

Configuration de plusieurs adresses IP publiques dans une zone démilitarisée (DMZ) sur les routeurs VPN RV042, RV042G et RV082

Objectif

La zone démilitarisée (DMZ) est un réseau interne d'une organisation, qui est mis à la disposition d'un réseau non fiable. En termes de sécurité, la DMZ se situe entre les réseaux sécurisés et non sécurisés. La maintenance de la zone DMZ permet d'améliorer la sécurité de l'accès au réseau interne d'une entreprise. Lorsqu'une liste de contrôle d'accès (ACL) est liée à une interface, ses règles d'élément de contrôle d'accès (ACE) sont appliquées aux paquets qui arrivent à cette interface. Les paquets qui ne correspondent à aucune des entrées ACE de la liste de contrôle d'accès sont mis en correspondance avec une règle par défaut dont l'action est d'abandonner les paquets sans correspondance.

L'objectif de ce document est de vous montrer comment configurer le port DMZ pour autoriser plusieurs adresses IP publiques et définir la liste de contrôle d'accès (ACL) pour les adresses IP sur le périphérique du routeur.

Périphériques pertinents

- RV042
- RV042G
- RV082

Version du logiciel

- v 4.2.2.08

Configuration DMZ

Étape 1. Connectez-vous à la page Web Configuration Utility et choisissez Setup > Network. La page Network s'ouvre :

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	

Save

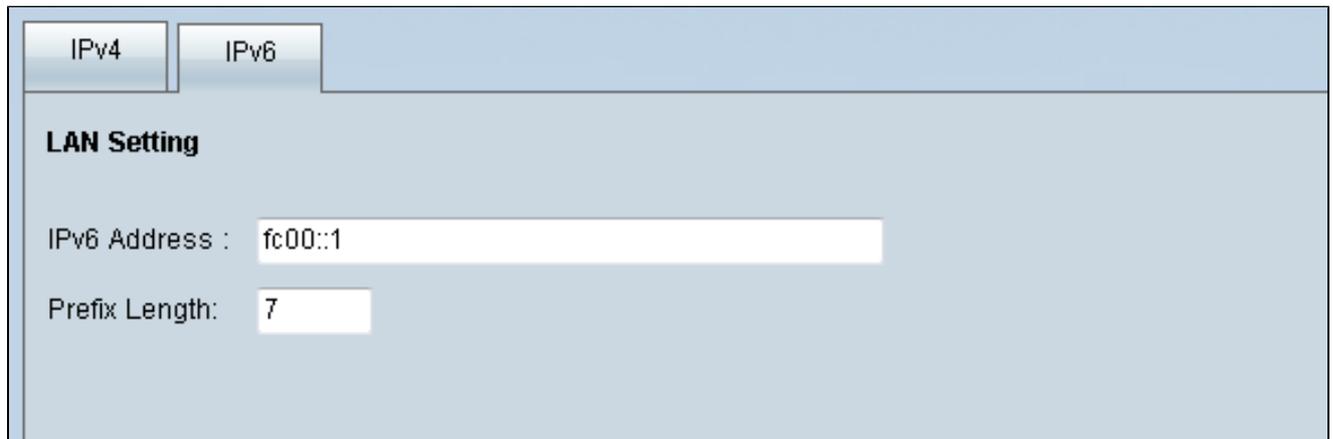
Cancel

Étape 2. Dans le champ IP Mode, cliquez sur la case d'option Dual-Stack IP pour activer la configuration des adresses IPv6.

IP Mode

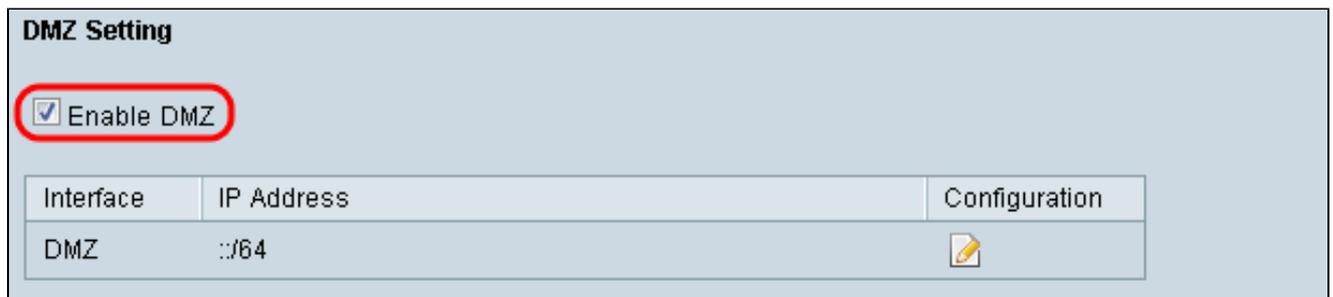
Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

Étape 3. Cliquez sur l'onglet IPv6 situé dans le champ LAN Setting pour être en mesure de configurer DMZ sur l'adresse IPv6.



The screenshot shows the 'LAN Setting' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6', with 'IPv6' being the active tab. Below the tabs, the 'LAN Setting' section is visible. It contains two input fields: 'IPv6 Address' with the value 'fc00::1' and 'Prefix Length' with the value '7'.

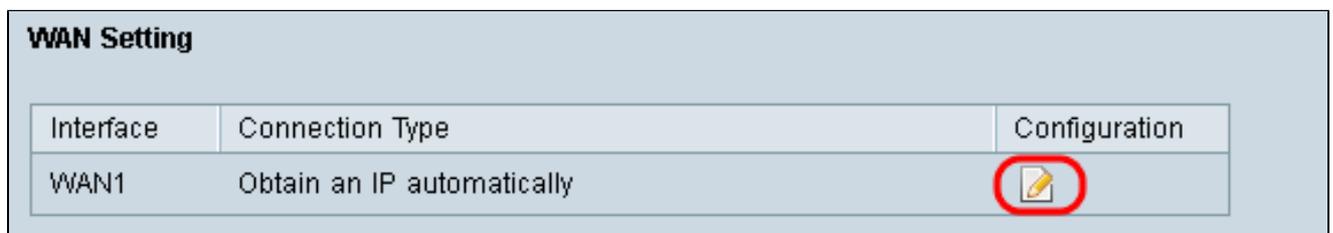
Étape 4. Faites défiler jusqu'à la zone DMZ Setting et cochez la case DMZ pour activer DMZ



The screenshot shows the 'DMZ Setting' configuration page. At the top, the 'DMZ Setting' section is visible. It contains a checkbox labeled 'Enable DMZ' which is checked and circled in red. Below this, there is a table with three columns: 'Interface', 'IP Address', and 'Configuration'.

Interface	IP Address	Configuration
DMZ	::/64	

Étape 5. Dans le champ WAN Setting, cliquez sur le bouton Edit pour modifier les paramètres IP Static des paramètres WAN1.



The screenshot shows the 'WAN Setting' configuration page. It contains a table with three columns: 'Interface', 'Connection Type', and 'Configuration'.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

La page Réseau s'ouvre :

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

Étape 6. Sélectionnez Static IP dans la liste déroulante WAN Connection Type.

Étape 7. Saisissez l'adresse IP WAN affichée sur la page System Summary dans le champ Specify WAN IP Address.

Étape 8. Saisissez l'adresse du masque de sous-réseau dans le champ Subnet Mask.

Étape 9. Saisissez l'adresse de la passerelle par défaut dans le champ Default Gateway Address.

Étape 10. Saisissez l'adresse du serveur DNS affichée sur la page System Summary dans le champ DNS Server (Required) 1.

Remarque : l'adresse 2 du serveur DNS est facultative.

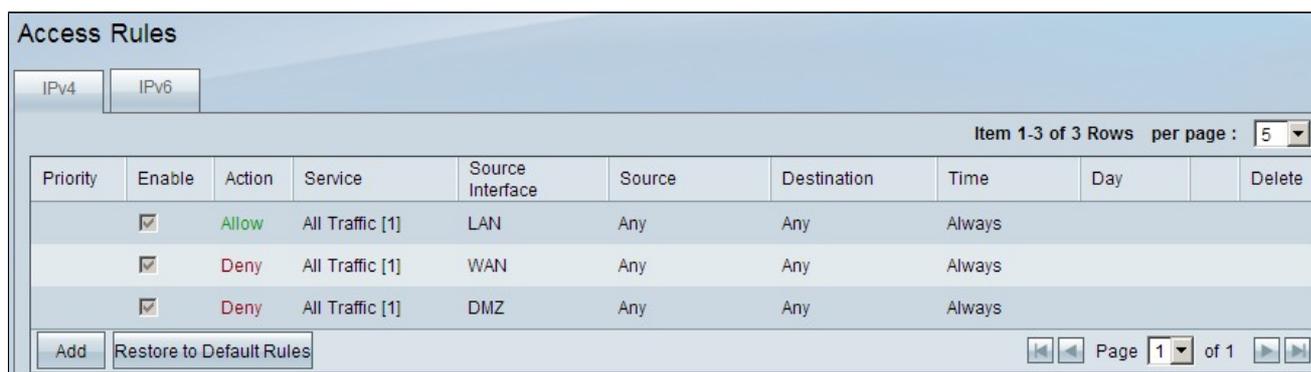
Étape 11. Choisissez l'unité de transmission maximale (MTU) Auto ou Manual. Si vous

choisissez Manual, saisissez les octets pour le MTU manuel.

Étape 12. Cliquez sur l'onglet Save pour enregistrer vos paramètres.

Définition ACL

Étape 1. Connectez-vous à la page Web Configuration Utility et choisissez Firewall > Access Rules. La page Access Rules s'ouvre :



Access Rules

IPv4 IPv6

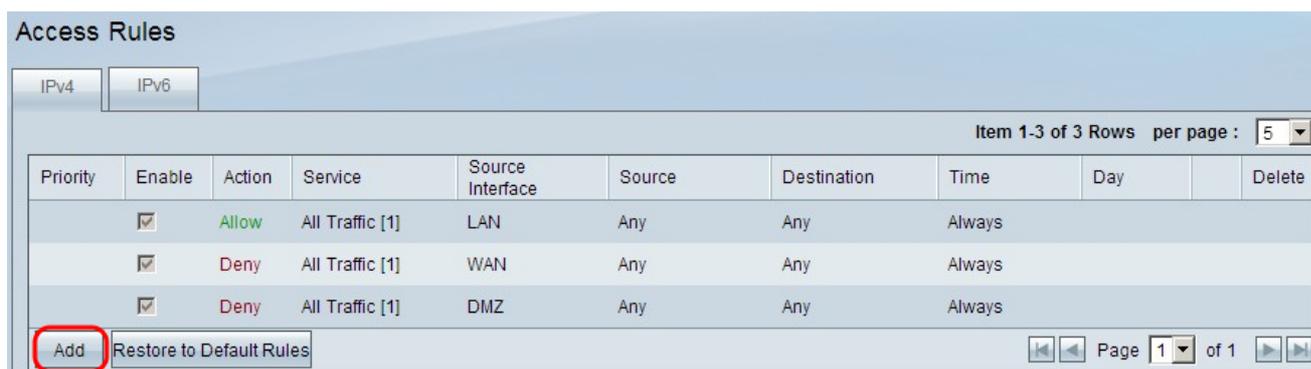
Item 1-3 of 3 Rows per page : 5

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

Remarque : lorsque vous accédez à la page Règles d'accès, les règles d'accès par défaut ne peuvent pas être modifiées.

Étape 2. Cliquez sur le bouton Add pour ajouter une nouvelle règle d'accès.



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

La page Règles d'accès affiche désormais les options des zones Service et Planification.

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

Étape 3. Choisissez Allow dans la liste déroulante Action pour autoriser le service.

Étape 4. Choisissez All Traffic [TCP&UDP/1~65535] dans la liste déroulante Service pour activer tous les services pour la DMZ.

Étape 5. Choisissez Log packets match this rule dans la liste déroulante Log pour sélectionner uniquement les journaux qui correspondent à la règle d'accès.

Étape 6. Sélectionnez DMZ dans la liste déroulante Source Interface. C'est la source des règles d'accès.

Étape 7. Choisissez Any dans la liste déroulante Source IP.

Étape 8. Choisissez Single dans la liste déroulante Destination IP.

Étape 9. Saisissez les adresses IP de la destination à autoriser selon les règles d'accès dans le champ Destination IP.

Étape 10. Dans la zone Scheduling, choisissez Always dans la liste déroulante Time pour que la règle d'accès soit active en permanence.

Remarque : si vous sélectionnez Toujours dans la liste déroulante Heure, la règle d'accès sera définie par défaut sur Tous les jours dans le champ Effectif sur.

Remarque : vous pouvez choisir un intervalle de temps spécifique (pour lequel les règles d'accès sont actives) en sélectionnant Interval dans la liste déroulante Time. Vous pouvez ensuite choisir les jours d'activation des règles d'accès à partir des cases à cocher Effectif le.

Étape 11. Cliquez sur Save pour enregistrer vos paramètres.

Remarque : si une fenêtre contextuelle apparaît, appuyez sur OK pour ajouter une autre règle d'accès ou sur Annuler pour revenir à la page des règles d'accès.

La règle d'accès que vous avez créée à l'étape précédente s'affiche



The screenshot shows the 'Access Rules' configuration window. It has tabs for 'IPv4' and 'IPv6'. The table below lists the rules:

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		

At the bottom, there are buttons for 'Add' and 'Restore to Default Rules', and a pagination control showing 'Page 1 of 1'.

Étape 12. Cliquez sur l'icône Edit pour modifier la règle d'accès créée.

Étape 13. Cliquez sur l'icône Supprimer pour supprimer la règle d'accès créée.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.