

# Configuration de Funk RADIUS pour authentifier les clients Cisco VPN

## Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Configuration du concentrateur VPN 3000](#)

[Configurer le serveur de RAYON](#)

[Informations connexes](#)

## [Introduction](#)

Ce document affiche comment configurer le concentrateur VPN 3000 et le serveur Funk RADIUS pour travailler ensemble pour authentifier un Client VPN Cisco. Après avoir authentifier le client vpn, le serveur Funk RADIUS fournit alors au client des adresses IP.

## [Avant de commencer](#)

### [Conventions](#)

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

### [Conditions préalables](#)

Les informations présentées dans ce document supposent que vous avez configuré les interfaces privées et publiques sur le concentrateur VPN.

### [Composants utilisés](#)

Les informations dans ce document sont basées sur toutes les releases du concentrateur VPN 3000 et s'appliquent au Cisco VPN 3000 Client (2.5.x) et au Client VPN Cisco (3.x).

Ces informations ont été créées des périphériques dans un environnement de travaux pratiques spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

## Configuration du concentrateur VPN 3000

Suivez les étapes ci-dessous pour configurer le côté de concentrateur VPN.

1. Allez à la **configuration > au système > aux serveurs > à l'authentification** et cliquez sur Add. Pour le type de serveur, **interne** choisi, cliquent sur Add alors.
2. Allez à la **configuration > au système > aux serveurs > à l'authentification**, cliquez sur Add, et configurez les paramètres suivants. Type de serveur : **RAYON** choisi. Serveur d'authentification : Écrivez l'adresse IP ou le nom d'hôte du serveur de RAYON. Secret de serveur : Entrez dans le précis la même chaîne que celui sur le serveur de RAYON. Quand vous avez configuré ces paramètres, cliquez sur Add.
3. Allez à la **configuration > au système > à la gestion d'adresses** et vérifiez l'option pour **l'adresse d'utilisation du serveur d'authentification**.
4. Allez au **Configuration > User Management > Groups**, cliquez sur Add, et configurez les paramètres pour l'identité, les DN, et l'authentification de groupe. Sur l'onglet d'identité, placez les paramètres suivants. Nom de groupe (distinguant majuscules et minuscules) Mot de passe (distinguant majuscules et minuscules) Sur l'onglet Général, placez les paramètres suivants. DNS principal DNS secondaire WINS primaires WINS secondaires **Remarque:** Les adresses IP des deux serveurs WINS sont passées au client vpn sur la connexion. Sur l'onglet d'IPSec, placez les paramètres suivants. Authentification : **RAYON** choisi. Quand vous avez configuré ces paramètres, cliquez sur Add.

Avec la release de 3.0 et plus tard, vous pouvez configurer différents serveurs Funk RADIUS pour différents groupes, par opposition à un serveur Funk RADIUS a défini globalement et utilisé par tous les groupes. Tous les groupes qui ne font pas configurer différents serveurs Funk RADIUS utiliseront le serveur de trouille qui est défini globalement.

L'exemple ci-dessus définit un serveur Funk RADIUS global. Vous pouvez également choisir de définir différents serveurs Funk RADIUS pour chaque groupe. Pour faire ceci, aller au **Configuration > User Management > Groups**, mettre en valeur un groupe, et choisir **modifiez le serveur authentique**.

## Configurer le serveur de RAYON

Suivez les étapes ci-dessous pour configurer le serveur de RAYON pour communiquer avec le concentrateur VPN. Pour plus d'informations complètes sur le serveur, référez-vous au [logiciel ou au Juniper Networks de trouille](#) .

1. Sur le menu de client RAS, cliquez sur Add et configurez les paramètres pour le nom de client, adresse IP et les faites/modèles. Nom de client : Écrivez le nom du concentrateur VPN. Adresse IP : Introduisez l'adresse de l'interface qui communique avec le serveur de RAYON. (Le serveur de RAYON visualise le concentrateur VPN en tant que client RADIUS.) Faites/modèle : Entrez dans le **concentrateur VPN 3000**.
2. Cliquez sur Edit le **secret d'authentification** et écrivez le secret partagé, puis cliquez sur la **sauvegarde**.
3. Sur le menu utilisateur, choisissez l'utilisateur/groupe que vous avez installé et ajoutez les attributs de retour-liste pour la classe et l'adresse IP encadrée. Classe : Écrivez le nom de groupe que vous avez configuré dans l'étape 4 ci-dessus. Adresse IP encadrée : Écrivez l'adresse IP ou le nom du pool du concentrateur VPN.

4. Arrêtez et redémarrez le service RADIUS.

## Informations connexes

- [Page d'assistance RADIUS](#)
- [Page d'assistance IPsec](#)
- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Page d'assistance du Client VPN 3000 Series Cisco](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)