Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 8 : Planification d'IPSec et résolution des problèmes

Table des matières

Microsoft®

Notes du formateur

Présentation : 90 minutes

Atelier : 30 minutes

Ce module fournit aux stagiaires les informations nécessaires à la planification et à la résolution des problèmes liés au déploiement du service de sécurité du protocole Internet (IPSec, *Internet Protocol Security*).

À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- expliquer le fonctionnement du service IPSec ;
- expliquer les stratégies IPSec par défaut ainsi que leurs règles et leurs paramètres ;
- planifier un déploiement IPSec ;
- résoudre les problèmes IPSec.

Matériel requis

Pour animer ce module, vous devez disposer des éléments suivants :

- Fichier Microsoft® PowerPoint® 2189A_07.ppt
- Fichier multimédia : *Vue d'ensemble du service IPSec*

Important Il est recommandé d'utiliser PowerPoint 2002 ou une version ultérieure pour afficher les diapositives de ce cours. Si vous utilisez la visionneuse PowerPoint ou une version antérieure de PowerPoint, il est possible que certains éléments des diapositives ne s'affichent pas correctement.

Préparation

Pour préparer ce module, vous devez effectuer les tâches suivantes :

- lire tous les supports de cours de ce module ;
- vous exercer à effectuer les applications pratiques et l'atelier, ainsi que réviser la clé de réponse de l'atelier ;
- visualiser la présentation multimédia ;
- passer en revue les cours et modules de connaissances préalables.

Comment animer ce module

Au moment de votre choix, expliquez aux stagiaires que la planification d'un déploiement IPSec passe par la détermination du moment et de l'endroit où des communications IPSec sont nécessaires pour leur organisation. Dans certains cas, l'utilisation du service IPSec peut être étendue à toute l'organisation. Dans d'autres, en revanche, il vaut mieux utiliser IPSec de manière beaucoup plus restreinte, par exemple, pour sécuriser les communications entre deux ordinateurs.

Pages de procédures, instructions, applications pratiques et ateliers

Expliquez aux stagiaires la relation entre les pages de procédures, les applications pratiques ainsi que les ateliers et ce cours. Un module contient au minimum deux leçons. La plupart des leçons comprennent des pages de procédures et une application pratique. À la fin de toutes les leçons, le module se termine par un atelier.

Pages de procédures

Les pages de procédures permettent au formateur de montrer comment réaliser une tâche. Les stagiaires n'exécutent pas les tâches des pages de procédures avec le formateur, mais utilisent ces procédures pour effectuer les exercices pratiques à la fin de chaque leçon.

Instructions

Les instructions vous fournissent les points de décision essentiels pour le sujet de la leçon en cours. Leur but est d'étayer le contenu et les objectifs de la leçon.

Applications pratiques

Une fois que vous avez couvert le contenu de la section et montré les procédures de la leçon, expliquez aux stagiaires qu'une application pratique portant sur toutes les tâches abordées est prévue à l'issue de la leçon.

Ateliers

À la fin de chaque module, l'atelier permet aux stagiaires de mettre en pratique les tâches traitées et appliquées tout au long du module.

À l'aide de scénarios appropriés à la fonction professionnelle, l'atelier fournit aux stagiaires un ensemble d'instructions dans un tableau à deux colonnes. La colonne de gauche indique la tâche (par exemple : Créer un groupe.). La colonne de droite contient des instructions spécifiques dont les stagiaires auront besoin pour effectuer la tâche (par exemple : À partir de **Utilisateurs et ordinateurs Active Directory**®, double-cliquez sur le nœud de domaine.).

Chaque exercice d'atelier dispose d'une clé de réponse que les stagiaires trouveront sur le CD-ROM du stagiaire s'ils ont besoin d'instructions étape par étape pour terminer l'atelier. Ils peuvent également consulter les applications pratiques et les pages de procédures du module.

Leçon : Compréhension des règles des stratégies par défaut

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Présentation multimédia : Vue d'ensemble du service IPSec

Avant de commencer cette leçon, avertissez les stagiaires que vous ne détaillerez pas toutes les spécificités des algorithmes utilisés. Veillez à bien connaître ces algorithmes ainsi que les paramètres d'échange de clés au cas où les stagiaires vous demanderaient un complément d'informations.

Règles des connexions IPSec

Veillez à ce que les stagiaires comprennent bien les éléments qui constituent une règle IPSec. Il est possible que vous deviez illustrer ces éléments en ouvrant les Stratégies de sécurité IP sur l'ordinateur du formateur et en passant en revue les éléments énumérés dans la diapositive. Informez les étudiants qu'ils utiliseront cet outil dans l'atelier.

Stratégies IPSec par défaut

Lorsque vous abordez ce sujet, insistez sur le fait qu'aucune des stratégies par défaut n'est attribuée par défaut, même si leur attribution permet de protéger les communications au moyen du service IPSec. Les stagiaires peuvent utiliser ces stratégies telles quelles ou comme bases de nouvelles stratégies, voire créer de nouvelles stratégies de toutes pièces. Illustrez la façon dont les stagiaires peuvent importer et exporter les stratégies d'un ordinateur à l'autre, même s'ils n'utilisent pas le service Active Directory pour attribuer les stratégies IPSec.

Règles de la stratégie par défaut Client (en réponse seule)

Lorsque vous abordez les règles de la stratégie Client (en réponse seule) par défaut, insistez sur le fait que celle-ci n'entame pas de communication avec IPSec mais répond si l'autre partie envoie une requête. En d'autres termes, le client prend en charge les communications IPSec, mais ne les entame pas. Pour illustrer le contenu de cette diapositive et des deux suivantes, il se peut que vous deviez revenir au composant logiciel enfichable Microsoft Management Console (MMC) et passer en revue les éléments de la stratégie.

Règles de la stratégie par défaut Serveur (demandez la sécurité)

Comparez cette stratégie avec la précédente. Cette stratégie demande, mais n'exige pas, une communication sécurisée au moyen du service IPSec.

Règles de la stratégie par défaut Sécuriser le serveur (nécessite la sécurité)

Comparez cette stratégie aux deux précédentes et soulignez le fait qu'un serveur utilisant cette stratégie ne répond pas aux autres systèmes qui n'utilisent pas le service IPSec pour protéger leurs communications. La seule exception à cette règle est le trafic ICMP (Internet Control Message Protocol). Par conséquent, vous pouvez effectuer un ping vers un serveur même lorsque cette règle est activée. Expliquez aux stagiaires qu'ils devront peut-être modifier la stratégie par défaut Serveur (demande la sécurité) de manière à interdire toutes les commandes PING ou à n'autoriser que celles venant de certains ordinateurs.

Application pratique : Gestion au moyen de stratégies

Informez les stagiaires que les réponses à cette application pratique, situées sur leur CD-ROM, fournissent plus de détail sur les éléments de l'onglet **Action de filtrage**. Préparez-vous à commenter ces composants si nécessaire en mémorisant les implications de chaque paramètre disponible dans la console MMC.

Leçon : Planification d'un déploiement IPSec

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Vue d'ensemble

Avant de commencer cette leçon, soulignez le fait qu'une bonne partie des choix intervenant dans la planification dépendent de l'infrastructure dans laquelle les stagiaires travaillent. Par exemple, les stagiaires pourraient être amenés à prendre la décision de limiter les communications IPSec aux ordinateurs d'une forêt Active Directory. S'ils choisissent de ne pas le faire, ils devront utiliser l'infrastructure de clés publiques (PKI, *Public Key Infrastructure*) au lieu de Kerberos, et ne pourront pas utiliser la stratégie de groupe pour appliquer une stratégie de groupe dans tout le réseau.

Choix de la méthode de déploiement de la stratégie IPSec

Assurez-vous que les stagiaires comprennent bien qu'ils peuvent appliquer des stratégies IPSec localement même si les ordinateurs font partie d'une infrastructure Active Directory, et donc restreindre la sécurisation IPSec à certains ordinateurs isolés.

Choix de la méthode d'authentification

Expliquez que Kerberos n'est pas toujours un choix possible. Par exemple, les stagiaires ne doivent pas utiliser Kerberos si certains ordinateurs sur le réseau ne font pas partie d'un domaine Active Directory approuvé.

Leçon : Résolution des problèmes de communications IPSec

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Vue d'ensemble

Avant de commencer cette leçon, insistez sur le fait que les problèmes les plus fréquents au niveau des communications IPSec proviennent d'une mauvaise configuration des stratégies elles-mêmes et d'une mauvaise compréhension de l'application de la stratégie de groupe Microsoft Windows® 2003. Invitez les stagiaires qui implémentent le service IPSec dans un environnement à utiliser le moniteur IPSec pour vérifier que le trafic est sécurisé comme prévu. Vous pouvez aussi utiliser le Moniteur réseau pour visualiser les paquets et vérifier qu'ils sont sécurisés comme il se doit. N'oubliez pas que les stagiaires le feront également dans le cadre de l'atelier.

Outils de résolution des problèmes IPSec

Si vous avez effectué une démonstration du trafic sécurisé par IPSec lors de la leçon précédente, il peut être intéressant d'analyser ces outils plus en profondeur et de montrer aux stagiaires les éléments qui prouvent que le flux de trafic est bel et bien sécurisé par le trafic IPSec.

Affichage des informations relatives à l'échange de clés dans l'Observateur d'événements

Veillez à ce que les stagiaires ne quittent pas la formation en ayant l'impression qu'une défaillance au niveau de l'échange de clés est une cause majeure du dysfonctionnement du service IPSec. S'il n'y a pas d'échange de clés, il est probable que la cause du problème se situe ailleurs (une erreur de configuration, par exemple).

Vérification de l'utilisation de RsoP lors de l'application d'une stratégie

Soulignez le fait qu'un environnement de stratégie de groupe trop complexe conduit souvent à une application des stratégies non conforme au but poursuivi, et par conséquent, à un fonctionnement imprévisible d'IPSec. Expliquez qu'il s'agit d'un problème général qui ne touche pas que le service IPSec.

Atelier A : Résolution des problèmes IPSec

Les stagiaires doivent avoir terminé toutes les applications pratiques avant de commencer l'atelier.

Rappelez aux stagiaires qu'ils peuvent revenir aux pages d'instructions et au contenu du module afin d'obtenir de l'aide. La clé de réponse correspondant à chaque atelier est fournie sur le CD-ROM du stagiaire.

Vous devez également effectuer les tâches suivantes pour configurer l'ordinateur Glasgow pour l'atelier.

Tâches	Instructions spécifiques
1. Ouvrir une session sur l'ordinateur Glasgow en tant qu'administrateur nwtraders.	**a.** Appuyez sur CTRL+ALT+SUPPR. **b.** Nom d'utilisateur : Administrateur **c.** Mot de passe : *mot de passe de l'administrateur de la classe*
2. Créer une console MMC avec le composant logiciel enfichable Gestion de la stratégie de sécurité IP configuré pour l'ordinateur local.	**a.** Cliquez sur **Démarrer**, sur **Exécuter**, tapez **mmc** dans la boîte de dialogue **Exécuter** et cliquez sur **OK**. **b.** Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**. **c.** Cliquez sur **Ajouter** et sélectionnez le composant logiciel enfichable **Gestion de la stratégie de sécurité IP**. **d.** Cliquez sur **Ajouter**, sélectionnez **Ordinateur local**, puis cliquez sur **Terminer**. **e.** Cliquez sur **Fermer**, puis sur **OK**.
3. Importer le fichier Glasgow_Base_Start.ipsec au moyen de la console MMC.	**a.** Dans l'arborescence, cliquez avec le bouton droit sur **Stratégies de sécurité IP sur Ordinateur local**. **b.** Pointez sur **Toutes les tâches**. **c.** Sélectionnez **Importer des stratégies**. **d.** Sélectionnez C:\MOC\2189\Labfiles\Glasgow_Base_Start.ipsec. **e.** Cliquez sur **Ouvrir** pour importer les stratégies.
4. Attribuer la stratégie Client_Policy.	**a.** Dans le volet Détails, cliquez avec le bouton droit sur **IPSec_Lab** et sélectionnez **Attribuer**.

Informations de personnalisation

Cette section identifie les caractéristiques des ateliers de ce module et les modifications apportées à la configuration des ordinateurs des stagiaires pendant les ateliers. Ces informations visent à vous aider à répliquer ou personnaliser le cours Microsoft Official Curriculum (MOC).

L'atelier de ce module dépend aussi de la configuration de la classe spécifiée dans la section « Informations de personnalisation » située à la fin du *Guide de configuration automatisée de la classe* du cours 2189, *Planification et maintenance d'une infrastructure réseau Microsoft Windows Server™ 2003*.

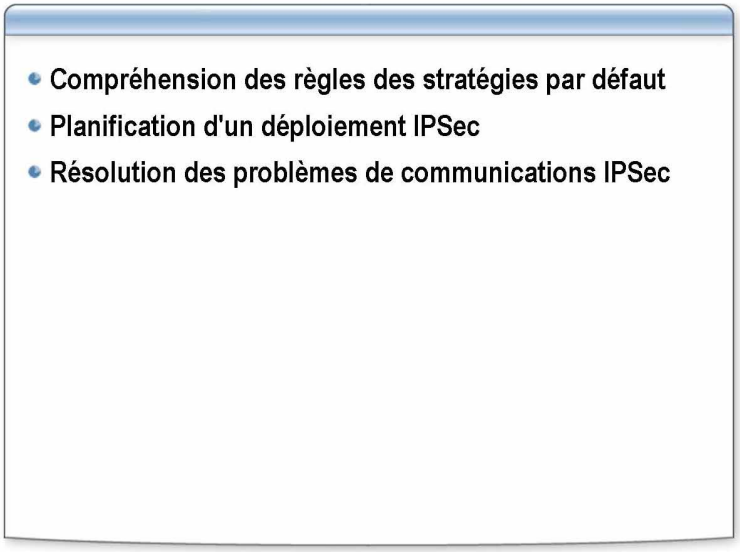
Mise en place de l'atelier

Aucune configuration de mise en place de l'atelier n'affecte la réplication ou la personnalisation.

Résultats de l'atelier

Aucun changement de configuration des ordinateurs des stagiaires n'affecte la réplication ou la personnalisation.

Vue d'ensemble



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

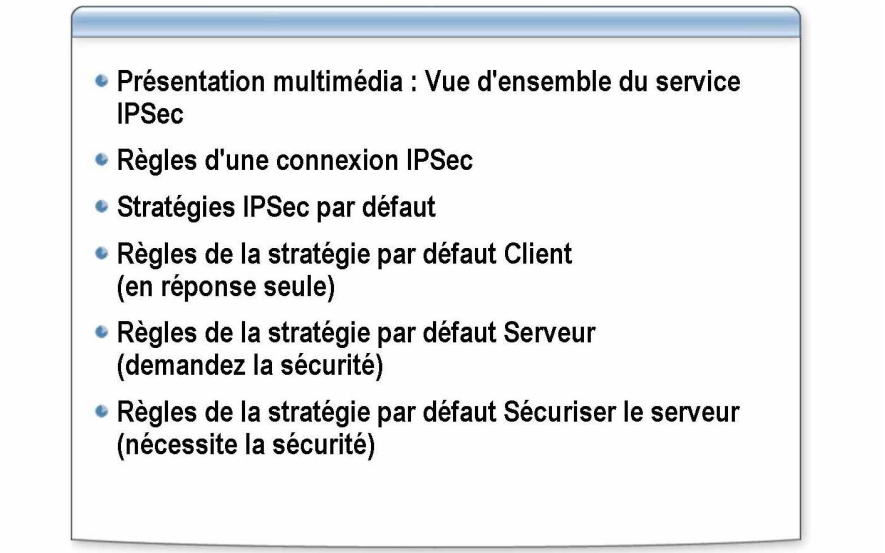
La sécurisation des ressources contre les attaques d'utilisateurs malveillants est un volet important du rôle d'un ingénieur système dans une entreprise. Dans ce module, vous allez apprendre à planifier un déploiement du service de sécurité du protocole Internet (IPSec, *Internet Protocol Security*). Ce module aborde également les outils et les compétences nécessaires à la résolution des problèmes IPSec.

Objectif du module

À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- expliquer le fonctionnement du service IPSec ;
- expliquer les stratégies IPSec par défaut ainsi que leurs règles et leurs paramètres ;
- planifier un déploiement IPSec ;
- résoudre les problèmes IPSec.

Leçon : Compréhension des règles des stratégies par défaut



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

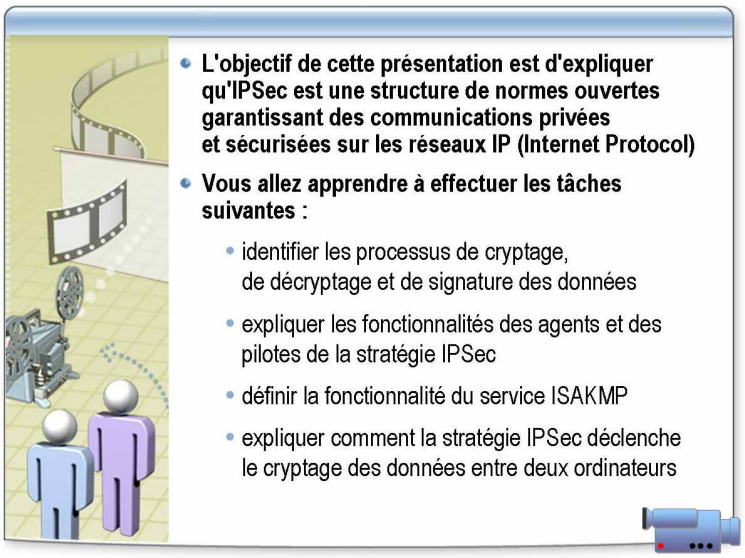
Une configuration particulière du service IPSec est couramment appelée « stratégie IPSec ». Chaque stratégie IPSec comprend ses propres règles auxquelles sont associés des paramètres. Ce module définit les stratégies IPSec par défaut et examine les règles qui y sont associées.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les règles d'une stratégie IPSec donnée ;
- décrire les trois stratégies IPSec par défaut ;
- comprendre les règles de la stratégie IPSec par défaut Client ;
- comprendre les règles de la stratégie IPSec par défaut Serveur ;
- comprendre les règles de la stratégie IPSec par défaut Sécuriser le serveur.

Présentation multimédia : Vue d'ensemble du service IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Emplacement du fichier

Pour visionner la présentation *Vue d'ensemble du service IPSec*, ouvrez la page Web sur le CD-ROM du stagiaire, cliquez sur **Multimédia**, puis cliquez sur le titre de la présentation.

Objectifs

Après avoir visionné cette présentation, vous serez à même d'effectuer les tâches suivantes :

- identifier les processus de cryptage, de décryptage et de signature des données ;
- expliquer les fonctionnalités des agents et des pilotes de la stratégie IPSec ;
- définir la fonctionnalité du service ISAKMP (Internet Security Association and Key Management Protocol) ;
- expliquer comment la stratégie IPSec déclenche le cryptage des données entre deux ordinateurs.

Questions clés

Pendant que vous visionnez la présentation, posez-vous les questions suivantes :

- Que se passe-t-il si aucune stratégie IPSec n'est attribuée au service d'annuaire Active Directory® ni au registre de l'ordinateur local ?
- Quel événement déclenche l'échange des clés de sécurité ?
- Quel protocole centralise l'administration des associations de sécurité ?
- Comment la stratégie IPSec déclenche-t-elle le cryptage des données entre deux ordinateurs ?

Règles d'une connexion IPSec

Règle	Description
Liste de filtres IP	Spécifie le trafic réseau qui sera sécurisé, par l'utilisation de filtres d'entrée et de sortie
Action de filtrage	Spécifie le mode de traitement du trafic correspondant au filtre (rejet, cryptage, etc)
Méthodes d'authentification	Spécifie le mode d'authentification entre deux ordinateurs (Kerberos, clé pré-partagée ou certificats X509)
Point de sortie du tunnel	Permet de spécifier un point de sortie pour les tunnels IPSec
Type de connexion	Permet l'application de la règle au trafic de réseau local, de réseau étendu ou des deux

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Une stratégie IPSec se compose d'une ou plusieurs règles qui déterminent le comportement du service IPSec. Chaque règle IPSec contient ses propres paramètres configurables. Les règles IPSec peuvent être configurées dans les propriétés d'une stratégie IPSec, onglet **Règles**. La section suivante énumère et décrit les différentes règles et leurs paramètres de configuration.

Liste de filtres IP

La liste de filtres contient un ou plusieurs filtres de paquets prédéfinis décrivant les types de trafic auxquels l'action du filtre configuré pour cette règle est appliquée. Une seule liste peut être sélectionnée à la fois. La liste de filtres peut être configurée dans les propriétés d'une règle IPSec, onglet **Liste de filtres IP**.

Action de filtrage

L'action de filtrage indique le type d'action requis (Autoriser, Refuser ou Négocier la sécurité) pour les paquets qui correspondent à la liste de filtres. Une seule action peut être sélectionnée à la fois. Pour l'action de filtrage Négocier la sécurité, les données de négociation contiennent plusieurs paramètres IPSec, dont une ou plusieurs méthodes de sécurité utilisées, par ordre de préférence, lors des négociations d'échange de clés Internet (IKE, *Internet Key Exchange*). Chaque méthode de sécurité détermine son protocole de sécurité (AH = authentification de l'en-tête ; ESP = Encapsulating Security Payload), les algorithmes de cryptographie et de hachage spécifiques, ainsi que les paramètres de régénération de clé de session utilisés. L'action de filtrage peut être configurée dans les propriétés d'une règle IPSec, onglet **Action de filtrage**.

Méthodes d'authentification

Une ou plusieurs méthodes d'authentification sont configurées (par ordre de préférence) et utilisées pour l'authentification d'homologues IPSec lors des négociations en mode principal. Les méthodes d'authentification disponibles sont la version 5 du protocole Kerberos (Kerberos V5) et l'utilisation d'un certificat délivré par une autorité de certification ou d'une clé pré-partagée. Les données de négociation peuvent être configurées dans les propriétés d'une règle IPSec, onglet **Méthodes d'authentification**.

Point de sortie du tunnel

Le point de terminaison du tunnel indique le tunneling ou l'absence de tunneling du trafic, et dans le premier cas, l'adresse de protocole Internet (IP, *Internet Protocol*) de ce point. Pour le trafic sortant, le point de terminaison du tunnel est l'adresse IP du tunnel homologue. Pour le trafic entrant, le point de terminaison du tunnel est une adresse IP locale. Le point de terminaison du tunnel peut être configuré dans les propriétés d'une règle IPSec, onglet **Paramètres du tunnel**.

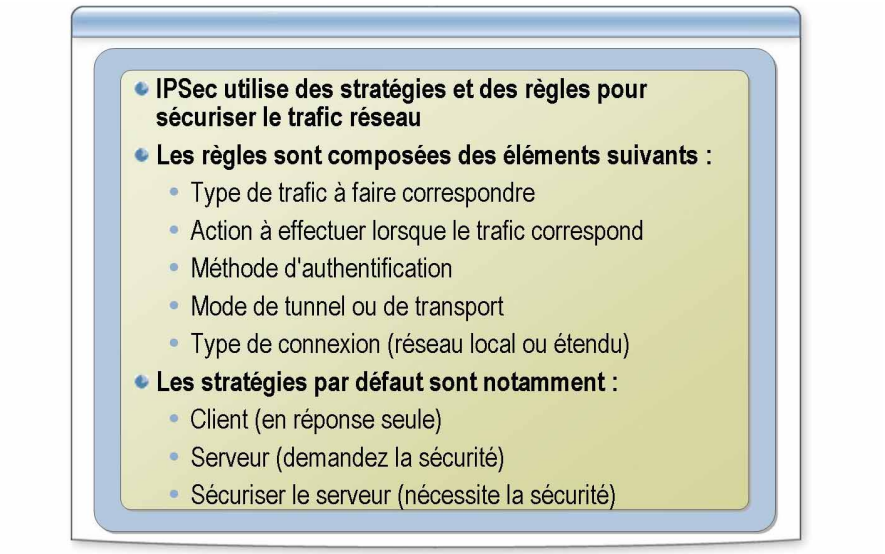
Type de connexion

Le type de connexion indique si la règle s'applique à des connexions de réseau local (LAN, *Local Area Network*), à des connexions à distance, ou aux deux. Le type de connexion peut être configuré dans les propriétés d'une règle IPSec, onglet **Type de connexion**.

Modalités d'application des règles

Les règles d'une stratégie sont affichées dans l'Éditeur d'objets de stratégie de groupe. Elles sont réparties dans quatre catégories : Configuration ordinateur, Paramètres Windows, Paramètres de sécurité et Stratégies de sécurité IP. Les règles sont classées par ordre alphabétique décroissant sur la base du nom de la liste de filtres sélectionnée. Il n'existe aucune méthode permettant de préciser l'ordre d'application des règles d'une stratégie. Le pilote IPSec applique automatiquement les règles correspondant à la liste de filtres la plus spécifique en premier lieu. Par exemple, le pilote IPSec appliquera une règle contenant une liste de filtres qui spécifie des adresses IP et des ports TCP (Transmission Control Protocol) isolés avant une règle contenant une liste de filtres qui spécifie toutes les adresses d'un sous-réseau.

Stratégies IPSec par défaut



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Microsoft® Windows® XP et la famille Microsoft Windows Server™ 2003 fournissent un ensemble de listes de filtres et d'actions de filtrage prédéfinies ainsi qu'une série de stratégies IPSec par défaut. Ces éléments prédéfinis sont fournis à titre d'exemple uniquement, et ne sont pas conçus pour être utilisés en l'état. Pour pouvoir être utilisées de manière effective, ces stratégies doivent être personnalisées, voire recréées, par un administrateur de réseau IPSec averti ou un utilisateur expérimenté.

Tout ordinateur connecté à Internet doit être soigneusement protégé contre les attaques réseau au moyen de stratégies personnalisées. Les stratégies fournies par défaut sont des exemples pour intranets parce qu'elles autorisent un ordinateur à recevoir du trafic non sécurisé. Les stratégies par défaut sont conçues pour des ordinateurs qui font partie d'un domaine Active Directory.

Voici les trois stratégies par défaut prédéfinies :

- Client (en réponse seule)
- Serveur (demandez la sécurité)
- Sécuriser le serveur (nécessite la sécurité)

Client (en réponse seule)

La stratégie par défaut Client (en réponse seule) est conçue pour les ordinateurs qui sécurisent les communications à la demande. Par exemple, les clients d'un intranet ne requièrent pas toujours la sécurisation au moyen du service IPSec, mais uniquement lorsqu'un autre ordinateur le demande. Cette stratégie autorise l'ordinateur sur lequel elle est activée à répondre à des requêtes de communications sécurisées. La stratégie intègre la règle de réponse par défaut, qui crée des filtres IPSec dynamiques pour le trafic entrant et sortant sur la base du protocole demandé et du trafic du port correspondant à la communication en cours de sécurisation.

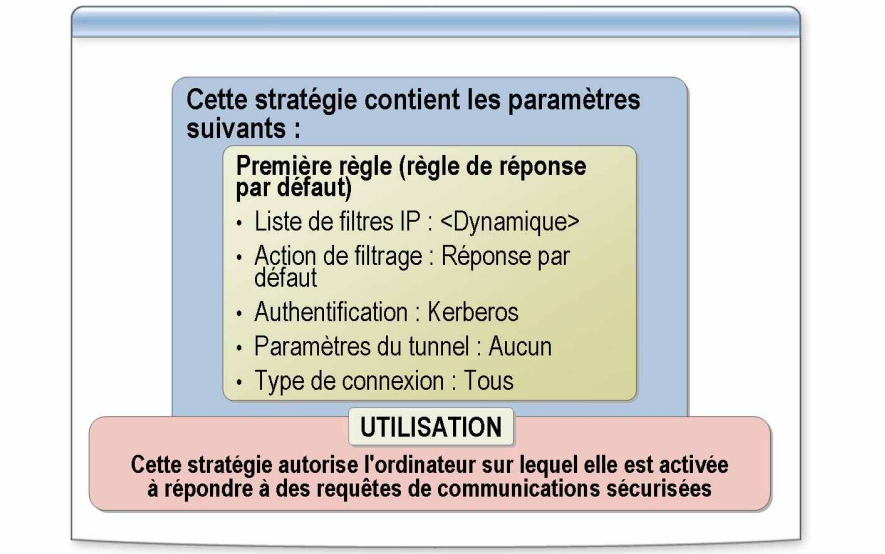
Serveur (demandez la sécurité)

La stratégie par défaut Serveur (demandez la sécurité) est conçue pour les ordinateurs qui demandent des communications IP sécurisées mais qui autorisent les communications IP non sécurisées avec les ordinateurs qui ne connaissent pas le protocole IPSec.

Sécuriser le serveur (nécessite la sécurité)

La stratégie par défaut Sécuriser le serveur (nécessite la sécurité) est conçue pour les ordinateurs d'un intranet exigeant des communications sécurisées, comme un serveur transmettant des données sensibles. Les filtres utilisés dans cette stratégie exigent la sécurisation de toutes les communications sortantes et entrantes, à l'exception de la requête initiale de communication entrante.

Règles de la stratégie par défaut Client (en réponse seule)



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

La stratégie par défaut Client (en réponse seule) est un exemple de stratégie conçu pour les ordinateurs qui sécurisent leurs communications à la demande. Cette stratégie autorise l'ordinateur sur lequel elle est activée à répondre à des requêtes de communications sécurisées. Elle intègre la règle de réponse par défaut, qui crée des filtres IPSec dynamiques pour le trafic entrant et sortant sur la base du protocole demandé et du trafic du port correspondant à la communication en cours de sécurisation.

Règle de la stratégie

La stratégie Client (en réponse seule) est paramétrée comme suit :

- Première règle (règle de réponse par défaut)

  Il s'agit de la règle de réponse par défaut qui vaut pour toutes les stratégies. Cette règle ne peut pas être supprimée, mais uniquement désactivée. Elle est activée par défaut dans toutes les stratégies.

- Liste de filtres IP : <Dynamique>

  Ce paramètre indique que la liste de filtres n'est pas préconfigurée. Tous les filtres sont créés automatiquement sur la base de la réception des paquets de négociation IKE.

- Action de filtrage : Réponse par défaut

  Ce paramètre indique que l'action du filtre n'est pas configurable. L'action de filtrage Négocier la sécurité est utilisée.

- Méthodes d'authentification : Kerberos

  Ce paramètre sélectionne l'authentification Kerberos pour toutes les authentifications.

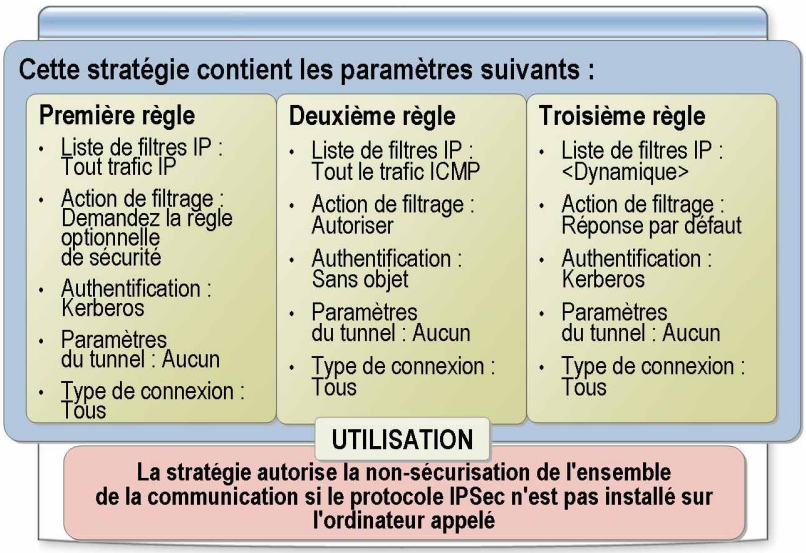
- Point de sortie du tunnel : Aucun

  Cette stratégie ne contient aucun paramètre de tunnel.

- Type de connexion : Tous

  Cette règle s'applique à tous les types de connexion.

Règles de la stratégie par défaut Serveur (demandez la sécurité)



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Avec la stratégie Serveur (demandez la sécurité), l'ordinateur accepte le trafic non sécurisé mais essaie toujours de sécuriser les communications supplémentaires en demandant la sécurité auprès de l'expéditeur initial.

Stratégie par défaut Serveur (demandez la sécurité)

La stratégie par défaut Serveur (demandez la sécurité) est un exemple de stratégie conçu pour les ordinateurs dont les communications devraient être sécurisées dans la plupart des cas. La stratégie autorise la non-sécurisation de l'ensemble de la communication si le protocole IPSec n'est pas installé sur l'ordinateur appelé. Cette stratégie autorise un serveur à sécuriser ses communications avec certains serveurs et, en même temps, à ne pas le faire avec les clients qui ne prennent pas en charge le protocole IPSec.

Règles de la stratégie

La stratégie par défaut Serveur (demandez la sécurité) comprend trois règles. La première règle sert à exiger la sécurisation de tout le trafic IP, la deuxième à autoriser le trafic ICMP (Internet Control Message Protocol) et la troisième (Réponse par défaut) à répondre aux demandes de sécurité émanant d'autres ordinateurs.

La stratégie par défaut Serveur (demandez la sécurité) est paramétrée comme suit :

Première règle

La première règle de la stratégie Serveur (demandez la sécurité) est paramétrée comme suit :

- Liste de filtres IP : Tout trafic IP

  Cette liste de filtres s'applique à tout le trafic IP.
- Action de filtrage : Demandez la sécurité (optionnel)

  Cette règle spécifie que l'ordinateur doit demander la sécurité.
- Méthodes d'authentification : Kerberos

- Point de sortie du tunnel : Aucun

  Aucune adresse IP de destination n'est spécifiée dans les paramètres du tunnel.

- Type de connexion : Tous

  Cette règle s'applique à tous les types de connexion.

Deuxième règle

La deuxième règle de la stratégie Serveur (demandez la sécurité) est paramétrée comme suit :

- Liste de filtres IP : Tout le trafic ICMP

  Cette liste de filtres s'applique à tout le trafic ICMP.

- Action de filtrage : Autoriser

  Cette règle oblige IPSec à transmettre le trafic ICMP sans modifier les spécifications de sécurité.

- Méthodes d'authentification : Aucun

  Aucune méthode d'authentification n'est associée à cette règle.

- Point de sortie du tunnel : Aucun

  Aucun paramètre de tunnel n'est associé à cette règle.

- Type de connexion : Tous

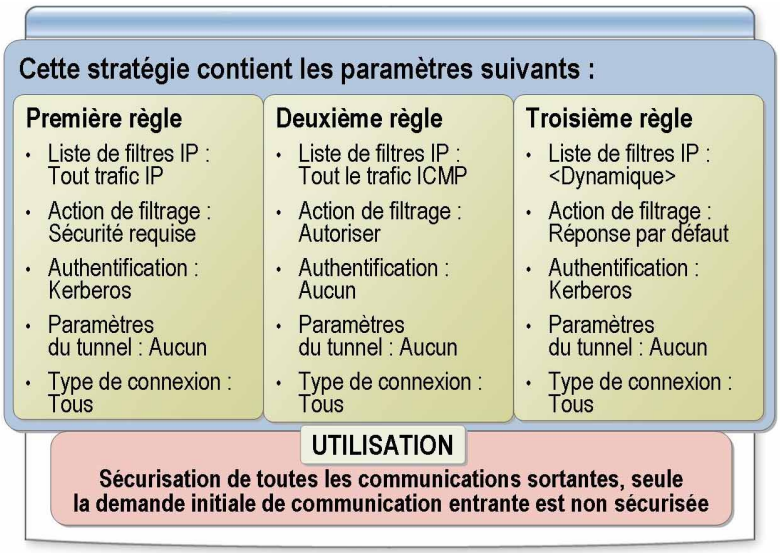
  Cette règle s'applique à tous les types de connexion.

Troisième règle (règle de réponse par défaut)

La troisième règle de la stratégie Serveur (demandez la sécurité) est paramétrée comme suit :

- Liste de filtres IP : <Dynamique>
- Action de filtrage : Réponse par défaut
- Méthodes d'authentification : Kerberos
- Point de sortie du tunnel : Aucun
- Type de connexion : Tous

Règles de la stratégie par défaut Sécuriser le serveur (nécessite la sécurité)



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

La stratégie par défaut Sécuriser le serveur (nécessite la sécurité) est un exemple de stratégie conçu pour les ordinateurs d'un intranet exigeant des communications sécurisées. Exemple : un serveur transmettant des données sensibles.

Stratégie par défaut Sécuriser le serveur (nécessite la sécurité)

Les administrateurs peuvent utiliser cette stratégie IPSec comme modèle lors de la création de leur propre stratégie personnalisée à usage effectif. Les filtres utilisés dans cette stratégie exigent la sécurisation de toutes les communications sortantes et entrantes, à l'exception de la requête initiale de communication entrante.

Règles de la stratégie

La stratégie par défaut Sécuriser le serveur (nécessite la sécurité) comprend trois règles. La première règle sert à exiger la sécurisation de tout le trafic IP, la deuxième à autoriser le trafic ICMP et la troisième (Réponse par défaut) à répondre aux demandes de sécurité émanant d'autres ordinateurs.

Première règle

La première règle de la stratégie Sécuriser le serveur (nécessite la sécurité) est paramétrée comme suit :

- Liste de filtres IP : Tout trafic IP
- Action de filtrage : Sécurité requise

  L'action de filtrage requiert la sécurisation de toutes les connexions.
- Méthodes d'authentification : Kerberos
- Point de sortie du tunnel : Aucun
- Type de connexion : Tous

Deuxième règle

La deuxième règle de la stratégie Sécuriser le serveur (nécessite la sécurité) est paramétrée comme suit :

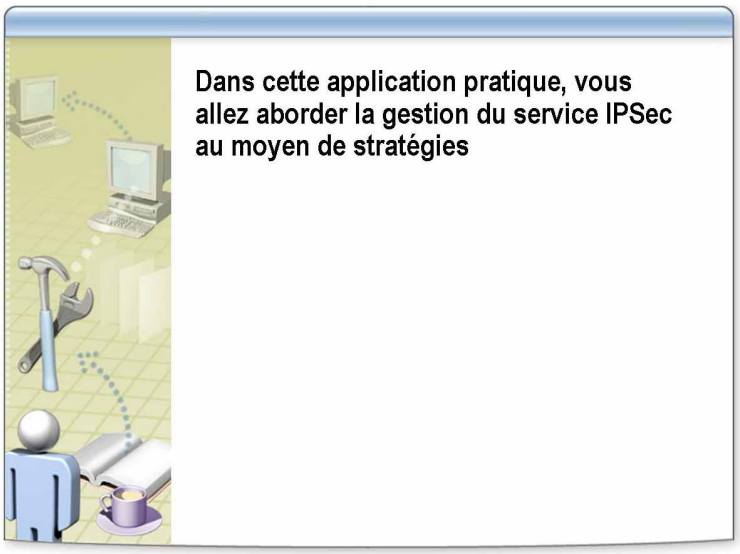
- Liste de filtres IP : Tout le trafic ICMP
- Action de filtrage : Autoriser
- Méthodes d'authentification : Aucun
- Point de sortie du tunnel : Aucun
- Type de connexion : Tous

Troisième règle (règle de réponse par défaut)

La troisième règle de la stratégie Sécuriser le serveur (nécessite la sécurité) est paramétrée comme suit :

- Liste de filtres IP : <Dynamique>
- Action de filtrage : Réponse par défaut
- Méthodes d'authentification : Kerberos
- Point de sortie du tunnel : Aucun
- Type de connexion : Tous

Application pratique : Gestion au moyen de stratégies



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Dans cette application pratique, vous allez aborder la gestion du service IPSec au moyen de stratégies.

Objectif

L'objectif de cette application pratique est de présenter la gestion du service IPSec au moyen de stratégies.

Instructions (facultatif)

1. Lisez le scénario.
2. Préparez une discussion sur les défis posés par cette tâche qui suivra l'application pratique.

Scénario

Le responsable du service informatique de la société Trey Research vous a engagé comme consultant sur un projet commun avec la société Proseware, Inc. Les deux sociétés ont signé un contrat de recherche conjointe et projettent d'échanger leurs données sur Internet. La sécurité fait partie des préoccupations des deux sociétés, qui souhaitent qu'aucune personne étrangère ne puisse lire ni modifier les informations qu'elles échangent.

Les deux sociétés ont installé Windows Server 2003. Trey Research a implémenté une forêt Active Directory et Proseware, Inc. dispose de trois ordinateurs autonomes équipés de Windows Server 2003. Le département informatique de Trey Research a suggéré de sécuriser les communications entre les deux sociétés au moyen du service IPSec, mais aucune des deux ne connaît le produit dans la pratique.

Les sociétés vous ont envoyé leur avant-projet ainsi que leurs suggestions. L'avant-projet prévoit l'utilisation de la stratégie par défaut Sécuriser le serveur (nécessite la sécurité) dans les deux sociétés.

Application pratique

Quelles suggestions adresseriez-vous au responsable du service informatique de Trey Research ? Commentez-les.

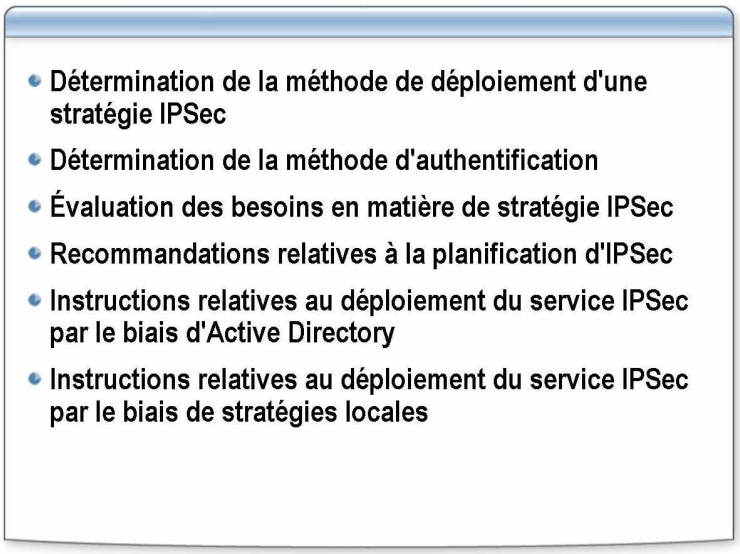
Vous devriez recommander à Trey Research de ne pas utiliser la stratégie par défaut dans sa configuration actuelle.

En effet, le premier problème posé par l'avant-projet est que la première règle, qui s'applique à tout le trafic IP, utilise Kerberos comme méthode d'authentification. Ceci ne fonctionnera pas parce qu'il n'y a pas d'approbation Active Directory entre les deux organisations. Vous devriez suggérer aux planificateurs d'opter pour la méthode d'authentification par certificats de clés publiques.

Le deuxième problème est que les stratégies par défaut sont conçues pour des intranets et, par conséquent, autorisent le trafic non sécurisé. Les planificateurs doivent modifier la stratégie par défaut s'ils comptent ouvrir un ordinateur à Internet.

La règle Action de filtrage doit aussi être examinée pour vérifier que les paramètres de cryptographie, de hachage et de régénération des clés de session correspondent aux besoins des deux sociétés.

Leçon : Planification d'un déploiement IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

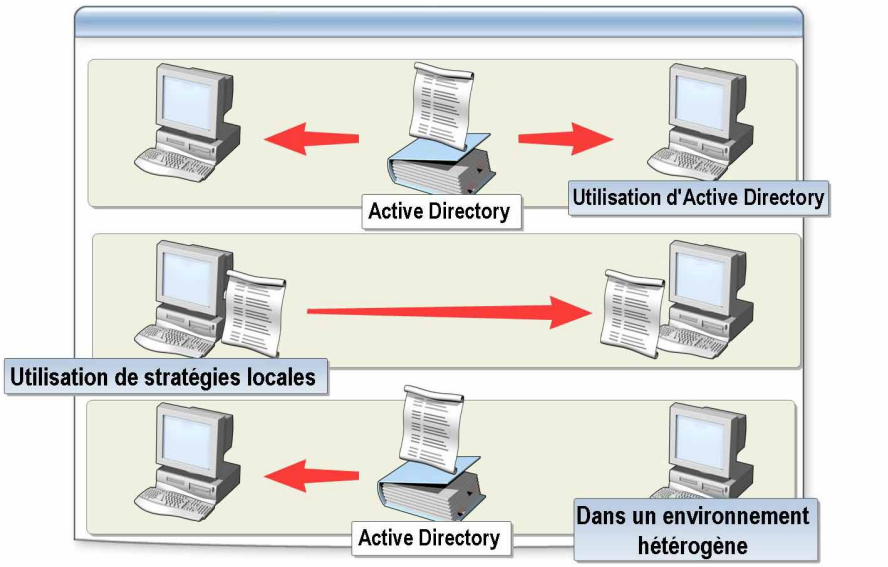
Cette leçon aborde les principes de la planification d'un déploiement IPSec. Elle couvre également les informations nécessaires pour la planification de l'accès entre réseaux privés ainsi que les éléments nécessaires au choix de la stratégie à implémenter.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- désigner les systèmes et les adresses IP qui seront intégrés au réseau privé ;
- déterminer le modèle par défaut idéal en fonction de la situation ;
- planifier un accès sécurisé entre les deux réseaux privés ;
- choisir la méthode d'implémentation de la stratégie ;
- prévoir l'optimisation nécessaire.

Détermination de la méthode de déploiement d'une stratégie IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Lorsque vous planifiez un déploiement IPSec, vous devez songer à la manière dont vous allez stocker et déployer les stratégies IPSec. Il existe deux manières de déployer les stratégies IPSec : utiliser Active Directory ou utiliser des stratégies locales.

Déploiement par le biais d'Active Directory

Vous pouvez attribuer des stratégies IPSec à l'objet Stratégie de groupe (GPO, *Group Policy Object*) d'un site, d'un domaine ou d'une unité d'organisation. Lorsqu'une stratégie IPSec est attribuée à un des GPO de l'objet Active Directory, elle se propage à tous les comptes d'ordinateurs concernés par ce GPO.

Pour administrer une stratégie Active Directory, utilisez la console Gestion de la stratégie de sécurité IP ou la commande **netsh**.

Une stratégie Active Directory remplace toute stratégie IPSec locale attribuée et, le cas échéant, se greffe sur la stratégie IPSec permanente déjà appliquée par l'agent de stratégie IPSec. En cas de conflit entre une stratégie IPSec locale ou une stratégie de domaine d'une part, et une stratégie permanente d'autre part, ce sont les paramètres de cette dernière qui l'emportent.

L'attribution d'une stratégie IPSec dans Active Directory doit tenir compte des éléments suivants :

- La série complète de stratégies IPSec peut être attribuée à n'importe quel niveau de la hiérarchie Active Directory. Toutefois, une seule stratégie IPSec peut être attribuée par niveau de hiérarchie.
- Une stratégie IPSec attribuée à une unité d'organisation dans Active Directory est prépondérante en cas de conflit avec une stratégie de domaine portant sur les membres de cette organisation.
- Une stratégie IPSec attribuée à l'unité d'organisation occupant le dernier niveau de la hiérarchie du domaine supplante toute stratégie IPSec attribuée à un niveau supérieur dans l'unité pour les ordinateurs membres de celle-ci.

- Une unité d'organisation hérite de la stratégie de son unité parente à moins que l'héritage de stratégies ne soit explicitement bloqué, ou qu'une stratégie n'ait été attribuée de forme explicite.
- Il est impossible de fusionner les stratégies IPSec d'unités d'organisation différentes.
- Les stratégies doivent être attribuées au plus haut niveau dans la hiérarchie Active Directory afin de réduire le temps de configuration et d'administration nécessaire.

Quand faut-il utiliser Active Directory pour déployer une stratégie IPSec ?

L'utilisation d'Active Directory pour le déploiement des stratégies IPSec est recommandée lorsque l'entreprise concernée réunit les critères suivants :

- Une infrastructure Active Directory est déjà en place.
- Le nombre d'ordinateurs justifie une attribution IPSec groupée.
- La stratégie IPSec de l'organisation doit être centralisée.

Déploiement par le biais de stratégies locales

Un seul GPO local, souvent appelé *stratégie de l'ordinateur local*, est stocké dans un ordinateur local. Ce GPO local vous permet de stocker des paramètres de stratégie de groupe sur des ordinateurs isolés indépendamment de leur appartenance à un domaine Active Directory.

Dans un réseau sans domaine Active Directory (c'est-à-dire, sans contrôleur de domaine Windows 2000 ou Windows Server 2003), ce sont les paramètres du GPO local qui déterminent le comportement du service IPSec parce qu'ils n'ont pas encore été remplacés par d'autres GPO. Un GPO local peut être remplacé par tout GPO associé à un site, un domaine ou une unité d'organisation faisant partie d'un environnement Active Directory.

Les paramètres d'une stratégie IPSec locale sont ajoutés, le cas échéant, à toute stratégie permanente déjà configurée. Les paramètres d'une stratégie IPSec Active Directory sont prépondérants lorsque l'ordinateur concerné est connecté à un domaine Active Directory.

Quand faut-il utiliser une stratégie locale ?

L'utilisation d'une stratégie locale est recommandée dans les cas de figure suivants :

- Aucune infrastructure Active Directory n'est en place, ou le nombre d'ordinateurs devant utiliser IPSec est limité.
- La stratégie IPSec de l'organisation ne doit pas être centralisée.

Déploiement dans un environnement hétérogène

Le déploiement d'IPSec peut se faire dans un environnement mixte contenant à la fois des ordinateurs membres d'un domaine, qui reçoivent leur stratégie IPSec par le biais d'une stratégie de groupe Active Directory, et des ordinateurs ne faisant pas partie d'un domaine, qui reçoivent leur stratégie IPSec par le biais d'une stratégie de groupe locale. Dans ce cas, indépendamment de la provenance de leur stratégie IPSec, les deux ordinateurs amenés à communiquer négocient sur la base des règles définies dans leur stratégie.

Détermination de la méthode d'authentification

Méthode d'authentification	Utilisation
Protocole de sécurité V5 Kerberos	• Clients et serveurs exécutant Windows 2000 (et versions ultérieures) appartenant à un domaine Active Directory
Certificat de clé publique	• Accès Internet • Accès distant aux ressources d'entreprise • Partenaires commerciaux externes • Ordinateurs n'exécutant pas le protocole de sécurité V5 Kerberos
Clé secrète pré-partagée	• Lorsque les deux ordinateurs doivent configurer manuellement IPSec

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Une méthode d'authentification doit toujours être associée à une stratégie IPSec. Les règles d'une stratégie IPSec comprennent une liste de méthodes d'authentification qui définissent les exigences en matière de contrôle des identités. La méthode d'authentification choisie dépend des ordinateurs concernés et du niveau de sécurité requis.

Méthodes d'authentification

Si les ordinateurs font partie d'un domaine Active Directory, l'authentification IPSec de mode principal se fait par le biais de la méthode d'authentification par défaut. Dans ce cas, il n'est pas nécessaire de déployer un certificat de clé publique pour la communication intranet. Attention, les ordinateurs équipés de Microsoft Windows XP Édition familiale ne prennent pas en charge la méthode d'authentification Kerberos V5. L'authentification par certificats constitue une alternative possible.

Une seule méthode peut être utilisée par paire d'ordinateurs, indépendamment du nombre de méthodes configurées. Si plusieurs règles s'appliquent à la même paire d'ordinateurs, une méthode d'authentification commune doit être configurée pour que les deux PC puissent utiliser la même méthode.

Protocole de sécurité Kerberos V5

Le protocole de sécurité Kerberos V5 est la technologie d'authentification par défaut. Cette méthode est valable pour tous les clients équipés du protocole Kerberos V5 (qu'ils exécutent Windows 2000, Windows XP Professionnel ou la famille Windows Server 2003) et membres d'un même domaine ou de domaines approuvés.

Certificat de clé publique

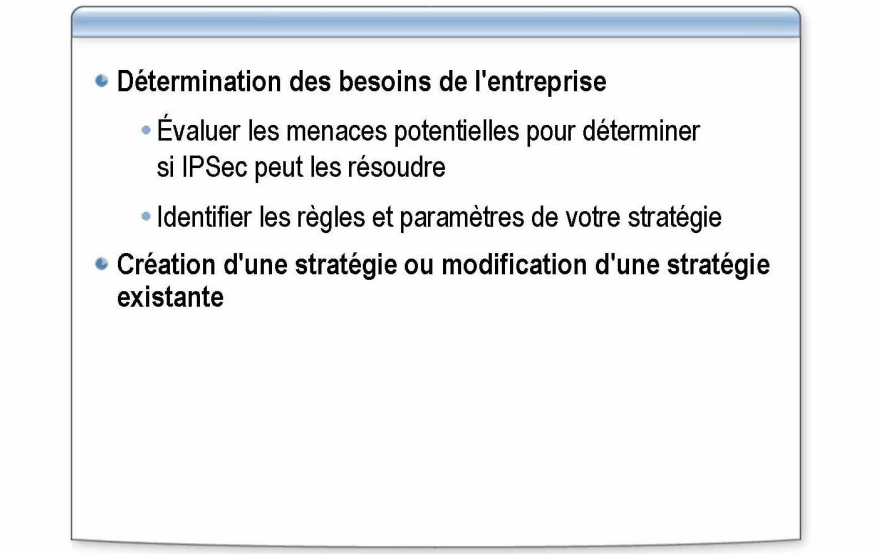
Le certificat de clé publique est la méthode qui convient le mieux aux situations impliquant un accès à Internet, un accès distant à des ressources centralisées, des communications avec des partenaires externes, ou des ordinateurs qui ne sont pas équipés du protocole Kerberos V5.

L'utilisation d'un certificat de clé publique requiert la configuration d'au moins une autorité de certification approuvée et du certificat de celle-ci. Les ordinateurs équipés de Windows 2000, Windows XP ou la famille Windows Server 2003 prennent en charge les certificats X.509 Version 3, y compris les certificats d'ordinateurs générés par les autorités de certification commerciales.

Clé secrète pré-partagée

Les clés secrètes partagées sont très conviviales car elles n'exigent pas la prise en charge du protocole Kerberos V5 ou l'utilisation d'un certificat de clé publique par le client. Les deux parties doivent indiquer explicitement l'utilisation de cette clé pré-partagée dans la configuration d'IPSec.

Évaluation des besoins en matière de stratégie IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Le choix de la stratégie IPSec dépend des critères établis dans le document de conception rédigé par la société cliente. Généralement, l'architecte réseau décrit le niveau de sécurité requis dans le document de conception. Cette information permet d'évaluer la nécessité d'une stratégie par défaut comme point de départ du plan de sécurité.

Évaluation des besoins en matière de stratégie IPSec

Au moment de choisir la stratégie IPSec qui sera utilisée, il est parfois nécessaire de créer une nouvelle stratégie et de la comparer avec la stratégie par défaut la plus proche des besoins de l'entreprise. La modification d'une stratégie existante est une autre possibilité. Par ailleurs, l'option Restaurer les stratégies par défaut du composant logiciel enfichable Gestion de la stratégie de sécurité IP permet de rétablir les stratégies d'origine lorsque trop de modifications ont été apportées.

Exemple

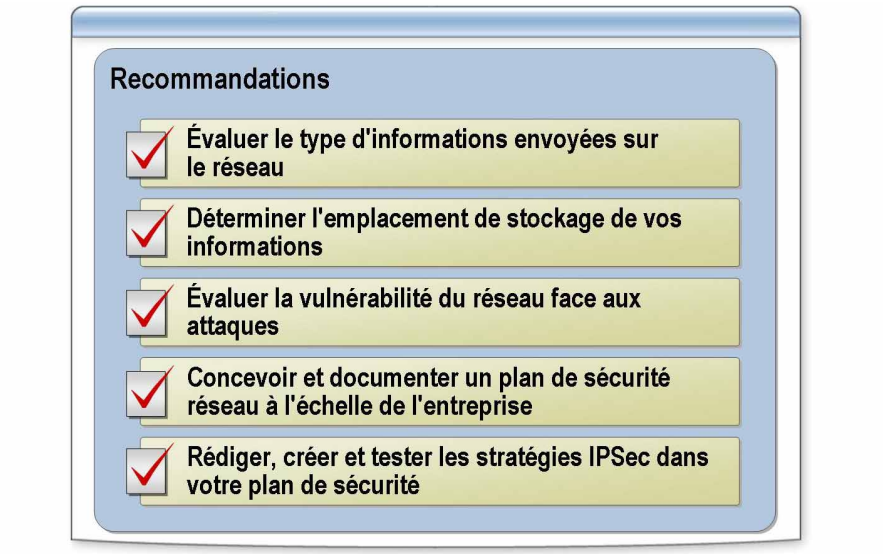
Par exemple, la stratégie par défaut Sécuriser le serveur (nécessite la sécurité) semble être une stratégie très sûre puisqu'elle exige la sécurisation de toute communication IP sortante.

Toutefois, elle utilise également une action de filtrage Sécurité requise prédéfinie qui autorise les paquets de requête de connexion entrants. La réponse de l'ordinateur à cette requête de connexion passe par le filtre sortant, ce qui provoque l'envoi d'une requête de sécurité à l'expéditeur du trafic non sécurisé. Si la négociation aboutit, le trafic est sécurisé dans les deux sens.
Si la négociation échoue, le trafic sortant n'est pas autorisé. L'ordinateur continue alors à recevoir le trafic entrant non sécurisé et à négocier la sécurité.

Par conséquent, si l'ordinateur est utilisé pour établir une connexion sécurisée avec des ordinateurs sur Internet, il pourrait être la cible d'attaques de refus de service. Il sera peut-être préférable, pour cette raison, de personnaliser cette action de filtrage avant de l'utiliser. Une modification possible consisterait à désactiver la case à cocher **Accepter les communications non sécurisées mais toujours répondre en utilisant IPSec** sur la page Action de filtrage, Méthodes de sécurité sur le serveur, ou de configurer les clients pour qu'ils initient une négociation de sécurité avec le serveur au lieu d'utiliser une règle de réponse par défaut.

Avertissement Les modifications de stratégie IPSec sont de préférence implémentées par des spécialistes de la sécurité Windows expérimentés qui peuvent en comprendre toutes les propriétés et tous les paramètres, ainsi que leurs ramifications et les conséquences. Avant de procéder à ces changements et à leur déploiement dans votre organisation, demandez conseil à un spécialiste de sécurité Windows.

Recommandations relatives à la planification d'IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Microsoft a prévu quelques recommandations à prendre en compte lors de la planification d'un déploiement IPSec. Les recommandations suivantes ont pour but de vous aider dans votre tâche de planification.

Recommandations

Le composant logiciel enfichable Gestion de la stratégie de sécurité IP pour Windows 2000 simplifie considérablement le déploiement. Les recommandations suivantes permettent de tirer le meilleur parti de cet outil, et d'éviter les problèmes d'implémentation :

- Évaluez le type d'informations envoyées sur le réseau.

  Ces informations comprennent-elles des données financières confidentielles, des informations propriétaires ou des messages électroniques ? Certains départements requièrent parfois un niveau de sécurité supérieur en raison de la nature de leur fonction.

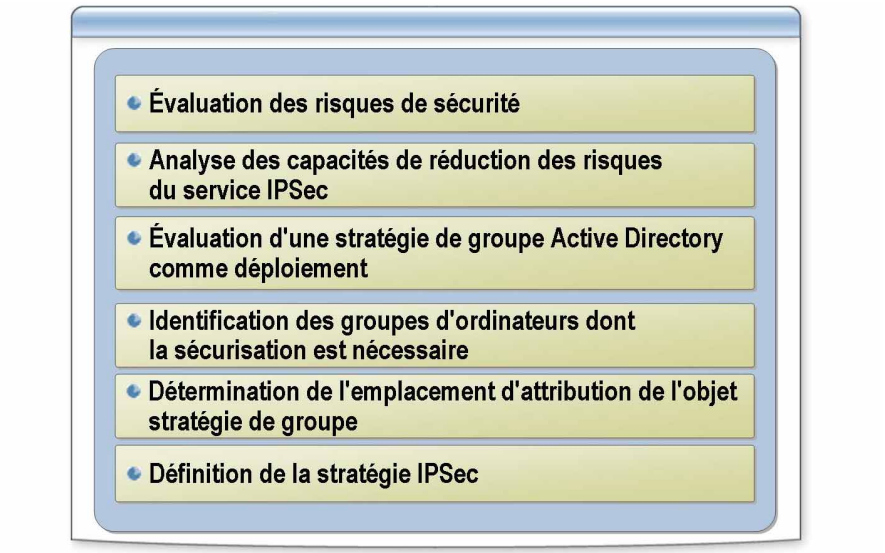
- Déterminez l'emplacement des informations stockées, leurs modes de routage sur le réseau et les ordinateurs pouvant accéder au réseau.

  Cet examen préalable fournit des informations concernant la vitesse, la capacité et l'utilisation du réseau avant d'y implémenter le service IPSec, et favorise ainsi l'optimisation des performances.

- Évaluez la vulnérabilité du réseau face aux attaques.

- Concevez et documentez un plan de sécurité pour tout le réseau en tenant compte des éléments suivants :
  - le cadre de sécurité général de Windows 2000, y compris le modèle Active Directory et la manière dont la sécurité est appliquée aux GPO ;
  - vos scénarios de communication probables : intranet, accès distant, extranets pour partenaires commerciaux, communication intersites (de routeur à routeur) ;
  - le niveau de sécurité nécessaire à chaque scénario (ex. confidentialité des communications Internet uniquement).
- Rédigez, créez et testez les stratégies IPSec pour chaque scénario. Ceci permet une clarification et une meilleure évaluation des stratégies nécessaires et de leurs structures.

Instructions relatives au déploiement du service IPSec par le biais d'Active Directory



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les instructions suivantes sont destinées à vous assister dans le déploiement de stratégies IPSec par le biais d'Active Directory.

Évaluation des risques de sécurité

Un examen des données et des réseaux est nécessaire afin de déterminer leur éventuelle vulnérabilité face à des attaques passives et actives.

Analyse des capacités de réduction des risques du service IPSec

Déterminez si les fonctions et les paramètres de service IPSec peuvent limiter les menaces d'attaques identifiées sur le réseau ?

Évaluation d'une stratégie de groupe Active Directory comme déploiement

Un déploiement par le biais d'Active Directory facilite la propagation automatique de la stratégie IPSec vers un grand nombre d'ordinateurs. À vous de déterminer s'il s'agit de la méthode idéale en fonction des besoins de votre entreprise.

Identification des groupes d'ordinateurs dont la sécurisation est nécessaire

Sur la base des risques potentiels identifiés, il convient de déterminer les ordinateurs pouvant être regroupés comme cible commune d'une stratégie IPSec limitant les risques.

Détermination de l'emplacement d'attribution de l'objet stratégie de groupe

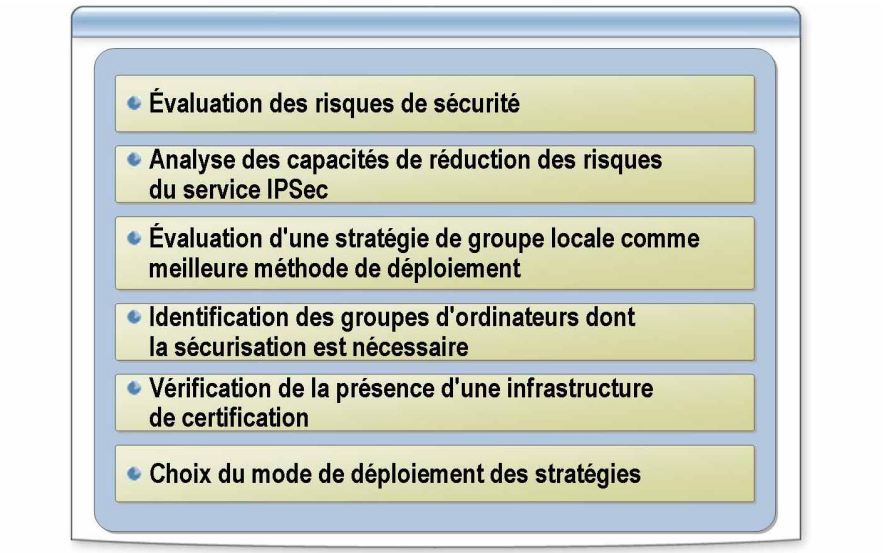
La stratégie s'applique-t-elle à un nombre élevé ou réduit d'ordinateurs ? Si les ordinateurs nécessitant une stratégie IPSec commune sont nombreux, il est intéressant d'attribuer la stratégie IPSec au GPO d'un site ou d'un domaine. Si la stratégie IPSec commune s'applique à un groupe plus restreint, il vaudra mieux attribuer une stratégie IPSec au GPO d'une unité d'organisation existante ou à un nouveau GPO.

Définition de la stratégie IPSec

Les éléments suivants doivent être définis pour toute stratégie nouvelle ou personnalisée :

- filtres IP ;
- action de filtrage et méthodes de sécurité associées ;
- méthodes d'authentification ;
- points de sortie du tunnel ;
- type de connexion.

Instructions relatives au déploiement du service IPSec par le biais de stratégies locales



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Si Active Directory n'est pas disponible, le déploiement du service IPSec doit se faire par le biais de stratégies de groupe locales.

Évaluation des risques de sécurité

Un examen des données et des réseaux est nécessaire afin de déterminer leur éventuelle vulnérabilité face à des attaques passives et actives.

Analyse des capacités de réduction des risques du service IPSec

Les fonctions et les paramètres du service IPSec limitent-ils les risques d'attaques identifiés ?

Évaluation d'une stratégie de groupe locale comme meilleure méthode de déploiement

La stratégie de groupe locale ne concerne que l'ordinateur local. Il s'agit de la seule méthode de déploiement disponible en l'absence d'Active Directory. À vous de déterminer si cette méthode répond suffisamment aux besoins de votre entreprise.

Identification des groupes d'ordinateurs dont la sécurisation est nécessaire

Une stratégie locale ne s'applique qu'à des ordinateurs isolés. Il faut donc identifier ceux-ci et vérifier qu'ils peuvent utiliser les mêmes stratégies IPSec actives.

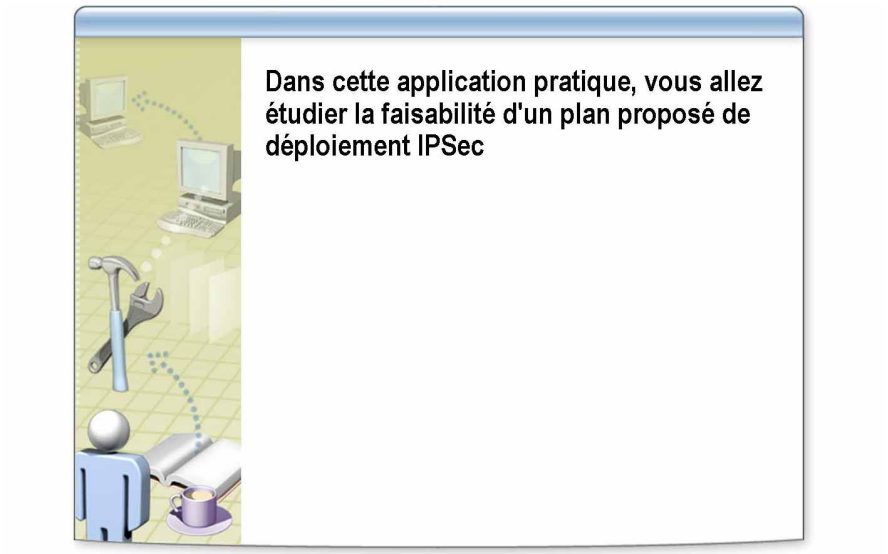
Vérification de la présence d'une infrastructure de certification

Si vous utilisez des stratégies locales et que vous ne prenez pas Kerberos comme méthode d'authentification (ou si Active Directory n'a pas été implémenté), vous devez vérifier la présence d'une infrastructure de certification pour la remplacer comme méthode d'authentification. En optant pour une autorité de certification Microsoft, vous pourrez utiliser l'inscription automatique pour stocker automatiquement les certificats d'ordinateurs comme propriété d'un compte d'ordinateur Active Directory. L'administration manuelle des certificats pour les ordinateurs qui les nécessitent reste également une possibilité.

Choix du mode de déploiement des stratégies

Si vous utilisez une stratégie de groupe locale dans votre déploiement IPSec, vous devez déterminer la meilleure manière de déployer la configuration de cette stratégie à tous les ordinateurs auxquels elle s'applique. Puisque vous n'utilisez pas la stratégie de groupe de domaine, Active Directory ne fait pas partie des méthodes de distribution possibles.

Application pratique : Planification d'un déploiement IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Dans cette application pratique, vous allez étudier la faisabilité d'un plan proposé de déploiement IPSec.

Objectif

L'objectif de cette application pratique est la planification d'un déploiement IPSec sur la base du scénario fourni.

Instructions

1. Lisez le scénario.
2. Préparez une discussion sur les défis posés par cette tâche qui suivra l'application pratique.

Scénario

La banque Woodgrove a équipé son siège social d'une infrastructure Active Directory d'environ 500 ordinateurs tournant sur Windows XP Professionnel, Windows 2000 ou Windows Server 2003. Le service des prêts hypothécaires de la banque dispose d'ordinateurs supplémentaires tournant également sur Windows 2000 Professionnel mais ne faisant pas partie du domaine.

Un programme pilote visant à sécuriser le trafic entre la succursale Prêts hypothécaires et le service des prêts hypothécaires au siège central est en cours de préparation. La succursale dispose d'un contrôleur de domaine pour un domaine enfant sur un site Active Directory séparé.

Le plan prévoit, d'une part, l'installation d'un serveur membre Windows 2000 au siège central et d'un serveur membre Windows Server 2003 dans la succursale et, d'autre part, la sécurisation des échanges d'informations relatives aux demandes de crédit par le biais de stratégies IPSec. Le plan de la stratégie IPSec prévoit l'utilisation de Kerberos comme méthode d'authentification et stipule en outre que la succursale utilisera une stratégie de groupe locale, tandis que le serveur du siège social utilisera une stratégie de groupe Active Directory. La stratégie doit permettre de sécuriser la totalité du trafic entre ces deux ordinateurs.

Application pratique

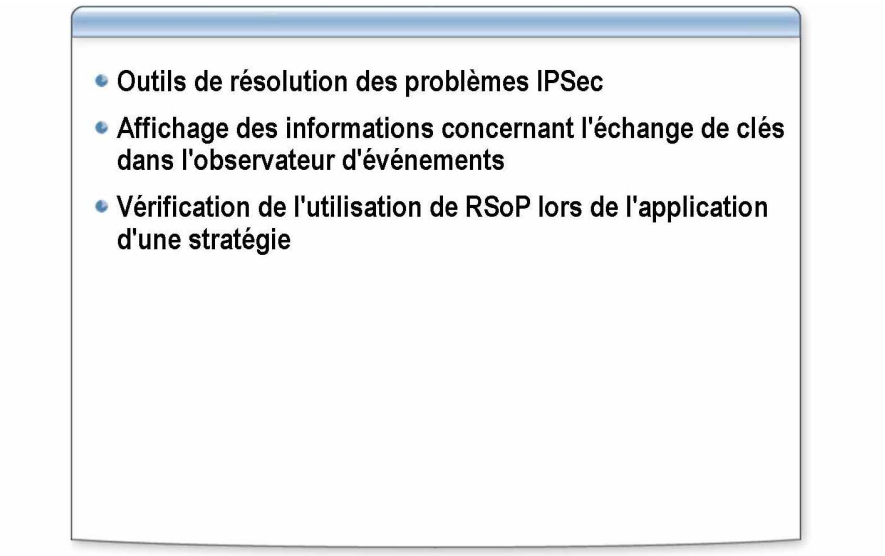
Ce plan est-il faisable ? Quelle que soit la réponse, justifiez-la.

Oui, il est faisable.

L'authentification Kerberos peut être utilisée parce que tous les ordinateurs utilisant le service IPSec pour communiquer sont des membres approuvés d'un domaine Active Directory. Toutefois, si la banque veut prévoir la communication entre les deux stations de travail Windows 2000 et les deux serveurs, il faudra les intégrer au domaine, ou sélectionner une autre méthode d'authentification (ex. certificats de clés publiques).

L'utilisation de deux méthodes de déploiement (stratégies locales) est également envisageable. La succursale peut déployer IPSec en utilisant une stratégie de groupe locale, tandis que le siège social utilise Active Directory. Attention, la configuration d'une stratégie IPSec Active Directory au niveau de la succursale remplacera toute stratégie locale existante. Sa planification doit être rigoureuse pour éviter tout risque de conséquences imprévues.

Leçon : Résolution des problèmes de communications IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Cette leçon couvre les connaissances requises pour résoudre les problèmes de communications IPSec. Ce module aborde et illustre également les outils utilisés pour la résolution de ces problèmes.

Objectifs

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- résoudre les problèmes touchant les communications IPSec ;
- vérifier la configuration IPSec d'un ordinateur au moyen de l'outil Configuration et analyse de la sécurité ;
- vérifier la configuration IPSec d'un ordinateur au moyen de l'Éditeur d'objets de stratégie de groupe ;
- vérifier la configuration IPSec d'un ordinateur au moyen du Jeu de stratégie résultant (RsoP, *Resultant Set of Policy*) ;
- corriger la configuration IPSec d'un ordinateur au moyen du composant logiciel enfichable Gestion des stratégies de groupe ;
- résoudre les problèmes de configuration IPSec d'un ordinateur au moyen du Moniteur de sécurité IP.

Outils de résolution des problèmes IPSec

Outil	Utilisations
Composant logiciel enfichable Moniteur de sécurité IP	• Recherche de tous les trafics correspondant à un filtre d'un type de trafic donné
Composant logiciel enfichable Gestion de stratégie de sécurité IP	• Création, modification et activation des stratégies IPSec
Utilisateurs et ordinateurs Active Directory et stratégie de groupe	• Résolution des problèmes de priorité des stratégies • Détermination des stratégies disponibles, attribuées ou appliquées
Jeu de stratégie résultant (RSoP)	• Détermination des stratégies attribuées mais non appliquées aux clients
Observateur d'événements	• Affichage des événements liés aux stratégies IPSec
Journal Oakley	• Affichage des détails du processus d'établissement des SA

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Cette section décrit les différents outils disponibles pour résoudre les problèmes liés au déploiement d'une infrastructure IPSec dans une entreprise.

Composant logiciel enfichable Moniteur de sécurité IP

Le Moniteur de sécurité IP est un outil utilisé pour la résolution de problèmes IPSec complexes. Il offre la possibilité de visualiser les détails d'une stratégie IPSec active appliquée localement ou à l'échelle d'un domaine et fournit plusieurs statistiques associées à la procédure d'échange de clés. Le Moniteur de sécurité IP permet de rechercher toutes les occurrences de filtrage pour un type de trafic particulier.

Pour ce qui est de la surveillance à distance, le moniteur vous offre également la possibilité de surveiller uniquement les ordinateurs qui fonctionnent sur la même version du système d'exploitation Windows. Pour surveiller le service IPSec à distance sur un ordinateur qui exécute une autre version de Windows, c'est la Connexion Bureau à distance qu'il faut utiliser.

Si votre ordinateur et les ordinateurs surveillés sont équipés de la famille Windows Server 2003, vous pouvez exécuter le moniteur de sécurité IP ou utiliser l'outil de ligne de commande Netsh à distance.

La console de gestion ne permet toutefois pas d'attribuer des stratégies IPSec Active Directory. Celles-ci ne peuvent être attribuées de manière effective qu'au moyen de l'Éditeur d'objet de stratégie de groupe. Notez que la console Gestion de la stratégie de sécurité IP permet d'attribuer des stratégies IPSec associées à une stratégie de groupe.

Le composant logiciel enfichable Moniteur de sécurité IP permet également de visualiser les détails des éléments suivants :

- filtres génériques de mode principal et de mode rapide, et associations de sécurité ;
- stratégies IKE ;

- stratégies de négociation ;
- statistiques de sécurité de mode principal et de mode rapide ;
- stratégie IPSec active.

Composant logiciel enfichable Gestion de la stratégie de sécurité IP

Le composant logiciel enfichable Gestion de la stratégie de sécurité IP permet de créer, de supprimer et de modifier une stratégie IPSec. Il permet de créer une console pour l'ordinateur local, le domaine Active Directory, un Active Directory différent ou un autre ordinateur.

Utilisateurs et ordinateurs Active Directory et stratégie de groupe

Le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory aide à résoudre des problèmes de priorité des stratégies et à déterminer les stratégies IPSec disponibles, attribuées ou appliquées à des clients IPSec.

Jeu de stratégie résultant (RsoP)

Le Jeu de stratégie résultant (RsoP) sert à déterminer les stratégies IPSec attribuées mais non appliquées à des clients IPSec. Le composant logiciel enfichable RSoP affiche des informations détaillées sur les paramètres de la stratégie IPSec. Il permet de visualiser les règles et les actions de filtrage, les méthodes d'authentification, les points de sortie du tunnel et le type de connexion de la stratégie appliquée.

Observateur d'événements

L'observateur d'événements permet de visualiser les éléments suivants :

- événements de l'agent de stratégie IPSec dans le journal d'audit ;
- événements du pilote IPSec dans le journal système ;
- événements IKE dans le journal d'audit ;
- événements de modification de stratégie IPSec dans le journal d'audit.

Remarque Lorsque la journalisation de l'observateur d'événements est activée, celui-ci se remplit rapidement d'événements. Si le nombre d'événements contrôlés est élevé, veillez à augmenter la taille des journaux d'événements en conséquence.

Journal Oakley

Le journal Oakley affiche des informations détaillées concernant la procédure d'établissement des SA. Le journal Oakley est activé dans le registre. Il n'est pas activé par défaut.

Le journal Oakley enregistre toutes les négociations ISAKMP en mode principal et en mode rapide. Un nouveau fichier Oakley.log est créé à chaque démarrage de l'agent de stratégie IPSec et la version précédente est enregistrée sous le nom Oakley.log.sav.

Console Gestion des stratégies de groupe

La console Gestion des stratégies de groupe est un ensemble d'interfaces programmables qui permet d'administrer une stratégie de groupe, ainsi qu'un composant logiciel enfichable MMC (Microsoft Management Console) conçu sur la base de ces interfaces. Tous les composants de la console Gestion des stratégies de groupe permettent de gérer la stratégie de groupe dans l'ensemble de l'entreprise depuis un emplacement central.

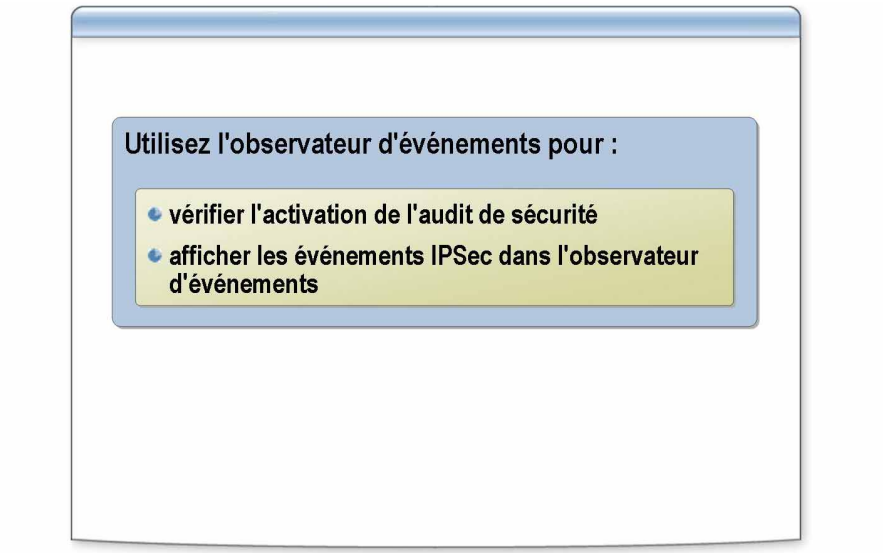
La console Gestion des stratégies de groupe combine la fonctionnalité de tous ces composants dans une interface utilisateur unique. Cette interface est organisée selon la manière dont vous utilisez et administrez la stratégie de groupe. Elle intègre, dans un composant logiciel enfichable MMC unique, la fonctionnalité de stratégie de groupe des outils suivants :

- Utilisateurs et ordinateurs Active Directory
- Sites et services Active Directory
- RSoP

La fonction Gestion de stratégie de groupe intègre également des fonctionnalités qui n'étaient pas disponibles dans les outils de stratégie de groupe précédents. La fonction Gestion de stratégie de groupe permet d'effectuer notamment les tâches suivantes :

- sauvegarder et restaurer des objets de stratégie de groupe ;
- copier et importer des GPO et des filtres d'instrumentation de gestion Windows (WMI, *Windows Management Instrumentation*) ;
- générer des rapports sur les objets de stratégie de groupe et le jeu de stratégie résultant ;
- rechercher des objets de stratégie de groupe.

Affichage des informations concernant l'échange de clés dans l'observateur d'événements



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

En cas de suspicion d'erreurs dans la procédure d'échange de clés, l'observateur est le meilleur outil pour visualiser les actions effectuées. En effet, ces événements peuvent confirmer le bon déroulement de l'échange de clés.

Vérification de l'activation de l'audit de sécurité

L'audit des négociations IKE est pris en charge dans Windows 2000, Windows XP et la famille Windows Server 2003. IKE utilise la catégorie Événements de connexion. La famille Windows Server 2003 prend aussi en charge l'audit de la base de données de stratégie de sécurité (SPD, *Security Policy Database*), qui utilise la catégorie Modification de stratégie.

Affichage des événements IPSec dans l'observateur d'événements

L'observateur d'événements permet d'afficher les événements IKE (négociation, réussite et échec) dans le journal de sécurité.

Pour que ces événements soient visibles, l'audit de réussite ou d'échec doit être activé pour la stratégie d'audit **Auditer les événements de connexion aux comptes** d'application dans votre domaine ou sur votre ordinateur local. La catégorie Événements IKE peut également servir à l'audit des événements de connexion à d'autres services que IPSec.

Lorsque l'audit de réussite ou d'échec est activé pour la stratégie d'audit **Auditer les événements de connexion aux comptes**, IPSec enregistre, comme événements séparés, la réussite ou l'échec de toutes les négociations IKE d'une part, et l'établissement et la fin de chaque négociation d'autre part. Cependant, l'activation de ce type d'audit peut entraîner la multiplication des événements IKE dans le journal de sécurité.

Exemple

Dans le cas de serveurs connectés à Internet, les attaques visant le protocole IKE peuvent entraîner l'apparition massive d'événements IKE dans le journal de sécurité. La même chose peut également se produire dans le cas de serveurs utilisant le service IPSec pour sécuriser le trafic vers un nombre élevé de clients. Pour éviter ceci, il suffit de désactiver l'audit des événements IKE dans le journal de sécurité en modifiant le registre.

Désactivation de l'audit des événements IKE

Voici la procédure permettant de désactiver l'audit des événements IKE dans le journal de sécurité :

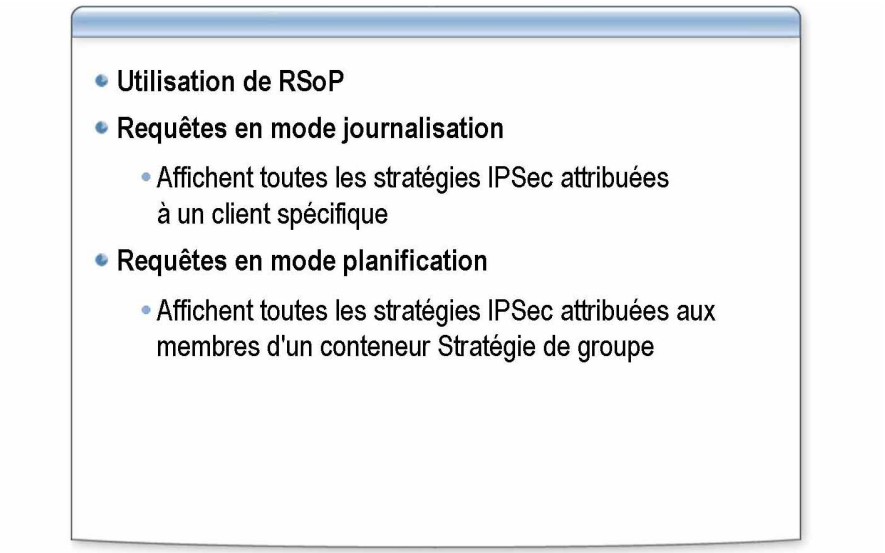
1. Attribuez la valeur 1 au paramètre de registre **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit\DisableIKEAudits**. Par défaut, la clé DisableIKEAudits n'existe pas ; il faut donc la créer.

Attention Toute erreur lors d'une modification du registre peut sérieusement affecter votre système. La sauvegarde des données importantes est donc recommandée avant de procéder à toute modification du registre.

2. Redémarrez l'ordinateur ou quittez puis rouvrez le service IPSec. Utilisez pour ce faire les commandes **net stop policyagent** et **net start policyagent** à l'invite de commandes.

L'arrêt et le redémarrage du service IPSec sur un ordinateur déconnectent tous les ordinateurs utilisant IPSec qui y sont reliés. La communication avec cet ordinateur est également suspendue. Si le redémarrage du service intervient dans l'immédiat, la communication TCP est rétablie en raison du comportement de retransmission adopté par le protocole TCP suite à l'établissement des nouvelles SA IKE et IPSec.

Vérification de l'utilisation de RSoP lors de l'application d'une stratégie



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Le jeu de stratégie résultant est un complément de la stratégie de groupe permettant de visualiser les attributions de stratégies IPSec pour un ordinateur ou pour les membres d'un conteneur Stratégie de groupe. Ces informations favorisent la résolution des problèmes de priorité des stratégies et facilitent la planification d'un déploiement IPSec.

Utilisation de RSoP

Pour visualiser les attributions de stratégies IPSec dans RSoP, vous devez d'abord ouvrir la console Jeu de stratégie résultant, puis exécuter une requête. RSoP fournit deux types de requêtes : les requêtes en mode journalisation (pour visualiser les stratégies IPSec attribuées à un ordinateur) et les requêtes en mode planification (pour visualiser les stratégies IPSec attribuées aux membres d'un conteneur Stratégie de groupe).

Requêtes en mode journalisation

Une requête RSoP en mode journalisation permet d'afficher la liste complète des stratégies IPSec attribuées à un client IPSec. Les résultats de la requête indiquent la priorité de chaque attribution de stratégie IPSec et mettent en évidence les stratégies attribuées mais non appliquées d'une part, et la stratégie en cours d'application d'autre part. La console RSoP affiche également les paramètres détaillés (règles et actions de filtrage, méthodes d'authentification, points de sortie du tunnel et type de connexion) correspondant à la stratégie appliquée.

Lors d'une requête en mode journalisation, RSoP récupère les informations concernant la stratégie à partir du répertoire de stockage WMI sur l'ordinateur cible et les affiche dans la console. Ce faisant, RSoP fournit une vue d'ensemble des paramètres de la stratégie en cours d'application sur un ordinateur à un moment donné.

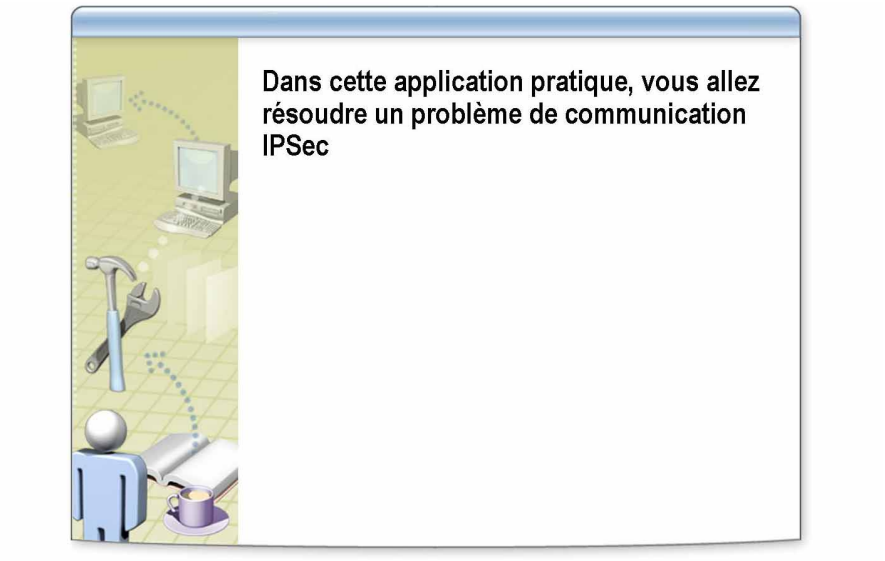
Requêtes en mode planification

Une requête RSoP en mode planification permet d'afficher la liste complète des stratégies IPSec attribuées aux membres d'un conteneur Stratégie de groupe. Ce type de requête peut s'avérer utile dans le cas d'une réorganisation de société impliquant le déménagement d'ordinateurs d'une unité d'organisation existante vers une nouvelle unité. Dans ce cas de figure, une requête en mode planification basée sur les informations adéquates permettrait de déterminer les stratégies IPSec attribuées mais non appliquées à la nouvelle unité d'organisation, ainsi que la stratégie IPSec en cours d'application. Ceci permettrait d'identifier la stratégie qui serait appliquée en cas de déménagement des ordinateurs dans la nouvelle unité d'organisation. À l'instar des requêtes en mode journalisation, les requêtes en mode planification affichent les paramètres détaillés de la stratégie IPSec en cours d'application dans la console RSoP.

Lors de l'exécution d'une requête en mode planification, RSoP récupère les noms de l'utilisateur, de l'ordinateur et du contrôleur de domaine cibles à partir du répertoire de stockage WMI situé sur le contrôleur de domaine. WMI utilise ensuite le service d'accès de données de la stratégie de groupe (GPDAS, *Group Policy Data Access Service*) pour créer les paramètres de stratégie qui seraient appliqués à l'ordinateur cible sur la base des paramètres de requête RSoP fournis. RSoP lit les paramètres de la stratégie dans le répertoire de stockage WMI situé sur le contrôleur de domaine et affiche ceux-ci dans l'interface utilisateur de la console RSoP.

Remarque Les requêtes RSoP en mode planification portent exclusivement sur les contrôleurs de domaines. Aussi, le nom du contrôleur de domaine doit être spécifié de manière explicite lors de l'exécution de la requête. Cela dit, n'importe quel client IPSec peut être désigné comme cible de la requête pour autant que les autorisations requises soient réunies.

Application pratique : Résolution des problèmes de communications IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Dans cette application pratique, vous allez résoudre les problèmes de communication IPSec en vous aidant des outils présentés dans la leçon.

Objectif

L'objectif de cette application pratique est la résolution des problèmes de communications IPSec.

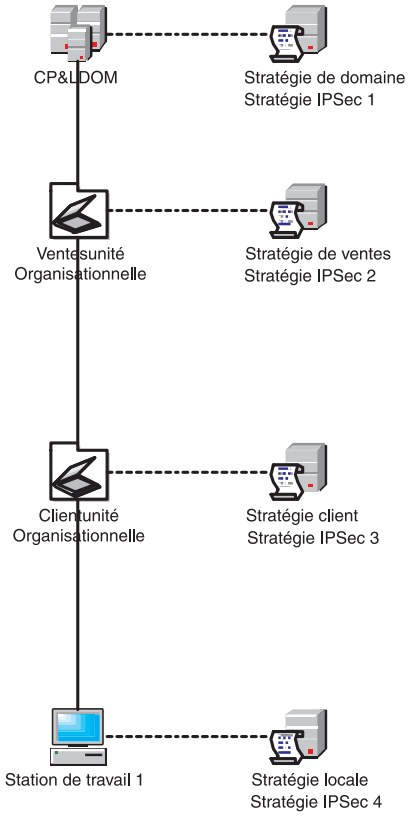
Instructions

1. Lisez le scénario.
2. Préparez une discussion sur les défis posés par cette tâche qui suivra l'application pratique.

Scénario

Plusieurs administrateurs de la société City Power & Light rencontrent des problèmes au niveau des stratégies IPSec qu'ils ont eux-mêmes configurées. Apparemment, personne ne sait quelles sont les stratégies IPSec en vigueur, ni quand elles sont appliquées.

Vous avez trouvé un vieux document de planification qui illustre les attributions de stratégies IPSec suivantes.



Application pratique

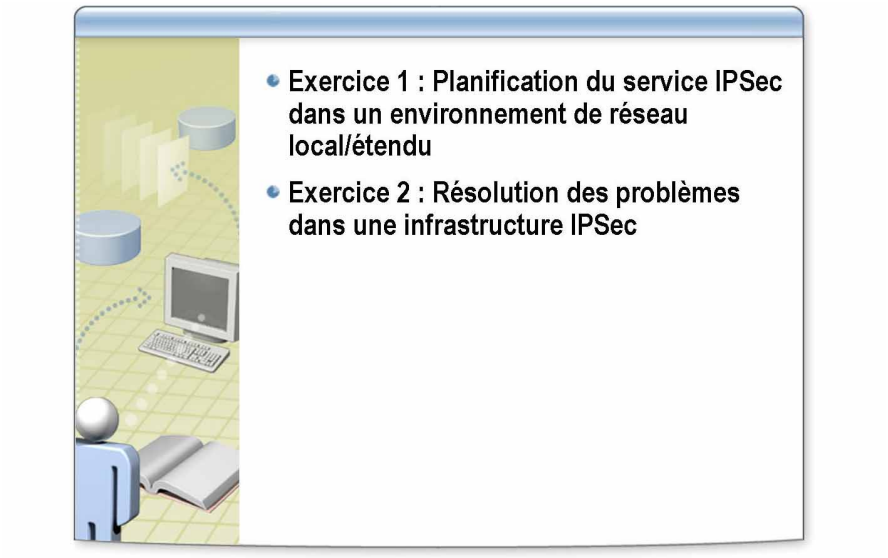
Si le document de planification est correct, quelle est la stratégie IPSec appliquée à la station de travail 1 ?

La stratégie IPSec n 3.

Quel est le meilleur outil pour vérifier votre réponse ?

Jeu de stratégie résultant en mode journalisation.

Atelier A : Résolution des problèmes IPSec



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Objectifs

À la fin de cet atelier, vous serez à même d'effectuer les tâches suivantes :

- planifier une infrastructure IPSec pour un environnement de réseau local/étendu ;
- résoudre les problèmes d'une infrastructure IPSec.

Scénario

Vous êtes ingénieur système chez Northwind Traders et vous avez reçu pour mission de planifier une nouvelle infrastructure IPSec destinée au département des ressources humaines de la société, situé au Royaume-Uni. Malgré son statut de site principal dans l'organisation de la société, le site de Londres n'abrite pas la totalité du département des ressources humaines, chaque site mondial disposant également de son propre personnel.

Un problème de sécurité récent a mis en évidence la nécessité de sécuriser les données RH au niveau des réseaux locaux de chaque site. Le département informatique souhaite doter le département des ressources humaines d'une nouvelle infrastructure sécurisée et vous en confie la planification. Les modifications que vous préconiserez seront étudiées par le département informatique et implémentées sur tous les sites une fois approuvées.

La répartition du personnel et des ressources du département RH sur les différents sites de Northwind Traders est la suivante :

- Londres : onze clients bureau, cinq clients sans fil, deux serveurs de fichiers et deux serveurs d'impression.
- Paris : trois clients bureau, un serveur de fichiers et d'impression.
- Sydney : deux clients bureau, un serveur de fichiers et d'impression.
- New York : cinq clients bureau, deux serveurs de fichiers et d'impression.

Durée approximative de cet atelier : 30 minutes

Exercice 1
Planification du service IPSec dans un environnement de réseau local/étendu

Dans cet exercice, vous allez élaborer le plan d'une nouvelle infrastructure IPSec répondant aux besoins en matière de sécurité formulés par le personnel du département des ressources humaines.

Décrivez les modifications ou dessinez l'infrastructure IPSec telle que vous l'implémenteriez chez Northwind Traders.

Scénario

La nouvelle configuration basée sur le service IPSec est destinée au personnel du département des ressources humaines du siège social et des différentes implantations d'outre-mer. Northwind Traders utilise Active Directory, et tous les employés (sauf un) du département des ressources humaines disposent d'un compte dans le domaine du siège social ou dans un domaine approuvé. La société Northwind Traders emploie également un consultant externe avec lequel elle communique principalement via messagerie cryptée. Au besoin, le consultant peut se connecter au réseau Northwind Traders au moyen d'un compte lui permettant de créer une connexion de réseau privé virtuel (VPN, *Virtual Private Network*). Ce compte invité est également utilisé par d'autres sous-traitants externes, ce qui explique les restrictions importantes au niveau de l'accès aux ressources.

Le groupe de planification informatique de Northwind Traders a rédigé un cahier des charges qui doit être respecté dans la planification de l'infrastructure IPSec du Royaume-Uni. En voici les points principaux :

- Northwind Traders ne souhaite pas pour l'instant implémenter une infrastructure de certification PKI (Public Key Infrastructure).
- Le niveau de sécurité le plus élevé possible (à la fois en termes d'intégrité et de cryptage) doit être utilisé pour tous les transferts de données RH entre les clients RH et les serveurs ou les imprimantes RH. Les ordinateurs associés au département des ressources humaines sont tous équipés d'un adaptateur réseau capable de déléguer la négociation de sécurité et le stockage des SA. Les pilotes de ces adaptateurs sont déjà installés.
- Le personnel doit continuer à pouvoir accéder à toutes les ressources non sécurisées sur Internet.
- Northwind Traders ne souhaite pas modifier son réseau pour isoler le département des ressources humaines. L'implémentation de réseaux locaux virtuels (VLAN, *Virtual Local Area Network*) ou sous-réseaux séparés n'est donc pas souhaitable.

Le groupe de planification informatique de Northwind Traders insiste également sur les éléments suivants :

- Le département des ressources humaines aimerait permettre à son consultant externe d'accéder aux ressources internes stockées sur un des serveurs du siège social. Cependant, le département ne souhaite pas lui créer de compte Active Directory propre.
- Le département informatique précise que, si possible, l'infrastructure doit empêcher le personnel du département d'utiliser des connexions homologue à homologue, sauf si celles-ci peuvent être sécurisées au moyen du service IPSec.

Vous avez examiné les niveaux actuels de trafic de données RH et pris note des faits suivants :

- Les clients impriment d'importants volumes de documents sécurisés. La taille moyenne d'une tâche d'impression est de 18 Mo (mégaoctets) et chaque utilisateur imprime en moyenne 100 à 170 Mo par jour.
- Les clients ouvrent beaucoup de pages Web et de documents sécurisés sur un serveur Microsoft SharePoint™ Portal Server. Le débit de données des clients vers ce serveur s'élève à 32 Mo par heure (de pointe) par utilisateur.

Tâches	Instructions spécifiques
1. Documenter les changements préconisés au niveau des ressources, des comptes d'ordinateurs et des comptes d'utilisateurs du département des ressources humaines pour réaliser l'activation du service IPSec pour tous les transferts de données RH.	
2. Documenter le nombre de stratégies IPSec requises.	Précisez, pour chaque type de stratégie requis, les informations suivantes : liste de filtres IP, méthode d'authentification, méthodes d'échange de clés et action de filtrage.
3. Documenter la méthodologie de déploiement de stratégie choisie.	Précisez les détails du déploiement des stratégies IPSec sur les ordinateurs concernés.

Exercice 2
Résolution des problèmes dans une infrastructure IPSec

Dans cet exercice, vous allez résoudre les problèmes touchant une infrastructure IPSec pour garantir à tous les clients une fonctionnalité et des niveaux de sécurité corrects.

Scénario

Vous êtes l'administrateur d'un réseau local. Un expert en sécurité vous informe que les communications entre un serveur sécurisé et les clients du réseau local se déroulent sans aucun cryptage. De plus, l'expert vous signale qu'il ne parvient pas à exécuter une commande PING pour le serveur sécurisé alors que cette méthode devrait vraisemblablement fonctionner.

Vous examinez la stratégie configurée sur le serveur sécurisé :

Stratégie du serveur de ressources :

Règle 1

Liste de filtres IP : Trafic vers serveurs DNS et WINS

Action de filtrage : Permit

Méthodes d'authentification : Aucun

Type de connexion : Réseau local

Règle 2

Liste de filtres IP : ICMP

Action de filtrage : Permit

Méthodes d'authentification : Aucun

Type de connexion : Réseau local

Règle 3

Liste de filtres IP : Tout trafic IP

Action de filtrage : Sécurité requise

Méthodes d'authentification : Kerberos

Type de connexion : Réseau local

Vous décidez d'exporter la stratégie utilisée sur le client et de l'importer dans votre ordinateur pour résoudre le problème. Le problème persiste sur votre ordinateur.

Remarque Les étapes 1 à 5 consistent à vérifier la connectivité de l'ordinateur Glasgow pour pouvoir examiner les paquets. Les étapes 6 à 12 concernent l'identification du problème au niveau de la stratégie IPSec.

Tâches	Instructions spécifiques
1. Ouvrir une session sur votre ordinateur au moyen du compte d'administrateur local.	▪ Nom d'utilisateur : Administrateur ▪ Mot de passe : *Mot de passe de l'administrateur de l'ordinateur*
2. Lancer le Moniteur réseau, sélectionner Réseau de la classe et démarrer la capture.	Sélectionnez **Réseau de la classe** pour lancer la capture des données.
3. Ouvrir une fenêtre de commande et exécuter une commande PING pour l'ordinateur Glasgow.	
4. Taper le nom du fichier texte du stagiaire sur \\Glasgow\Ipsec_test \ipsec.txt.	À l'invite de commandes, tapez **\\Glasgow\Ipsec_test\ipsec.txt**
5. Arrêter la capture et examiner les données.	
Identifiez les paquets ICMP et le texte du fichier. _____	
6. Créer une console MMC avec le composant logiciel enfichable Gestion de la stratégie de sécurité IP configuré pour l'ordinateur local.	
7. Importer le fichier Student_Client_Policy_Start.ipsec au moyen de la console MMC.	Emplacement du fichier : C:\MOC\2189\Labfiles\
8. Attribuer la stratégie Client_Policy.	
9. Démarrer la capture dans le Moniteur réseau.	N'enregistrez pas la capture précédente lorsque le système vous le propose.
10. Exécuter une commande PING pour l'ordinateur Glasgow.	
11. Taper le nom du fichier texte du stagiaire sur \\Glasgow\Ipsec_test \ipsec.txt.	À l'invite de commandes, tapez **\\Glasgow\Ipsec_test\ipsec.txt**
12. Arrêter la capture pour examiner les données.	Utilisez les informations capturées pour répondre aux questions suivantes.
Examinez les données collectées pendant l'application de la stratégie IPSec et expliquez pourquoi les données ne sont pas cryptées. _____	
Examinez les données collectées pendant l'application de la stratégie IPSec et expliquez pourquoi les paquets ICMP ne sont pas transmis. _____	