Configuration de l’accès réseau VPN

Sommaire

1.Introduction à l'infrastructure d'accès réseau

1.1. Composants d'une infrastructure d'accès réseau

Pour mettre en place une infrastructure d'accès réseau sécurisée, l'administrateur doit avoir une parfaite connaissance des éléments constitutifs de ce type d'infrastructure, à savoir :

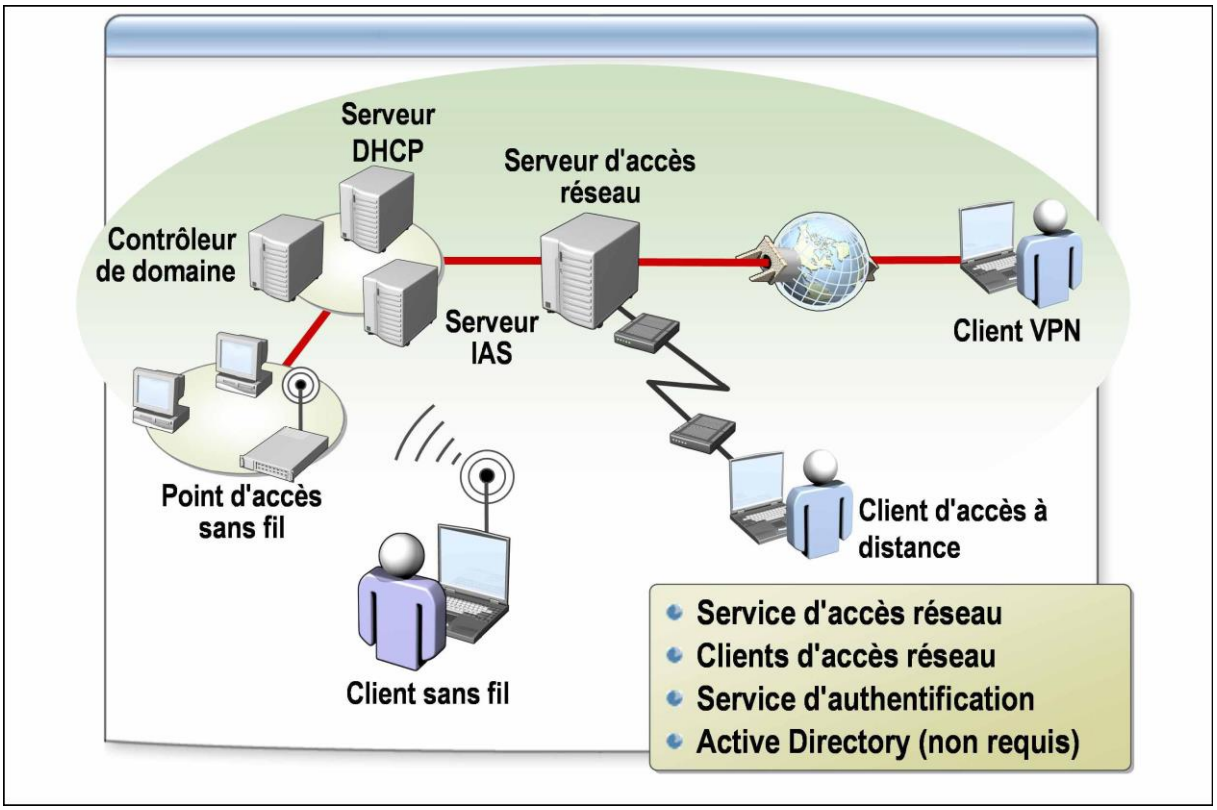
- Serveur d'accès réseau
- Clients d'accès réseau
- Service d'authentification
- Service d'annuaire Active Directory

Le service Routage et accès distant de Microsoft prend en charge l'accès non traditionnel à un réseau. Vous pouvez configurer le service Routage et accès distant de manière à ce qu'il fasse office de serveur d'accès distant et connecter ainsi des télétravailleurs aux réseaux d'une entreprise. Pour ces clients considérés comme non traditionnels, le serveur d'accès distant authentifie les sessions pour les utilisateurs et services jusqu'à ce que l'utilisateur ou l'administrateur y mette fin. Les utilisateurs distants peuvent alors travailler comme si leurs ordinateurs étaient connectés physiquement au réseau.
Un serveur d'accès réseau fournit la connectivité nécessaire aux clients d'accès à distance et VPN.
Ces clients d'accès à distance peuvent accéder aux ressources à l'aide d'outils standard. À titre d'exemple, sur un serveur configuré avec le service Routage et accès distant, les clients distants peuvent utiliser l'Explorateur Windows pour établir des connexions à des unités et se connecter à des imprimantes. Les connexions sont permanentes, ce qui signifie que les clients ne doivent pas se reconnecter aux ressources réseau lors d'une session à distance.

Offrir un accès réseau étendu implique l'augmentation du niveau de sécurité afin de protéger le réseau contre tout accès non autorisé et empêcher l'utilisation d'équipement interne. Pour ce faire, vous pouvez appliquer une authentification renforcée afin de valider l'identité des utilisateurs, en plus d'un cryptage renforcé destiné à protéger les données.
En règle générale, les méthodes d'authentification utilisent un protocole d'authentification négocié lors de l'établissement d'une connexion. Le serveur d'accès distant (serveur configuré avec le service Routage et accès distant) gère l'authentification entre le client d'accès distant et le contrôleur de domaine.
Dans une infrastructure à plusieurs serveurs d'accès réseau, il est possible de centraliser l'authentification en utilisant le service RADIUS afin d'authentifier et d'autoriser les clients d'accès réseau. L'utilisation de ce service dispense chacun des serveurs d'accès de votre réseau d'effectuer les opérations d'authentification et d'autorisation.

Les domaines Active Directory contiennent les comptes d'utilisateurs, les mots de passe et les propriétés d'accès à distance nécessaires pour authentifier les informations d'identification des utilisateurs et évaluer les contraintes d'autorisation et de connexion.
Une fois un client connecté à votre réseau, vous pouvez contrôler l'accès aux ressources au moyen de divers contrôles administratifs sur l'ordinateur client et les serveurs d'accès réseau, parmi lesquels : Partage de fichiers et

d'imprimantes, Stratégie de groupe local et Stratégie de groupe via le service Active Directory.



1.2. Configuration requise pour un serveur d'accès réseau

Un *serveur d'accès réseau* est un serveur qui fait office de passerelle vers un réseau pour un client. Dans ce module, le serveur d'accès réseau est un serveur configuré avec le service Routage et accès distant. Il peut également être qualifié de serveur d'accès distant (pour les connexions d'accès à distance) ou de serveur VPN, selon le type de connexion qu'il est habilité à négocier.
Lors de l'activation initiale du service Routage et accès distant sur un serveur, l'Assistant Installation du serveur de routage et d'accès distant apparaît. Il affiche des instructions pour vous aider à configurer correctement votre serveur d'accès réseau. Avant de configurer votre serveur d'accès réseau, vous devez disposer des informations de configuration suivantes :

- Quelle est la finalité du serveur : routeur et/ou serveur d'accès distant ?
- Quels sont les fournisseurs et méthodes d'authentification utilisés ?
- Un client réseau est-il autorisé à accéder uniquement à ce serveur ou à l'ensemble du réseau ?
- Comment les adresses IP (Internet Protocol) doivent-elles être affectées aux clients qui se connectent ?
- Quelles sont les options de configuration PPP (Point-to-Point Protocol) ?
- Quelles sont les préférences en matière d'enregistrement des événements ?

1.3. Client d'accès réseau

Type de client	Description
 Client VPN	• Se connecte via un réseau public ou partagé • Émule une liaison point à point sur un réseau privé
 Client d'accès à distance	• Se connecte par le biais d'un réseau de communication • Crée une connexion physique à un port sur un serveur d'accès distant situé sur un réseau privé • Utilise un modem ou une carte RNIS pour se connecter au serveur d'accès distant
 Client sans fil	• Se connecte à un réseau au moyen de technologies infrarouges (IR) ou à fréquences radio (RF) • Comprend de nombreux types de périphériques

Pour gérer un réseau informatique, l'administrateur doit rendre les ressources réseau accessibles aux utilisateurs qui ne sont pas directement connectés au réseau local. Ces utilisateurs peuvent être des employés, des sous-traitants, des fournisseurs ou encore des clients. Quant à l'accès au réseau, il peut s'effectuer au moyen de connexions d'appel entrant, Internet ou sans fil. En votre qualité d'administrateur système, il vous appartient de configurer un accès sécurisé pour les utilisateurs autorisés à se connecter à votre réseau et de refuser cet accès aux autres utilisateurs. Vous devez donc être en mesure de configurer et de sécuriser votre serveur d'accès réseau pour les méthodes d'accès suivantes :

- Réseau privé virtuel (VPN)
- Accès réseau à distance
- Accès sans fil

Un *client VPN* se connecte via un réseau public ou partagé, comme Internet, selon une méthode qui émule une liaison point à point sur un réseau privé.
Un *client d'accès à distance* se connecte par le biais d'un réseau de communication, tel que le réseau téléphonique public commuté (RTPC), afin de créer une connexion physique à un port sur un serveur d'accès distant situé sur un réseau privé. Plusieurs technologies peuvent être utilisées pour établir ce type de connexion au serveur d'accès distant : modem, carte RNIS ou adaptateur DSL.
Dans le cas d'un *client sans fil*, la connexion s'établit au moyen de technologies infrarouges (IR) ou à fréquences radio (RF) optimisées pour les connexions à courte distance. Parmi les dispositifs utilisés couramment dans le cadre des réseaux sans fil, citons les ordinateurs portables, les ordinateurs de poche, les assistants numériques (PDA), les téléphones cellulaires, les ordinateurs avec stylet et les récepteurs de radiomessagerie.

1.4. Autorisation et authentification de l'accès réseau

Lorsqu'une entreprise décide d'étendre l'accès à son réseau, elle doit également veiller à ce que son niveau de sécurité soit suffisamment élevé pour protéger le réseau contre tout accès non autorisé et empêcher l'utilisation d'équipement interne.
Dans le cas des connexions VPN, sans fil et d'accès à distance, Microsoft® Windows Server. 2003 implémente l'authentification dans deux processus : ouverture de session interactive et autorisation d'accès au réseau. Pour accéder aux ressources réseau, l'utilisateur doit obligatoirement satisfaire à ces deux processus.
Il est essentiel de faire la distinction entre authentification et autorisation pour bien comprendre comment les tentatives de connexion sont acceptées ou refusées.

- L'*authentification* est la validation des informations d'identification lors d'une tentative de connexion. Cette procédure d'ouverture de session comprend l'envoi des informations d'identification du client d'accès réseau (un nom et un mot de passe, par exemple) vers le serveur d'accès réseau en texte clair ou sous une forme cryptée en utilisant un protocole d'authentification. L'identification de l'utilisateur est ensuite transmise à un compte de domaine pour confirmation.
- L'*autorisation* est la procédure par laquelle le serveur vérifie que la tentative de connexion est autorisée. Une fois le client distant authentifié, l'accès lui est autorisé ou refusé en fonction des informations d'identification du compte et des stratégies d'accès distant. La procédure d'autorisation ne peut avoir lieu qu'après une tentative d'ouverture de session réussie. En cas d'échec, l'accès est refusé.

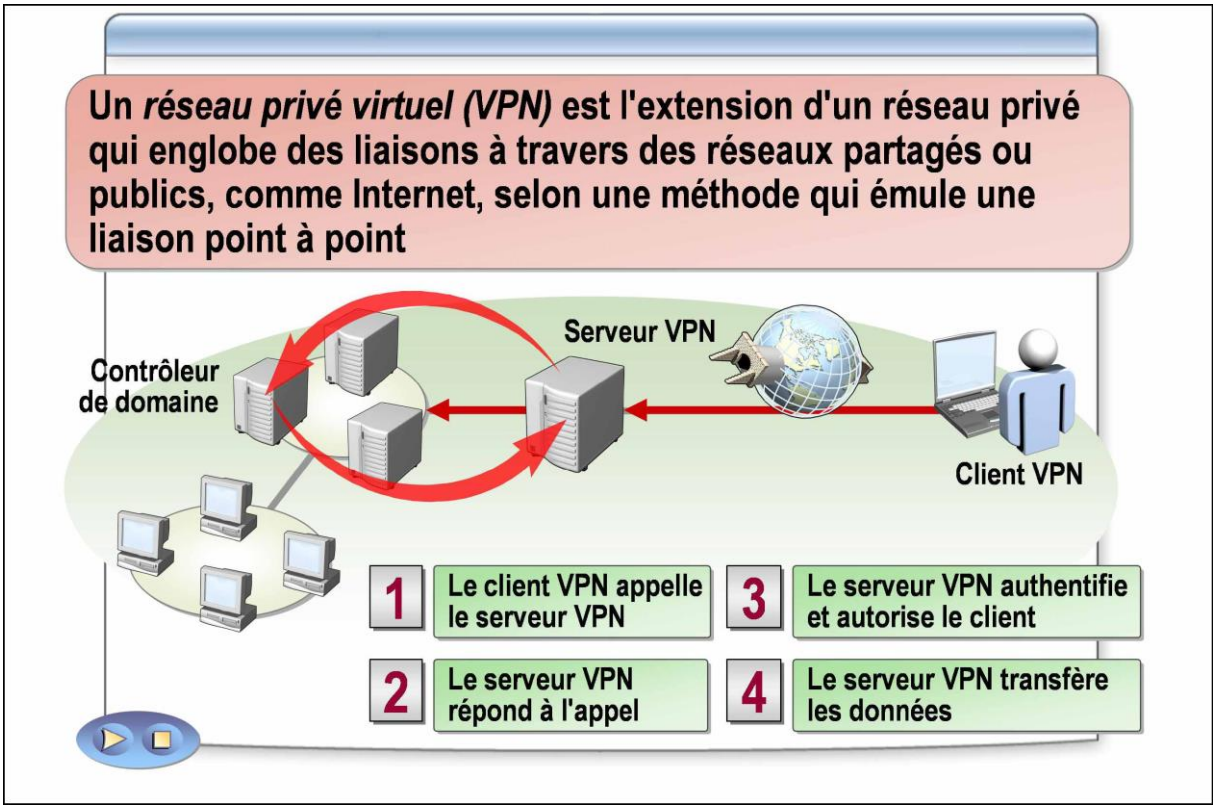
1.5. Méthodes d'authentification disponibles

L'authentification des clients d'accès distant constitue un problème important en matière de sécurité. En règle générale, les méthodes d'authentification utilisent un protocole d'authentification négocié lors de l'établissement de la connexion.
Les produits de la famille Windows Server 2003 prennent en charge les méthodes d'authentification ci-dessous.

Méthode d'authentification	Description
Protocole CHAP (Challenge Handshake Authentication Protocol)	• Plusieurs fournisseurs de clients et serveurs d'accès distant utilisent le protocole CHAP. • Le service Routage et accès distant prend en charge le protocole CHAP.
Protocole PAP (Password Authentication Protocol)	• Le protocole PAP utilise des mots de passe en clair. Il s'agit du protocole d'authentification le moins sophistiqué.
Protocole SPAP (Shiva Password Authentication Protocol)	• Protocole d'authentification par mot de passe crypté simple. • Les serveurs d'accès distant Shiva prennent en charge le protocole SPAP.
Protocole MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)	• Les clients Microsoft Windows 95 utilisent le protocole MS-CHAP. • Il prend uniquement en charge les clients Microsoft.
Protocole MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2)	• Ce protocole effectue une authentification mutuelle. • Microsoft Windows 2000 et les versions ultérieures du système d'exploitation installent, par défaut, le protocole MS-CHAP v2 comme protocole d'authentification d'accès distant.
EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)	• Ce protocole effectue une authentification mutuelle. • Elle exige une infrastructure de certificats à cartes à puce. • Elle offre le niveau de sécurité d'authentification le plus élevé.
Protocole PEAP (Protected Extensible Authentication Protocol)	• Ce protocole est utilisé avec les réseaux 802.1x afin de sécuriser les réseaux câblés et sans fil. • L'accès est accordé en fonction de l'identité de l'utilisateur. • Il renforce la sécurité du cryptage des réseaux sans fil.
MD-5 Challenge	• Cette méthode permet une autorisation EAP au moyen de combinaisons nom/mot de passe standard.

2. Configuration d'une connexion VPN

2.1. Fonctionnement d'une connexion VPN



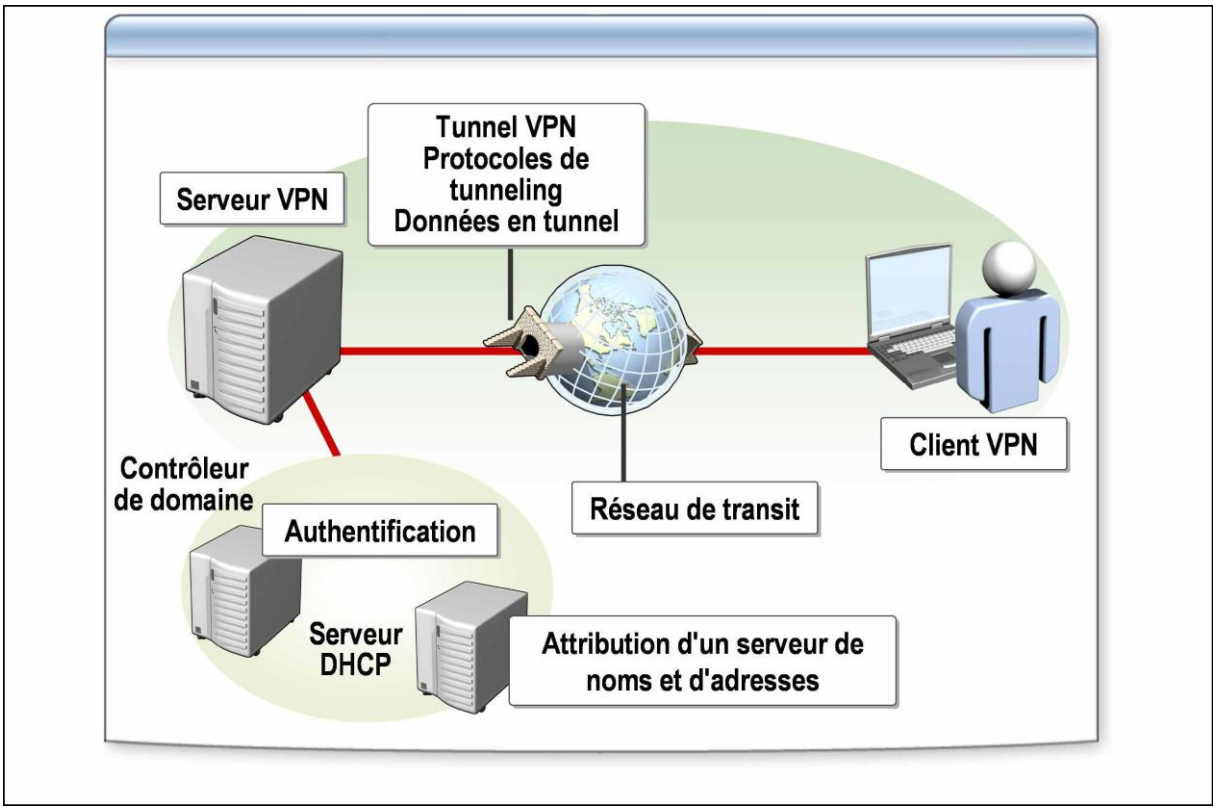
Le service Routage et accès distant fournit des services VPN pour permettre aux utilisateurs d'accéder à des réseaux d'entreprise de manière sécurisée en cryptant les données transmises sur un réseau de transport non sécurisé, comme Internet.
Un réseau privé virtuel (VPN, *Virtual Private Network*) est l'extension d'un réseau privé qui englobe des liaisons à travers des réseaux partagés ou publics, comme Internet. Ce type de réseau permet un échange de données cryptées entre deux ordinateurs à travers un réseau partagé ou public, selon un mode qui émule une liaison point à point sur un réseau privé.
Pour émuler une liaison point à point, les données sont encapsulées, ou enrobées, à l'aide d'un en-tête qui contient les informations de routage, ce qui permet aux données de traverser le réseau partagé ou public jusqu'à leur destination finale. Pour émuler une liaison privée, les données sont cryptées à des fins de confidentialité. Les paquets interceptés sur le réseau partagé ou public ne peuvent pas être lus sans les clés de cryptage. La liaison servant à l'encapsulation et au cryptage des données privées est une connexion VPN.
Une connexion VPN est également désignée sous le nom de tunnel VPN.
Le processus d'établissement d'une connexion VPN est décrit ci-dessous :
1. Un client VPN établit une connexion VPN à un serveur d'accès distant/VPN relié à Internet. (Le serveur VPN fait office de passerelle. Il est, en principe, configuré en vue de fournir l'accès à tout le réseau auquel il est connecté.)
2. Le serveur VPN répond à l'appel virtuel.
3. Le serveur VPN authentifie l'appelant et vérifie son autorisation de connexion.

4. Le serveur VPN transfère les données entre le client VPN et le réseau d'entreprise.

Les réseaux privés virtuels permettent aux utilisateurs ou aux entreprises de se connecter à des serveurs distants, des succursales ou à d'autres entreprises sur un réseau public, tout en bénéficiant de communications sécurisées. Aux yeux de l'utilisateur, la connexion sécurisée apparaît toujours comme une communication sur un réseau privé, et ce, bien qu'elle soit établie sur un réseau public. Autres avantages :

- *Réduction des coûts*. Le réseau VPN n'utilise pas de ligne téléphonique et requiert un minimum de matériel (c'est à votre fournisseur de services Internet qu'il appartient de gérer l'équipement de communication).
- *Sécurité accrue*. Les données sensibles sont dissimulées pour les utilisateurs non autorisés, mais les utilisateurs autorisés peuvent y accéder par l'intermédiaire de la connexion. Le serveur VPN applique l'authentification et le cryptage.
- *Prise en charge des protocoles réseau*. Vous pouvez exécuter à distance une application qui dépend des protocoles réseau les plus courants, dont TCP/IP (*Transmission Control Protocol/Internet Protocol*).
- *Sécurité des adresses IP*. Les informations envoyées sur un réseau privé virtuel étant cryptées, les adresses que vous spécifiez sont protégées et seule l'adresse IP externe est visible pour le trafic transmis sur Internet. Aucun frais administratif n'est lié à la modification des adresses IP pour l'accès distant sur Internet.

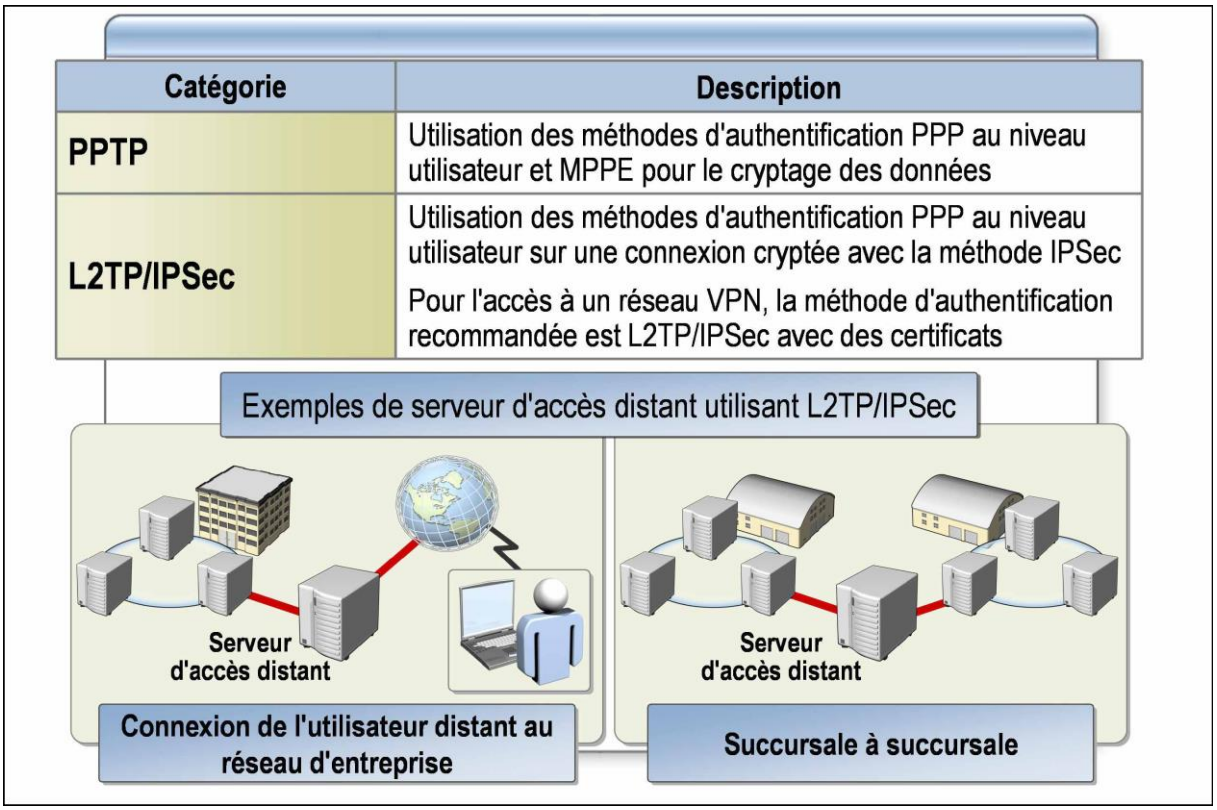
2.2. Composants d'une connexion VPN



Une connexion VPN est constituée des composants suivants :

- *Serveur VPN*. Ordinateur qui accepte les connexions VPN émanant de clients VPN ; un serveur configuré avec le service Routage et accès distant par exemple.
- *Client VPN*. Ordinateur qui amorce une connexion VPN à un serveur VPN.
- *Réseau de transit*. Réseau public ou privé traversé par les données encapsulées.
- *Tunnel ou connexion VPN*. Segment de la connexion dans lequel vos données sont cryptées et encapsulées.
- *Protocoles de tunneling*. Protocoles utilisés pour gérer les tunnels et encapsuler des données privées (c'est le cas du protocole PPTP, par exemple).
- *Données en tunnel*. Données acheminées généralement via une liaison point à point privée.
- *Authentification*. Dans une connexion VPN, l'identité du client et du serveur est authentifiée. Un réseau VPN authentifie également les données envoyées afin de s'assurer que les données reçues proviennent bien de l'autre extrémité de la connexion et qu'elles n'ont pas été interceptées et modifiées.
- *Attribution d'un serveur de noms et d'adresses*. Le serveur VPN est responsable de l'attribution d'adresses IP. Pour ce faire, il utilise soit le protocole par défaut, à savoir DHCP (Dynamic Host Configuration Protocol), soit un pool statique créé par l'administrateur. Il alloue également des adresses de serveur DNS (Domain Name System) et WINS (Windows Internet Name Service) aux clients. Les serveurs de noms alloués sont ceux qui desservent le réseau Intranet auquel le serveur VPN se connecte.

2.3. Protocoles de cryptage pour une connexion VPN



Les produits de la famille Windows Server 2003 utilisent deux types de protocoles de tunneling (cryptage) pour sécuriser les communications :

- *PPTP (Point-to-Point Tunneling Protocol)*. Utilisation des méthodes d'authentification PPP au niveau utilisateur et MPPE (Microsoft Point-to Point Encryption) pour le cryptage des données.
- *L2TP/IPSec (Layer Two Tunneling Protocol with Internet Protocol Security)*. Utilisation des méthodes d'authentification PPP au niveau utilisateur sur une connexion cryptée avec la méthode IPSec. Cette méthode nécessite une authentification de l'hôte au moyen du protocole Kerberos, d'un secret partagé ou de certificats d'ordinateur.

Il est conseillé d'utiliser la méthode L2TP/IPSec avec des certificats pour bénéficier d'une authentification VPN sécurisée. Grâce à l'authentification et au cryptage IPSec, le transfert des données par l'intermédiaire d'un réseau privé virtuel compatible L2TP est aussi sûr qu'au sein d'un réseau local d'entreprise.
Le client et le serveur VPN doivent prendre en charge les méthodes L2TP et IPSec. La prise en charge de L2TP par le client est intégrée dans le client d'accès distant Windows XP et la prise en charge de L2TP par le serveur VPN est intégrée dans les produits de la famille Windows Server 2003.
La prise en charge de L2TP par le serveur est installée lors de l'installation du service Routage et accès distant. Selon les options sélectionnées lors de l'exécution de l'Assistant Installation du serveur d'accès distant et de routage, le protocole L2TP est configuré pour 5 ou 128 ports L2TP.

2.4. Configuration requise pour un serveur VPN

Le tableau suivant répertorie ce qu'il faut savoir avant de configurer un serveur d'accès distant/VPN.

Avant d'ajouter un rôle de serveur VPN	Commentaires
Identifiez l'interface réseau qui assure la connexion à Internet et celle qui assure la connexion à votre réseau privé.	Durant la configuration, vous serez invité à choisir l'interface réseau qui assure la connexion à Internet. Si vous spécifiez une interface incorrecte, le serveur d'accès distant/VPN ne fonctionnera pas correctement.
Déterminez si les clients distants recevront des adresses IP d'un serveur DHCP situé sur votre réseau privé ou du serveur VPN en cours de configuration.	Si votre réseau privé comporte un serveur DHCP, le serveur VPN peut prendre en bail dix adresses à la fois à partir du serveur DHCP et affecter ces adresses à des clients distants. En revanche, si vous ne disposez pas d'un tel serveur, le serveur VPN peut automatiquement générer des adresses IP et les attribuer à des clients distants. Si vous souhaitez que le serveur d'accès distant/VPN affecte des adresses IP à partir d'une plage d'adresses que vous spécifiez, déterminez cette plage.
Indiquez si les demandes de connexion en provenance des clients VPN doivent être authentifiées par un serveur RADIUS ou par le serveur VPN en cours de configuration.	L'ajout d'un serveur RADIUS se révèle utile si vous envisagez d'installer plusieurs serveurs VPN, points d'accès sans fil ou autres clients RADIUS dans votre réseau privé. Cette opération est décrite de manière plus détaillée dans les autres leçons de ce module.

Pour inscrire un serveur d'accès distant dans Active Directory, procédez comme suit :
1. Ouvrez une session avec un compte d'utilisateur autorisé à inscrire un serveur d'accès distant dans Active Directory.

2. À l'invite de commandes, tapez ce qui suit : **netsh ras add registeredserver** *Nom_Domaine Nom_Ordinateur* (où *Nom_Domaine* est le nom du domaine dans lequel vous inscrivez le serveur d'accès distant et *Nom_Ordinateur* le nom d'ordinateur du serveur d'accès distant)

Pour configurer un serveur d'accès distant pour une connexion VPN, procédez comme suit :

1. Ouvrez une session avec un compte d'utilisateur ne disposant pas de droits d'administration.
2. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
3. Dans le Panneau de configuration, ouvrez **Outils d'administration**, cliquez avec le bouton droit sur **Gérer votre serveur**, puis sélectionnez **Exécuter en tant que**.
4. Dans la boîte de dialogue **Exécuter en tant que**, sélectionnez l'option **L'utilisateur suivant**, entrez un compte d'utilisateur (ainsi que le mot de passe) autorisé à effectuer la tâche, puis cliquez sur **OK**.
5. Dans la fenêtre **Gérer votre serveur**, cliquez sur **Ajouter ou supprimer un rôle** pour accéder à l'**Assistant Configurer votre serveur**.
6. Sur la page **Étapes préliminaires**, cliquez sur **Suivant**.
7. Sur la page **Rôle du serveur**, cliquez sur **Serveur VPN / Accès distant**, puis sur **Suivant**.
8. Sur la page **Aperçu des sélections**, cliquez sur **Suivant**.
9. Sur la page de **Bienvenue**, cliquez sur **Suivant**.
10. Sur la page **Configuration**, sélectionnez **Accès à distance (connexion à distance ou VPN**), puis cliquez sur **Suivant**.
11. Sur la page **Accès distant**, vérifiez que l'option **VPN** est sélectionnée, puis cliquez sur **Suivant**.
12. Sur la page **Connexion VPN**, cliquez sur l'interface réseau qui assure la connexion de cet ordinateur à Internet. L'interface réseau sélectionnée sera configurée pour recevoir des connexions de clients VPN. Toute interface non sélectionnée sera configurée pour la connexion à votre réseau privé.
13. Sur la page **Attribution d'adresses IP**, sélectionnez soit **Automatiquement**, soit **À partir d'une plage d'adresses spécifiée**. L'option sélectionnée par défaut est **Automatiquement**. Cette option configure votre serveur de façon à ce qu'il génère et attribue des adresses IP à des clients distants. Cliquez sur **Suivant**.
14. Sur la page **Gestion des serveurs d'accès distant multiples**, l'option **Non, utiliser Routage et accès à distance pour authentifier les requêtes de connexion** est sélectionnée automatiquement. Ne modifiez pas cette sélection. De cette façon, le serveur est configuré pour authentifier les demandes de connexion localement au moyen de l'authentification Windows, de la gestion des comptes Windows et des stratégies d'accès distant stockées en local. Cliquez sur **Suivant**.
15. Sur la page **Fin de l'Assistant Installation du serveur du routage et d'accès distant**, passez en revue les informations résumées. Vérifiez les points suivants :

- les clients VPN se connectent à l'interface publique appropriée ;
- des adresses IP sont attribuées aux clients VPN pour l'interface réseau appropriée ;
- les connexions clientes sont acceptées et authentifiées à l'aide de stratégies d'accès distant pour ce serveur VPN.

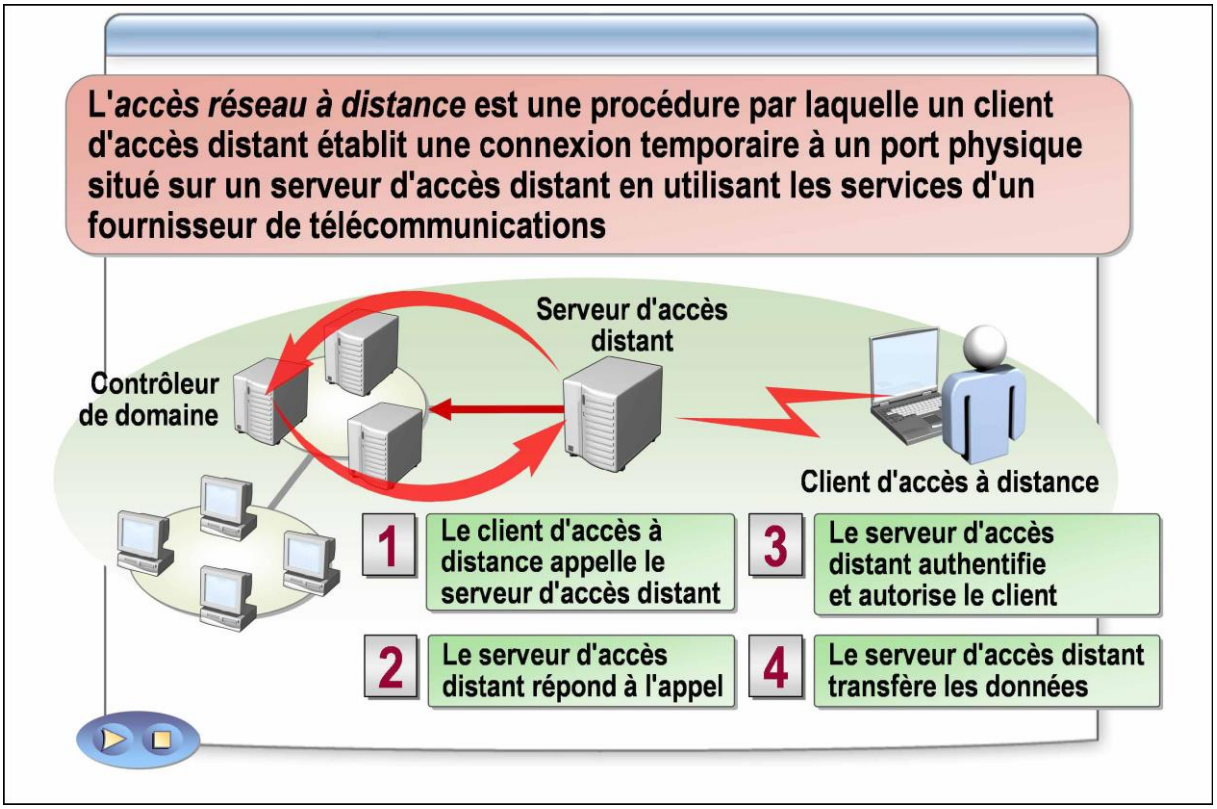
16. Si l'une des informations résumées ne convient pas, cliquez sur **Précédent** et apportez les modifications nécessaires. Si les informations sont correctes, cliquez sur **Terminer**.
17. Un message **Routage et accès distant** indique alors ce qui suit : « Windows n'a pas pu ajouter cet ordinateur à la liste des serveurs d'accès distants valides dans Active Directory. Pour que vous puissiez utiliser cet ordinateur comme un serveur d'accès distant, l'administrateur de domaine doit terminer cette tâche ». Cliquez sur **OK**.
18. Un autre message **Routage et accès distant** indique ce qui suit : « Pour prendre en charge le relais des messages DHCP à partir de clients d'accès distant, vous devez configurer les propriétés de l'agent de relais DHCP avec l'adresse IP de votre serveur DHCP ». Cliquez sur **OK**.
19. Le service Routage et accès distant démarre automatiquement et l'Assistant Configurer votre serveur réapparaît. Sur la page **Ce serveur est maintenant un serveur d'accès distant et de réseau VPN**, cliquez sur **Terminer**.

2.5. Comment configurer un client d'accès distant pour une connexion VPN

Pour configurer un client d'accès distant pour une connexion VPN, procédez comme suit :
1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
2. Dans le Panneau de configuration, cliquez sur **Connexions réseau**.
3. Dans les Connexions réseau, double-cliquez sur **Assistant Nouvelle Connexion**.
4. Sur la page **Bienvenue dans l'Assistant Nouvelle connexion**, cliquez sur **Suivant**.
5. Sur la page **Type de connexion réseau**, sélectionnez **Connexion au réseau d'entreprise**, puis cliquez sur **Suivant**.
6. Sur la page **Connexion réseau**, sélectionnez **Connexion réseau privé virtuel**, puis cliquez sur **Suivant**.
7. Entrez le nom de la connexion sur la page **Nom de la connexion** (il s'agit généralement du nom de votre entreprise), puis cliquez sur **Suivant**.
8. Sur la page **Sélection de serveur VPN**, entrez le nom d'hôte (Microsoft.com, par exemple) ou l'adresse IP du serveur VPN auquel vous vous connectez, puis cliquez sur **Suivant**.
9. Si vous disposez d'autorisations d'administration sur l'ordinateur local, vous pouvez sélectionner l'option **Tous les utilisateurs** ou **Mon utilisation uniquement** sur la page **Disponibilité de connexion**. Si vous avez ouvert une session avec un compte d'utilisateur ne disposant pas de droits d'administration, seule l'option **Mon utilisation uniquement** peut être sélectionnée. Cliquez sur **Suivant**.
10. Sur la page **Fin de l'Assistant Nouvelle connexion**, cliquez sur **Terminer**.

3. Configuration d'une connexion d'accès à distance

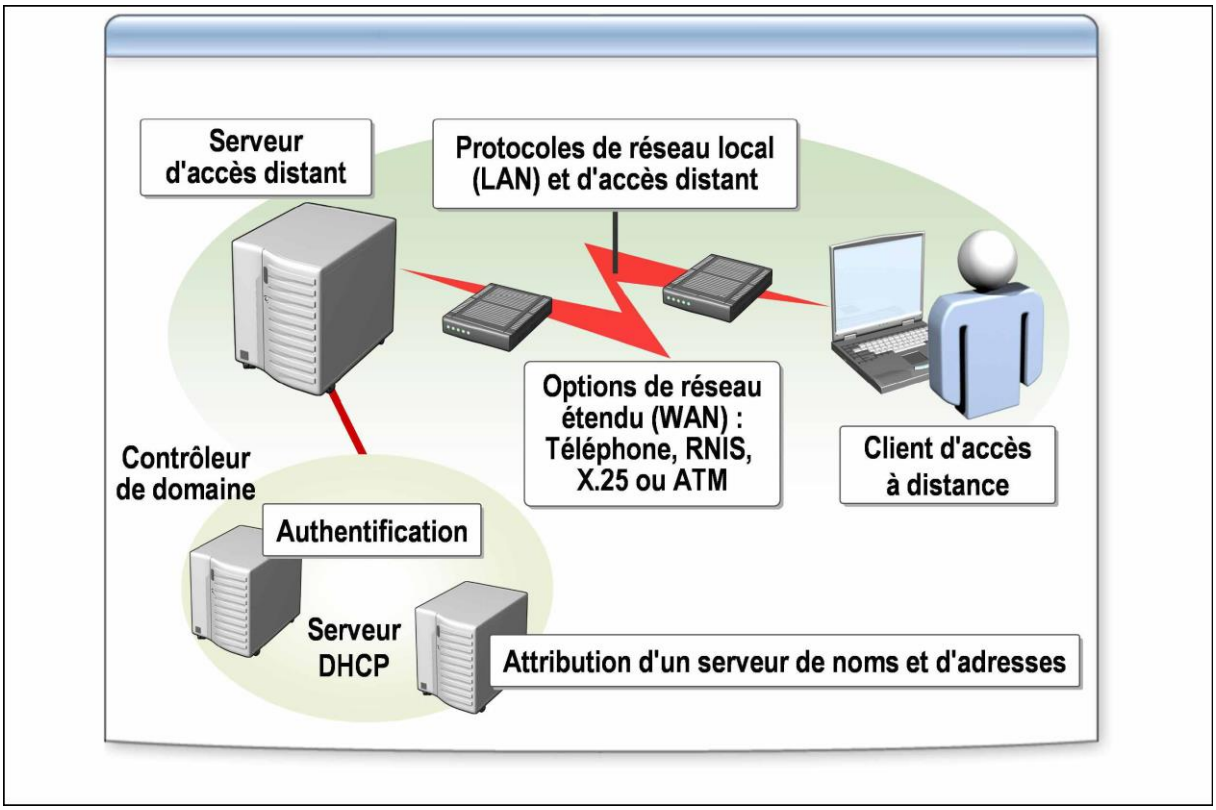
3.1. L'accès réseau à distance



Vous pouvez utiliser un serveur configuré avec le service Routage et accès distant pour permettre l'accès à distance à l'intranet de votre entreprise.
L'*accès réseau à distance* est une procédure par laquelle un client d'accès distant établit une connexion temporaire à un port physique situé sur un serveur d'accès distant en utilisant les services d'un fournisseur de télécommunications, tel qu'un téléphone analogique, RNIS (Réseau Numérique à Intégration de Services) ou X.25.
L'accès réseau à distance sur une ligne de téléphone analogique ou RNIS est une connexion physique entre le client et le serveur d'accès réseau à distance.
Vous pouvez crypter les données transmises sur la connexion, mais cela n'est pas obligatoire.
Le processus d'établissement d'une connexion réseau à distance est décrit cidessous
:
1. Un client appelle le serveur d'accès distant.
2. L'équipement d'accès réseau à distance installé sur un serveur d'accès distant répond aux demandes de connexion entrantes émanant de clients d'accès distant.
3. Le serveur d'accès distant authentifie et autorise l'appelant.
4. Le serveur d'accès distant transfère des données entre le client d'accès réseau à distance et le réseau intranet de l'entreprise. (Le serveur d'accès distant fait

office de passerelle. Il fournit l'accès à l'intégralité du réseau auquel il est connecté.)

3.2. Composants d'une connexion d'accès à distance



Une connexion d'accès à distance est constituée des composants suivants :

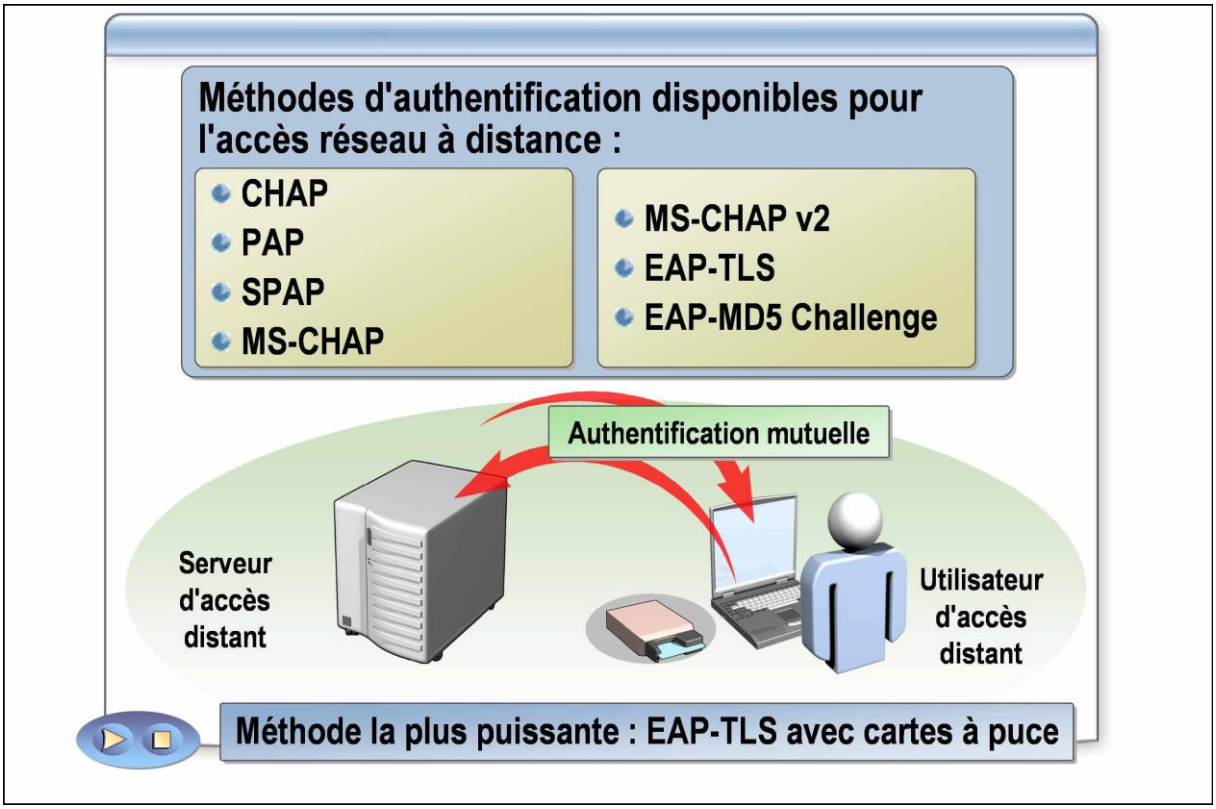
- *Serveur d'accès distant*. Ordinateur qui accepte les connexions d'accès à distance émanant de clients d'accès à distance ; un serveur configuré avec le service Routage et accès distant, par exemple.
- *Client d'accès à distance*. Ordinateur qui amorce une connexion d'accès à distance à un serveur d'accès à distance.
- *Protocoles de réseau local (LAN) et d'accès distant*. Les programmes d'application utilisent des protocoles de réseau local (LAN) pour transporter les informations. Les protocoles d'accès distant sont utilisés pour négocier les connexions et assurer le tramage des données des protocoles LAN qui sont envoyées sur des liaisons de réseau étendu (WAN).
- *Options de réseau étendu (WAN)*. Les clients peuvent se connecter au réseau en utilisant des lignes téléphoniques standard et un modem ou un pool de modems. La technologie RNIS permet l'établissement de liaisons plus rapides. Il est également possible de connecter des clients d'accès distant à des serveurs d'accès distant au moyen de liaisons X.25 ou ATM (Asynchronous Transfer Mode). La prise en charge des connexions directes est assurée par un câble Null Modem RS-232C, une connexion par port parallèle ou une connexion infrarouge.

- *Authentification*. Dans une connexion d'accès à distance, l'identité du client et du serveur est authentifiée. L'utilisation de cartes à puce dans le cadre

de l'authentification des utilisateurs constitue la forme d'authentification la plus puissante dans la famille Windows Server 2003.

- *Attribution d'un serveur de noms et d'adresses*. Le serveur d'accès distant est responsable de l'attribution d'adresses IP. Pour ce faire, il utilise soit le protocole par défaut, à savoir DHCP (Dynamic Host Configuration Protocol). Il affecte également des adresses de serveur DNS (Domain Name System) et WINS (Windows Internet Name Service) aux clients. Les serveurs de noms qui allouent des adresses aux clients d'accès distant sont ceux qui desservent le réseau intranet auquel le serveur d'accès distant se connecte.

3.3. Méthodes d'authentification disponibles pour une connexion d'accès à distance



Les produits de la famille Windows Server 2003 prennent en charge les méthodes d'authentification suivantes pour l'accès réseau à distance :

- CHAP
- PAP
- SPAP
- MS-CHAP
- MS-CHAP v2
- EAP-TLS
- EAP-MD5 Challenge

La méthode d'authentification la plus puissante pour les versions antérieures de Windows est EAP-TLS, une méthode d'authentification mutuelle par laquelle le

client et le serveur prouvent leurs identités respectives. Lors du processus d'authentification, le client d'accès distant envoie son certificat d'utilisateur, tandis que le serveur d'accès distant envoie son certificat d'ordinateur. Si l'un des certificats n'est pas envoyé ou n'est pas valide, la connexion est interrompue.
L'utilisation de certificats de cartes à puce avec EAP-TLS dans le cadre de l'authentification des utilisateurs constitue la forme d'authentification la plus puissante dans la famille Windows Server 2003. La mise en place d'une infrastructure de clés publiques (PKI) est obligatoire pour utiliser des certificats de cartes à puce dans le cadre de l'authentification des utilisateurs.

3.4. Configuration requise pour un serveur d'accès distant

Le tableau suivant répertorie ce qu'il faut savoir avant de configurer un serveur d'accès distant pour l'accès à distance.

Avant d'ajouter un rôle de serveur d'accès distant	**Commentaires**
Déterminez si les clients distants recevront des adresses IP d'un serveur DHCP situé sur votre réseau privé ou du serveur d'accès distant en cours de configuration.	Si votre réseau privé comporte un serveur DHCP, le serveur VPN peut prendre en bail dix adresses à la fois à partir du serveur DHCP et affecter ces adresses à des clients distants. En revanche, si vous ne disposez pas d'un tel serveur, le serveur d'accès à distance peut automatiquement générer des adresses IP et les attribuer à des clients distants. Si vous souhaitez que le serveur d'accès distant affecte des adresses IP à partir d'une plage d'adresses que vous spécifiez, déterminez cette plage.
Indiquez si les demandes de connexion en provenance des clients d'accès à distance doivent être authentifiées par un serveur RADIUS ou par le serveur d'accès distant en cours de configuration.	L'ajout d'un serveur RADIUS se révèle utile si vous envisagez d'installer plusieurs serveurs d'accès distant, points d'accès sans fil ou autres clients RADIUS dans votre réseau privé. Cette opération est décrite de manière plus détaillée dans les autres leçons de ce module.
Vérifiez que tous les utilisateurs disposent d'un compte d'utilisateur configuré pour permettre l'accès réseau à distance.	Pour qu'un utilisateur puisse se connecter au réseau, il doit posséder un compte d'utilisateur sur le serveur d'accès distant ou dans Active Directory. Chaque compte d'utilisateur contient des propriétés qui déterminent si l'utilisateur peut se connecter.

Pour configurer le serveur d'accès distant pour une connexion d'accès à distance, procédez comme suit :
1. Ouvrez Gérer votre serveur, puis cliquez sur **Ajouter ou supprimer un rôle**.
2. Sur la page **Étapes préliminaires**, cliquez sur **Suivant**.
3. Sur la page **Rôle du serveur**, sélectionnez **Serveur VPN / Accès distant**, puis cliquez sur **Suivant**.
4. Sur la page **Aperçu des sélections**, cliquez sur **Suivant**.
5. Sur la page de **Bienvenue**, cliquez sur **Suivant**.
6. Sur la page **Configuration** , sélectionnez **Accès à distance (connexion à distance ou VPN**), puis cliquez sur **Suivant**.
7. Sur la page **Accès distant**, cliquez sur **Accès à distance**, puis sur **Suivant**.
8. Sur la page **Sélection du réseau**, sélectionnez l'interface réseau connectée à Internet, puis cliquez sur **Suivant**.
9. Sur la page **Attribution d'adresses IP**, cliquez sur **Suivant**.
10. Sur la page **Gestion des serveurs d'accès distant multiples**, cliquez sur **Suivant**.
11. Sur la page **Fin de l'Assistant Installation du serveur du routage et d'accès distant**, cliquez sur **Terminer**.
12. Dans la boîte de dialogue **Routage et accès distant**, cliquez sur **OK**.
13. Sur la page **Ce serveur est maintenant un serveur d'accès distant et de réseau VPN**, cliquez sur **Terminer**.

3.5. Comment configurer un client d'accès distant pour une connexion d'accès à distance

Les connexions réseau vous permettent de configurer un client pour une connexion d'accès à distance. Vous pourrez changer cette connexion ultérieurement en en modifiant les paramètres. Les paramètres d'une connexion d'accès à distance (tels que le numéro de téléphone, le nombre de tentatives de renumérotation, etc.) sont définis pour chaque connexion. Ces paramètres de pré-connexion et post-connexion n'affectent pas ceux des autres connexions.

Pour configurer un client d'accès distant en vue d'une connexion d'accès à distance, procédez comme suit :
1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
2. Dans le Panneau de configuration, cliquez sur **Connexions réseau**.
3. Dans les Connexions réseau, double-cliquez sur **Assistant Nouvelle Connexion**.
4. Dans la page **Bienvenue dans l'Assistant Nouvelle connexion**, cliquez sur **Suivant**.
5. Sur la page **Type de connexion réseau**, sélectionnez **Connexion au réseau d'entreprise**, puis cliquez sur **Suivant**.
6. Sur la page **Connexion réseau**, choisissez **Connexion d'accès à distance**, puis cliquez sur **Suivant**.
7. Entrez le nom de la connexion sur la page **Nom de la connexion** (il s'agit généralement du nom de votre entreprise), puis cliquez sur **Suivant**.
8. Sur la page **Entrez le numéro de téléphone à composer**, entrez le numéro de téléphone de la connexion, puis cliquez sur **Suivant**.
9. Sur la page **Disponibilité de connexion**, sélectionnez **Tous les utilisateurs** ou **Mon utilisation uniquement**, puis cliquez sur **Suivant**.
10. Sur la page **Fin de l'Assistant Nouvelle connexion**, cliquez sur **Terminer**.

4. Configuration d'une connexion sans fil

Microsoft Windows XP et Windows Server 2003 offrent une prise en charge étendue de la technologie réseau sans fil afin d'accepter les périphériques sans fil sur le réseau d'entreprise.
La technologie utilisée sur un réseau sans fil permet à plusieurs périphériques de communiquer au moyen de protocoles réseau standard et d'ondes électromagnétiques (et non de câbles réseau) afin de transporter des signaux sur toute ou une partie de l'infrastructure réseau. Parmi les dispositifs utilisés couramment dans le cadre des réseaux sans fil, citons les ordinateurs portables, les ordinateurs de poche, les assistants numériques (PDA), les téléphones cellulaires, les ordinateurs à stylet et les récepteurs de radiomessagerie.
Vous pouvez utiliser un réseau local sans fil (WLAN) dans des bureaux provisoires ou d'autres endroits où l'installation de câbles serait trop onéreuse, ou pour compléter un LAN existant afin de permettre aux utilisateurs de travailler en différents endroits d'un bâtiment à divers moments. Les utilisateurs mobiles peuvent employer des téléphones cellulaires, des assistants numériques (PDA), des ordinateurs portables ou d'autres périphériques pour accéder à la messagerie électronique. Les personnes qui voyagent et qui sont munies d'ordinateurs portables peuvent se connecter à Internet par le biais de stations de base installées dans des aéroports, des gares et d'autres lieux publics.

Un réseau WLAN fonctionne selon deux modes différents, définis par la norme IEEE (Institute of Electrical and Electronics Engineers) 802.11 :

- *Infrastructure à points d'accès*. Les stations sans fil (périphériques aveccartes réseau radio ou modems externes) se connectent aux points d'accès sans fil qui fonctionnent comme des ponts entre les stations et le segment principal du réseau existant. Ainsi, les utilisateurs sans fil au sein d'une entreprise ou d'un bâtiment de campus peuvent-ils accéder aux ressources réseau comme s'ils se connectaient normalement au réseau.
- *Égal à égal (ad hoc)*. Dans un réseau d'égal à égal, les clients sans fil communiquent directement entre eux sans utiliser de câbles. Ainsi, plusieurs utilisateurs situés dans une zone limitée, telle qu'une salle de conférence, peuvent-ils former un réseau provisoire sans utiliser de points d'accès. Bien qu'ils puissent communiquer et partager des ressources, il leur est impossible d'accéder aux ressources réseau qui ne font pas partie de ce réseau d'égal à égal.

4.1. Composants d'une connexion sans fil

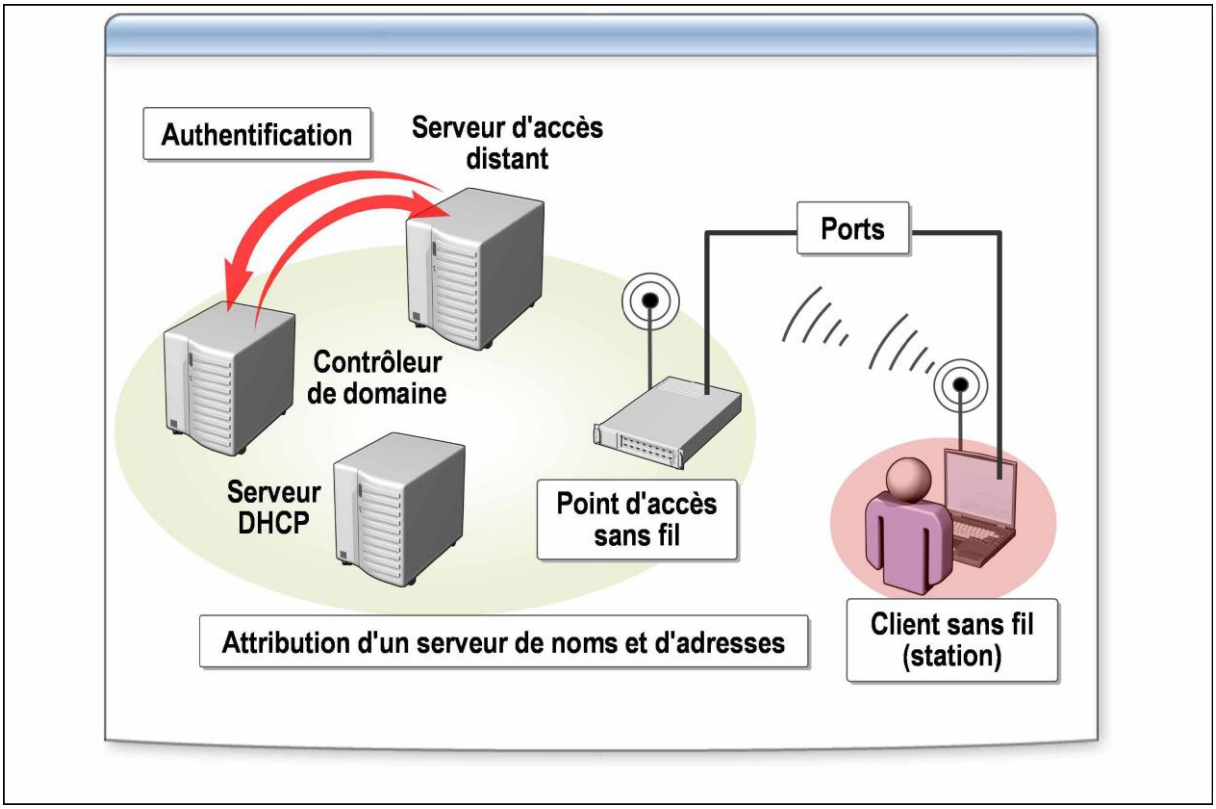
Un réseau local sans fil (WLAN) est constitué des composants suivants :

- *Client sans fil (station)*. Une station est un périphérique informatique équipé d'une carte réseau sans fil. Un ordinateur personnel équipé d'une carte réseau sans fil est désigné sous le nom de client sans fil. Les clients sans fil peuvent communiquer directement entre eux ou par le biais d'un point d'accès sans fil.
- *Point d'accès sans fil*. Un point d'accès sans fil est un périphérique réseau équipé d'une carte réseau sans fil qui fait office de pont entre les stations et un réseau câblé traditionnel. Un point d'accès comprend les éléments suivants :

• Au moins une interface qui connecte le point d'accès à un réseau câblé existant (un segment Ethernet, par exemple).

• Un équipement radio au moyen duquel il établit une connexion sans fil à des clients sans fil.
• Un logiciel de pontage IEEE 802.1D lui permettant de faire office de pont transparent entre les réseaux sans fil et câblés.

- *Ports*. Un port est le canal d'un périphérique capable de gérer une seule connexion point à point. Un client sans fil standard équipé d'une seule carte réseau sans fil possède un seul port et peut gérer une seule connexion sans fil. Un point d'accès sans fil type possède plusieurs ports et peut prendre en charge plusieurs connexions sans fil simultanées.
- *Authentification*. Le service Routage et accès distant fournit des services d'authentification, tels que les méthodes d'authentification 802.1x et IAS Windows Server 2003 fournit également des services personnalisables pour l'émission et la gestion de certificats qui sont utilisés dans les systèmes de sécurité logiciels employant la technologie de clé publique.
- *Attribution d'un serveur de noms et d'adresses*. Le service Routage et accès distant prend en charge les réseaux sans fil comme s'il s'agissait d'autres clients d'accès distant, tels que des clients VPN ou d'accès à distance. Ce service fournit des stratégies d'accès distant et d'allocation d'adresses IP propres aux clients réseau sans fil.



4.2. Normes sans fil

Norme	Description
802.11	• Groupe de spécifications pour les réseaux WLAN élaborées par l'IEEE • Définit la partie physique et MAC de la couche de liaison de données du modèle OSI
802.11b	• 11 Mbit/s • Bonne couverture, mais sensibilité aux interférences radio • Norme répandue auprès des utilisateurs domestiques et des petites entreprises
802.11a	• Vitesses de transmission de l'ordre de 54 Mbit/s • Permet d'optimiser les performances des applications de conférence et vidéo sur un réseau local sans fil • Fonctionnement optimal dans les zones densément peuplées • Incompatible avec les normes 802.11, 802.11b et 802.11g
802.11g	• Amélioration de la norme 802.11b, avec laquelle elle est compatible • Débit de 54 Mbit/s, mais avec une portée inférieure à la spécification 802.11b
802.1x	• Authentifie les clients avant de leur donner accès au réseau • Utilisable avec les réseaux locaux câblés ou sans fil • Investissement plus important sur le plan du matériel et de l'infrastructure

La norme 802.11, également connue sous le nom de *Wi-Fi*, regroupe un ensemble de spécifications destinées aux réseaux WLAN, élaborées par un groupe de travail de l'IEEE. 802.11 définit la partie physique et MAC (Media Access Control) de la couche de liaison de données du modèle OSI (Open Systems Interconnection). La couche MAC est la même pour toutes les normes 802.11. Cependant, l'implémentation varie en fonction de la norme.
La norme 802.11b prend en charge des débits binaires plus élevés que la spécification 802.11 d'origine. 802.11b gère deux vitesses de transmission supplémentaires, à savoir : 5,5 Mbit/s (mégabits par seconde) et 11 Mbit/s. Cette spécification offre une bonne portée, mais est sensible aux interférences radio. De nombreux fabricants commercialisent des périphériques 802.11b abordables pour le marché des réseaux domestiques et des petites entreprises. 802.11a offre des vitesses de transmission plus élevées, de l'ordre de 54 Mbits/s, moyennant toutefois une portée réduite. Cette technologie plus rapide permet d'optimiser les performances des applications de conférence et vidéo sur un réseau local sans fil. Elle utilise 12 canaux distincts qui ne se chevauchent, ce qui se traduit par un fonctionnement optimal dans les zones densément peuplées, ainsi que par une résistance accrue aux interférences et un meilleur débit. Cette technologie utilise une autre partie du spectre radioélectrique que les spécifications 802.11, 802.11b et 802.11g, ce qui empêche toute interopérabilité.
802.11g est une amélioration de la norme 802.11b, avec laquelle elle est compatible. Pour mettre à niveau la norme 802.11b vers 802.11g, une simple mise à jour du microprogramme peut se révéler nécessaire. Les vitesses de transmission prises en charge peuvent atteindre 54 Mbit/s, mais la portée est inférieure à la spécification 802.11b. À l'instar de la norme 802.11b, 802.11g est sensible aux interférences.

802.1x est une extension de la norme 802.11 qui définit une méthode d'authentification de l'accès au port avant d'autoriser l'accès au réseau. Cette spécification a été conçue pour pallier certaines des lacunes de la sécurité sans fil 802.11. Cependant, elle peut également être utilisée pour les réseaux locaux câblés. Dans le cadre de l'authentification, 802.1x peut utiliser des certificats avec EAP-TLS, des mots de passe avec EAP-MS-CHAP v2 ou encore le protocole PEAP. Le protocole PEAP peut être configuré avec la méthode TLS ou MS-CHAP v2. L'utilisation du mécanisme d'authentification PEAP-TLS est conseillée, dans la mesure où il constitue la méthode de détermination des clés et d'authentification la plus puissante. Un certificat est nécessaire sur le serveur d'accès distant pour la méthode MS-CHAP v2. Dans le cas de la méthode PEAP-TLS, des certificats sont nécessaires pour les serveurs d'accès distant et le client. La mise en .uvre de la spécification 802.1x demande un investissement sur le plan du matériel et de l'infrastructure.

4.3. Méthodes d'authentification disponibles pour les réseaux sans fil

S'agissant de l'authentification, la norme 802.11 définit des types d'authentification à clé partagée et à système ouvert. Pour la confidentialité des données, la norme 802.11 définit une clé WEP (Wired Equivalent Privacy).
La norme 802.11 ne définit, ni ne fournit de protocole de gestion des clés WEP prévoyant la détermination et le renouvellement automatiques des clés de cryptage. Il s'agit là d'une limitation des services de sécurité IEEE 802.11, notamment pour un mode d'infrastructure sans fil avec un grand nombre de clients sans fil.
Pour remédier à ce problème, il est possible d'associer un contrôle d'accès au réseau basé sur le port IEEE 802.1x à la méthode EAP-TLS pour les réseaux
IEEE 802.11. 802.1x utilise EAP comme protocole d'authentification. Le protocole EAP permet un échange de messages et l'établissement d'une conversation ouverte entre le client et le serveur lors du processus d'authentification en vue d'une négociation des protocoles d'authentification. La prise en charge offerte par la norme 802.1x pour les types de protocole EAP vous permet de choisir parmi plusieurs méthodes d'authentification pour les serveurs et clients sans fil, à savoir :

- *EAP-MS-CHAP v2*. EAP-MS-CHAP v2 effectue une authentification mutuelle. Cette méthode utilise des certificats pour l'authentification du serveur et des informations d'identification basées sur un mot de passe pour l'authentification du client.
- *EAP-TLS*. EAP-TLS effectue une authentification mutuelle. Il s'agit de la méthode la plus puissante en matière d'authentification et de détermination des clés. Elle utilise des certificats pour l'authentification du client et du serveur.
- *PEAP (Protected EAP)*. Le protocole PEAP assure une protection accrue du processus d'authentification grâce au cryptage des paquets de négociation EAP initiaux. PEAP prend en charge les méthodes EAP-TLS et EAP-MSCHAP v2.

4.4. Comment configurer le client d'accès réseau pour une connexion sans fil

Pour configurer un client d'accès réseau pour une connexion sans fil, procédez comme suit :
1. Ouvrez le dossier Connexions réseau.
2. Cliquez avec le bouton droit sur la connexion réseau sans fil appropriée, sélectionnez **Propriétés**, puis cliquez sur l'onglet **Configuration réseaux sans fil**.
3. Indiquez si vous souhaitez ajouter une nouvelle connexion réseau sans fil ou modifier ou supprimer une connexion existante, puis sélectionnez la tâche correspondante dans le tableau ci-dessous.
4. Si vous ajoutez ou modifiez une connexion réseau sans fil, cliquez sur l'onglet **Association**, puis configurez les paramètres selon vos besoins.
5. Pour configurer l'authentification 802.1x pour la connexion réseau sans fil, cliquez sur l'onglet **Authentification**, puis configurez les paramètres selon vos besoins.
6. Pour vous connecter à un réseau sans fil après avoir configuré les paramètres, cliquez sur le nom du réseau dans la section **Réseaux disponibles** de l'onglet **Réseaux sans fil**, puis sur **Configurer** et **OK**.

7. Pour modifier l'ordre dans lequel les tentatives de connexion aux réseaux favoris sont effectuées, sous **Réseaux favoris**, cliquez sur le réseau sans fil dont vous souhaitez modifier la position dans la liste, puis cliquez sur **Haut** ou **Bas**.
8. Pour mettre à jour la liste des réseaux disponibles situés à portée de votre ordinateur, cliquez sur **Actualiser**.
9. Pour vous connecter automatiquement aux réseaux disponibles qui n'apparaissent pas dans **Réseaux favoris**, cliquez sur **Avancé**, puis activez la case à cocher **Se connecter automatiquement aux réseaux non favoris**.