

# Konfiguration mehrerer öffentlicher IPs in der DMZ auf RV042-, RV042G- und RV082-VPN-Routern

## Ziel

Die DMZ (Demilitarized Zone) ist ein internes Netzwerk einer Organisation, das einem nicht vertrauenswürdigen Netzwerk zur Verfügung gestellt wird. Wie aus Sicherheitsgründen hervorgeht, befindet sich die DMZ zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken. Die Wartung der DMZ trägt zur Verbesserung der Sicherheit des internen Netzwerks eines Unternehmens bei. Wenn eine Zugriffskontrollliste (Access Control List, ACL) an eine Schnittstelle gebunden ist, werden die entsprechenden Zugriffskontrollelement-Regeln (Access Control Element, ACE) auf Pakete angewendet, die an dieser Schnittstelle eintreffen. Pakete, die keinem der ACEs in der Zugriffskontrollliste entsprechen, werden einer Standardregel zugeordnet, deren Aktion darin besteht, nicht übereinstimmende Pakete zu verwerfen.

In diesem Dokument wird erläutert, wie der DMZ-Port so konfiguriert wird, dass mehrere öffentliche IP-Adressen zugelassen werden, und wie die Zugriffskontrollliste (ACL) für IPs auf dem Router definiert wird.

## Unterstützte Geräte

• RV042  
• RV042G  
• RV082

## Software-Version

• v4.2.2.08

## DMZ-Konfiguration

Schritt 1: Melden Sie sich bei der Seite für das Webkonfigurationsprogramm an, und wählen Sie **Setup > Network (Setup > Netzwerk)**. Die Seite *Netzwerk* wird geöffnet:

## 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

### WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	<input type="button" value="Edit"/>

### DMZ Setting

Enable DMZ

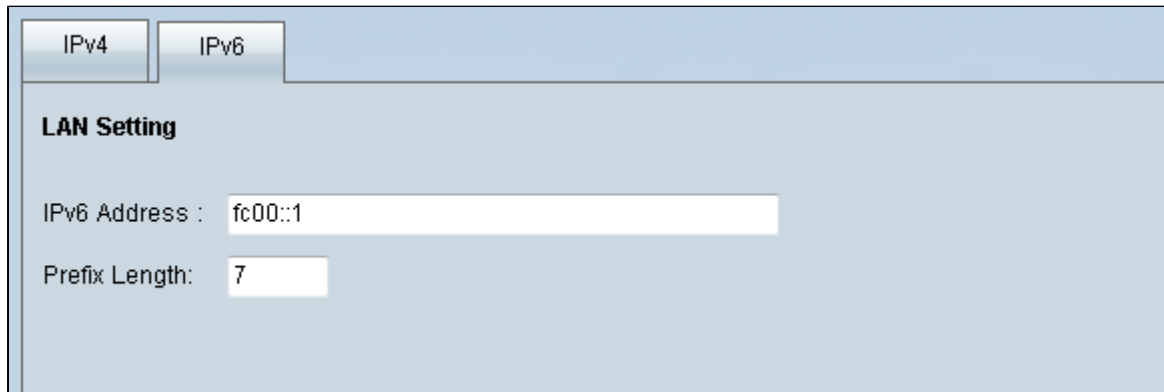
Interface	IP Address	Configuration
DMZ	0.0.0.0	<input type="button" value="Edit"/>

Schritt 2: Klicken Sie im Feld "IP Mode" (IP-Modus) auf das Optionsfeld **Dual-Stack IP**, um die Konfiguration von IPv6-Adressen zu aktivieren.

### 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

Schritt 3: Klicken Sie auf die Registerkarte IPv6 im Feld *LAN Setting (LAN-Einstellung)*, um die DMZ für die IPv6-Adresse konfigurieren zu können.



The screenshot shows the 'LAN Setting' configuration page with the 'IPv6' tab selected. The 'IPv6 Address' field contains 'fc00::1' and the 'Prefix Length' field contains '7'.

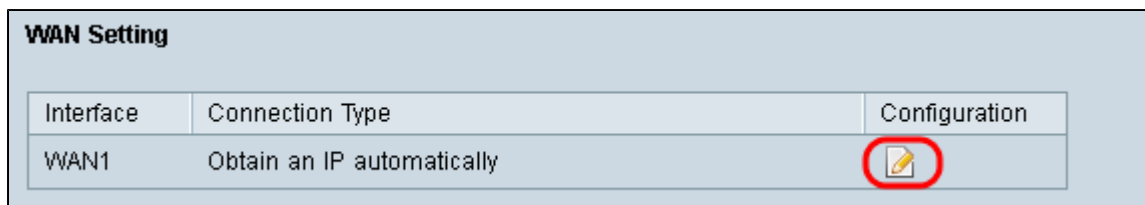
Schritt 4: Blättern Sie nach unten zum Bereich für DMZ-Einstellungen, und klicken Sie auf das Kontrollkästchen **DMZ**, um DMZ zu aktivieren.




The screenshot shows the 'DMZ Setting' configuration page. The 'Enable DMZ' checkbox is checked and circled in red. Below it is a table with columns for Interface, IP Address, and Configuration.

Interface	IP Address	Configuration
DMZ	::64	

Schritt 5: Klicken Sie im Feld *WAN-Einstellung* auf die Schaltfläche **Bearbeiten**, um die IP-Statik der WAN1-Einstellungen zu bearbeiten.



The screenshot shows the 'WAN Setting' configuration page. A table lists WAN1 with the connection type 'Obtain an IP automatically'. The 'Configuration' button (edit icon) is circled in red.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

Die Seite *Netzwerk* wird geöffnet:

**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

Schritt 6: Wählen Sie in der Dropdown-Liste *WAN Connection Type* (WAN-Verbindungstyp) die Option **Static IP (Statische IP)** aus.

Schritt 7. Geben Sie die WAN-IP-Adresse ein, die auf der Seite *Systemübersicht* im Feld *WAN-IP-Adresse angeben* angezeigt wird.

Schritt 8: Geben Sie die Adresse der Subnetzmaske in das Feld *Subnetzmaske ein*.

Schritt 9. Geben Sie die Standard-Gateway-Adresse in das Feld *Standard-Gateway-Adresse ein*.

Schritt 10. Geben Sie die DNS-Serveradresse ein, die auf der Seite *Systemübersicht* im Feld *DNS Server (erforderlich) 1* angezeigt wird.

**Hinweis:** Die DNS-Serveradresse 2 ist optional.

Schritt 11. Wählen Sie als Maximum Transmission Unit (MTU) entweder **Auto (Automatisch)** oder **Manual (Manuell)**. Wenn Sie Manual (Manuell) auswählen, geben Sie die Bytes für die Manual MTU (Manuelle MTU) ein.

Schritt 12: Klicken Sie auf die Registerkarte **Speichern**, um Ihre Einstellungen zu speichern.

## ACL-Definition

Schritt 1: Melden Sie sich bei dem Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Rules**. Die Seite *Zugriffsregeln* wird geöffnet:

### Access Rules

IPv4 IPv6

Item 1-3

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
	<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

**Hinweis:** Wenn Sie die Seite "Zugriffsregeln" aufrufen, können die Standardzugriffsregeln nicht bearbeitet werden.

Schritt 2: Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Zugriffsregel hinzuzufügen.

### Access Rules

IPv4 IPv6

Item 1-3

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
	<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

Auf der Seite *Access Rules* (Zugriffsregeln) werden nun Optionen für die Bereiche *Service* und *Planung* angezeigt.

### 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

Schritt 3: Wählen Sie **Zulassen** aus der Dropdown-Liste *Aktion* aus, um den Dienst zuzulassen.

Schritt 4: Wählen Sie in der Dropdown-Liste "*Service*" die Option **Gesamter Datenverkehr [TCP&UDP/1~65535]** aus, um alle Services für die DMZ zu aktivieren.

Schritt 5: Wählen Sie **Protokollpakete, die mit dieser Regel übereinstimmen**, aus der Dropdown-Liste *Protokoll*, um nur Protokolle auszuwählen, die mit der Zugriffsregel übereinstimmen.

Schritt 6: Wählen Sie **DMZ** aus der Dropdown-Liste "*Source Interface*" aus. Dies ist die Quelle für die Zugriffsregeln.

Schritt 7. Wählen Sie **Any (Beliebig)** aus der Dropdown-Liste *Source IP* (Quell-IP) aus.

Schritt 8: Wählen Sie **Single** aus der Dropdown-Liste *Destination IP* aus.

Schritt 9. Geben Sie die IP-Adressen des Ziels ein, dem die Zugriffsregeln im Feld *Ziel-IP* zugewiesen werden sollen.

Schritt 10. Wählen Sie im Bereich *Zeitplanung* in der Dropdown-Liste *Zeit* die Option **Immer** aus, um die Zugriffsregel jederzeit zu aktivieren.

**Hinweis:** Wenn Sie in der *Dropdown-Liste "Zeit"* die Option "**Immer**" auswählen, wird die Zugriffsregel im Feld "**Jeden Tag am**" standardmäßig auf "**Täglich**" gesetzt.

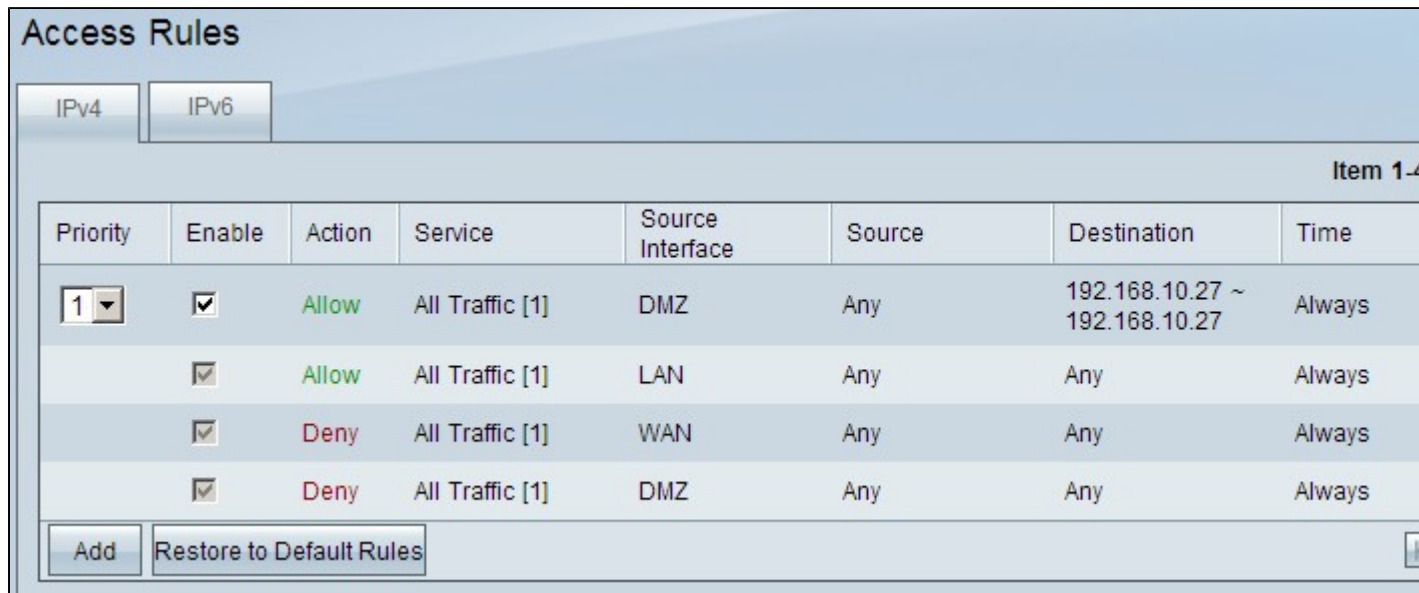
**Hinweis:** Sie können ein bestimmtes Zeitintervall (für das die Zugriffsregeln aktiv sind) auswählen, indem Sie in der Dropdown-Liste *Zeit* die Option **Intervall** auswählen. Anschließend können Sie die Tage auswählen, an denen die Zugriffsregeln aktiv sein sollen. Aktivieren Sie dazu die

Kontrollkästchen *Gültig für*.

Schritt 11. Klicken Sie auf **Speichern**, um Ihre Einstellungen zu speichern.

**Hinweis:** Wenn ein Popup-Fenster angezeigt wird, drücken Sie 'OK', um eine weitere Zugriffsregel hinzuzufügen, oder 'Abbrechen', um zur Seite 'Zugriffsregeln' zurückzukehren.

Die im vorherigen Schritt erstellte Zugriffsregel wird jetzt angezeigt.



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
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

Buttons: Add, Restore to Default Rules

Schritt 12: Klicken Sie auf das Symbol **Bearbeiten**, um die erstellte Zugriffsregel zu bearbeiten.

Schritt 13: Klicken Sie auf das Symbol **Löschen**, um die erstellte Zugriffsregel zu löschen.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.