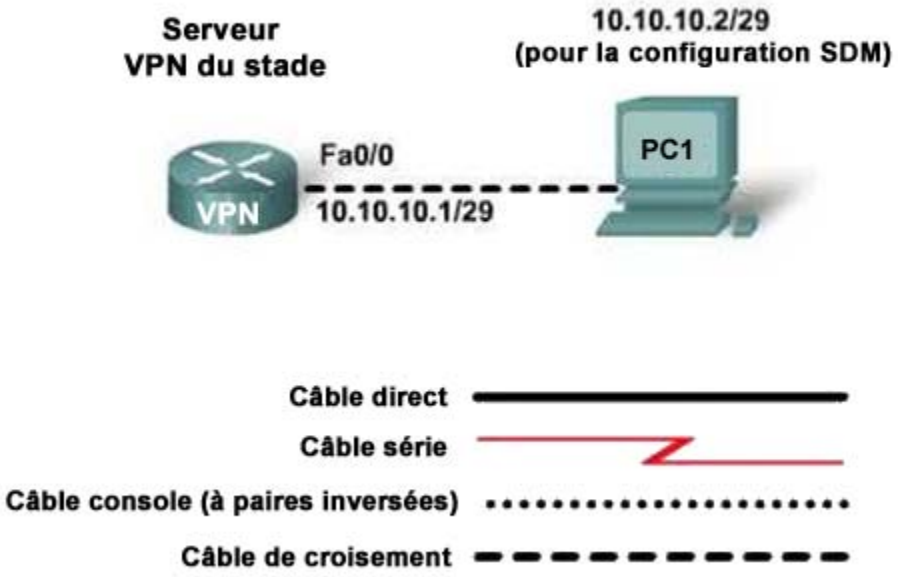
Travaux pratiques 8.3.4.3 Création d'un serveur Cisco EasyVPN (facultatif)



Objectifs

- Configurer les paramètres de base d'un routeur à l'aide du logiciel IOS pour accéder à SDM
- Configurer un serveur EasyVPN en utilisant SDM sur un routeur Cisco

Objectifs de l'examen CCNA 640-802

Ces travaux pratiques font appel à des compétences pour remplir l'objectif suivant :

- Décrire la technologie VPN (notamment son importance, ses avantages, sa fonction, ses incidences et ses composants)

Résultats attendus et critères de réussite

Avant de commencer ces travaux pratiques, lisez l'énoncé des exercices proposés. Selon vous, quel sera le résultat de l'exécution de ces tâches ?

_____

_____

_____

Dans quelle mesure la possibilité de créer un serveur VPN dans la conception et le prototype d'un réseau est-elle importante ?

_____

_____

_____

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez configurer un routeur 1841 en tant que serveur VPN à l'aide de l'interface utilisateur graphique de SDM et de l'assistant d'installation du serveur EasyVPN. Ce routeur est la simulation du serveur VPN dans le prototype du réseau du stade. Il doit autoriser les accès à distance. Il représente un point d'extrémité d'un tunnel VPN IPSec pour les clients VPN. Vous serez amené à tester la configuration VPN à l'aide des outils intégrés, conformément au plan de test défini précédemment au cours des travaux pratiques 8.3.2.

REMARQUE : même s'il n'existe pas d'équipement approprié pour effectuer ces travaux pratiques, vous devez en prendre connaissance pour mieux comprendre le fonctionnement des réseaux privés virtuels.

Configuration requise :

- Routeur Cisco 1841 avec image de IOS Advanced IP Services 12.4, un module VPN (réseau privé virtuel) et SDM version 2.4 (installé)
- Ordinateur Windows XP avec Internet Explorer 5.5 ou version ultérieure et SUN Java Runtime Environment (JRE) version 1.4.2_05 ou ultérieure (ou Java Virtual Machine (JVM) 5.0.0.3810).
- Accès à la configuration TCP/IP de réseau du PC et ligne de commande
- Câble console avec adaptateur DB-9 ou RJ-45
- Câblage conforme à la topologie et au plan de test présentés dans les travaux pratiques 8.3.2

Tâche 1 : conception du réseau et configuration des périphériques pour un accès SDM

Étape 1 : configuration de base du routeur pour accéder à SDM

REMARQUE : si les PC utilisés au cours de ces travaux pratiques sont également reliés au réseau local de votre établissement ou à Internet, notez bien les raccordements des câbles et les paramètres TCP/IP pour pouvoir les rétablir à la fin des exercices.

a. Reliez le PC au port console du routeur à l'aide d'un câble console doté d'un adaptateur DB-9/RJ-45. En mode d'exécution privilégié, utilisez les commandes **`erase startup-config`** et **`reload`** pour supprimer les configurations existantes.

b. Configurez les paramètres de base du routeur avec SDM.

```
Router(config)#hostname VPN
VPN(config)#line console 0
VPN(config-line)#password cisco
VPN(config-line)#login
VPN(config-line)#line vty 0 4
VPN(config-line)#password cisco
VPN(config-line)#login
VPN(config-line)#enable password cisco
VPN(config)#enable secret class
VPN(config)#no ip domain-lookup
VPN(config)#
VPN(config)#interface Fa0/0
VPN(config-if)#ip address 10.10.10.1 255.255.255.248
VPN(config-if)#no shutdown
VPN(config-if)#
VPN(config-if)#ip http server
VPN(config)#ip http authentication local
VPN(config)#username admin privilege 15 password 0 cisco123
VPN(config)#end
```

c. Enregistrez la configuration actuelle (**`running-config`**) dans la configuration initiale (**`startup-config`**).

Étape 2 : configuration du PC pour une connexion au routeur, puis lancement de Cisco SDM

a. Désactivez les programmes qui bloquent les fenêtres publicitaires intempestives. Ces programmes empêchent l'affichage des fenêtres SDM.

b. Connectez la carte réseau du PC au port FastEthernet 0/0 du routeur de service intégré Cisco 1841 à l'aide du câble de croisement Ethernet. Cette connexion intrabande va permettre de configurer le réseau privé virtuel à l'aide d'un navigateur sur le PC et de l'interface graphique utilisateur de SDM.

REMARQUE : un routeur SDM autre que le routeur 1841 peut nécessiter une connexion à un port différent pour accéder à SDM.

c. Attribuez l'adresse IP 10.10.10.2 au PC avec le masque de sous-réseau 255.255.255.248.

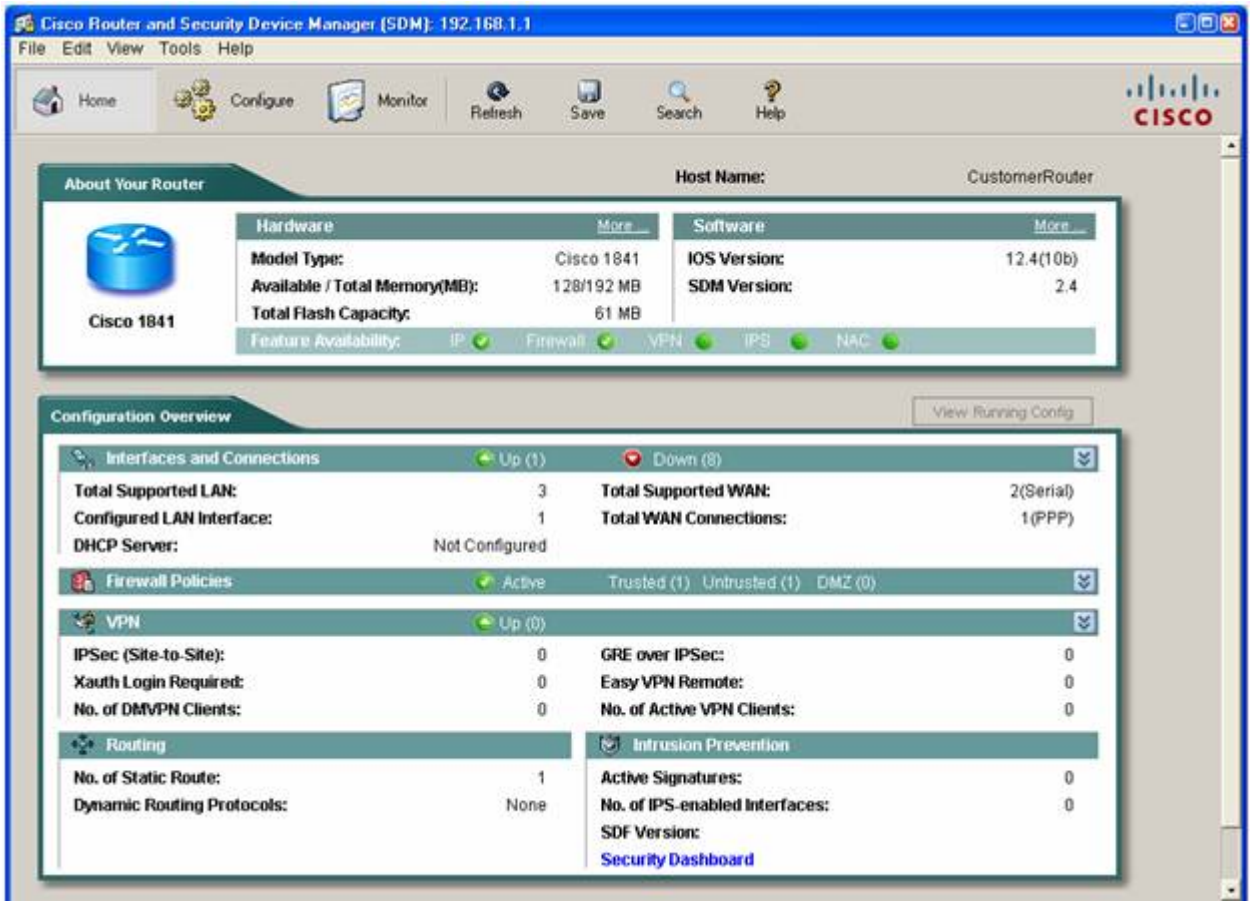
d. SDM ne se charge pas automatiquement sur le routeur. Vous devez ouvrir le navigateur Web pour y accéder. Ouvrez le navigateur Web sur le PC et connectez-vous à l'adresse URL suivante : http://10.10.10.1

e. Dans la boîte de dialogue **Connect to**, entrez **admin** comme nom d'utilisateur et **cisco123** comme mot de passe. Cliquez sur **OK**. L'application Web SDM principale démarre et vous êtes invité à utiliser le mode sécurisé HTTPS. Cliquez sur **Cancel**. Dans la fenêtre Security Warning, cliquez sur **Yes** pour accepter l'application Cisco.

f. Vérifiez que vous utilisez bien la dernière version de SDM. L'écran initial de SDM s'affichant immédiatement après la connexion indique le numéro de la version actuellement utilisée. Il s'affiche également sur l'écran principal de SDM (illustré ci-dessous) avec la version IOS.

REMARQUE : si la version actuelle n'est ni 2.4, ni une version supérieure, avertissez votre formateur avant de poursuivre ces travaux pratiques. Il vous faudra télécharger le dernier fichier .zip (http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm) et l'enregistrer sur le PC que vous utilisez pour accéder au routeur SDM. Dans le menu **Tools** de l'interface graphique utilisateur de SDM, utilisez l'option **Update SDM** pour indiquer l'emplacement du fichier ZIP et lancer la mise à jour.

Notez également que l'ordinateur Windows XP que vous utilisez doit comporter Internet Explorer 5.5 ou version ultérieure et SUN Java Runtime Environment (JRE) version 1.4.2_05 ou ultérieure (ou Java Virtual Machine (JVM) 5.0.0.3810). Si ce n'est pas le cas, vous ne pouvez pas utiliser SDM. Vous devrez télécharger et installer JRE sur le PC avant de poursuivre les travaux pratiques.



Étape 3 : configuration de SDM pour afficher les commandes de l'ILC de Cisco IOS

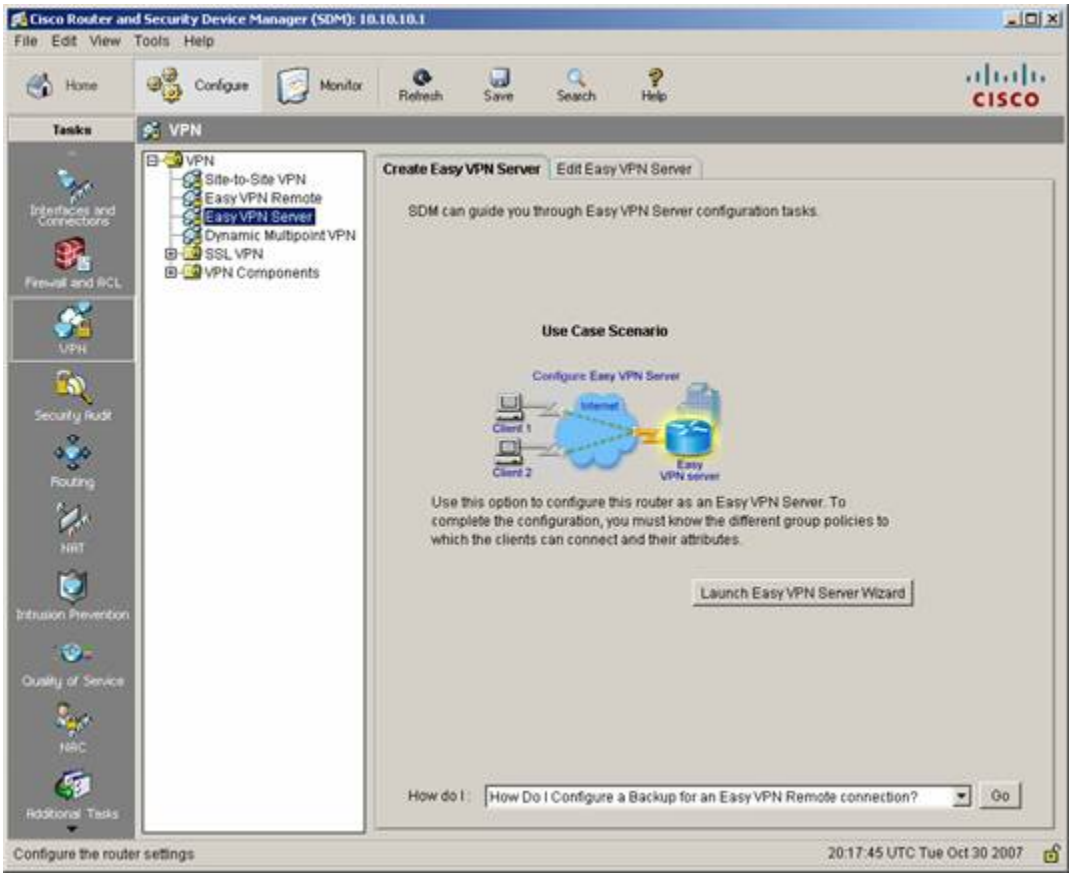
a. Dans le menu **Edit** de la fenêtre principale de SDM, sélectionnez **Preferences**.

b. Cochez la case **Preview commands before delivering to router**. Lorsqu'elle est activée, vous pouvez voir les commandes de l'ILC de Cisco IOS que vous utiliserez pour exécuter une fonction de configuration sur le routeur avant qu'elles ne lui soient transmises. Vous pouvez ainsi apprendre les commandes ILC de Cisco IOS.

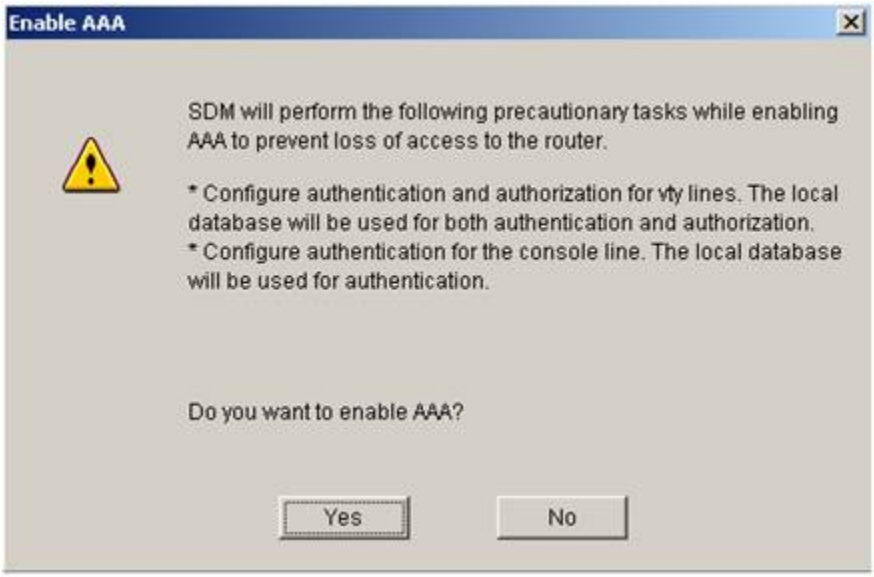
Tâche 2 : utilisation de EasyVPN pour configurer le routeur en tant que serveur VPN

Étape 1 : assistant d'installation du serveur EasyVPN

a. Dans le menu **Configure**, cliquez sur le bouton **VPN** pour afficher la page de configuration VPN. Sélectionnez **Easy VPN Server** dans la fenêtre principale et cliquez sur **Launch Easy VPN Server Wizard**.



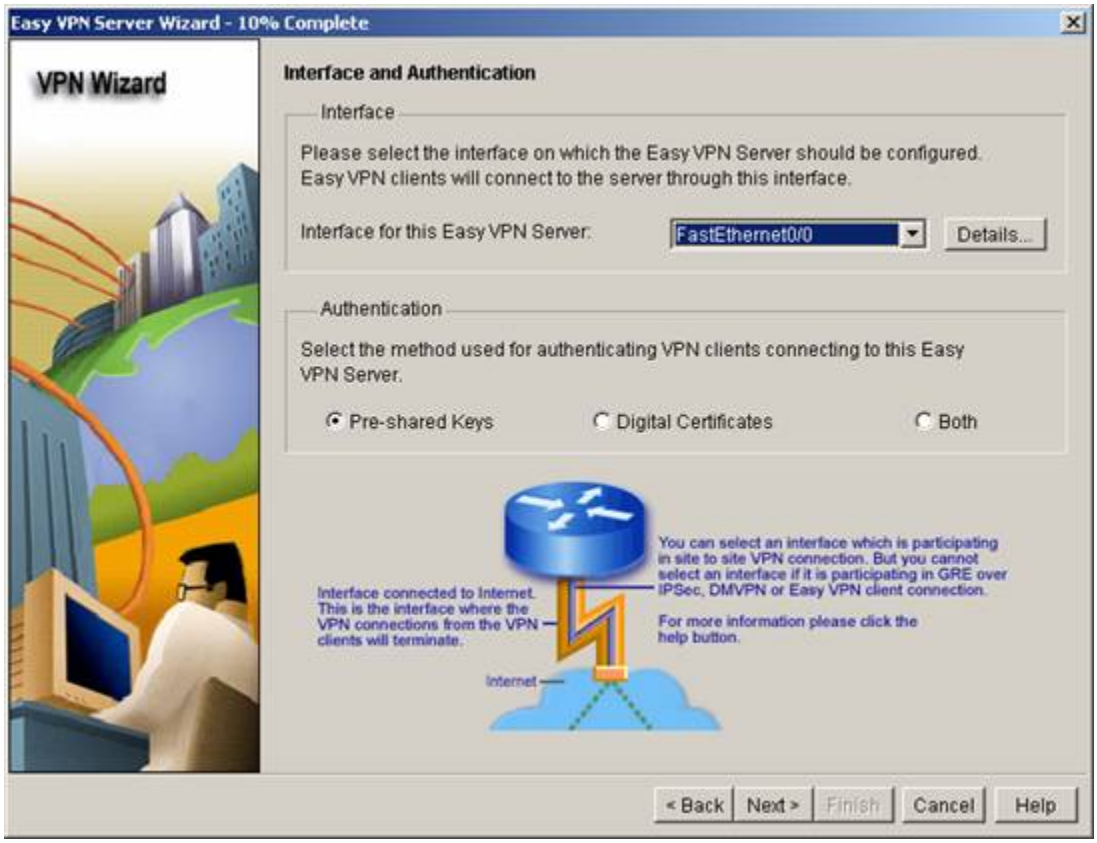
b. La fenêtre Enable AAA s'affiche. Vous devez activer le protocole AAA sur le routeur avant de configurer le serveur Easy VPN. Cliquez sur **Yes** pour continuer. Cliquez sur le bouton **Deliver** pour transmettre la configuration AAA au routeur. Un message s'affiche dans la fenêtre pour indiquer que le protocole AAA est activé sur le routeur.



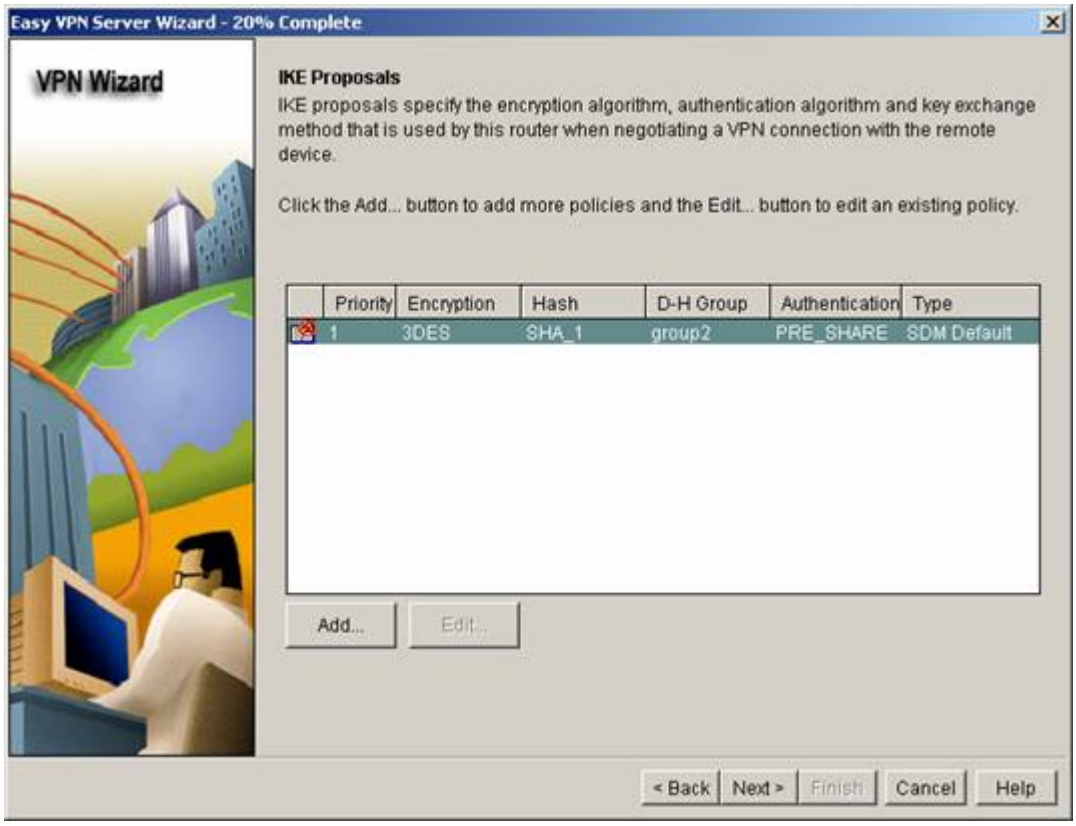
c. Cliquez sur **OK** pour afficher l'écran d'accueil de l'assistant. Cliquez sur **Next** pour démarrer l'assistant **Easy VPN Server Wizard**.

Étape 2 : sélection de l'interface et de la méthode d'authentification

a. Sélectionnez l'interface sur laquelle les connexions des clients aboutissent, ainsi que le type d'authentification. Cette connexion arrive sur l'interface Fa0/0. Elle fait intervenir des clés pré-partagées.

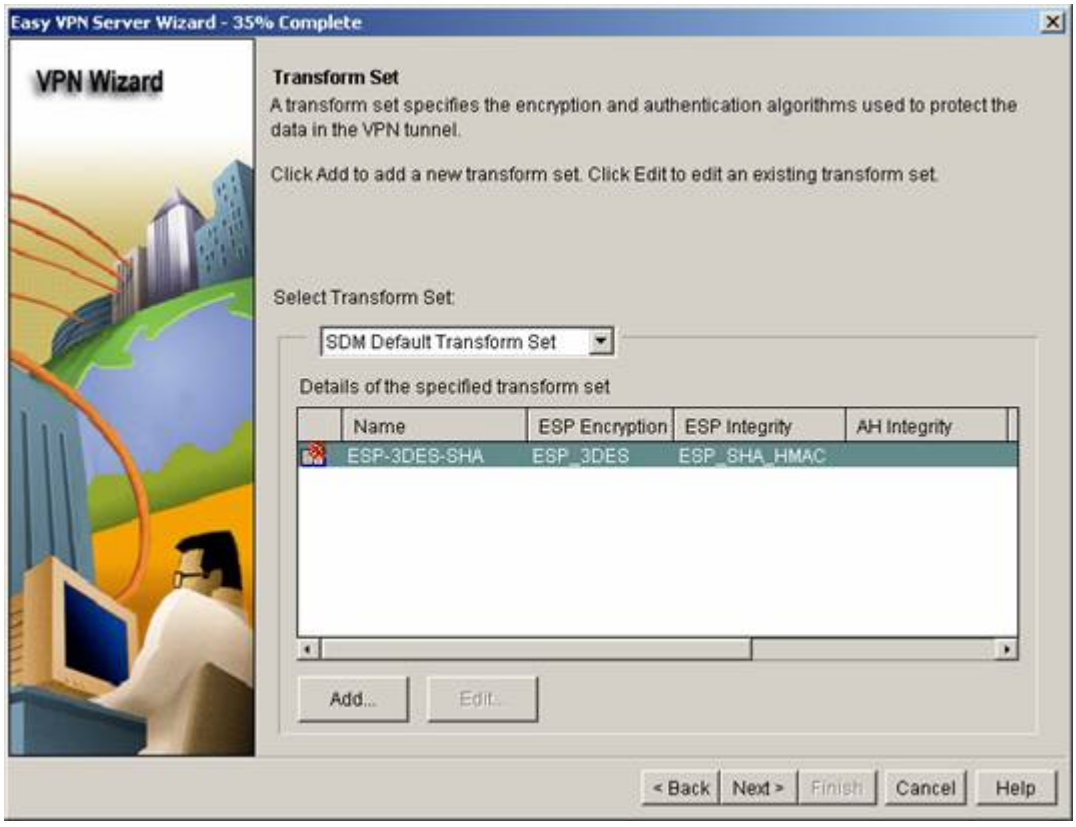


b. Cliquez sur **Next** pour configurer le protocole IKE (Internet Key Exchange). Utilisez le bouton **Add** pour créer une politique. Les configurations doivent être identiques aux deux extrémités du tunnel. Le client Cisco VPN sélectionne automatiquement la configuration appropriée. Vous n'avez donc pas besoin de configurer le protocole IKE sur le PC client.



Étape 3 : sélection d'une commande transform set

Cliquez sur **Next** pour accepter l'option par défaut pour le cryptage des données et les algorithmes d'authentification.



Étape 4 : définition des autorisations de groupes et recherche d'une politique

Cliquez sur **Next** pour créer une liste de méthodes d'authentification AAA (Authentication, Authorization, and Accounting) et rechercher une politique de groupe. Conservez l'option par défaut **Local**.

Étape 5 : configuration de l’authentification de l’utilisateur (XAuth)

a. Vous pouvez enregistrer les paramètres d’authentification de l’utilisateur sur un serveur externe (par exemple, un serveur RADIUS) ou dans une base de données locale, ou les deux. Cochez la case **Enable User Authentication** et acceptez l’option par défaut **Local Only**.

b. Cliquez sur le bouton **Add User Credentials** pour afficher les utilisateurs enregistrés ou pour en rajouter.

Quel est le nom de l’utilisateur enregistré et quels sont ses droits d’accès ?

_____

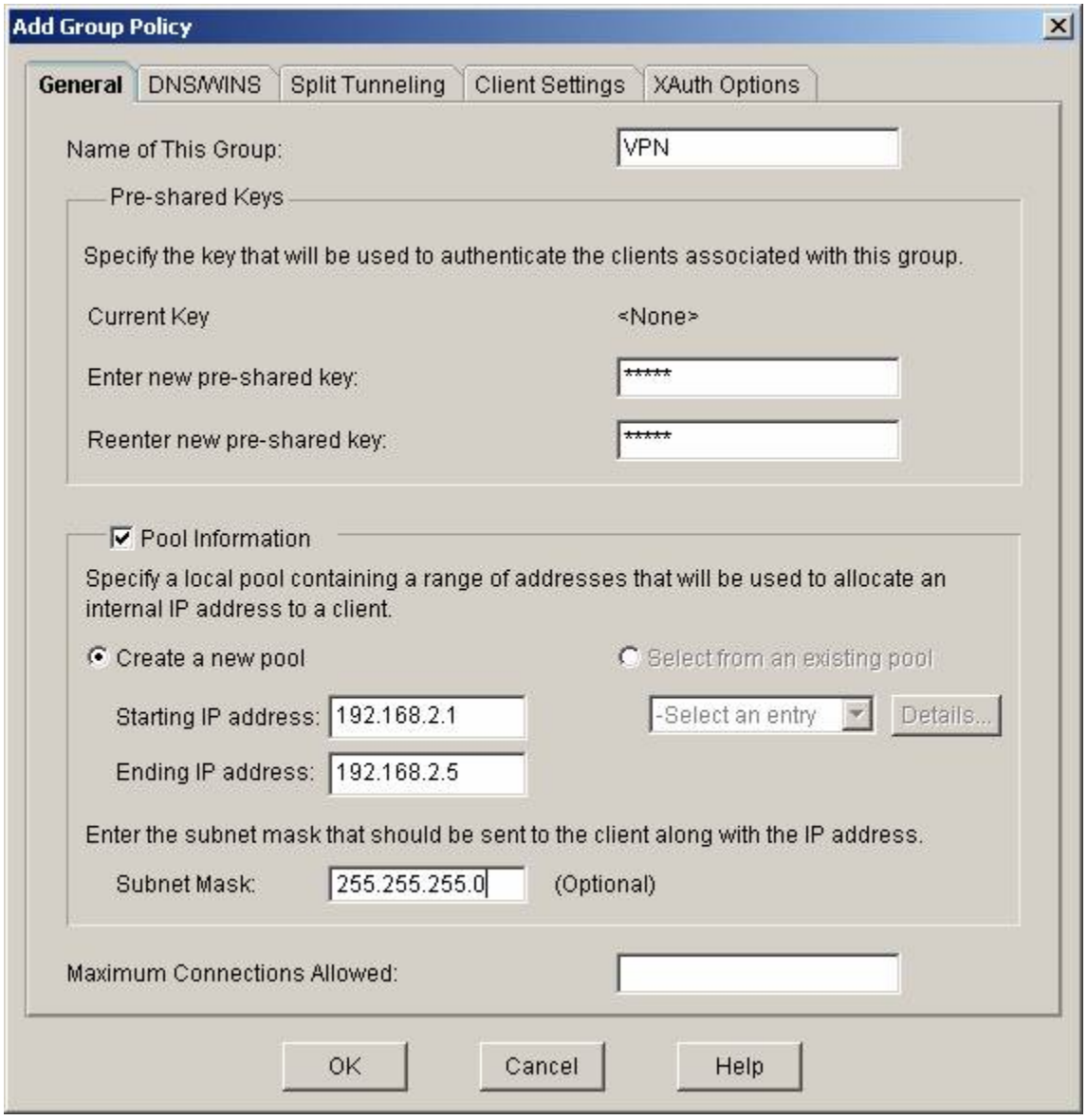
Quand cet utilisateur a-t-il été enregistré ?

_____

Étape 6 : configuration d'une politique de groupe

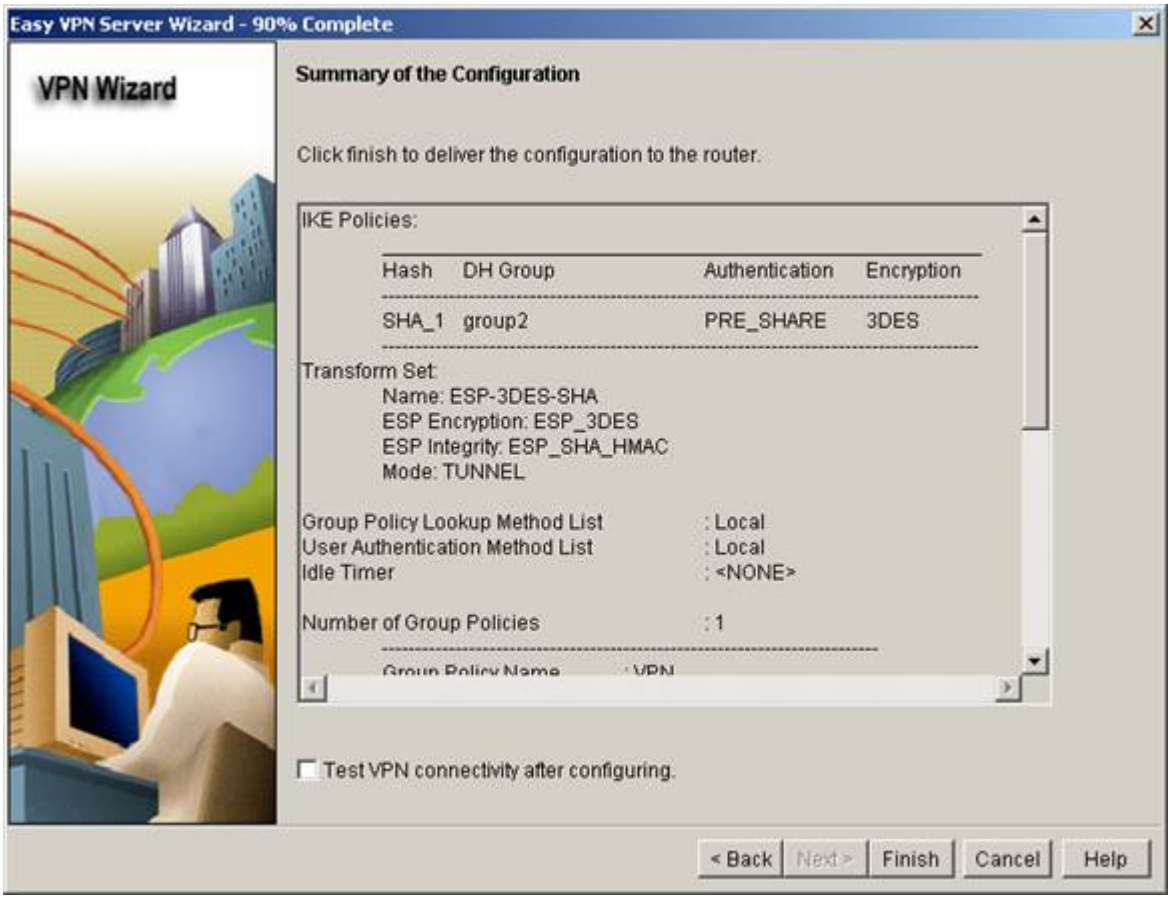
a. Cliquez sur **Next** pour afficher l'écran Group Authorization and User Group Policies. Vous devez créer au moins une politique de groupe pour le serveur VPN.

b. Cliquez sur **Add** pour créer une politique. Tapez **VPN** pour indiquer le nom de groupe du tunnel. Tapez la nouvelle clé pré-partagée **cisco** et saisissez-la à nouveau. La case Pool Information doit rester cochée. Indiquez l'adresse de début, l'adresse de fin et le masque de sous-réseau, comme indiqué ci-dessous. Cliquez sur **OK** pour valider. Dans la fenêtre Group Authorization, cliquez sur **Next**.



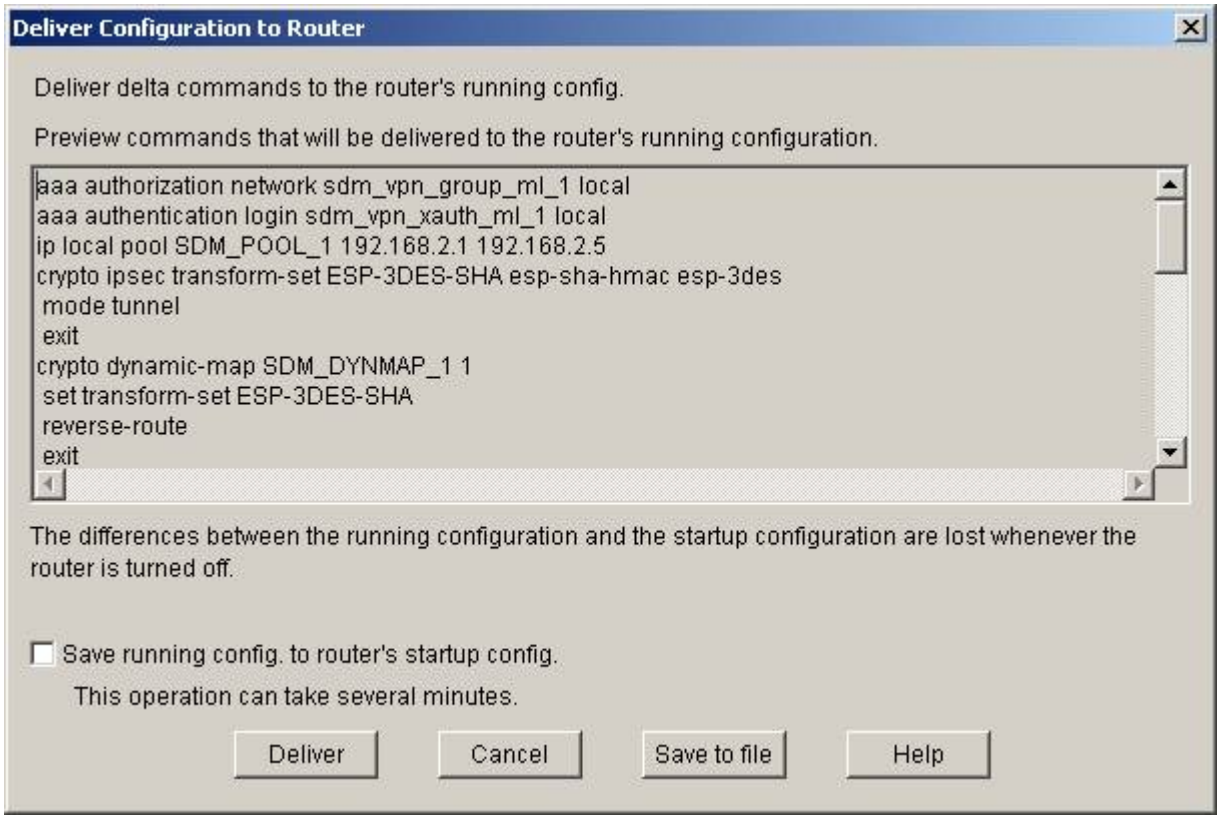
Étape 7 : récapitulatif de la configuration que vous avez créée

La zone Summary of the Configuration affiche le récapitulatif des opérations que vous avez effectuées. Cliquez sur **Finish** si la configuration vous convient.



Étape 8 : transfert de la configuration au routeur

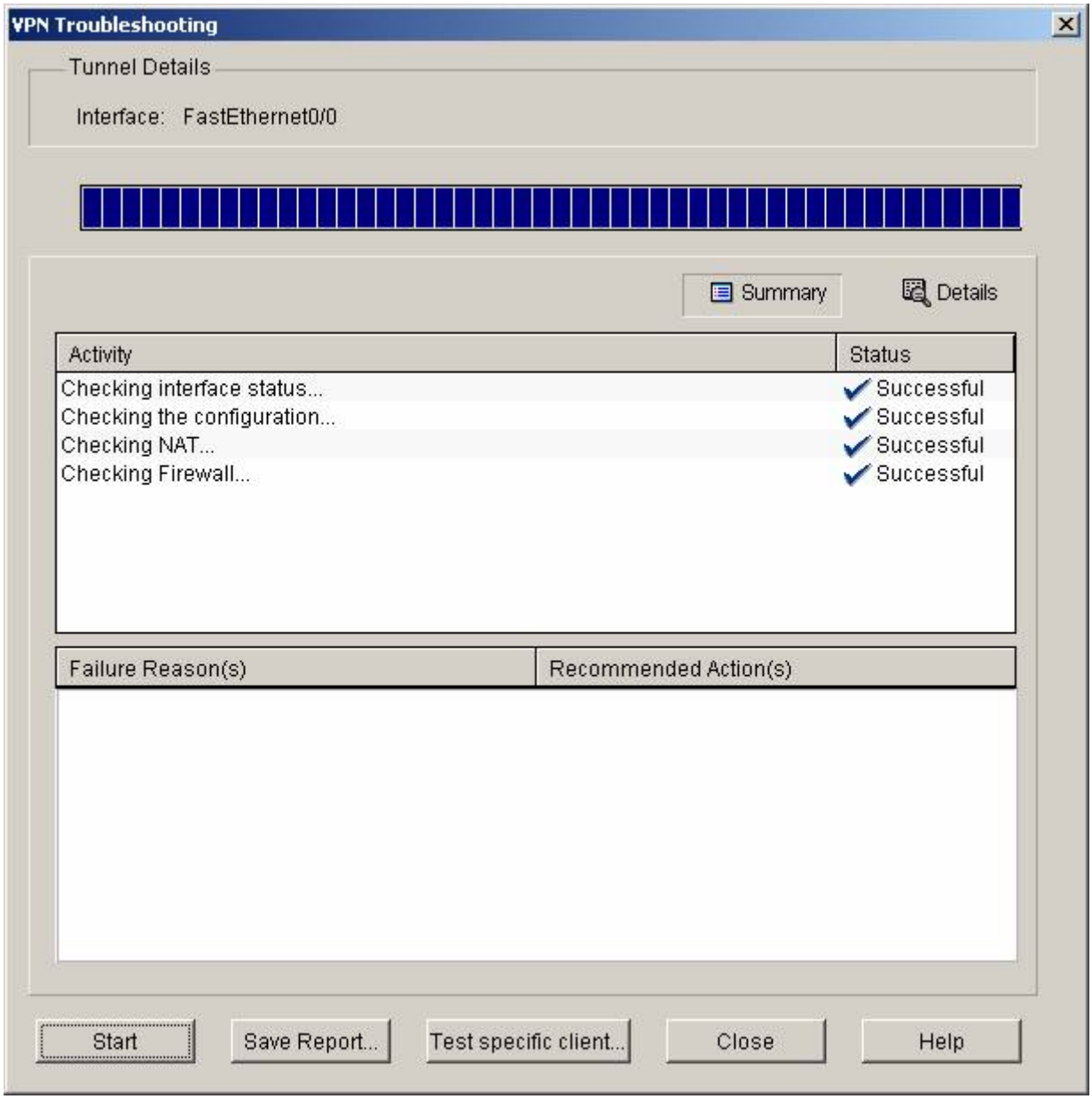
La fenêtre ci-dessous affiche les commandes IOS qui vont être transmises au routeur. Elles confirment les sélections et les saisies que vous avez effectuées. Cochez la case **Save running-config to router's startup config**. Cliquez sur **Deliver** pour transférer les commandes au routeur.



Étape 9 : test de la configuration VPN de base sur le routeur

a. Testez la configuration du réseau privé virtuel, conformément au test 1 présenté au cours des travaux pratiques 8.3.2. « Création d'un plan de test de la connectivité d'un réseau privé virtuel ».

b. Dès que les commandes sont transférées, l'écran de configuration VPN principal s'affiche à nouveau. Sélectionnez le nom de la configuration VPN que vous avez créée et cliquez sur **Test VPN Server** dans la partie inférieure droite de l'écran. Vous devez obtenir les informations suivantes :



Tâche 3 : remarques générales

Pourquoi configurer un réseau privé virtuel avec SDM EasyVPN plutôt qu'avec la ligne de commande ?

_____

_____

_____

_____

Résumez les étapes de configuration

_____

_____

_____

_____

_____

_____