

Configuración del puerto de zona desmilitarizada con máscara de subred en los routers VPN RV016, RV042, RV042G y RV082

Objetivo

Una zona desmilitarizada (DMZ) es una parte de una red interna de una organización que está disponible para una red no fiable como Internet. Una DMZ ayuda a mejorar la seguridad en la red interna de una organización. En lugar de que todos los recursos internos estén disponibles en Internet, sólo están disponibles determinados hosts, como los servidores Web.

Cuando una lista de control de acceso (ACL) se enlaza a una interfaz, las reglas del 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 en la ACL se hacen coincidir con una regla predeterminada cuya acción es descartar paquetes no coincidentes. En este artículo se muestra cómo configurar el puerto DMZ y permitir el tráfico desde la DMZ a direcciones IP de destino específicas.

Dispositivos aplicables

• RV016

• RV042

• RV042G

• RV082

Versión del software

• v4.2.2.08

Configuración de DMZ con subred

Paso 1. Inicie sesión en la página Router Configuration Utility (Utilidad de configuración del router) y seleccione **Setup > Network (Configuración > Red)**. 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 : 64:9E:F3:88:C6:88

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable

WAN Setting

Interface	Connection Type	Configuration
WAN1	Static IP	

DMZ Setting

Enable DMZ

Interface	IP Address	Configuration
DMZ	0.0.0.0	

Paso 2. Para configurar DMZ en direcciones IPv4 o IPv6, haga clic en la ficha correspondiente situada en el campo Configuración de LAN.

Nota: Si desea configurar IPv6, debe habilitar Dual-Stack IP en el área *IP Mode*.

Paso 3. Desplácese hacia abajo hasta el campo DMZ Setting (Parámetros de DMZ) y haga clic en el botón de radio **Enable DMZ** (Activar DMZ) para activar DMZ.

WAN Setting

Please choose how many WAN ports you prefer to use : (Default value is 2)

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

Interface	IP Address	Configuration
DMZ	0.0.0.0	

Paso 4. Haga clic en el icono de **configuración DMZ** para configurar la subred. La configuración se puede realizar para [IPv4](#) e [IPv6](#) de la siguiente manera:

Configuración de IPv4

Network

Edit DMZ Connection

Interface : DMZ

Subnet Range (DMZ & WAN within same subnet)

Specify DMZ IP Address :

Subnet Mask :

Paso 5. Haga clic en el botón de radio **Subnet** para configurar DMZ en una subred distinta de la WAN. Para la IP de subred, se debe configurar lo siguiente

- Especificar dirección IP de DMZ: introduzca la dirección IP de DMZ en el campo **Especificar dirección IP de DMZ**.
- Máscara de subred: introduzca la máscara de subred en el campo **Máscara de subred**.

Advertencia: Los hosts con una dirección IP en la DMZ no son tan seguros como los hosts dentro de su LAN interna.

Paso 6. Haga clic en **Range** para configurar la DMZ para que esté en la misma subred que la WAN. El intervalo de direcciones IP se debe introducir en el campo **Intervalo IP para puerto DMZ**.

Configuración de IPv6

Network

Edit DMZ Connection

Interface : DMZ

Specify DMZ IPv6 Address : 2001:DB8:0:AB::2

Prefix Length : 64

Save Cancel

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

Paso 7. Especificar dirección IPv6 de DMZ: introduzca la dirección IPv6.

Paso 8. Longitud del prefijo: se debe introducir la longitud del prefijo del dominio de dirección IP de DMZ mencionado anteriormente.

Paso 9. Haga clic en **Save** para guardar la configuración.

Configuración de reglas de acceso

Esta configuración se realiza para definir las listas de acceso para las IP configuradas en las múltiples máscaras de subred.

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

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

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		

Add Restore to Default Rules Page 1 of 1

Nota: Las reglas de acceso predeterminadas no se pueden editar.

Paso 2. Haga clic en el botón **Agregar** para agregar una nueva regla de acceso. La página *Access Rules* cambia para mostrar las áreas *Services* y *Scheduling*.

Nota: Esta configuración se puede realizar para IPv4 e IPv6 seleccionando las fichas correspondientes en la página *Access Rules (Reglas de acceso)*. Los pasos de configuración específicos de IPv4 e IPv6 se mencionan en los siguientes pasos.

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 acceso al 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 **Registrar paquetes que coincidan con esta regla** en la lista desplegable Registro para elegir sólo los registros que coincidan con la regla de acceso.

Paso 6. Elija **DMZ** en la lista desplegable Source Interface (Interfaz de origen), que es el origen de las reglas de acceso.

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

Paso 8. Seleccione cualquiera de las siguientes opciones disponibles de la lista desplegable IP de destino.

- Único: elija único para aplicar esta regla a una única dirección IP.
- Rango: elija el rango para aplicar esta regla a un rango de direcciones IP. Introduzca la primera y la última dirección IP del intervalo. Esta opción sólo está disponible en IPv4.
- Subred: Seleccione Subred para aplicar estas reglas a una subred. Introduzca la dirección IP y el número de notación CIDR que se utiliza para asignar direcciones IP y enrutar paquetes de protocolo de Internet para la subred. Esta opción sólo está disponible en IPv6.
- Cualquiera: seleccione Cualquiera para aplicar la regla a cualquiera de las direcciones IP.

Ahorro de tiempo: vaya al paso 10 si está configurando reglas de acceso a IPv6.

Paso 9. Elija un método para definir cuándo están activas las reglas en la lista desplegable Hora. Las fallas son las siguientes:

- Siempre: si selecciona Siempre en la lista desplegable Hora, las reglas de acceso se aplicarán siempre al tráfico.
- Intervalo: puede elegir un intervalo de tiempo específico en el que las reglas de acceso están activas si selecciona Intervalo en la lista desplegable Tiempo. Después de especificar el intervalo de tiempo, seleccione los días en los que desea que las reglas de acceso estén activas en las casillas de verificación Vigente el.

Paso 10. Haga clic en **Save** para guardar la configuración.

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		

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

Paso 12. 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).