

Module 9 : Planification de l'accès réseau

Table des matières

Vue d'ensemble	1
Leçon : Présentation de l'accès réseau	2
Leçon : Sélection des méthodes de connexion d'accès réseau	14
Considérations relatives à une solution de connexion à distance	19
Présentation multimédia : Planification des clients VPN et de connexion d'accès à distance	21
Leçon : Sélection d'un plan de stratégie d'accès distant	28
Leçon : Sélection d'une méthode d'authentification de l'accès réseau	41
Leçon : Planification d'une stratégie d'accès réseau	49
Atelier A : Planification de l'accès réseau	55



Les informations contenues dans ce document, notamment les adresses URL et les références à des sites Web Internet, pourront faire l'objet de modifications sans préavis. Sauf mention contraire, les sociétés, les produits, les noms de domaine, les adresses de messagerie, les logos, les personnes, les lieux et les événements utilisés dans les exemples sont fictifs et toute ressemblance avec des sociétés, produits, noms de domaine, adresses de messagerie, logos, personnes, lieux et événements existants ou ayant existé serait purement fortuite. L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicables dans son pays. Sans limitation des droits d'auteur, aucune partie de ce manuel ne peut être reproduite, stockée ou introduite dans un système d'extraction, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), sans la permission expresse et écrite de Microsoft Corporation.

Les produits mentionnés dans ce document peuvent faire l'objet de brevets, de dépôts de brevets en cours, de marques, de droits d'auteur ou d'autres droits de propriété intellectuelle et industrielle de Microsoft. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

© 2003 Microsoft Corporation. Tous droits réservés.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, IntelliMirror, MSDN, PowerPoint, Visual Basic et Windows Media sont soit des marques de Microsoft Corporation, soit des marques déposées de Microsoft Corporation, aux États-Unis d'Amérique et/ou dans d'autres pays.

Les autres noms de produits et de sociétés mentionnés dans ce document sont des marques de leurs propriétaires respectifs.

Notes du formateur

Présentation :
60 minutes

Ce module présente aux stagiaires la planification, les outils et la documentation correspondant à l'infrastructure réseau Microsoft® Windows Server™ 2003.

Atelier :
30 minutes

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

- expliquer les spécifications et les protocoles d'authentification d'une stratégie d'accès réseau ;
- appliquer les instructions de sélection d'une stratégie de connexion d'accès réseau ;
- appliquer les instructions de sélection d'un plan d'accès distant ;
- sélectionner une méthode d'authentification de l'accès réseau ;
- planifier une stratégie d'accès réseau.

Matériel requis

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

- Fichier Microsoft PowerPoint® 2189A_09.ppt
- Fichier multimédia Planification des clients VPN (Virtual Private Network) et de connexion d'accès à distance

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 et vous reporter à la clé de réponse de l'atelier ;
- visualiser les présentations multimédias ;
- passer en revue les cours et modules de connaissances préalables.

Comment animer ce module

Cette section contient des informations qui ont pour but de vous aider à animer ce module.

Informations générales

Ce module explique le concept d'accès réseau et son rapport à la planification d'une infrastructure réseau Windows Server 2003. Dans ce module, le concept d'accès distant n'est pas abordé d'un point de vue général, mais combine les connexions LAN (Local Area Network), VPN et d'accès réseau à distance, appelées « accès réseau ». Il explique comment planifier une stratégie complète d'accès réseau.

Pages d'instructions, applications pratiques et ateliers

Pages d'instructions

Les pages d'instructions contiennent des points de décision essentiels associés à la rubrique de la leçon. Vous allez utiliser ces instructions pour renforcer les acquis de la leçon et les objectifs.

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 : Présentation de l'accès réseau

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

Spécifications de l'accès réseau

Expliquez le concept d'accès réseau et vérifiez que les stagiaires en comprennent les caractéristiques. Effectuez une présentation générale des spécifications de l'accès réseau. En cas de questions de la part des stagiaires sur ces spécifications, indiquez-leur qu'elles seront abordées en détail dans la leçon.

Connexions d'accès réseau

Identifiez et décrivez chaque type de connexion réseau. Étant donné que de nombreux stagiaires peuvent déjà connaître les types de connexions, passez cette section en revue.

Protocoles d'authentification de l'accès réseau	Identifiez chacun des protocoles et demandez aux stagiaires de les définir avant de les passer en revue. La définition des protocoles vous permet d'évaluer les connaissances des stagiaires sur les protocoles d'authentification.
Recommandations relatives à la sécurisation des connexions	Expliquez que la sécurité des connexions est un élément essentiel d'une stratégie d'accès réseau. L'identification des différents composants peut sembler confuse aux stagiaires, mais ils pourront en avoir une image globale et complète à mesure qu'ils acquerront des connaissances dans le cadre de cette rubrique.

Leçon : Sélection des méthodes de connexion d'accès réseau

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

Dans cette leçon, les stagiaires vont découvrir les différentes méthodes de connexion réseau abordées dans ce cours. Ils doivent comprendre la manière de choisir une méthode qui leur fournisse la solution la mieux adaptée à leur réseau.

Considérations relatives à une solution LAN	Expliquez aux stagiaires l'intérêt d'une solution LAN et pourquoi ils doivent la sélectionner. Passez en revue les avantages et les inconvénients de ce type de solution.
Considérations relatives à une solution VPN	Expliquez aux stagiaires l'intérêt d'une solution VPN et pourquoi ils doivent la sélectionner. Passez en revue les avantages et les inconvénients de ce type de solution.
Considérations relatives à une solution d'accès à distance	Expliquez aux stagiaires l'intérêt d'une solution d'accès à distance et pourquoi ils doivent la sélectionner. Passez en revue les avantages et les inconvénients de ce type de solution.
Présentation multimédia : Planification des clients VPN et de connexion d'accès à distance	Revenez plusieurs fois sur la présentation pour vous assurer que les stagiaires comprennent les principaux concepts. Passez en revue les principales questions et recherchez les réponses dans la présentation. Veillez à pouvoir répondre aux questions des stagiaires relatives à la Planification des clients VPN et de connexion d'accès à distance. Si les explications semblent confuses aux stagiaires, il est préférable d'arrêter la présentation et de répondre à leurs questions.
Considérations relatives à une solution sans fil	Expliquez aux stagiaires l'intérêt d'une solution sans fil et pourquoi ils doivent la sélectionner. Passez en revue les avantages et les inconvénients de ce type de solution.
Infrastructure d'authentification RADIUS	Expliquez qu'il est important de ne pas choisir des solutions qui génèrent un surcroît de tâches d'administration ainsi que les manières dont les stagiaires peuvent utiliser le service RADIUS (Remote Authentication Dial-In User Service) pour centraliser l'administration.
Instructions de sélection des méthodes de connexion d'accès réseau	Passez en revue les instructions et expliquez aux stagiaires pourquoi il est préférable d'utiliser une méthode de connexion d'accès réseau plutôt qu'une autre. Vérifiez que les stagiaires comprennent les conséquences du non-respect de ces instructions.
Application pratique : Sélection des méthodes de connexion d'accès réseau	Cette application pratique permet aux stagiaires d'évaluer leurs connaissances relatives à la sélection d'une méthode de connexion d'accès réseau.

Leçon : Sélection d'un plan de stratégie d'accès distant

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

Dans cette leçon, les stagiaires vont apprendre à sélectionner la stratégie d'accès distant adaptée à leur solution réseau. Si cela vous semble opportun, montrez la présentation multimédia *Présentation de l'accès distant* qui figure sur le CD-ROM du stagiaire. Cette présentation donne une vue d'ensemble des concepts d'accès à distance que les stagiaires peuvent déjà connaître. Passez en revue la présentation avant de le déterminer.

Stratégies d'accès distant

Expliquez que cette rubrique est une révision des stratégies d'accès distant et indiquez comment ces dernières s'intègrent aux services d'annuaire Active Directory®.

Propriétés de numérotation des comptes d'utilisateurs

Passez en revue les propriétés de numérotation des comptes d'utilisateurs et les deux méthodes de définition des autorisations d'accès distant.

Instructions de sélection d'un plan de stratégie d'accès distant

Passez en revue les instructions et expliquez aux stagiaires pourquoi ils doivent respecter chaque instruction. Vérifiez que les stagiaires comprennent les conséquences du non-respect de ces instructions.

Application pratique : Détermination d'un plan de stratégie d'accès distant

Cette application pratique permet aux stagiaires d'évaluer leurs connaissances relatives à la détermination d'un plan de stratégie d'accès distant.

Notes du formateur

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cet atelier.

Atelier A : Planification de l'accès réseau

Cet atelier peut sembler difficile aux stagiaires, car ils ne disposent d'aucune illustration du nouveau site. L'une des principales tâches à réaliser dans cet atelier, individuellement ou en groupe, consiste à créer un schéma général du nouveau réseau et du réseau étendu (WAN, *Wide Area Network*) du siège social de Londres.

Demandez aux stagiaires de lire l'ensemble du scénario et de sélectionner les informations qui leur semblent importantes pour prendre leurs décisions. Ils peuvent ensuite regrouper ces informations dans des listes associées à une même tâche. Les informations relatives à la bande passante, par exemple, sont disséminées dans l'ensemble du scénario. En collectant et en regroupant les informations de chaque zone logique du réseau, les stagiaires peuvent obtenir d'importantes informations sur les réseaux locaux virtuels (VLAN, *Virtual LAN*) et sur la bande passante nécessaire à la solution.

Insistez sur le fait que les stagiaires ne doivent pas lier les tâches de planification du réseau physique aux décisions de sécurité logique qu'ils prendront au niveau du système d'exploitation. L'exercice 1 ne demande pas aux stagiaires de planifier la sécurité physique. En conséquence, ils n'ont pas à analyser l'infrastructure physique.

Les stagiaires peuvent passer beaucoup trop de temps à rechercher des solutions qui interdisent aux utilisateurs non autorisés d'enregistrer le trafic LAN ou WAN. En cas de discussion sur ce sujet, invitez les stagiaires à réfléchir sur la sécurité que fournit une infrastructure commutée (les données ne sont pas reflétées sur tous les ports s'ils n'ont pas été configurés en conséquence). Les stagiaires peuvent être également confrontés aux problèmes de sécurité associés aux commutateurs de la couche 3, comme la gestion Web ou SNMP (Simple Network Management Protocol) des périphériques. L'authentification par port peut constituer la meilleure solution pour sécuriser tous les ports.

Lors de la discussion sur les solutions, invitez les stagiaires à identifier les éléments des solutions des autres groupes qui pourraient les aider dans leur tâche de planification.

Demandez aux stagiaires d'expliquer comment ils répartissent les tâches et les informations issues du scénario. Si, par exemple, les stagiaires passent plus de temps sur une tâche que sur une autre, cela peut impliquer qu'ils ne savent pas gérer un projet. Demandez aux stagiaires de déterminer constamment les points pour lesquels les contraintes de temps doivent être prises en compte.

Informations de personnalisation

Cette section identifie les caractéristiques des ateliers d'un 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*.

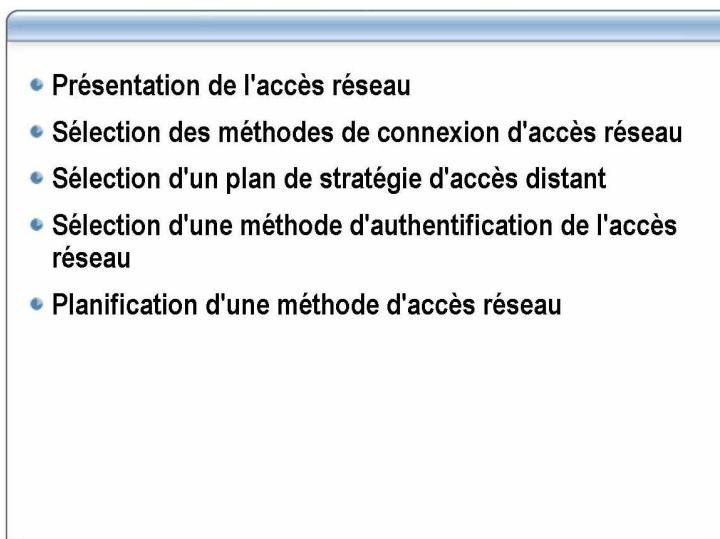
Mise en place de l'atelier

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

Ce module présente les considérations relatives à la planification d'une stratégie d'accès réseau en utilisant Microsoft® Windows Server™ 2003. Ces considérations portent sur la stratégie de connexion, les stratégies d'accès distant et l'utilisation du service IAS (Internet Authentication Service) pour centraliser l'authentification.

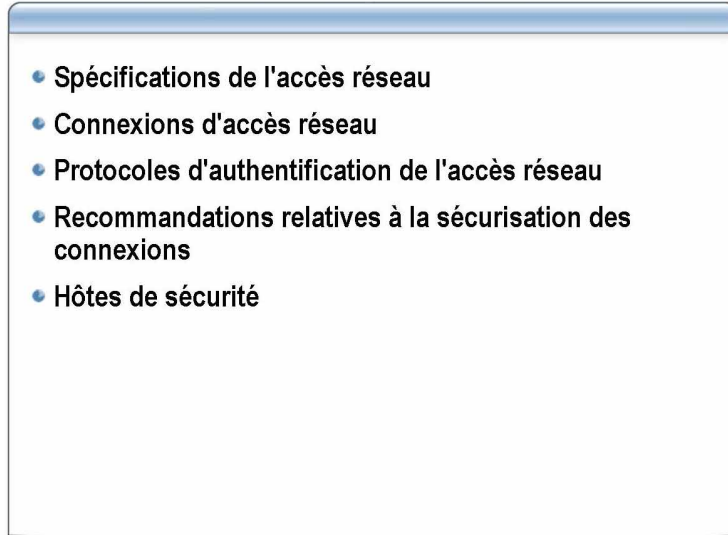
Le module présente le concept d'accès réseau. Dans ce module, l'expression « accès réseau » correspond à n'importe quelle méthode utilisée pour se connecter au réseau. Vous allez apprendre à planifier des méthodes de connexion telles que réseaux locaux, réseaux étendus sans fil, connexions d'accès à distance ou tunnels VPN (Virtual Private Networking).

Objectifs

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

- expliquer les éléments et les protocoles d'authentification d'une stratégie d'accès réseau ;
- appliquer les instructions de sélection d'une stratégie de connexion d'accès réseau ;
- appliquer les instructions de sélection d'un plan d'accès distant ;
- sélectionner une méthode d'authentification de l'accès réseau ;
- planifier une stratégie d'accès réseau.

Leçon : Présentation de l'accès réseau



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

Introduction

Une stratégie d'accès réseau occupe une place essentielle dans la planification d'une infrastructure réseau. Vous devez permettre aux utilisateurs distants d'accéder en toute sécurité aux ressources du réseau et à vos clients d'acheter vos produits et vos services.

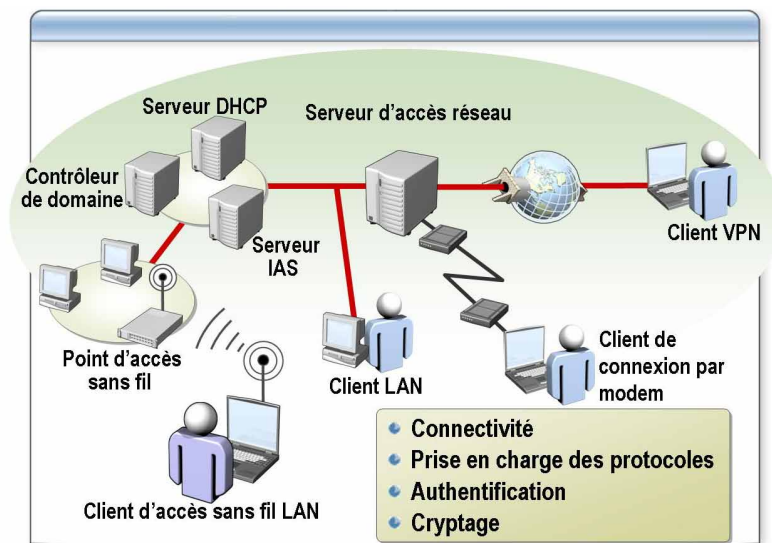
Définir la manière dont les utilisateurs se connectent et sont authentifiés et déterminer si vous devez renforcer la sécurité de l'entreprise sont des éléments essentiels d'une stratégie d'accès réseau.

Objectifs de la leçon

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

- identifier les spécifications de l'accès réseau ;
- expliquer comment les utilisateurs distants peuvent se connecter au réseau de l'entreprise ;
- identifier les méthodes d'authentification de l'accès réseau ;
- appliquer les recommandations relatives à la sécurisation des connexions d'accès réseau ;
- expliquer les différences existant entre les spécifications des hôtes de sécurité.

Spécifications de l'accès réseau



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

Introduction

Votre entreprise peut employer des milliers d'utilisateurs distants qui nécessitent d'accéder au réseau pour utiliser ses ressources et ses services. Les partenaires commerciaux et les clients doivent pouvoir accéder aux informations sur les produits 24h/24, 7j/7.

Pour répondre aux besoins de tous les utilisateurs, vous devez planifier une solution complète d'accès réseau.

Définition

L'*accès réseau* définit la manière dont les périphériques (clients, serveurs, etc.) peuvent se connecter aux ressources d'un réseau et les utiliser.

Votre solution d'accès réseau doit inclure tous les éléments ci-dessous :

- les technologies utilisées pour se connecter au niveau des couches physique et de liaison de données ;
- les mesures et les protocoles de sécurité utilisés pour protéger les données et les utilisateurs autorisés à y accéder ;
- les processus d'administration qui permettent aux utilisateurs d'accéder aux ressources appropriées en appliquant les mesures de sécurité correspondantes.

Spécification de l'accès réseau

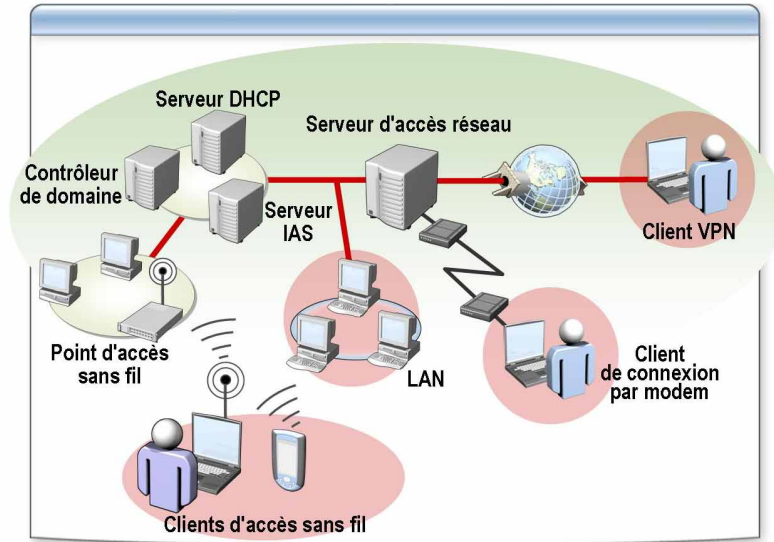
Le plan d'accès réseau doit identifier les périphériques de connexion, la prise en charge des protocoles et les méthodes d'authentification et de cryptage des utilisateurs distants. Le tableau ci-dessous répertorie chacune des spécifications et des fonctionnalités d'accès réseau.

Spécification	Description
Connectivité	Un périphérique doit pouvoir se connecter physiquement au réseau via des câbles, un signal radioélectrique ou d'autres méthodes.
Prise en charge des protocoles	Les protocoles appropriés doivent exister pour permettre l'établissement des connexions au niveau de la couche de liaison de données. Les protocoles des couches supérieures font ensuite l'objet d'une négociation jusqu'à la couche Application.
Authentification	L'authentification de chaque utilisateur et/ou périphérique peut être négociée dans chaque couche.
Cryptage	Les protocoles de cryptage peuvent être négociés et des conditions de connexion, des contraintes, des filtres et des profils peuvent être appliqués à un périphérique ou à un utilisateur donné.

Intégration du service Routage et accès distant

Le service Routage et accès distant de Windows Server 2003 s'intègre aisément à un environnement d'annuaire Active Directory® ou non-Active Directory. Il fait appel aux stratégies d'authentification et d'accès distant Windows et RADIUS (Remote Authentication Dial-In Service) pour définir les conditions, les contraintes et les filtres des demandes de connexion.

Connexions d'accès réseau



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

Introduction

Votre plan d'infrastructure détermine la manière dont les utilisateurs se connectent localement ou à distance au réseau de l'entreprise.

Connexions d'accès réseau

Il existe une multitude de formes d'accès réseau différentes. Outre les réseaux locaux câblés traditionnels, vous pouvez être amené à inclure une solution d'accès alternative telle qu'une connexion VPN, d'accès à distance ou sans fil. Le tableau ci-dessous répertorie les types de connexions d'accès réseau que vous allez étudier, accompagnés de leur description.

Connexion réseau	Description
LAN	<p>Une connexion LAN (Local Area Network) correspond généralement à une connexion câblée qui utilise des technologies telles que Ethernet ou Token Ring dans les couches physique et de liaison de données.</p> <p>En règle générale, la vitesse de transmission est très élevée (de 10 Mbps (mégabits par seconde) à 1 000 Mbps) et la liaison peut parfois fonctionner en mode duplex intégral.</p>
VPN	<p>Une connexion VPN est constituée lorsqu'un protocole de tunnel, comme PPTP (Point-to-Point Tunneling Protocol) ou L2TP (Layer Two Tunneling Protocol), est utilisé pour faire transiter les données dans un réseau existant tel qu'Internet ou un intranet. Les deux périphériques peuvent correspondre à un client qui communique avec un serveur ou à deux routeurs qui utilisent un tunnel pour se connecter à différents réseaux pour former un réseau étendu.</p> <p>La vitesse de transmission dépend de la connexion sous-jacente utilisée par le tunnel. Cette connexion peut être un réseau LAN, DSL (Digital Subscriber Line), RNIS (Réseau numérique à intégration de services), un câble ou une ligne commutée de 56 Kbps (kilo-octets par seconde).</p>

(suite)

Connexion réseau	Description
Connexion d'accès à distance	<p>Les connexions d'accès à distance utilisent généralement un modem ou un périphérique RNIS pour connecter deux périphériques dans un réseau téléphonique public commuté (PSTN, <i>Public Switched Telephone Network</i>). Ces connexions peuvent impliquer un client et un serveur ou deux routeurs. Ils peuvent être connectés en fonction des besoins, comme dans le cadre d'une connexion entre un client et un serveur, ou peuvent rester connectés lorsqu'ils sont souvent utilisés, comme c'est généralement le cas dans le cadre d'une connexion entre deux routeurs.</p> <p>Le débit se situe généralement entre 128 Kbps pour une connexion RNIS et 56 Kbps pour un modem standard d'accès à distance.</p>
Réseau local sans fil	<p>Vous pouvez également accéder à un réseau à l'aide d'un réseau local qui n'utilise pas de câble pour connecter les périphériques au réseau, mais de signaux radioélectriques ou autres.</p> <p>Les vitesses de transmission sont généralement comprises entre 11 Mbps et 54 Mbps, mais le débit réel dépend de la longueur du signal.</p>

Protocoles d'authentification de l'accès réseau

Protocole	Description
EAP	Le protocole EAP est un mécanisme d'authentification PPP (<i>Point-to-Point Protocol</i>) qui a été adapté aux segments de réseau local point à point
PEAP	Le protocole PEAP est un type de protocole EAP qui répond aux problèmes de sécurité EAP en créant préalablement un canal sécurisé dont le cryptage et l'intégrité sont assurés par TLS
IEEE.802.1x	IEEE 802.1x utilise les caractéristiques physiques de l'infrastructure réseau local commuté pour authentifier les périphériques connectés à un port LAN
Kerberos	L'authentification Kerberos permet d'accéder aux ressources d'un domaine ou à celles des domaines autorisés en identifiant une seule fois l'utilisateur

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

Introduction

Lorsque vous planifiez une stratégie d'accès réseau, vous devez déterminer la meilleure méthode d'authentification à utiliser. Vous pouvez mettre en œuvre l'authentification en utilisant un grand nombre de méthodes et de protocoles différents. Cette section donne une vue d'ensemble des méthodes et des protocoles d'authentification.

EAP

Le protocole EAP (Extensible Authentication Protocol) est un mécanisme d'authentification PPP (Point-to-Point Protocol) qui a été adapté aux segments de réseau local point à point. Les messages EAP envoyés correspondent généralement à la charge utile des trames PPP. Le protocole EAP fournit le meilleur niveau de flexibilité pour appliquer des méthodes d'authentification renforcées. Vous pouvez utiliser EAP pour prendre en charge des schémas d'authentification tels que Generic Token Card, One Time Password, MD5-Challenge et TLS (Transport Layer Security), pour les cartes à puce et les certificats en complément des futures technologies d'authentification. EAP est un élément technologique important pour sécuriser les connexions.

PEAP

Bien que le protocole EAP fournisse une souplesse d'authentification en utilisant plusieurs types EAP, la totalité de la conversation EAP peut être envoyée sous la forme d'un texte en clair (non crypté). Le protocole PEAP (Protected Extensible Authentication Protocol) est un type de protocole EAP qui répond aux problèmes de sécurité EAP en créant préalablement un canal sécurisé dont le cryptage et l'intégrité sont assurés par TLS. Ensuite, une nouvelle négociation EAP est établie avec un autre type EAP pour authentifier la tentative d'accès du client.

Le protocole PEAP peut servir à authentifier les clients sans fil 802.11, mais il n'est pas pris en charge pour les clients VPN, ni pour les autres clients d'accès à distance. En conséquence, vous pouvez configurer PEAP comme méthode d'authentification dans le cadre d'une stratégie d'accès distant uniquement lorsque vous utilisez le service IAS.

IEEE 802.1x	<p>La norme IEEE (Institute of Electrical and Electronics Engineers) 802.1x définit le contrôle d'accès réseau par port servant à authentifier l'accès aux réseaux Ethernet. IEEE 802.1x utilise les caractéristiques physiques de l'infrastructure réseau local commuté pour authentifier les périphériques connectés à un port LAN. L'accès au port peut être refusé si la procédure d'authentification échoue. IEEE 802.1x utilise EAP comme protocole d'authentification. EAP a été conçu pour pouvoir être étendu à pratiquement n'importe quelle méthode d'authentification.</p>
Kerberos	<p>Le protocole Kerberos version 5 (Kerberos V5) vérifie l'identité de l'utilisateur et des services réseau. Cette double vérification s'appelle l'<i>authentification mutuelle</i>. L'authentification Kerberos permet d'accéder aux ressources d'un domaine ou à celles des domaines autorisés en identifiant une seule fois l'utilisateur.</p>
NTLM	<p>NTLM ou NTLM version 2 (NTLM v2) est utilisé comme protocole d'authentification entre deux ordinateurs lorsque l'un des ordinateurs ou les deux ordinateurs utilisent Microsoft Windows NT® 4.0. Les réseaux ayant ce type de configuration s'appellent des <i>réseaux mixtes</i>. En outre, NTLM v2 est le protocole d'authentification des ordinateurs qui <i>ne participent pas</i> dans un domaine, tels les serveurs autonomes ou les groupes de travail.</p>
Certificats de clé publique	<p>Un certificat de clé publique est un type d'authentification qui permet de vérifier l'identité de manière fiable. Ces certificats permettent de vérifier l'identité des ordinateurs qui utilisent des systèmes d'exploitation non-Microsoft, des ordinateurs autonomes, des clients membres d'un domaine autorisé ou des ordinateurs qui n'utilisent pas le protocole d'authentification Kerberos V5 et le service Routage et accès distant.</p> <p>Les certificats utilisent des techniques cryptographiques pour résoudre le problème d'absence de contact physique entre les parties qui communiquent. En utilisant ces techniques, vous limitez les possibilités pour une personne malveillante d'intercepter, de modifier ou de contrefaire les messages. Ces techniques cryptographiques rendent les certificats difficilement modifiables. En conséquence, il est difficile pour une entité de se faire passer pour quelqu'un d'autre. Un certificat peut être stocké localement dans le magasin des certificats du périphérique ou sur une carte à puce. Une <i>carte à puce</i> est un périphérique de la taille d'une carte de crédit que vous utilisez en entrant un code d'accès pour activer l'authentification par certificat et l'identification unique et vous connecter à l'entreprise.</p>
Clé prépartagée	<p>La méthode de clé prépartagée implique que les parties qui se connectent reconnaissent mutuellement une clé secrète partagée qui est utilisée dans le cadre de l'authentification. Cette méthode s'appelle également <i>secret partagé</i>. Les clés prépartagées ne constituent pas une méthode d'authentification très fiable, car leur origine et leur histoire restent inconnues, contrairement aux certificats. Utilisez une infrastructure de clé publique si vous voulez disposer d'une méthode d'authentification efficace à long terme.</p> <p>Lors de la négociation de la sécurité, les informations sont cryptées avant d'être transmises par une clé de session. La clé de session est créée par un calcul Diffie-Hellman et à l'aide de la clé secrète partagée. Les informations sont décryptées à la réception en utilisant cette clé. L'homologue authentifie le paquet de l'autre homologue en décryptant et en vérifiant le hachage dans le paquet, qui correspond au hachage de la clé prépartagée.</p>

Authentification biométrique

La méthode d'authentification biométrique vérifie l'identité d'une personne en comparant ses caractéristiques physiques, telles les empreintes digitales ou les caractéristiques de l'iris, à des données stockées. Les périphériques d'authentification biométrique incluent les scanners d'empreintes digitales, les scanners d'iris et les systèmes de vérification vocale. Les données biométriques peuvent remplacer potentiellement les mots de passe et les codes personnels des cartes à puce, car elles ne peuvent pas être oubliées, perdues, volées, ni partagées. Vous pouvez utiliser l'authentification biométrique en créant une extension EAP.

Recommandations relatives à la sécurisation des connexions

- Configuration des cartes réseau Ethernet
 - Carte à puce
 - EAP Protégé
 - MD5-Challenge
- Prise en charge de l'ouverture de session interactive par clé publique
- Utilisation d'IPSec
- Authentification d'homologue à homologue
- Utilisation d'une infrastructure RADIUS

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

Introduction

La sécurité d'accès réseau occupe une place essentielle dans la planification d'une infrastructure réseau. Bien que les composants décrits dans cette section puissent sembler incompatibles à première vue, ils jouent tous un rôle important dans la planification et l'implémentation de la sécurité de l'accès réseau.

Configuration des cartes réseau Ethernet

Sur Windows Server 2003, vous pouvez configurer les cartes réseau Ethernet pour authentifier les ordinateurs ou les utilisateurs avec un commutateur Ethernet. Vous pouvez configurer les cartes réseau Ethernet pour qu'elles utilisent l'authentification 802.1x. Vous pouvez sélectionner n'importe lequel des types EAP suivants :

- Carte à puce ou autre certificat

Ce type EAP permet d'utiliser une carte à puce ou le magasin des certificats local pour fournir les informations de certificat de l'authentification du commutateur.
- PEAP

Ce type EAP protège les connexions EAP. Avec PEAP, vous pouvez choisir la méthode d'authentification **Mot de passe sécurisé (EAP-MSCHAP v2)** ou **Carte à puce ou autre certificat**.
- MD5-Challenge

Ce type EAP est une méthode d'authentification par mot de passe. Il utilise le même protocole de négociation par challenge que le protocole CHAP (Challenge Handshake Authentication Protocol) basé sur PPP, mais il envoie les challenges et les réponses d'accès sous forme de messages EAP.

Prise en charge de l'ouverture de session interactive par clé publique

Vous pouvez utiliser Windows Server 2003 pour prendre en charge l'ouverture de session interactive par clé publique à l'aide d'un certificat X.509 version 3 stocké sur une carte à puce avec une clé privée. Au lieu d'entrer un mot de passe, l'utilisateur tape, dans l'interface GINA (Graphical Identification and Authentication), un code personnel qui l'identifie.

Le certificat de clé publique de l'utilisateur est extrait de la carte par un processus sécurisé pour être validé et pour vérifier qu'il s'agit d'un utilisateur autorisé. Au cours de la procédure d'authentification, une clé publique basée sur un challenge, contenue dans le certificat, est envoyée à la carte. Le challenge vérifie que la carte que détient l'utilisateur est valide et qu'elle peut utiliser la clé privée correspondante.

Une fois les clés publique et privée vérifiées, l'identité de l'utilisateur figurant dans le certificat est utilisée pour référencer l'objet Utilisateur dans l'annuaire Active Directory, créer un jeton et envoyer un ticket d'accord de ticket au client. L'ouverture de session par clé publique a été intégrée à l'implémentation Microsoft de Kerberos V5 qui est compatible avec l'extension de clé publique spécifiée dans le document RFC-1510 « The Kerberos Network Verification Service (V5) » du comité Internet Engineering Task Force.

Utilisation de IPSec

Vous pouvez utiliser IPSec (Internet Protocol Security) pour protéger le réseau et les couches de transport. La sécurité dans ces couches est transparente dans toutes les couches supérieures, ce qui implique que les applications et les périphériques intermédiaires n'ont pas besoin d'être configurés de manière spécifique pour fonctionner avec IPSec. IPSec fournit également l'authentification mutuelle.

Authentification d'homologue à homologue

L'authentification d'homologue à homologue intervient lorsque deux homologues s'authentifient mutuellement. Si, par exemple, deux serveurs autonomes qui utilisent le service Routage et accès distant se connectent pour router des informations, les serveurs s'authentifient mutuellement au lieu d'utiliser la base de données Active Directory ou un serveur RADIUS. La même procédure s'applique lorsque deux ordinateurs configurés pour IPSec utilisent une clé prépartagée. Pour s'authentifier, il suffit aux deux ordinateurs de communiquer.

Utilisation d'une infrastructure RADIUS

Vous pouvez utiliser une infrastructure RADIUS pour lier toutes les conditions d'authentification du réseau. Que vous disposiez de commutateurs, de serveurs d'accès distant, de points d'accès sans fil ou autre devant authentifier les utilisateurs ou les périphériques, vous pouvez utiliser un serveur RADIUS pour les authentifier dans un même emplacement à l'aide d'un ensemble de stratégies d'accès distant dans cet emplacement.

Un serveur RADIUS permet de centraliser l'authentification, ce qui réduit considérablement les tâches d'administration en évitant de créer des îlots d'authentification et simplifie la définition de stratégies d'authentification, de conditions et de restrictions cohérentes.

Hôtes de sécurité

- **Comparaison des hôtes de sécurité**
 - Hôte de sécurité qui vérifie l'authentification au cours de la demande de connexion
 - Hôte de sécurité appelé lors de la procédure d'authentification de la connexion
- **Utilisation d'un modèle d'ouverture de session interactive**

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

Introduction

Un hôte de sécurité permet de renforcer la sécurité déjà appliquée par les connexions réseau et la famille Windows Server 2003. Lorsque vous planifiez une stratégie d'accès réseau, vous devez déterminer si vous devez renforcer la sécurité.

Définition

Un *hôte de sécurité* est un périphérique d'authentification qui vérifie si une connexion est autorisée à se connecter à un serveur d'accès réseau.

Comparaison des hôtes de sécurité

Pour pouvoir implémenter des hôtes de sécurité, vous devez connaître les différences existant entre les types d'hôtes de sécurité suivants :

- Hôtes de sécurité qui vérifient l'authentification au cours de la demande de connexion

Ce type d'hôte de sécurité se trouve entre vous et le serveur d'accès réseau et vérifie l'authentification avant que vous soyez authentifié par le serveur d'accès réseau. Il permet généralement de renforcer la sécurité en demandant une clé matérielle pour l'authentification. Il vérifie que vous possédez physiquement la clé avant de vous autoriser à accéder au serveur d'accès réseau. Grâce à cette architecture ouverte, l'administrateur système dispose de divers hôtes de sécurité pour renforcer la sécurité des connexions réseau, mais il peut limiter les vérifications d'authentification à certains types de connexions.

- Hôte de sécurité appelé lors de la procédure d'authentification de la connexion

Ce type d'hôte de sécurité permet d'appliquer une procédure d'authentification d'accès réseau personnalisée. Cette authentification peut renforcer ou remplacer la vérification standard de vos informations d'identification réseau, effectuée par le serveur d'accès réseau. Les serveurs RADIUS, par exemple, correspondent à ce type d'hôte de sécurité, car ils authentifient les utilisateurs à la place du serveur d'accès réseau. Avec l'introduction de EAP, les autres constructeurs peuvent désormais créer des interfaces entre l'authentification d'accès réseau et leurs propres serveurs propriétaires. Ces types de serveurs sont utilisés pour vérifier les cartes à puce et d'autres formes d'authentification étendue.

Exemple de système de sécurité

Supposons qu'un système de sécurité soit constitué de deux périphériques matériels : d'un hôte de sécurité et d'une carte de sécurité. L'hôte de sécurité se trouve entre le serveur d'accès réseau et sa connexion réseau. La carte de sécurité est de la taille d'une carte de crédit qui ressemble à une calculatrice de poche sans touches. La carte de sécurité affiche un numéro d'accès différent toutes les minutes. Le numéro est synchronisé avec un numéro similaire que l'hôte de sécurité calcule toutes les minutes. Lors de la connexion, vous envoyez un code personnel et le numéro de la carte de sécurité à l'hôte. Si ces informations correspondent au numéro calculé par l'hôte, l'hôte de sécurité vous connecte au serveur d'accès réseau.

Un autre hôte de sécurité de même type vous demande de taper un nom d'utilisateur (qui peut être ou non identique au nom d'utilisateur d'accès distant) et un mot de passe (qui n'est pas identique au mot de passe d'accès distant).

Utilisation d'un modèle d'ouverture de session interactive

GINA, un composant DLL (Dynamic Link Library) chargé par Winlogon, implémente les conditions d'authentification en utilisant un modèle d'ouverture de session interactive. Ce modèle exécute toutes les interactions d'identification et d'authentification des utilisateurs. Msgina.dll, le composant GINA standard fourni par Microsoft et chargé par Winlogon, peut être remplacé par un composant GINA personnalisé par un tiers.

Vous pouvez également créer un composant GINA qui utilise les services de l'hôte de sécurité pour l'authentification.

Leçon : Sélection des méthodes de connexion d'accès réseau

- Considérations relatives à une solution LAN
- Considérations relatives à une solution VPN
- Considérations relatives à une solution de connexion à distance
- Présentation multimédia : Planification des clients VPN et des clients de connexion d'accès à distance
- Considérations relatives à une solution sans fil
- Infrastructure d'authentification RADIUS
- Instructions de sélection des méthodes de connexion d'accès réseau

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

Introduction

Lorsque vous sélectionnez une méthode de connexion d'accès réseau, vous devez évaluer toutes les méthodes de connexion disponibles (LAN, VPN, à distance ou sans fil, par exemple), puis déterminer la méthode adaptée à votre solution d'accès réseau.

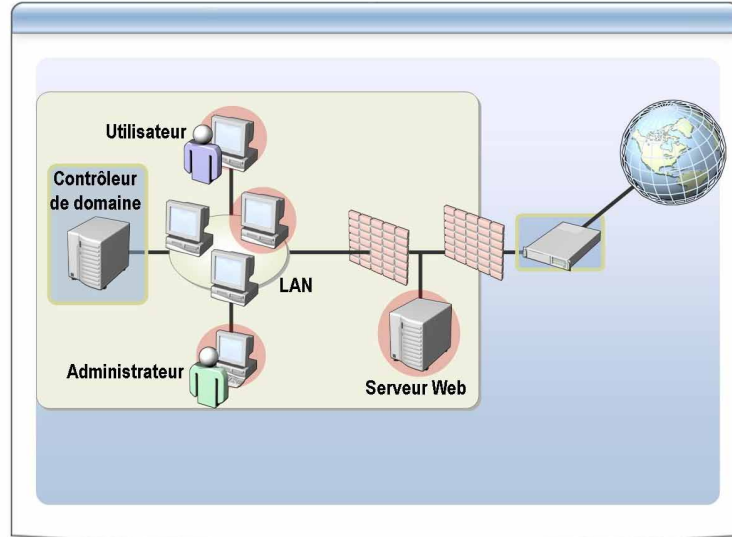
Pour réduire les tâches d'administration, vous devez envisager d'utiliser Microsoft IAS Server (Internet Authentication Server) pour centraliser l'authentification des utilisateurs distants dans un emplacement.

Objectifs de la leçon

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

- déterminer si une solution LAN constitue une méthode appropriée pour votre stratégie d'accès réseau ;
- déterminer si une solution VPN constitue une méthode appropriée pour votre stratégie d'accès réseau ;
- déterminer si une solution de connexion à distance constitue une méthode appropriée pour votre stratégie d'accès réseau ;
- expliquer comment planifier des clients VPN et des clients de connexion par modem ;
- déterminer si une solution sans fil constitue une méthode appropriée pour votre stratégie d'accès réseau ;
- expliquer comment centraliser l'authentification des clients en utilisant l'authentification IAS Server et RADIUS ;
- appliquer les instructions de sélection d'une méthode de connexion d'accès réseau.

Considérations relatives à une solution LAN



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

Introduction

Vous pouvez déterminer que la stratégie d'infrastructure réseau doit inclure une connexion LAN. Toutefois, avant de définir le réseau local, vous devez comprendre les besoins de votre entreprise. La stratégie LAN présentée dans cette section documente l'implémentation du plan de sécurité.

Vous devez savoir que l'implémentation d'une solution LAN peut avoir un impact négatif sur les performances du réseau. Par exemple, une entreprise qui utilise un média partagé (tel un concentrateur) doit le partager avec tous les autres nœuds du support, ce qui réduit le débit potentiel. Toutefois, l'utilisation d'un commutateur à la place d'un concentrateur peut atténuer l'impact sur les performances du réseau.

Sélection d'un LAN

En règle générale, les entreprises optent pour une solution LAN pour les serveurs et les clients fixes qui nécessitent des connexions haut débit. Par exemple, une entreprise qui dispose d'un serveur (Web, de fichiers et de bases de données) ou de clients devant bénéficier d'un haut débit, sans besoin de mobilité, implémentera généralement une solution LAN. Les clients à haut débit incluent ;

- n'importe quel serveur (Active Directory, DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), Web, etc.) ;
- les stations de travail graphiques ;
- les stations de travail multimédias ;
- tout autre système qui transfère de gros volumes de données sur le réseau.

Choix d'une solution LAN

Pour pouvoir déterminer si une solution LAN est adaptée à votre stratégie d'infrastructure réseau, vous devez tenir compte des avantages et des inconvénients de ce type d'accès réseau qui sont décrits dans le tableau ci-dessous.

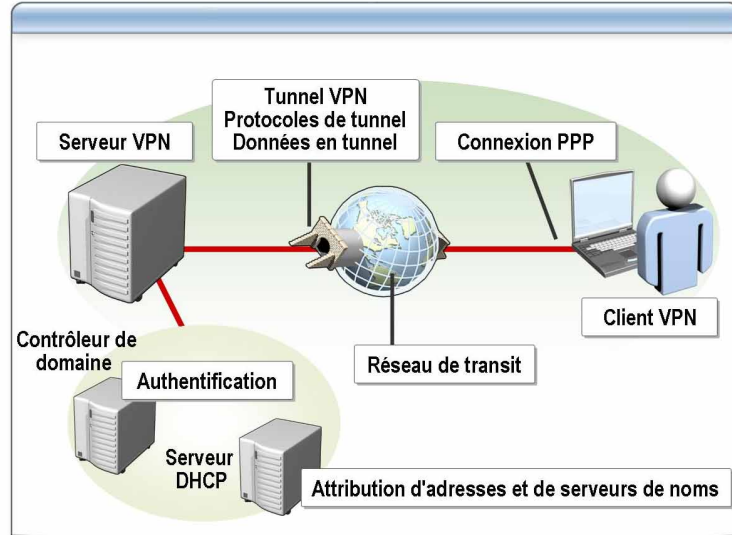
Considération	Exemples
Avantages	<ul style="list-style-type: none"> • Transmission haut débit (10 - 1 000 Mbps pour Ethernet). • Connexion sans interférence de signal. • Le réseau n'est généralement pas affecté par des pertes de connexion ou une diminution de la vitesse de transmission résultant d'une interférence de signal. • Média non partagé. • Les technologies de commutation existantes permettent d'effectuer des transmissions point à point (semi duplex ou duplex intégral). Ces technologies augmentent le débit du média. • Technologie éprouvée maîtrisée utilisant des matériels courants économiques.
Inconvénients	<ul style="list-style-type: none"> • Les périphériques doivent être connectés physiquement, ce qui limite la mobilité. • Le coût initial élevé de l'implémentation d'une solution LAN peut être prohibitif. Le câblage de l'infrastructure doit être effectué, ce qui peut être onéreux et prendre beaucoup de temps.

Options de sécurité

Une solution LAN contient de nombreuses fonctions de sécurité bien intégrées. Il peut s'agir de mécanismes d'authentification tels que Kerberos V5 et NTLM. En complément de ces méthodes intégrées, vous pouvez utiliser :

- TLS avec IPSec ;
- la sécurité SSL (Secure Sockets Layer) ;
- TLS avec des certificats de sécurité X.509 v3.

Considérations relatives à une solution VPN



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

Introduction

Si la stratégie de réseau inclut une solution VPN, vous devez sécuriser l'accès aux ressources du réseau. Pour éviter de louer votre propre ligne privée pour vous connecter à un réseau, vous pouvez créer un tunnel sécurisé sur un réseau public tel qu'Internet pour former un réseau VPN. Le réseau VPN est authentifié et crypté à des fins de sécurité.

Sachez qu'une solution VPN peut affecter les performances. Si, par exemple, vous dépendez d'une connexion réseau sous-jacente qui fournit un débit LAN ou une connexion par modem de 28 Kbps, vous pouvez subir une charge supplémentaire associée au protocole de tunnel.

Sélection d'une solution VPN

Les entreprises adoptent de manière croissante des connexions VPN comme solution d'accès réseau. Ce type de solution peut permettre à une entreprise de répondre non seulement aux besoins de sécurité, mais également aux besoins des clients distants. Une solution VPN peut s'avérer appropriée :

- lorsque les employés de l'entreprise se trouvent dans des emplacements éloignés ;
- lorsque l'entreprise doit connecter deux périphériques (un client et un serveur ou deux routeurs).

Choix d'une solution VPN

Pour pouvoir déterminer si une solution VPN est adaptée à votre stratégie d'infrastructure réseau, vous devez tenir compte des avantages et des inconvénients de ce type d'accès réseau qui sont décrits dans le tableau ci-dessous.

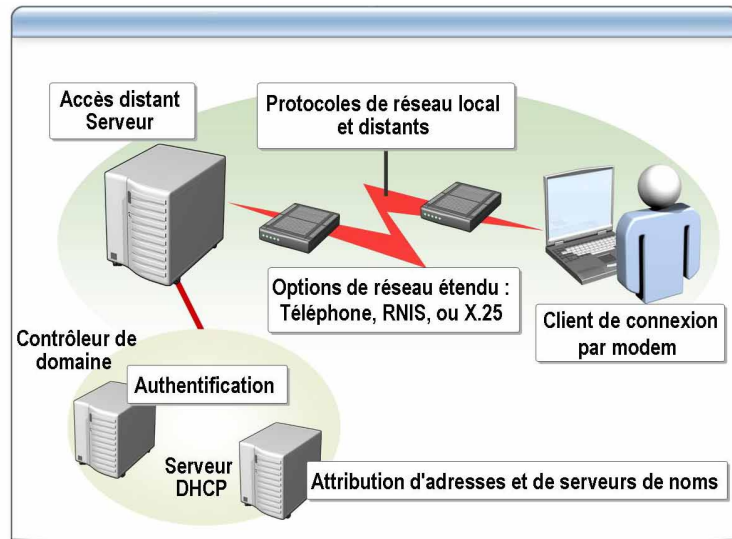
Considération	Exemples
Avantages	<ul style="list-style-type: none"> • Possibilité d'utiliser une infrastructure réseau existante (Internet ou intranet) pour transporter les données tunnelées. • Aucune nécessité d'utiliser une connexion privée entre les périphériques. • Plus évolutive qu'une solution de connexion à distance.
Inconvénients	<ul style="list-style-type: none"> • Le tunneling des données peut créer une surcharge. • Les deux périphériques doivent prendre en charge les protocoles de tunnel (PPTP ou L2TP). • Plus grand risque de visualisation et d'analyse des paquets par des intrus. Bien que les paquets puissent être cryptés, hachés et authentifiés, ils sont toujours transmis dans un réseau public (Internet, en l'occurrence). • Prise en charge supplémentaire nécessaire. Vous devez vous assurer que votre infrastructure réseau permet de transmettre les données tunnelées d'Internet vers votre réseau privé.

Options de sécurité

La sécurité est un élément important quelle que soit la connexion à distance. Vous pouvez sécuriser une solution VPN des manières suivantes :

- Authentification
 - Méthodes d'authentification PPP standard ([MS-CHAPv2], MS-CHAP [Microsoft - Challenge Handshake Authentication Protocol], PAP [Password Authentication Protocol], etc).
 - Méthodes d'authentification EAP (incluant des certificats de clé publique).
 - IPSec
- Cryptage des données
 - Microsoft Point-to-Point Encryption (MPPE 40, 56 ou 128 bits)
 - IPSec
- Contraintes de connexion (heure, durée de connexion, etc).
Ces contraintes permettent de restreindre les connexions.

Considérations relatives à une solution de connexion à distance



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

Introduction

Avant de sélectionner une solution de connexion à distance, sachez qu'une telle solution est peut être la solution d'accès distant la plus coûteuse pour l'entreprise. Toutefois, il s'agit probablement de la solution la plus économique pour l'utilisateur, les deux périphériques étant reliés par une connexion téléphonique directe.

Sachez également qu'une solution de connexion à distance peut poser des problèmes de performances liés principalement à la bande passante limitée lorsque vous utilisez un réseau téléphonique public commuté ou à l'intégrité de la ligne téléphonique.

Sélection d'une solution de connexion à distance

Si vous devez établir une connexion point à point entre deux périphériques, qu'il s'agisse d'un client et d'un serveur ou de deux routeurs, vous pouvez utiliser le réseau téléphonique public commuté pour connecter les périphériques pour un coût relativement faible pour l'utilisateur final. Toutefois, les coûts supplémentaires associés au matériel nécessaire seront à la charge de l'entreprise.

Choix d'une solution de connexion à distance

Pour pouvoir déterminer si une solution de connexion à distance est adaptée à votre stratégie d'infrastructure réseau, vous devez tenir compte des avantages et des inconvénients de ce type d'accès réseau qui sont décrits dans le tableau ci-dessous.

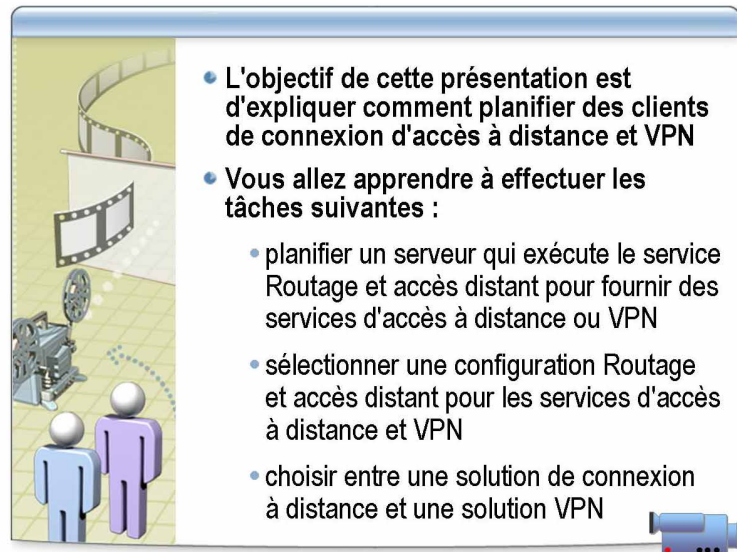
Considération	Exemples
Avantages	<ul style="list-style-type: none"> • Le coût de la ligne est faible. • Une solution de connexion à distance est immédiatement disponible. • La technologie est éprouvée et fiable (dans la plupart des pays). • La configuration est simple.
Inconvénients	<ul style="list-style-type: none"> • La vitesse de transmission peut être lente (entre 28 Kbps et 128 Kbps). • L'évolutivité est limitée. • Elle nécessite un modem pour chaque connexion et vous devez donc acheter et configurer des composants matériels supplémentaires. • Elle peut ne pas être fiable dans certains pays. • Elle peut être soumise à des interférences et du bruit parasite du fait de la nature analogique du signal.

Options de sécurité

Vous pouvez sécuriser une solution de connexion à distance de la même manière qu'une solution VPN en utilisant les options suivantes :

- Authentification
 - Méthodes d'authentification PPP standard ([MS-CHAPv2], MS-CHAP, PAP, etc).
 - Méthodes d'authentification EAP (incluant des certificats de clé publique)
- Cryptage des données
MPPE 40, 56 ou 128 bits
- Contraintes de connexion (heure, durée de connexion, etc).
Vous pouvez utiliser ces contraintes pour restreindre les connexions.

Présentation multimédia : Planification des clients VPN et de connexion d'accès à distance



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

Emplacement du fichier Pour visualiser la présentation multimédia *Planification des clients VPN et de connexion d'accès à distance*, ouvrez la page Web du CD-ROM du stagiaire, cliquez sur **Multimédia**, puis sur le titre de la présentation.

Objectifs Cette présentation explique comment planifier des clients de connexion d'accès à distance et VPN.

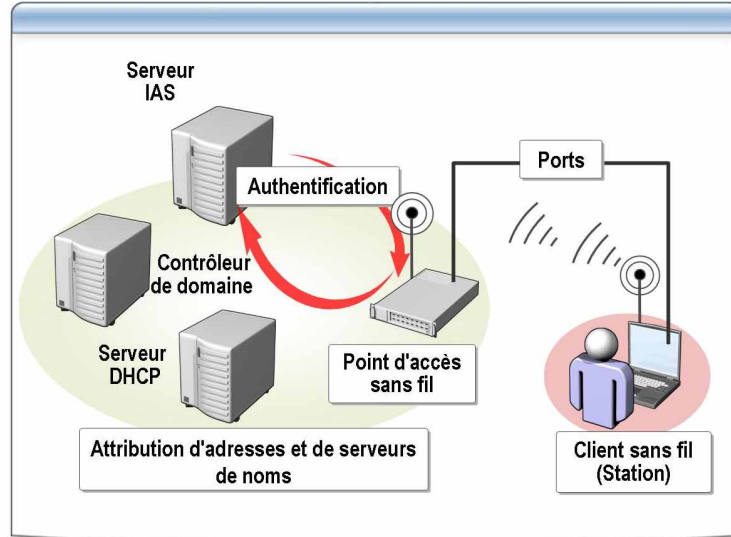
Vous allez apprendre à effectuer les tâches suivantes :

- planifier un serveur qui exécute le service Routage et accès distant pour fournir des services d'accès à distance ou VPN ;
- sélectionner une configuration Routage et accès distant pour les services d'accès à distance et VPN ;
- choisir entre une solution de connexion à distance et une solution VPN.

Questions clés Au cours de cette présentation, vous devez vous poser les questions suivantes :

- Quelle est la première étape de la planification d'une solution d'accès distant ?
- Quelles sont les procédures qui doivent être exécutées avant que l'utilisateur se connecte au serveur d'accès distant ?
- Quel est le protocole de tunnel qui fournit la meilleure sécurité ?

Considérations relatives à une solution sans fil



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

Introduction

Une solution sans fil permet aux utilisateurs itinérants de se déplacer tout en restant connectés au réseau. Les technologies de communication sans fil étendent le concept « pas de câble supplémentaire ». Dans un réseau sans fil, tous les ordinateurs transmettent les données via un point d'accès sans fil central en utilisant des signaux radioélectriques. Lorsque vous déterminez une solution d'accès réseau sans fil, vous devez tenir compte de la sécurité de la connexion et des inconvénients d'un réseau sans fil.

Les réseaux sans fil posent deux problèmes de performance principaux. Le premier problème réside dans le média partagé qui peut réduire la bande passante disponible. Le second problème réside dans le fait que la faiblesse du signal peut affecter non seulement la connexion, mais également la vitesse de transmission. Les transmissions radioélectriques (et les autres formes de transmission) sont efficaces sur une certaine distance, puis se dégradent.

Sélection d'une solution sans fil

Si l'entreprise dispose de clients mobiles, une connexion sans fil peut être appropriée. Un client mobile n'est pas nécessairement un ordinateur portable de base, mais peut être un périphérique informatique très puissant capable d'exécuter les mêmes tâches informatiques qu'un ordinateur de bureau, et qui nécessite donc des capacités réseau similaires.

Choix d'une solution sans fil

Avant de déterminer si une solution sans fil est adaptée à votre stratégie d'infrastructure réseau, vous devez tenir compte des avantages et des inconvénients de ce type d'accès réseau qui sont décrits dans le tableau ci-dessous.

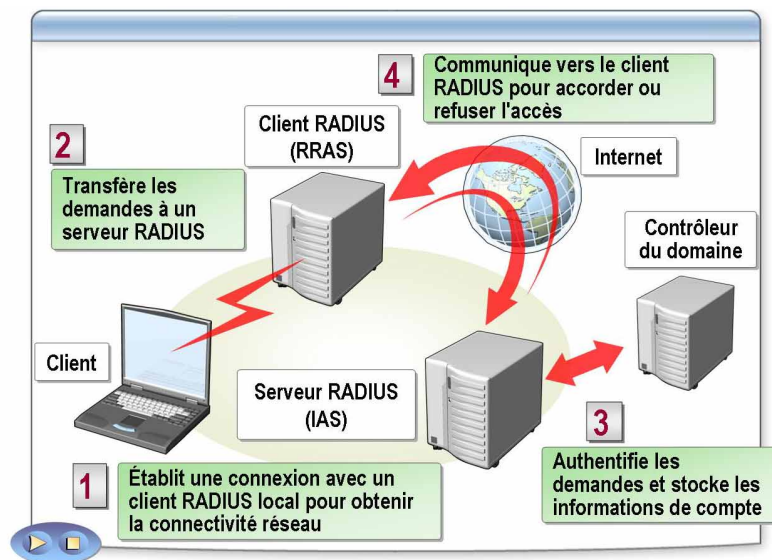
Considération	Exemples
Avantages	<ul style="list-style-type: none"> • Mobilité (notamment déplacement entre les points d'accès sans fil). • Aucun besoin d'infrastructure câblée coûteuse. • Intégration simple aux réseaux câblés. • Prise en charge des mêmes protocoles et technologies que les réseaux câblés (Ethernet, TCP/IP, etc). • Débit (entre 11 Mbps et 54 Mbps maximum).
Inconvénients	<ul style="list-style-type: none"> • Média partagé. • Portée limitée. • Affectée par les interférences ou les obstacles. • Complexité de la planification, de la configuration et de l'administration du fait qu'il s'agit d'une technologie relativement nouvelle. • Sécurité mal intégrée.

Options d'authentification

Deux options d'authentification sont disponibles avec les réseaux sans fil. Les deux méthodes utilisent Wired Equivalent Privacy pour le cryptage. Ces options sont les suivantes :

- La norme 802.11 définit les types d'authentification en système ouvert et par clé partagée. Cette norme est considérée comme étant la moins sûre pour les réseaux sans fil. L'authentification en système ouvert permet d'identifier les utilisateurs, mais pas de les authentifier, et l'authentification par clé partagée n'est pas très souple.
- La norme 802.1x définit le contrôle d'accès réseau par port qui est utilisé pour authentifier l'accès aux réseaux Ethernet. Bien que cette norme soit conçue pour les réseaux Ethernet câblés, elle a été adaptée aux réseaux locaux 802.11 sans fil. Cette norme est considérée comme étant la plus sûre pour les réseaux sans fil ; elle inclut des méthodes d'authentification EAP en utilisant des cartes à puce et d'autres certificats ainsi que la vitesse de transmission ou les connexions interrompues PEAP.

Infrastructure d'authentification RADIUS



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

Introduction

Bien que vous puissiez créer et administrer plusieurs méthodes d'authentification pour les connexions d'accès réseau, cette stratégie peut accroître les tâches d'administration.

Pour éviter ce problème, vous pouvez utiliser IAS Server pour disposer d'une infrastructure RADIUS pour authentifier, dans un même emplacement, tous les clients (VPN, connexion à distance, sans fil) qui accèdent au réseau.

Authentification IAS Server et RADIUS

IAS Server fournit un emplacement central pour toutes les stratégies d'accès distant, ce qui facilite l'administration des contraintes, des paramètres et des profils de connexion.

Une fois l'infrastructure RADIUS en place, vous pouvez configurer les serveurs d'accès réseau (notamment les serveurs qui exécutent le service Routage et accès distant et les points d'accès sans fil) pour qu'ils utilisent IAS Server pour exécuter toutes les opérations d'authentification sur le réseau.

Authentification Active Directory

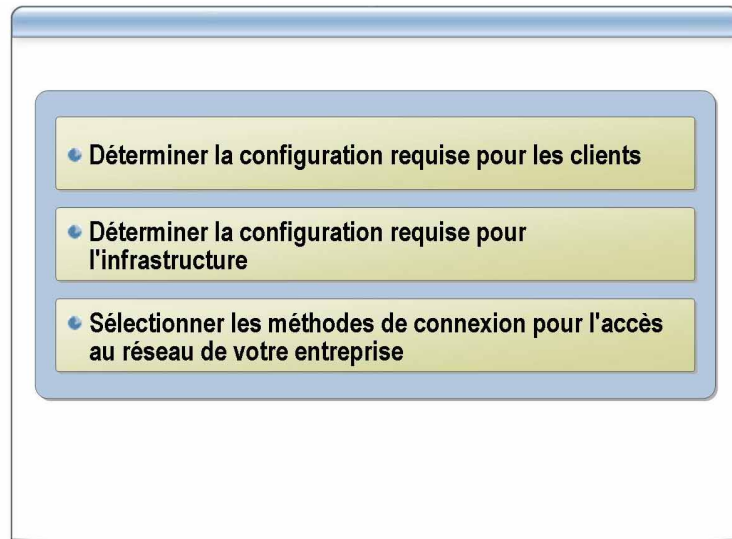
Active Directory inclut une infrastructure d'authentification Kerberos V5 qui fonctionne en transparence à l'arrière plan et ne nécessite qu'un nombre limité de tâches de configuration et d'administration. L'authentification NTLM présente les mêmes avantages. Ces deux méthodes d'authentification font partie de l'authentification intégrée du système d'exploitation.

Authentification de l'accès réseau

L'authentification n'est pas clairement définie pour les options d'accès distant (VPN, connexion à distance et sans fil). Les serveurs d'accès réseau pouvant constituer potentiellement des îlots d'authentification, vous pouvez être amené à exécuter des tâches d'administration et de configuration distinctes qui peuvent entraîner l'existence de stratégies et de paramètres différents sur chacun des serveurs.

L'existence de stratégies et de paramètres différents sur chaque serveur peut créer des environnements utilisateur incohérents en fonction du serveur auquel l'utilisateur se connecte. Dans ce cas, l'accès distant peut augmenter la charge de travail des responsables de l'administration et entraîner des problèmes de sécurité sur le serveur d'accès réseau.

Instructions de sélection des méthodes de connexion d'accès réseau



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

Introduction

Avant de sélectionner une méthode de connexion d'accès réseau, vous devez tenir compte des spécifications des clients et de l'infrastructure du réseau. Vous devez tenir compte des éléments suivants :

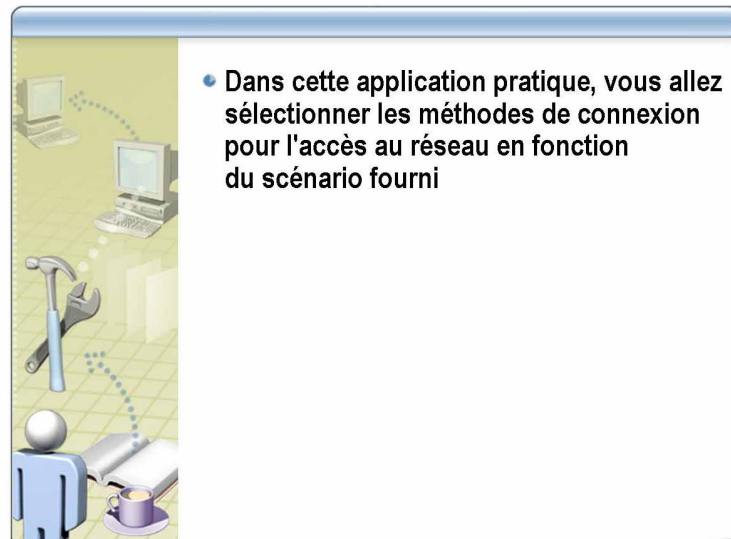
- Les spécifications des utilisateurs distants peuvent inclure la bande passante appropriée, la sécurisation des connexions, la mobilité et la fiabilité.
- Les spécifications de l'infrastructure réseau peuvent inclure des services et des ressources hautement disponibles, très fiables et très sécurisées.

Sélection d'une stratégie d'accès réseau

Après avoir déterminé les spécifications de l'accès réseau, consultez le tableau suivant et choisissez la stratégie d'accès réseau appropriée. Dans le tableau, le niveau Haute, Moyenne ou Basse est affecté à chacune des spécifications. Le tableau ne contient pas toutes les spécifications car elles peuvent dépendre d'éléments dont vous n'avez pas le contrôle.

Stratégie de connexion	Bande passante	Sécurité	Mobilité	Fiabilité
LAN	Haute	Haute	Basse (points fixes)	Haute
VPN	Moyenne (dépend de la méthode de connexion)	Haute (sécurité nécessaire)	Fonctionne avec n'importe quelle connexion	Dépend de la disponibilité du réseau public
Connexion à distance	Basse (moyenne pour les technologies numériques)	Basse	N'importe quel point d'accès PSTN	Dépend de la disponibilité du réseau PSTN
Sans fil	Basse à moyenne (média partagé)	Haute (sécurité nécessaire)	Haute dans la cellule Taille de cellule et disponibilité limitées	Bruit et encombrement

Application pratique : Sélection des méthodes de connexion d'accès réseau



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

Introduction	Dans cette application pratique, vous allez lire le scénario, puis sélectionner la méthode de connexion d'accès réseau qui convient le mieux.
Objectif	L'objectif de cette application pratique consiste à sélectionner la méthode appropriée de connexion d'accès réseau.
Instructions	<ol style="list-style-type: none">1. Lisez le scénario.2. Préparez-vous à discuter des problèmes associés à cette tâche après l'application pratique.
Scénario	<p>Fabrikam, Inc. est une société en pleine expansion qui doit étendre l'accès aux données. Les employés du service commercial demandent de pouvoir accéder aux fichiers de la base de données des ventes et des clients pendant qu'ils sont en déplacement. La société utilise une liaison T1 en dehors de son intranet, qui n'est pas très utilisée actuellement, pour accéder à son fournisseur de services Internet.</p> <p>En outre, le service technique se plaint de l'absence de connexions dans les salles de conférence que l'entrepreneur a oublié d'équiper avec un câble de catégorie 5. Toutefois, les employés du service technique sont tous équipés d'ordinateurs portables qu'ils pourraient utiliser pendant les réunions pour accéder aux informations techniques s'ils pouvaient se connecter au réseau dans les salles de conférence.</p>

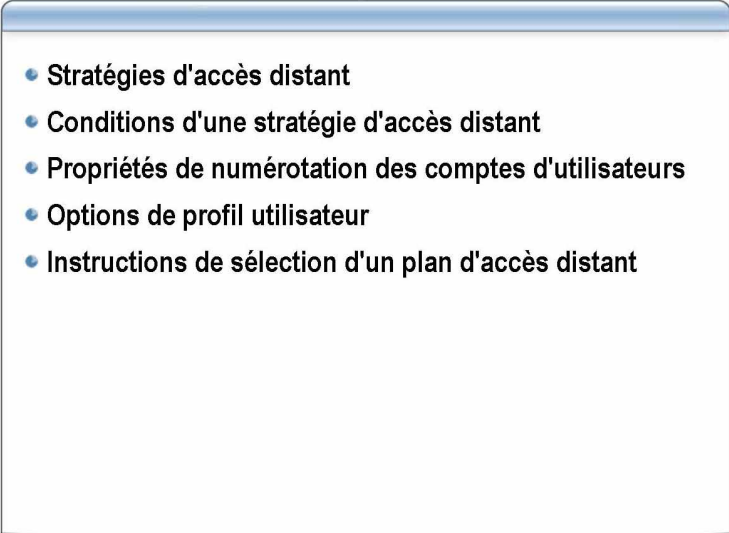
Application pratique

Quelles options de connexion suggérez-vous pour les services commercial et technique et pourquoi ?

Pour le service commercial, suggérez une solution VPN qui permettrait d'exploiter la connexion Internet actuelle de la société. La configuration d'un serveur d'accès réseau VPN apparaît plutôt simple et éviterait de mettre en place une infrastructure complète de connexion à distance. La société pourrait utiliser son infrastructure réseau actuelle pour permettre au service commercial d'accéder à son intranet. La société devrait ensuite créer un plan pour permettre à ses utilisateurs distants itinérants d'accéder aisément et efficacement à Internet en passant peut être un accord avec un fournisseur de services Internet pour authentifier les utilisateurs distants de Fabrikam, Inc. par rapport à sa propre base de données d'utilisateurs.

Un réseau sans fil semblerait répondre le mieux aux besoins du service technique. Ce réseau éliminerait les coûts et les problèmes de recâblage des salles de conférence, associés à une connexion LAN et pourrait fournir une bande passante comparable adaptée aux besoins des utilisateurs. Bien qu'il serait nécessaire de planifier, tester, implémenter et administrer une infrastructure sans fil et de fournir les services d'assistance technique appropriés, une solution sans fil pourrait être la meilleure solution à long terme car il s'agit d'une technologie plus souple qui permet aux utilisateurs d'accéder aux informations depuis n'importe quel emplacement.

Leçon : Sélection d'un plan de stratégie d'accès distant

- 
- Stratégies d'accès distant
 - Conditions d'une stratégie d'accès distant
 - Propriétés de numérotation des comptes d'utilisateurs
 - Options de profil utilisateur
 - Instructions de sélection d'un plan d'accès distant

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

Introduction

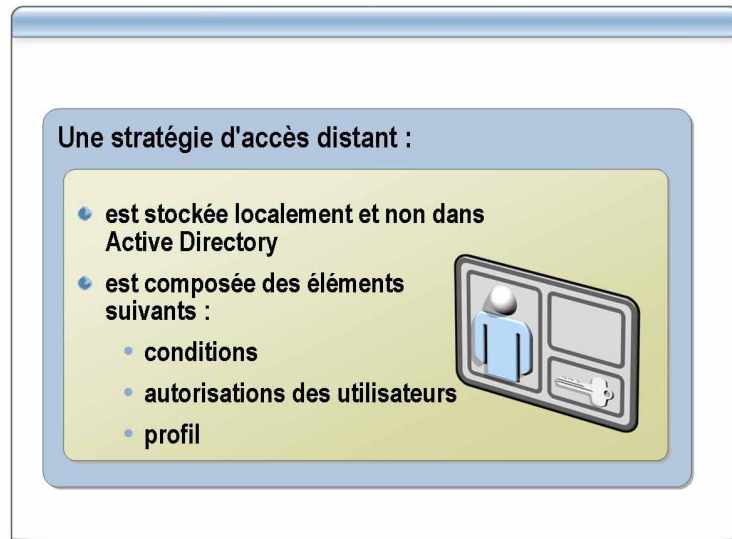
Lorsque vous sélectionnez un plan de stratégie d'accès distant, vous devez appliquer les stratégies appropriées qui définissent la manière dont les utilisateurs distants se connectent au réseau de l'entreprise. Les conditions des stratégies et les propriétés d'accès distant déterminent les autorisations et l'authentification des utilisateurs qui font partie de leur profil utilisateur.

Objectifs de la leçon

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

- expliquer comment les stratégies d'accès distant sont appliquées ;
- identifier les attributs des conditions des stratégies d'accès distant ;
- expliquer comment définir les autorisations d'accès distant ;
- expliquer comment créer des options de profil utilisateur ;
- appliquer les instructions de sélection d'une stratégie d'accès distant.

Stratégies d'accès distant



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

Introduction

L'autorisation d'accès réseau est accordée en fonction des propriétés de connexion de votre compte d'utilisateur et de stratégies d'accès distant. Ces stratégies définissent comment les connexions sont autorisées ou refusées. Chaque règle inclut au moins une condition, des paramètres de profil et un paramètre d'autorisation d'accès distant.

Pour pouvoir utiliser des stratégies d'accès distant, vous devez savoir comment ces stratégies sont appliquées. Les stratégies d'accès distant peuvent :

- fournir un accès personnalisé aux utilisateurs et aux groupes de votre entreprise ;
- fournir une souplesse d'octroi des autorisations d'accès distant et d'utilisation ;
- permettre d'affecter des paramètres à une connexion en fonction de l'utilisateur qui se connecte et des propriétés de la connexion.

Emplacement des stratégies d'accès distant

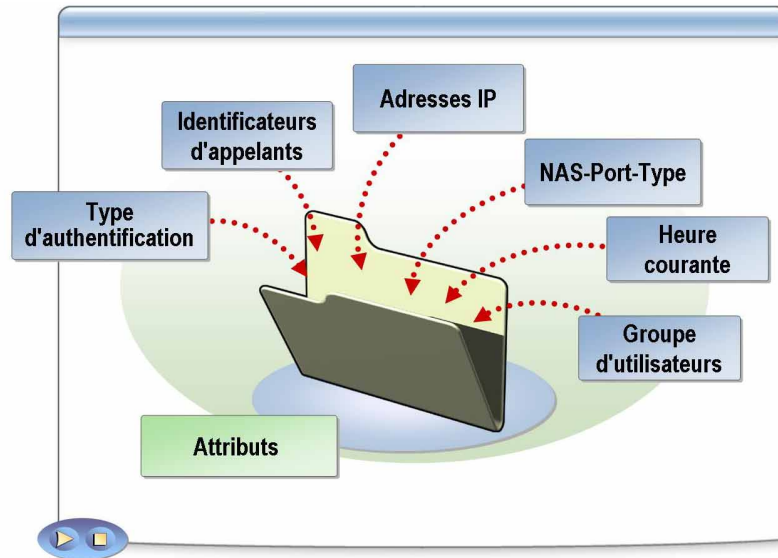
Windows Server 2003 stocke les stratégies d'accès distant sur le serveur d'accès réseau, et non dans Active Directory, pour que les stratégies puissent varier en fonction des capacités du serveur d'accès distant.

Remarque Vous pouvez centraliser les stratégies d'accès distant à l'aide du service IAS. Pour plus d'informations sur le service IAS, consultez le module 9, « Extension des fonctionnalités d'accès distant à l'aide du service IAS » du cours 2172, *Implémentation d'une infrastructure réseau Microsoft Windows 2000*.

Coopération avec Active Directory

Les trois composants d'une stratégie d'accès distant, qui coopèrent avec Active Directory pour fournir un accès sécurisé aux serveurs d'accès distant, sont les conditions, les autorisations et le profil de la stratégie.

Conditions d'une stratégie d'accès distant



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

Introduction

Les conditions d'une stratégie d'accès distant correspondent à une liste de paramètres, tels l'heure, les groupes d'utilisateurs, les identificateurs d'appelants ou les adresses IP (Internet Protocol), qui sont comparés aux paramètres du client qui se connecte au serveur. Le premier ensemble de conditions de la stratégie qui correspond aux paramètres de la demande de connexion entrante est traité pour déterminer les autorisations et la configuration de l'accès.

Attributs des conditions d'une stratégie d'accès distant

Les deux attributs de condition suivants sont les plus utilisés :

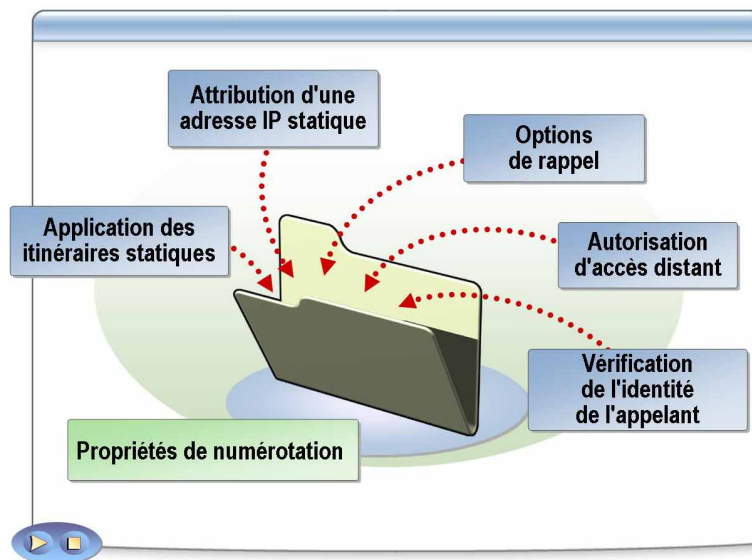
- **NAS-Port-Type** : cet attribut de condition vous permet de spécifier le type de connexion réseau tel que Ethernet, sans fil, modem, VPN, etc.
- **Windows-Groups** : vous pouvez utiliser cet attribut pour définir un groupe d'utilisateurs auquel vous voulez appliquer une stratégie. Vous pouvez, par exemple, combiner les attributs **NAS-Port-Type** et **Windows-Groups** pour appliquer une stratégie à tous les employés du service commercial, qui se connectent via un tunnel VPN.

Autres attributs de condition

Votre stratégie d'accès réseau peut vous amener à définir de nombreuses autres conditions. Utilisez le tableau d'attributs ci-dessous pour faire correspondre les demandes aux conditions.

Attribut	Description
Authentication-Type (Type-Authentification)	Définit le schéma d'authentification utilisé pour vérifier l'utilisateur.
Called-Station-Id (ID de la station appelée)	Définit le numéro de téléphone de la connexion d'accès à distance utilisée par l'utilisateur.
Calling-Station-Id (ID de station appelant)	Définit le numéro de téléphone de l'appelant ; par exemple, 555-****.
Client-Friendly-Name (Nom convivial du client)	Définit le nom convivial du client RADIUS ; par exemple, RASCL**.
Client-IP-Address (Adresse IP du client)	Définit l'adresse IP du client RADIUS.*.
Client-Vendor (Client-Fournisseur)	Définit le fabricant du système d'authentification du réseau ; par exemple, Microsoft, Cisco ou Shiva.
Day-And-Time-Restrictions (Restrictions jour et heure)	Définit l'heure ou le jour/la semaine pendant lesquels RAS (Remote Access Service) ne peut être utilisé. Par défaut, aucune autorisation n'est accordée.
Framed-Protocol (Protocole tramé)	Définit le protocole à utiliser ; par exemple PPP, SLIP (Serial Line Internet Protocol), X25 ou AppleTalk.
NAS-IP-Address (Adresse IP NAS)	Définit l'adresse IP du serveur NAS.
NAS-Identifiant (Identificateur NAS)	Définit une chaîne qui identifie le serveur qui envoie la demande ; par exemple, RADIUS_Server.
NAS-Port-Type (Type de port NAS)	Définit le port physique utilisé par le serveur NAS qui envoie la demande ; par exemple, Async (Modem), Sync (ligne T1), RNIS sync ou Virtuel (VPN).
Service-Type (Type de service)	Définit le type de service que demande l'utilisateur ; par exemple, Administrative-User, Callback-Login et Shell-User.
Tunnel-Type (Type de tunnel)	Définit le protocole de tunnel utilisé.
Windows-Groups (Groupes Windows)	Définit les groupes Windows auxquels appartient l'utilisateur ; par exemple, Administrateurs.

Propriétés de numérotation des comptes d'utilisateurs



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

Introduction

Le service Routage et accès distant et le service IAS de la famille Windows Server 2003 et sur Windows 2000 autorisent l'accès réseau en fonction des propriétés de numérotation des comptes d'utilisateurs et des stratégies d'accès distant.

L'autorisation d'accès via le paramètre d'autorisation des comptes d'utilisateurs ou le paramètre d'autorisation de la stratégie ne constitue que la première étape de l'acceptation de la connexion.

Dans la famille Windows Server 2003, vous pouvez configurer un attribut RADIUS pour ignorer les propriétés de numérotation des comptes d'utilisateurs et des comptes d'ordinateurs dans les propriétés de profil d'une stratégie d'accès distant. Pour prendre en charge plusieurs types de connexions que le service IAS authentifie et autorise, vous pouvez être amené à désactiver le traitement des propriétés de numérotation des comptes d'utilisateurs.

Paramètres d'accès distant

La tentative de connexion dépend des paramètres des propriétés de numérotation du compte d'utilisateur et des paramètres des propriétés du profil de la stratégie. Si la tentative de connexion ne correspond pas aux paramètres du compte d'utilisateur ou des propriétés du profil de la stratégie, la connexion échoue. Vous pouvez définir les autorisations d'accès distant des deux manières suivantes :

- **Définition des autorisations d'accès distant d'un compte d'utilisateur**

Vous pouvez accorder ou refuser les autorisations d'accès distant pour chaque utilisateur. L'autorisation d'accès distant d'un utilisateur remplace celle de la stratégie. Lorsque l'autorisation d'accès distant dans un compte d'utilisateur est définie par le paramètre **Contrôler l'accès via la Stratégie d'accès distant**, l'autorisation d'accès distant de la stratégie détermine si l'utilisateur peut accéder au réseau.

- **Définition des autorisations d'accès distant d'une stratégie**

Si toutes les conditions d'une stratégie d'accès distant sont respectées, l'autorisation d'accès distant est acceptée ou refusée. Vous pouvez utiliser l'option **Accorder l'autorisation d'accès distant** ou **Refuser l'autorisation d'accès distant** pour définir l'autorisation d'accès distant d'une stratégie.

Remarque Les paramètres de profil définissent un ensemble de restrictions de connexion. Le cas échéant, les restrictions de connexion des comptes d'utilisateurs remplacent les restrictions de connexion des profils des stratégies d'accès distant.

Autres propriétés de numérotation des comptes d'utilisateurs

Dans la famille Windows Server 2003, le compte d'utilisateur d'un serveur autonome ou d'un serveur qui exécute Active Directory contient un groupe de propriétés de numérotation, qui est utilisé pour autoriser ou refuser une tentative de connexion d'un utilisateur. Sur un serveur autonome, vous pouvez définir les propriétés de numérotation dans l'onglet **Appel entrant** du compte d'utilisateur dans la console Utilisateurs et groupes locaux. Sur un serveur qui exécute Active Directory, vous pouvez définir les propriétés de numérotation dans l'onglet **Appel entrant** du compte d'utilisateur dans la console Utilisateurs et ordinateurs Active Directory.

Les autres propriétés de numérotation des comptes d'utilisateurs sont les suivantes :

- **Vérifier l'identité de l'appelant**

Si cette propriété est active, le serveur vérifie le numéro de téléphone de l'appelant. Si le numéro de téléphone de l'appelant ne correspond pas à celui défini, la connexion est refusée.

- **Options de rappel**

Si cette propriété est active, le serveur répond à l'appelant au cours de la procédure de connexion. Le numéro de téléphone qu'utilise le serveur est défini par l'appelant ou par l'administrateur du réseau.

- **Attribution d'une adresse IP statique**

Utilisez cette propriété pour affecter une adresse IP à un utilisateur lorsque la connexion est établie.

Attribut Ignore-User-Dialin-Properties**■ Appliquer les itinéraires statiques**

Utilisez cette propriété pour définir une série d'itinéraires IP fixes qui sont ajoutés à la table de routage du serveur qui exécute le service Routage et accès distant lorsqu'une connexion est établie. Ce paramètre est destiné aux comptes d'utilisateurs qu'un routeur, qui exécute la famille Windows Server 2003, utilise pour le routage à la demande.

Vous pouvez utiliser le service IAS pour activer le traitement des propriétés de numérotation des comptes d'utilisateurs et des comptes d'ordinateurs dans certains scénarios (appel entrant, par exemple) et les désactiver dans d'autres scénarios (commutateur sans fil et d'authentification).

L'attribut **Ignore-User-Dialin-Properties** est défini comme suit :

- Pour activer le traitement des propriétés de numérotation, supprimez l'attribut **Ignore-User-Dialin-Properties** ou affectez-lui la valeur **Faux**. Pour une stratégie d'accès distant conçue pour les connexions d'appels entrants, par exemple, aucune opération de configuration supplémentaire n'est nécessaire.
- Pour désactiver le traitement des propriétés de numérotation, affectez la valeur **Vrai** à l'attribut **Ignore-User-Dialin-Properties**. Définissez cette configuration, par exemple, pour la stratégie d'accès distant utilisée pour les connexions sans fil et les connexions d'authentification commutées. Lorsque les propriétés de numérotation du compte d'utilisateur sont ignorées, l'autorisation d'accès distant est déterminée par le paramètre de la stratégie d'accès distant.

Options de profil utilisateur

Composant	Définit...
Authentification	Les protocoles d'authentification à utiliser
Cryptage	Le niveau de cryptage MPPE à accepter
Contraintes pour les appels entrants	Les contraintes que vous souhaitez appliquer dans la stratégie
IP	L'adresse IP affectée au client et les filtres appliqués à la connexion
Liaisons multiples	Les connexions multiliaisons autorisées dans lesquelles plusieurs ports peuvent être combinés pour la connexion
Paramètres avancés	D'autres attributs de connexion (RADIUS ou spécifique au fabricant) qui peuvent être envoyés au serveur d'accès réseau auquel le client est connecté

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

Introduction

Vous pouvez utiliser une stratégie d'accès distant pour créer un profil d'appel entrant et définir l'accès en fonction de l'appartenance aux groupes Windows 2000, de l'heure, du jour et du type de connexion. Vous pouvez également définir les paramètres d'options telles que la durée maximale des sessions, les conditions d'authentification et les stratégies BAP (Bandwidth Allocation Protocol).

Définition de profils

Chaque stratégie inclut un profil de paramètres, tels les protocoles d'authentification et de cryptage, qui est appliqué à la connexion. Les paramètres du profil sont appliqués à la connexion immédiatement et peuvent rejeter la connexion.

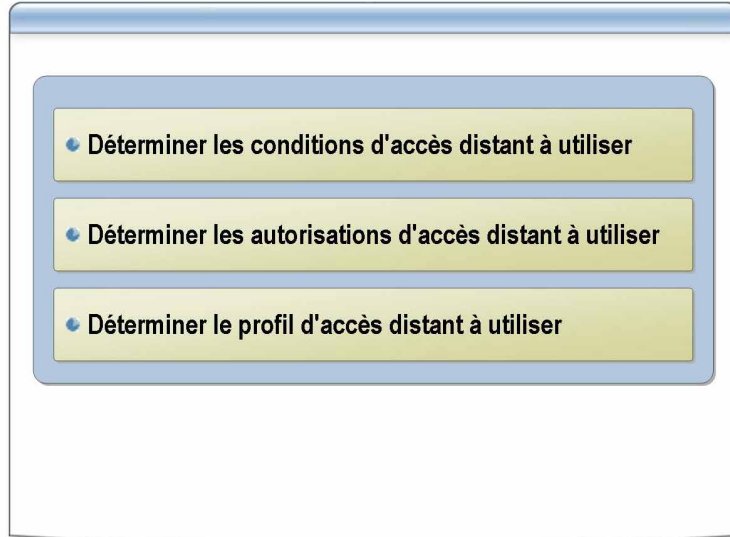
Le profil contient également le niveau de cryptage, la méthode d'authentification, les connexions multiliaisons autorisées, l'affectation d'adresse IP et d'autres contraintes de connexion. À des fins de sécurité, vous devez prêter une attention particulière à la méthode d'authentification et au paramètre de cryptage et sélectionner les options les plus sûres que peut prendre en charge votre entreprise.

Si, par exemple, les paramètres du profil d'une connexion indiquent que l'utilisateur peut uniquement se connecter pendant 30 minutes, l'utilisateur est déconnecté du serveur d'accès distant après 30 minutes.

Options de profil d'appel entrant Le tableau suivant répertorie les options d'un profil d'appel entrant.

Composant	Définit
Authentification	Les protocoles d'authentification à utiliser. Vous disposez des protocoles d'authentification PPP (MS-CHAP v2, PEAP, etc.) ou vous pouvez choisir EAP et les divers types EAP.
Cryptage	Le niveau de cryptage MPPE à accepter. Vous disposez d'un éventail de niveaux allant d'aucun cryptage à un cryptage 128 bits. Cet onglet contient la liste des niveaux de cryptage pris en charge par le service Routage et accès distant. Si vous utilisez un serveur d'accès réseau d'un autre fabricant, vérifiez qu'il prend en charge les niveaux que vous sélectionnez dans cet onglet.
Contraintes pour les appels entrants	Les contraintes à appliquer dans la stratégie, telles les restrictions d'heure et de jour, la durée d'inactivité de la connexion avant la déconnexion, la durée de la connexion avant la déconnexion, etc.
IP	L'adresse IP affectée au client et les filtres appliqués à la connexion. Si le serveur d'accès réseau exécute le service Routage et accès distant, vous pouvez définir des filtres d'entrée et de sortie pour les appliquer à la connexion. Vous pouvez, par exemple, appliquer le filtre qui permet uniquement le trafic FTP (File Transfer Protocol) sur la connexion.
Liaisons multiples	Les connexions multiliasons autorisées dans lesquelles plusieurs ports peuvent être combinés pour la connexion. Cette option permet également d'indiquer si les paramètres BAP sont utilisés pour contrôler l'utilisation des paramètres de liaison multiple de la connexion.
Paramètres avancés	D'autres attributs de connexion (RADIUS ou spécifique au fabricant) qui peuvent être envoyés au serveur d'accès réseau auquel le client est connecté.

Instructions de sélection d'un plan d'accès distant



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

Introduction

Avant de sélectionner une stratégie d'accès distant, vous devez déterminer les conditions, les autorisations et les paramètres de profil à utiliser pour activer la connexion, l'authentification et la sécurité de la connexion.

Détermination des conditions et des paramètres d'accès distant

Lorsque vous déterminez les conditions et les paramètres d'accès distant, vous devez tenir compte des éléments suivants :

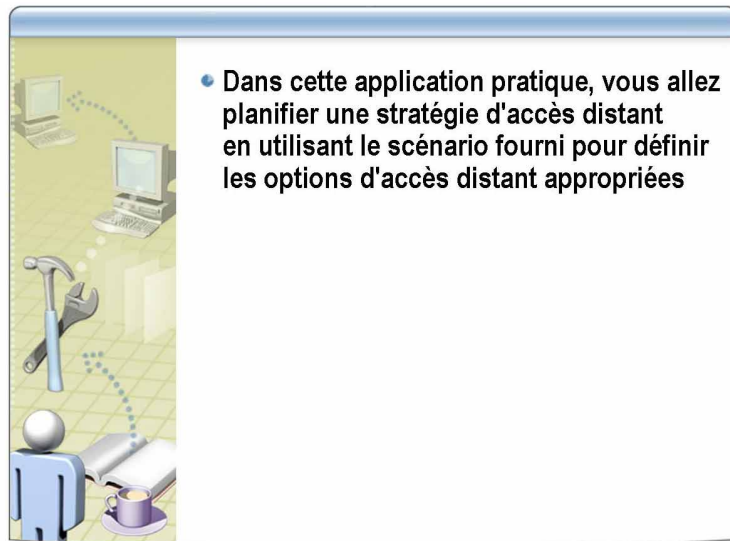
- Utilisez les conditions d'un ou de plusieurs attributs qui sont comparés aux paramètres de la tentative de connexion. S'il existe plusieurs conditions, elles doivent toutes correspondre aux paramètres de la tentative de connexion pour que cette dernière corresponde à la stratégie. En conséquence, vous devez sélectionner des attributs de la liste et définir les conditions à faire correspondre pour que le paramètre de la stratégie soit appliqué.
- Les autorisations d'un compte d'utilisateur et celles d'une stratégie indiquent si l'accès distant est refusé ou accordé aux utilisateurs qui correspondent aux conditions associées à une stratégie. Si le compte d'utilisateur autorise l'accès et que les conditions correspondent, les paramètres du profil sont appliqués à la connexion.

Détermination des stratégies des profils d'accès distant

Lorsque vous déterminez les options à implémenter pour la stratégie du profil d'accès distant, tenez compte des recommandations suivantes :

- Utilisez la méthode d'authentification la plus efficace pour l'accès distant.
N'autorisez pas les connexions qui utilisent d'anciens protocoles d'authentification, tels PAP, SPAP (Shiva Password Authentication Protocol) et CHAP, et restreignez l'accès aux connexions qui utilisent MS-CHAP v2 ou EAP.
- Utilisez EAP avec un type EAP de carte à puce ou autre certificat.
L'utilisation d'une carte à puce pour stocker le certificat constitue la méthode d'authentification la plus sûre pour les clients distants. Toutefois, cette méthode nécessite qu'une procédure de certificat existe pour que les utilisateurs et les ordinateurs puissent obtenir leurs certificats de clé publique, ainsi que des matériels supplémentaires pour les lecteurs de carte à puce.
- Utilisez PEAP avec des certificats ou avec MS-CHAP v2 pour les clients d'accès sans fil.
S'il n'est pas possible de mettre en œuvre une procédure pour les certificats clients (les certificats sont toujours nécessaires pour les serveurs d'authentification), PEAP/MS-CHAP v2 est pris en charge sur les clients Microsoft Windows XP Service Pack 1 ou les autres clients sur lesquels Microsoft 802.1x Authentication Client (téléchargeable gratuitement) est installé.
- Utilisez le niveau de cryptage de données le plus élevé pour l'accès distant.
Le niveau de cryptage possible peut être déterminé par les systèmes d'exploitation dont disposent les utilisateurs sur leurs ordinateurs.
- Utilisez des stratégies d'accès distant qui limitent l'accès distant uniquement aux utilisateurs ou aux groupes appropriés et qui répondent aux normes de sécurité de votre réseau.
Dans la mesure du possible, appliquez des stratégies d'accès distant à des groupes plutôt qu'à des utilisateurs individuels pour faciliter l'administration des stratégies.

Application pratique : Détermination d'un plan de stratégie d'accès distant



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

- Introduction** Dans cette application pratique, vous allez définir un plan de stratégie d'accès distant en utilisant le scénario fourni pour définir les options d'accès à distance appropriées.
- Objectif** L'objectif de cette application pratique consiste à déterminer un plan de stratégie d'accès distant.
- Instructions**
1. Lisez le scénario.
 2. Préparez-vous à discuter des problèmes associés à cette tâche après l'application pratique.
- Scénario**
- Environ trois cents sous-traitants de Trey Research travaillent sur un nouveau projet de trois ans qu'a remporté la société. La société impose aux sous-traitants de travailler en dehors de leurs propres bureaux externes et doivent pouvoir télécharger les données techniques sur le serveur FTP de son intranet. Les informations seront ensuite entrées dans une base de données pour pouvoir être consultées par le superviseur des sous-traitants.
- Auparavant, les sous-traitants disposaient de leurs propres comptes d'utilisateurs et autorisations pour accéder à distance au réseau de la société via une connexion VPN. Cela posait toutefois des problèmes car des utilisateurs restaient connectés très longtemps et accédaient à d'autres services tels qu'aux serveurs proxy Web de la société.
- Pour ce projet, la société veut limiter les sous-traitants au téléchargement amont ou aval des données sur le serveur FTP de son intranet et restreindre la durée des connexions à 30 minutes. Cette restriction doit être appliquée sans affecter les connexions à distance des autres employés à temps complet.
- La société utilise une infrastructure Active Directory et le service Routage et accès distant de Windows Server 2003 comme serveur d'accès réseau VPN.

Application pratique

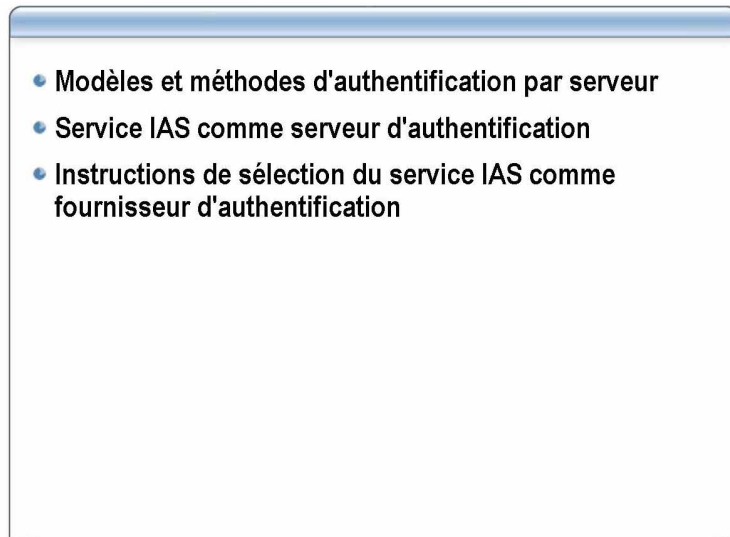
Quel plan définissez-vous pour résoudre le problème des sous-traitants en utilisant une stratégie d'accès distant ?

Planifiez un nouveau groupe pour les sous-traitants et appelez-le Remote Contractors. Supprimez les sous-traitants du groupe actuellement utilisé pour fournir un accès distant aux employés et ajoutez au nouveau groupe les comptes d'utilisateurs des sous-traitants qui accéderont au serveur FTP.

Planifiez une nouvelle stratégie d'accès distant qui fournit une autorisation d'accès distant à la condition que Windows-Groups corresponde au groupe Remote Contractors et que le type de port NAS (NAS-Port-Type) soit « Virtuel (VPN) ».

Planifiez une modification de profil pour laquelle la durée de connexion est de 30 minutes. Pour les filtres d'entrée et de sortie IP à changer, autorisez uniquement l'échange de paquets FTP avec le serveur FTP.

Leçon : Sélection d'une méthode d'authentification de l'accès réseau



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

Introduction

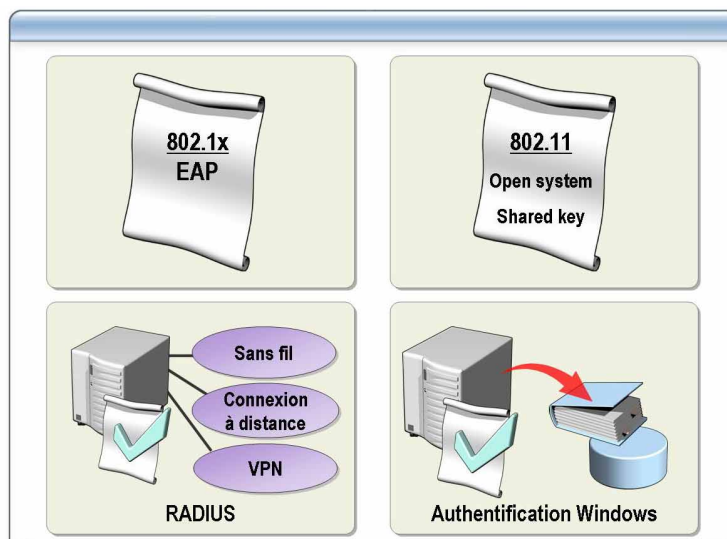
Vous pouvez intégrer le service IAS à votre stratégie d'accès réseau pour prendre en charge plusieurs types de connexions et permettre au serveur proxy RADIUS d'authentifier les utilisateurs distants et les autoriser à se connecter.

Objectifs de la leçon

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

- identifier les modèles et les méthodes d'authentification par serveur ;
- expliquer comment utiliser le service IAS comme serveur d'authentification ;
- appliquer les instructions de sélection du service IAS comme fournisseur d'authentification.

Modèles et méthodes d'authentification par serveur



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

Introduction

Si votre stratégie d'accès réseau nécessite de centraliser l'authentification, vous devez sélectionner un modèle d'authentification qui limite au maximum la charge de travail. Vous avez le choix entre plusieurs modèles d'authentification.

Authentification Windows

Bien que l'authentification Windows soit simple à configurer et à utiliser, elle est intégrée à la famille Windows Server 2003 et peut donc générer des îlots d'authentification d'accès réseau qui nécessitent chacun une administration et une configuration de stratégie distinctes.

Un serveur Windows Server 2003 qui exécute le service Routage et accès distant peut utiliser une base de données de comptes locaux ou une base de données de comptes de domaine pour authentifier l'accès distant ou les informations de connexion d'accès à la demande. Une base de données de comptes de domaine peut correspondre à une base de données Active Directory ou à une base de données de comptes de domaine Windows NT 4.0. Le serveur consigne les informations d'authentification dans des fichiers journaux configurés dans les propriétés du dossier Connexion par accès distant.

Authentification par le serveur RADIUS

Dans de nombreux environnements, RADIUS est utilisé pour l'authentification. Le serveur RADIUS vérifie les informations d'authentification de l'accès à distance dans les comptes d'utilisateurs et journalise les événements de gestion de compte d'accès distant.

L'utilisation de RADIUS offre une excellente méthode pour centraliser la solution d'authentification. En effet, vous pouvez non seulement centraliser l'authentification et les stratégies de tous les serveurs d'accès réseau traditionnels (tels les serveurs qui exécutent le service Routage et accès distant), mais également fournir une authentification et des stratégies pour d'autres types de périphériques et de serveurs d'accès réseau (serveurs VPN, points d'accès sans fil, commutateurs, etc).

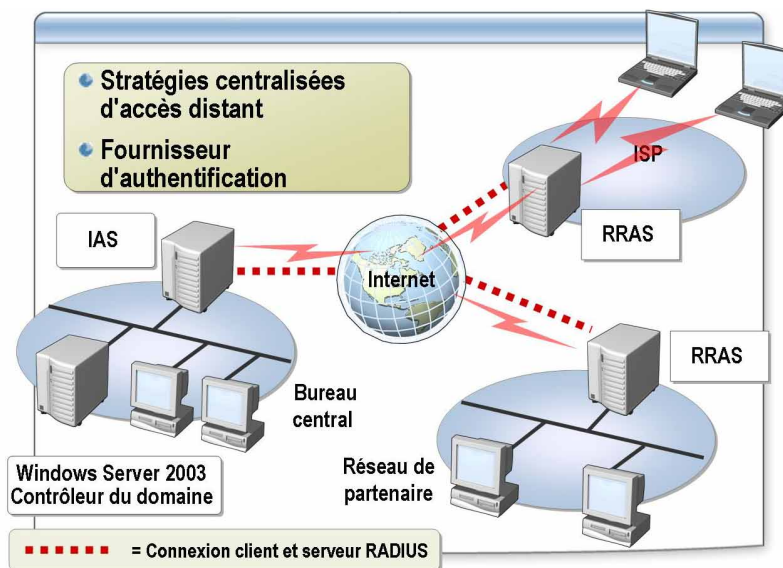
Les points d'accès sans fil utilisent différents mécanismes d'authentification. Ils peuvent utiliser l'authentification définie dans la spécification 802.11 (non recommandé) ou 802.1x avec un serveur RADIUS.

**Méthodes
d'authentification 802.11**

Le tableau ci-dessous répertorie et décrit les méthodes d'authentification de la spécification 802.11.

Méthode d'authentification	Description
Authentification 802.11	<p>L'authentification en système ouvert ne fournit pas de fonction d'authentification, mais uniquement des fonctions d'identification en utilisant l'adresse MAC (Media Access Control) de la carte sans fil. Utilisez l'authentification en système ouvert lorsque aucune authentification n'est nécessaire. L'authentification en système ouvert est l'algorithme d'authentification par défaut de l'authentification 802.11.</p> <p>L'authentification par clé partagée vérifie qu'un poste qui lance l'authentification a connaissance d'une clé secrète partagée. Ce type d'authentification est similaire à l'authentification par clé prépartagée de IPSec. La norme 802.11 suppose que la clé secrète partagée est envoyée aux clients d'accès sans fil participant via un canal sécurisé indépendant de IEEE 802.11. Dans la pratique, la clé secrète est tapée sur le point d'accès sans fil et sur le client d'accès sans fil.</p>
802.1x	<p>802.1x utilise EAP pour communiquer les informations d'authentification entre les clients d'accès sans fil et les points d'accès sans fil. Le point d'accès sans fil est ensuite configuré pour communiquer avec un serveur RADIUS, les messages EAP étant envoyés entre le client d'accès sans fil et le serveur RADIUS.</p> <p>Cette forme d'authentification des clients d'accès sans fil est la plus sûre parce qu'elle fait appel à une solution souple et au protocole EAP et qu'elle s'adapte plus aisément que les solutions 802.11.</p>

Service IAS comme serveur d'authentification



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

Introduction

Si votre stratégie d'accès réseau nécessite de prendre en charge plusieurs types de connexions ou que vous disposez de serveurs d'accès différents (à distance, VPN, sans fil) qui peuvent tirer parti de l'administration centralisée, utilisez le service IAS comme serveur d'authentification.

Pour prendre en charge plusieurs types de connexions, vous devez désactiver le traitement des propriétés de numérotation des comptes d'utilisateurs. Dans la famille Windows Server 2003, vous pouvez configurer un attribut RADIUS pour ignorer les propriétés de numérotation des comptes d'utilisateurs et des comptes d'ordinateurs dans les propriétés de profil d'une stratégie d'accès distant.

Utilisation du service IAS comme serveur proxy

Vous pouvez utiliser le service IAS comme proxy RADIUS pour router les messages RADIUS entre les clients RADIUS (serveurs d'accès) et les serveurs RADIUS qui authentifient les utilisateurs, leur accordent les autorisations et exécutent les opérations de gestion de comptes associées à la tentative de connexion. Le serveur proxy est configuré pour identifier le serveur RADIUS auquel une demande d'authentification spécifique doit être envoyée.

Lorsque IAS est utilisé comme proxy RADIUS, il fait office de point de commutation ou de routage central par lequel transitent les messages de comptabilité et d'accès RADIUS. IAS enregistre, dans un journal de comptabilité, les informations sur les messages envoyés.

Vous pouvez utiliser IAS comme proxy RADIUS pour :

- authentifier et autoriser les comptes d'utilisateurs qui ne sont pas membres du domaine du serveur IAS ou membres d'un autre domaine qui applique une approbation directionnelle avec le domaine IAS ;
- authentifier et autoriser les utilisateurs en utilisant une base de données qui n'est pas une base de données de comptes Windows ;
- traiter un grand nombre de demandes de connexion ;
- appliquer l'authentification et les autorisations RADIUS aux fournisseurs de services externalisés et réduire les tâches de configuration du pare-feu de l'intranet.

Positionnement d'un serveur IAS

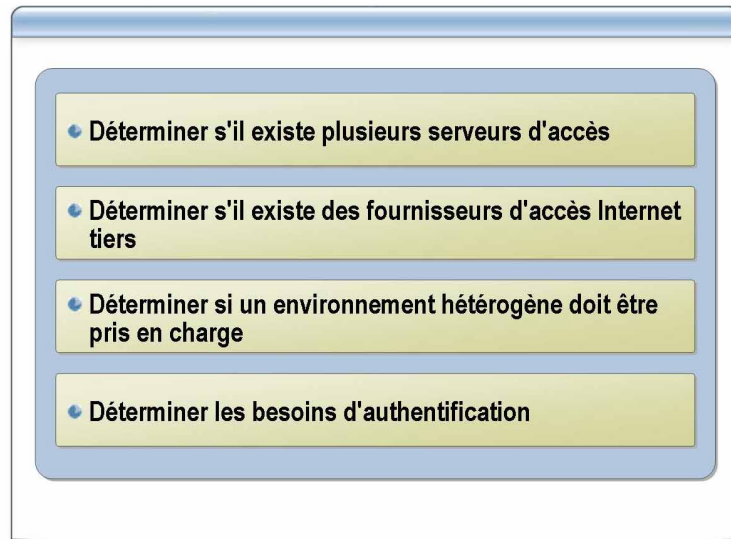
Vous devez d'abord déterminer le domaine dont le serveur IAS fait partie. Pour les environnements à plusieurs domaines, un serveur IAS peut authentifier les informations d'identification des comptes d'utilisateurs du domaine dont il est membre et de tous les domaines qui font confiance au domaine. Toutefois, pour lire les propriétés de numérotation des comptes d'utilisateurs, vous devez ajouter le compte d'ordinateur du serveur IAS aux groupes de serveurs d'accès distant et IAS de chaque domaine.

Recommandations relatives au positionnement des serveurs IAS et RADIUS

Tenez compte des recommandations suivantes relatives au positionnement des serveurs IAS et RADIUS :

- Vous devez placer le serveur IAS dans le domaine contenant le plus grand nombre de comptes d'utilisateurs et de comptes d'ordinateurs à authentifier.
- Vous devez placer un serveur RADIUS dans un sous-réseau filtré pour ne pas exposer les comptes d'utilisateurs et les stratégies à l'extérieur de votre réseau privé.
- Utilisez toujours aux moins deux serveurs IAS pour protéger l'authentification et la comptabilité basées sur RADIUS : un serveur qui correspond au serveur RADIUS principal et un autre serveur qui fait office de serveur de secours. Les serveurs d'accès sont configurés pour les serveurs IAS et le commutateur pour utiliser le serveur IAS de secours en cas de non-disponibilité du serveur IAS principal.

Instructions de sélection du service IAS comme fournisseur d'authentification



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

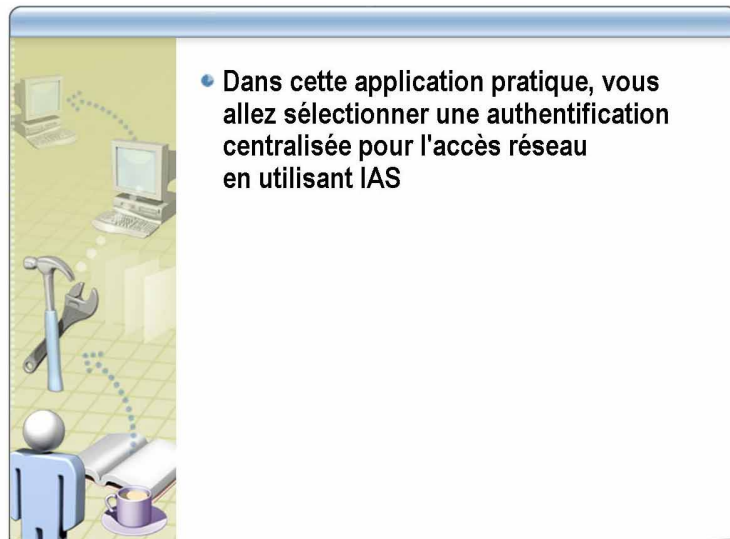
Introduction

Avant de sélectionner le service IAS comme fournisseur d'authentification, vous devez tenir compte des instructions suivantes. Votre infrastructure d'accès réseau et vos besoins d'administration peuvent vous amener à choisir IAS comme serveur RADIUS ou serveur proxy.

Suivez les instructions ci-dessous pour sélectionner IAS comme fournisseur d'authentification :

- Déterminez s'il existe plusieurs serveurs d'accès qui peuvent tirer parti d'une approche centralisée.
- Déterminez si vous disposez, ou disposerez, de fournisseurs d'accès Internet tiers qui pourraient authentifier les utilisateurs dans votre infrastructure RADIUS.
- Déterminez s'il existe plusieurs serveurs d'accès qui peuvent tirer parti d'une stratégie et d'une administration centralisées.
- Si vous disposez d'un environnement hétérogène avec des impératifs d'autorisation et de stratégie, déterminez si RADIUS peut être la seule solution qui réponde à tous ces impératifs.
- Déterminez si vous devez authentifier les utilisateurs en utilisant une base de données de comptes d'utilisateurs de domaine non autorisé ou d'une base de données d'utilisateurs non-Windows.

Application pratique : Sélection de l'authentification centralisée de l'accès réseau à l'aide du service IAS



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

Introduction

Dans cette application pratique, vous allez déterminer si le service IAS correspond à la solution appropriée d'un scénario donné.

Objectif

L'objectif de cette application pratique consiste à sélectionner une authentification centralisée pour l'accès réseau en utilisant IAS.

Instructions

1. Lisez le scénario.
2. Préparez-vous à discuter des problèmes associés à cette tâche après l'application pratique.

Scénario

La société Phone Company utilise plusieurs serveurs d'accès réseau pour répondre à ses besoins d'accès distant. Certains de ces serveurs sont des ordinateurs Windows Server 2003 qui exécutent le service Routage et accès distant et les autres serveurs sont d'anciens serveurs d'autres fabricants. Actuellement, tous les serveurs sont gérés séparément.

La société envisage d'installer un réseau sans fil et le service informatique étudie les options d'authentification disponibles. Les données initiales indiquent qu'il existera au début des milliers de clients d'accès sans fil dont le nombre augmentera probablement de plusieurs centaines chaque année.

Application pratique

Quelle est la meilleure méthode de planification d'une stratégie d'authentification à long terme pour Phone Company ?

Une solution RADIUS serait probablement la meilleure stratégie d'authentification à long terme.

Citez quelques avantages de cette stratégie.

Toutes les tâches d'authentification et de stratégie pourraient être exécutées dans un emplacement central pour faciliter l'administration. Cette solution est beaucoup mieux adaptée aux accès sans fil, car une stratégie d'authentification par clé partagée sans fil nécessite de distribuer la clé partagée sur chaque périphérique sans fil.

Cette solution permet d'authentifier les clients d'accès sans fil avec diverses méthodes EAP, ce qui offre une flexibilité considérable au personnel informatique en terme de protocoles d'authentification.

Citez quelques inconvénients de cette stratégie.

Certains serveurs d'accès réseau peuvent ne pas pouvoir utiliser l'authentification RADIUS. Dans ce cas, vous devez les mettre à jour ou les remplacer.

Le personnel informatique doit savoir planifier, tester, implémenter et effectuer la maintenance d'une infrastructure RADIUS. Cela peut demander du temps et une formation supplémentaire.

Si la société dispose de clients d'accès sans fil dont le système d'exploitation ne prend pas en charge le protocole 802.1x, ces clients ne pourront pas participer à la stratégie d'authentification.

Leçon : Planification d'une stratégie d'accès réseau

- Stratégie de connexion d'accès réseau
- Méthodes d'authentification basées sur la sécurité
- Plans de stratégie d'accès distant
- Instructions de planification d'une stratégie d'accès réseau

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

Introduction

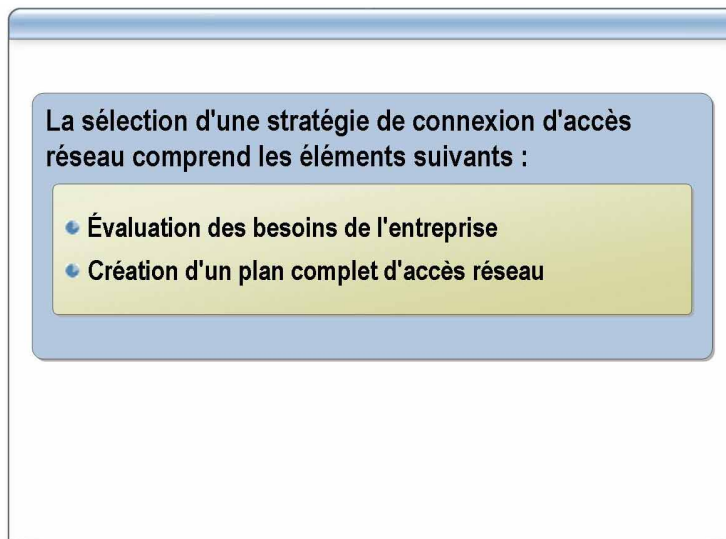
Cette leçon combine des informations des trois leçons précédentes. Vous allez apprendre à intégrer la sélection d'une stratégie d'accès réseau, d'une méthode d'authentification et d'une stratégie d'accès distant.

Objectifs de la leçon

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

- déterminer une stratégie de connexion d'accès réseau ;
- déterminer des méthodes d'authentification basées sur la sécurité ;
- définir des plans de stratégie d'accès distant ;
- appliquer les instructions de planification d'une stratégie d'accès réseau.

Stratégie de connexion d'accès réseau



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

Introduction

La sélection d'une stratégie d'accès réseau nécessite de déterminer non seulement les besoins des clients et de l'infrastructure, mais également la méthode de connexion. Lorsque vous sélectionnez la stratégie, tenez compte des recommandations suivantes :

Évaluation des besoins de l'entreprise

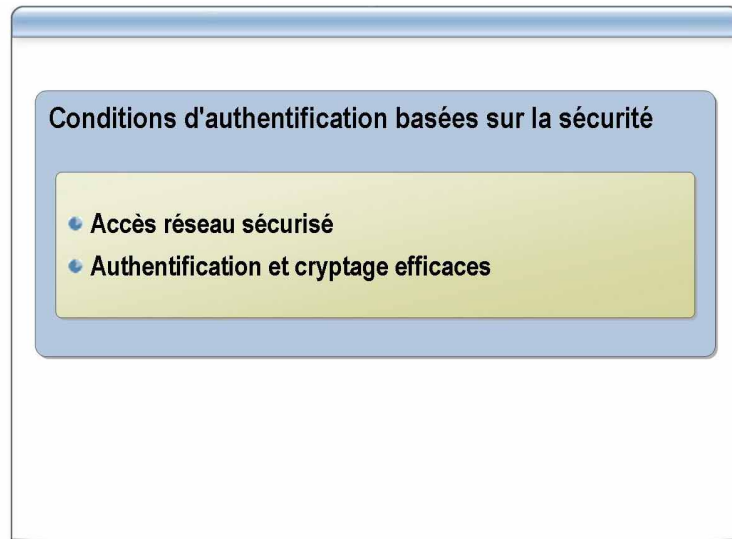
Vous devez évaluer les besoins de l'entreprise pour pouvoir planifier correctement votre stratégie d'accès réseau. Tenez compte des points suivants :

- Bande passante du réseau
Pour les éléments nécessitant une grande bande passante et un haut niveau de disponibilité (tels les serveurs ou les stations de travail haut de gamme), vous devez utiliser une connexion LAN et planifier une bande passante suffisante pour tenir compte de l'évolution future du réseau (10 Mbps, par exemple, peuvent être suffisants pour répondre aux besoins actuels de l'entreprise, mais pas à ses besoins futurs).
- Besoins de connectivité
Il est recommandé d'utiliser des connexions VPN et non des connexions d'accès réseau à distance pour les clients. La plupart des entreprises considèrent qu'une solution VPN qui utilise leur connectivité Internet est plus simple à administrer et plus évolutive.
- Besoins de sécurité
Il est important de déterminer le niveau de sécurité de la connexion. Vous devez également déterminer la méthode de connexion qui répond le mieux aux besoins de l'entreprise.

Création d'un plan complet d'accès réseau

Après avoir défini les besoins de bande passante, de connectivité et de sécurité du réseau, vous devez sélectionner une stratégie d'accès réseau qui répond à ces besoins. Dans le cadre de cette stratégie, vous pouvez également déterminer si vous avez besoin d'une stratégie d'authentification intégrée.

Méthodes d'authentification basées sur la sécurité



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

Introduction

Une méthode d'authentification centralisée peut faciliter l'administration de l'accès réseau. Le service IAS permet de planifier une stratégie complète d'authentification et de cryptage simple à administrer. Vous pouvez suivre plusieurs recommandations pour sélectionner une méthode d'authentification basée sur la sécurité.

Accès réseau sécurisé

Il est important de protéger le réseau contre les accès non autorisés. Vous pouvez disposer d'un grand nombre de serveurs d'accès réseau différents (connexion à distance, VPN, point d'accès sans fil, commutateurs d'authentification, etc.). Dans ce cas, vous pouvez centraliser les stratégies d'authentification en utilisant RADIUS.

Le service IAS s'intègre à la console MMC (Microsoft Management Console) et à Active Directory pour fournir un seul annuaire pour valider et administrer toutes les demandes d'accès pour les données d'applications ou les services. Cette intégration permet de consolider le contrôle d'accès et la stratégie d'authentification dans un référentiel administré, répliqué et sécurisé de manière centralisée.

Authentification et cryptage efficaces

Microsoft Windows Server 2003 fournit l'infrastructure d'authentification et de cryptage qui protège les connexions.

Du fait que Microsoft prend en charge les normes VPN telles que L2TP/IPSec et l'authentification des cartes à puce, les entreprises ont accès au cryptage, à l'authentification et à l'interopérabilité qui répondent le mieux à leurs besoins de sécurité VPN. En outre, du fait que Microsoft prend en charge l'ensemble des normes des extensions de sécurité IPSec, les entreprises peuvent crypter efficacement l'ensemble du trafic du réseau sans avoir à apporter des modifications fastidieuses au niveau des applications, des serveurs ou des matériels réseau déployés.

Outre le cryptage efficace, Windows Server 2003 peut répondre aux besoins d'authentification via sa prise en charge du protocole d'authentification IEEE 802.1x. Cette prise en charge supplémentaire permet aux clients et aux serveurs du réseau de s'authentifier mutuellement en utilisant des certificats numériques. Le protocole 802.1x fournit le contrôle au niveau du port qui peut empêcher des intrus de se connecter au réseau et d'effectuer des opérations malveillantes.

Si votre entreprise veut créer un système d'authentification intégré qui authentifie efficacement les utilisateurs par rapport à un seul annuaire, indépendamment de la méthode ou du périphérique d'accès utilisé, vous pouvez utiliser le service IAS Windows Server 2003. Ce service RADIUS standard intégré fonctionne avec les périphériques d'accès réseau d'une multitude de constructeurs.

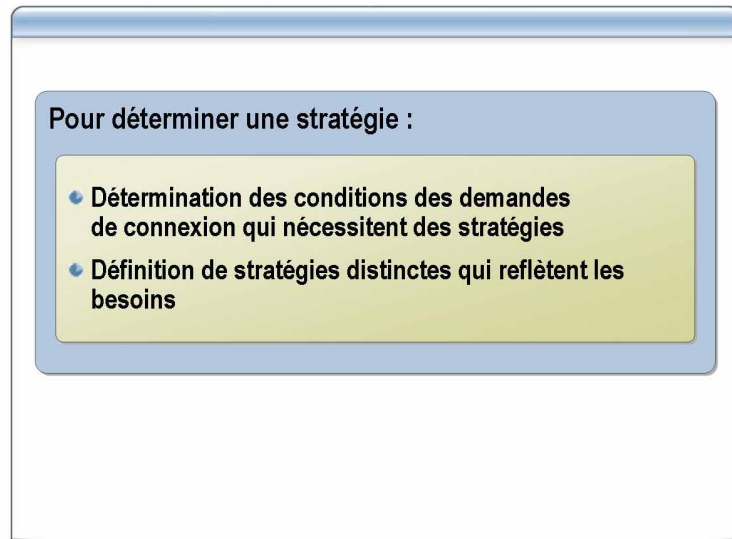
Vous pouvez tirer parti des technologies et des produits Microsoft pour sécuriser les connexions Internet des manières suivantes :

- Sécurisation de la messagerie
- Authentification plus efficace des utilisateurs
- Accès VPN et LAN sans fil vers les réseaux d'entreprise

Vous pouvez contrôler toutes ces solutions via une interface d'administration commune et les administrer en utilisant des stratégies Active Directory. Cette stratégie permet d'appliquer les stratégies de manière cohérente et complète à toutes les demandes d'accès, d'où qu'elles viennent.

Vous pouvez même envisager de mettre en œuvre une solution biométrique pour remplacer les codes personnels pour accéder aux informations des cartes à puce.

Plans de stratégie d'accès distant



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

Introduction

La sélection d'un plan d'accès distant nécessite de déterminer les besoins de l'ensemble de vos méthodes de connexion, groupes d'utilisateurs ou autres conditions de stratégie, puis d'intégrer ces besoins aux stratégies d'accès distant. Ces stratégies d'accès distant peuvent être définies sur un serveur qui exécute le service Routage et accès distant ou sur un serveur IAS (RADIUS), en fonction de la stratégie du fournisseur d'authentification.

Détermination des conditions des demandes de connexion qui nécessitent des stratégies

Chaque méthode d'accès réseau peut avoir des caractéristiques différentes. Vous pouvez, par exemple, utiliser une stratégie différente pour les clients LAN qui s'authentifient auprès d'un commutateur et une autre stratégie pour les clients d'accès sans fil qui s'authentifient via un point d'accès sans fil. Il peut également exister une autre stratégie pour les clients VPN qui s'authentifient via un serveur qui exécute le service Routage et accès distant.

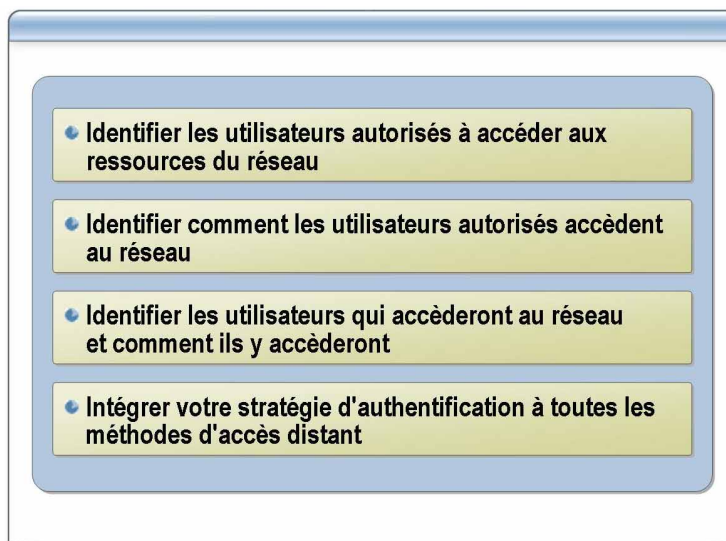
En outre, vous pouvez avoir d'autres impératifs qui nécessitent d'autres conditions de stratégie pour certains groupes d'utilisateurs, heures, jours, etc., par exemple.

Pour chaque stratégie que vous définissez, vous pouvez spécifier des paramètres différents qui reflètent les caractéristiques spécifiques d'une demande de connexion qui correspond à une condition de stratégie donnée.

Définition de stratégies distinctes qui reflètent les besoins

Si vous déterminez qu'il existe des besoins de stratégies différents, vous devez définir les stratégies d'accès distant de chacun des besoins. Cette détermination permet de garantir que les besoins définis seront satisfaits par les stratégies pour chacune des conditions de demande de connexion.

Instructions de planification d'une stratégie d'accès réseau



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

Introduction

Les instructions suivantes fournissent les éléments de décision dont vous devez tenir compte lors de la planification de la stratégie d'accès réseau.

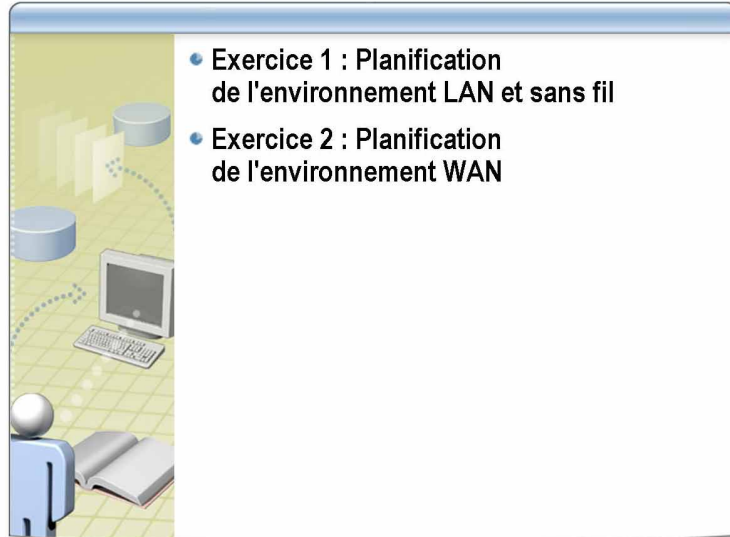
- Identifiez les utilisateurs autorisés à accéder aux ressources du réseau. Vous devez d'abord identifier les ressources qui seront accessibles et les utilisateurs qui y accéderont. Ensuite, vous devez placer les utilisateurs dans un groupe et appliquer la stratégie d'accès réseau au groupe pour faciliter l'administration.
- Identifiez comment les utilisateurs autorisés accèdent au réseau en évaluant les besoins des clients et des matériels.

Synchronisation et administration

Si une partie de la solution vous impose de synchroniser et d'administrer plusieurs points d'accès réseau, comme Internet, extranets, lignes allouées, LAN sans fil, VPN et accès réseau à distance, tenez compte des points suivants :

- Identifiez les utilisateurs qui accéderont au réseau et comment ils y accéderont. Vous devez appliquer les méthodes de sécurité appropriées à ces connexions. Il est vivement recommandé d'utiliser une seule méthode d'authentification, quel que soit le type d'accès (à distance, sans fil, VPN, etc.) pour faciliter l'administration.
- Intégrez votre stratégie d'authentification à toutes les méthodes d'accès distant (connexions à distance, VPN et sans fil). L'extension de la connectivité du réseau s'accompagne de problèmes techniques et d'administration des processus qui permettent difficilement aux administrateurs de gérer l'accès réseau de manière centralisée et cohérente.

Atelier A : Planification de l'accès réseau



*****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 l'accès d'un réseau local/étendu/sans fil ;
- planifier l'authentification d'un réseau.

Scénario

Vous êtes ingénieur système chez Northwind Traders et on vous demande de planifier l'infrastructure réseau d'un nouveau site. Le siège social de la société se trouve à Londres, au Royaume-Uni, et vous voulez transférer son service de comptabilité, son service de distribution et un petit groupe de recherche vers un autre site.

La décision de transférer ces services et ce groupe vers le même site est dictée par un incident de sécurité qui s'est produit au siège. Les informations commerciales des clients sont publiques et il apparaît que l'incident de sécurité s'est produit lorsqu'un employé interne a capturé des données sur le réseau interne. Il est nécessaire de planifier le nouveau site pour protéger les données au maximum et réduire les coûts de la sécurité physique. Seules les ressources des serveurs locaux nécessitent une sécurité physique supplémentaire sous la forme d'un petit local informatique sécurisé.

Le service de distribution se trouve toujours au siège et rencontre des problèmes d'espace et opérationnels. Les produits à livrer sont prélevés dans des armoires de stockage où l'entrée des données et la lecture des codes à barres sont effectuées sur des ordinateurs personnels fixes situés près de l'entrepôt de distribution. Dans le nouveau site, le personnel du service de distribution sera équipé de périphériques sans fil et de lecteurs de codes à barres. Il s'agit de petits PC dotés de cartes sans fil PCMCIA (Personal Computer Memory Card International Association) standard qui exécutent les mêmes applications et systèmes d'exploitation que les ordinateurs de bureau fixes.

Le service Recherche travaille sur un nouveau projet sensible et veut isoler les développeurs dans une salle sécurisée disposant de son propre réseau et de ses propres services. Ce projet nécessite de grandes bandes passantes, car il s'agit d'un projet multimédia.

Les plans que vous fournissez seront étudiés par le service informatique et implémentés après avoir été validés.

Le nouveau site est un entrepôt de 48 000 m² qui abritera le service de distribution et le système d'armoires de stockage. Une mezzanine située dans l'une des extrémités de l'entrepôt sera convertie en bureaux et en bureaux paysagés à l'attention du personnel des services Distribution et Comptabilité. Une petite zone de l'entrepôt proche de la mezzanine sera fermée et accueillera le service Recherche.

Caractéristiques du réseau

Les caractéristiques du réseau des services sont les suivantes :

- Comptabilité

Le service Comptabilité emploie 27 personnes qui utilisent principalement des PC pour accéder aux serveurs locaux. Cinq responsables et chefs de groupes utilisent des ordinateurs de bureau et des ordinateurs portables. Du fait que les ordinateurs portables seront utilisés principalement pour le courrier électronique et offrir une mobilité lors des réunions, ils nécessitent un accès sans fil. Les ressources des serveurs locaux incluent deux contrôleurs de domaine, un serveur d'impression, un serveur de services qui exécute les services DHCP et WINS (Windows Internet Name Service), cinq imprimantes réseau, un serveur de fichiers et un cluster Microsoft SQL Server™.

- Distribution

Le service Distribution compte 18 employés. Sept employés utilisent des ordinateurs personnels et les onze employés restants qui prélèvent les produits du stock utilisent des ordinateurs personnels sans fil. Six autres ordinateurs, situés près de la zone de distribution, sont utilisés pour la saisie des données. Les ressources locales du groupe Distribution incluent trois imprimantes réseau et un serveur d'accès distant pour l'accès sans fil. Les ressources sont connectées au réseau Comptabilité pour le contrôleur de domaine, la base de données, DHCP et WINS.

- Recherche

Le service Recherche compte 6 personnes qui utilisent chacune des ordinateurs de bureau. Trois de ces ordinateurs sont utilisés pour l'édition vidéo et nécessitent des connexions haut débit à un serveur multimédia. Les ressources locales incluent le serveur multimédia, un contrôleur de domaine et un serveur d'impression et de services. Les connexions sans fil ne sont pas autorisées.

Le service informatique Northwind Traders vous a fourni une liste d'éléments dont il pense que vous aurez besoin pour compléter le plan. L'installation matérielle sera effectuée lorsque vous aurez fourni les informations de planification.

Configuration

Les éléments suivants correspondent à la configuration réseau et au matériel disponible du nouveau site :

- La salle informatique sécurisée de la mezzanine contient tous les serveurs et les équipements réseau des services Comptabilité et Distribution. Une liaison WAN (Wide Area Network) T1 reliera le routeur de la salle au siège de Londres.
- Aucune salle informatique sécurisée n'est nécessaire pour le service Recherche car la zone de recherche est sécurisée. Une seule connexion doit relier le routeur du service Recherche au routeur de la salle informatique de la mezzanine pour fournir une connexion avec le siège de Londres.
- La zone de distribution nécessite des points d'accès sans fil installés sur le toit pour fournir une couverture sans fil. Les fournisseurs ont accès au nouveau site et, bien que les points d'accès sans fil couvrent un rayon de 91,5 m, les fournisseurs ne garantissent qu'une couverture de 30,5 m à partir des points d'accès installés sur le toit. Ils suggèrent d'installer six unités en pont pour n'utiliser qu'un seul point de connexion.
- Les besoins de bande passante de la connexion du service Comptabilité du siège de Londres indiquent actuellement un débit maximum de 2,3 Mbps pour chaque client et un débit maximum de 18 Mbps (en entrée et en sortie) sur le serveur d'impression. Le débit maximum vers le cluster SQL Server est de 14 Mbps. Le débit maximum des ordinateurs portables est de 1,2 Mbps.
- La connexion du service Distribution fournit un débit maximal de 500 Kbps vers les ordinateurs de bureau et les PC fixes et les PC sans fil auront vraisemblablement besoin du même débit.
- La connexion du service Recherche est inconnue actuellement, mais du fait que trois PC seront utilisés pour l'édition vidéo de fichiers multimédias volumineux, le fournisseur du logiciel estime que le débit type doit être compris entre 60 et 85 Mbps.
- Quatre ordinateurs seront installés pour d'autres services si vous estimez qu'ils sont nécessaires. Ces ordinateurs pourraient être configurés comme serveurs VPN exécutant le service Routage et accès distant, des serveurs d'accès à distance ou IAS Server.
- Le réseau reposera sur des commutateurs de couche 3 avec des interfaces pour les réseaux 10/100 Mbps. Trois unités 48 ports d'un prix moyen ont été commandées, mais si nécessaire, deux unités pourraient être remplacées par des unités quatre lames plus chères. Les unités d'entrée de gamme peuvent accepter une seule carte modulaire qui fournit des interfaces 3*1 000 Mbps. Les unités haut de gamme utilisent des lames enfichables avec des ports 16*10/100 Mbps ou 5*1 000 Mbps par lame. Le passage des interfaces à 1 000 Mbps augmenterait considérablement les coûts et vous devez donc justifier ce besoin. Les deux types de commutateurs de couche 3 prennent en charge l'authentification par port en utilisant un serveur RADIUS, et IPSec en utilisant des certificats ou des secrets partagés.
- Tous les câbles du réseau sont des câbles CAT5 de 1 000 Mbps, mais pour réduire les coûts, la société veut que vous justifiiez l'utilisation d'interfaces haut débit.

- Un haut niveau de sécurité est nécessaire pour le service Comptabilité et vous devez interdire à tout PC non autorisé d'accéder au réseau.
- Le service Recherche du nouveau site nécessite une connexion sécurisée entre le site et le service Recherche du siège de Londres, qui repose sur une connexion WAN entre la salle informatique du service Comptabilité et le siège social de Londres. Vous devez formuler des recommandations sur la sécurisation de la connexion et sur l'authentification.

**Durée approximative de
cet atelier :
30 minutes**

Exercice 1

Planification de l'environnement LAN et sans fil

Introduction

Dans cet exercice, vous allez créer le plan de la nouvelle infrastructure réseau câblé et sans fil en fonction des besoins définis pour les services Comptabilité, Distribution et Recherche.

Décrivez les modifications ou dessinez l'infrastructure que vous implémenteriez pour le nouveau site.

Scénario

La nouvelle configuration correspond au réseau LAN/sans fil du nouveau site et doit définir la stratégie d'accès réseau qui répond aux besoins.

Tâches	Instructions spécifiques
1. Pour le plan réseau LAN/sans fil du nouveau site, indiquer le nombre de points d'accès nécessaires et le débit LAN des connexions.	Conseil : essayez de maintenir le trafic dans des réseaux VLAN séparés.
2. Documenter les caractéristiques de sécurité et d'authentification des utilisateurs qui se connectent au réseau local câblé.	Incluez les connexions pour lesquelles les ordinateurs doivent être authentifiés avant les utilisateurs.

Exercice 2

Planification de l'environnement WAN

Introduction

Dans cet exercice, vous allez créer le plan de l'infrastructure du réseau étendu du service Recherche en fonction des besoins définis.

Décrivez les modifications ou dessinez l'infrastructure que vous implémenteriez pour le nouveau site.

Scénario

La nouvelle configuration correspond au réseau sans fil du nouveau site et doit définir la stratégie d'accès réseau qui répond aux besoins.

Tâches	Instructions spécifiques
1. Expliquer comment la connexion WAN sécurisée du service Recherche doit être implémentée.	
2. Documenter les caractéristiques d'authentification de la connexion WAN.	