

# Configuration du concentrateur VPN 3000 pour communiquer avec le client VPN à l'aide de certificats

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Certificats de concentrateur VPN 3000 pour des clients vpn](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## Introduction

Ce document comporte des instructions pas à pas sur la façon dont configurer les Concentrateurs de la gamme Cisco VPN 3000 avec des clients VPN avec l'utilisation des Certificats.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

Les informations dans ce document sont basées sur la version 4.0.4A de logiciel du concentrateur de Cisco VPN 3000.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Certificats de concentrateur VPN 3000 pour des clients vpn

Terminez-vous ces étapes afin de configurer des Certificats de concentrateur VPN 3000 pour des clients vpn.

1. La stratégie IKE doit être configurée pour utiliser des Certificats sur le gestionnaire de gamme de concentrateur VPN 3000. Afin de configurer la stratégie IKE, **configuration > protocoles de système > de Tunnellisation > IPsec > propositions d'IKE**, et mouvement choisis **CiscoVPNClient-3DES-MD5-RSA** aux propositions actives.
2. Vous devez également configurer la stratégie d'IPsec pour utiliser des Certificats. **La configuration > la Gestion des stratégies > la gestion de trafic > les associations de sécurité** choisies, le point culminant **ESP-3DES-MD5** et cliquent sur alors **modifient pour configurer la stratégie d'IPsec** pour configurer la stratégie d'IPsec.
3. Sur la fenêtre de modifier, sous des Certificats numériques, veillez à sélectionner votre certificat d'identité installé. Sous la proposition d'IKE, **CiscoVPNClient-3DES-MD5-RSA** choisis et cliquent sur Apply.
4. Afin de configurer un groupe d'IPsec, le **Configuration > User Management > Groups** choisi > **ajoutent**, ajoutent un groupe appelé l'**IPSECCERT** (le nom de groupe IPSECCERT apparie l'unité organisationnelle (OU) dans le certificat d'identité), et sélectionnent un mot de passe. Ce mot de passe n'est pas utilisé n'importe où si vous utilisez des Certificats. Dans cet exemple, "cisco123" est le mot de passe.
5. À la même page, cliquez sur l'onglet Général et assurez-vous que vous sélectionnez **IPsec** en tant que perçage d'un tunnel Protocol.
6. Cliquez sur l'onglet d'IPsec et assurez-vous que votre association configurée de sécurité IPsec (SA) est sélectionnée sous IPsec SA et cliquez sur Apply.
7. Afin de configurer un groupe d'IPsec sur le concentrateur VPN 3000, le **Configuration > User Management** choisi > les **utilisateurs > ajoutent**, spécifient un nom d'utilisateur, le mot de passe, et le nom de groupe, et puis cliquent sur Add. Dans l'exemple, ces champs sont utilisés : Nom d'utilisateur = cert\_user Mot de passe = cisco123 Vérifiez = cisco123 Groupe = IPSECCERT
8. Afin d'activer l'élimination des imperfections sur la **configuration > le système > les événements > les classes** choisis de concentrateur VPN 3000 et ajouter ces classes : CERT 1-13 IKE 1-6 IKEDBG 1-10 IPSEC 1-6 IPSECDBG 1-10
9. **La surveillance** choisie > commande **filtrable de procédure de connexion d'événement** pour visualiser met au point. **Remarque:** Si vous décidez de changer les adresses IP, vous pouvez faire une inscription des nouvelles adresses IP et installer le certificat délivré plus tard avec ces nouvelles adresses.

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

Référez-vous aux [problèmes de connexion de dépannage sur le concentrateur VPN 3000](#) pour davantage d'information de dépannage.

## Informations connexes

- [Concentrateurs VPN de la gamme Cisco 3000](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)