# Déploiement d'IPSec à l'aide de stratégies et de règles de sécurité de connexion

## Sommaire

**IPSec sous les réseaux Windows 2008** ..... 2

**Exercice 1 : Installation des services Telnet** ..... 4

**Exercice 2 : Création d'une stratégie IPSec** ..... 5

**Exercice 3 : Création d'une règle de stratégie IPSec et filtre** ..... 7

**Exercice 4 : Utilisation de l'Assistant Action de filtrage** ..... 8

**Exercice 5 : Test de la nouvelle stratégie IPSec** ..... 11

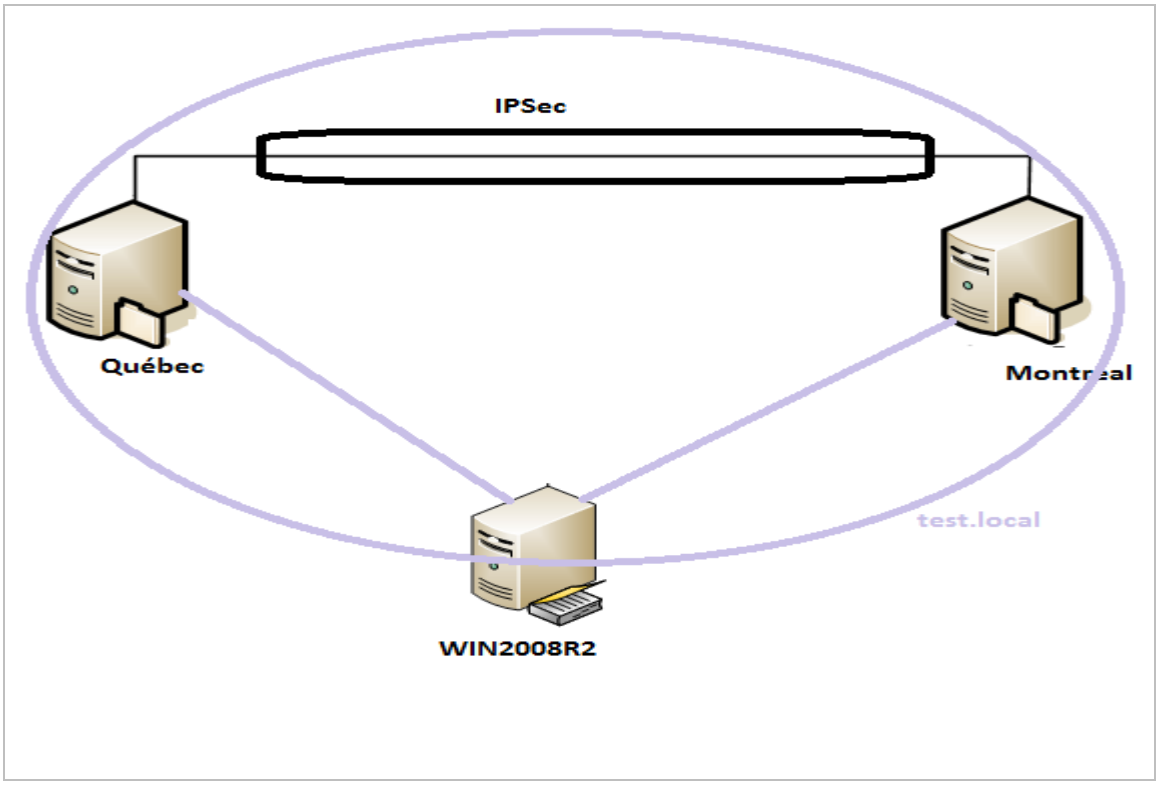
**Exercice 6 : application IPSec en vertu des règles de sécurité de connexion** ..... 12

## IPSec sous les réseaux Windows 2008

- IPSec Permet de protéger le trafic réseau en proposant l'authentification et/ou le chiffrement des données. La sécurité d'IPSec est obtenu à l'aide de 2 protocoles, AH (Authentication Header) et EPS (Encapsulation Security Payload). AH procure l'authentification de l'origine des données, l'intégrité des données et une protection anti-répliques pour la totalité du paquet IP. ESP procure le chiffrement des données, l'authentification de l'origine des données, et la protection anti-répliques pour la charge utile ESP.
- Vous pouvez mettre en œuvre IPSec sur les réseaux Windows 2008 (R2) à l'aide de stratégie IPSec ou de règle de sécurité de connexion. Lorsque toutefois une passerelle VPN particuliere n'est pas compatible avec lesVPN L2TP/IPSec, vous pouvez à la place employer IPSec en mode tunnel.
- Les stratégies IPSec, déployées via la stratégie local de l'ordinateur ou un GPO, sont constituées d'un ensemble de de règles IPSec. Chaque règle se décompose à son tour en une liste de filtres IP et une action de filtre de sécurité. La liste de filtrage définit le type de trafic auquel s'applique l'action de filtre de sécurité. Les actions de filtre sont autoriser, bloquer et négocier la sécurité (authentification, chiffrement ou les deux)
- Les règles de sécurité de connexion protègent tout le trafic entre des sources et des destinations particulières. Par défaut, elles ne chiffrent pas les données, se bornant à garantir l'intégrité de celles-ci. Vous pouvez configurer des règles de sécurité de connexion depuis la console Pare-feu Windows avec fonctions avancées de sécurité sur un ordinateur individuel ou les mettre en œuvre à l'aide d'un GPO.

Dans mettre en pratique les concepts d'IPSec sous Windows Server 2012, vous devez disposer de :

- D'un contrôleur de domaine Windows server 2008 (R2) nommé ***WIN2008R2.test.local***.
- D'une machine Windows server 2008 (R2) nommée ***Montreal.test.local*** membre du domaine test.local et dont le partage de fichier est activé.
- D'une machine troisième machine Windows server 2008 (R2) nommée ***Quebec.test.local*** membre du domaine test.local.



Dans la première étape de cette pratique, vous allez installer les services Telnet et puis configurer une stratégie IPSec pour crypter le trafic Telnet entre **Montreal.test.local** et **Quebec.test.local**. Dans la deuxième étape, vous allez créer une règle de sécurité de connexion qui authentifie tout le trafic réseau entre ces deux ordinateurs.

## Exercice 1 : Installation des services Telnet

Dans cet exercice, vous allez installer les services Telnet sur les deux ordinateurs **Montreal** et **Quebec**.

1. Ouvrer une session sur **test** depuis **Montreal** en tant qu'administrateur du domaine.
2. Insérez le DVD (ou l'ISO) du produit Windows Server 2008 R2 dans le lecteur de disque dur local.
3. Dans la fenêtre tâches **initiales de configuration** ou le **Gestionnaire de serveur**, cliquez sur **Ajouter des fonctionnalités**.

   La page **Sélectionner des fonctionnalités** de **l'Assistant Ajout de fonctionnalités** s'ouvre.

4. Dans la liste des fonctionnalités, sélectionnez (case à cocher) les options **Client Telnet et Serveur Telnet**, puis cliquez sur **Suivant**.
5. Sur la page **Confirmer les sélections pour l'installation de l'Assistant Ajout de fonctionnalités**, cliquez sur **Installer**.
6. Une fois l'installation terminée, cliquez sur **Fermer** sur la page **Résultats de l'installation**.
7. Ouvrez la console **Services** en cliquant sur **Démarrer**, en pointant sur **Outils d'administration**, puis en choisissant **Services**.
8. Dans la console **Services**, recherchez et double-cliquez sur **Telnet** pour ouvrir ses propriétés.
9. Dans la boîte de dialogue **Propriétés de Telnet**, modifier le type de démarrage sur **Automatique**, puis cliquez sur **Appliquer**.
10. Dans la zone **Statut du service**, cliquez sur **Démarrer**.

11. Lorsque le statut du service s'est modifié en **Démarré**, cliquez sur **OK** pour fermer la boîte de dialogue des **Propriétés Telnet**, puis fermez la console **Services**.
12. Dans la zone de **Recherche** du menu **Démarrer**, tapez **lusrmgr.msc**, puis appuyez sur **Entrée**.
13. Dans l'arborescence de la console **Utilisateurs et groupes locaux**, sélectionnez le dossier **Groupes**.
14. Dans le volet **Détails**, double-cliquez sur **ClientsTelnet**.
15. Dans la boîte de dialogue des propriétés **ClientsTelnet**, cliquez sur le bouton **Ajouter**.
16. Dans la boîte de dialogue Sélectionner Utilisateurs, ordinateurs ou groupes, dans la zone de texte **Entrez les noms des objets à sélectionner,** tapez **Admins du domaine**, puis cliquez sur **OK**.
17. Dans la boîte de dialogue **Propriétés de ClientsTelnet**, cliquez sur **OK**.
18. Fermer la session sur **Montreal**.
19. Ouvrez une session sur **test** depuis **Quebec**, puis effectuez les étapes 2 à 18 sur **Quebec**.

## Exercice 2 : Création d'une stratégie IPSec

Dans cet exercice, vous allez créer un GPO et une stratégie **IPSec** que vous allez configurer pour chiffrer le trafic **Telnet** sur le domaine **test.local**.

1. Ouvrez une session sur **test** depuis ***WIN2008R2*** en tant qu'administrateur du domaine.
2. Ouvrez la console de gestion des stratégies de groupe (GPM, Group Policy Management) en cliquant sur **Démarrer**, pointez sur **Outils d'administration**, puis en choisissant Gestion d'une Stratégie de groupe.
3. Dans l'arborescence de la console GPM, développez le conteneur Domaines, puis sélectionnez le nœud **test.local**.

4. Cliquez-droit sur le nœud **test.local** et choisissez **Créer un objet GPO dans ce domaine et le lier ici.**
5. Dans la zone Nom de la boite de dialogue **Nouvel objet GPO**, tapez **GPO IPSec**, puis cliquez sur **OK**.
6. Dans la console GPM, dans le volet Détails, cliquez droit sur le **GPO IPSec**, puis, à partir du menu contextuel, choisissez **Modifier**.
7. Dans la fenêtre Éditeur de gestion des stratégies de groupe, naviguer jusqu'au nœud **Configuration ordinateur/Stratégies/Paramètres Windows/ Paramètres de sécurité/Stratégies de sécurité IP sur Active Directory**.
8. Cliquez-droit sur le nœud **Stratégies de sécurité IP** sur Active Directory, puis choisissez **Créer une stratégie de sécurité IP** dans le menu contextuel.

   L'**Assistant Stratégie de sécurité IP** s'ouvre.
9. Cliquez sur **Suivant**.
10. Sur la page **Nom de la stratégie de sécurité IPSec**, tapez **Stratégie IPSec test**.
11. Dans le champ **Description**, tapez **Cette stratégie IPSec chiffre le trafic Telnet**.
12. Cliquez sur **Suivant**.
13. sur la page **Requêtes pour une communication sécurisée**, lisez tout le texte, puis cliquez sur **Suivant**.
14. Cliquez sur **Terminer**.

    La boîte de dialogue des propriétés de **Stratégie IPSec test** apparaît.
15. Laisser toutes les fenêtres ouvertes et passez à l'**exercice 3**.

## Exercice 3 : Création d'une règle de stratégie IPSec et filtre

Dans cet exercice, vous allez configurer la **Stratégie IPSec test** nouvellement créé avec des règles qui exigent une sécurité élevée pour le trafic Telnet. Ce faisant, vous allez exécuter l'assistant **Règle de sécurité**, l'**Assistant Filtre d'adresse IP**, et l'**Assistant action de filtrage**.

1. Avec une session toujours ouverte sur **WIN2008R2**, cliquer dans la boite de dialogue **Propriétés de Stratégie IPSec test** sur **Ajouter**.

   L'Assistant de création d'une règle de sécurité IP s'ouvre. (Cet assistant est aussi appelé **Assistant règle de sécurité**).

2. Lisez tout le texte de la première page, puis cliquez sur **Suivant**.
3. Sur la page **Point de sortie du tunnel** (Tunnel Endpoint), lisez tout le texte, puis cliquez sur **Suivant**.
4. Sur la page **Type de réseau**, lisez tout le texte, puis cliquez sur **Suivant**.
5. Sur la page **Liste de filtres IP**, lisez tout le texte, puis cliquez sur **Ajouter**.

   La boîte de dialogue **Liste de filtres IP** s'ouvre.

6. Dans la zone de texte **Nom**, tapez **Liste de filtres de chiffrage Telnet**, puis cliquez sur **Ajouter**.

   L'Assistant **Filtre d'adresses IP** s'ouvre.

7. Cliquez sur **Suivant**.
8. Sur la page **Description du filtre IP et propriété mise en miroir**, lisez tout le texte, puis cliquez sur **Suivant**
9. Sur la page **Source du trafic IP**, laissez la sélection par défaut de **Toute adresse IP**, puis cliquez sur **Suivant**.
10. Sur la page **Destination du trafic IP**, laissez la sélection par défaut de **Toute adresse IP**, puis cliquez sur **Suivant**.
11. Sur la page **Type de protocole IP**, sélectionnez **TCP** dans la liste déroulante **Sélectionnez un type Protocole**, puis cliquez sur **Suivant**.

Telnet utilise le port **TCP 23**, vous devez donc spécifier à la fois TCP et le port approprié.

12. Sur la page **Port Protocole IP**, sélectionnez **Vers ce port**, puis tapez **23** dans la zone de texte associée. Laissez Depuis n'importe quel port sélectionné.
13. Cliquez sur **Suivant**, puis cliquez sur **Terminer** pour fermer **l'Assistant filtre d'adresses IP.**
14. Dans la boîte de dialogue **Liste de filtres IP**, cliquez sur **OK**.

    La page **Liste de filtres IP** de l'**Assistant règle de sécurité** réapparaît.
15. Dans la zone **Liste de filtres IP**, sélectionnez le bouton d'option **Liste de filtres de chiffrageTelnet**, puis cliquez sur **Suivant**.
16. Sur la page **Action de filtrage**, lisez tout le texte, puis cliquez sur **Ajouter.**

    L'Assistant **Action de filtre de sécurité IP** s'ouvre. Laissez cet assistant ouvert et continuer à pratiquer l'**exercice 4**.

## Exercice 4 : Utilisation de l'Assistant Action de filtrage

Dans cet exercice, vous utilisez l'Assistant Action de filtre de sécurité IP pour configurer une action de filtre de sécurité personnalisé à appliquer au trafic Telnet. Bien que les actions de filtre par défaut proposées dans une stratégie de groupe sont généralement suffisantes pour la création de règles IPSec, c'est une bonne idée de renforcer la sécurité pour le trafic Telnet.

1. Sur la page d'accueil de l'Assistant de filtre de sécurité, action, lisez tout le texte, puis cliquez sur **Suivant**.
2. Sur la page **Nom** d'action de filtrage, dans la zone de texte **Nom**, tapez **Exiger une authentification et un chiffrage élevés.**
3. Dans le champ **Description**, tapez **Exiger une authentification AH et un chiffrement 3DES.**
4. Cliquez sur **Suivant**.
5. Sur la page **Options générales** d'action de filtrage, vérifiez que l'option **Négocier la sécurité** est sélectionnée, puis cliquez sur **Suivant**.

6. Sur la page **Communiquer avec des ordinateurs qui ne prennent pas en charge IPSec**, vérifiez que **Ne pas autoriser les communications non sécurisées** est sélectionnée, puis cliquez sur **Suivant**.
7. Sur la page **Sécurité trafic IP**, sélectionnez **Personnaliser**, puis cliquez sur **Paramètres**.
8. Dans la boîte de dialogue **Paramètres personnalisé de la méthode de sécurité**, cochez l'option **Intégrité des adresses et des données sans chiffrement (AH)**.
9. Dans la zone **Paramètres de la clé de session**, cochez les deux options **Générer une nouvelle clé tous les** et **Générer une nouvelle clé toutes les**.
10. Vérifiez que l'option **Intégrité de chiffrement des données (ESP)** est sélectionnée, puis cliquez sur **OK**. (Notez aussi que **3DES** est l'algorithme de chiffrage sélectionné.)
11. Sur la page **Sécurité trafic IP**, cliquez sur **Suivant**.
12. Sur la page **Fin de l'Assistant Action de filtrage de sécurité IP**, cliquez sur **Terminer**.
13. Sur la page **Action de filtrage de l'Assistant règle de sécurité**, dans la liste des actions de filtre, sélectionnez **Exiger une authentification et un chiffrage élevés**, puis cliquez sur **Suivant**.
14. Sur la page **Méthode d'authentification** de l'**Assistant règle de sécurité**, laissez la valeur par défaut **Authentification Active Directory** (protocole Kerberos V5), puis cliquez sur **Suivant**.

    La page **Fin de l'Assistant Règle de sécurité** apparaît.
15. Cliquez sur **Terminer**.
16. Dans la boîte de dialogue **Propriétés de Stratégie IPSec Test**, cliquez sur **OK**.
17. Dans l'éditeur gestion des stratégies de groupe, cliquez-droit sur **Stratégie IPSec Test**, puis, dans le menu contextuel, choisissez **Attribuer**.
18. Sur **Montreal** et **Quebec**, exécutez la commande ***Gpupdate*** à une invite de commande.

## Exercice 5 : Test de la nouvelle stratégie IPSec

Dans cet exercice, vous allez lancer une session Telnet de **Montreal** à **Quebec**. Vous allez vérifier ensuite que l'authentification et le cryptage des données sont appliqués à la session Telnet.

1. Sur **Montreal**, ouvrez une invite de commande.
2. À l'invite de commande, tapez **telnet Quebec**.
3. Une session Telnet au serveur Telnet sur **Quebec** commence.
4. Sur **Montreal**, dans le menu Démarrer, pointez sur **Outils d'administration**, puis choisissez Pare-feu Windows avec fonctions avancées de sécurité (**WFAS**).
5. Dans l'arborescence de la console **WFAS**, développez le nœud **Analyse** puis le nœud **Associations de sécurité**.
6. Dans le nœud associations de sécurité, sélectionnez le dossier **Mode principal**, puis le Dossier **Mode rapide**. Vous verrez qu'une **SA** apparaît dans le volet **Détails** lors de la sélection de chaque dossier. Consacrez quelques instants à l'examen des informations affichées sur ces SA. Si la SA de mode rapide disparaît, entrez une commande comme **dir** à l'invite Telnet pour rétablir.
7. À l'invite de **Telnet**, tapez **exit**.

| |
|---|
| **Question** : Comment pouvez-vous savoir que la SA de mode rapide sécurise en particulier le trafic Telnet ? |
| **Réponse** :…… …… …… ….. |

Il faut maintenant désactiver le GPO IPSec afin qu'il n'interfère pas avec l'exercice suivant.

8. Sur **WIN2008R2**, ouvrez la console **GPM**.
9. Dans l'arborescence de la console **GPM**, vérifier que le domaine domaine **test.local** est sélectionné.

10. Dans le volet **Détails**, cliquez-droit sur le GPO nommé **GPO IPSec**, puis choisissez **Lien activé**.
11. Dans la boîte de message **Console de gestion des stratégies de groupe**, cliquez sur **OK** pour modifier l'état lien activé.
12. Vérifiez que l'état **Lien activé du GPO IPSec** est maintenant fixé à **Non**.
13. À l'invite de commande sur **Montreal** et **Quebec**, exécutez la commande **Gpupdate**.

## Exercice 6 : application IPSec en vertu des règles de sécurité de connexion

Dans cet exercice, vous allez configurer les règles de sécurité de connexion sur le domaine, afin que tout le trafic IP entre ces clients soit authentifié.

1. Si ce n'est pas déjà fait, ouvrez une session sur **test** depuis **WIN2008R2** en tant qu'administrateur de domaine.
2. Dans l'arborescence de la console GPM, sous le conteneur Domaines, cliquez-droit sur le nœud **test.local**, puis cliquez sur **Créer un objet GPO dans ce domaine et le lier ici**.
3. Dans la boîte de dialogue **Nouvel objet GPO**, saisissez **GPO de règle de sécurité de connexion**, puis cliquez sur **OK**.
4. Dans la console **GPM**, dans le volet **Détails**, cliquez-droit sur **GPO de règle de sécurité de connexion**, puis, dans le menu contextuel, choisissez **Modifier**.
5. Dans la fenêtre de l'éditeur de gestion des stratégies de groupe, développez Configuration ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Pare-feu Windows avec fonctions avancées de sécurité, puis Pare-feu Windows avec fonctions avancée de sécurité - LDAP: // adresse.

   Ce dernier objet du GPO est souvent appelé nœud **WFAS** (pour *Windows Firewall with Advanced Security*)
6. Dans le noeud WFAS, sélectionnez **Règles de sécurité de connexion**.
7. Cliquez-droit sur le noeud **Règles de sécurité de connexion**, puis, dans le menu contextuel, choisissez **Nouvelle règle**.

L'Assistant **Nouvelle règles de sécurité de connexion** apparaît.

8. Sur la page **Type de règle**, lisez tout le texte, puis, en conservant l'option par défaut d'isolation, cliquez sur **Suivant**.
9. Sur la page **Exigence**, lisez tout le texte, puis cliquez sur **Suivant**.
10. Sur la page **Méthode d'authentification**, conservez la sélection par défaut, puis cliquez sur **Suivant**.
11. Sur la page de **Profil**, conservez la sélection par défaut, puis cliquez sur **Suivant**.
12. Sur la page **Nom**, tapez **Demander l'authentification des données**, puis cliquez sur **Terminer**.
13. Sur **Montreal** et sur **Quebec**, exécutez la commande **Gpupdate** à une invite de commande.
14. Dans le menu Démarrer de **Quebec**, tapez **Montreal** dans Démarrer la recherche, puis appuyez sur **Entrée**.

    Une fenêtre apparaît et affiche le dossier Imprimantes et tous les partages réseau disponibles sur **Montreal**.
15. Ouvrez la console WFAS sur **Quebec**.
16. Dans l'arborescence de la console **WFAS**, développez le nœud ***Analyse*** puis développer le nœud ***Associations de sécurité***.
17. Dans celui-ci, sélectionnez le dossier **Mode principal**, puis le dossier **Mode rapide** vous voyez qu'au moins une SA apparaît dans le volet Détails lors de la sélection de chaque dossier. Consacrez quelques instant à l'examen des informations sur ces SA.

| |
|---|
| **Questions** : Quelle SA révèle-t-elle que la confidentialité ESP est Aucune ? |
| **Réponse** :…… |

| |
|---|
| **Questions** : Pouvez-vous configurer une règle de sécurité de connexion qui ne chiffre que le trafic Telnet ? |

**Réponse** :……...……

……

……

Référence :

Microsoft MCTS (Exam 70-642) Course