# Configuration de port de zone démilitarisée avec le 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 rendue disponible à un réseau non approuvé tel que l'Internet. Un DMZ aide à améliorer la Sécurité dans le réseau interne d'une organisation. Au lieu de toutes les ressources internes étant fournies par l'Internet, seulement certains hôtes tels que des web server sont disponibles.

Quand une liste de contrôle d'accès (ACL) est liée à une interface, des règles d'élément de contrôle d'accès (ACE) sont appliquées aux paquets qui arrivent à cette interface. Des paquets qui n'apparient pas les as l'uns des dans l'ACL sont appariés à une règle par défaut dont l'action est de relâcher les paquets inégalés. Cet article affiche comment configurer le port DMZ et et permettre le trafic du DMZ aux adresses IP spécifiques de destination.

## Périphériques applicables

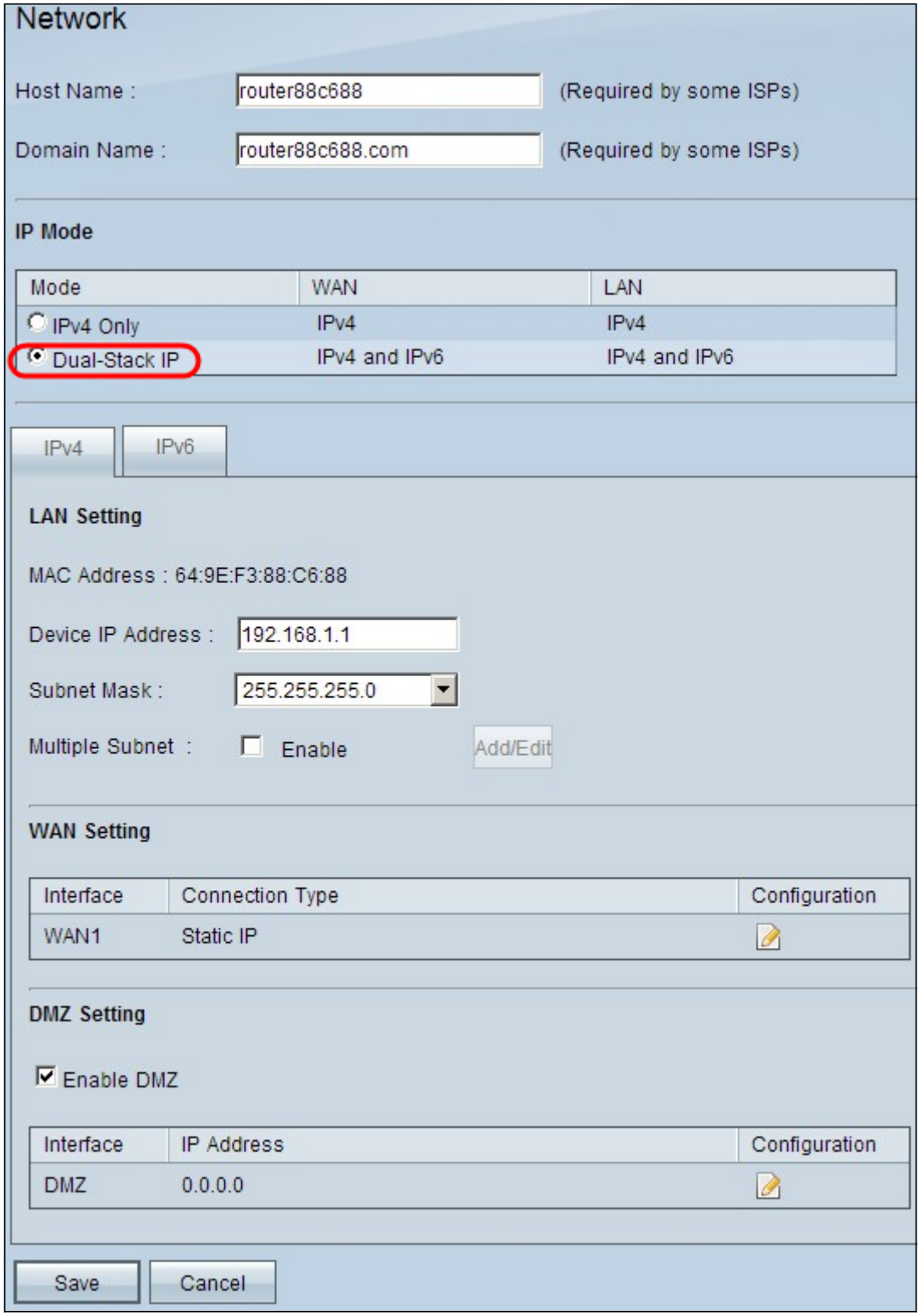
- RV016
- RV042
- RV042G
- RV082

## Version de logiciel

- v4.2.2.08

## Configuration DMZ avec le sous-réseau

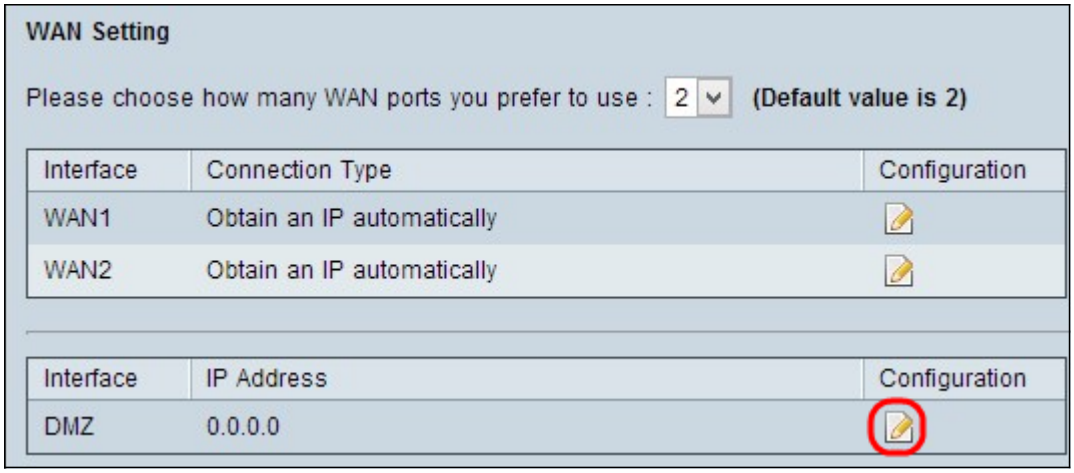
Étape 1. Connectez-vous dans la page d'utilitaire de configuration de routeur et choisissez l' **installation > le réseau**. La page de *réseau* s'ouvre :




**Étape 2.** Pour configurer DMZ sur l'ipv4 ou ipv6 addres cliquez sur l'onglet correspondant situé au champ de configuration de RÉSEAU LOCAL.

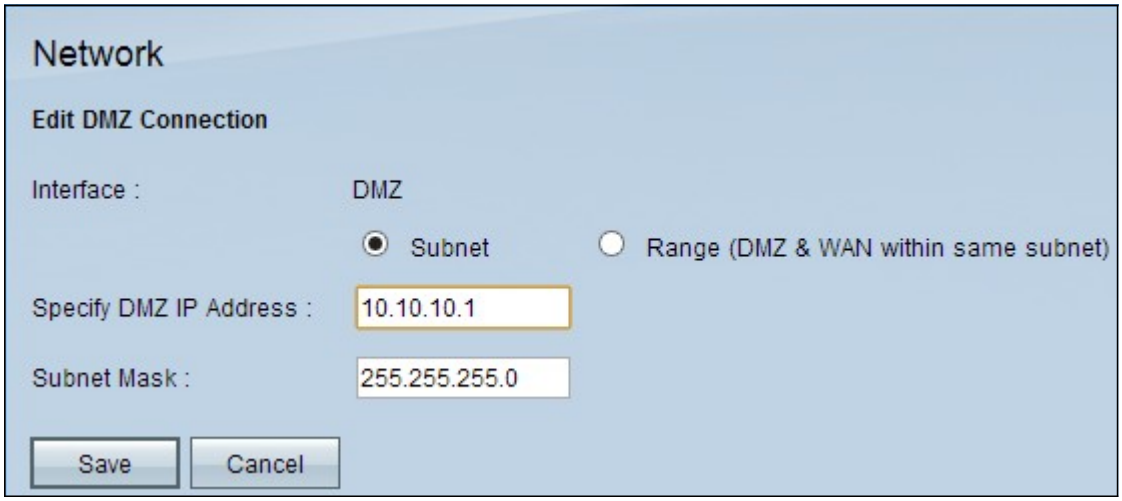
**Remarque:** L'IP de Double-pile dans la région de *mode IP* doit être activé si vous voulez configurer l'IPv6.

Étape 3. Faites descendre l'écran au champ de configuration DMZ et cliquez sur la case d'option de l'**enable DMZ** pour activer DMZ.




Étape 4. Cliquez sur en fonction l'icône de **configuration DMZ** pour configurer le sous-réseau. La configuration peut être faite pour l'ipv4 et l'IPv6 de la façon suivante :

## Configuration d'ipv4



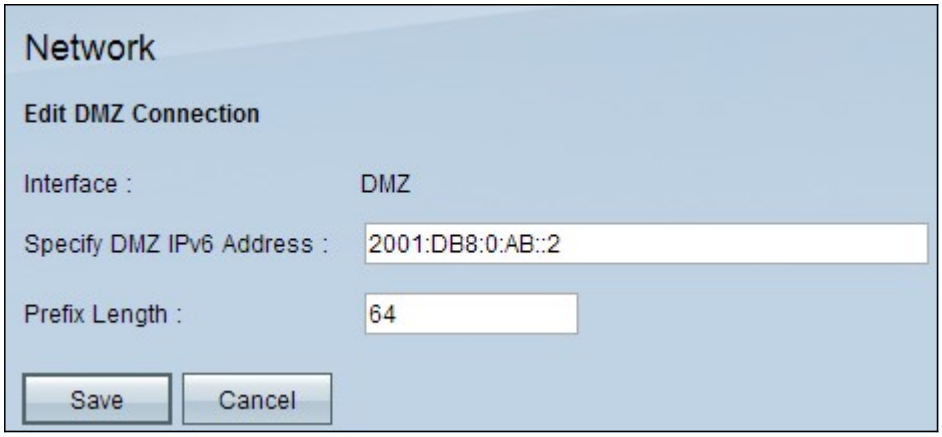

Étape 5. Cliquez sur la case d'option de **sous-réseau** pour configurer DMZ à un autre sous-réseau que cela du WAN. Pour l'IP de sous-réseau ce qui suit devrait être configuré

- Spécifiez l'adresse IP DMZ — Écrivez l'adresse IP DMZ dans le **champ IP Address du spécifier DMZ**.
- Masque de sous-réseau — Écrivez le masque de sous-réseau dans le domaine de **masque de sous-réseau.**

**Avertissement :** Les hôtes avec une adresse IP dans le DMZ ne sont pas aussi sécurisés que des hôtes à l'intérieur de votre RÉSEAU LOCAL interne.

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

## Configuration d'IPv6




**Remarque:** Pour la configuration d'IPv6 les options suivantes sont disponibles :

Étape 7. Spécifient l'ipv6 addres DMZ — Entrez dans l'ipv6 addres.

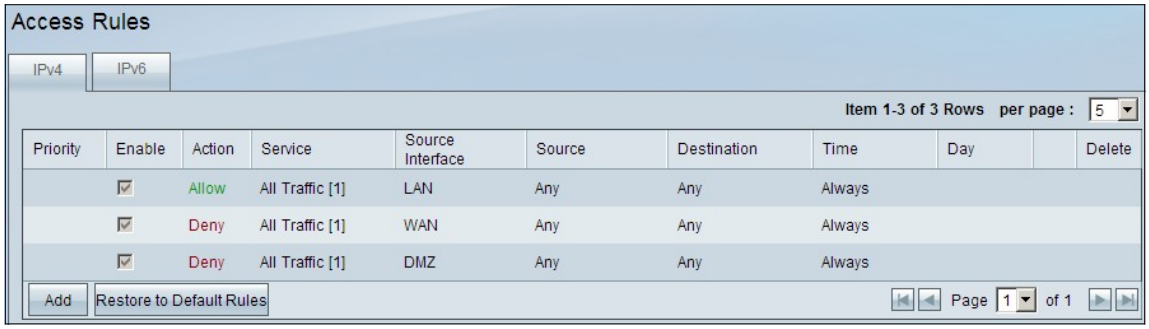
Étape 8. Longueur de préfixe — La longueur de préfixe du domaine d'adresse IP DMZ mentionné ci-dessus doit être entrée.

Étape 9. **Sauvegarde de** clic pour sauvegarder la configuration.

# Configuration de règles d'accès

Cette configuration est faite pour définir les Listes d'accès l'IPS configuré sur les plusieurs masques de sous-réseau.

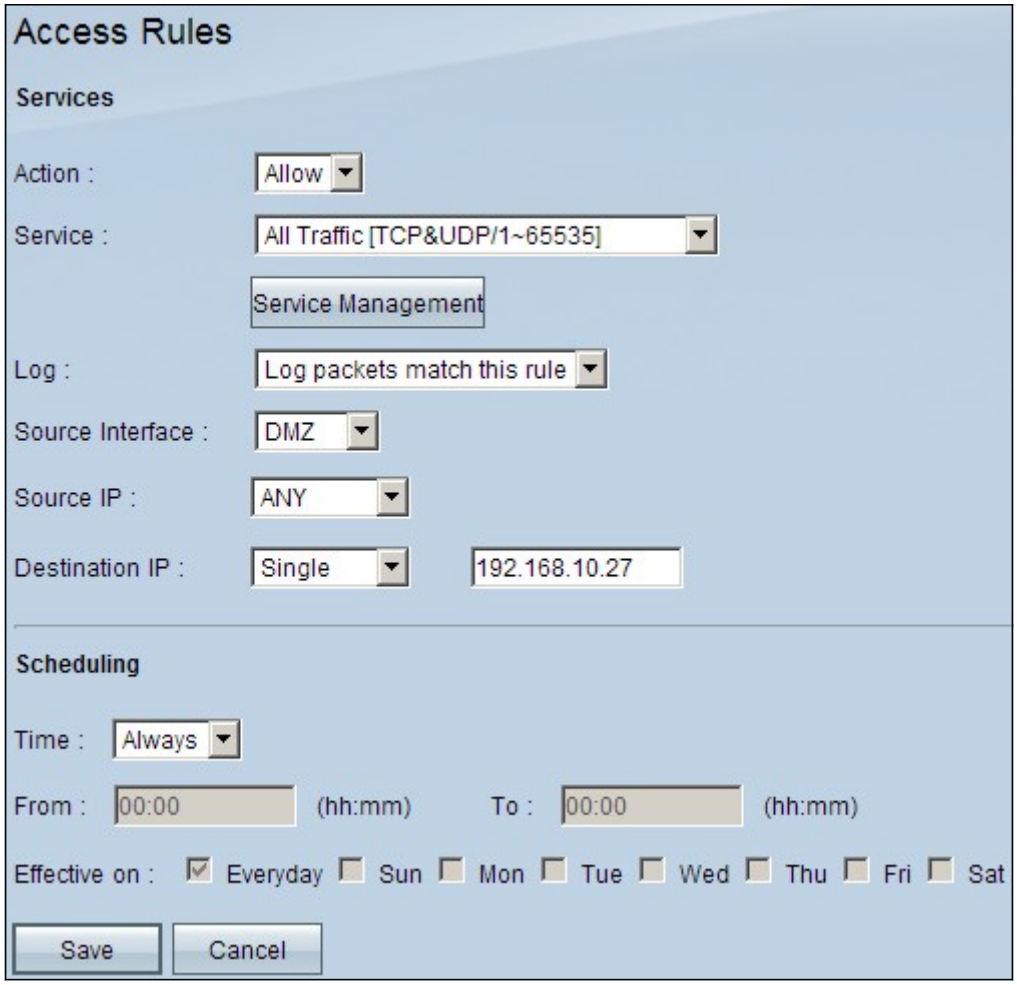
Étape 1. Connectez-vous dans la page d'utilitaire de configuration de routeur et choisissez le **Pare-feu > les règles d'accès**. La page de *règles d'accès* s'ouvre :




**Remarque:** Les règles d'accès par défaut ne peuvent pas être éditées.

Étape 2. Cliquez sur le bouton d'**ajouter** pour ajouter une nouvelle règle d'accès. La page de *règles d'accès* change pour afficher les services et les régions de Scheduling.

**Remarque:** Cette configuration peut être faite pour l'ipv4 et l'IPv6 en sélectionnant ces onglets respectifs à la page de *règles d'accès*. Les étapes de configuration spécifiques à l'ipv4 et à l'IPv6 sont mentionnées dans les étapes suivantes.




Étape 3. Choisissez **autorisent de la** liste déroulante d'action à permettre le le service.

Étape 4. Choisissez **tout le trafic [TCP&UDP/1~65535] de la** liste déroulante de service pour activer tous les services pour le DMZ.

Étape 5. Choisissez les **paquets de log qui apparient cette règle de la** liste déroulante de log de choisir seulement les logs qui apparient la règle d'accès.

Étape 6. Choisissez **DMZ de la** liste déroulante d'interface de source qui est la source pour les règles d'accès.

Étape 7. En choisissez de la liste déroulante de source ip.

Étape 8. Choisissez les options disponibles suivantes l'unes des de la liste déroulante IP de destination.

- Simple — Choisissez simple de s'appliquer cette règle à une adresse IP simple.

- Plage — Choisissez la plage pour s'appliquer cette règle à une plage des adresses IP. Écrivez la première et dernière adresse IP de la plage. Cette option est disponible seulement dans l'ipv4.

- Sous-réseau — Choisissez le sous-réseau pour appliquer ceci ordonne à un sous-réseau. Introduisez l'adresse IP et le nombre de notation CIDR qui est utilisé pour allouer des adresses IP et des paquets d'Internet Protocol de routage pour le sous-réseau. Cette option est disponible seulement dans l'IPv6.

- Quels — En choisissez pour s'appliquer la règle à l'adresse IP l'une des.

**Timesaver :** Ignorez à l'étape 10 si vous configurez des règles d'accès d'IPv6.

Étape 9. Choisissez une méthode pour définir quand les règles sont en activité de la liste déroulante de temps. Elles sont :

- Toujours — Si vous choisissez toujours de la liste déroulante de temps, les règles d'accès seront toujours appliquées de trafiquer.

- Intervalle — Vous pouvez choisir un intervalle heure précise auquel les règles d'accès sont en activité si vous sélectionnez l'intervalle de la liste déroulante de temps. Après que vous spécifiiez l'intervalle de temps, choisissez les jours où vous voulez les règles d'accès d'être en activité de l'efficace sur des cases.

Étape 10. **Sauvegarde de** clic pour sauvegarder vos configurations.


Étape 11. Cliquez sur l'icône d'**éditer** pour éditer la règle d'accès créée.

Étape 12. Cliquez sur l'icône d'**effacement** pour supprimer la règle d'accès créée.