Configuration du concentrateur Cisco VPN 3000 et du client Network Associates PGP

Contenu

Introduction

Ce document décrit comment configurer le concentrateur de Cisco VPN 3000 et la version 6.5.1 courante de client de l'intimité plutôt bonne de networks associates (PGP) pour recevoir des connexions de l'un l'autre.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 4.7 de concentrateur de Cisco VPN 3000
- Version du client 6.5.1 PGP d'associés de réseaux

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.

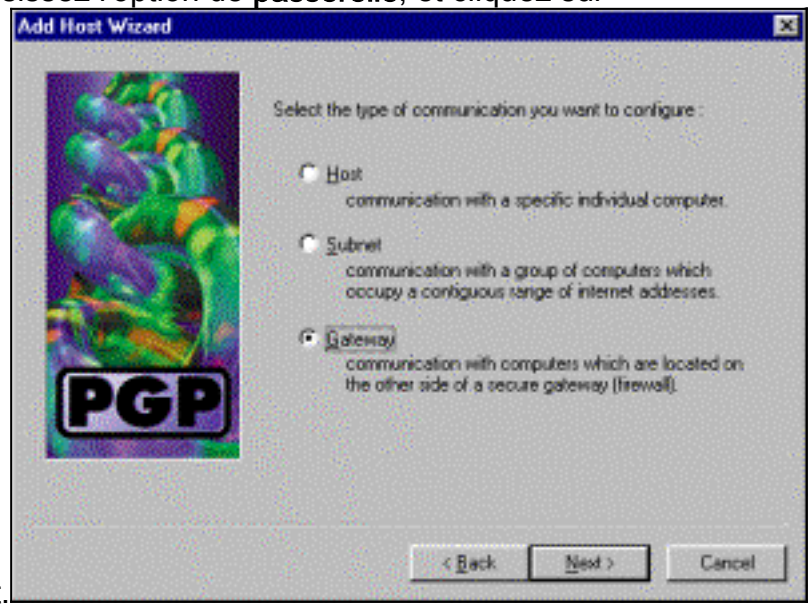
Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

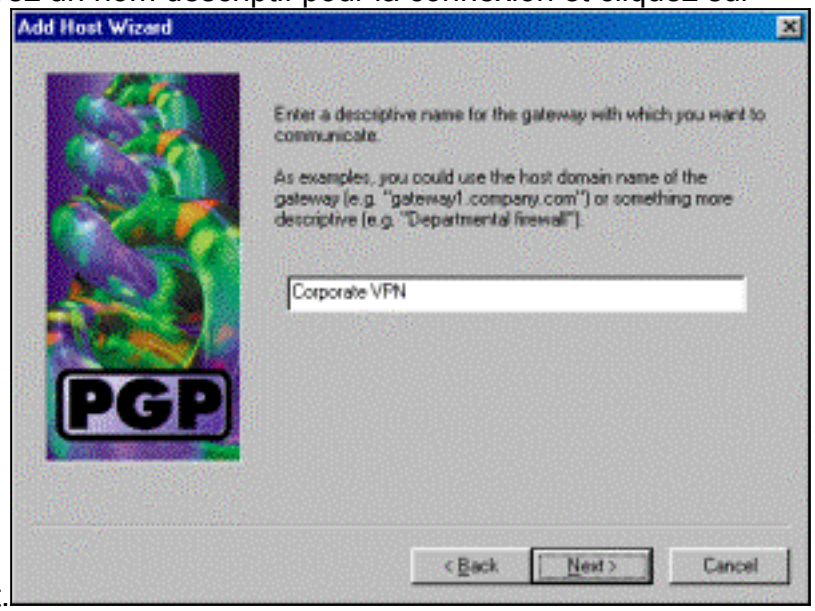
Configurez le client de Network Associates PGP pour se connecter au concentrateur de Cisco VPN 3000

Employez cette procédure pour configurer le client de Network Associates PGP pour se connecter au concentrateur VPN 3000.

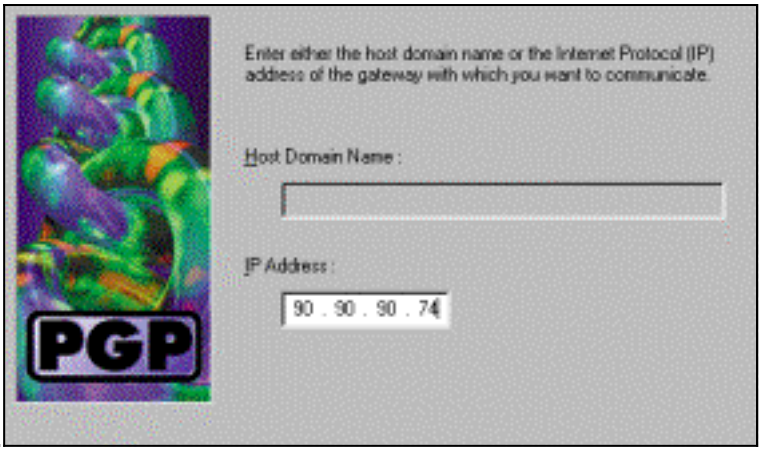
1. Lancement **PGPNet > hôtes**.
2. Cliquez sur Add et puis cliquez sur Next.
3. Choisissez l'option de **passerelle**, et cliquez sur Next.



4. Écrivez un nom descriptif pour la connexion et cliquez sur Next.

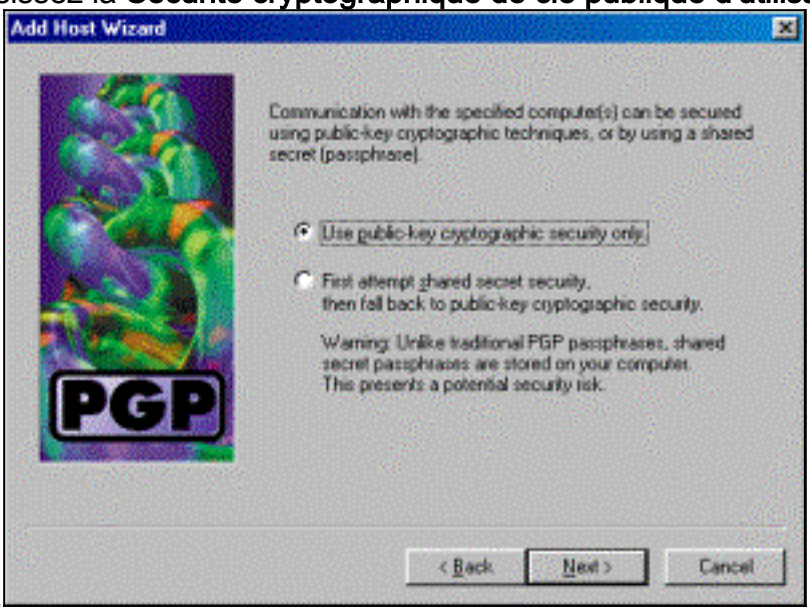


5. Écrivez le nom de domaine d'hôte ou l'adresse IP de l'interface publique du concentrateur



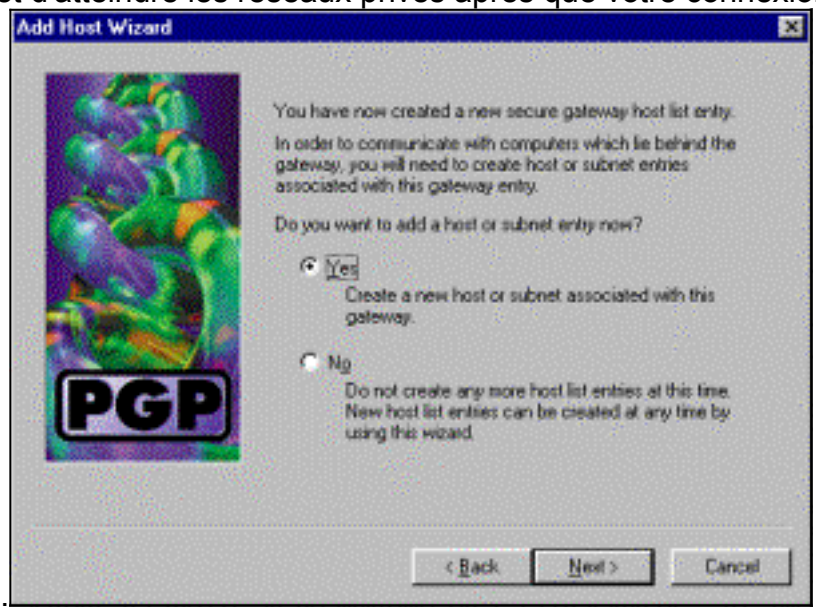
VPN 3000 et cliquez sur Next.

6. Choisissez la **Sécurité cryptographique de clé publique d'utilisation seulement** et cliquez sur



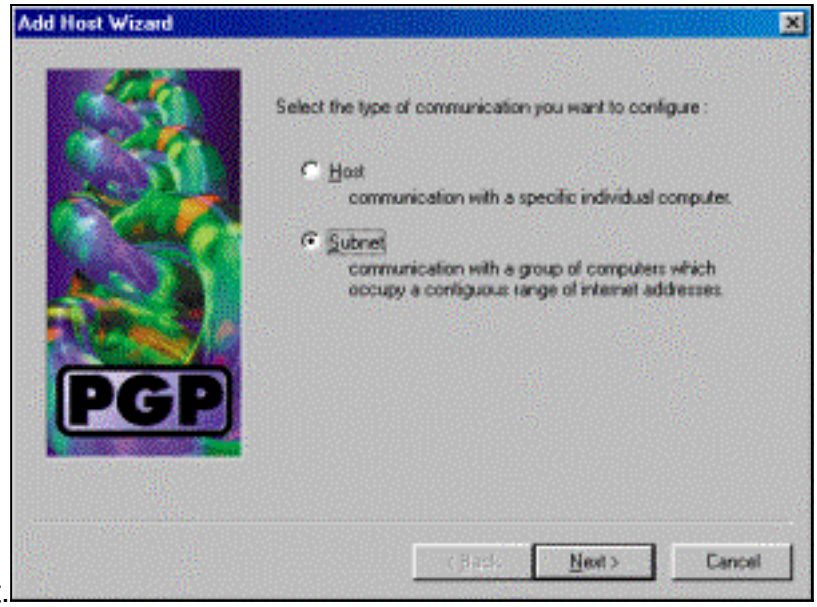
Next.

7. Sélectionnez **oui**, et cliquez sur Next. Quand vous ajoutez un nouveau hôte ou sous-réseau, il te permet d'atteindre les réseaux privés après que votre connexion soit



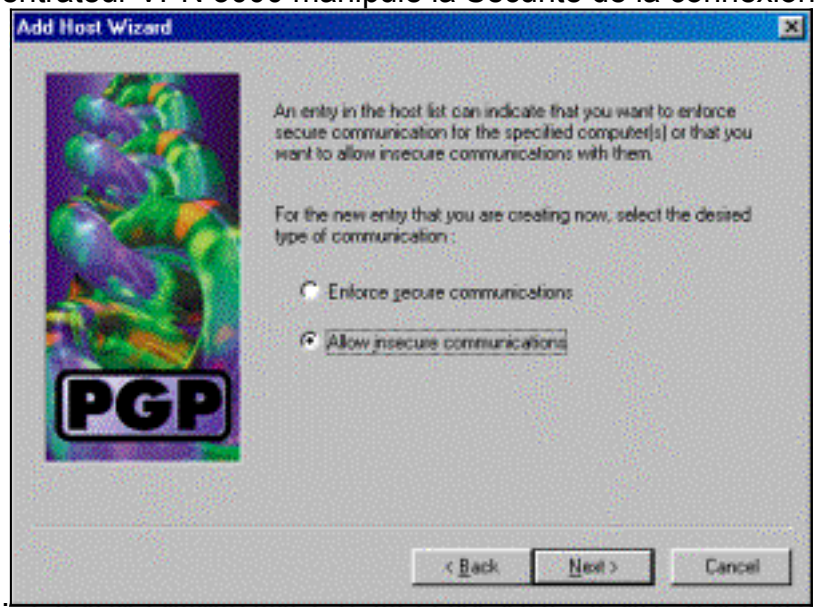
sécurisée.

8. **Le sous-réseau** choisi et cliquent sur



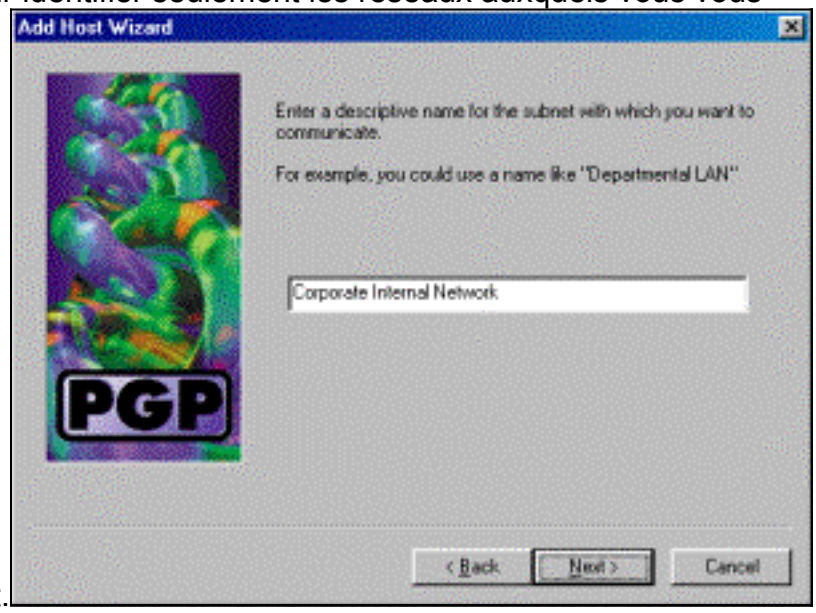
Next.

9. Choisissez **permettent des transmissions non sécurisées** et cliquent sur Next.Le concentrateur VPN 3000 manipule la Sécurité de la connexion, pas le logiciel client



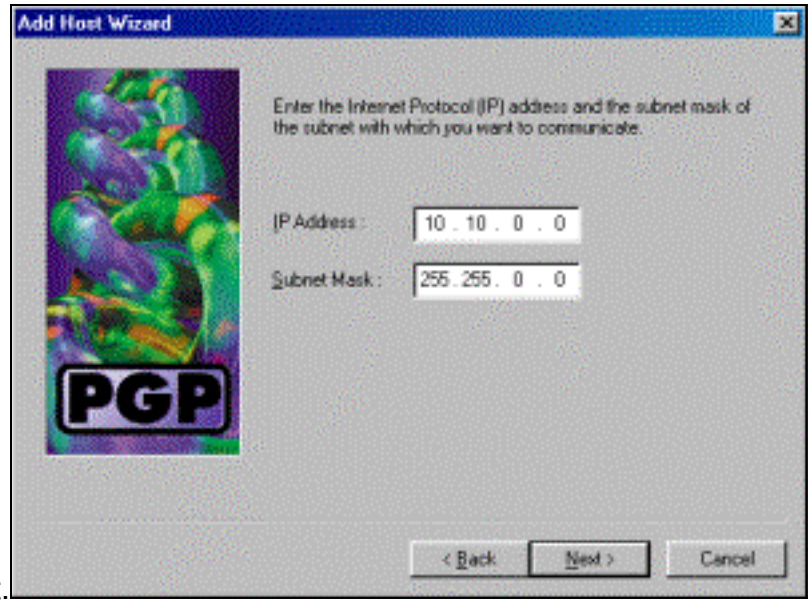
PGP.

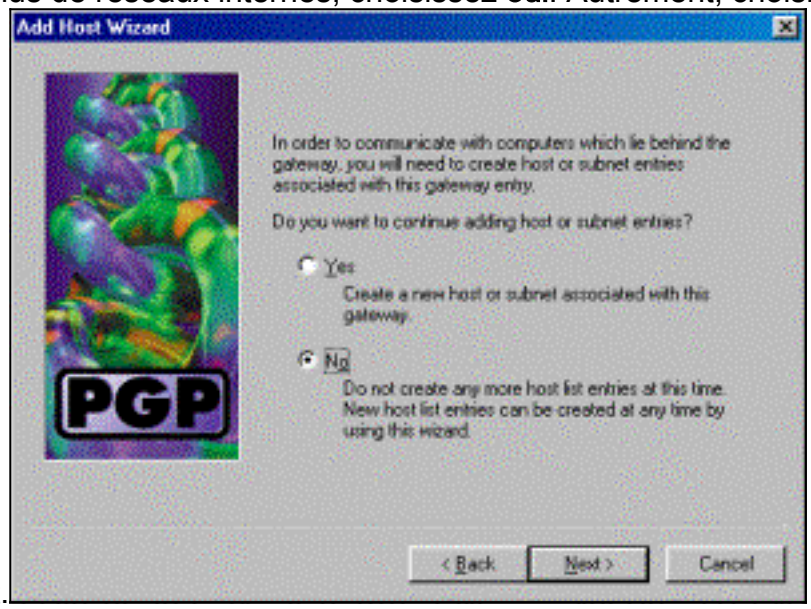
10. Écrivez un nom descriptif pour identifier seulement les réseaux auxquels vous vous



connectez et cliquez sur Next.

11. Écrivez le network number et le masque de sous-réseau pour le réseau derrière le concentrateur VPN 3000 et cliquez sur

Next. 

12. S'il y a plus de réseaux internes, choisissez **oui**. Autrement, choisissez l'**aucun** et cliquez sur Next. 

Configurez le concentrateur de Cisco VPN 3000 pour recevoir des connexions de client de Network Associates PGP

Employez cette procédure pour configurer le concentrateur de Cisco VPN 3000 pour recevoir des connexions d'un client de Network Associates PGP :

1. **Configuration > Tunnellisation et Sécurité > IPSec > propositions** choisis d'**IKE**.
2. Lancez la proposition **IKE-3DES-SHA-DSA** en la sélectionnant dans la colonne inactive de propositions. Ensuite, cliquez sur le bouton de **lancement** et puis cliquez sur le bouton **nécessaire par sauvegarde**.
3. **Configuration > Gestion des stratégies > gestion de trafic > SAS** choisies.
4. Cliquez sur **Add**.
5. Laissez tous excepté ces champs à leurs valeurs par défaut :**Nom SA :** Créez un nom unique pour identifier ceci.**Certificat numérique :** Choisissez le serveur installé identifient le certificat.**Proposition d'IKE : IKE-3DES-SHA-DSA** choisi.
6. Cliquez sur **Add**.
7. Sélectionnez le **Configuration > User Management > Groups**, cliquez sur Add le **groupe**, et

configurez ces champs :**Note**: Si tous vos utilisateurs sont des clients PGP, vous pouvez utiliser le groupe de base (**Configuration > User Management > groupe de base**) au lieu de créer de nouveaux groupes. Si oui, ignorez les étapes pour l'identité tabulent et se terminent les étapes 1 et 2 pour l'onglet d'IPSec seulement.Sous l'onglet d'identité, écrivez ces informations :**Nom de groupe :** Écrivez un nom unique. (Ce nom de groupe doit être égal au champ OU dans le certificat numérique du client PGP.)**Mot de passe :** Entrez le mot de passe pour le groupe.Sous l'onglet d'IPSec, écrivez ces informations :**Authentification :** Placez ceci à **aucun**.**Configuration de mode :** Décochez ceci.

8. Cliquez sur **Add**.
9. Sauvegardez comme nécessaire partout.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance IPsec
- Téléchargement de logiciel VPN (clients enregistrés seulement)
- Support technique - Cisco Systems