Configuration sur le tunnel VPN passerelle à passerelle à l'aide de DynDNS sur un côté du tunnel sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectifs

Un système DDNS (Dynamic Domain Name System) permet l'accès Internet au serveur à l'aide d'un nom de domaine plutôt que d'une adresse IP. Le service DDNS conserve également les informations d'adresse IP même lorsque le client reçoit une affectation IP dynamique soumise à des modifications constantes par le FAI. Avec cette configuration, le serveur est toujours disponible quelle que soit l'adresse IP. Ce service n'est utilisable qu'après avoir établi un compte auprès d'un fournisseur de services DDNS.

L'objectif de ce document est d'expliquer comment configurer un VPN passerelle à passerelle à l'aide de DynDNS côté groupe local, et d'IP statique avec un nom de domaine enregistré côté groupe distant pour les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

- RV016
- RV042
- RV042G
- RV082

Version du logiciel

- 4.2.2.08

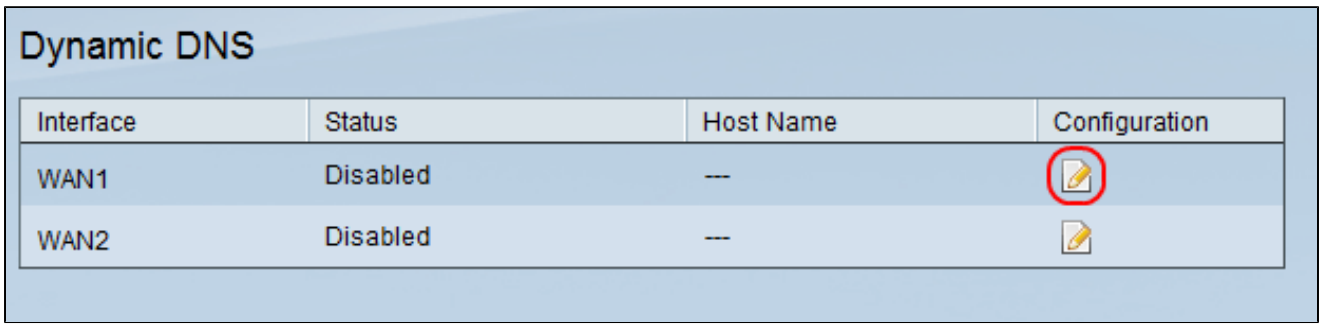
Configuration du tunnel VPN

Configurer DDNS

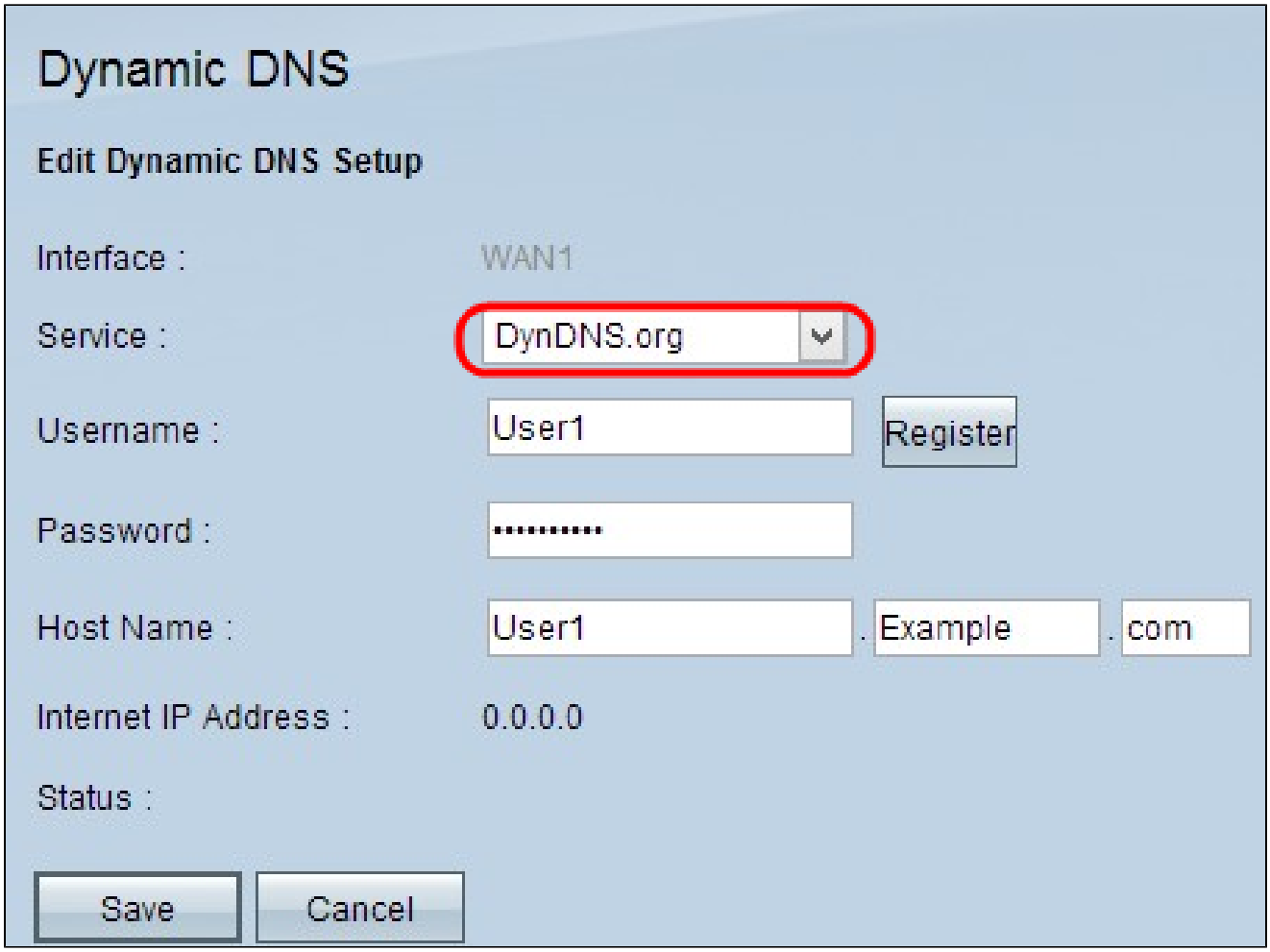
Étape 1. Visitez www.dyndns.org et enregistrez un nom de domaine.

Étape 2. Connectez-vous à l'utilitaire de configuration du routeur et choisissez Setup > Dynamic DNS. La page Dynamic DNS s'ouvre.

Étape 3. Cliquez sur l'icône Edit pour WAN1.



La page Edit Dynamic DNS Setup s'ouvre :



Étape 4. Sélectionnez DynDNS.org dans la liste déroulante Service.

Étape 5. Dans le champ Username, saisissez vos informations de nom d'utilisateur de compte DynDNS.org.

Étape 6. Dans le champ Password, saisissez le mot de passe correspondant au nom d'utilisateur enregistré sur DynDNS.org

Étape 7. Saisissez votre nom d'hôte dans le champ Host Name.

Remarque : les deux champs restants de la page Edit Dynamic DNS Setup affichent des informations et ne sont pas configurables :

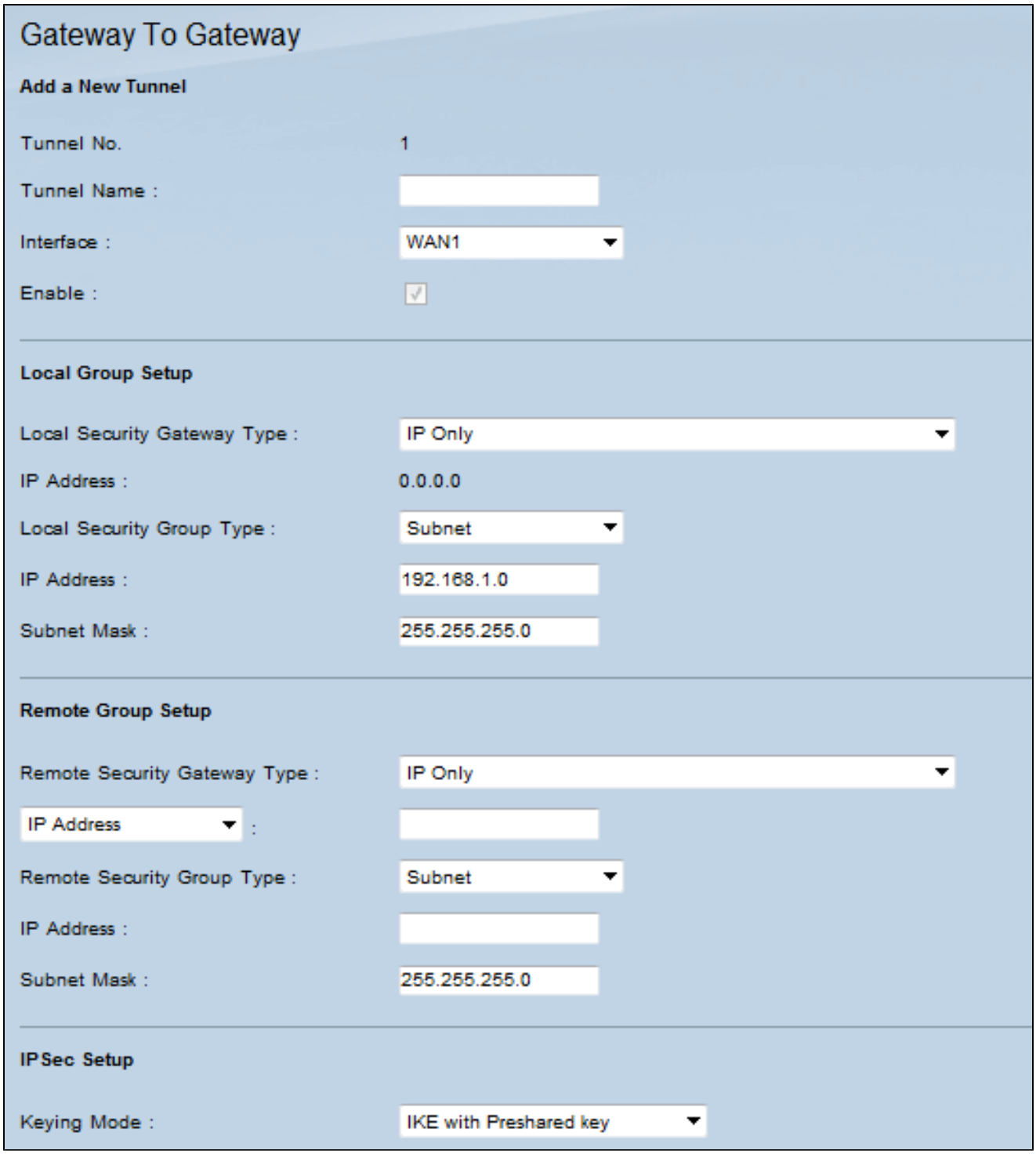
· Internet IP Address : affiche l'adresse IP du routeur. Cette adresse va changer car elle est dynamique.

· Status : affiche l'état du DDNS. En cas d'erreur, vérifiez que vous avez correctement saisi les informations DDNS.

Étape 8. Cliquez sur Save.

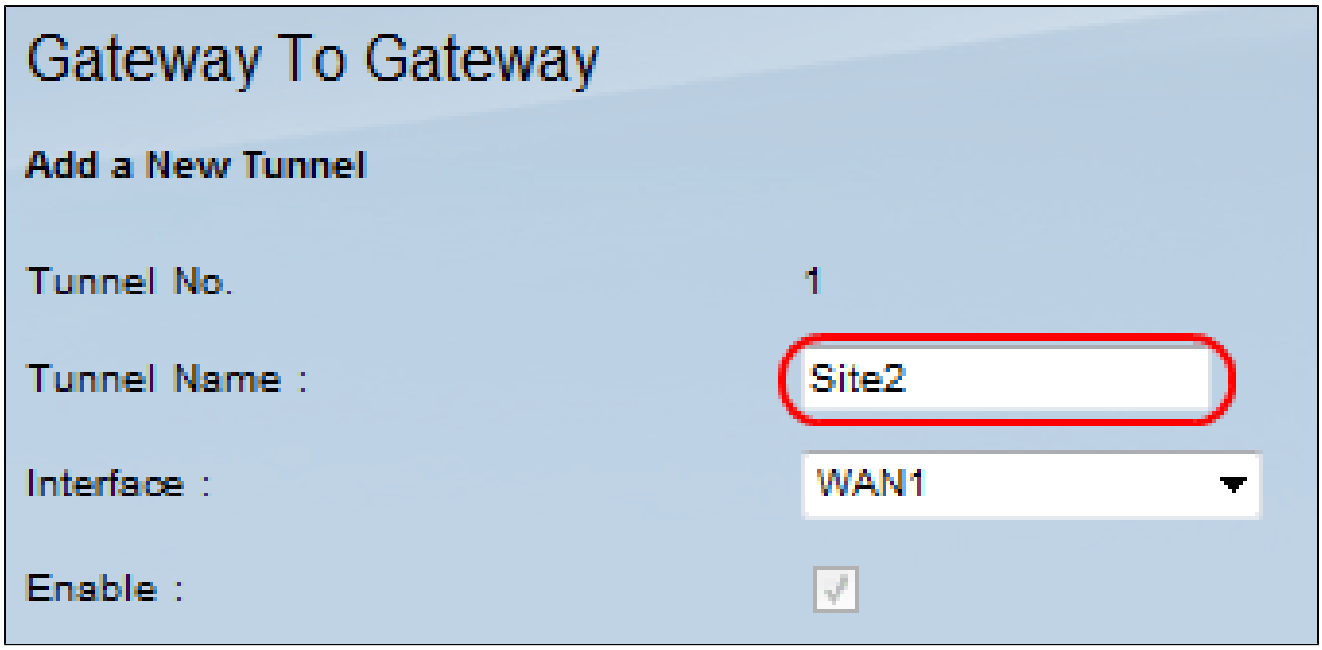
Configuration du tunnel VPN du site 1 au site 2

Étape 9. Connectez-vous à l'utilitaire de configuration du routeur et choisissez VPN > Gateway to Gateway. La page Gateway to Gateway s'ouvre :



Remarque : avant de quitter cette page, cliquez sur Enregistrer pour enregistrer les paramètres ou sur Annuler pour les annuler.

Étape 10. Dans le champ Tunnel Name, entrez un nom pour le tunnel VPN entre le site 1 et le site 2.

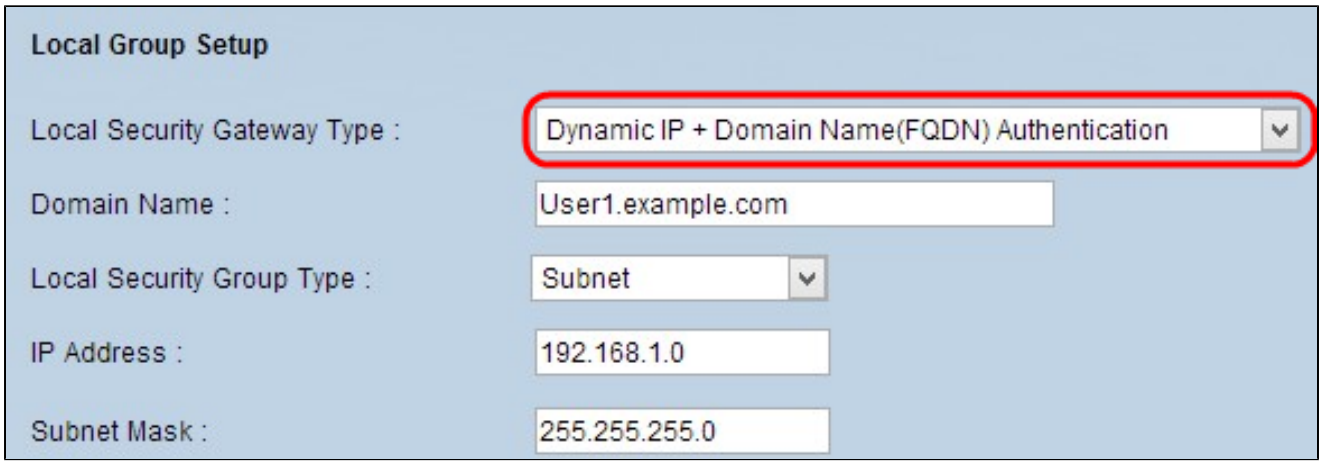


Remarque : le nom du tunnel n'est fourni qu'à titre de référence et ne doit pas nécessairement correspondre au nom utilisé à l'autre extrémité du tunnel VPN.

Étape 11. Choisissez le port WAN à utiliser pour ce tunnel dans la liste déroulante Interface.

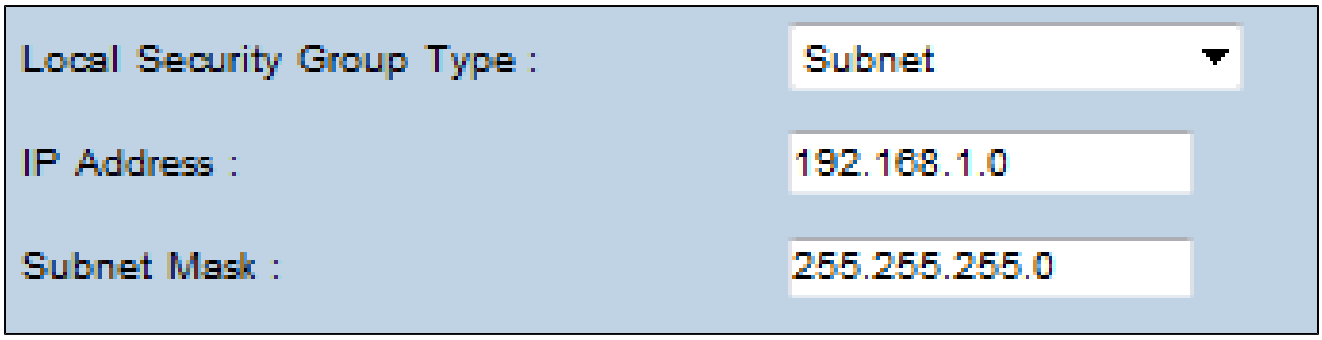
Étape 12. Cochez Enable pour activer le tunnel VPN. La case à cocher sera désactivée une fois le tunnel VPN créé.

Étape 13. Dans la zone Local Group Setup, choisissez Dynamic IP + Domain Name (FQDN) Authentication dans la liste déroulante Local Security Gateway Type.



Étape 14. Dans le champ Domain Name, saisissez le nom de domaine DynDNS enregistré.

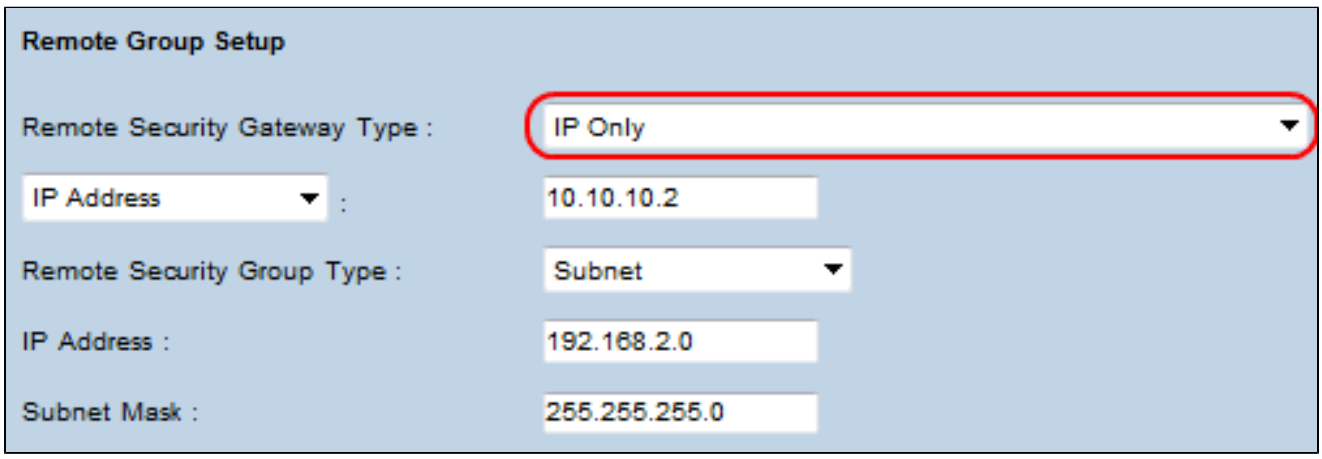
Étape 15. Choisissez Subnet dans la liste déroulante Local Security Group Type. Le type de groupe de sécurité local définit quelles ressources LAN peuvent utiliser le tunnel VPN.



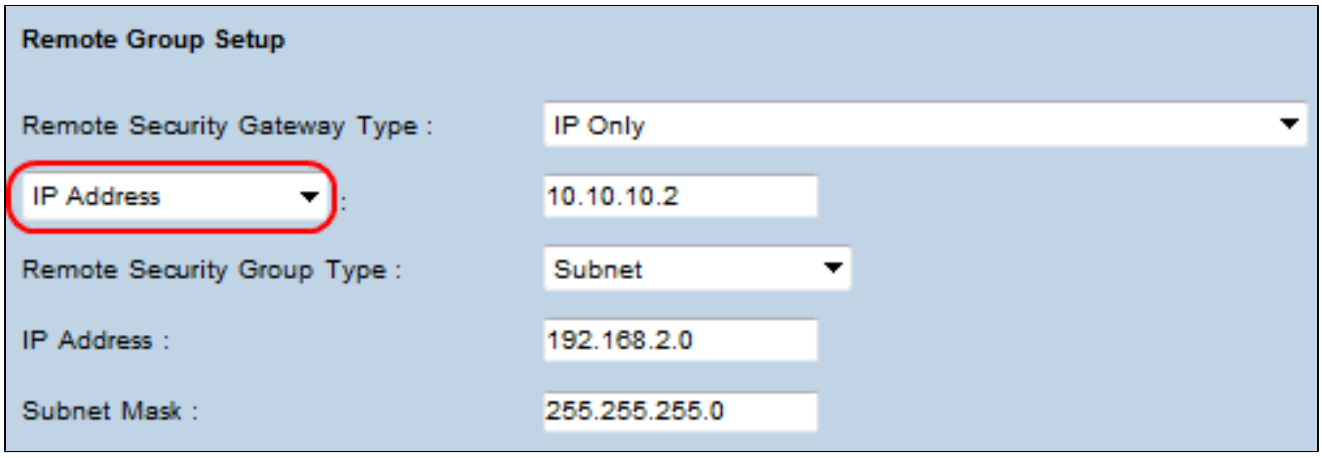
Étape 16. Saisissez l'adresse IP dans le champ IP Address.

Étape 17. Saisissez le masque de sous-réseau dans le champ Subnet Mask.

Étape 18. Dans la zone Remote Group Setup, choisissez IP Only dans la liste déroulante Remote Security Gateway Type.

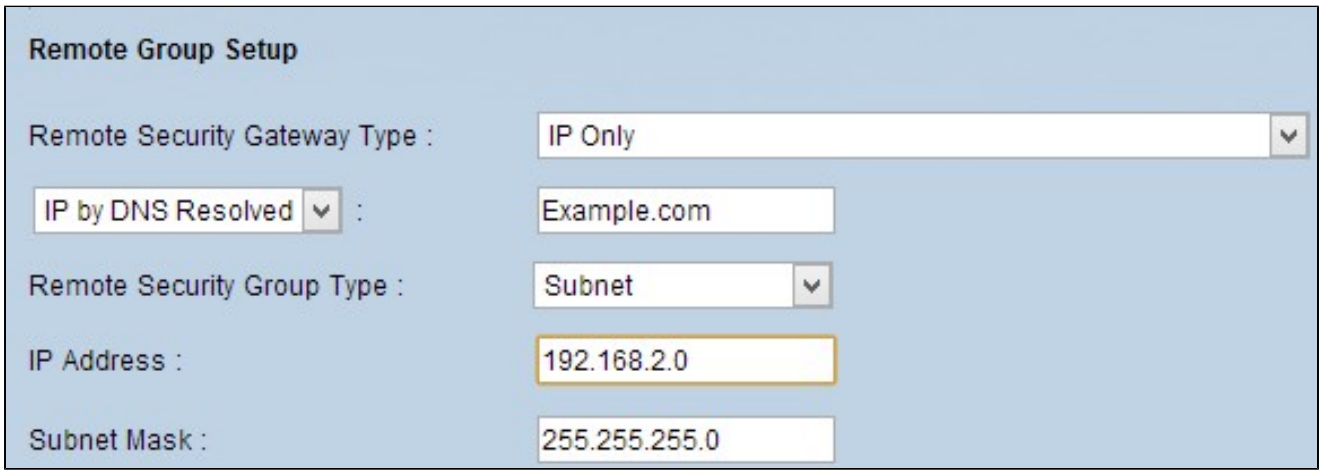


Étape 19. Choisissez IP by DNS Resolved dans la liste déroulante suivante pour spécifier un périphérique.



Étape 20. Après avoir sélectionné IP by DNS Resolved dans la liste déroulante, entrez le

nom de domaine enregistré du routeur dans le champ en regard de celui-ci.

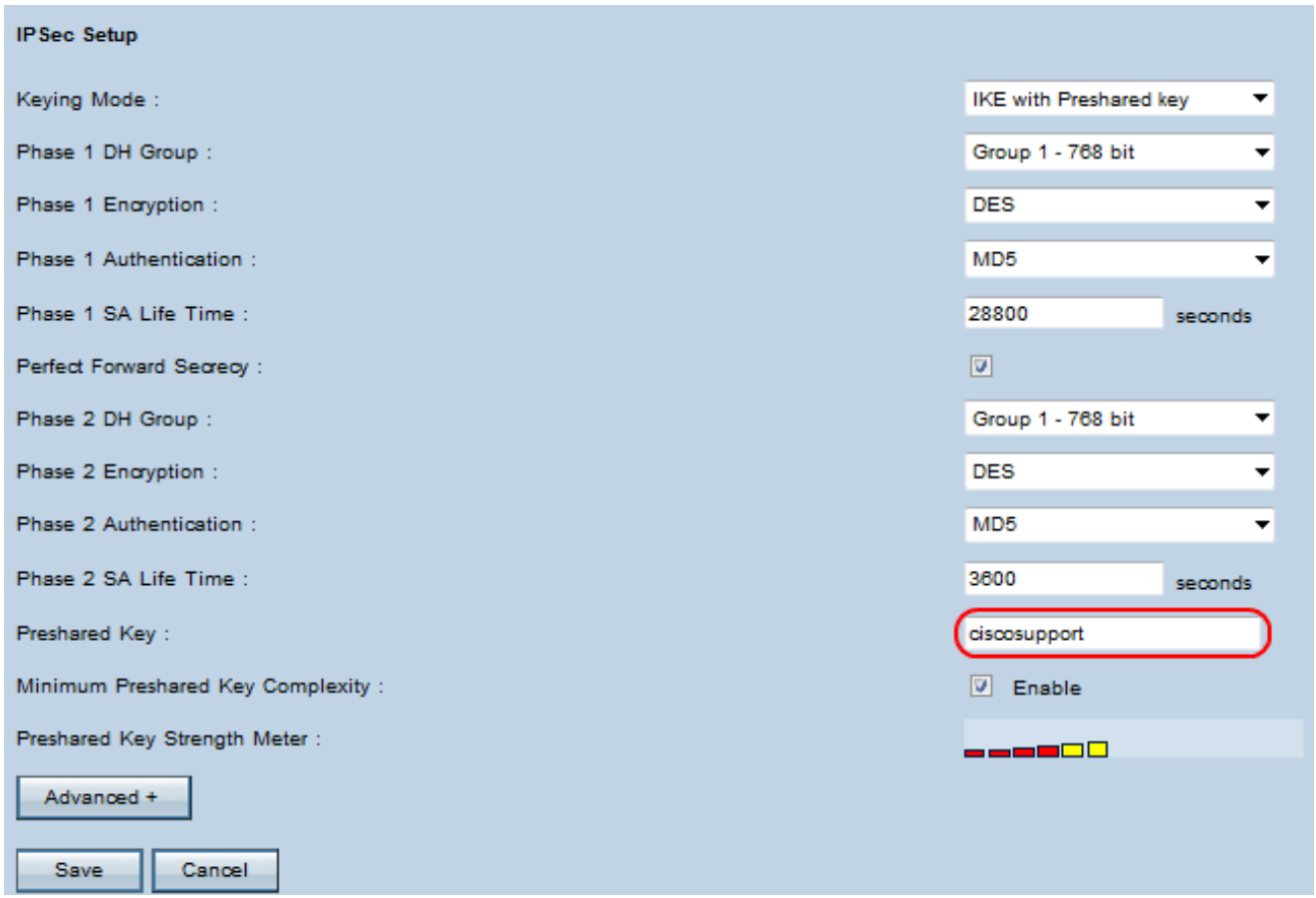


Étape 21. Choisissez Subnet dans la liste déroulante Remote Security Group Type. Le type de groupe de sécurité distant spécifie quelles ressources du réseau local distant peuvent accéder au tunnel VPN.

Étape 22. Saisissez l'adresse IP du sous-réseau dans le champ IP Address.

Étape 23. Saisissez le masque de sous-réseau dans le champ Subnet Mask.

Étape 24. Dans la zone IP Sec Setup, recherchez le champ Preshared Key, et entrez une clé pré-partagée à utiliser pour authentifier l'homologue IKE distant. Vous pouvez saisir jusqu'à 30 caractères de clavier et valeurs hexadécimales. Les deux extrémités du tunnel VPN doivent utiliser la même clé prépartagée. Les autres champs de la zone IPSec Setup peuvent utiliser des valeurs par défaut.



Étape 25. Cliquez sur Save pour enregistrer les modifications.

Remarque : configurez l'autre routeur en suivant les étapes 9 à 25 avec la configuration de Local Group Setup et de Remote Group Setup commutée. La configuration effectuée dans la zone Local Group Setup pour le premier routeur sera la configuration dans la zone Remote Group Setup sur le second routeur.

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.