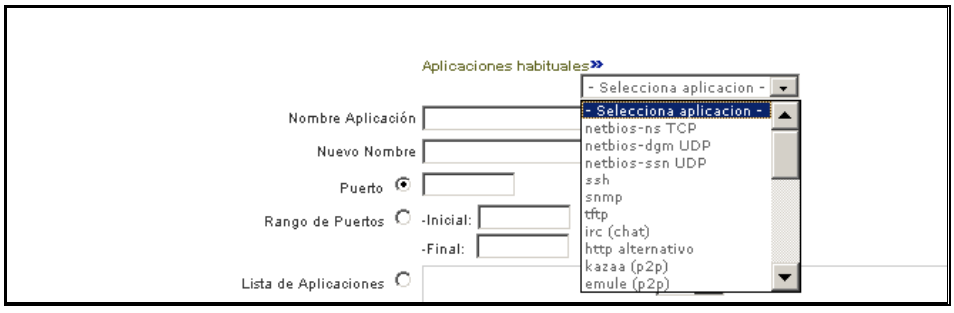
Seleccionando una macro y dando a Eliminar se solicitará la confirmación para ejecutar esta acción.

3.3 Gestión de Aplicaciones

En este apartado se permitirá una gestión completa de las Aplicaciones. En primer lugar se tendrá una lista de las aplicaciones existentes con las opciones de eliminación, modificación o de añadir nuevas aplicaciones. Cada una de estas acciones se completará al dar a Aceptar, o en el caso contrario, se cancelará pulsando en Cancelar.



Un link de Aplicaciones habituales mostrará una lista con todas las aplicaciones usuales que un cliente de Firewall suele utilizar:



En los anexos se adjunta una lista con los puertos por defecto que utilizan las aplicaciones de intercambio de ficheros P2P.

Si se desea añadir una nueva Aplicación, el usuario deberá pulsar en Añadir, se deshabilitará la lista y se mostrará activo el campo Nombre Aplicación, así como una de las posibles opciones de la que se compone una Macro:

- Puerto
- Rango de Puertos
- Lista de Aplicaciones: Ya que una aplicación puede constar de varias aplicaciones, por lo que aparecerá de nuevo la lista con la posibilidad de añadir las que desee.

Si lo que quiere es modificar, pulsando en Modificar se copiarán las características de la aplicación en los campos correspondientes, permitiendo modificar el nombre, así como sus parámetros.

Las dos acciones anteriores se completan con los enlaces de Aceptar y Cancelar para la aceptación o cancelación de las acciones de alta y/o modificación.

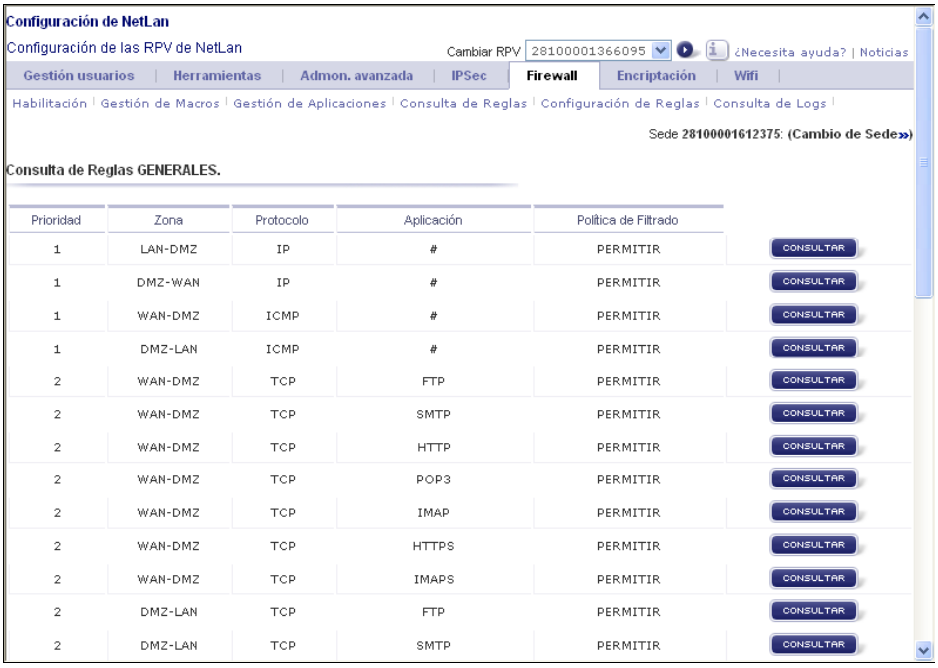
Seleccionando una aplicación y pulsando Eliminar se solicitará la confirmación para ejecutar esta acción.

3.4 Gestión de Reglas: Consulta

La consulta comienza desde el menú principal de FW, donde se podrá elegir el tipo de reglas a consultar:

- Generales
- Activas
- No Activas
- Prefijadas: en este caso aparecerá un nuevo combo con las opciones de nivel de las reglas: Alto, Medio, Bajo, Nulo.

Se mostrará entonces una lista de las reglas encontradas así como un enlace de detalle en cada una de ellas. Al pinchar en detalle accederemos a una pantalla donde se mostrarán todos los datos de la regla seleccionada y que por ser muchos no aparecen en la lista inicial.



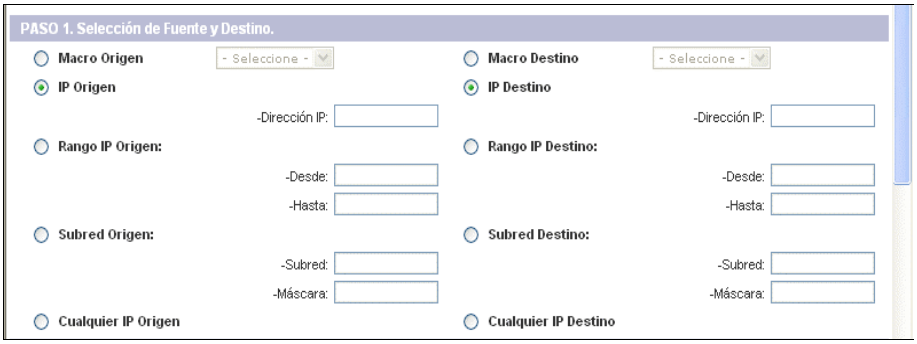
3.5 Gestión de Reglas: Configuración

Desde esta opción se podrá configurar las reglas existentes, dar prioridad a las activas, modificar de activas a no activas y viceversa, eliminar, etc. Todo ello se podrá hacer siguiendo una serie de pasos. Todos estos pasos se encontrarán situados en la misma página y le guiarán a gestionar de forma ordenada sus reglas.

3.5.1 PASO 1

En el primer paso tendrá que seleccionar la fuente y destino de la regla. Para ello podrá seleccionar entre las diferentes opciones expuestas. Permitirá una selección tanto en el origen como el destino:

- Macro: Con una lista de las Macros existentes.
- Dirección IP.
- Rango IP (IP inicio y fin).
- Subred más máscara.
- Opción de cualquier IP.



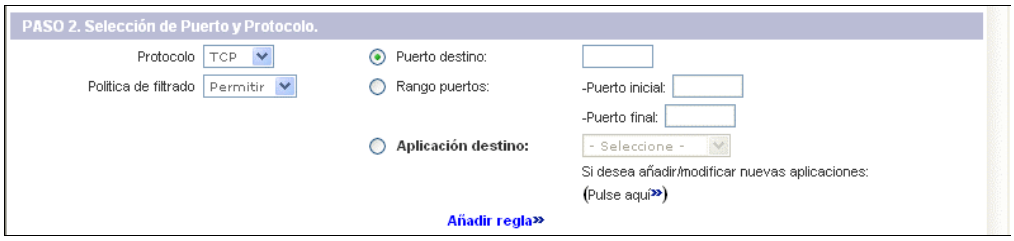
3.5.2 PASO 2

Permitirá la selección del tipo de puerto, tanto si es uno sólo, como un rango o una aplicación (donde se podrá seleccionar de una lista con las existentes). Solo se podrá seleccionar un tipo de puerto. También habrá que seleccionar el tipo de Protocolo:

- IP
- ICMP
- UDP
- TCP

La Política de filtrado tendrá dos opciones: Permitir y No Permitir.

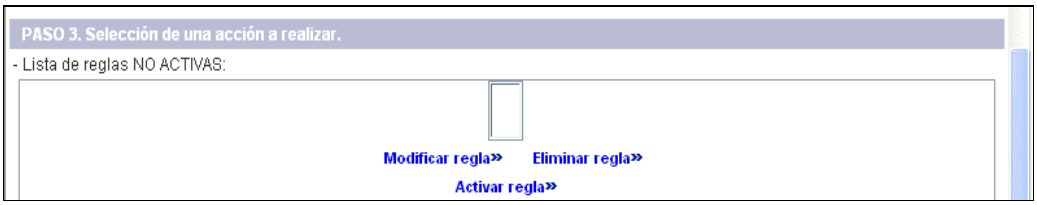
Este paso permitirá acceder directamente a las pantallas anteriormente escritas para añadir nuevas aplicaciones o modificar las que se presentan en la lista.



3.5.3 *PASO 3*

En este paso se podrá añadir la regla definida en los pasos anteriores o seleccionar de la lista una para modificarla. Además, se permite la opción de la eliminación de una regla, así como de la activación de reglas existentes en la caja de reglas *No Activas*.

Se mostrarán todas las reglas no activas que tenga.



3.5.4 *PASO 4*

En este paso se podrán establecer prioridades para las reglas activas así como desactivarlas y por tanto añadirlas a la lista anterior.

En este campo, se mostrarán todas las reglas activas que tenga.

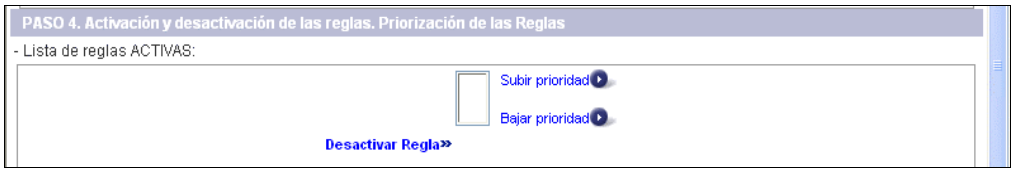


Fig. 4.12: Configuración de Reglas: Paso 4

3.5.5 *PASO 5*

Este último paso será el de confirmación de todas las acciones realizadas en los pasos anteriores, si no se salva la configuración las reglas se quedarán como al inicio.

3.6 Desconexión

Podrá cerrar la sesión en el Portal del Servicio pulsando el enlace de desconexión.

Si elige desconectar, se le redirigirá a la página de portada de Movistar.es

De esta manera se borran los datos de sesión del usuario Administrador y se cierran todas las conexiones establecidas con el servidor.

Así se mejora la seguridad del Portal de Clientes, evitando que personas no deseadas realicen accesos al portal utilizando una sesión que haya quedado abierta.

4. EJEMPLO DE CONFIGURACIÓN

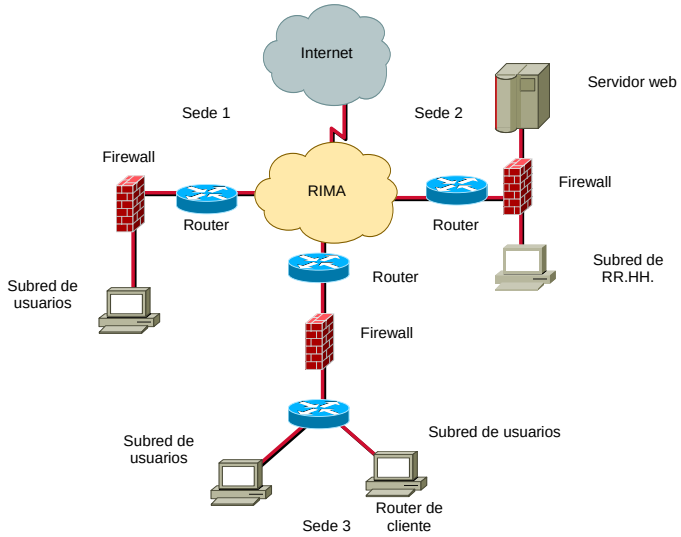
A continuación se muestran algunas configuraciones habituales como ejemplo. Para ello se utilizará una RPV-IP como escenario:

4.1 Escenario del ejemplo:

Se trata de una RPV-IP Net-LAN con las siguientes características:

- 3 sedes ADSL
  - sede 1: una única subred de usuarios
  - sede 2: dos subredes, una de LAN directamente conectada y otra de DMZ también directamente conectada, donde se hospedará un servidor con una aplicación web de la empresa. La primera subred descrita pertenece al departamento de contabilidad y RR.HH. de la empresa y contiene información más delicada y confidencial.
  - sede 3: tres subredes, una directamente conectada y dos no directamente conectadas utilizadas por usuarios normales de la empresa.
- Tiene contratado el servicio de Firewall en las tres sedes
- Topología mallada
- Salida a Internet

Así, el esquema de red sería el siguiente:



4.2 Filtrado del tráfico de una sede hacia una subred perteneciente a otra sede

Si por ejemplo la compañía no desea que desde otras sedes se acceda a la subred de RR.HH. de la sede 2, donde están conectados PCs con datos sensibles e importantes, deberá filtrar este tráfico. Lo podrá hacer en los Firewalls remotos o en el de la propia sede a proteger, siendo más lógico y cómodo este último caso. Además lo podrá hacer de diferentes maneras.

Una opción es dejar el nivel bajo que viene configurado por defecto y añadir una regla prohibiendo el tráfico de la WAN a la LAN.

Otra opción es configurar un nivel alto o medio en todas las zonas del Firewall de la sede a proteger. En ese caso deberá configurarse una regla que permita el paso del tráfico HTTP de la zona WAN a la DMZ para no cortar el tráfico del servidor web que hay en la DMZ. Esta es la recomendada por dar mayor seguridad a la sede.

Los pasos a seguir se describen en los apartados siguientes.

4.2.1 Cambio del nivel de seguridad a uno prefijado

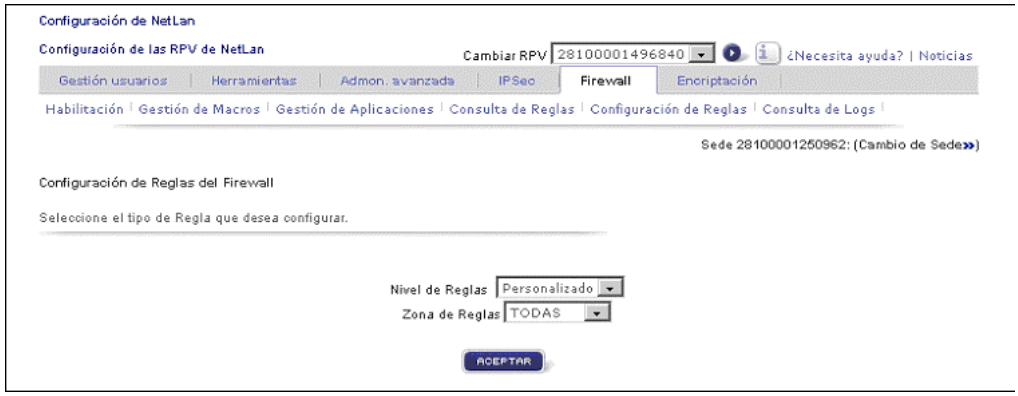
En este caso será un cambio a nivel medio o alto (según se desee).

Para ello deberá acceder al portal de gestión Net-LAN (www.movistar.es/negocios/netlan) y autentificarse con el usuario y password.

Una vez aquí seleccionaremos la pestaña de “Firewall” y posteriormente se accederá a la configuración del Firewall de la sede 2 en este caso, la cual se elegirá a través de su número de teléfono.

Tras seleccionar la sede, aparecerá una pantalla como la siguiente:

Para poner el Firewall en un nivel prefijado de seguridad se deberá seleccionar "Configuración de reglas". Después debe elegirse el nivel en el desplegable (en este caso Alto) y la pareja de zonas (TODAS, LAN-WAN, LAN-DMZ, etc.) a modificar y pulsar el botón "configurar". Cada configuración supone un acceso remoto al equipo Firewall, por lo que tiene una duración más larga de carga de lo que es habitual en la navegación por el portal.



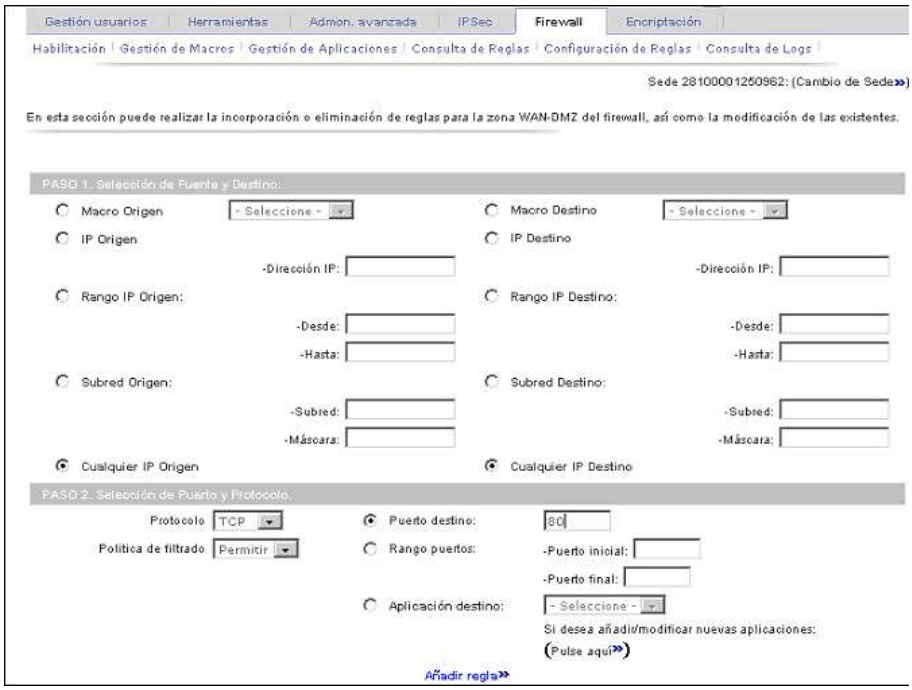
4.2.2 Configuración de una regla personalizada:

Después debe permitirse el paso de tráfico web desde la WAN a la DMZ. Para ello debe configurarse una regla personalizada en el portal.

Para ello seleccionar el nivel "Personalizado" y la zona "WAN-DMZ" y pulsar "configurar".

Posteriormente aparecerá el formulario de configuración de reglas, en el cual deberemos seleccionar:

- Origen: cualquier IP origen
- Destino: cualquier IP destino (aquí podría seleccionarse la IP del servidor, para restringir más el acceso)
- Protocolo: TCP
- Puerto destino: 80 (HTTP)
- Política de filtrado: permitir



Después seleccionar "Añadir" y después "Activar Regla", lo que provocará que la nueva regla aparezca en la lista de reglas activas, tal y como se muestra a continuación.

Por último se deberá pulsar "Enviar", momento en el que se configurará el Firewall y se activará la nueva configuración.

4.2.3 Filtrado del tráfico Internet de una sede:

En el caso de que el cliente desee que alguna de sus sedes no acceda a Internet (a ningún tipo de tráfico) se deberá prohibir el tráfico desde la LAN y la DMZ hacia la WAN hacia direcciones públicas. Para ello lo más sencillo es crear unas macros con las direcciones públicas y después un par de reglas de filtrado personalizadas.

4.2.4 Creación de Macros

Las macros son una herramienta para facilitar la configuración de reglas personalizadas.

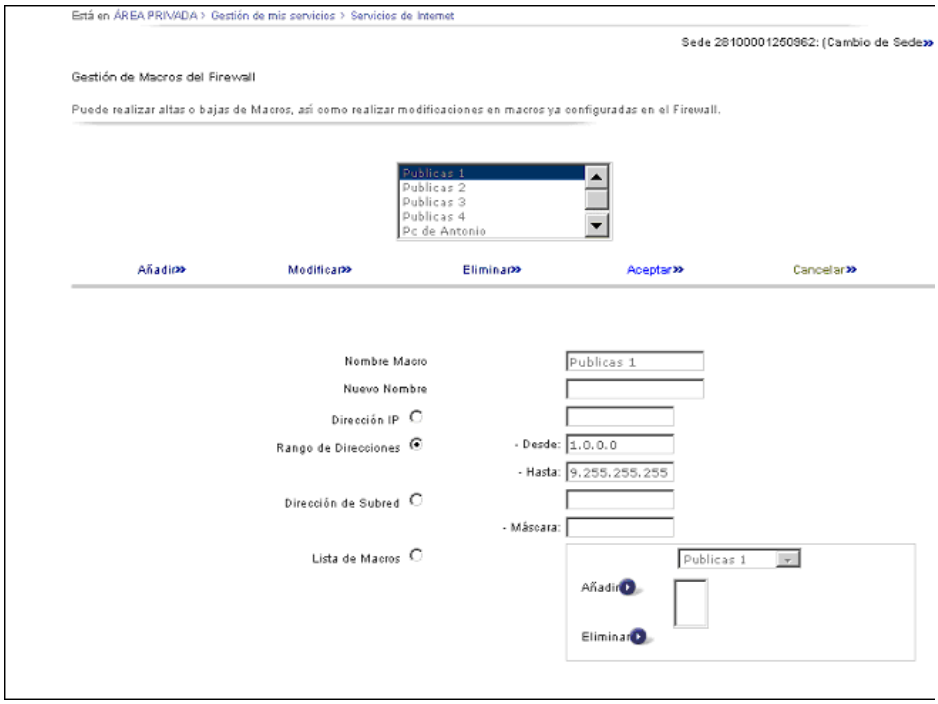
Para acceder a la gestión deberá accederse a la gestión del Firewall y después en el apartado de gestión de macros.

Una vez allí se deberán crear 5 macros, cuatro de ellas incluirán las direcciones públicas de Internet y la quinta será una agrupación de las cuatro anteriores. De esta manera tendremos todas las direcciones IP públicas definidas en una macro.

Para ello se deberá pulsar "Añadir", rellenar el campo de el nombre, seleccionar "Rango de direcciones", colocar como inicio y final del rango las parejas de la lista siguiente y pulsar "Aceptar". Este paso debe repetirse para cada pareja de direcciones:

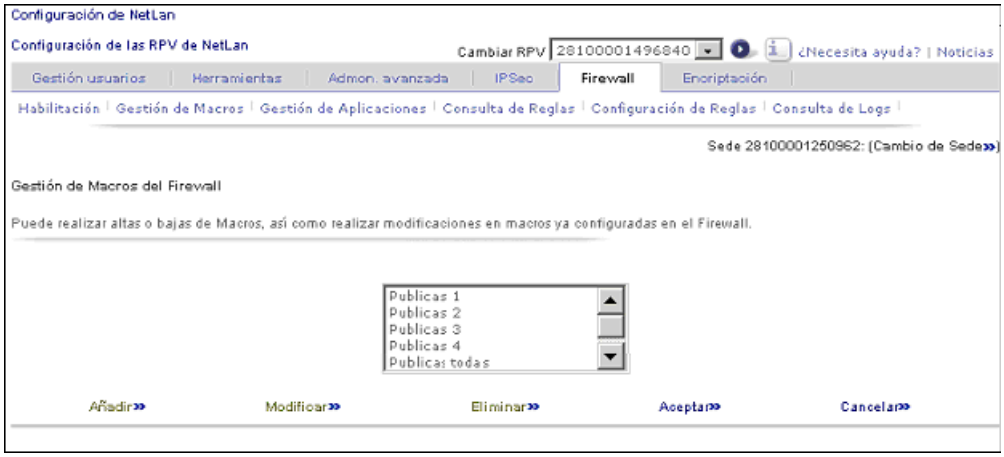
- Nombre: Públicas 1.
  Dirección origen: 1.0.0.0 Dirección final: 9.255.255.255
- Nombre: Públicas 2.
  Dirección origen: 11.0.0.0 Dirección final: 172.15.255.255
- Nombre: Públicas 3.
  Dirección origen: 172.32.0.0 Dirección final: 192.167.255.255
- Nombre: Públicas 4.
  Dirección origen: 192.170.0.0 Dirección final: 223.255.255.255

Estas direcciones en realidad son todas menos las privadas.



Después deberá crearse la macro que sea la unión de las cuatro anteriores, y deberá pulsarse "Añadir", pulsar "lista de macros", añadir las macros anteriores y pulsar aceptar.

El resultado será como sigue:



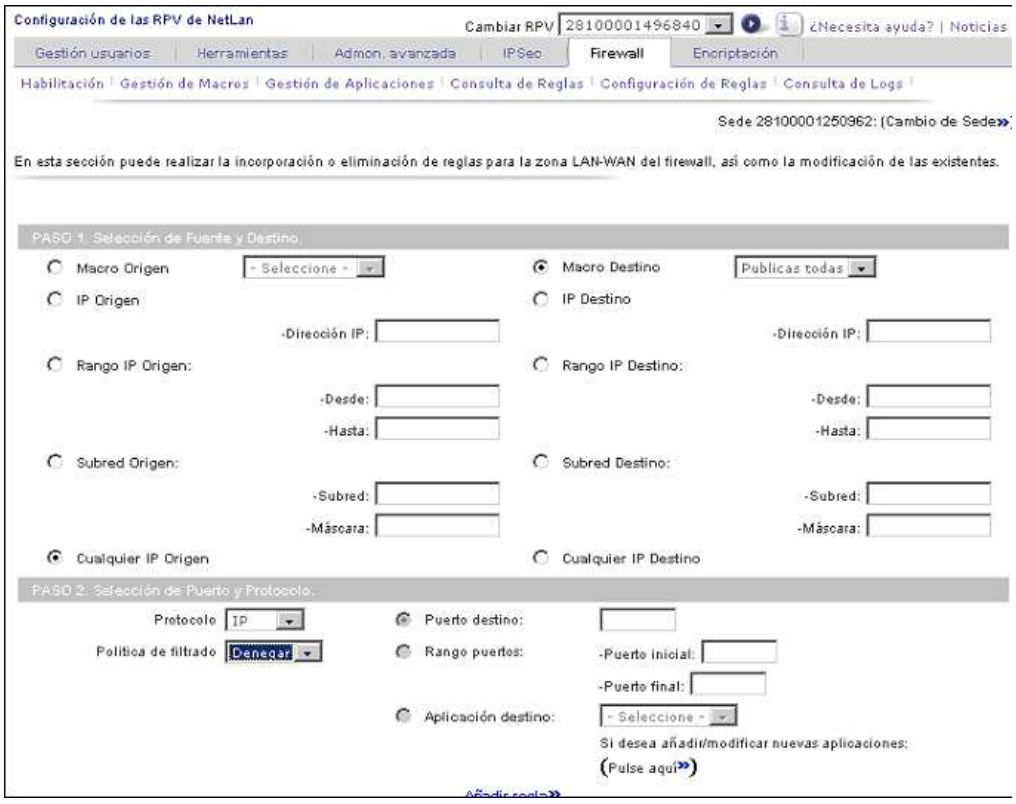
4.2.5 Configuración de reglas personalizadas:

Posteriormente deben crearse las reglas de filtrado para evitar que desde la LAN ni la DMZ se mande tráfico hacia direcciones públicas, hacia Internet.

Para ello seleccionar el nivel "Personalizado" y la zona "LAN-WAN" y pulsar "Aceptar".

Posteriormente aparecerá el formulario de configuración de reglas, en el cual deberemos seleccionar:

- Origen: cualquier IP origen
- Destino: macro destino "Publicas todas"
- Protocolo: IP (todo el tráfico)
- Política de filtrado: denegar



Después seleccionar "Añadir" y después "Activar Regla", lo que provocará que la nueva regla aparezca en la lista de reglas activas, tal y como se muestra a continuación.

En caso de que haya más de una regla activa, deberá subirse la prioridad hasta que esté la primera de la lista, puesto que se trata de una regla de denegación y debe ir antes de las que permitan el tráfico. Después pulsar "Enviar"

Deben repetirse estos pasos para las zonas DMZ-LAN si se desea que tampoco la DMZ tenga acceso a Internet.

5. ANEXOS

5.1 Anexo 1: puertos por defecto de aplicaciones P2P

Se adjunta una tabla con los puertos utilizados por defecto en las aplicaciones P2P más habituales.

Servicio P2P	Puertos TCP por defecto	Puertos UDP por defecto
BearShare	6346	
Bittorrent	2181, 6881-6999	
Blubster		41170-41350
eDonkey	4661-4662	5737
eDonkey2000	4661-4662	4665
eMule	4661-4662, 4711	4665, 4672
Gnutella	6346/6347	6346/6347
Grouper	8038	8038
Kazaa	1214	1214
Limewire	6346/6347	6346/6347
Morpheus	6346/6347	6346/6347
Shareaza	6346	6346
WinMx	6699	6257