Vérification de l'état VPN sur les routeurs VPN RV016 RV042 RV042G et RV082

Objectif

Un réseau privé virtuel (VPN) est une connexion sécurisée entre deux points d'extrémité. Le VPN crée un tunnel sécurisé entre ces deux points d'extrémité et assure la sécurité du trafic de données le long du tunnel. Un réseau privé virtuel (VPN) est une connexion sécurisée établie au sein d'un réseau ou entre des réseaux. Pour que ce tunnel fonctionne correctement, la configuration VPN des deux côtés de la connexion doit être effectuée avec soin et certaines informations doivent correspondre. L'objectif de ce document est d'expliquer comment vérifier l'état VPN sur les routeurs VPN RV016, RV042, RV042G et RV082. Les VPN servent à isoler le trafic entre les hôtes et les réseaux spécifiés du trafic des hôtes et des réseaux non autorisés.

Périphériques pertinents

â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Version du logiciel

â€¢4.2.1.02

Paramètres VPN courants à vérifier

Pour qu'une connexion VPN fonctionne correctement, les deux extrémités de la connexion doivent répondre aux mêmes exigences. En cas de défaillance de la connexion VPN, vous pouvez vérifier deux éléments susceptibles de faire la différence. Ces scénarios sont les suivants :

· L'adresse IP locale est en conflit entre les deux points d'extrémité VPN.

· Il existe des différences dans les paramètres de cryptage et d'authentification des deux points d'extrémité.

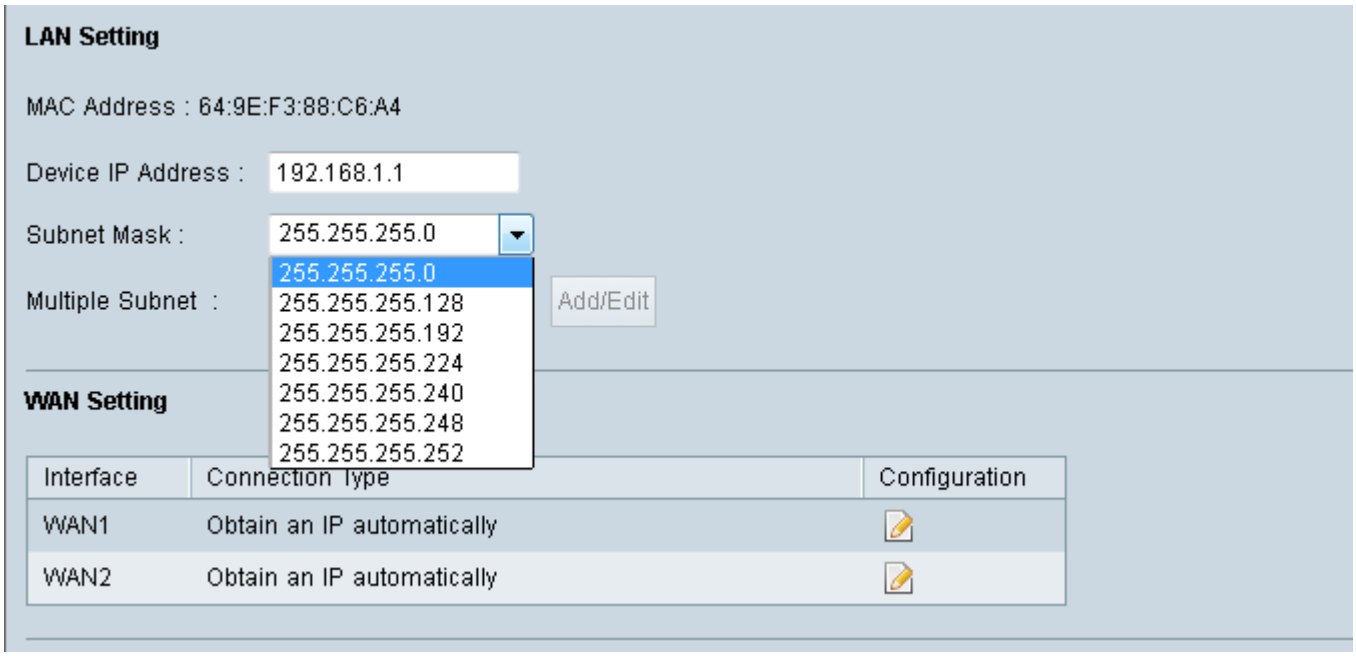
La section suivante explique comment vérifier le schéma d'adresses IP d'un VPN et comment effectuer les modifications appropriées.

Modifier l'adresse IP LAN du routeur

L'interface LAN des deux extrémités de la connexion VPN doit faire partie d'une adresse réseau différente. Si les deux parties appartiennent à la même adresse réseau, la connexion VPN ne fonctionnera pas. Les étapes suivantes expliquent comment apporter des modifications à votre adresse IP LAN sur les routeurs VPN RV042, RV042G et RV082.

Étape 1. Connectez-vous à l'utilitaire Web de configuration et choisissez **Setup > Network**. La page *Réseau* s'ouvre :

Étape 2. Sous LAN Setting, dans le champ Device IP Address, entrez une adresse IP qui appartient à une adresse réseau différente de l'autre extrémité de la connexion VPN.



Étape 3. Dans la liste déroulante Subnet Mask, sélectionnez le masque de sous-réseau approprié pour votre connexion VPN.

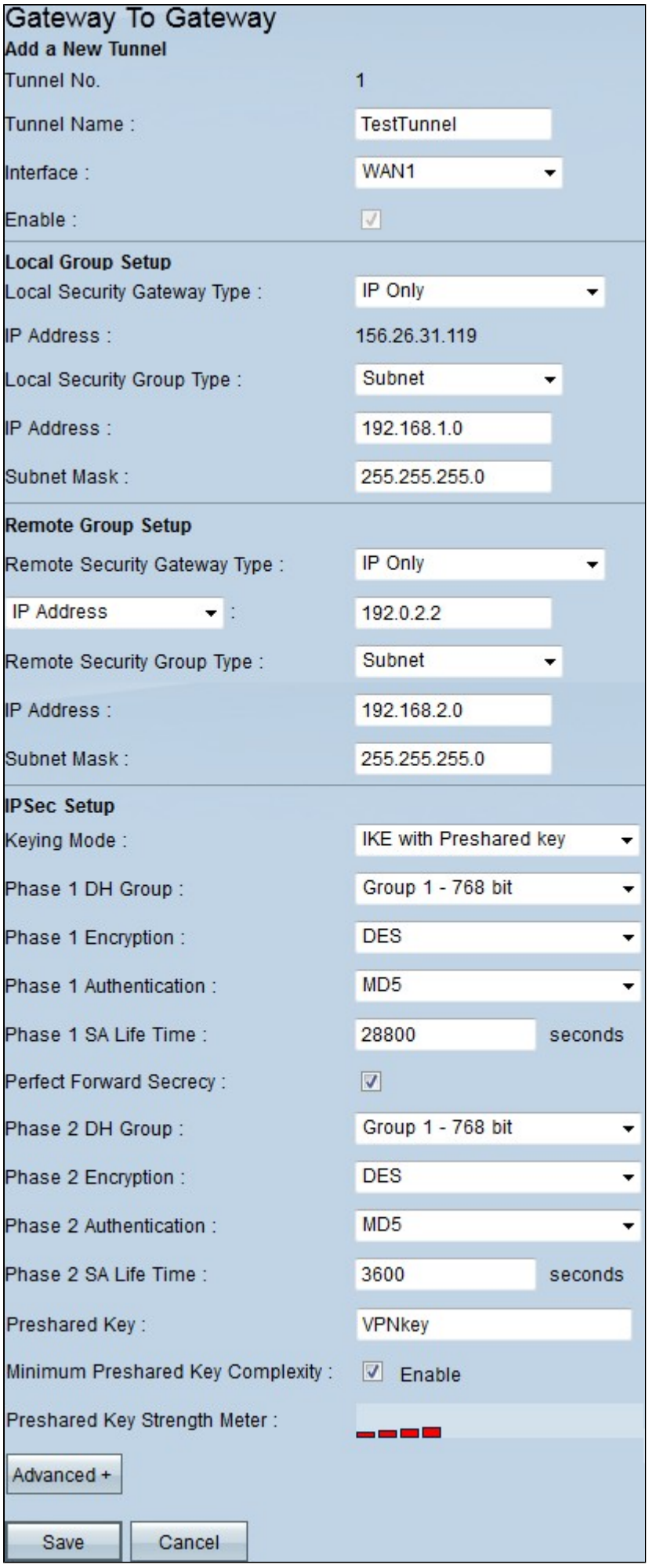
Étape 4. (Facultatif) Pour activer lâ€™utilisation de plusieurs sous-réseaux, dans le champ Multiple Subnet, cochez la case Enable.

Étape 5. Cliquez sur **Save** pour appliquer vos nouveaux paramètres.

Vérifiez les paramètres de sécurité de la connexion VPN

La configuration de sécurité de la connexion VPN doit être identique à chaque extrémité de la connexion. La procédure suivante explique comment vérifier ces paramètres sur les routeurs VPN RV042, RV042G et RV082.

Étape 1. Connectez-vous à l'utilitaire de configuration basé sur le Web et choisissez **VPN** > Gateway to Gateway. La page *Gateway to Gateway* s'ouvre.


Gateway To Gateway
Add a New Tunnel
Tunnel No.
1
Tunnel Name :
TestTunnel
Interface :
WAN1
Enable :
Local Group Setup
Local Security Gateway Type :
IP Only
IP Address :
156.26.31.119
Local Security Group Type :
Subnet
IP Address :
192.168.1.0
Subnet Mask :
255.255.255.0
Remote Group Setup
Remote Security Gateway Type :
IP Only
IP Address :
192.0.2.2
Remote Security Group Type :
Subnet
IP Address :
192.168.2.0
Subnet Mask :
255.255.255.0
IPSec Setup
Keying Mode :
IKE with Preshared key
Phase 1 DH Group :
Group 1 - 768 bit
Phase 1 Encryption :
DES
Phase 1 Authentication :
MD5
Phase 1 SA Life Time :
28800
seconds
Perfect Forward Secrecy :
Phase 2 DH Group :
Group 1 - 768 bit
Phase 2 Encryption :
DES
Phase 2 Authentication :
MD5
Phase 2 SA Life Time :
3600
seconds
Preshared Key :
VPNkey
Minimum Preshared Key Complexity :
Enable
Preshared Key Strength Meter :
Advanced +
Save
Cancel

Étape 2. Vérifiez les paramètres suivants. Assurez-vous que les deux extrémités de la connexion VPN ont les mêmes paramètres :

· Le type de groupe de sécurité local est identique au segment LAN du routeur local.

· Le type de groupe de sécurité distant est identique au segment LAN du routeur distant.

· Remote Security Gateway Type (Type de passerelle de sécurité distante) : adresse IP WAN/Internet du routeur distant.

· Les champs de configuration IPSec doivent correspondre des deux côtés du tunnel VPN.

· La clé pré-partagée doit être identique des deux côtés du tunnel VPN.

Étape 3. (Facultatif) Cliquez sur **Avancé+** pour afficher plus de propriétés de sécurité. Comme précédemment, ces paramètres doivent être identiques des deux côtés de la connexion.

Étape 4. Cliquez sur **Save** pour appliquer les nouveaux paramètres si quelque chose a été modifié.

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.