Configuration et résolution des problèmes d'accès à distance

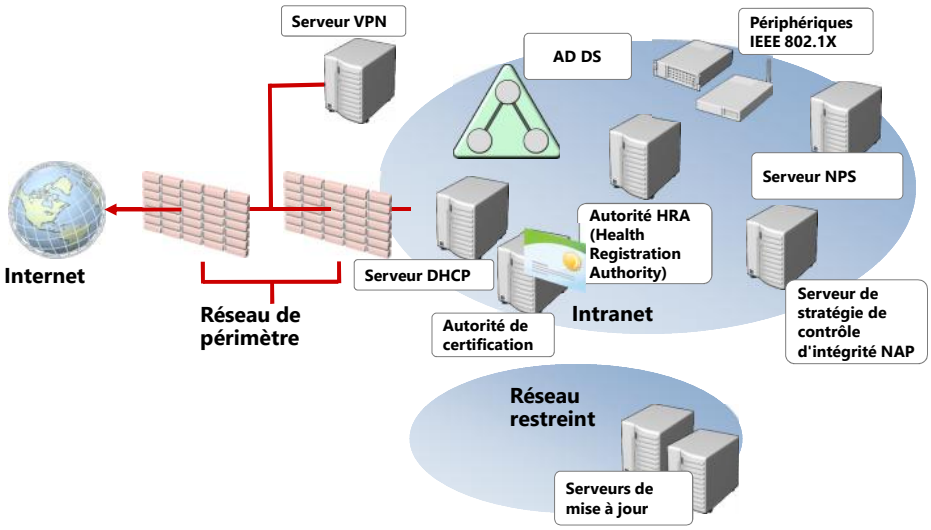
A. Maizate

ESTC-17/18

Leçon 1: Configuration de l'accès réseau

- Composants d'une infrastructure de services d'accès réseau
- Qu'est-ce que le rôle Services de stratégie et d'accès réseau ?
- Qu'est-ce que le rôle Accès à distance ?
- Authentification réseau et autorisation
- Méthodes d'authentification
- Qu'est-ce qu'une infrastructure à clé publique ?
- Intégration du protocole DHCP au service Routage et accès distant

Composants d'une infrastructure de services d'accès réseau



Qu'est-ce que le rôle Services de stratégie et d'accès réseau ?

Avec le rôle Services de stratégie et d'accès réseau, vous pouvez :

- Appliquer des stratégies de contrôle d'intégrité
- Aider à sécuriser l'accès sans fil et câblé
- Centraliser la gestion de la stratégie réseau

Qu'est-ce que le rôle Accès à distance ?

Vous pouvez utiliser le rôle d'accès à distance pour :

- Fournir aux utilisateurs distants un accès aux ressources d'un réseau privé au moyen de services VPN ou de services d'accès à distance
- Fournir des services NAT
- Fournir des services de réseau local et étendu pour connecter des segments réseau
- Activer et configurer DirectAccess

Authentification réseau et autorisation

- Authentification :
  - Vérifie les informations d'identification d'une tentative de connexion
  - Utilise un protocole d'authentification pour envoyer les informations d'identification du client d'accès à distance au serveur d'accès à distance sous la forme de texte en clair ou sous forme chiffrée
- L'autorisation :
  - Vérifie que la tentative de connexion est autorisée
  - Se produit une fois que l'authentification a réussi

Méthodes d'authentification

Protocole	Description	Niveau de sécurité
PAP	Mots de passe en clair. Généralement utilisé si le client d'accès à distance et le serveur d'accès à distance ne peuvent pas négocier une forme de validation plus sécurisée	Protocole d'authentification le moins sécurisé. N'offre aucune protection contre les attaques par relecture, l'emprunt d'identité du client distant et l'emprunt d'identité du serveur distant
CHAP	Protocole d'authentification de type demande/réponse qui utilise le schéma de hachage MD5	Sécurité accrue par rapport au protocole PAP dans le sens où le mot de passe n'est pas envoyé sur le lien PPP Une version en clair du mot de passe est requise pour valider la réponse à la demande d'accès. N'offre aucune protection contre l'emprunt d'identité du serveur distant
MS-CHAPv2	Mise à niveau du protocole MS-CHAP. Propose une authentification bidirectionnelle, également appelée authentification mutuelle. Le client d'accès à distance reçoit confirmation que le serveur d'accès à distance auquel il tente d'accéder a accès au mot de passe de l'utilisateur	Assure une plus forte sécurité que le protocole CHAP
EAP	Permet l'authentification arbitraire d'une connexion d'accès à distance en utilisant des modèles d'authentification, appelés types de protocole EAP	Offre la plus forte sécurité en proposant la plus grande flexibilité en termes de solutions d'authentification

Qu'est-ce qu'une infrastructure à clé publique ?

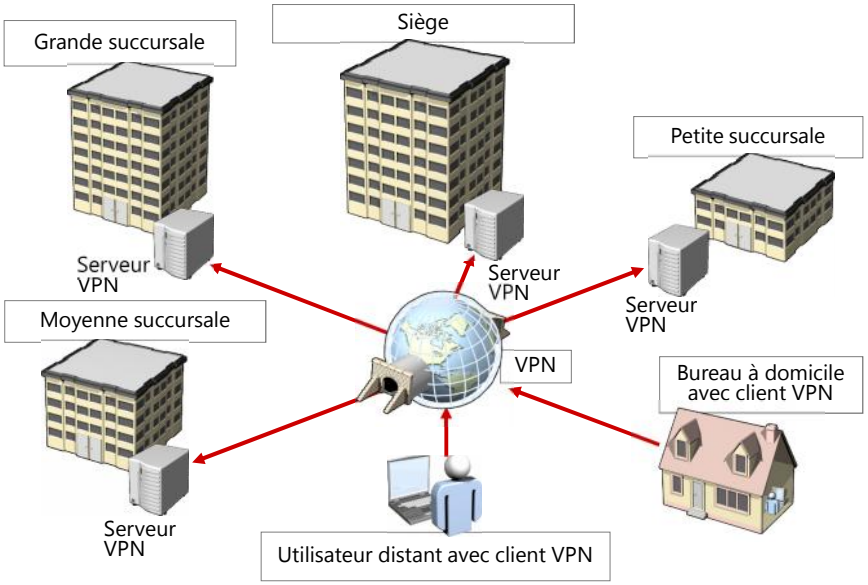
Intégration du protocole DHCP au service Routage et accès distant

- Vous pouvez fournir des configurations IP aux clients distants en utilisant l'un des deux moyens suivants :
  - Un pool statique créé sur le serveur de routage et d'accès à distance à utiliser avec les clients distants
  - Un serveur DHCP
- Les serveurs DHCP exécutant Windows Server 2012 :
  - Fournissent une classe d'utilisateur prédéfinie appelée Classe de routage et d'accès distant par défaut
  - Sont utiles pour affecter des options fournies uniquement aux clients de routage et d'accès à distance

Leçon 2: Configuration de l'accès VPN

- Qu'est-ce qu'une connexion VPN ?
- Protocoles de tunneling pour les connexions VPN
- Qu'est-ce qu'une Reconnexion VPN ?
- Configuration requise
- Démonstration : Procédure de configuration d'un accès VPN
- Réalisation de tâches de configuration supplémentaires
- Qu'est-ce que le Kit d'administration du Gestionnaire des connexions ?
- Démonstration : Procédure de création d'un profil de connexion

Qu'est-ce qu'une connexion VPN ?



Protocoles de tunneling pour les connexions VPN

- Windows Server 2012 prend en charge les protocoles de tunneling VPN suivants :
  - PPTP
  - L2TP/IPsec
  - SSTP
  - IKEv2

Qu'est-ce qu'une Reconnexion VPN ?

La reconnexion VPN maintient la connectivité lors des pannes réseau

- Reconnexion VPN :
  - Fournit une connectivité VPN transparente et cohérente
  - Utilise la technologie IKEv2
  - Rétablit automatiquement les connexions VPN quand la connectivité est disponible
  - Maintient la connexion si les utilisateurs se déplacent entre plusieurs réseaux
  - Fournit un statut de connexion transparent aux utilisateurs

Configuration requise

- La configuration requise du serveur VPN comprend les éléments suivants :
  - Deux interfaces réseau (publique et privée)
  - Allocation d'adresses IP (pool statique ou serveur DHCP)
  - Fournisseur d'authentification (serveur NPS/RADIUS ou le serveur VPN)
  - Considérations relatives à l'agent de relais DHCP
  - Appartenance au groupe Administrateurs local ou équivalent

Démonstration : Procédure de configuration d'un accès VPN

Dans cette démonstration, vous allez apprendre à :

- Configurer l'accès à distance en tant que serveur VPN
- Configurer un client VPN

Leçon 3: Configuration de DirectAccess

- Complexités liées à la gestion des connexions VPN
- Qu'est-ce que DirectAccess ?
- Composants de DirectAccess
- Qu'est-ce que la Table de stratégie de résolution de noms ?
- Fonctionnement de DirectAccess pour les clients internes
- Fonctionnement de DirectAccess pour les clients externes
- Conditions prérequises pour l'implémentation de DirectAccess
- Configuration de DirectAccess

Complexités liées à la gestion des connexions VPN

Les connexions VPN peuvent poser les problèmes suivants :

- Les utilisateurs doivent initialiser les connexions VPN
- Les connexions peuvent exiger plusieurs étapes d'initialisation
- Les pare-feu peuvent soulever d'autres considérations
- Le dépannage des connexions VPN défectueuses peut être long
- La gestion des ordinateurs disposant de connexions VPN s'avère complexe

Qu'est-ce que DirectAccess ?

Fonctionnalités de DirectAccess :

- Se connecte automatiquement au réseau d'entreprise sur le réseau public
- Utilise plusieurs protocoles, notamment HTTPS, pour établir une connectivité IPv6
- Prend en charge l'accès au serveur sélectionné et l'authentification IPsec
- Prend en charge l'authentification de bout en bout et le chiffrement
- Prend en charge la gestion des ordinateurs clients distants
- Permet la connexion directe des utilisateurs distants aux serveurs intranet

Composants de DirectAccess

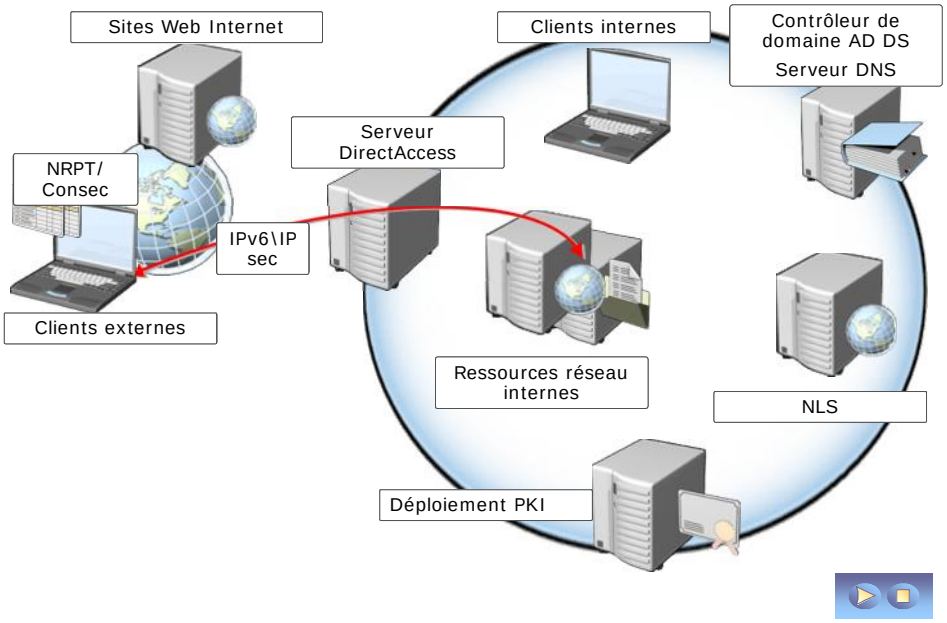


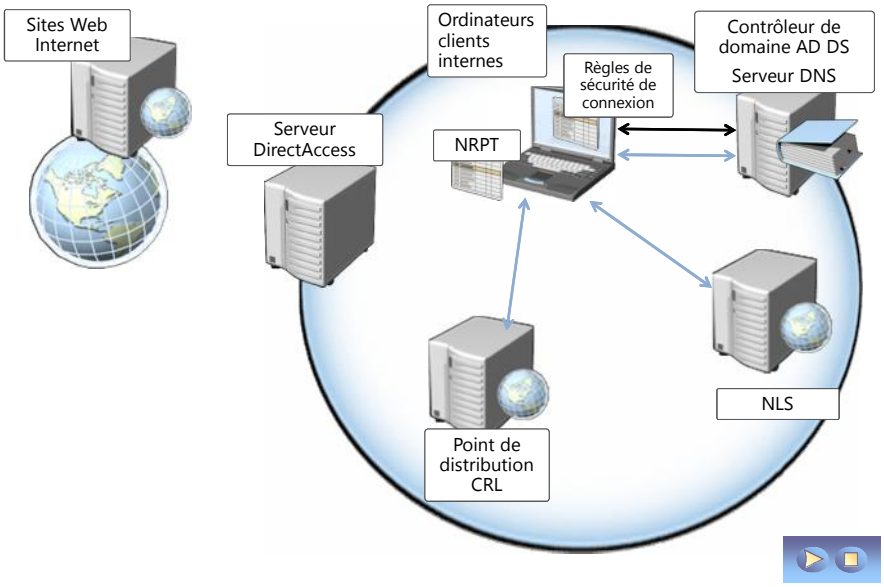
Tableau Politique de résolution de noms

Le tableau NRPT définit les serveurs DNS pour différents espaces de noms et les paramètres de sécurité correspondants ; il est utilisé avant les paramètres DNS de l'adaptateur

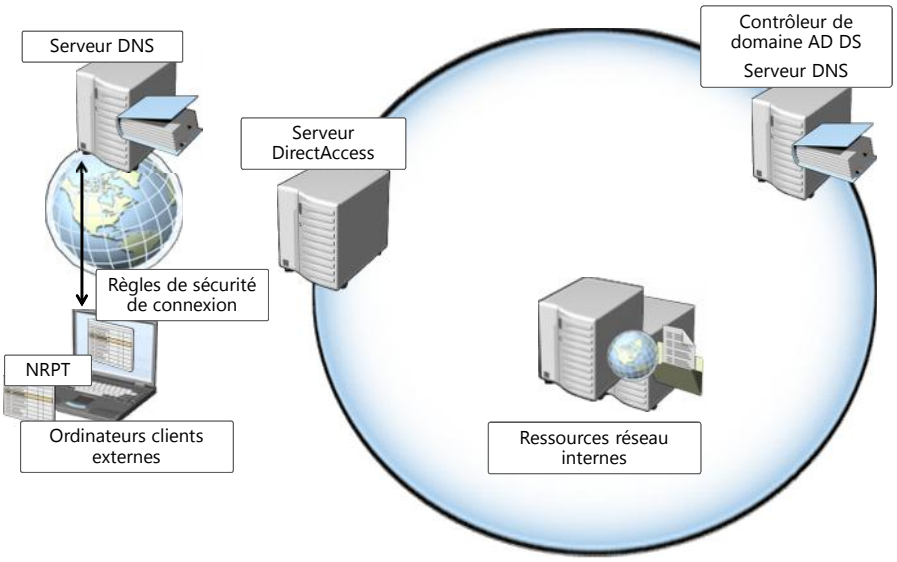
Utilisation de NRPT

- Des serveurs DNS peuvent être définis pour chaque espace de nom DNS plutôt que pour chaque interface
- Les requêtes DNS pour des espaces de noms spécifiques peuvent éventuellement être sécurisées à l'aide d'IPSec

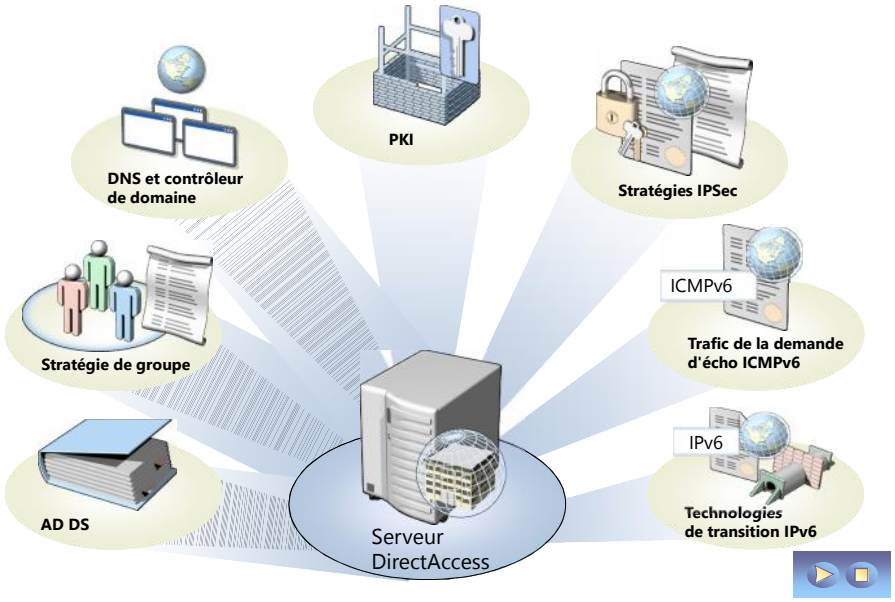
Fonctionnement de DirectAccess pour les ordinateurs clients internes



fonctionnement de DirectAccess pour les ordinateurs clients externes



Conditions prérequises pour l'implémentation de DirectAccess



Configuration de DirectAccess

Pour configurer DirectAccess :

1. Configurez le contrôleur de domaine AD DS et DNS
2. Configurez l'environnement PKI
3. Configurer le serveur DirectAccess
4. Configurez les clients DirectAccess et testez l'intranet et l'accès à Internet