Configuration de l’accès à distance

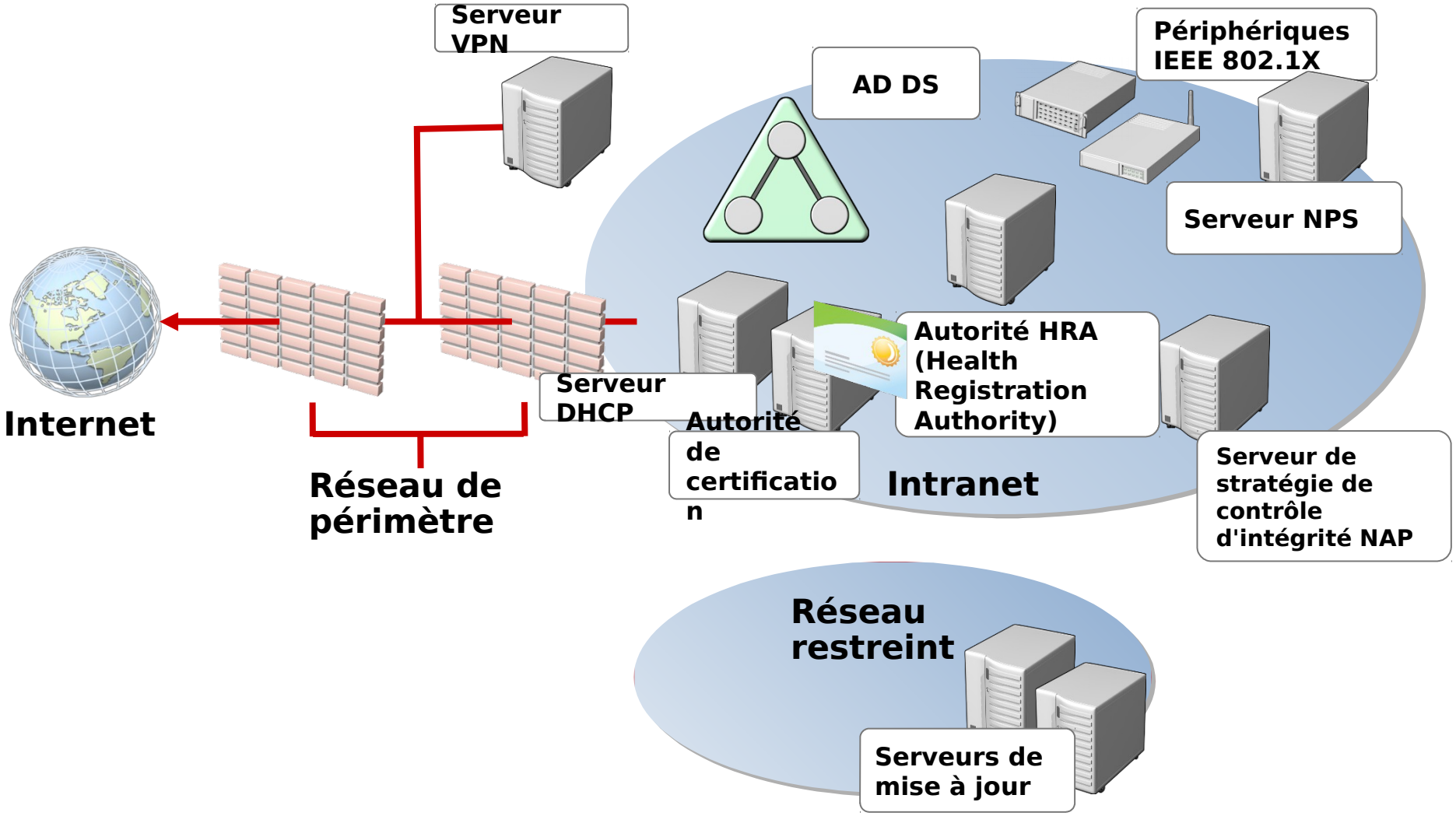
Windows 2012 Server

1. Configuration de l’accès réseau

La majorité des entreprises ont des **employers nomades**. Pour faciliter leur **connexions à distance**, vous devez mettre en œuvre des **technologies d’accès à distance** tel que :

- **VPN (réseau privé virtuel)**
  - Est une technologie permettant une **connexion sécurisée** à un **réseau d'entreprise** pour un **PC distant**,
  - La sécurité est basée sur le **cryptage** des données
- **DirectAccess**
  - Est une technologie permettant une **connectivité transparente** au r**éseau de votre organisation** à partir de tout **emplacement distant** équipé d’Internet.
  - Il diffère d’une connexion VPN puisqu’il n’y a **pas besoin d’établir une connexion** dans le gestionnaire de connexion.

1. Configuration de l'accès réseau



1. Configuration de l'accès réseau

- Une infrastructure de services d'accès réseau complète dans Windows Server 2012 inclut généralement les composants suivants:
- Serveur VPN
- AD DS et AD CS pour l'authentification par certificats
- DHCP
- NPS (Network Policy Server) fournit l'authentification pour d'autres composants d'accès réseau
- Les composants de protection réseau NAP qui est composé par le **serveur NAP** (Évalue d'integrité du système par rapport aux stratégies de contrôle d'integrité configurées), **l'autorité HRA** (Obtient des certificats d'integrité pour les clients qui passent avec succès la vérification de la stratégie de contrôle d'integrité) et **les serveurs de mise à jours** (Proposent des services de mise à jour aux clients qui ne répondent pas aux conditions d'integrité du réseau d'entreprise).

1. Configuration de l’accès réseau

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: Ces stratégies définissent les configurations requises en matière de logiciels, de matériel et de mise à jour de sécurité.
- Aider à sécuriser l'accès sans fil et câblé: l’accès sans fil sécurisé offre aux utilisateurs sans fil une méthode d’authentification facile à déployer reposant sur un certificat ou un mot de passe sécurisé.

1. Configuration de l’accès réseau

Rôle d’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 et de routage
- Activer et configurer DirectAccess

1. Configuration de l’accès réseau

Authentification réseau et autorisation

- Authentification :
  - Vérifie les informations d'identification d'une tentative de connexion par la base SAM, AD DS ou serveur RADIUS.
  - 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

1. Configuration de l’accès réseau

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.
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
MS-CHAPv2	Mise à niveau du protocole MS-CHAP. Propose une authentification bidirectionnelle, également appelée authentification mutuelle.	Assure une plus forte sécurité que le protocole CHAP
EAP	Permet l'authentification arbitraire d'une connexion d'accès à distance	Offre la plus forte sécurité en proposant la plus grande flexibilité en termes de solutions d’authentication

1. Configuration de l'accès réseau

Infrastructure à clé publique

- Une infrastructure à clé publique se compose de plusieurs composants qui permettent de sécuriser les communications et transactions de l'entreprise, notamment celles utilisées dans des scénarios d'accès à distance. Différents composants fonctionnent ensemble pour fournir une solution **PKI** complète. Les composants PKI de Windows Server 2012 sont les suivants :

- *Autorité de certification (CA)*. L'autorité de certification sont des organismes de confiance qui émet et gère les certificats numériques pour les utilisateurs, les ordinateurs et les services.
- *Certificats numériques*. Les certificats numériques s'apparentent à un passeport électronique. Un certificat numérique est utilisé pour justifier l'identité de l'utilisateur (ou de toute autre entité). Il contient des informations d'identification électroniques associées à une clé publique et à une clé privée, utilisées pour authentifier des utilisateurs et d'autres périphériques tels que des serveurs Web et des serveurs de messagerie.
- *Modèles de certificats*. Ce composant décrit le contenu ainsi que l'objectif d'un certificat numérique.

1. Configuration de l’accès réseau

Intégration du protocole DHCP au service Routage et accès distant

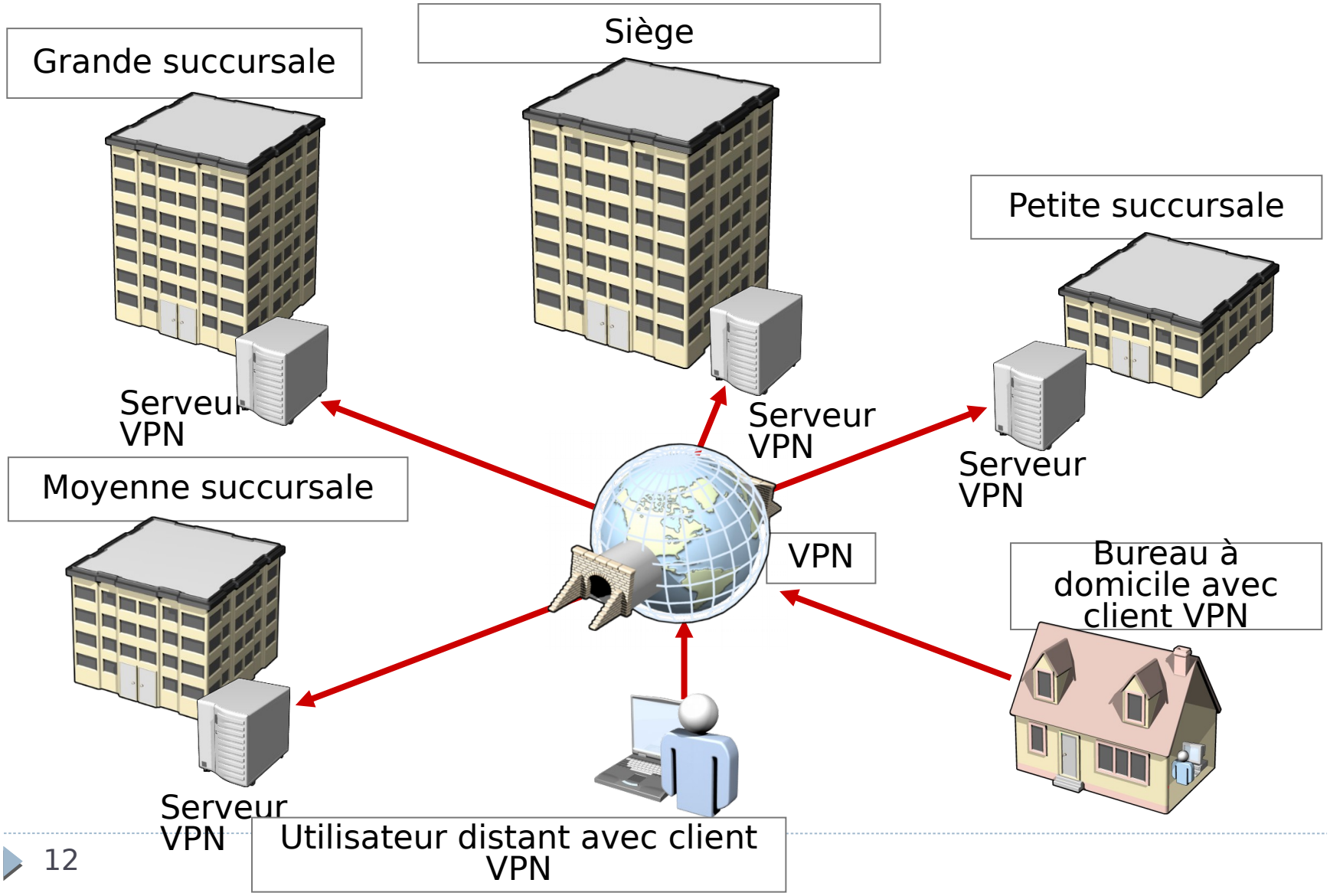
- Vous pouvez fournir des configurations IP aux clients distants en utilisant l'un des deux moyens suivants :
  - Un pool statique créé sur le serveur de routage et d'accès à distance à utiliser avec les clients distants
  - Un serveur DHCP (où le serveur accès distant reserve 10 addresses IP pour les distribuer aux clients accès distants)
- 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

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
Réalisation de tâches de configuration supplémentaires

- Qu'est-ce que le Kit d'administration du Gestionnaire des connexions ?

2. Configuration de l’accès VPN



2. Configuration de l'accès VPN

Qu'est ce qu'une connexion VPN?

- La liaison dans laquelle les données privées sont encapsulées et chiffrées est appelée *connexion VPN*.
- Il existe deux types de connexions VPN :

- **accès à distance** ;
- **de site à site**.

- Les connexions VPN qui utilisent le protocole PPTP, le protocole L2TP/IPsec ou le protocole SSTP ont les propriétés suivantes:

- Encapsulation: les données privées sont encapsulées avec un en-tête contenant les informations de routage permettant aux données d'être transmises sur le réseau de transit.
- Authentification: au niveau utilisateur à l'aide de l'authentification PPP, au niveau ordinateur à l'aide du protocole IKE (Internet Key Exchange).
- Chiffrement: Pour assurer la confidentialité des données transmises sur le réseau de transit partagé ou public avec une clé de chiffrement commune.

2. Configuration de l’accès VPN

Une reconnexion VPN

- Vous pouvez configurer la fonctionnalité Reconnexion VPN disponible dans Windows Server 2012, Windows Server 2008 R2, Windows 8 et Windows 7.
- Grâce à cette fonctionnalité, les utilisateurs peuvent accéder aux données de la société à l’aide d’une connexion VPN, qui se reconnectera automatiquement en cas d’interruption de la connectivité. La Reconnexion VPN permet également le déplacement entre différents réseaux surtout pour les réseaux sans fils.
- La Reconnexion VPN utilise la technologie IKEv2 pour fournir une connectivité VPN transparente et cohérente.

2. Configuration de l’accès VPN

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

2. Configuration de l’accès VPN

Kit d’administration de gestionnaire des connexions

La console CMAK :

- Vous permet de personnaliser l'expérience de connexion à distance des utilisateurs en créant des connexions prédéfinies sur les serveurs et les réseaux à distance
- L’Assistant Kit d’administration du Gestionnaire des connexions crée un fichier exécutable que vous pouvez distribuer de différentes manières ou intégrer dans l’image du système d’exploitation qui peut être exécuté sur un ordinateur client pour établir une connexion réseau que vous avez designée
- Le Kit d’administration du Gestionnaire des connexions est un composant facultatif qui n’est pas installé par défaut.
- Réduit les demandes adressées à l'assistance technique concernant la configuration des connexions d'accès à distance en :
  - Facilitant la résolution des problèmes dans la mesure où la configuration est connue
  - Réduisant les risques d'erreur des utilisateurs lors de la configuration de leurs propres objets de connexion

3. Configuration de DirectAccess

Complexités liées à la gestion des connexions VPN
Qu'est-ce que DirectAccess ?

- Composants de DirectAccess

3. Configuration de DirectAccess

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 bloquer les connexions VPN s’ils sont mal configurés
- Le dépannage des connexions VPN défectueuses peut être long
- La gestion des ordinateurs disposant de connexions VPN s'avère complexe

3. Configuration de DirectAccess

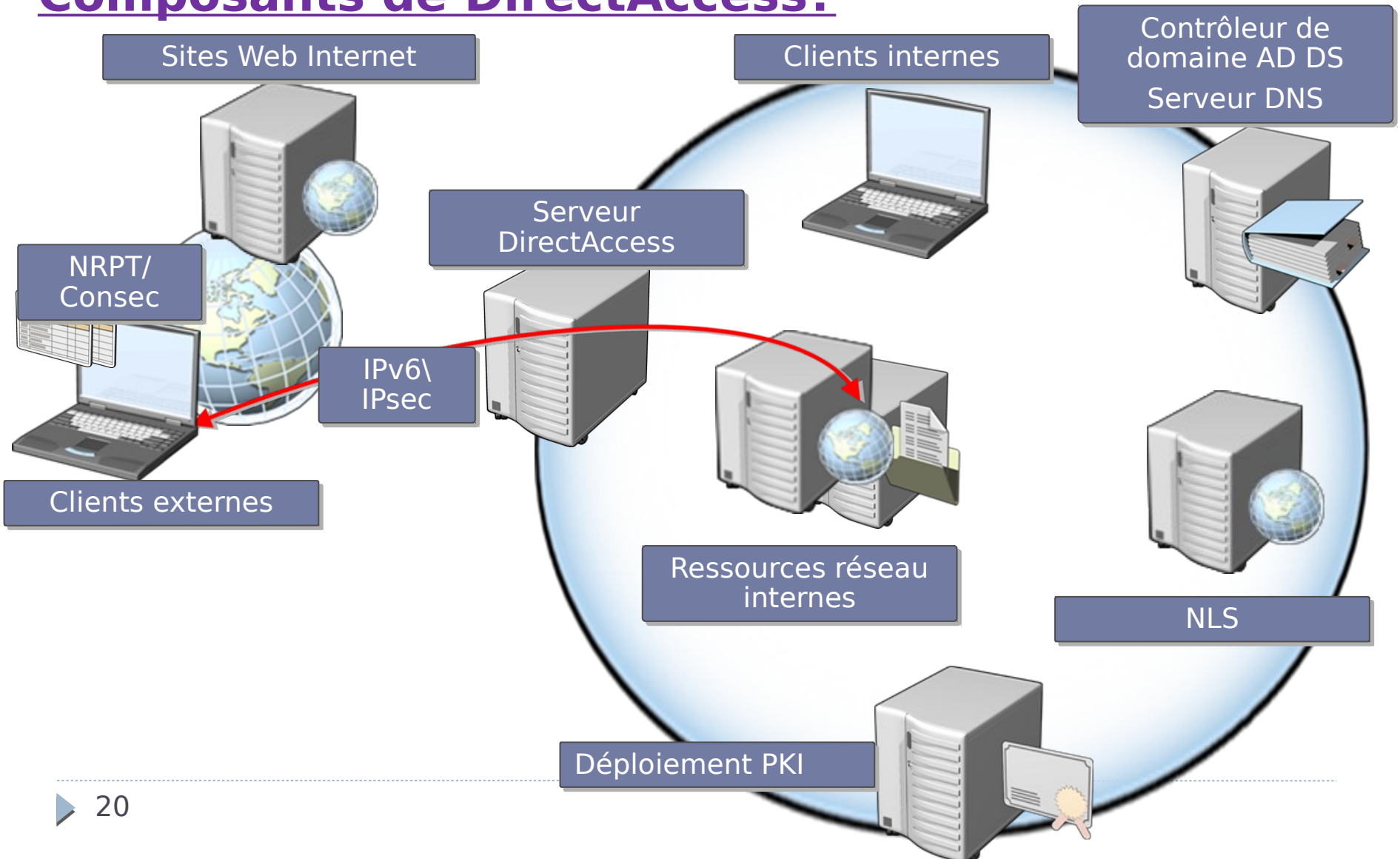
Qu’est ce que DirectAccess?

La fonctionnalité DirectAccess dans Windows Server 2012 active l’accès à distance transparent aux ressources intranet sans établir de connexion VPN au préalable. Ses Fonctionnalités :

- 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

3. Configuration de DirectAccess

Composants de DirectAccess?



3. Configuration de DirectAccess

- Pour déployer et configurer DirectAccess, votre organisation doit prendre en charge les composants d'infrastructure suivants:
- Serveur DirectAccess: il accepte les connexions à partir des clients DirectAccess et établit la communication avec les ressources intranet, il fournit les services d'authentification pour les clients DirectAccess et agit comme point de terminaison de mode de tunnel IPsec pour le trafic externe.
- Client DirectAccess: Les clients DirectAccess peuvent être tout ordinateur connecté à un domaine fonctionnant sous Windows 8 Enterprise, Windows 7 Enterprise ou Windows 7 Ultimate.
- Serveur d'emplacement réseau (NLS): Les clients DirectAccess utilisent le serveur NLS pour déterminer leur emplacement. Si l'ordinateur client peut se connecter avec HTTPS, il suppose alors qu'il est sur l'intranet et il désactive les composants DirectAccess, sinon alors il est sur l'internet. Il est installé Avec le rôle serveur web.
- Ressources internes: Vous pouvez configurer n'importe quelle application compatible avec IPv6 qui s'exécute sur les serveurs internes ou les ordinateurs clients de manière à la rendre disponible pour les clients DirectAccess.

3. Configuration de DirectAccess

- Domaine Active Directory: Vous devez déployer au moins un domaine Active Directory doté, au minimum, du niveau fonctionnel du domaine Windows Server 2003.
- GPO: La stratégie de groupe est nécessaire à l'administration centralisée et au déploiement des paramètres DirectAccess.
- PKI: Le déploiement de l'infrastructure PKI est facultatif pour la configuration et la gestion simplifiées.
- DNS: Lorsque le protocole **ISATAP** (est un mécanisme de transition de IPv4 vers IPv6) est exécuté, vous devez utiliser au moins Windows Server 2008 R2 ou plus récent, ou un serveur DNS non-Microsoft qui prend en charge les échanges de messages DNS sur le protocole ISATAP.
- Serveur NAP: La protection d'accès réseau (**NAP**) est un composant facultatif qui permet d'effectuer un contrôle de conformité et d'appliquer la stratégie de sécurité pour les clients DirectAccess sur Internet.