Configuración del puerto de la zona desmilitarizada con la máscara de subred en el Routers RV016, RV042, RV042G y RV082 VPN

Objetivo

Un De-Militarized Zone (DMZ) es una porción de una red interna de una organización que se ponga a disposición una red no confiable tal como el Internet. Un DMZ ayuda a mejorar la Seguridad en la red interna de una organización. En vez de todos los recursos internos que son disponible desde Internet, solamente ciertos host tales como servidores Web están disponibles.

Cuando una lista de control de acceso (ACL) está limitada a una interfaz, las reglas del elemento del control de acceso (ACE) se aplican a los paquetes que llegan esa interfaz. Los paquetes que no hacen juego a los aces uces de los en el ACL se corresponden con a una regla predeterminada cuya acción sea caer los paquetes incomparables. Este artículo muestra cómo configurar el puerto DMZ y y permitir el tráfico del DMZ a los IP Address de destino específicos.

Dispositivos aplicables

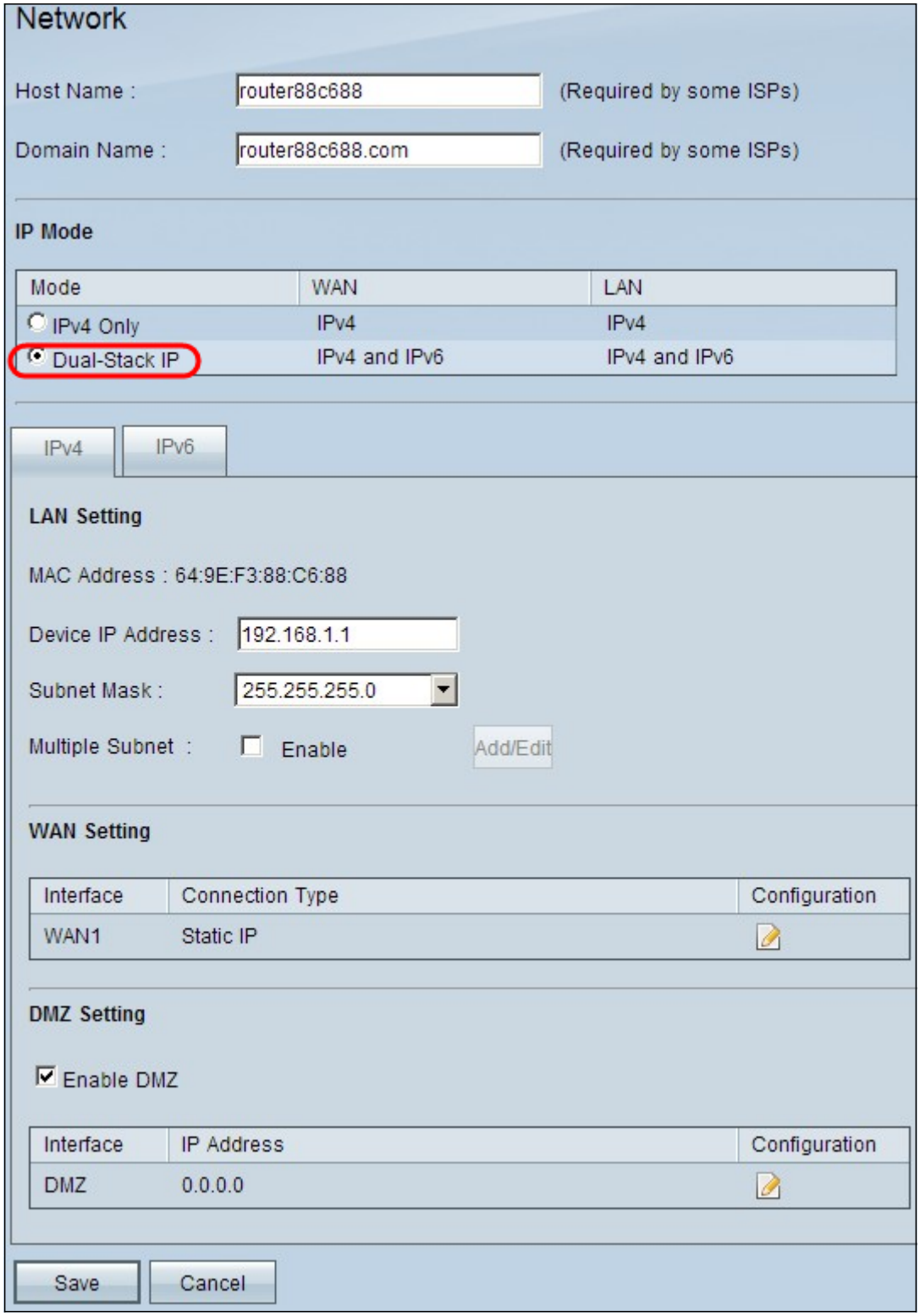
- RV016
- RV042
- RV042G
- RV082

Versión del software

- v4.2.2.08

Configuración de DMZ con la subred

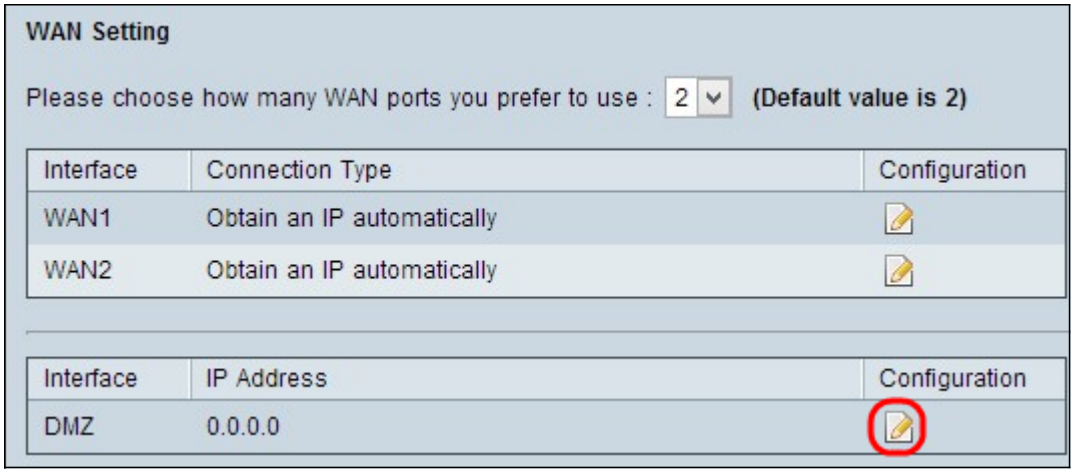
Paso 1. El registro en la página de utilidad de la configuración del router y elige la **configuración > la red**. La página de la *red* se abre:



Paso 2. Para configurar el DMZ en tecleo del direccionamiento del IPv4 o del IPv6 la lengueta correspondiente situada en el campo de la configuración LAN.

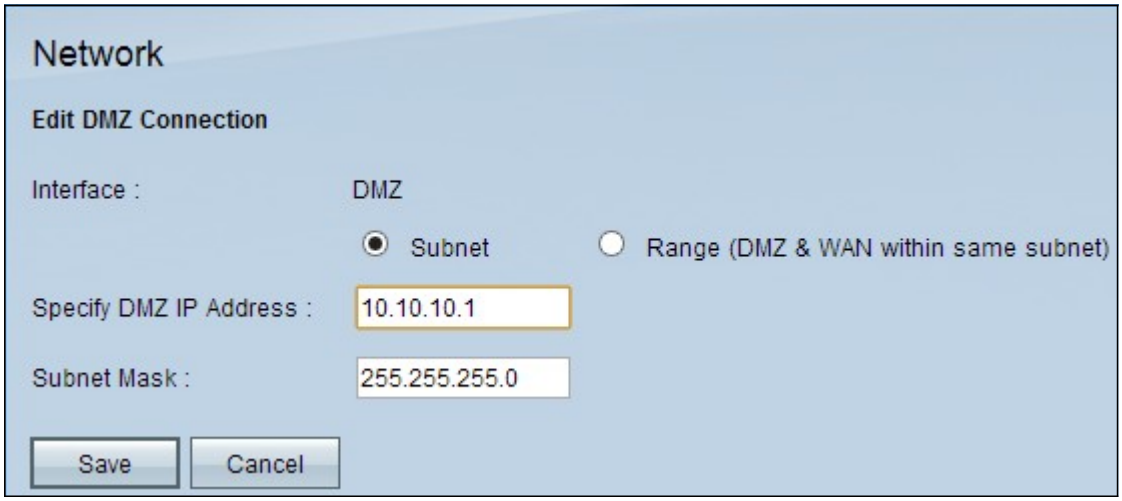
Nota: El IP del doble pila en el área del *modo IP* debe ser habilitado si usted quiere configurar el IPv6.

Paso 3. Navegue hacia abajo al campo de la configuración DMZ y haga clic el botón de radio del **habilitar DMZ** para habilitar el DMZ.



Paso 4. Haga clic en el icono de la **configuración de DMZ** para configurar la subred. La configuración se puede hacer para el IPv4 y el IPv6 así:

Configuración del IPv4



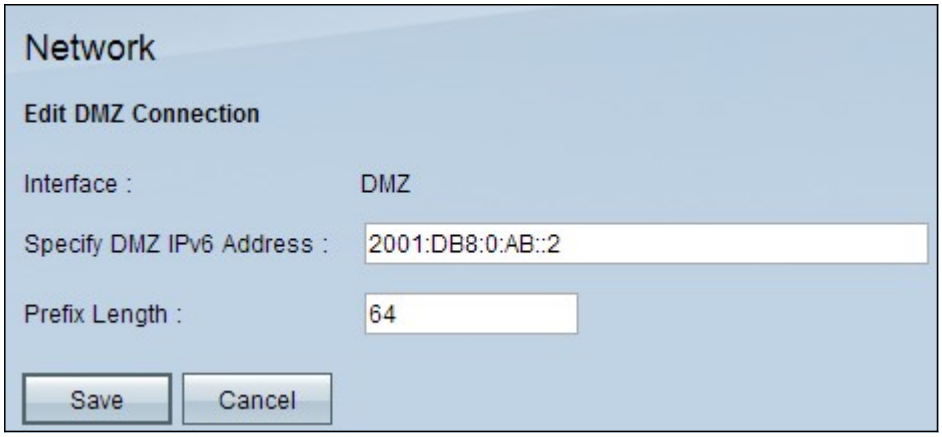
Paso 5. Haga clic el botón de radio de la **subred** para configurar el DMZ a otra subred que el de WAN. Para el IP de la subred lo que sigue debe ser configurado

- Especifique el IP Address DMZ — Ingrese el IP Address DMZ en el campo del **IP Address del especificar DMZ**.
- Máscara de subred — Ingrese a la máscara de subred en el campo de la **máscara de subred.**

Advertencia: Los host con una dirección IP en el DMZ no son tan seguros como los host dentro de su LAN interno.

Paso 6. Haga clic el **rango** para configurar el DMZ para estar en la misma subred como WAN. El rango de los IP Addresses debe ser ingresado en el **rango IP para el** campo de **puerto DMZ**.

Configuración del IPv6



Nota: Para la configuración del IPv6 las opciones siguientes están disponibles:

Paso 7. Especifique el direccionamiento del IPv6 DMZ — Ingrese el direccionamiento del IPv6.

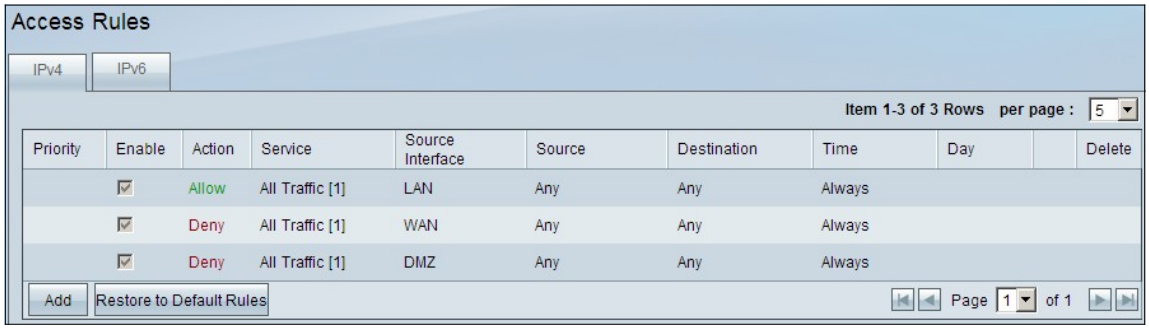
Paso 8. Longitud del prefijo — La longitud del prefijo del dominio del IP Address DMZ mencionado anteriormente debe ser ingresada.

Paso 9. **Salvaguardia del** tecleo para salvar la configuración.

Configuración de las reglas de acceso

Esta configuración se hace para definir las Listas de acceso para los IP configurados en las máscaras de la subred múltiple.

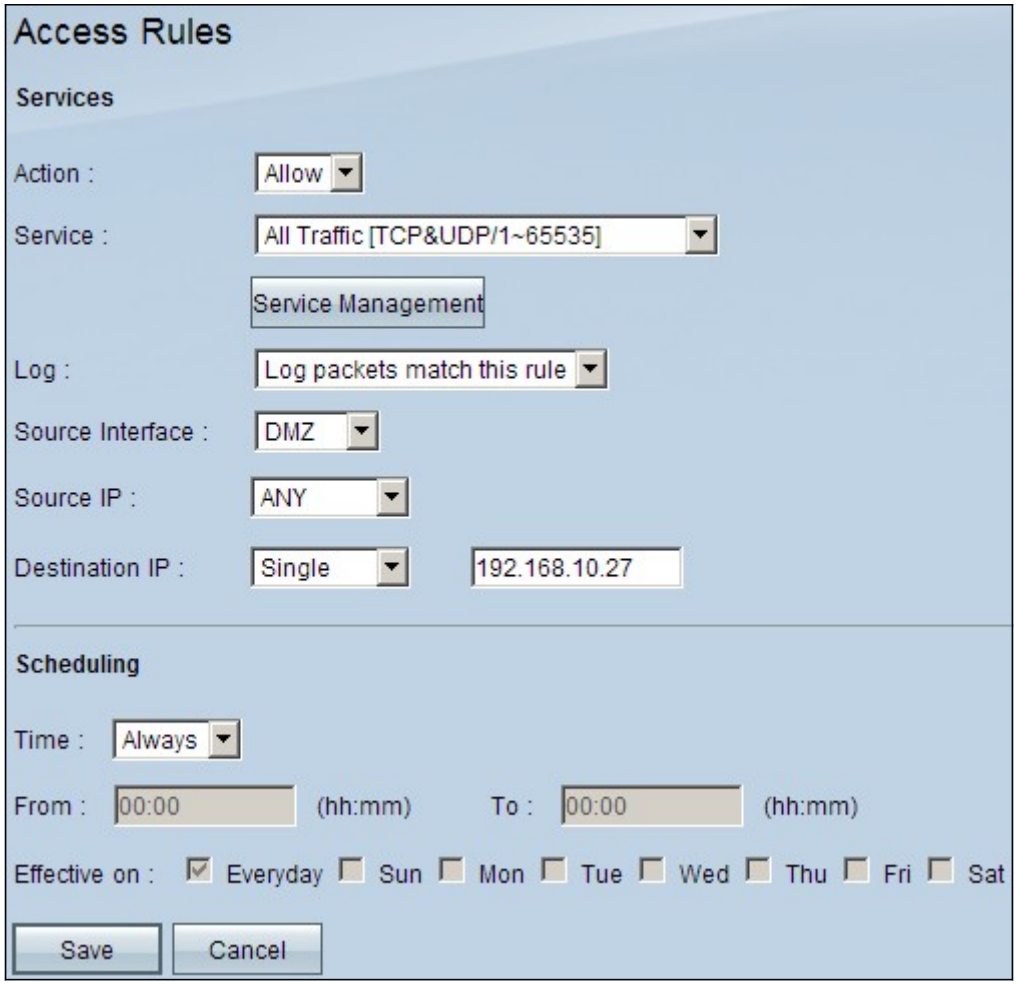
Paso 1. El registro en la página de utilidad de la configuración del router y elige el **Firewall > las reglas de acceso**. La página de las *reglas de acceso* se abre:



Nota: Las reglas de acceso predeterminadas no pueden ser editadas.

Paso 2. Haga clic el **botón Add** para agregar una nueva regla de acceso. La página de las *reglas de acceso* cambia para mostrar los servicios y las áreas del Scheduling.

Nota: Esta configuración se puede hacer para el IPv4 y el IPv6 seleccionando esas lenguetas respectivas en la página de las *reglas de acceso*. Los pasos para la configuración específicos al IPv4 y al IPv6 se mencionan en los pasos siguientes.



Paso 3. Elija **permiten de la** lista desplegable de la acción permitir el servicio.

Paso 4. Elija **todo el tráfico [TCP&UDP/1~65535] de la** lista desplegable del servicio para habilitar todos los servicios para el DMZ.

Paso 5. Elija los **paquetes del registro que hacen juego esta regla de la** lista desplegable del registro para elegir solamente los registros que hacen juego la regla de acceso.

Paso 6. Elija el **DMZ de la** lista desplegable de la interfaz de origen que es la fuente para las reglas de acceso.

Paso 7. Elija **ningunos de la** lista desplegable IP de la fuente.

Paso 8. Elija las opciones disponibles de siguiente unas de los de la lista desplegable del IP de destino.

- Escoja — Elija solo aplicar esta regla a una sola dirección IP.
- Rango — Elija el rango para aplicar esta regla a un rango de los IP Addresses. Ingrese el primer y dure el IP Address del rango. Esta opción está disponible solamente en el IPv4.
- Subred — Elija la subred para aplicar esto gobierna a un red secundario. Ingrese el número del IP Address y de la notación de CIDR que se utiliza para afectar un aparato los IP Addresses y los paquetes del protocolo de Internet de encaminamiento para la subred. Esta opción está disponible solamente en el IPv6.
- Ningunos — Elija ningunos para aplicar la regla a la dirección IP ua de los.

Timesaver: Salte al paso 10 si usted está configurando las reglas de acceso del IPv6.

Paso 9. Elija un método para definir cuando las reglas son activas de la lista desplegable del tiempo. Las fallas son las siguientes:

- Siempre — Si usted elige siempre del menú desplegable del tiempo, las reglas de acceso serán aplicadas siempre para traficar.

- Intervalo — Usted puede elegir un intervalo de tiempo específico en el cual las reglas de acceso sean activas si usted selecciona el intervalo del menú desplegable del tiempo. Después de que usted especifique el intervalo de tiempo, elija los días en que usted quiere las reglas de acceso para ser activo del eficaz en las casillas de verificación.

Paso 10. **Salvaguardia del** tecleo para salvar sus configuraciones.

Paso 11 Haga clic el icono del **editar** para editar la regla de acceso creada.

Paso 12. Haga clic el icono de la **cancelación** para borrar la regla de acceso creada.