Configuration de la connexion VPN client-à-site sur le routeur de la gamme RV34x

Objectif

Dans une connexion de réseau privé virtuel (VPN) client-à-site, les clients d'Internet peuvent se connecter au serveur pour accéder au réseau d'entreprise ou au réseau local (LAN) derrière le serveur, tout en conservant la sécurité du réseau et de ses ressources. Cette fonctionnalité est très utile car elle crée un nouveau tunnel VPN qui permettrait aux télétravailleurs et aux voyageurs d'affaires d'accéder à votre réseau en utilisant un logiciel client VPN sans compromettre la confidentialité et la sécurité.

L'objectif de ce document est de vous montrer comment configurer la connexion VPN client à site sur le routeur de la gamme RV34x.

Périphériques pertinents

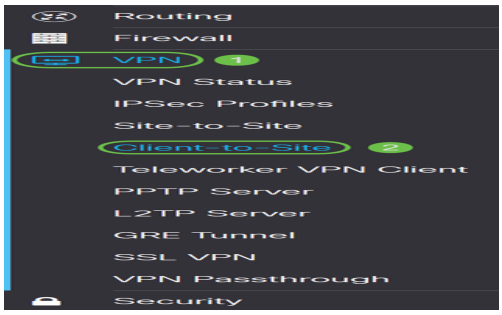
- Gamme RV34x

Version du logiciel

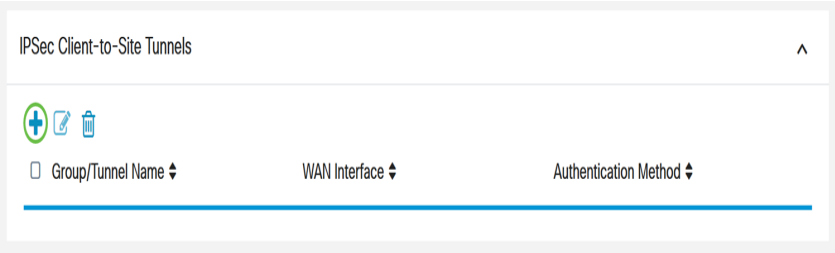
- 1.0.01.16

Configuration du VPN client à site

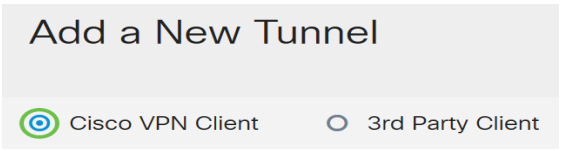
Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **VPN > Client-to-Site**.



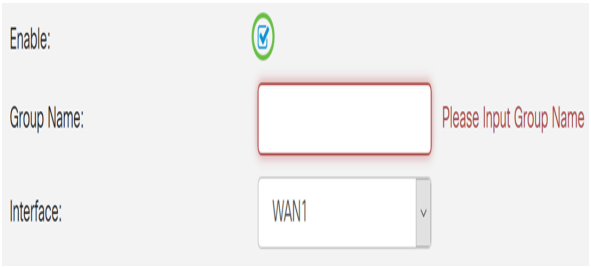
Étape 2. Cliquez sur le bouton **Add** sous la section IPSec Client-to-Site Tunnels.



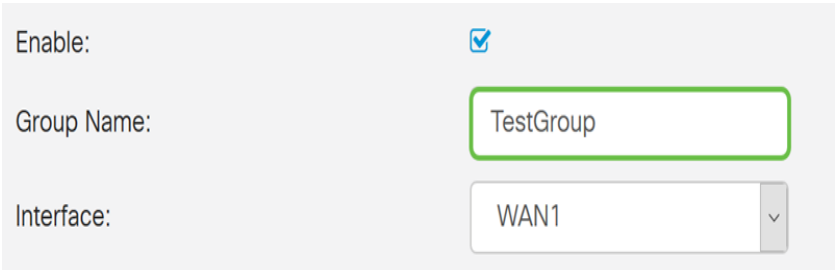
Étape 3. Dans la zone *Ajouter un nouveau tunnel*, cliquez sur la case d'option **Client VPN Cisco**.



Étape 4. Cochez la case **Activer** pour activer la configuration.



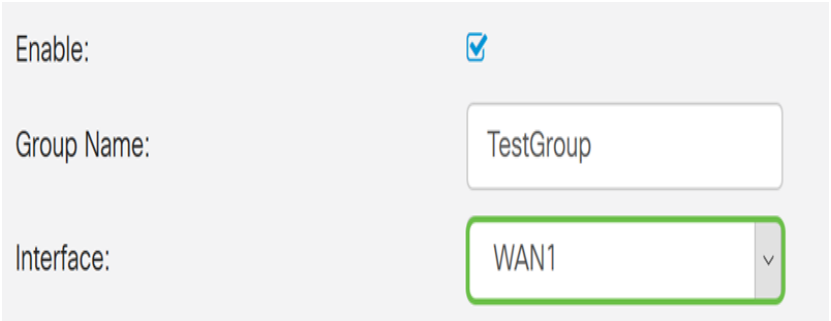
Étape 5. Entrez un nom de groupe dans le champ fourni. Cela servira d'identificateur pour tous les membres de ce groupe lors des négociations IKE (Internet Key Exchange).



Note: Entrez des caractères compris entre A et Z ou entre 0 et 9. Les espaces et les caractères spéciaux ne sont pas autorisés pour le nom du groupe. Dans cet exemple, TestGroup est utilisé.

Étape 6. Cliquez sur la liste déroulante pour choisir l'interface. Les options sont les suivantes :

- WAN1
- WAN2
- USB1
- USB2



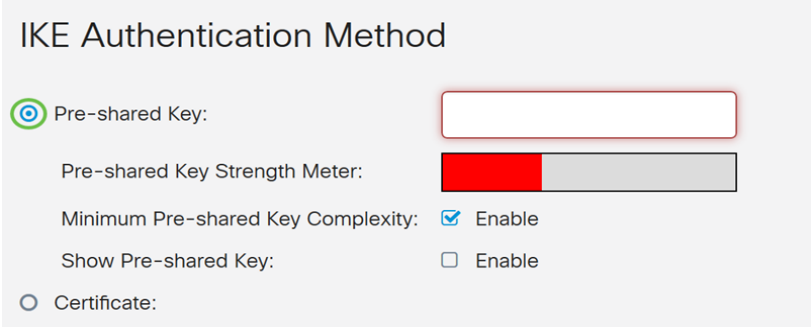
Note: Dans cet exemple, WAN1 est choisi. Voici la configuration par défaut .

Étape 7. Dans la zone IKE Authentication Method, choisissez une méthode d'authentification à utiliser dans les négociations IKE dans le tunnel basé sur IKE. Les options sont les suivantes :

- Pre-shared Key : les homologues IKE s'authentifient mutuellement en calculant et en envoyant un hachage de données comportant la clé Pre-shared Key. Si l'homologue

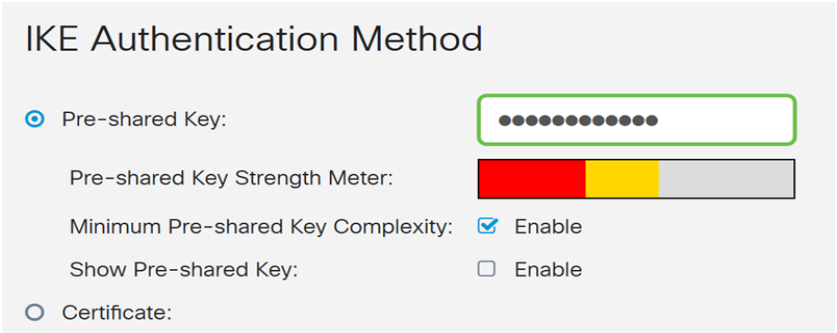
récepteur est capable de créer le même hachage indépendamment à l'aide de sa clé pré-partagée, il sait que les deux homologues doivent partager le même secret, authentifiant ainsi l'autre homologue. Les clés pré-partagées ne s'adaptent pas correctement, car chaque homologue IPSec doit être configuré avec la clé pré-partagée de tous les autres homologues avec lesquels il établit une session.

- Certificat — Le certificat numérique est un package qui contient des informations telles qu'une identité de certificat du porteur : nom ou adresse IP, date d'expiration du numéro de série du certificat et copie de la clé publique du titulaire du certificat. Le format de certificat numérique standard est défini dans la spécification X.509. X.509 version 3 définit la structure de données des certificats.



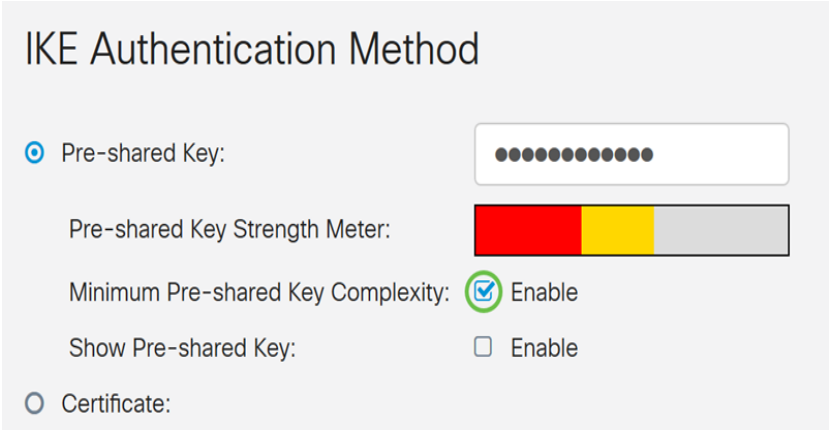
Note: Dans cet exemple, la clé pré-partagée est choisie. Voici la configuration par défaut .

Étape 8. Saisissez une clé pré-partagée dans le champ fourni. Il s'agit de la clé d'authentification de votre groupe d'homologues IKE.

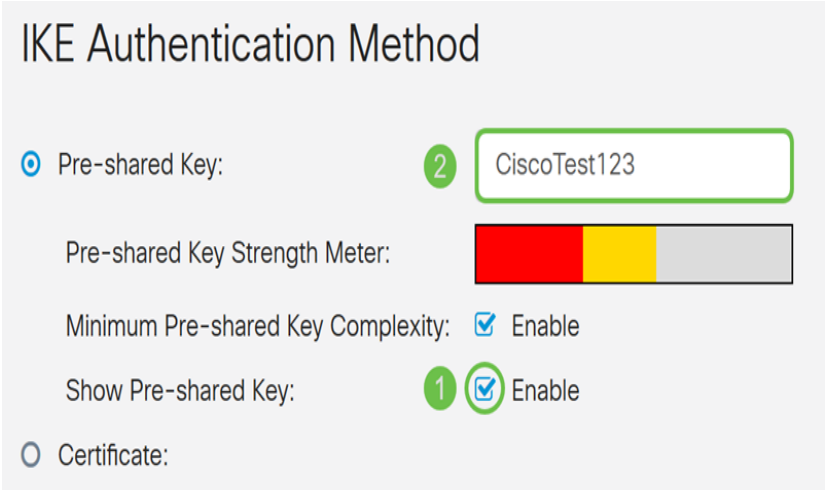


Étape 9. (Facultatif) Cochez la case **Activer** pour la Complexité de clé pré-partagée minimale afin d'afficher le compteur de force de clé pré-partagée et de déterminer la force de votre clé. La force de votre clé est définie comme suit :

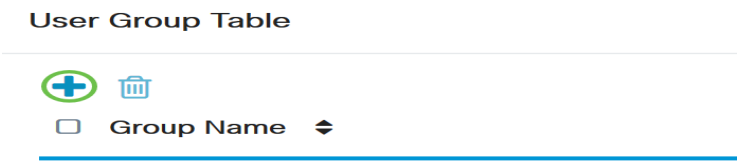
- Rouge : le mot de passe est faible.
- Orange : le mot de passe est assez fort.
- Vert : le mot de passe est fort.



Note: Vous pouvez cocher la case **Activer** dans le champ *Afficher la clé prépartagée* pour vérifier votre mot de passe en texte clair.

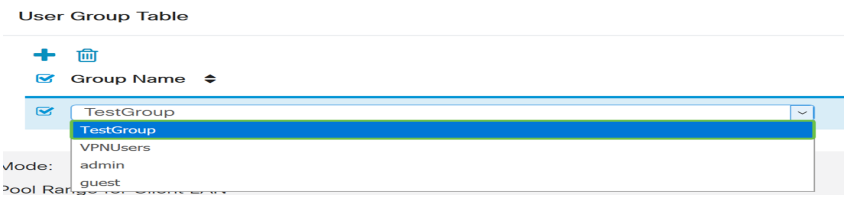


Étape 10. (Facultatif) Cliquez sur l'icône **plus** dans le tableau Groupe d'utilisateurs pour ajouter un groupe.



Étape 11. (Facultatif) Choisissez dans la liste déroulante si le groupe d'utilisateurs est réservé à l'administrateur ou aux invités. Si vous avez créé votre propre groupe d'utilisateurs avec des comptes d'utilisateurs, vous pouvez le sélectionner. Dans cet exemple, nous allons sélectionner TestGroup.

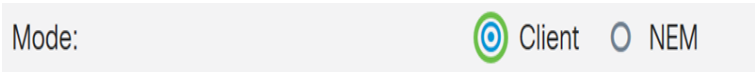
Note: TestGroup est un groupe d'utilisateurs que nous avons créé dans **Configuration système > Groupes d'utilisateurs**.



Note: Dans cet exemple, TestGroup est sélectionné. Vous pouvez également cocher la case en regard du groupe d'utilisateurs, puis cliquer sur le bouton **Supprimer** si vous voulez supprimer un groupe d'utilisateurs.

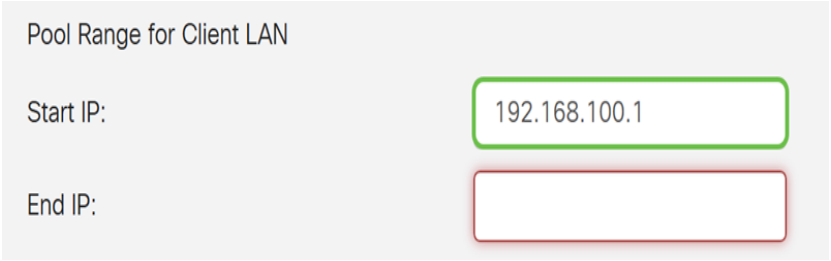
Étape 12. Cliquez sur une case d'option pour choisir un mode. Les options sont les suivantes :

- Client : cette option permet au client de demander une adresse IP et le serveur fournit les adresses IP de la plage d'adresses configurée.
- Network Extension Mode (NEM) : cette option permet aux clients de proposer leur sous-réseau pour lequel les services VPN doivent être appliqués sur le trafic entre le LAN derrière le serveur et le sous-réseau proposé par le client.



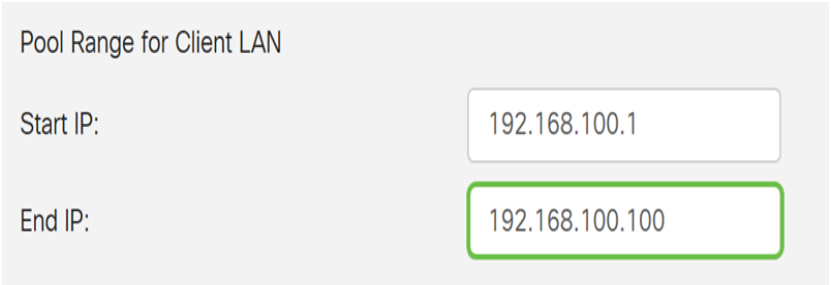
Note: Dans cet exemple, Client est sélectionné.

Étape 13. Entrez l'adresse IP de début dans le champ *Start IP*. Il s'agit de la première adresse IP du pool pouvant être attribuée à un client.



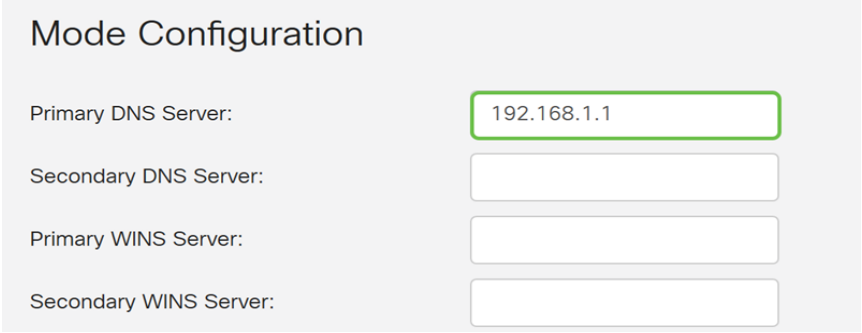
Note: Dans cet exemple, 192.168.100.1 est utilisé.

Étape 14. Entrez l'adresse IP de fin dans le champ *End IP*. Il s'agit de la dernière adresse IP du pool pouvant être attribuée à un client.



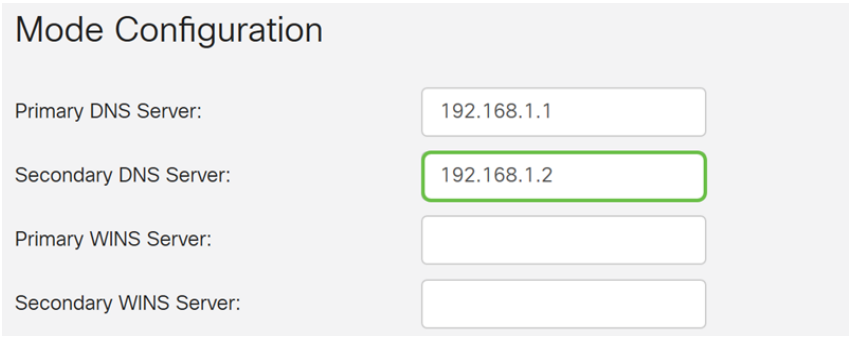
Note: Dans cet exemple, 192.168.100.100 est utilisé.

Étape 15. (Facultatif) Dans la zone *Configuration du mode*, saisissez l'adresse IP du serveur DNS principal dans le champ prévu à cet effet.



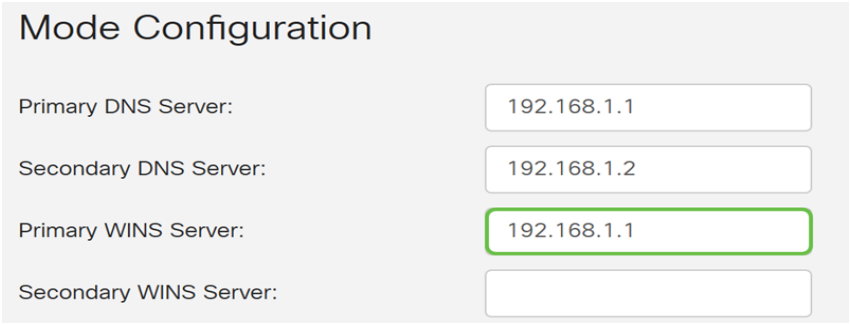
Note: Dans cet exemple, 192.168.1.1 est utilisé.

Étape 16. (Facultatif) Saisissez l'adresse IP du serveur DNS secondaire dans le champ fourni.



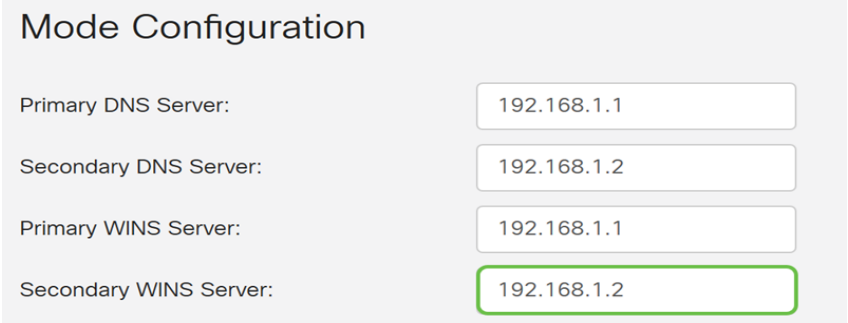
Note: Dans cet exemple, 192.168.1.2 est utilisé.

Étape 17. (Facultatif) Saisissez l'adresse IP du serveur WINS principal dans le champ fourni.



Note: Dans cet exemple, 192.168.1.1 est utilisé.

Étape 18. (Facultatif) Saisissez l'adresse IP du serveur WINS secondaire dans le champ fourni.



Note: Dans cet exemple, 192.168.1.2 est utilisé.

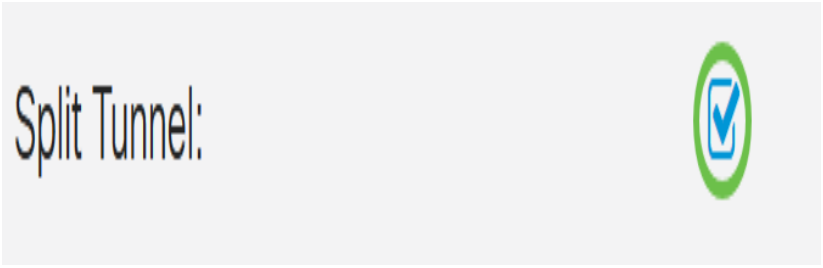
Étape 19. (Facultatif) Saisissez le domaine par défaut à utiliser dans le réseau distant dans le champ prévu à cet effet.

Note: Dans cet exemple, sample.com est utilisé.

Étape 20. (Facultatif) Dans le champ *Backup Server 1*, saisissez l'adresse IP ou le nom de domaine du serveur de sauvegarde. C'est là que le périphérique peut démarrer la connexion VPN en cas de défaillance du serveur VPN IPSec principal. Vous pouvez saisir jusqu'à trois serveurs de sauvegarde dans les champs fournis. Le serveur de sauvegarde 1 a la priorité la plus élevée parmi les trois serveurs et le serveur de sauvegarde 3 la plus faible.

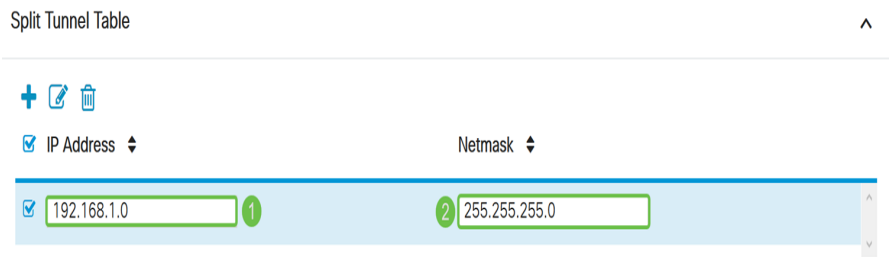
Note: Dans cet exemple, Example.com est utilisé pour Backup Server 1.

Étape 21. (Facultatif) Cochez la case **Tunnel fractionné** pour activer le tunnel fractionné. La transmission tunnel partagée vous permet d'accéder simultanément aux ressources d'un réseau privé et d'Internet.



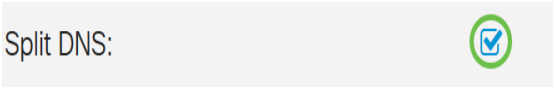
Étape 22. (Facultatif) Sous la *table Fractionner le tunnel*, cliquez sur l'icône **plus** pour ajouter une adresse IP pour le tunnel partagé.

Étape 23. (Facultatif) Saisissez l'adresse IP et le masque de réseau du tunnel partagé dans les champs fournis.

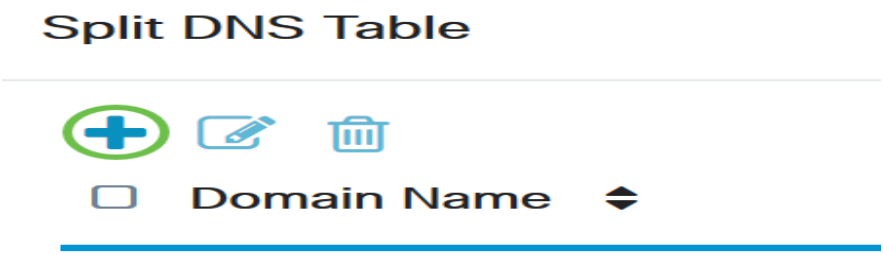


Note: Dans cet exemple, 192.168.1.0 et 255.255.255.0 sont utilisés. Vous pouvez également cocher cette case et cliquer sur les boutons **Ajouter**, **Modifier** et **Supprimer** pour ajouter, modifier ou supprimer un tunnel partagé, respectivement.

Étape 24. (Facultatif) Cochez la case **Split DNS** pour activer le DNS partagé. Split DNS vous permet de créer des serveurs DNS distincts pour les réseaux internes et externes afin de préserver la sécurité et la confidentialité des ressources réseau.



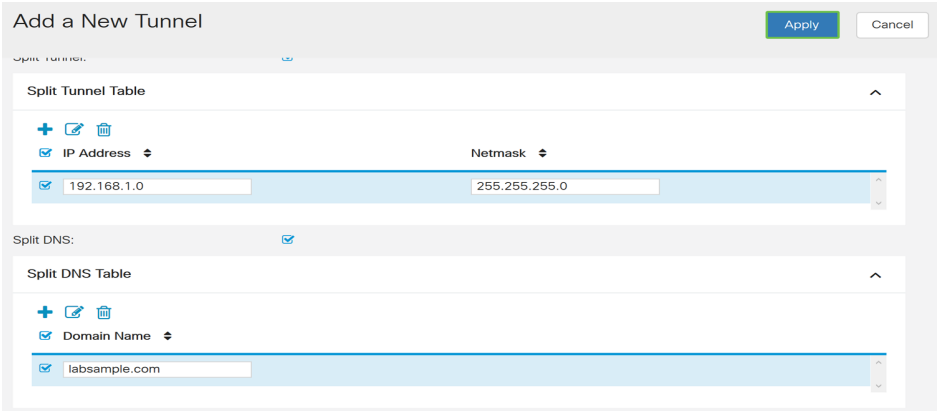
Étape 25. (Facultatif) Cliquez sur l'icône **plus** sous la *table DNS fractionnée* pour ajouter un nom de domaine pour DNS fractionné.



Étape 26. (Facultatif) Entrez le nom de domaine du DNS fractionné dans le champ fourni.

Note: Dans cet exemple, labsample.com est utilisé. Vous pouvez également cocher cette case et cliquer sur les boutons **Ajouter**, **Modifier** et **Supprimer** pour ajouter, modifier ou supprimer un DNS fractionné, respectivement.

Étape 27. Cliquez sur Apply.



Conclusion

Vous devez maintenant avoir correctement configuré la connexion client-à-site sur le routeur de la gamme RV34x.

Cliquez sur les articles suivants pour en savoir plus sur les sujets suivants :

- Configuration d'un client VPN de télétravailleur sur le routeur de la gamme RV34x

- Utiliser le client VPN TheGreenBow pour se connecter avec un routeur de la gamme RV34x
- Créer un compte d'utilisateur pour la configuration du client VPN sur le routeur RV34x

- Créer un groupe d'utilisateurs pour la configuration VPN sur le routeur RV34x

Afficher une vidéo relative à cet article...

Cliquez ici pour afficher d'autres présentations techniques de Cisco