Configuration d'un client VPN pour télétravailleurs sur le routeur de la gamme RV34x

Objectif

La fonctionnalité Client VPN pour télétravailleurs minimise les exigences de configuration sur les sites distants en permettant au périphérique de fonctionner en tant que client matériel VPN Cisco. Lorsque le client VPN pour télétravailleurs démarre la connexion VPN, le serveur VPN IPSec transmet les stratégies IPSec au client VPN pour télétravailleurs et crée le tunnel correspondant.

Cet article a pour but de vous montrer comment configurer le client VPN pour télétravailleurs sur le routeur de la gamme RV34x.

Périphériques pertinents

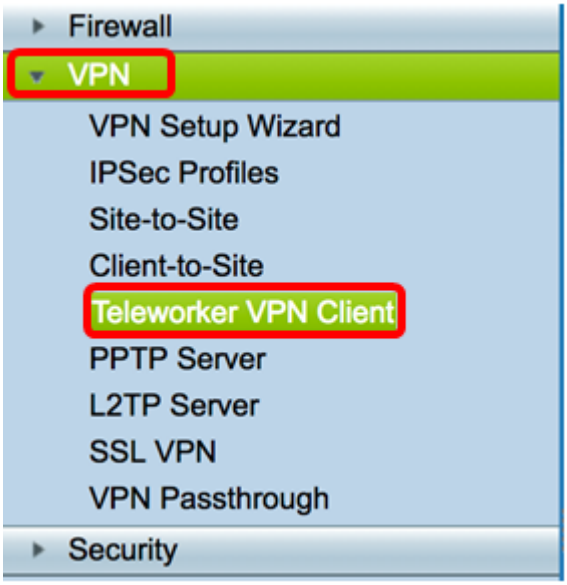
- Routeur série RV34x

Version du logiciel

- 1.0.01.17

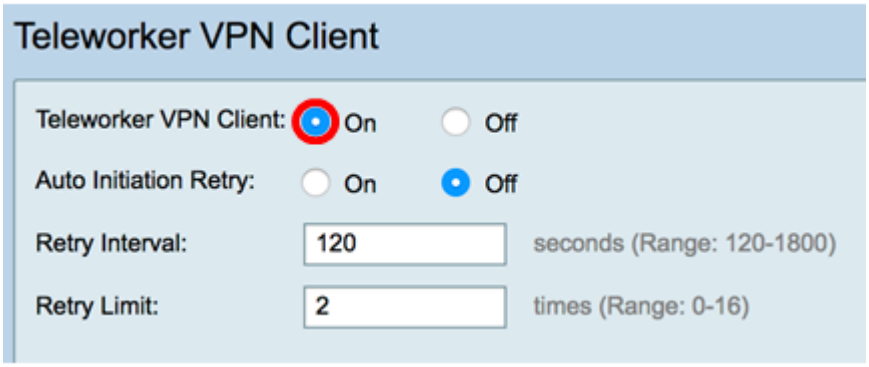
Configuration du client VPN pour télétravailleurs

Étape 1. Connectez-vous à l’utilitaire Web et choisissez VPN > Teleworker VPN Client.



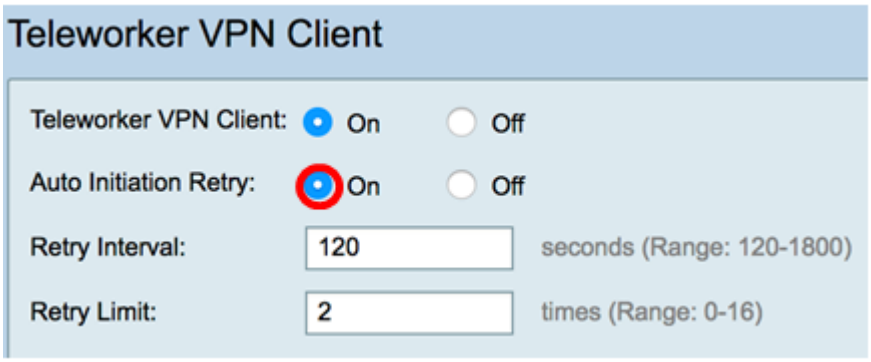
Étape 2. Dans la zone Teleworker VPN Client, cliquez sur la case d'option On pour activer Telework VPN Client.

Remarque : Un seul client VPN de télétravailleur peut avoir une connexion active au démarrage.



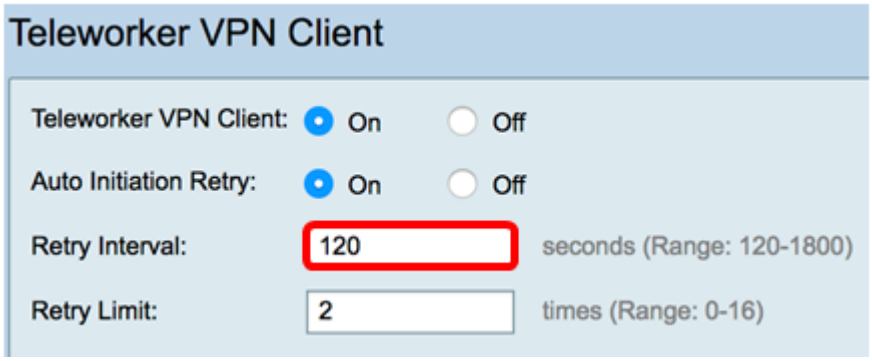
Étape 3. (Facultatif) Dans la zone Auto Initiation Retry, cliquez sur une case d'option On ou Off pour activer ou désactiver une tentative de lancement automatique après un échec. Si vous cliquez sur On, cela signifie que le routeur tentera d'effectuer une initialisation après une panne.

Remarque : Dans cet exemple, On est sélectionné.



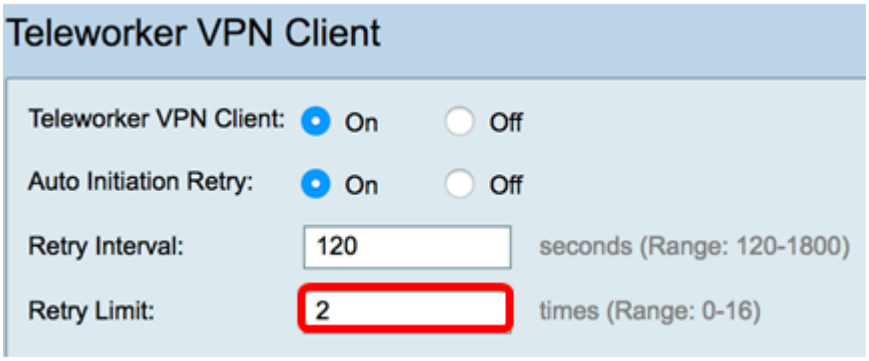
Étape 4. Dans le champ Retry Interval, entrez une valeur en secondes pour que le routeur tente d'établir une connexion. La valeur par défaut est 120 secondes.

Remarque : Dans cet exemple, la valeur par défaut est utilisée.



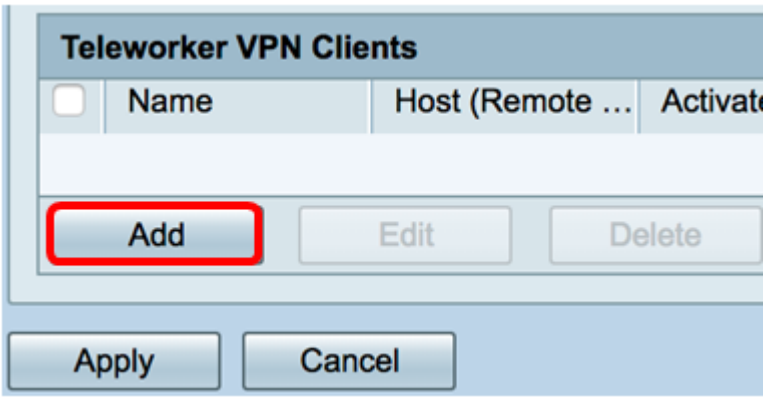
Étape 5. Dans le champ Retry Limit, spécifiez le nombre de fois que le routeur tentera automatiquement d'effectuer une initialisation après une défaillance.

Remarque : Dans cet exemple, le nombre entré est 2.



Configuration des paramètres de base

Étape 6. Dans le tableau Clients VPN de télétravailleurs, cliquez sur Add pour créer et configurer un client VPN de télétravailleurs.



Étape 7. Dans la zone Basic Settings, saisissez un nom pour le tunnel VPN dans le champ Name.

Remarque : Dans cet exemple, Dracarys est utilisé.



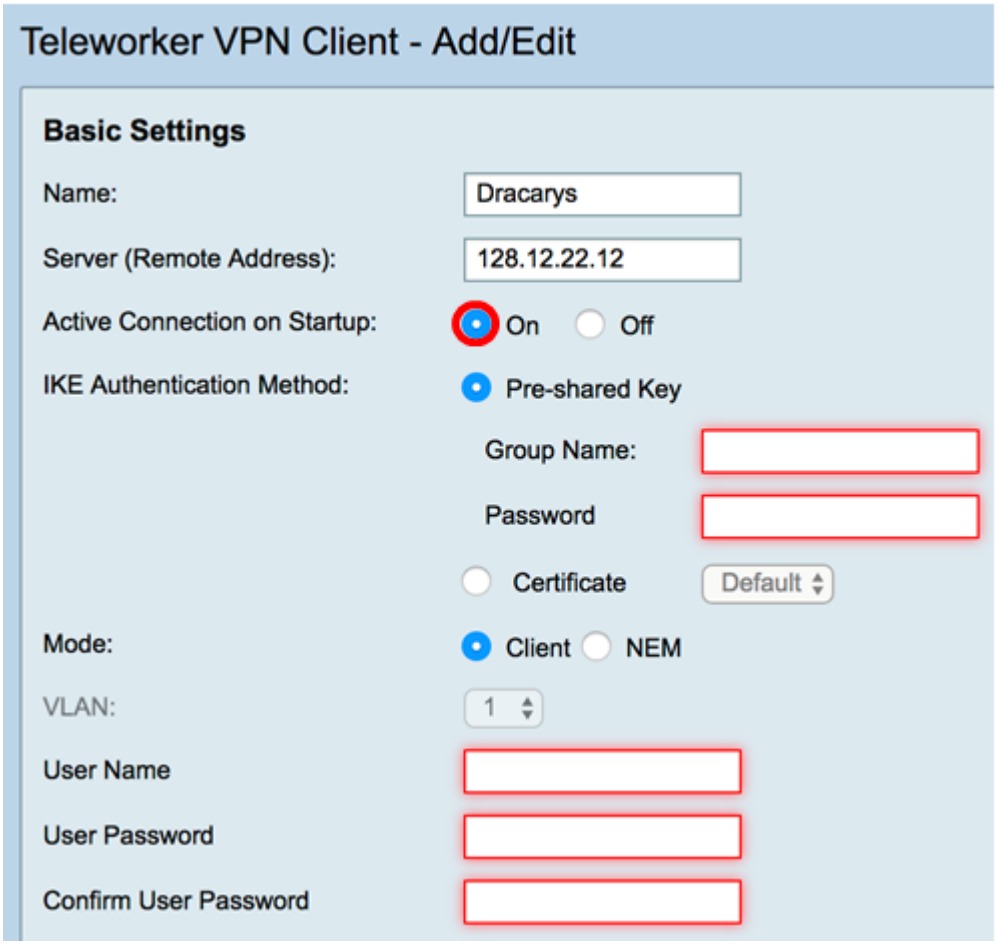
Étape 1. 8. Dans le champ Server (Remote Address), saisissez l'adresse IP du serveur distant.

Remarque : Dans cet exemple, 128.13.22.12 est utilisé.



Étape 9. Pour établir une connexion au démarrage, cliquez sur On dans la zone Active Connection on Startup. Pour démarrer manuellement une connexion, cliquez sur Off.

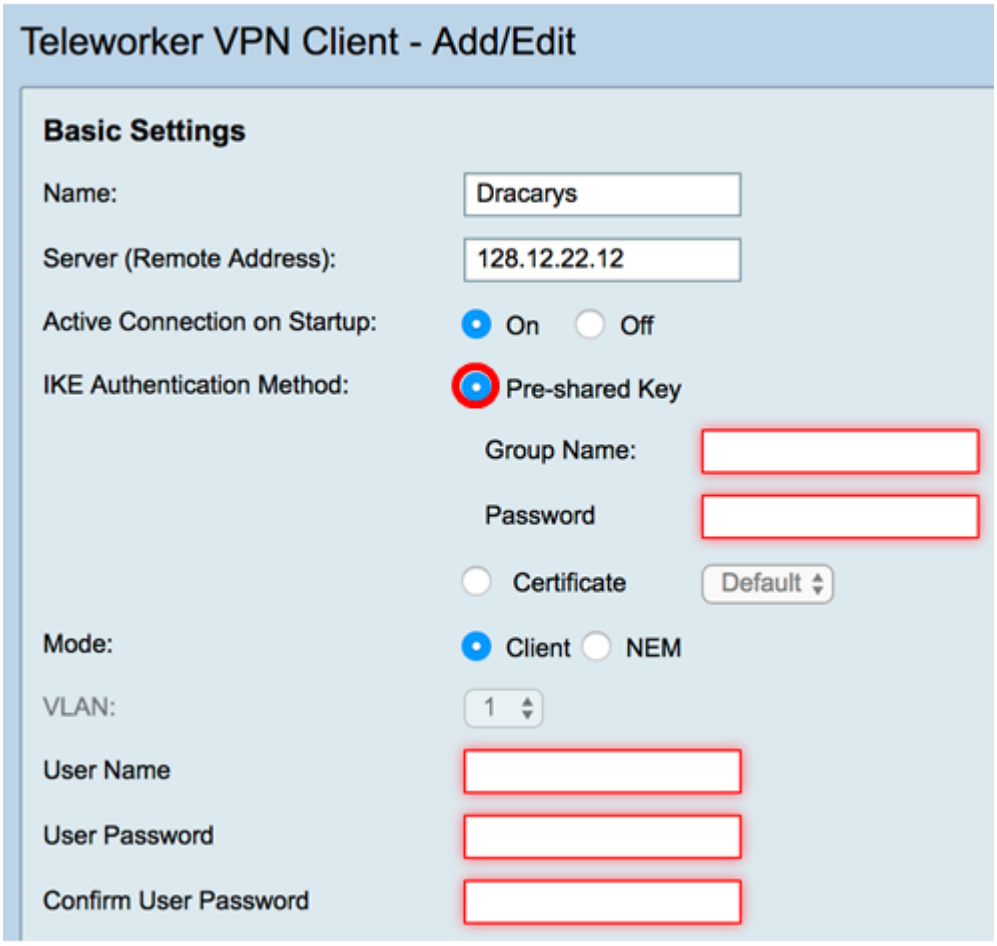
Remarque : Dans cet exemple, On est sélectionné.



Étape 10. Dans la zone IKE Authentication Method, choisissez une méthode d'authentification à utiliser dans les négociations IKE dans le tunnel IKE. Les options sont les suivantes :

- Pre-shared Key : les homologues IKE s'authentifient mutuellement en calculant et en envoyant un hachage de données contenant la clé pré-partagée. Si l'homologue récepteur peut 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 sont pas suffisamment évolutives, car chaque homologue IPSec doit être configuré avec la clé pré-partagée de chaque autre homologue avec lequel il établit une session. Si cette option est sélectionnée, passez à l'étape suivante.
- Certificate : le certificat numérique est un package contenant des informations telles que l'identité du certificat du support : le nom ou l'adresse IP, le numéro de série, la date d'expiration du certificat et une copie de la clé publique du support de certificat. Le format de certificat numérique standard est défini dans la spécification X.509. X.509 version 3 définit la structure des données pour les certificats. Si cette option est sélectionnée, passez à l'étape 13.

Remarque : Dans cet exemple, la clé pré-partagée est choisie.



Étape 11. Si vous avez choisi Clé pré-partagée à l'étape 10, entrez un nom de groupe dans le champ Nom du groupe.

Remarque : Dans cet exemple, FreeFolk est utilisé comme nom de groupe.



Étape 12. Dans le champ Mot de passe, saisissez un mot de passe à associer au groupe.



Étape 13. Si vous avez choisi Certificate à l’étape 10, choisissez le certificat approprié pour votre routeur.

Remarque : Dans cet exemple, Default est sélectionné.



Étape 14. 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 au serveur de fournir les adresses IP de la plage d'adresses configurée. Si cette option est sélectionnée, passez à l'étape 16.
- 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. Vous serez également invité à choisir un VLAN. Si cette option est sélectionnée, passez à l'étape 15.

Remarque : Dans cet exemple, Client est sélectionné.



Étape 15. Si NEM a été choisi à l'étape 14, choisissez un VLAN dans la liste déroulante. Les options peuvent varier en fonction des paramètres VLAN préconfigurés.

Remarque : Dans cet exemple, on choisit 25.



Étape 16. Dans le champ User Name, saisissez un nom d'utilisateur à associer au client VPN de télétravail.

Remarque : Dans cet exemple, Tormound est utilisé.



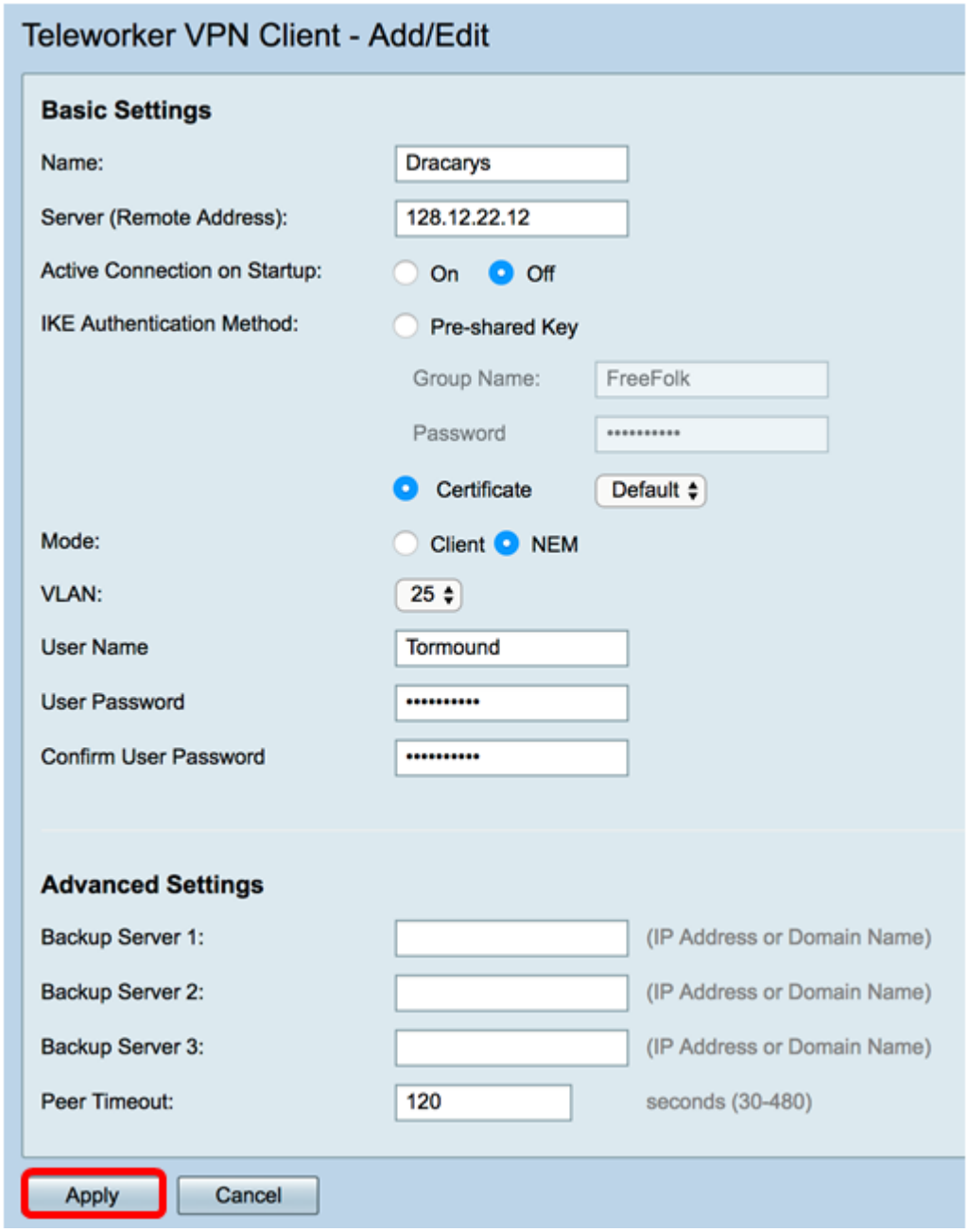
Étape 17. Dans le champ User Password, entrez un mot de passe pour le nom d'utilisateur.



Étape 18. Dans le champ Confirm User Password, saisissez à nouveau le mot de passe pour le confirmer. Si le mot de passe saisi est incorrect, le champ devient rouge.

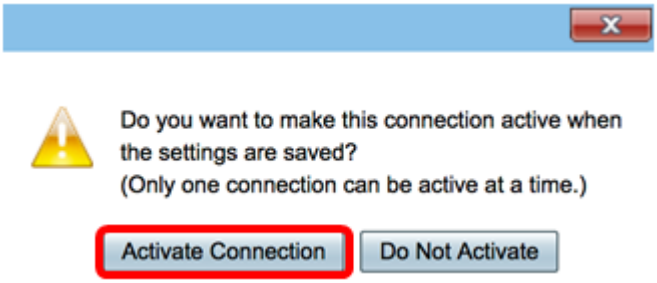


Étape 19. Cliquez sur Apply pour enregistrer les paramètres.

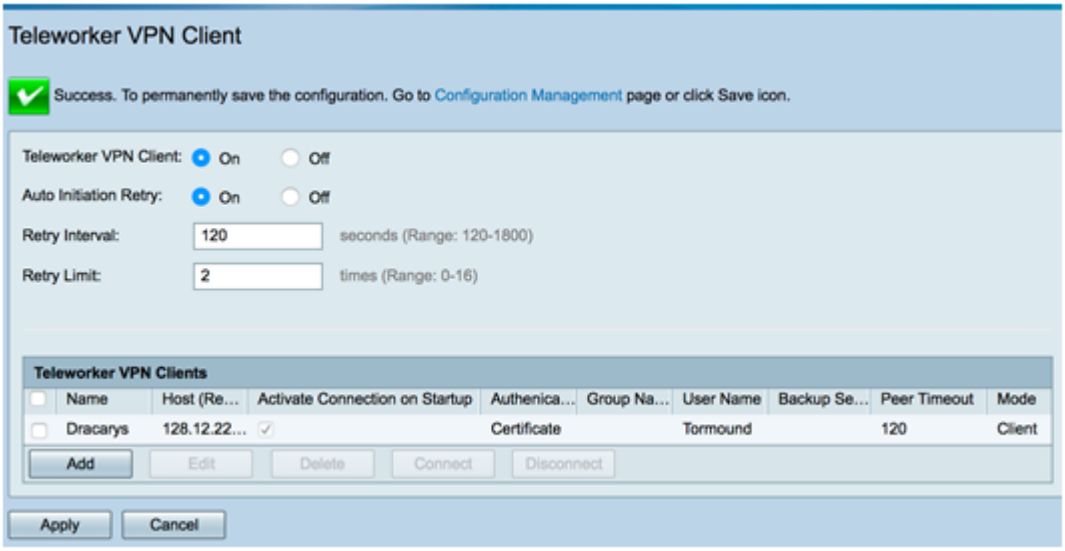


Étape 20. Une fenêtre contextuelle s'affiche pour vous demander d'activer la connexion lors de l'enregistrement des paramètres. Cliquez sur le bouton Activate Connection pour confirmer l'activation et sur le bouton Do Not Activate pour activer la connexion ultérieurement.

Remarque : Dans cet exemple, Activer la connexion est sélectionné.



Vous serez redirigé vers la page principale du client VPN pour télétravailleurs.



Vous devez maintenant avoir correctement configuré les paramètres de base du client VPN pour télétravailleurs sur le routeur de la gamme RV34x.

Configuration des paramètres avancés

Étape 1. (Facultatif) Dans le champ Backup Server 1, saisissez l'adresse IP ou le nom de domaine du serveur de sauvegarde. C'est à ce niveau 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 prévus à cet effet. Le serveur de sauvegarde 1 a la priorité la plus élevée parmi les trois serveurs et le serveur de sauvegarde 3 a la priorité la plus faible.

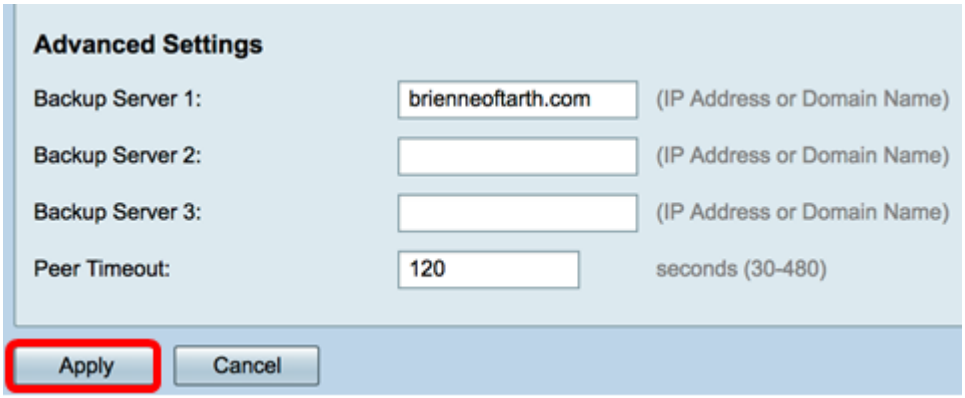
Remarque : Dans cet exemple, brienneoftarth.com est utilisé.



Étape 2. Dans le champ Peer Timeout, entrez la durée en secondes pendant laquelle un homologue peut rester inactif avant de se déconnecter. La plage est comprise entre 30 et 480 secondes. Il est défini par défaut à 120.



Étape 3. Cliquez sur Apply (appliquer).



Vous devez maintenant avoir correctement configuré les paramètres avancés du VPN pour télétravailleurs sur le routeur de la gamme RV34x.

Cliquez sur les liens suivants pour accéder à des articles sur les sujets suivants :

- Configuration de la connexion de réseau privé virtuel (VPN) client-site sur le routeur de la gamme RV34x
- Page produit : Liens vers tous les articles sur les routeurs de la gamme RV34x

Visionner une vidéo connexe à cet article...

Cliquez ici pour consulter les autres discussions techniques (Tech Talks) de Cisco

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.