

# Configurazione della porta della zona demilitarizzata con subnet mask sui router VPN RV016, RV042, RV042G e RV082

## Obiettivo

Una zona demilitarizzata (DMZ) è una parte di una rete interna di un'organizzazione che viene resa disponibile a una rete non attendibile come Internet. Una DMZ consente di migliorare la sicurezza della rete interna di un'organizzazione. Anziché rendere disponibili tutte le risorse interne da Internet, sono disponibili solo alcuni host, ad esempio i server Web.

Quando un elenco di controllo di accesso (ACL, Access Control List) è associato a un'interfaccia, le regole ACE (Access Control Element) vengono applicate ai pacchetti che arrivano a quell'interfaccia. I pacchetti che non corrispondono a nessuna delle voci ACE nell'ACL vengono associati a una regola predefinita che prevede l'eliminazione dei pacchetti non corrispondenti. In questo articolo viene mostrato come configurare la porta DMZ e consentire il traffico dalla DMZ a indirizzi IP di destinazione specifici.

## Dispositivi interessati

- RV016
- RV042
- RV042G
- RV082

## Versione del software

- v4.2.2.08

## Configurazione DMZ con subnet

Passaggio 1. Accedere alla pagina Router Configuration Utility (Utilità di configurazione router) e scegliere **Setup > Network (Impostazione > Rete)**. Viene visualizzata la pagina *Rete*:

## 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

### 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	



Passaggio 2. Per configurare DMZ su indirizzo IPv4 o IPv6, fare clic sulla scheda corrispondente nel campo Impostazioni LAN.

**Nota:** se si desidera configurare IPv6, è necessario abilitare l'indirizzo IP a doppio stack nell'area della modalità IP.


Passaggio 3. Scorrere verso il basso fino al campo Impostazione DMZ e fare clic sul pulsante di opzione **Abilita DMZ** per abilitare 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	

Passaggio 4. Fare clic sull'icona di **configurazione DMZ** per configurare la subnet. La configurazione può essere eseguita sia per [IPv4](#) che per [IPv6](#) nel modo seguente:

### Configurazione IPv4

**Network**

Edit DMZ Connection

Interface : DMZ

Subnet       Range (DMZ & WAN within same subnet)

Specify DMZ IP Address :

Subnet Mask :

Passaggio 5. Fare clic sul pulsante di opzione **Subnet** per configurare DMZ su una subnet diversa da quella della WAN. Per l'indirizzo IP della subnet è necessario configurare quanto segue

- Specifica indirizzo IP DMZ - Immettere l'indirizzo IP DMZ nel campo **Specifica indirizzo IP DMZ**.
- Subnet mask: immettere la subnet mask nel campo **Subnet mask**.

**Avviso:** gli host con un indirizzo IP nella DMZ non sono sicuri come gli host nella LAN interna.

Passaggio 6. Fare clic su **Range** (Intervallo) per configurare la DMZ in modo che si trovi sulla stessa subnet della WAN. L'intervallo degli indirizzi IP deve essere immesso nel campo **Intervallo IP per porta DMZ**.

### Configurazione IPv6

**Network**

**Edit DMZ Connection**

Interface : DMZ

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

Prefix Length : 64

Save Cancel

**Nota:** per la configurazione IPv6 sono disponibili le opzioni seguenti:

Passaggio 7. Specifica indirizzo IPv6 DMZ: immettere l'indirizzo IPv6.

Passaggio 8. Lunghezza prefisso "immettere la lunghezza del prefisso del dominio di indirizzi IP DMZ indicato in precedenza.

Passaggio 9. Fare clic su **Save** (Salva) per salvare la configurazione.

## Configurazione delle regole di accesso

Questa configurazione viene effettuata per definire gli elenchi degli accessi per gli IP configurati sulle diverse subnet mask.

Passaggio 1. Accedere alla pagina Router Configuration Utility e scegliere **Firewall > Regole di accesso**. Viene visualizzata la pagina *Regole di accesso*:

**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:** le regole di accesso predefinite non possono essere modificate.

Passaggio 2. Fare clic sul pulsante **Aggiungi** per aggiungere una nuova regola di accesso. La pagina *Regole di accesso* cambia per visualizzare le aree Servizi e Pianificazione.

**Nota:** questa configurazione può essere eseguita sia per IPv4 che per IPv6 selezionando le rispettive schede nella pagina *Regole di accesso*. La procedura di configurazione specifica per IPv4 e IPv6 è descritta nei passaggi seguenti.

### 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

Passaggio 3. Scegliere **Consenti** dall'elenco a discesa Azione per consentire il servizio.

Passaggio 4. Selezionare **All Traffic [TCP&UDP/1~65535]** dall'elenco a discesa Service (Servizio) per abilitare tutti i servizi per la DMZ.

Passaggio 5. Selezionare **Registra pacchetti corrispondenti a questa regola** dall'elenco a discesa Registra per scegliere solo i registri corrispondenti alla regola di accesso.

Passaggio 6. Scegliere **DMZ** dall'elenco a discesa Interfaccia di origine, che rappresenta l'origine delle regole di accesso.

Passaggio 7. Selezionare **Any** (Qualsiasi) dall'elenco a discesa Source IP (IP origine).

Passaggio 8. Selezionare una delle seguenti opzioni disponibili dall'elenco a discesa IP di destinazione.

- Singolo: scegliere singolo per applicare questa regola a un singolo indirizzo IP.
- Intervallo: scegliere un intervallo per applicare questa regola a un intervallo di indirizzi IP. Immettere il primo e l'ultimo indirizzo IP dell'intervallo. Questa opzione è disponibile solo in IPv4.
- Subnet: scegliere Subnet per applicare le regole a una sottorete. Immettere l'indirizzo IP e il numero di notazione CIDR utilizzati per allocare gli indirizzi IP e instradare i pacchetti del protocollo Internet per la subnet. Questa opzione è disponibile solo in IPv6.
- Qualsiasi - Scegliere Qualsiasi per applicare la regola a qualsiasi indirizzo IP.

**Timesaver:** passare al passaggio 10 se si stanno configurando le regole di accesso IPv6.

Passaggio 9. Dall'elenco a discesa Ora, scegliere un metodo per definire quando le regole sono attive. più di un'opzione:

- **Sempre:** se si sceglie Sempre dall'elenco a discesa Ora, le regole di accesso vengono sempre applicate al traffico.
- **Intervallo:** se si seleziona Intervallo dall'elenco a discesa Tempo, è possibile scegliere un intervallo di tempo specifico per l'attivazione delle regole di accesso. Dopo aver specificato l'intervallo di tempo, selezionare le caselle di controllo Validità il per indicare i giorni in cui si desidera che le regole di accesso siano attive.

Passaggio 10. Fare clic su **Save** (Salva) per salvare le impostazioni.

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		

Passaggio 11. Fare clic sull'icona **Modifica** per modificare la regola di accesso creata.

Passaggio 12. Fare clic sull'icona **Elimina** per eliminare la regola di accesso creata.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).