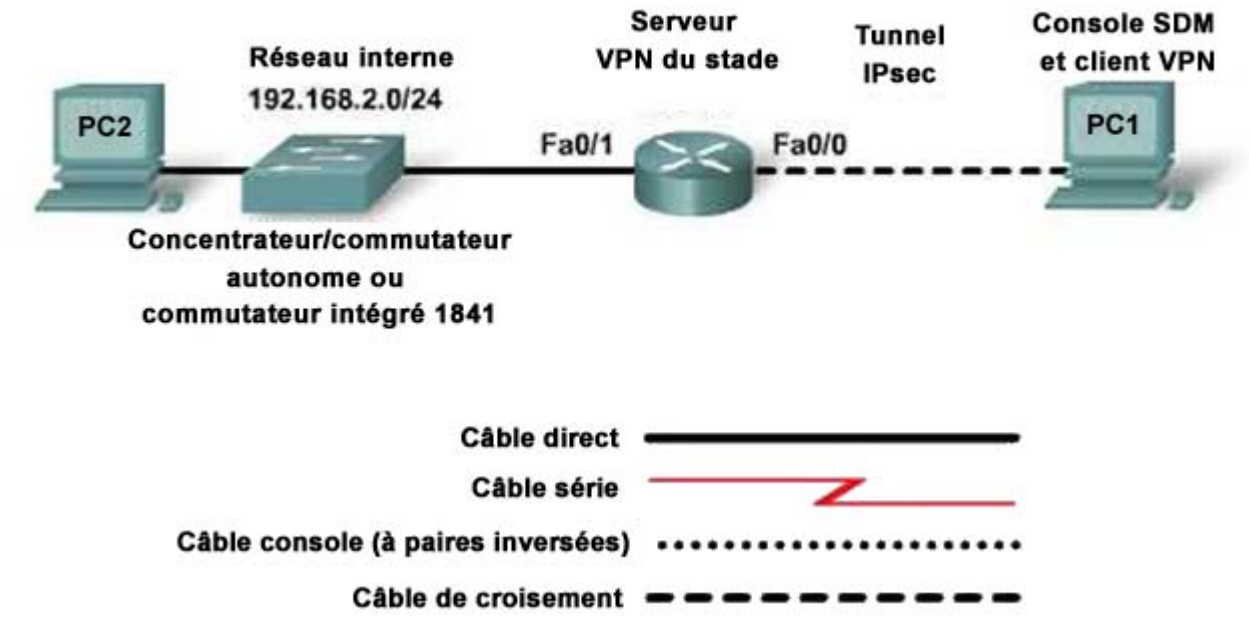
Travaux pratiques 8.3.4.4 Configuration et test d'un client VPN (facultatif)



Équipement	Nom de l'hôte	Adresse IP de l'interface FastEthernet 0/0 ou de la carte réseau	Adresse IP de l'interface FastEthernet 0/1	Passerelle par défaut	Mot de passe secret actif	Mots de passe VTY et console actifs
Routeur 1	VPN	10.10.10.1 /29	192.168.2.99 /24		class	cisco
Commutateur 1	Comm1					
Hôte 1	PC1	10.10.10.2 /29		10.10.10.1		
Hôte 2	PC2	192.168.2.6 /24		192.168.2.99		

Objectifs

- Configurer les paramètres de base du routeur à l'aide du logiciel IOS
- Configurer un client VPN pour un accès à distance
- Configurer le réseau interne
- Vérifier la configuration d'un tunnel VPN entre un client et un serveur
- Vérifier l'accès du client VPN aux ressources du réseau interne

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 d'implémenter la technologie VPN dans la conception et le prototype d'un réseau est-elle importante ?

_____

_____

_____

Contexte / Préparation

Au cours de ces travaux pratiques, vous pourrez configurer un client VPN pour simuler un accès distant aux ressources du réseau local interne du stade via un serveur VPN. Avant toute chose, vous devez effectuer les travaux pratiques 8.3.4.3 pour apprendre à configurer le serveur VPN 1841 à l'aide de l'interface graphique utilisateur et de l'assistant d'installation de EasyVPN Server. Vous allez tester l'accès du client VPN, conformément au plan de test présenté 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.

Ressources requises :

- Un routeur Cisco 1841 doté de 2 interfaces Fast Ethernet routées, ainsi que les éléments suivants :
  - Image IOS version 12.4 avec services IP avancés
  - Réseau privé virtuel (VPN)
  - SDM version 2.4 installé
  - Commutateur complémentaire à 4 ports (peut être remplacé par un concentrateur externe ou un commutateur)
- PC Windows XP à utiliser avec la configuration SDM EasyVPN en tant que client VPN doté des éléments suivants :
  - Internet Explorer 5.5 ou version ultérieure
  - SUN Java Runtime Environment (JRE) version 1.4.2_05 ou ultérieure (ou Java Virtual Machine (JVM) 5.0.0.3810)
  - Client Cisco VPN installé
- PC Windows XP ou un autre ordinateur comme hôte interne (l'utilisation du CD Discovery est possible, mais l'adressage du réseau interne doit correspondre à l'adresse 172.16.1.1/16 du serveur)
- Câble console avec adaptateur DB-9 ou RJ-45
- Accès à la configuration TCP/IP de réseau du PC et ligne de commande
- 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 : connexion des PC et des périphériques, conformément au diagramme de la topologie

a. Il est possible de connecter l'interface Fa0/1 du routeur VPN interne au commutateur Ethernet 1841 intégré (s'il est installé). Il est également possible de la relier à un concentrateur ou à un commutateur autonome.

b. Il n'est pas nécessaire de configurer le commutateur. Si vous utilisez un commutateur autonome externe, supprimez le fichier de configuration et le fichier vlan.dat. Exécutez la commande **reload** pour supprimer les configurations précédentes. Vous pouvez également mettre le commutateur hors tension, puis sous tension.

c. Connectez l'hôte PC2 au commutateur (1841 intégré ou commutateur/concentrateur autonome) qui est relié à l'interface Fa0/1 du routeur. Configurez l'adresse IP, conformément au diagramme de la topologie.

Étape 2 : configuration du routeur sous la forme d'un serveur VPN

a. L'hôte PC1 se connecte au port console du routeur dans le cas d'une configuration IOS de base et au port Fa0/0 du routeur s'il s'agit d'une configuration SDM EasyVPN. Les travaux pratiques 8.3.4.3 expliquent comment configurer un PC pour accéder à l'interface graphique utilisateur SDM du routeur. Lorsque le routeur est configuré comme un serveur VPN, l'hôte PC1 joue le rôle du client VPN.

b. Reportez-vous aux instructions figurant dans les travaux pratiques 8.3.4.3. Elles expliquent comment configurer le routeur 1841 comme un serveur VPN à l'aide des commandes IOS et de SDM. N'oubliez pas de supprimer le fichier de configuration initiale et d'exécuter la commande **reload** pour supprimer les configurations précédentes.

c. Attribuez une adresse IP du réseau local interne à l'interface Fa0/1 du serveur VPN pour obtenir la passerelle des hôtes internes.

```
VPN(config)#interface FastEthernet0/1
VPN(config-if)#ip address 192.168.2.99 255.255.255.0
VPN(config-if)#no shutdown
```

Tâche 2 : configuration du client VPN

Étape 1 : installation du client Cisco VPN

S'il ne l'est pas déjà, installez le logiciel Cisco VPN Client sur l'hôte PC1. Si vous ne disposez pas de ce logiciel ou que vous avez besoin de précisions, renseignez-vous auprès du formateur.

Étape 2 : configuration du PC comme client VPN pour accéder au serveur VPN

a. Ouvrez le programme **Cisco VPN Client** et sélectionnez **Connection Entries > New**.

b. Saisissez les informations suivantes pour définir la nouvelle entrée de connexion. Cliquez sur **Save** lorsque vous avez terminé.

Connection Entry: **VPN**

Description: **Connexion au réseau du stade**

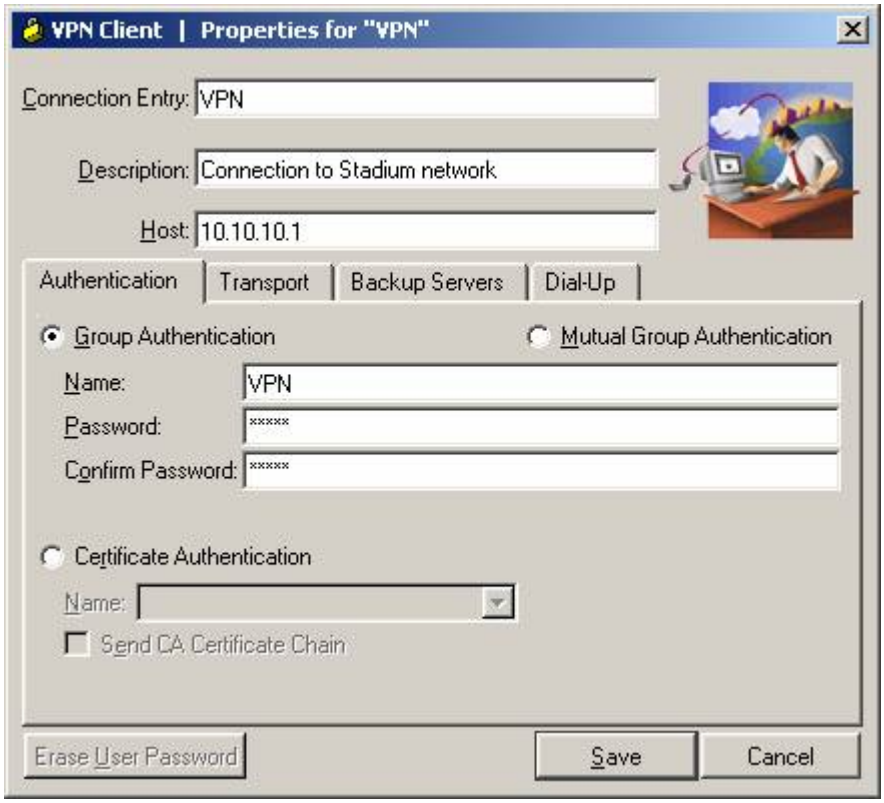
Host: **10.10.10.1**

Group Authentication Name: **VPN** (configuré au cours des travaux pratiques 8.3.4.3)

Password: **cisco** (configuré au cours des travaux pratiques 8.3.4.3)

Confirm Password: **cisco**

REMARQUE : le nom et le mot de passe sont sensibles à la casse et doivent correspondre à ceux que vous avez créés sur le serveur VPN.



c. Sélectionnez la connexion que vous venez de créer et cliquez sur **Connect**.

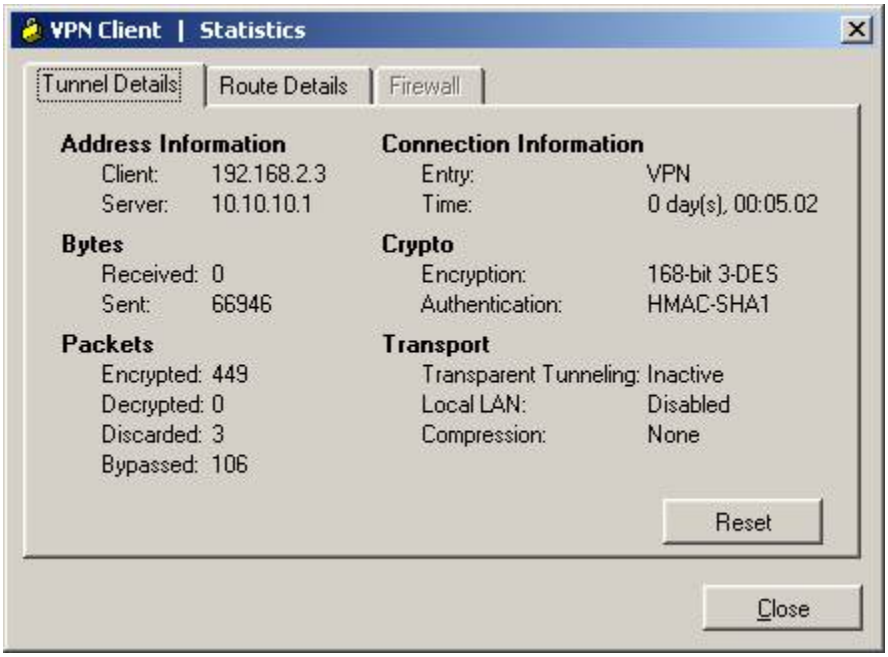
d. Tapez le nom d'utilisateur **admin** créé précédemment sur le routeur VPN, puis le mot de passe **cisco123**. Cliquez sur **OK** pour continuer. La fenêtre est icônisée dans la barre des tâches.

Tâche 3 : vérification du tunnel VPN entre le client, le serveur et le réseau interne

Effectuez les tests. Pour ce faire, reportez-vous au plan de test de la connectivité VPN (test 2) défini au cours des travaux pratiques 8.3.2, ainsi qu'aux instructions ci-après.

Étape 1 : vérification des statistiques relatives au tunnel

Affichez la fenêtre du client VPN et sélectionnez le menu **Status**, puis l'option **Statistics** pour afficher la page d'options Tunnel Details.



Quelle est l'adresse IP du client que vous obtenez du serveur VPN ?

_____

Quelle est l'adresse du serveur VPN ? _____

Quel est le nombre de paquets chiffrés ? _____

Quelle est la méthode de chiffrement employée ? _____

Quelle est la méthode d'authentification employée ? _____

Étape 2 : affichage de la fenêtre d'invite de commandes et vérification de la connexion VPN

Cliquez sur **Démarrer > Exécuter,** puis tapez **cmd** et appuyez sur la touche **Entrée**. Utilisez la commande **`ipconfig /all`** pour afficher les connexions réseau actives.

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : PC1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 1:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network
Connection
        Physical Address. . . . . . . . . : 00-07-E9-63-CE-53
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.10.10.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.248
        Default Gateway . . . . . . . . . : 10.10.10.1

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Cisco Systems VPN Adapter
        Physical Address. . . . . . . . . : 00-05-9A-3C-78-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.2.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.4
```

Quelle est la configuration IP de la première connexion au réseau local ?

Adresse IP : _____

Masque de sous-réseau : _____

Passerelle par défaut : _____

Description : _____

Quelle est la configuration IP de la deuxième connexion au réseau local ?

Adresse IP : _____

Masque de sous-réseau : _____

Passerelle par défaut : _____

Description : _____

Étape 3 : test de connectivité entre le client VPN distant et le réseau interne du stade

Exécutez la commande ping sur l'hôte PC1 externe (distant) pour interroger l'hôte PC2 (adresse IP 192.168.2.6) sur le réseau interne du stade et simuler un accès aux ressources internes.

Les requêtes ping sont-elles concluantes ? _____ Dans le cas contraire, procédez aux ajustements nécessaires.

```
C:\>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=1ms TTL=64
Reply from 192.168.2.6: bytes=32 time<1ms TTL=64
Reply from 192.168.2.6: bytes=32 time<1ms TTL=64
Reply from 192.168.2.6: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tâche 4 : remarques générales

Pourquoi un réseau privé virtuel est-il un bon choix pour les utilisateurs distants ?

_____

_____

_____

_____

Que se passe-t-il lorsque le protocole de transmission tunnel du client VPN ou le chiffrement n'est pas compatible avec ceux du serveur VPN ?

_____

_____