Mise en œuvre d'une connexion VPN

Public(s)	Section de BTS SIO 2ème année option :SISR
Savoir(s)	C21 Installer et configurer un microordinateur C22 Installer et configurer un réseau C31 Assurer les fonctions de base de l'administration d'un réseau Techniques d'accès, et de contrôle, normes et standards Câblage, connectique et électronique active, normes et standards de fait Techniques de commutation, de routage et d'adressage, normes et standards de fait Notion PKI
Capacité(s)	C22 Installer et configurer un réseau C26 Installer un périphérique Routage accès distant
Objectif(s)	• Relier deux sites par une connexion Internet crypté • L'accès distant d'un client aux serveurs situés dans un autre réseau privé

Théorie et mise en œuvre d'un VPN simple

Introduction

Un **VPN** (*Virtual Private Network*) ou RPV (Réseau Privé Virtuel), permet de déployer des communications sécurisées entre différents sites distants d'une entreprise, au travers d'un réseau partagé public (Internet par exemple…), selon un mode qui émule une liaison privée **point à point**. Il permet ainsi à deux ordinateurs de communiquer via Internet, comme s'il existait entre eux un réseau privé dédié

Pour émuler et sécuriser cette liaison point à point, les données sont encapsulées et munies d'un en-tête qui contient les **informations de routage**, ce qui leur permet de traverser le réseau partagé ou public jusqu'à destination finale. Pour émuler une liaison privée, les données sont cryptées à des fins de confidentialité. Les paquets qui seraient éventuellement interceptés sur le réseau partagé ou public sont donc indéchiffrables.

Composants d'un réseau privé virtuel

Un réseau privé virtuel comporte au minimum un **serveur VPN**, un **client VPN**, une **connexion VPN** (la partie de la connexion où les données sont cryptées) et **un tunnel** (la partie de la connexion où les données sont encapsulées). La tunellisation est effectuée par le biais d'un protocole de tunellisation ; protocole installé sous Windows 2003, avec le service Routage et accès distant ou RRAS (*Routing and Remote Access*). Ces protocoles de tunellisation sont – en ce qui concerne Windows :

- **PPTP** (*Point-to-Point Tunneling Protocol*) qui assure le cryptage des données à l'aide du cryptage point à point Microsoft.
- **L2TP** (*Layer Two Tunneling Protocol*)/**IPSec** qui assure le cryptage, l'authentification et l'intégrité des données.

Les protocoles du VPN

Différences entre PPTP et L2TP/IPSec

Le protocole **PPTP** utilise la méthode de chiffrement **MPPE** (*Microsoft Point to Point Encryption*) qui permet de chiffrer sur 40, 56 et 128 bits ; tandis que **L2TP** est basé sur **IPSec** (*Internet Protocol Security*). Toutefois les VPN peuvent intégrer dorénavant des protocoles de sécurité plus élaborés tels que **SSL** (*Secure Socket Layer*)…

Voici un tableau des principales caractéristiques des protocoles PPTP et L2TP

Caractéristiques	PPTP	L2TP
Compression d'en-tête	Non	Oui
Authentification du tunnel	Non	Oui
Cryptage intégré	Oui	Non
Transmission sur des réseaux basés sur IP	Oui	Oui
Transmet sur des réseaux basés sur UDP, Frame Relay, X.25 ou ATM	Non	Oui

Principales différences entre PPTP et L2TP

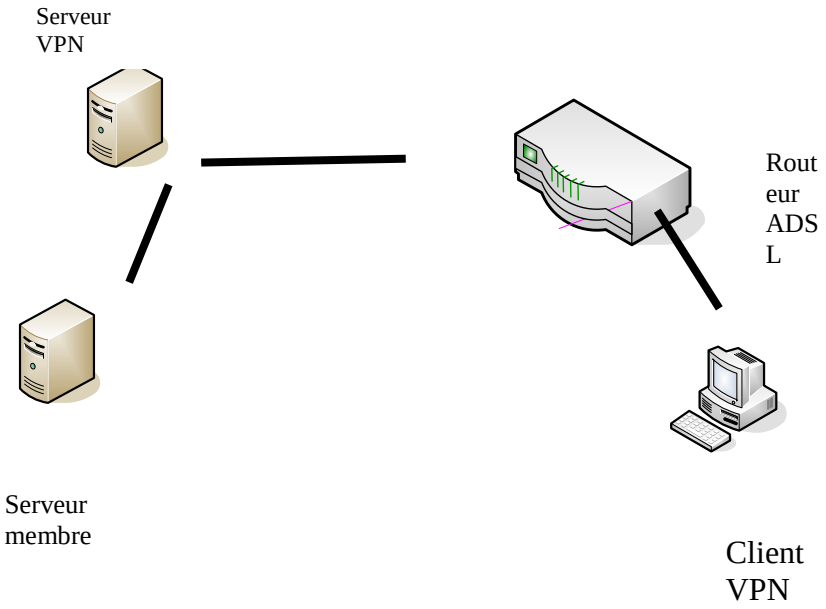
Contrôle du filtrage des paquets

Si l'entreprise possède un firewall pour protéger son réseau il va falloir autoriser le passage du trafic sur le port 1723 via TCP, du firewall vers le serveur VPN et vice versa.

Partie I Mise en œuvre de VPN client - Serveur

Pour cet exemple de mise en œuvre d'un VPN simple, nous allons utiliser quatre postes.

- Un **client VPN** en Windows XP Pro, **CLIENT** d'adresse 192.168.0.3/24
- Un **routeur ADSL** en Windows Server 2003, avec 2 interfaces :
  - une sur le réseau local privé : 192.168.0.2/24
  - l'autre sur le réseau « public » 12.0.0.2/8.
- Un **serveur VPN** en Windows Server 2003, **VPN**, avec deux interfaces : 12.0.0.1/8 et 172.16.0.1
- Un serveur membre avec une seule interface 172.16.0.2



Dans ce TP le poste faisant office de serveur VPN possède une interface vers Internet (ADSL, câble…) et c'est via cette interface que les clients VPN distants se connecteront. Le serveur VPN dispose aussi d'une interface vers le réseau local et sert de routeur vers ce réseau local.

Attention : pour le TP vous devez être en **Workgroup**. Il est possible de faire du VPN avec des postes en domaine mais on aurait des options de configuration différentes, liées notamment au niveau fonctionnel du domaine…

I) Infrastructure :

1a) Compléter le schéma réseau des IP de différents postes puis cloner les postes en full pour construire l'infrastructure

1b) Configurer les IP de postes

1c) Renommer les postes (client, adsl, vpn, serveur)

1d) Compléter les tables de routage des routeurs avec l'option persistante

1e) Activer le service routage

1f) Tester la connectivité par le protocole ICMP

1g) Sur le serveur membre, créer un dossier puis le partager (partage et sécurité, tout le monde, contrôle total)

1h) A partir du poste client, vérifier si on peut voir le poste serveur et son partage.
OUI ou NON

1i) A partir du poste client, créer un lecteur réseau par l'IP puis par le nom.

Résultat OUI ou NON

II) Installation du serveur VPN

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Serveur VPN**.

Le serveur VPN doit disposer d'un lot d'adresses IP à attribuer à l'interface « virtuelle » du serveur VPN et aux clients VPN au cours de la phase de négociation **IPCP** (*IP Control Protocol*) du processus de connexion. Avec les serveurs VPN Windows les adresses IP des clients VPN sont délivrées par défaut par un serveur DHCP mais on peut aussi choisir de définir un groupe d'adresses IP statiques.

Le serveur VPN doit également être configuré au besoin avec les adresses des serveurs de résolution de noms (DNS et/ou WINS) à attribuer au client VPN lors de la négociation IPCP.

Pour installer et activer le serveur VPN, procédez comme suit :

1. Désactivez le service « Pare-feu Windows/Partage de connexion Internet ».
2. Faites **Démarrer**, **Programmes**, **Outils d'administration**, **Routage et accès distant** ce qui va ouvrir la console MMC (*Microsoft Managment Console*) de Routage et Accès Distant.
3. Faites un clic droit sur le nom du serveur qui apparaît dans l'arborescence (ou **Action**, **Ajouter un serveur…** et sélectionnez le serveur en cours si aucun n'apparaît dans la console), puis cliquez sur **Configurer et activer le routage et l'accès distant** et sur « Suivant » (si le service « Routage et accès distant » est déjà installé désactivez le avant de le réactiver.

4. Sélectionnez, dans la boîte de dialogue « Configuration », « Accès à distance (connexion à distance ou VPN) », puis cliquez sur « Suivant ».
5. Cochez, dans la boîte de dialogue « Accès distant », l'option « VPN » puis cliquez sur « Suivant ».
6. Sélectionnez, dans la boîte de dialogue « Connexion VPN », l'interface connectant le serveur à Internet (12.0.0.1 dans notre cas), laissez cochée la case « Autoriser la sécurité sur l'interface sélectionnée… » puis cliquez sur « Suivant ».
7. Sélectionnez, dans la boîte de dialogue « Attribution d'adresses IP », « A partir d'une étendue d'adresse spécifiée » afin de ne pas utiliser un éventuel serveur DHCP mais de définir vous-même la plage d'adresses statiques affectées aux clients d'accès distant, puis cliquez sur « Suivant ».
8. Cliquez, dans la boîte de dialogue « Assignation de plage d'adresses », sur « Nouveau… » puis entrez comme adresses de départ et de fin **10.0.0.101** et **10.0.0.105** ce qui autorise **5** clients VPN à se connecter au serveur. Cliquez sur « OK » puis sur « Suivant ».
9. Sélectionnez, dans la boîte de dialogue « Gestion des serveurs d'accès distant multiples », l'option « Non, utiliser Routage et accès à distance pour authentifier les requêtes de connexion ». Cliquez sur « Terminer ».
10. Cliquez sur « OK » si un message s'affiche, signalant de mettre en œuvre un éventuel relais DHCP. Le serveur VPN démarre. Patientez un peu…

Attention : si, à la suite de manipulations « hasardeuses », le service **Routage et accès distant** du serveur VPN est inaccessible, il peut être nécessaire de le désactiver puis de le réactiver et de **reconfigurer la stratégie de sécurité par défaut**. Voir en fin de TP : « **Reconfigurer le service Routage et accès distant** ».

III) Autoriser les appels entrants

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Serveur VPN**.

Par défaut, personne (pas même l'administrateur) n'est autorisé à recevoir des appels entrants sur le serveur au moyen d'une connexion VPN ou d'un accès distant quelconque et non protégé. Il faut en effet configurer les propriétés de connexion à distance sur les comptes utilisateurs et les stratégies d'accès distant pour l'accès distant au réseau et les connexions VPN. Ces autorisations d'accès entrants peuvent être gérées de diverses manières. Nous allons commencer par la plus simple, l'accès par un **compte d'utilisateur**.

Accès distant géré au niveau de l'utilisateur.

1. Utilisez **Gestion de l'ordinateur** (ou l'**Active Directory** si vous êtes en domaine) pour afficher les propriétés du compte de l'utilisateur : **Administrateur**.
2. Cliquez sur l'onglet « Appel entrant ».
3. Sélectionnez les options « Autoriser l'accès » et « Pas de rappel » puis cliquez sur « OK ».

IV) Installation du client VPN

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Client VPN**.

Création d'une connexion d'accès distant

1. Faites un clic droit sur l'icône **Favoris réseau**, cliquez sur **Propriétés**, faites un double clic sur l'icône « Assistant Nouvelle Connexion » puis cliquez sur « Suivant ».
2. Sélectionnez l'option « Connexion au réseau d'entreprise » qui permet d'établir une connexion VPN puis cliquez sur « Suivant ».
3. Sélectionnez l'option « Connexion réseau privé virtuel » puis cliquez sur « Suivant ».
4. Saisissez le nom **Accès VPN** dans la zone « Nom de la société » puis cliquez sur « Suivant ».
5. Saisissez l'adresse IP du serveur VPN (soit **12.0.0.1** dans notre cas) puis cliquez sur « Suivant ». Bien entendu si un serveur DNS est en service et correctement configuré, on peut entrer le nom du serveur VPN au lieu de son adresse.
6. Sélectionnez l'option « Mon utilisation uniquement » puis cliquez sur « Suivant » et sur « Terminer ».
7. Saisissez, dans la boîte de dialogue qui s'affiche, le nom d'utilisateur et le mot de passe d'un utilisateur autorisé à accéder au **serveur VPN**, **Administrateur** et **son mot de passe** (s'il s'agit d'un login valide **sur le serveur VPN**) puis cliquez sur « Se connecter » (vous pouvez choisir de conserver le nom et le mot de passe en cochant la case appropriée).

Après quelques instants un message vous signalant que vous êtes connecté doit s'afficher.

8. Faites un double clic sur l'icône « Accès_VPN » et cliquez sur l'onglet « Détails ».

- Quel est le type de serveur utilisé ?
- Quel est le service de transport utilisé ?
- Quelle méthode d'authentification est utilisée ?
- Quelle est la méthode de cryptage utilisée ?
- Quelle adresse IP a été attribuée au client d'accès distant ?

9. Cliquez sur « Fermer », faites un clic-droit sur l'icône « Accès_VPN » puis **Se déconnecter**.

V) Teste l'accès VPN

5a) Enlever l'IP passerelle sur le serveur membre.

5b) Tester la connectivité par le protocole ICMP

5c) A partir du poste client, vérifier si on peut voir le poste serveur et son partage.

OUI ou NON

5d) A partir du poste client, créer un lecteur réseau par l'IP puis par le nom.

Résultat OUI ou NON

VI) Optimisation et sécurisation du serveur VPN

Afin d'améliorer les performances et la sécurité de la connexion VPN, il est possible de procéder à quelques « réglages ». Comme ce TP n'est qu'une « approche » du VPN, nous allons juste procéder à quelques manipulations simples.

Limitation au seul protocole PPTP

Les deux protocoles d'accès distant proposés par défaut sont PPTP et L2TP/IPSec. Nous allons décider, pour l'exemple, de n'exploiter que le seul protocole PPTP et empêcher l'utilisation du protocole L2TP en réduisant à zéro le nombre de ports qui lui sont affectés et en désactivant tous les accès pour ce protocole. Nous allons également réduire le nombre de ports PPTP à exploiter (un port par connexion) en fonction du nombre d'utilisateurs, mais aussi en fonction du débit du réseau et du processeur (le cryptage étant gourmand en ressources).

Un port permet au client de se connecter au serveur et le nombre de ports configurés dépend donc du nombre d'adresse IP laissées à disposition dans la plage d'adresses configurée plus haut. Pour ne pas saturer le serveur VPN il est conseillé d'augmenter le nombre de ports libres au fur et à mesure de la mise en œuvre du VPN, tout en procédant à des mesures éventuelles via l'analyseur de performance ou un autre outil adapté.

Réduire le nombre de ports ouverts

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Serveur VPN**.

Commençons par afficher les propriétés des ports du serveur VPN dans la console MMC.

1. Faites si besoin, **Démarrer**, **Programmes**, **Outils d'administration**, **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant ».
2. Développez les propriétés du serveur en cliquant sur la petite croix d'extension. Observez que la ligne « Clients d'accès distant » qui doit afficher (0) si votre client est bien déconnecté (au besoin cliquez sur cette ligne pour réactualiser l'affichage).
3. Cliquez sur le nœud « Ports » et observez, dans la partie droite de la fenêtre, la liste de tous les ports disponibles (128 par défaut pour chaque protocole).
4. Faites un clic droit sur le nœud « Ports » et cliquez sur **Propriétés**.
5. Sélectionnez, dans la boîte de dialogue **«** Propriétés de Ports », le périphérique **Miniport réseau étendu WAN (L2TP)**, puis cliquez sur « Configurer… ».
6. Décochez, les deux cases « Connexion d'accès distant (uniquement entrantes) » et « Connexion de routage à la demande (entrantes et sortantes) » et saisissez, dans la zone « Nombre maximum de ports : », la valeur **0** comme nombre maximum de connexions L2TP simultanées autorisées.
7. Cliquez sur « OK ». Un message signalant que vous tentez de réduire le nombre de ports s'affiche. Confirmez que vous portez le nombre de ports L2TP à 0 en cliquant sur « Oui ».
8. Faites un double clic sur le périphérique « Miniport réseau étendu (PPTP) » (ou sélectionnez la ligne et cliquez sur « Configurer… »).
9. Saisissez, dans la zone « Nombre maximum de ports : », la valeur **5** (ce nombre de connexions dépendra du nombre d'adresses IP à distribuer aux clients VPN). Vérifiez que les 2 cases « Connexion d'accès distant (uniquement entrantes) » et « Connexion de routage à la demande (entrantes et sortantes) » sont **cochées** puis cliquez sur « OK ».

10. Confirmez que vous souhaitez réduire le nombre de ports PPTP en cliquant sur « Oui » au message qui s'affiche.
11. Refermez la boîte de dialogue « Propriétés de Ports » en cliquant sur « OK ».
12. Cliquez sur le nœud « Ports » et rafraîchissez l'affichage (F5) ou patientez quelques secondes et observez que le nombre de lignes « Miniport réseau étendu WAN (PPTP) » a bien été réduit.

Activer le protocole EAP

Le service Routage et accès distant propose plusieurs protocoles pour authentifier les utilisateurs distants, donnés ici en ordre décroissant de sécurisation :

- **EAP** (*Extensible Authentification Protocol*) qui est un mécanisme **d'authentification** qui permet de valider une connexion d'accès distant.
- **MS-CHAP v2** est une amélioration du protocole MS-CHAP avec des clés de cryptage plus fortes et une authentification mutuelle entre le client et le serveur d'accès distant.
- **MS-CHAP** (Microsoft CHAP) plus ancien, qui est un protocole propriétaire Microsoft basé sur CHAP utilisant le protocole de cryptage **MPPE** (*Microsoft Point-to-Point Encryption*).
- **CHAP** (*Challenge Handshake Authentification Protocol*) qui autorise le cryptage des mots de passe envoyés du client au serveur d'accès distant.
- **SPAP** (*Shiva Password Authentification Protocol*) qui permet aux postes clients équipés avec du matériel de marque Shiva de se connecter au serveur d'accès distant. Les mots de passe sont protégés par un cryptage réversible (faible sécurité).
- **PAP** (*Password Authentification Protocol*) qui est un protocole non sécurisé où identifiants et mots de passe sont transmis sans cryptage entre le client et le serveur d'accès distant.

Le modèle d'authentification utilisé par **EAP** est négocié entre le **client d'accès distant** et le **serveur d'authentification** (le serveur VPN lui-même ou un serveur tiers **IAS** (*Internet Authentication Service*). EAP prend en charge divers modèles d'authentification tels que Generic Token Card, MD5-Challenge, TLS (*Transport Level Security*), S/Key…

Les échanges entre le client d'accès distant et le serveur d'authentification sont composés de demandes (défi, *challenge*…) d'authentification émanant du serveur d'authentification et de réponses (*response…*) provenant du client. Par exemple, si EAP est utilisé avec des cartes à jeton de sécurité, le serveur d'authentification peut demander au client un nom, un code confidentiel et un jeton de carte. Après chaque question/réponse, le client passe au niveau suivant d'authentification. Quand toutes les questions ont fait l'objet d'une réponse satisfaisante, le client est considéré comme authentifié.

Un modèle d'authentification EAP s'appelle un **type EAP**. Le client d'accès distant et le serveur d'authentification doivent tous les deux prendre en charge le **même type EAP** pour que l'authentification soit réussie. Windows offre une infrastructure EAP, divers types EAP (EAP-MD5 CHAP, EAP-TLS…) et la possibilité de transmettre des messages EAP à un serveur d'authentification RADIUS (EAP-RADIUS). RADIUS (*Remote Authentication Dial-In User Service*) étant un protocole client/serveur d'authentification de sécurité.

Après cette séquence « culture » passons à la mise en place de EAP sur notre serveur VPN.

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Serveur VPN**.

1. Faites si besoin, **Démarrer**, **Programmes**, **Outils d'administration**, **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant ».
2. Faites un clic-droit sur le nom du serveur pour lequel vous souhaitez configurer le protocole EAP, puis cliquez sur **Propriétés**.
3. Cliquez, dans l'onglet « Sécurité », sur le bouton « Méthodes d'authentification… ».

4. Vérifiez que les cases « Protocole EAP (Extensible Authentification Protocol) », « Authentification cryptée Microsoft version 2 (MS-CHAP v.2) » et « Authentification cryptée Microsoft (MS-CHAP) » sont **cochées**. Pour afficher les méthodes EAP installées, vous pouvez cliquer sur le bouton « Méthodes EAP… ». Cliquez sur « OK » puis sur « OK »… pour revenir à la console.

Mise en place d'une stratégie d'accès distant personnalisée

Afin de sécuriser une connexion VPN il est possible de lui appliquer diverses stratégies de sécurité (limiter la plage horaire autorisée aux connexions, choisir un mode de cryptage…).

Au départ il est possible que vous disposiez déjà de stratégies par défaut telles que « Connexions au serveur d'accès à distance et de routage Microsoft » ou « Connexions à d'autres serveurs d'accès ». Nous allons les supprimer et définir notre propre stratégie de sécurité VPN.

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Serveur VPN**.

1. Faites, si besoin, **Démarrer**, **Programmes**, **Outils d'administration**, **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant » et sélectionnez la ligne **Stratégies d'accès distant** dans la partie gauche de la fenêtre.
2. Sélectionnez la stratégie « Connexions à d'autres serveurs d'accès ». Vous devriez avoir en principe deux stratégies en place par défaut « Connexions au serveur d'accès à distance et de routage Microsoft » et « Connexions à d'autres serveurs d'accès ». Remarquez leur ordre d'application.
3. Faites **Action**, **Nouvelle Stratégie d'accès distant**, puis cliquez sur « Suivant ».
4. Sélectionnez l'option « Utiliser cet Assistant pour paramétrer une stratégie par défaut pour un scénario commun », saisissez dans la zone « Nom de la stratégie : » le nom : **Stratégie VPN** puis cliquez sur « Suivant ».
5. Sélectionnez l'option « VPN » comme méthode d'accès pour laquelle vous voulez appliquer une stratégie puis cliquez sur « Suivant ».
6. Sélectionnez l'option « Utilisateur » pour que la stratégie s'applique à tel ou tel utilisateur (mais on pourrait choisir l'option « Groupe » pour attribuer la stratégie à un groupe comme celui des « Commerciaux »… par exemple) puis cliquez sur « Suivant ».
7. Cochez les options « Protocole EAP (Extensible Authentification Protocol) » et « Authentification cryptée Microsoft version 2 (MS-CHAPv2) » car notre utilisateur ne pourra fournir ici que son mot de passe et son login (nous n'avons ni carte à puce de sécurité ni autre dispositif à lecture d'empreintes digitales…) puis cliquez sur « Suivant ».
8. Cochez la case « Cryptage de base (IPSec 56 bits DES ou MPPE 40 bits) » et décochez les autres options. Le cryptage sera certes moins sécurisé mais pour le TP c'est suffisant et le poste utilisera moins le processeur. Cliquez sur « Suivant » puis sur « Terminer ».
9. Faites, au besoin, un clic-droit sur notre nouvelle stratégie puis **Monter**, de façon à ce que notre stratégie personnalisée se retrouve à être exécutée en premier.
10. Faites un double clic sur la stratégie « Stratégie VPN », que vous venez de créer puis cliquez sur « Ajouter ».
11. Sélectionnez, dans la liste des attributs, l'attribut **Day-And-Time-Restrictions** et cliquez sur « Ajouter… ».

    Attention : un problème de compatibilité entre les semaines Anglo-saxonnes et Française semble être à l'origine d'un bug. Le « Lundi » que vous voyez sur le planning correspond en fait au « Dimanche » Anglo-saxon, etc.… Pensez donc à en tenir compte pour régler vos plages horaires…

12. Configurez les horaires de sorte que seules les seules plages horaires du Lundi au Vendredi 8h-12h et 14h-18h soient autorisées, **sauf** la plage horaire pendant laquelle vous êtes en train de réaliser ce TP qui doit être refusée (pour vérifier si la stratégie s'applique ou pas – Attention à la remarque précédente…) puis cliquez sur « OK ».
13. Sélectionnez l'option « Accorder l'autorisation d'accès distant » si une demande de connexion est conforme aux conditions spécifiées puis cliquez sur « OK » pour revenir à la console « Routage et accès distant ».
14. Redémarrez le service « Routage et accès distant ».
15. Essayez de vous connecter, sur le poste **Client VPN**, en tant que client d'accès distant (déconnectez vous préalablement au besoin).

- Y arrivez-vous ? ☐ OUI ☐ NON

  Que se passe-t-il ? La stratégie semble ne pas s'appliquer bien que vous ayez refusé l'accès sur cette plage horaire !?… Rassurez vous, à ce stade du TP c'est « normal ».

16. Déconnectez-vous de l'accès distant.
17. Revenez sur le poste **Serveur VPN** et ouvrez les propriétés du compte **Administrateur** puis cliquez sur l'onglet « Appel entrant ».

    L'option « Contrôler l'accès via la Stratégie d'accès distant » n'est pas celle sélectionnée ! Voilà la cause de notre disfonctionnement… On autorise l'accès au compte de l'Administrateur, sans tenir compte de la stratégie d'accès distant !
18. Sélectionnez donc l'option « Contrôler l'accès via la Stratégie d'accès distant » et validez cette modification.
19. Revenez sur le poste **Client d'accès distant** et tentez une nouvelle connexion VPN.

- Y arrivez-vous ? ☐ OUI ☐ NON

20. Vérifiez en autorisant maintenant la connexion dans la plage horaire du TP (pensez à redémarrer le service « Routage et accès distant »), que c'est bien cette restriction qui empêchait la connexion.

Modifier une stratégie d'accès distant

On peut considérer qu'une stratégie est trop ou pas assez restrictive et décider de la modifier (on pourrait également créer une autre stratégie et la placer avant ou après telle ou telle autre car elles s'appliquent dans l'ordre où elles sont placées dans la liste).

Nota : ces opérations sont à effectuer sur le poste jouant le rôle de **Serveur VPN**.

1. Faites si besoin **Démarrer**, **Programmes**, **Outils d'administration**, puis **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant ».
2. Sélectionnez la ligne **Stratégies d'accès distant** dans la partie gauche de la fenêtre et faites un double-clic, sur la ligne référençant notre stratégie « Stratégie VPN ».
3. Cliquez sur « Ajouter… » puis faites un double clic sur l'attribut **Tunnel-Type**. Dans la nouvelle boîte de dialogue, faites un double clic sur **Point-to-Point Tunneling Protocol (PPTP)** afin de limiter le tunnel VPN à ce seul protocole puis cliquez sur « OK ».
4. Observez les diverses possibilités de restriction offertes en cliquant sur le bouton « Modifier le profil… » et sur les divers onglets proposés dans la boîte de dialogue suivante mais **ne modifiez rien** et quittez en cliquant sur « Annuler ».
5. Quittez la boîte de propriétés de la stratégie en cliquant sur « OK » et redémarrez le service « Routage et accès distant ».
6. Refermez la console MMC de routage et d'accès distant.

7. Revenez sur le poste **Client d'accès distant** et tentez une nouvelle connexion VPN.

- Y arrivez-vous ? ☐ OUI ☐ NON

Reconfigurer le service Routage et accès distant et les stratégies

Attention : si, à la suite de manipulations « hasardeuses », le service **Routage et accès distant** du serveur VPN est inaccessible, il peut être nécessaire de le désactiver puis de le réactiver et de reconfigurer la **stratégie de sécurité par défaut**. Voici les étapes à suivre :

Reconfigurer le service Routage et accès distant

1. Faites **Démarrer**, **Programmes**, **Outils d'administration**, puis **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant ».
2. Faites un clic droit sur le nom du serveur qui apparaît dans l'arborescence et cliquez sur **Désactiver le service Routage et accès distant** puis sur « Oui » pour confirmer la désactivation de ce service.
3. Procédez à une réinstallation du service **Routage et accès distant** comme vue précédemment.

Reconfigurer les stratégies d'accès distant par défaut

Il peut être nécessaire de rétablir les stratégies d'accès distant par défaut. Pour cela :

1. Faites, **Démarrer**, **Programmes**, **Outils d'administration**, puis **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant ».
2. Dans l'arborescence de console, faites un clic droit sur **Stratégies d'accès distant** puis **Nouvelle stratégie d'accès distant** et cliquez sur « Suivant ».
3. Sélectionnez l'option « Installer une stratégie personnalisée » et saisissez, dans la dans la zone « Nom de la stratégie : », le nom de la stratégie par défaut : **Connexions au serveur d'accès à distance et de routage Microsoft** (d'après Microsoft ce nom exact n'est pas obligatoire mais semble « conseillé ») puis cliquez sur « Suivant ».
4. Sur la page « Conditions de la stratégie », cliquez sur « Ajouter… ».
5. Sélectionnez l'attribut **MS-RAS-Vendor**, cliquez sur « Ajouter » et entrez comme mot : **311$** puis cliquez sur « OK », puis sur « Suivant ».
6. Sur la page « Autorisations », sélectionnez l'option « Refuser l'autorisation d'accès distant », puis cliquez sur « Suivant ».
7. Sur la page « Profil utilisateur », n'apportez aucune modification au profil d'utilisateur, cliquez simplement sur « Suivant » puis sur « Terminer ».
8. Dans l'arborescence de console, faites un clic droit sur **Stratégies d'accès distant** puis **Nouvelle stratégie d'accès distant** et cliquez sur « Suivant ».
9. Sélectionnez l'option « Installer une stratégie personnalisée » et saisissez, dans la dans la zone « Nom de la stratégie : », le nom de la stratégie par défaut : **Connexions à d'autres serveurs d'accès** (d'après Microsoft ce nom exact n'est pas obligatoire mais semble « conseillé ») puis cliquez sur « Suivant ».
10. Sur la page « Conditions de la stratégie », cliquez sur « Ajouter… ».
11. Sélectionnez l'attribut **Day-And-Time-Restrictions** (Contraintes heures du jour), cliquez sur « Ajouter » et configurez l'attribut de sorte que toutes les heures et tous les jours soient autorisés puis cliquez sur « OK », puis sur « Suivant ».
12. Sur la page « Autorisations », sélectionnez l'option « Refuser l'autorisation d'accès distant », puis cliquez sur « Suivant ».

13. Sur la page « Profil utilisateur », n'apportez aucune modification au profil d'utilisateur, cliquez simplement sur « Suivant » puis sur « Terminer ».
14. Au besoin désactivez puis réactivez à nouveau le service **Routage et accès distant**.

Redémarrer le service Routage et accès distant

Pour redémarrer le service de routage et d'accès distant – opération conseillée après toute modification des paramètres, rien de plus simple :

1. Faites au besoin **Démarrer**, **Programmes**, **Outils d'administration**, puis **Routage et accès distant** pour ouvrir la console « Routage et Accès Distant ».
2. Faites un clic droit sur le nom du serveur puis **Toutes les tâches**, **Redémarrer** et patientez le temps que le service redémarre.

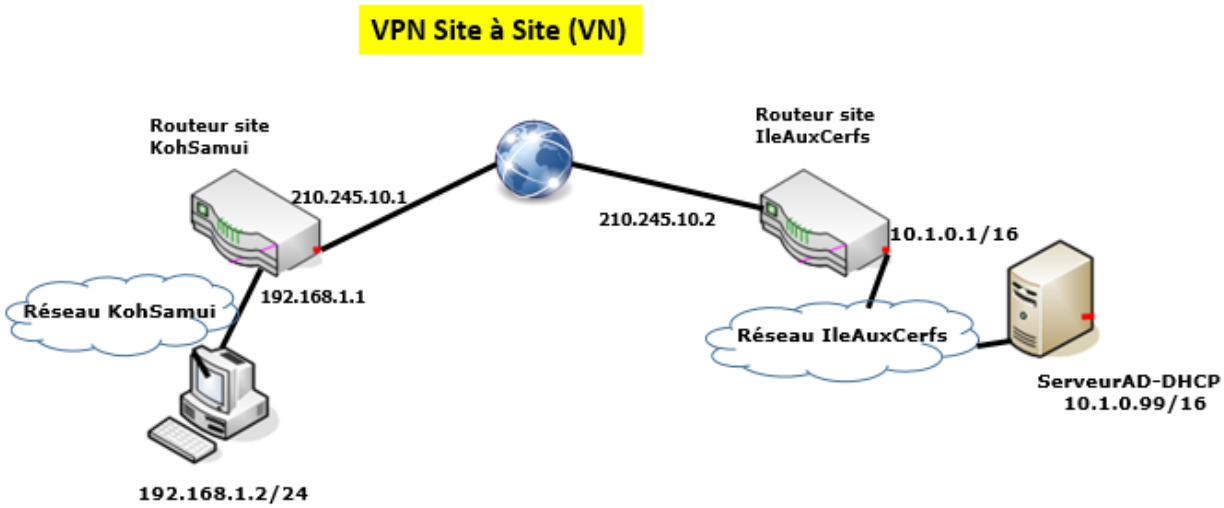
Conclusion

La solution VPN Microsoft est relativement facile à mettre en place, cependant il ne faut pas perdre de vue qu'ouvrir un accès VPN c'est ouvrir un accès potentiel au réseau de l'entreprise. Il est donc conseillé de surveiller de près les accès autorisés ou refusés sur un serveur de tests avant de passer en production. Vous pouvez pour cela utiliser les fonctions d'audit intégrés à Windows.

En ce qui concerne les ressources, prenez garde à bien dimensionner la taille de votre serveur en fonction du nombre d'utilisateurs accédant au VPN et pensez à bien limiter les accès. Il n'est pas forcement utile que les utilisateurs aient accès à un serveur FTP ou bien à certains partages réseaux lorsqu'ils utilisent l'accès distant.

A une époque où les utilisateurs sont de plus en plus mobiles et les accès Internet de plus en plus performants et aisés, il est utile de pouvoir accéder de manière sécurisée et distante aux services de l'entreprise. Par exemple l'Administrateur réseau pourra ainsi intervenir depuis son domicile sur les serveurs de l'entreprise… Les technologies VPN permettent de répondre à ces attentes avec des coûts raisonnables puisque ce sont ceux des seuls accès Internet et avec une sécurisation tout à fait convenable - si vous avez bien configuré votre serveur VPN et si vous utilisez notamment des méthodes un peu plus élaborées telles que des serveurs d'authentification RADIUS ou des cartes à puces…

Partie II Mise en œuvre de VPN site à site



Objectif du TP :

Créer un "tunnel" entre deux serveurs VPN afin que les clients de deux sites distants puissent se communique par ce réseau privé virtuel, Comme si ils étaient dans le même site géographique et d'une manière transparente.

Les données seront chiffrées et transitées dans ce réseau virtuel.

Les étapes des travaux préparatifs :

I) Cloner les machines virtuelles : Une XP – 3 serveurs 2003.

II) Configurer les adresses IP selon le schéma réseau ci-dessus.

III) Renommer les noms des postes : **Client1VPN – KohSamui – IleAuxCerfs - ServeurAD.**

IV) Ajouter les lignes dans les tables de routage des routeurs **KohSamui – IleAuxCerfs**. (route add ….)

V) Tester la connectivité par l'intermédiaire du protocole ICMP.

A ce stade, tous les postes doivent pouvoir se parler (se pinguent).

En suite vous enlevez les lignes que vous avez ajoutées dans IV), ça signifie que **Client1VPN** ne peut plus communiquer avec le **ServeurAD.**

VI) Sur les routeurs VPN **IleauxCerfs et KohSamui** vous procédez la commande suivantes **route print >> c:\KohSamui_table.txt** et **ipconfig >> c:\KohSamui_ipconfig.txt,** vous obtiendrez des fichiers contenant la tables de routage et la configuration des deux routeurs.

V) La mise en place du réseau privé virtuel :

Sur le routeur KohSamui :

a) Se loguer en tant que l'administrateur.

b) Démarrer – Outils d'administration – Routage et Accès distant

c) Si le nom du serveur n'apparait pas, faites ceci :

Clic droit sur Routage et Accès distant - Ajouter un serveur – Cet ordinateur – Serveur au nom de **KohSamui** apparait.

d) Clic droit sur le nom du serveur –

➔Configurer et Activer le routage et Accès distant – Suivant –

➔Cocher Accès à Distance (Connexion à distance ou VPN) –suivant –

➔Cocher VPN puis suivant –

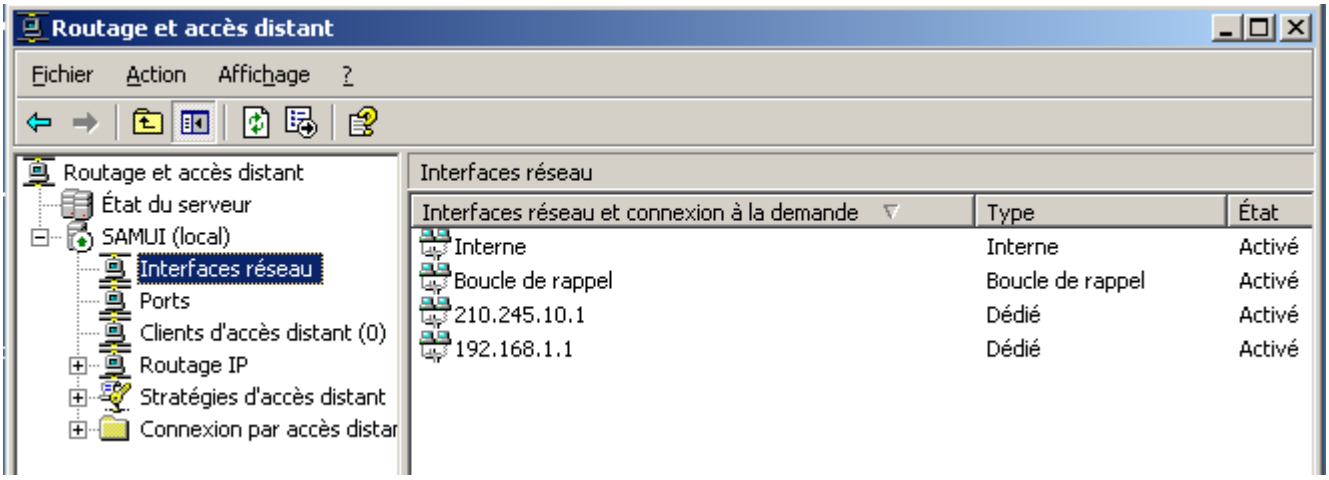
➔Choisir l'interface publique (normalement selon le schéma réseau c'est **210.245.10.1**) – suivant –

➔Choisir : A partir d'une plage d'adresse spécifiée – suivant – Nouveau –

➔Saisir une plage d'IP (exemple : 192.168.1.11 à .15 soit 5 IP) que le serveur VPN donnera aux futures clients VPN qui communiqueront avec les postes du site **KohSamui (192.168.1.0 /24).** – suivant –

➔Choisir l'option : non, utiliser Routage et Accès distant pour authentifier les requêtes de connexion – Terminer – Confirmer OK pour le message concernant l'agent relais DHCP.

Vous obtenez quelques choses comme celui-ci :



e) Choisir l'option Interface Réseau :

➔Clic doit – nouvelle interface de numérisation à la demande – suivant –

➔Choisir le nom du routeur distant, ici c'est **IleAuxCerfs** – suivant –

➔Choisir : se connecter en utilisant un réseau privé virtuel –

➔Choisir protocole **PPTP** –

➔Saisir l'adresse IP du routeur du site distant **IleAuxCerfs** (**210.245.10.2) –**
➔Cocher **Router les paquets IP…** et **Ajouter un compte d'utilisateur … -** suivant –

➔Ajouter Itinéraires statiques pour les réseaux distants **10.0.0.0 / 8 métric =1** – suivant –

➔Informations d'identification… Mot de passe Cmsi2019 ! – Suivant –
➔Informations d'identification pour les appels sortants : Nom d'utilisateur **KohSamui**, MDP **Cmsi2019!** – Suivant – terminer -

A faire de même sur le routeur **IleAuxCerfs**.

f) Etablir la connexion VPN entre deux sites (deux routeur)

Sur le routeur KohSamui :

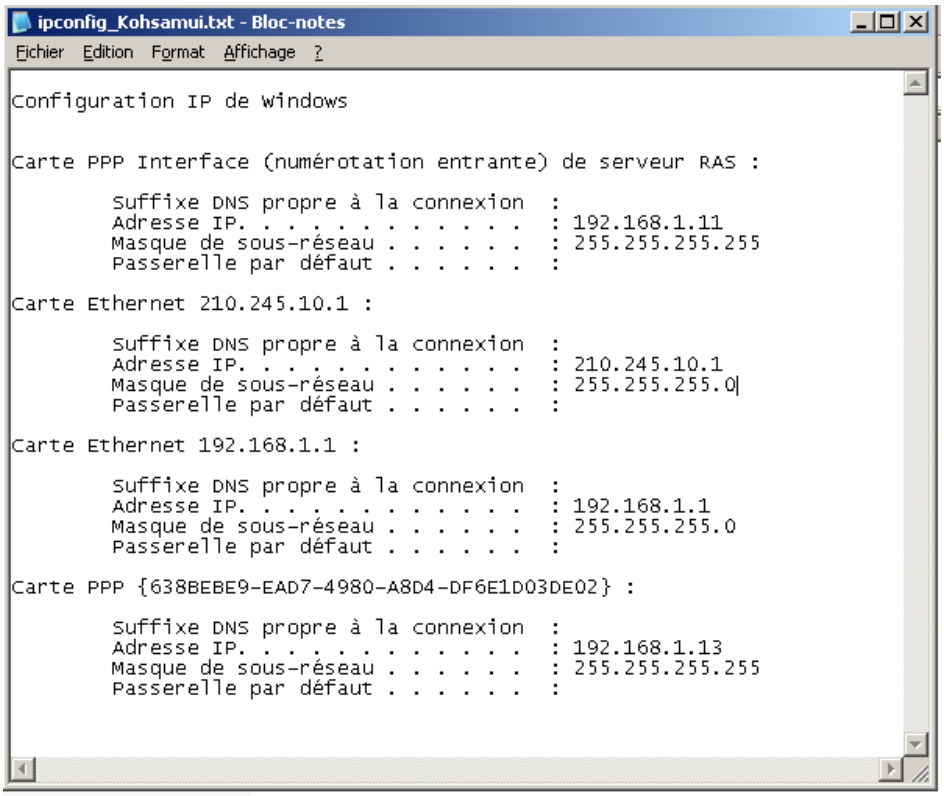
⇨ Clic droit sur l'interface **KohSamui** – se connecter

Sur le routeur IleAuxCerfs :

⇨ Clic droit sur l'interface **IleAuxCerfs** – se connecter

g) Effectuer les commandes **ipconfig** sur chaque routeur cela donne

Routeur **KohSamui**

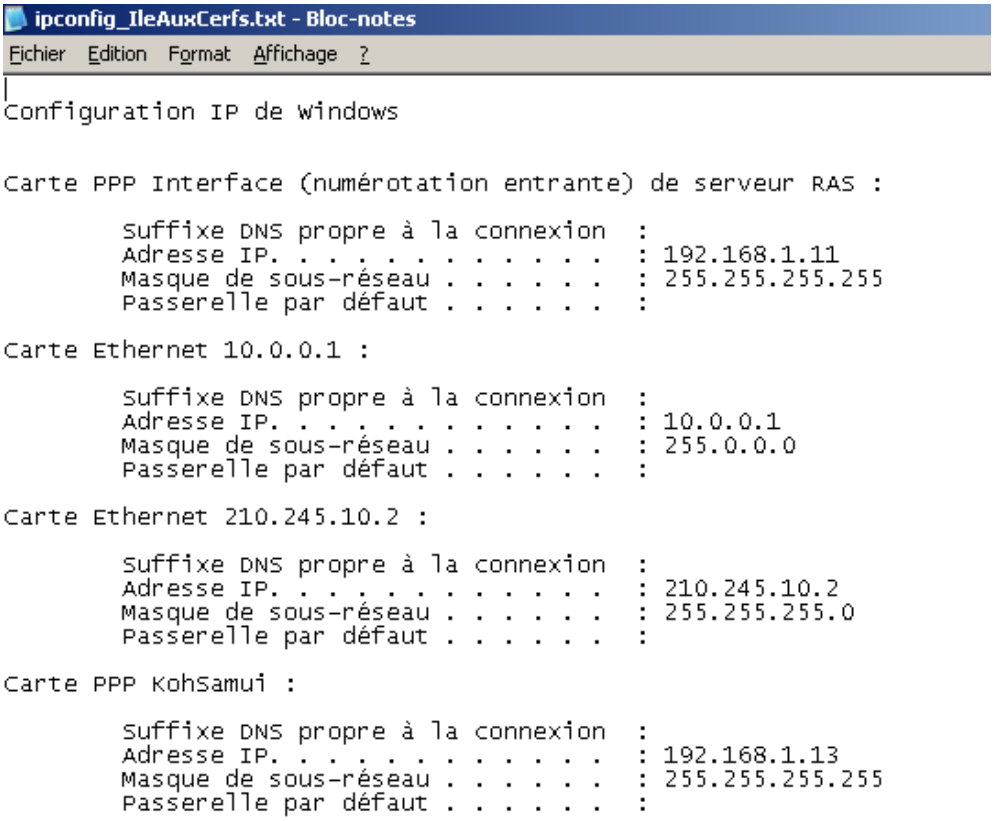


ipconfig_Kohsamui.txt - Bloc-notes

Fichier Edition Format Affichage ?

```
Configuration IP de Windows


Carte PPP Interface (numérotation entrante) de serveur RAS :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 192.168.1.11
        Masque de sous-réseau . . . . . .  : 255.255.255.255
        Passerelle par défaut . . . . . .  :

Carte Ethernet 210.245.10.1 :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 210.245.10.1
        Masque de sous-réseau . . . . . .  : 255.255.255.0
        Passerelle par défaut . . . . . .  :

Carte Ethernet 192.168.1.1 :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 192.168.1.1
        Masque de sous-réseau . . . . . .  : 255.255.255.0
        Passerelle par défaut . . . . . .  :

Carte PPP {638BEBE9-EAD7-4980-A8D4-DF6E1D03DE02} :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 192.168.1.13
        Masque de sous-réseau . . . . . .  : 255.255.255.255
        Passerelle par défaut . . . . . .  :
```

Routeur **IleAuxCerfs**



ipconfig_IleAuxCerfs.txt - Bloc-notes

Fichier Edition Format Affichage ?

```
Configuration IP de Windows


Carte PPP Interface (numérotation entrante) de serveur RAS :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 192.168.1.11
        Masque de sous-réseau . . . . . .  : 255.255.255.255
        Passerelle par défaut . . . . . .  :

Carte Ethernet 10.0.0.1 :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 10.0.0.1
        Masque de sous-réseau . . . . . .  : 255.0.0.0
        Passerelle par défaut . . . . . .  :

Carte Ethernet 210.245.10.2 :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 210.245.10.2
        Masque de sous-réseau . . . . . .  : 255.255.255.0
        Passerelle par défaut . . . . . .  :

Carte PPP KohSamui :

        Suffixe DNS propre à la connexion  :
        Adresse IP. . . . . . . . . . . .  : 192.168.1.13
        Masque de sous-réseau . . . . . .  : 255.255.255.255
        Passerelle par défaut . . . . . .  :
```

Comparer avec les fichiers obtenus en **IV),** commentez.

h) Effectuer les commandes **route print** sur chaque routeur cela donne

Routeur **KohSamui**

table_KohSamui.txt - Bloc-notes

Fichier Edition Format Affichage ?

```
IPv4 Table de routage
===========================================================================
Liste d'Interfaces
0x1 ........................... MS TCP Loopback interface0x10002 ...00 53 45 00 00 00
===========================================================================
Itin,raires actifsÿ:
Destination r,seau    Masque r,seau  Adr. passerelle   Adr. interface M,trique
        10.0.0.0        255.0.0.0     192.168.1.13     192.168.1.13      1
       127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
     192.168.1.0    255.255.255.0      192.168.1.1      192.168.1.1     10
     192.168.1.1  255.255.255.255        127.0.0.1        127.0.0.1     10
    192.168.1.11  255.255.255.255        127.0.0.1        127.0.0.1     50
    192.168.1.13  255.255.255.255        127.0.0.1        127.0.0.1     50
   192.168.1.255  255.255.255.255      192.168.1.1      192.168.1.1     10
   192.168.1.255  255.255.255.255     192.168.1.13     192.168.1.13     50
    210.245.10.0    255.255.255.0     210.245.10.1     210.245.10.1     10
    210.245.10.1  255.255.255.255        127.0.0.1        127.0.0.1     10
    210.245.10.2  255.255.255.255     210.245.10.1     210.245.10.1     10
  210.245.10.255  255.255.255.255     210.245.10.1     210.245.10.1     10
        224.0.0.0        240.0.0.0      192.168.1.1      192.168.1.1     10
        224.0.0.0        240.0.0.0     192.168.1.13     192.168.1.13     50
        224.0.0.0        240.0.0.0     210.245.10.1     210.245.10.1     10
  255.255.255.255  255.255.255.255      192.168.1.1      192.168.1.1      1
  255.255.255.255  255.255.255.255     192.168.1.13     192.168.1.13      1
  255.255.255.255  255.255.255.255     210.245.10.1     210.245.10.1      1
===========================================================================
Itin,raires persistantsÿ:
  Aucun
```

Routeur **IleAuxCerfs**

table_IleAuxCerfs.txt - Bloc-notes

Fichier Edition Format Affichage ?

```
IPv4 Table de routage
===========================================================================
_iste d'Interfaces
)x1 ........................... MS TCP Loopback interface0x10002 ...00 53 45 00 00
===========================================================================
Itin,raires actifsÿ:
)estination r,seau    Masque r,seau  Adr. passerelle   Adr. interface M,trique
        10.0.0.0        255.0.0.0       10.0.0.1         10.0.0.1     10
        10.0.0.1  255.255.255.255      127.0.0.1        127.0.0.1     10
  10.255.255.255  255.255.255.255       10.0.0.1         10.0.0.1     10
        11.0.0.0        255.0.0.0       10.0.0.2         10.0.0.1      1
       127.0.0.0        255.0.0.0      127.0.0.1        127.0.0.1      1
    192.168.1.0    255.255.255.0        0.0.0.0     192.168.1.13      1
    192.168.1.0    255.255.255.0     192.168.1.13     192.168.1.13      1
   192.168.1.11  255.255.255.255      127.0.0.1        127.0.0.1     50
   192.168.1.13  255.255.255.255      127.0.0.1        127.0.0.1     50
  192.168.1.255  255.255.255.255     192.168.1.13     192.168.1.13     50
    210.245.10.0    255.255.255.0     210.245.10.2     210.245.10.2     10
    210.245.10.1  255.255.255.255     210.245.10.2     210.245.10.2     10
    210.245.10.2  255.255.255.255      127.0.0.1        127.0.0.1     10
  210.245.10.255  255.255.255.255     210.245.10.2     210.245.10.2     10
        224.0.0.0        240.0.0.0       10.0.0.1         10.0.0.1     10
        224.0.0.0        240.0.0.0     192.168.1.13     192.168.1.13     50
        224.0.0.0        240.0.0.0     210.245.10.2     210.245.10.2     10
  255.255.255.255  255.255.255.255       10.0.0.1         10.0.0.1      1
  255.255.255.255  255.255.255.255     192.168.1.13     192.168.1.13      1
  255.255.255.255  255.255.255.255     210.245.10.2     210.245.10.2      1
===========================================================================
```

Comparer avec les fichiers obtenus en **IV),** commentez.

Faire le test pour mettre en évidence l'existence du tunnel VPN (ICMP – tracert – Wireshark)

VI) A faire évoluer l'infrastructure comme celle ci-dessous :

Objectifs à atteindre :

➔Le client1VPN obtient d'une IP délivrée par le serveurDHCP **10.1.0.99**.

➔ Le client1VPN peut communiquer avec le réseau 10.0.0.0 surtout avec **10.2.0.2**