

Configurazione di più IP pubblici in una zona demilitarizzata (DMZ) su router VPN RV042, RV042G e RV082

Obiettivo

La zona demilitarizzata (DMZ) è una rete interna di un'organizzazione, resa disponibile a una rete non attendibile. Per quanto riguarda la protezione, la DMZ si trova tra reti attendibili e non attendibili. La manutenzione della DMZ consente di migliorare la sicurezza della rete interna di un'organizzazione. Quando un elenco di controllo di accesso (ACL) è associato a un'interfaccia, le relative regole ACE (Access Control Element) vengono applicate ai pacchetti che arrivano all'interfaccia. I pacchetti che non corrispondono a nessuna delle voci ACE nell'elenco di controllo di accesso vengono associati a una regola predefinita che prevede l'eliminazione dei pacchetti non corrispondenti.

L'obiettivo di questo documento è quello di mostrare come configurare la porta DMZ in modo da consentire più indirizzi IP pubblici e definire l'elenco di controllo di accesso (ACL) per gli IP sul dispositivo router.

Dispositivi interessati

RV042
RV042G
RV082

Versione del software

· v4.2.2.08

Configurazione DMZ

Passaggio 1. Accedere alla pagina Web Configuration Utility 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

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

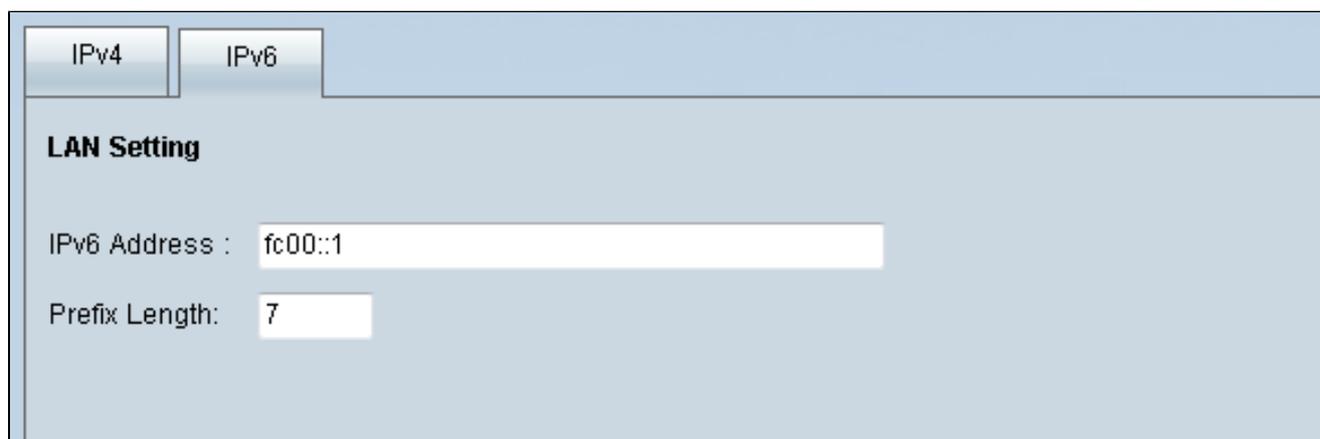
Interface	IP Address	Configuration
DMZ	0.0.0.0	

Passaggio 2. Nel campo Modalità IP, fare clic sul pulsante di opzione IP a doppio stack per abilitare la configurazione degli indirizzi 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

Passaggio 3. Fare clic sulla scheda IPv6 nel campo Impostazione LAN per configurare DMZ su indirizzo IPv6.



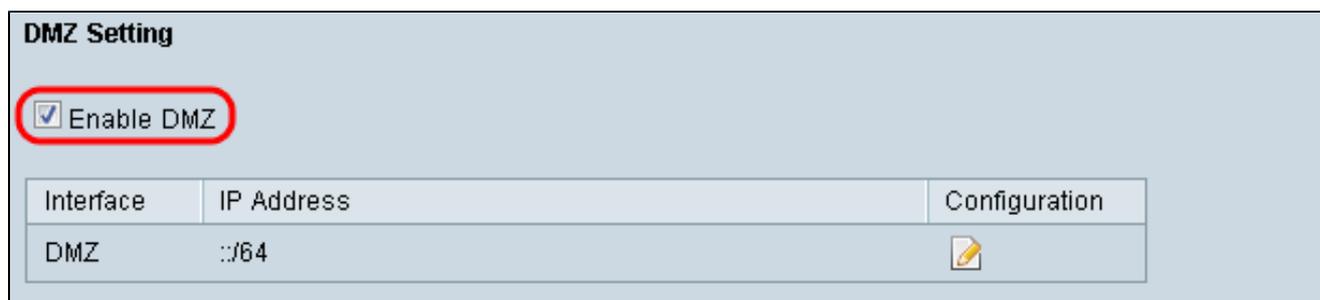
IPv4 IPv6

LAN Setting

IPv6 Address : fc00::1

Prefix Length: 7

Passaggio 4. Scorrere verso il basso fino all'area Impostazione DMZ e fare clic sulla casella di controllo DMZ per attivare DMZ

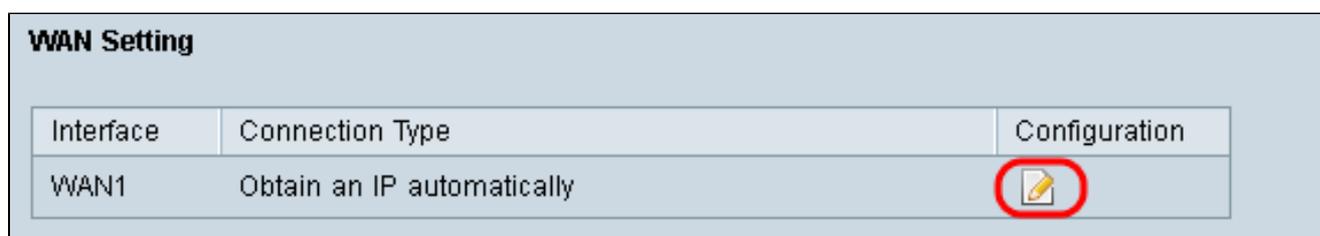


DMZ Setting

Enable DMZ

Interface	IP Address	Configuration
DMZ	::/64	

Passaggio 5. Nel campo WAN Setting (Impostazioni WAN) fare clic sul pulsante Edit (Modifica) per modificare le impostazioni IP Static della WAN1.



WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

Viene visualizzata la pagina Rete:

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

Passaggio 6. Selezionare Static IP dall'elenco a discesa WAN Connection Type (Tipo di connessione WAN).

Passaggio 7. Immettere l'indirizzo IP WAN visualizzato nella pagina System Summary (Riepilogo sistema) nel campo Specify WAN IP Address (Specifica indirizzo IP WAN).

Passaggio 8. Immettere l'indirizzo della subnet mask nel campo Subnet mask.

Passaggio 9. Immettere l'indirizzo del gateway predefinito nel campo Indirizzo gateway predefinito.

Passaggio 10. Immettere l'indirizzo del server DNS visualizzato nella pagina Riepilogo sistema nel campo Server DNS (obbligatorio) 1.

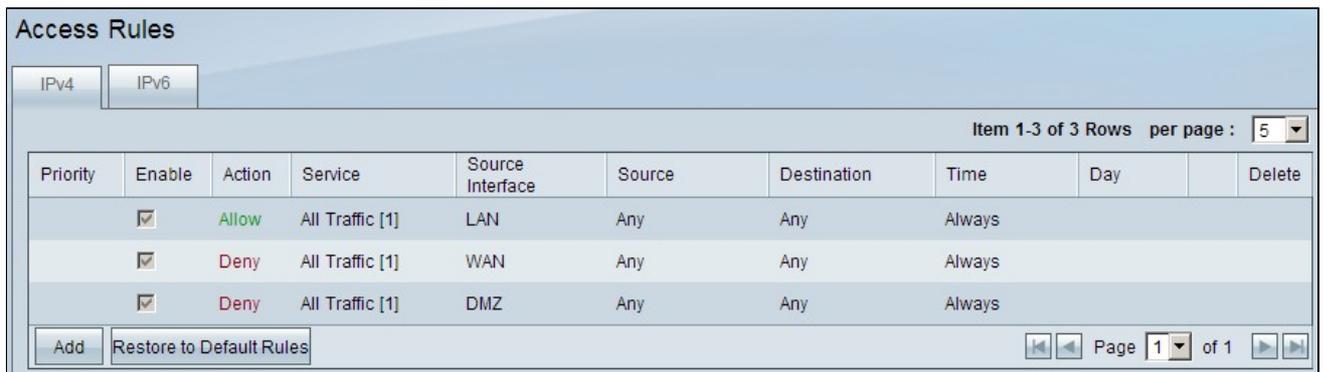
Nota: l'indirizzo 2 del server DNS è facoltativo.

Passaggio 11. Selezionare l'MTU (Maximum Transmission Unit) da impostare su Auto o Manuale. Se si sceglie manuale, immettere i byte per l'MTU manuale.

Passaggio 12. Fare clic sulla scheda Salva per salvare le impostazioni.

Definizione ACL

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



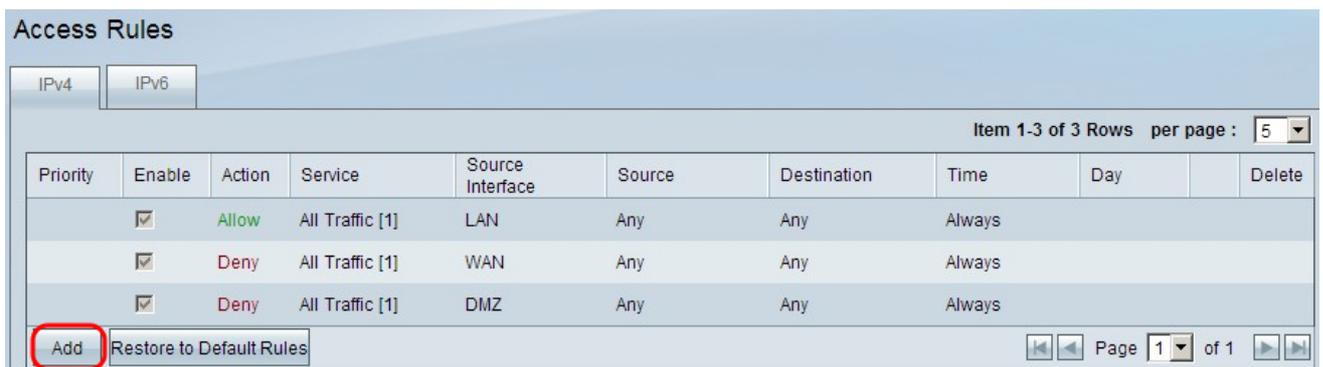
Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ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

Item 1-3 of 3 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

Nota: quando si immette la pagina Regole di accesso, le regole di accesso predefinite non possono essere modificate.

Passaggio 2. Fare clic sul pulsante Aggiungi per aggiungere una nuova regola di accesso.



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		

Item 1-3 of 3 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

Nella pagina Regole di accesso verranno visualizzate le opzioni per le aree Servizio e Pianificazione.

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. Scegliere Registra pacchetti corrispondenti a questa regola dall'elenco a discesa Registra per scegliere solo i registri corrispondenti alla regola di accesso.

Passaggio 6. Selezionate DMZ dall'elenco a discesa Interfaccia origine (Source Interface). Questa è l'origine delle regole di accesso.

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

Passaggio 8. Selezionare Single (Singolo) dall'elenco a discesa Destination IP (IP destinazione).

Passaggio 9. Immettere gli indirizzi IP della destinazione a cui consentire le regole di accesso nel campo IP destinazione.

Passaggio 10. Nell'area Programmazione scegliere Sempre dall'elenco a discesa Ora per rendere sempre attiva la regola di accesso.

Nota: se si sceglie Sempre dall'elenco a discesa Ora, per impostazione predefinita la regola di accesso verrà impostata su Ogni giorno nel campo Validità il.

Nota: è possibile scegliere un intervallo di tempo specifico (per il quale sono attive le regole di accesso) selezionando Intervallo dall'elenco a discesa Tempo. È quindi possibile selezionare i giorni in cui si desidera che le regole di accesso siano attive nelle caselle di controllo Validità il.

Passaggio 11. Fare clic su Save (Salva) per salvare le impostazioni.

Nota: se viene visualizzata una finestra popup, premere 'OK' per aggiungere un'altra regola di accesso oppure 'Annulla' per tornare alla pagina Regole di accesso.

Viene visualizzata la regola di accesso creata nel passaggio precedente

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

Passaggio 12. Fare clic sull'icona Modifica per modificare la regola di accesso creata.

Passaggio 13. 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).