

Configuration du port de zone démilitarisée avec masque de sous-réseau sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Une zone démilitarisée (DMZ) est une partie d'un réseau interne d'une organisation qui est mise à la disposition d'un réseau non fiable tel qu'Internet. Une DMZ permet d'améliorer la sécurité du réseau interne d'une entreprise. Au lieu que toutes les ressources internes soient disponibles à partir d'Internet, seuls certains hôtes tels que les serveurs Web sont disponibles.

Lorsqu'une liste de contrôle d'accès (ACL) est liée à une interface, les 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. Cet article explique comment configurer le port DMZ et autoriser le trafic de la DMZ vers des adresses IP de destination spécifiques.

Périphériques pertinents

- RV016
- RV042
- RV042G
- RV082

Version du logiciel

- v 4.2.2.08

Configuration DMZ avec sous-réseau

Étape 1. Connectez-vous à la page Router 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 : 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	

Étape 2. Pour configurer DMZ sur une adresse IPv4 ou IPv6, cliquez sur l'onglet

correspondant situé dans le champ LAN Setting.

Remarque : l'IP à double pile dans la zone IP Mode doit être activée si vous souhaitez configurer IPv6.

Étape 3. Faites défiler jusqu'au champ DMZ Setting et cliquez sur la case d'option Enable DMZ pour activer 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	

Étape 4. Cliquez sur l'icône de configuration DMZ pour configurer le sous-réseau. La configuration peut être effectuée pour [IPv4](#) et [IPv6](#) de la manière suivante :

Configuration IPv4

Network

Edit DMZ Connection

Interface : DMZ

Subnet Range (DMZ & WAN within same subnet)

Specify DMZ IP Address :

Subnet Mask :

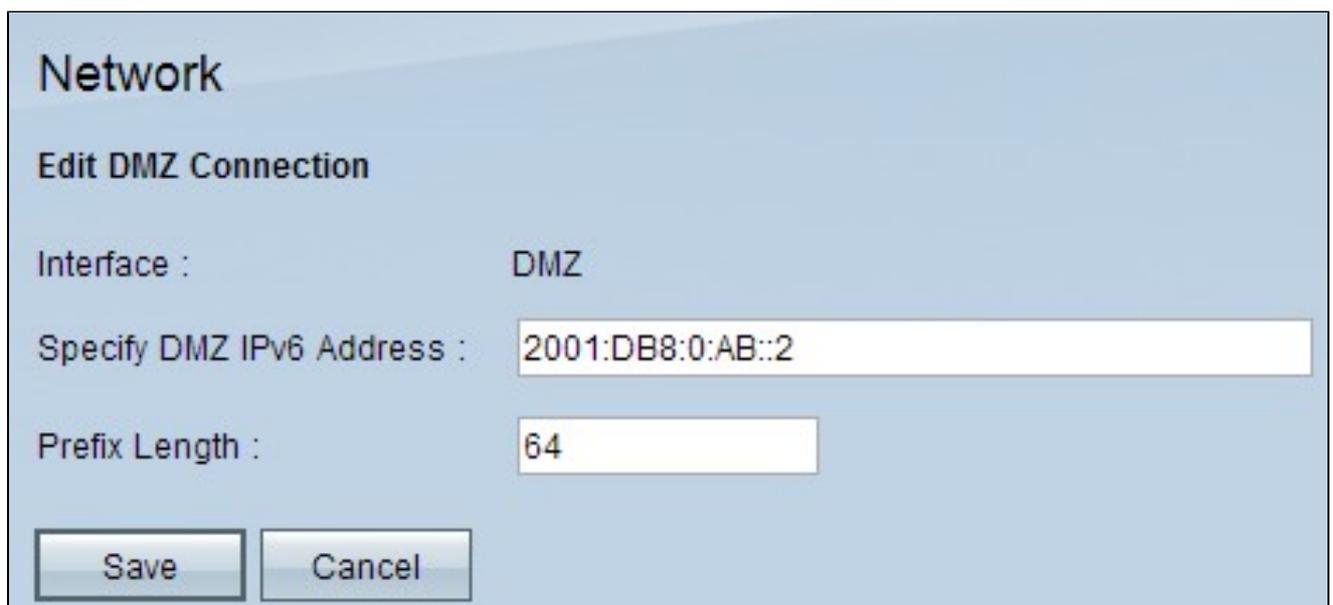
Étape 5. Cliquez sur la case d'option Subnet pour configurer DMZ sur un autre sous-réseau que celui du WAN. Pour Subnet IP, les éléments suivants doivent être configurés :

- Specify DMZ IP Address : saisissez l'adresse IP DMZ dans le champ Specify DMZ IP Address.
- Subnet Mask : saisissez le masque de sous-réseau dans le champ Subnet Mask.

Avertissement : les hôtes dont l'adresse IP se trouve dans la zone DMZ ne sont pas aussi sécurisés que les hôtes de votre réseau local interne.

Étape 6. Cliquez sur Range pour configurer la DMZ sur le même sous-réseau que le WAN. La plage des adresses IP doit être entrée dans le champ IP Range for DMZ port.

Configuration IPv6



The screenshot shows a window titled "Network" with a sub-header "Edit DMZ Connection". It contains the following fields and buttons:

- Interface : DMZ
- Specify DMZ IPv6 Address : 2001:DB8:0:AB::2
- Prefix Length : 64
- Buttons: Save, Cancel

Remarque : pour la configuration IPv6, les options suivantes sont disponibles :

Étape 7. Specify DMZ IPv6 Address : saisissez l'adresse IPv6.

Étape 8. Prefix Length : la longueur de préfixe du domaine d'adresse IP DMZ mentionné ci-dessus doit être entrée.

Étape 9. Cliquez sur Save pour enregistrer la configuration.

Configuration des règles d'accès

Cette configuration permet de définir les listes d'accès pour les adresses IP configurées sur les différents masques de sous-réseau.

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

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		

Remarque : 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. La page Access Rules change pour afficher les zones Services et Scheduling.

Remarque : cette configuration peut être effectuée pour IPv4 et IPv6 en sélectionnant ces onglets respectifs sur la page Access Rules. Les étapes de configuration spécifiques à IPv4 et IPv6 sont mentionnées dans les étapes suivantes.

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

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

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

Étape 8. Choisissez l'une des options disponibles suivantes dans la liste déroulante Destination IP.

- Single : choisissez single pour appliquer cette règle à une adresse IP unique.
- Range : choisissez range pour appliquer cette règle à une plage d'adresses IP. Saisissez la première et la dernière adresse IP de la plage. Cette option est disponible uniquement dans IPv4.
- Subnet : sélectionnez Subnet pour appliquer ces règles à un sous-réseau. Saisissez l'adresse IP et le numéro de notation CIDR utilisés pour l'allocation d'adresses IP et le routage des paquets du protocole Internet pour le sous-réseau. Cette option est disponible uniquement dans IPv6.
- Any : sélectionnez Any pour appliquer la règle à l'une des adresses IP.

Gain de temps : passez à l'étape 10 si vous configurez des règles d'accès IPv6.

Étape 9. Choisissez une méthode pour définir le moment où les règles sont actives dans la liste déroulante Heure. Elles sont :

- Always : si vous choisissez Always dans la liste déroulante Time, les règles d'accès seront toujours appliquées au trafic.
- Interval : vous pouvez choisir un intervalle de temps spécifique auquel les règles d'accès sont actives si vous sélectionnez Interval dans la liste déroulante Time. Après avoir spécifié l'intervalle de temps, sélectionnez les jours pendant lesquels vous souhaitez que les règles d'accès soient actives dans les cases à cocher Effectif le.

Étape 10. Cliquez sur Save pour enregistrer vos paramètres.

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		

Add Restore to Default Rules Page 1 of 1

Étape 11. Cliquez sur l'icône Edit pour modifier la règle d'accès créée.

Étape 12. 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.