

Configuración de varias IP públicas en la zona desmilitarizada (DMZ) en los routers VPN RV042, RV042G y RV082

Objetivo

La zona desmilitarizada (DMZ) es una red interna de una organización que está disponible para una red no fiable. En cuanto a la seguridad, la DMZ se encuentra entre redes de confianza y no fiables. El mantenimiento de la DMZ ayuda a mejorar la seguridad de la red interna de una organización. Cuando una lista de control de acceso (ACL) se enlaza a una interfaz, sus reglas de Elemento de control de acceso (ACE) se aplican a los paquetes que llegan a esa interfaz. Los paquetes que no coinciden con ninguna de las ACE de la Lista de control de acceso coinciden con una regla predeterminada cuya acción es descartar paquetes no coincidentes.

El objetivo de este documento es mostrarle cómo configurar el puerto DMZ para permitir varias direcciones IP públicas y definir la lista de control de acceso (ACL) para las IP en el dispositivo del router.

Dispositivos aplicables

- RV042
- RV042G
- RV082

Versión del software

- v4.2.2.08

Configuración DMZ

Paso 1. Inicie sesión en la página Web Configuration Utility (Utilidad de configuración web) y seleccione Setup > Network. Se abre la página Red:

Network

Host Name : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

LAN Setting

MAC Address : 50:57:A8:79:F3:7A

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable Add/Edit

WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

DMZ Setting

Enable DMZ

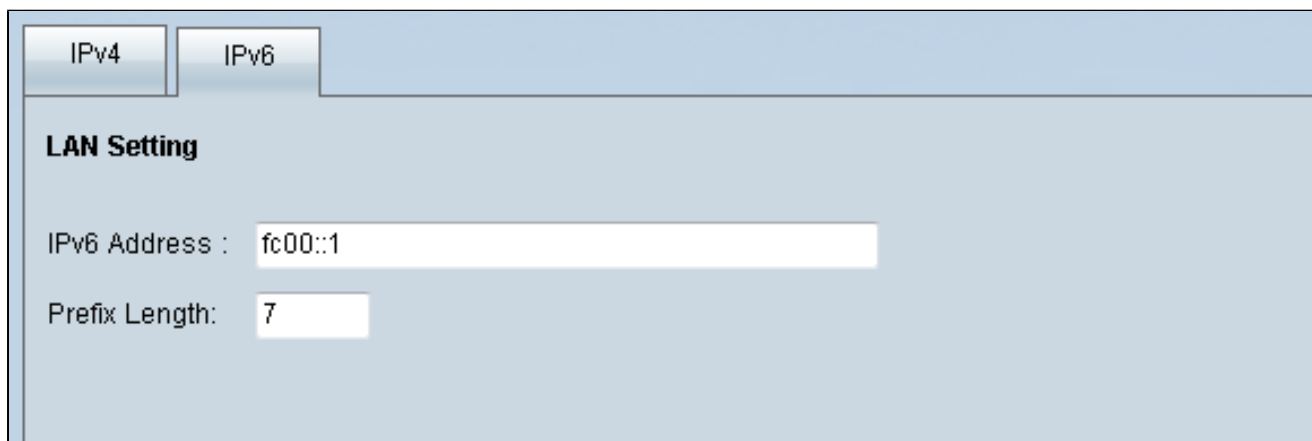
Interface	IP Address	Configuration
DMZ	0.0.0.0	

Paso 2. En el Campo IP Mode, haga clic en el botón de opción Dual-Stack IP para habilitar la configuración de direcciones IPv6.

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

Paso 3. Haga clic en la ficha IPv6 situada en el campo Configuración de LAN para poder configurar DMZ en la dirección IPv6.



The screenshot shows the 'LAN Setting' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6', with 'IPv6' being the active tab. Below the tabs, the 'LAN Setting' section is visible. It contains two input fields: 'IPv6 Address' with the value 'fc00::1' and 'Prefix Length' with the value '7'.

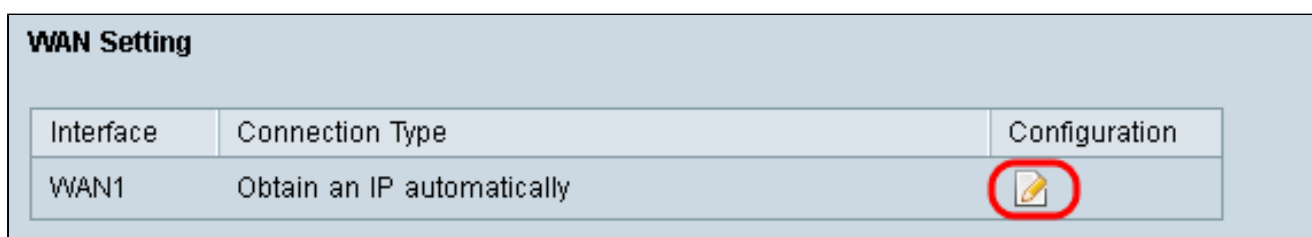
Paso 4. Desplácese hacia abajo hasta el área Configuración DMZ y haga clic en la casilla de verificación DMZ para activar DMZ




The screenshot shows the 'DMZ Setting' configuration page. At the top, the 'DMZ Setting' section is visible. It contains a checkbox labeled 'Enable DMZ' which is checked and circled in red. Below this, there is a table with three columns: 'Interface', 'IP Address', and 'Configuration'.

Interface	IP Address	Configuration
DMZ	::/64	

Paso 5. En el campo WAN Setting, haga clic en el botón Edit para editar el IP Static de los parámetros de WAN1.



The screenshot shows the 'WAN Setting' configuration page. It contains a table with three columns: 'Interface', 'Connection Type', and 'Configuration'.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

Se abre la página Red:

Network

Edit WAN Connection

Interface : WAN1

WAN Connection Type : Static IP

Specify WAN IP Address : 192.168.3.1

Subnet Mask : 255.255.255.0

Default Gateway Address : 192.168.3.2

DNS Server (Required) 1 : 0.0.0.0

2 : 0.0.0.0

MTU : Auto Manual 1500 bytes

Save Cancel

Paso 6. Elija Static IP en la lista desplegable WAN Connection Type.

Paso 7. Introduzca la dirección IP de WAN que se muestra en la página Resumen del sistema en el campo Especificar dirección IP de WAN.

Paso 8. Introduzca la dirección de máscara de subred en el campo Subnet Mask.

Paso 9. Introduzca la dirección de gateway predeterminada en el campo Default Gateway Address.

Paso 10. Introduzca la dirección del servidor DNS que se muestra en la página Resumen del sistema en el campo Servidor DNS (obligatorio) 1.

Nota: La dirección 2 del servidor DNS es opcional.


Paso 11. Elija la unidad de transmisión máxima (MTU) para que sea Automática o Manual.

Si elige manual, introduzca los bytes para la MTU manual.

Paso 12. Haga clic en la pestaña Save para guardar la configuración.

Definición de ACL

Paso 1. Inicie sesión en la página Web Configuration Utility y elija Firewall > Access Rules. Se abre la página Access Rules:



The screenshot shows the 'Access Rules' configuration page. At the top, there are tabs for 'IPv4' and 'IPv6'. Below the tabs, it indicates 'Item 1-3 of 3 Rows' and 'per page : 5'. The main content is a table with the following columns: Priority, Enable, Action, Service, Source Interface, Source, Destination, Time, Day, and Delete. There are three rows of rules, each with a checked 'Enable' box. The first row is 'Allow' for 'All Traffic [1]' on the 'LAN' interface. The second and third rows are 'Deny' for 'All Traffic [1]' on the 'WAN' and 'DMZ' interfaces, respectively. At the bottom left, there is an 'Add' button and a 'Restore to Default Rules' button. At the bottom right, there are navigation arrows and a page indicator 'Page 1 of 1'.

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

Nota: Al acceder a la página Reglas de acceso, no se pueden editar las reglas de acceso por defecto.

Paso 2. Haga clic en el botón Agregar para agregar una nueva regla de acceso.



This screenshot is identical to the previous one, but the 'Add' button at the bottom left is highlighted with a red circle, indicating the next step in the process.

La página Access Rules (Reglas de acceso) ahora mostrará las opciones para las áreas Service y Scheduling.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 3. Elija Allow en la lista desplegable Action para permitir el servicio.

Paso 4. Elija All Traffic [TCP&UDP/1~65535] de la lista desplegable Service para habilitar todos los servicios para DMZ.

Paso 5. Elija Log packets match this rule de la lista desplegable Log para elegir solamente los logs que coincidan con la regla de acceso.

Paso 6. Elija DMZ en la lista desplegable Source Interface. Este es el origen de las reglas de acceso.

Paso 7. Elija Any en la lista desplegable Source IP.

Paso 8. Elija Single en la lista desplegable Destination IP.

Paso 9. Introduzca las direcciones IP del destino al que se permitirán las reglas de acceso en el campo Destination IP.

Paso 10. En el área Programación, seleccione Siempre en la lista desplegable Hora para que la regla de acceso esté activa todo el tiempo.

Nota: Si selecciona Siempre en la lista desplegable Hora, la regla de acceso se establecerá de forma predeterminada en Todos los días en el campo Vigente el.

Nota: Puede seleccionar un intervalo de tiempo específico (para el que están activas las reglas de acceso) seleccionando Intervalo en la lista desplegable Hora. A continuación, puede elegir los días en los que desea que las reglas de acceso estén activas desde las casillas de verificación Vigente el.

Paso 11. Haga clic en Save para guardar la configuración.

Nota: Si aparece una ventana emergente, pulse 'Aceptar' para agregar otra regla de acceso, o pulse 'Cancelar' para volver a la página de Reglas de acceso.

Ahora se muestra la regla de acceso que ha creado en el paso anterior

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	DMZ	Any	192.168.10.27 ~ 192.168.10.27	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

Item 1-4 of 4 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

Paso 12. Haga clic en el icono Edit para editar la regla de acceso creada.

Paso 13. Haga clic en el icono Eliminar para eliminar la regla de acceso creada.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).