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

Contenu

Introduction

Ce document décrit comment configurer à la fois le concentrateur Cisco VPN 3000 et le client PGP de Network Associates exécutant la version 6.5.1 pour accepter les connexions entre eux.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Concentrateur VPN Cisco 3000 version 4.7
- Client PGP de Networks Associates version 6.5.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

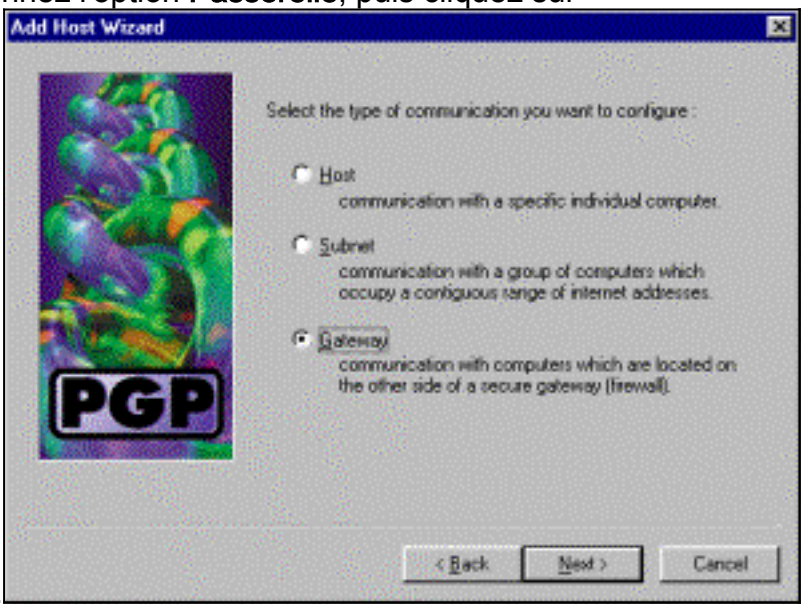
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

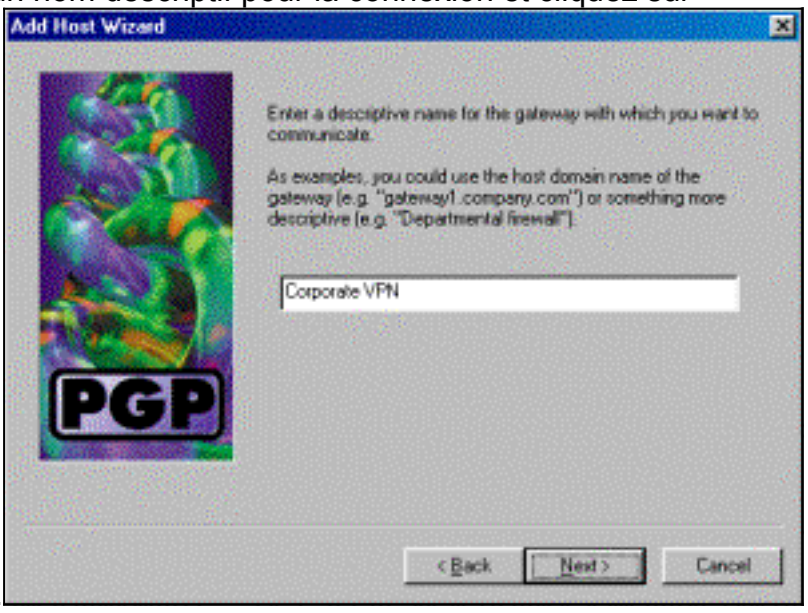
Configurer le client PGP de Network Associates pour la connexion au concentrateur VPN Cisco 3000

Suivez cette procédure pour configurer le client PGP de Network Associates afin qu'il se connecte au concentrateur VPN 3000.

1. Lancez **PGPNet > Hosts**.
2. Cliquez sur **Ajouter**, puis sur **Suivant**.
3. Sélectionnez l'option **Passerelle**, puis cliquez sur **Suivant**.

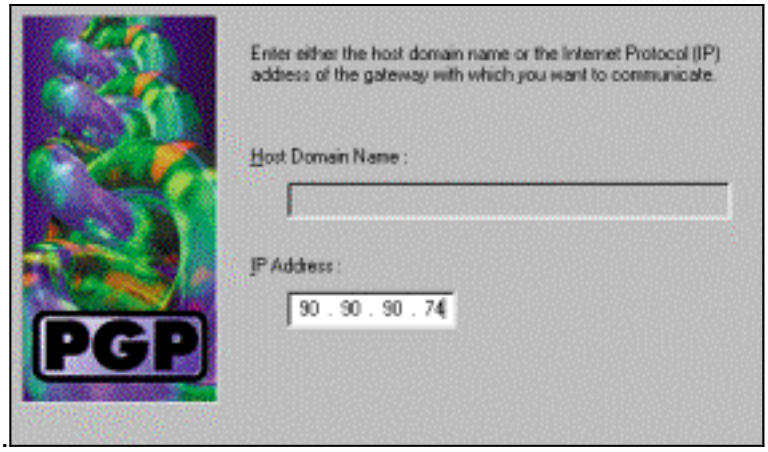


4. Entrez un nom descriptif pour la connexion et cliquez sur **Suivant**.

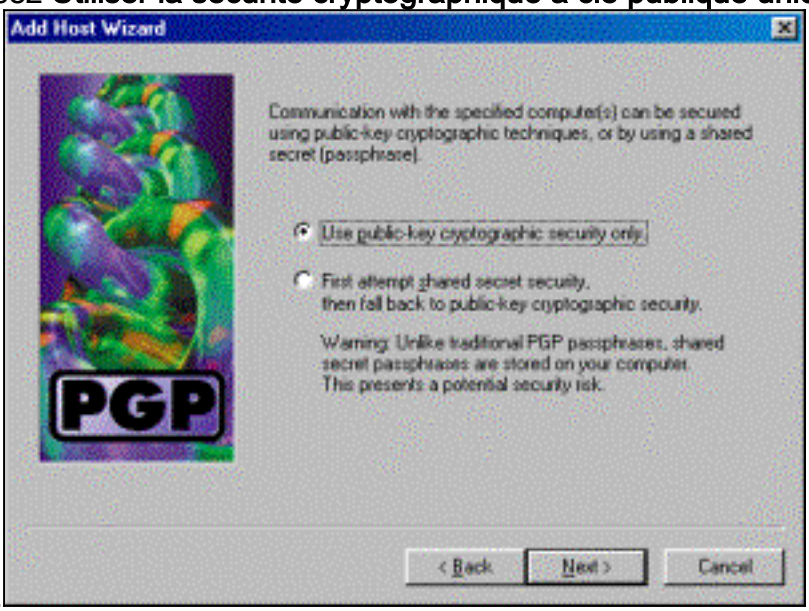


5. Entrez le nom de domaine hôte ou l'adresse IP de l'interface publique du concentrateur VPN

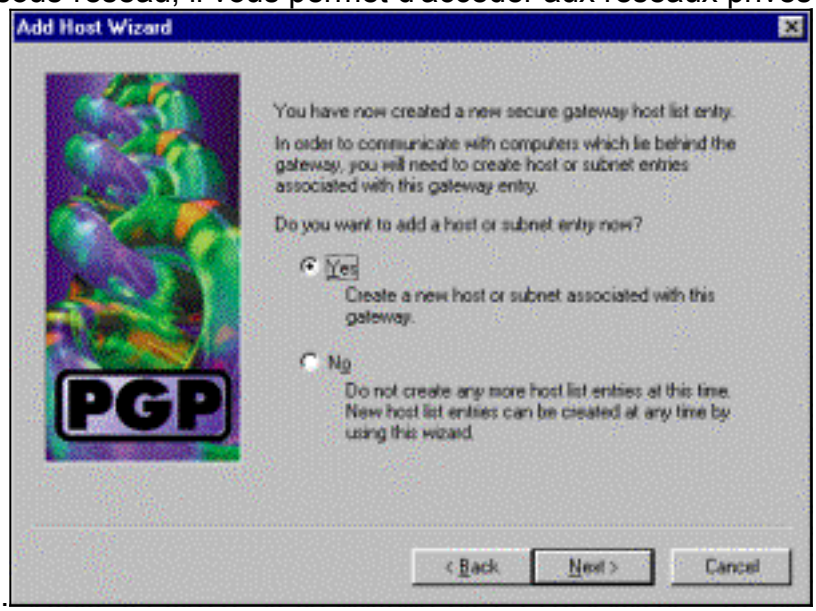
3000 et cliquez sur **Next (Suivant)**.



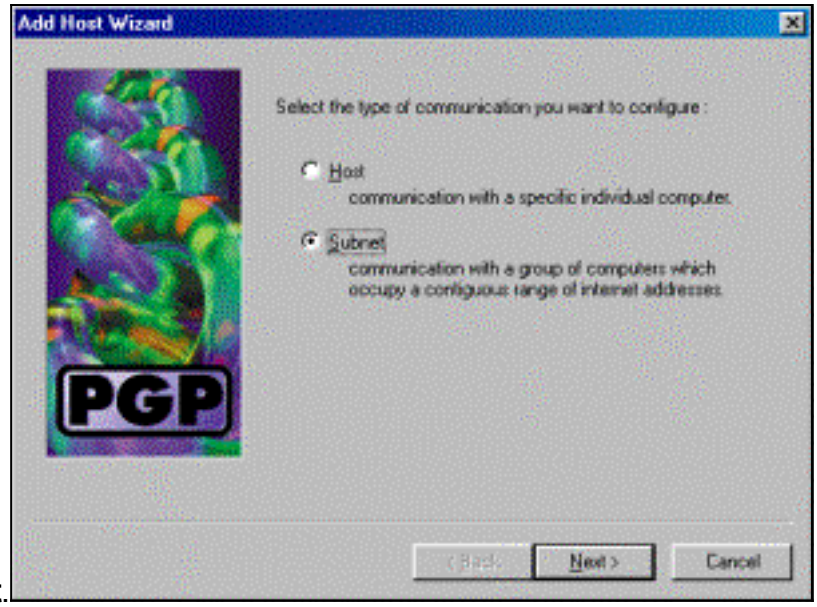
6. Choisissez **Utiliser la sécurité cryptographique à clé publique uniquement** et cliquez sur **Suivant**.



7. Sélectionnez **Oui**, puis cliquez sur **Suivant**. Lorsque vous ajoutez un nouvel hôte ou un nouveau sous-réseau, il vous permet d'accéder aux réseaux privés une fois votre connexion sécurisée.

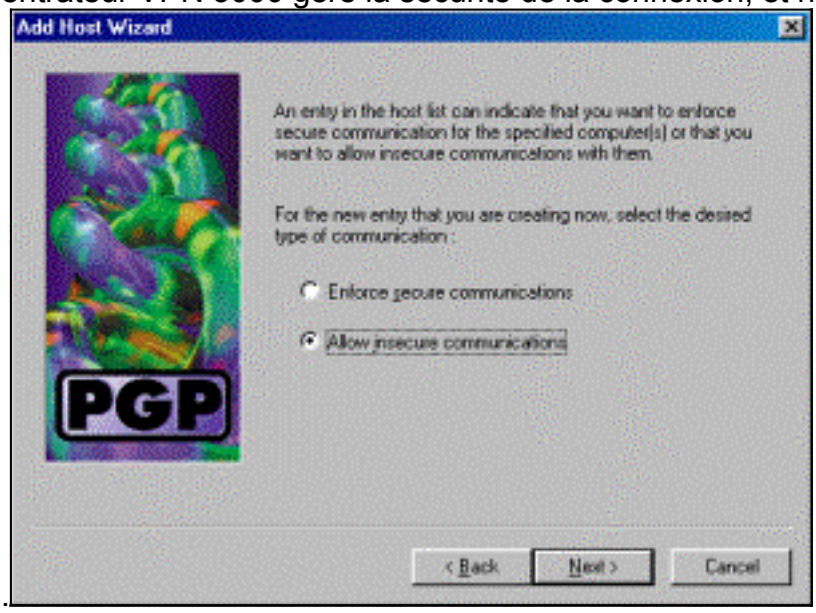


8. Sélectionnez **Subnet** et cliquez sur



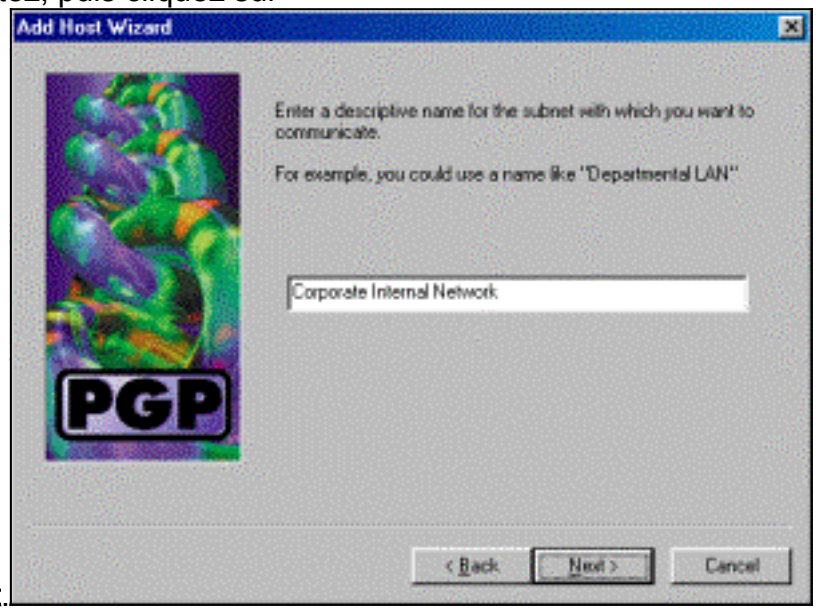
Next.

9. Sélectionnez **Autoriser les communications non sécurisées** et cliquez sur **Suivant**.Le concentrateur VPN 3000 gère la sécurité de la connexion, et non le logiciel client



PGP.

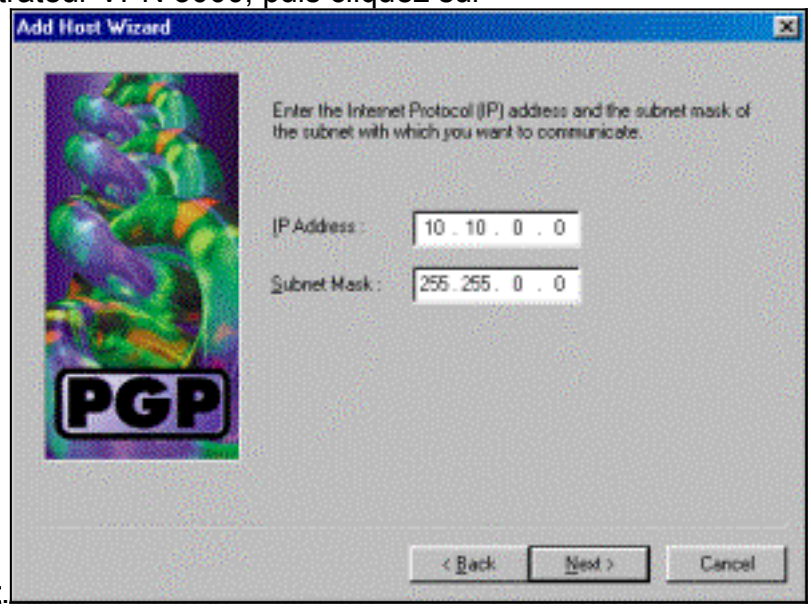
10. Entrez un nom descriptif pour identifier de manière unique les réseaux auxquels vous vous connectez, puis cliquez sur



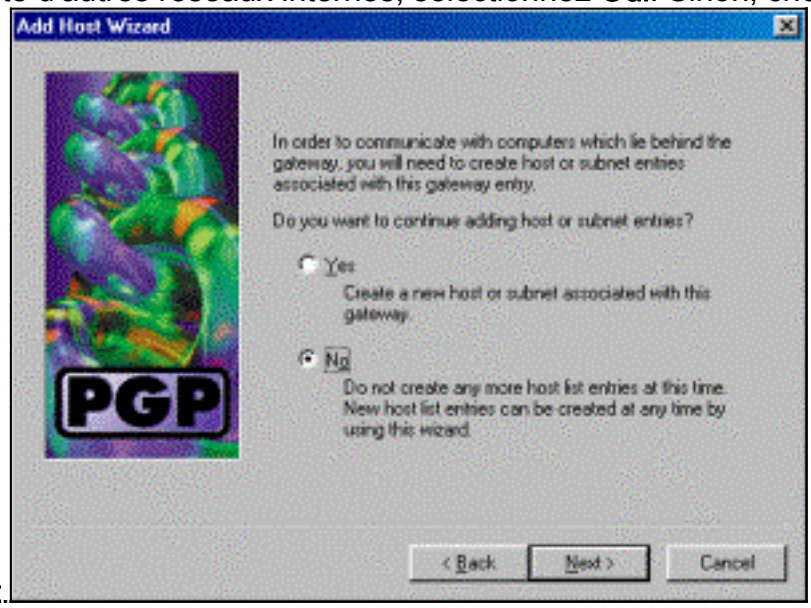
Suivant.

11. Entrez le numéro de réseau et le masque de sous-réseau du réseau situé derrière le

concentrateur VPN 3000, puis cliquez sur **Suivant**.



12. S'il existe d'autres réseaux internes, sélectionnez **Oui**. Sinon, choisissez **Non** et cliquez sur **Suivant**.



Configurer le concentrateur Cisco VPN 3000 pour accepter les connexions à partir du client PGP de Network Associates

Utilisez cette procédure pour configurer le concentrateur Cisco VPN 3000 afin qu'il accepte les connexions d'un client PGP Network Associates :

1. Sélectionnez **Configuration > Tunneling and Security > IPSec > IKE Propositions**.
2. Activez la proposition **IKE-3DES-SHA-DSA** en la sélectionnant dans la colonne Propositions inactives. Ensuite, cliquez sur le bouton **Activate**, puis sur le bouton **Save Needed**.
3. Sélectionnez **Configuration > Policy Management > Traffic Management > SA**.
4. Cliquez sur **Add**.
5. Conservez tous les champs à l'exception de ceux-ci dans leurs paramètres par défaut :**Nom du SA :** Créez un nom unique pour l'identifier.**Certificat numérique :** Sélectionnez le certificat d'identification du serveur installé.**Proposition IKE :** Sélectionnez **IKE-3DES-SHA-DSA**.
6. Cliquez sur **Add**.
7. Sélectionnez **Configuration > User Management > Groups**, cliquez sur **Add Group** et

configurez ces champs :**Remarque :** Si tous vos utilisateurs sont des clients PGP, vous pouvez utiliser le groupe de base (**Configuration > User Management > Base Group**) au lieu de créer de nouveaux groupes. Si c'est le cas, ignorez les étapes de l'onglet Identité et complétez les étapes 1 et 2 de l'onglet IPSec uniquement.Sous l'onglet Identité, saisissez les informations suivantes :**Nom du groupe :** Entrez un nom unique. (Ce nom de groupe doit être égal au champ OU du certificat numérique du client PGP.)**Mot de passe :** Saisissez le mot de passe du groupe.Sous l'onglet IPSec, saisissez les informations suivantes :**Authentification:** Définissez cette valeur sur **Aucun**.**Configuration du mode :** Décochez ceci.

8. Cliquez sur **Add**.
9. Économisez autant que nécessaire.

Informations connexes

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