

# Configuratie van meerdere openbare IPâ€™s in gemilitariseerde zone (DMZ) op RV042, RV042G en RV082 VPN-routers

## Doel

De gedemilitariseerde zone (DMZ) is een intern netwerk van een organisatie, dat beschikbaar wordt gesteld aan een onbetrouwbaar netwerk. Zoals per veiligheid, valt DMZ tussen vertrouwde op en onbetrouwbare netwerken. Onderhoud van de DMZ helpt de beveiliging van de communicatie naar het interne netwerk van een organisatie te verbeteren. Wanneer een toegangscontrolelijst (ACL) aan een interface is gebonden, worden de regels van het Toegangsbeheer Element (ACE) toegepast op pakketten die bij die interface aankomen. Pakketten die niet overeenkomen met een van de ACE's in de toegangscontrolelijst worden gekoppeld aan een standaardregel waarvan de actie is om ongeëvenaarde pakketten te laten vallen.

Het doel van dit document is u te tonen hoe u de DMZ-poort kunt configureren om meerdere openbare IP-adressen toe te staan en de toegangscontrolelijst (ACL) voor IPâ€™s op het routerapparaat te definiëren.

## Toepasselijke apparaten

- RV042
- RV042G
- RV082

## Softwareversie

- v4.2.2.08

## DMZ-configuratie

Stap 1. Log in op de pagina van het hulpprogramma Web Configuration en kies **Setup > Netwerk**. De pagina *Netwerk* wordt geopend:

## 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

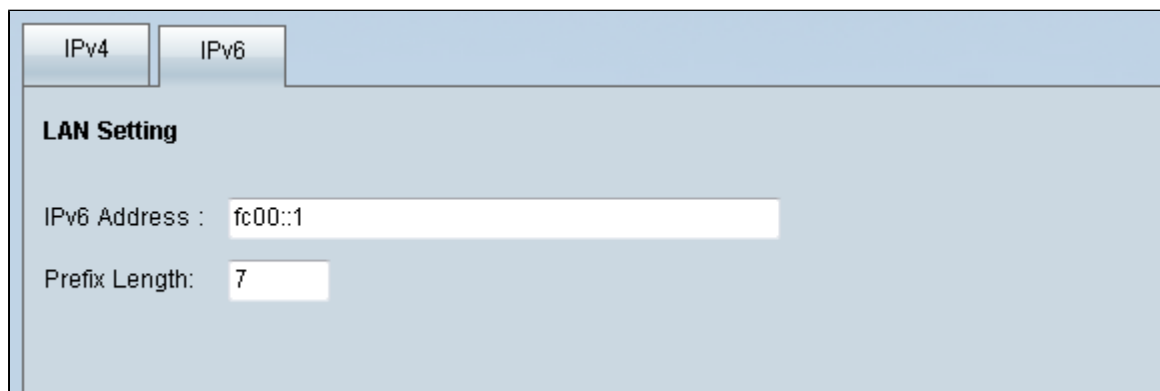
Interface	IP Address	Configuration
DMZ	0.0.0.0	<input type="button" value="Edit"/>

Stap 2. Klik in het veld *IP-modus* op de radioknop **Dual-Stack IP** om de configuratie van IPv6-adressen mogelijk te maken.

### 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

Stap 3. Klik op het tabblad IPv6 in het veld *LAN-instelling* om DMZ op IPv6-adres te kunnen configureren.



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'.

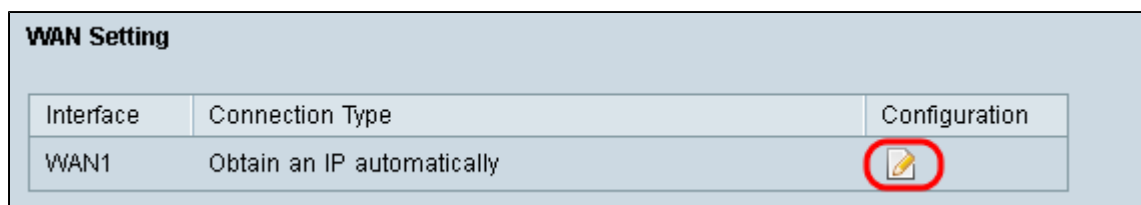
Stap 4. Blader naar beneden naar het DMZ-instellingsgebied en klik op het selectievakje **DMZ** om DMZ in te schakelen




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	

Stap 5. Klik in het veld *WAN Settings* op de knop **Edit** om de IP-statisch van de WAN1-instellingen te bewerken.



The screenshot shows the 'WAN Setting' configuration page. The 'Edit' icon (pencil) in the 'Configuration' column for the 'WAN1' interface is circled in red.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

De pagina *Netwerk* wordt geopend:

**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

Stap 6. Kies **Statische IP** in de vervolkeuzelijst *WAN-verbindingstype*.

Stap 7. Voer het WAN IP-adres in dat wordt weergegeven op de pagina *Systeemoverzicht* in het veld *WAN-IP-adres opgeven*.

Stap 8. Voer het subnetmasker in het veld *Subnetmasker in*.

Stap 9. Voer het standaardgatewayadres in in het veld *Default Gateway Address*.

Stap 10. Voer het adres van de DNS-server in dat wordt weergegeven op de pagina *Systeemoverzicht* in het veld *DNS-server (verplicht) 1*.

**Opmerking:** DNS-serveradres 2 is optioneel.

Stap 11. Kies de Maximum Transmission Unit (MTU) in **Auto** of **Manual**. Als u handmatig kiest, voert u de bytes voor de Handmatige MTU in.

Stap 12. Klik op het tabblad **Opslaan** om uw instellingen op te slaan.

## ACL-definitie

Stap 1. Log in op de pagina van het hulpprogramma Web Configuration en kies **Firewall > Toegangsregels**. De pagina *Toegangsregels* wordt geopend:

### 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

**Opmerking:** wanneer u de pagina *Toegangsregels* invoert, kunnen de standaardtoegangsregels niet worden bewerkt.

Stap 2. Klik op de knop **Toevoegen** om een nieuwe toegangsregel toe te voegen.

### 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

De pagina *Toegangsregels* toont nu opties voor de gebieden *Service* en *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

Stap 3. Kies **Toestaan** in de vervolgkeuzelijst *Actie* om de service toe te staan.

Stap 4. Kies **All Traffic [TCP&UDP/1~65535]** in de vervolgkeuzelijst *Service* om alle services voor de DMZ in te schakelen.

Stap 5. Kies **Logpakketten overeenkomen met deze regel** uit de vervolgkeuzelijst *Log* om alleen logs te kiezen die overeenkomen met de toegangsregel.

Stap 6. Kies **DMZ** in de vervolgkeuzelijst *Source Interface*. Dit is de bron voor de toegangsregels.

Stap 7. Kies **om het even welk** van de vervolgkeuzelijst *BronIP*.

Stap 8. Kies **Single** uit de vervolgkeuzelijst *Bestemming IP*.

Stap 9. Voer in het veld *Bestemming* de IP-adressen in van de bestemming waarvoor de toegangsregels gelden.

Stap 10. In het gebied *Scheduling* kies **altijd** uit de vervolgkeuzelijst *Tijd* om de toegangsregel altijd actief te maken.

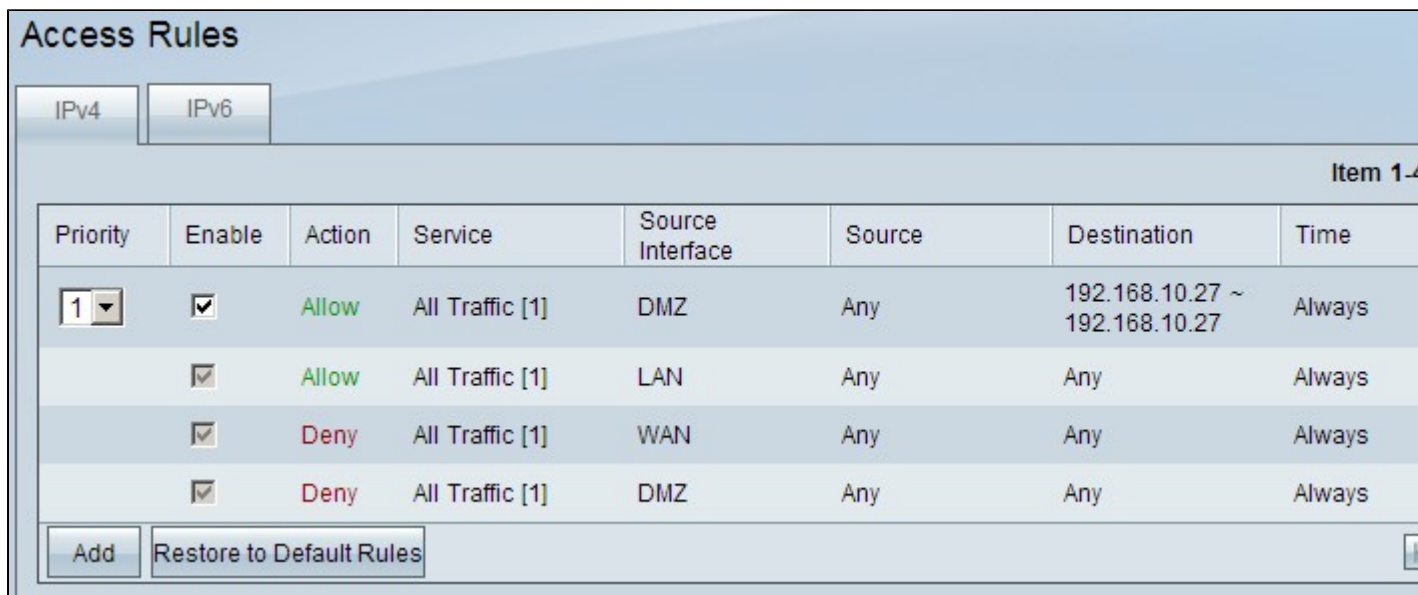
**Opmerking:** Als u **altijd** kiest uit de vervolgkeuzelijst *Tijd*, wordt de toegangsregel standaard ingesteld op **Dagelijks** in het veld *Effectief op*.

**N.B.:** U kunt een specifiek tijdsinterval kiezen (waarvoor de toegangsregels actief zijn) door **Interval** te selecteren uit de vervolgkeuzelijst *Tijd*. Vervolgens kunt u de dagen kiezen waarop u wilt dat de toegangsregels actief zijn vanuit de selectievakjes *Effectief op*.

Stap 11. Klik op **Opslaan** om de instellingen op te slaan.

**Opmerking:** Als een pop-upvenster verschijnt, drukt u op 'OK' om een andere toegangsregel toe te voegen of drukt u op 'Annuleren' om terug te keren naar de pagina met toegangsregels.

De toegangsregel die u in de vorige stap hebt gemaakt, wordt nu weergegeven



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

Stap 12. Klik op het pictogram **Bewerken** om de gemaakte toegangsregel te bewerken.

Stap 13. Klik op het pictogram **Delete** om de gemaakte toegangsregel te verwijderen.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.