Microsoft® Official Course

Module 7

Configuration et résolution des problèmes d'accès à distance

Microsoft

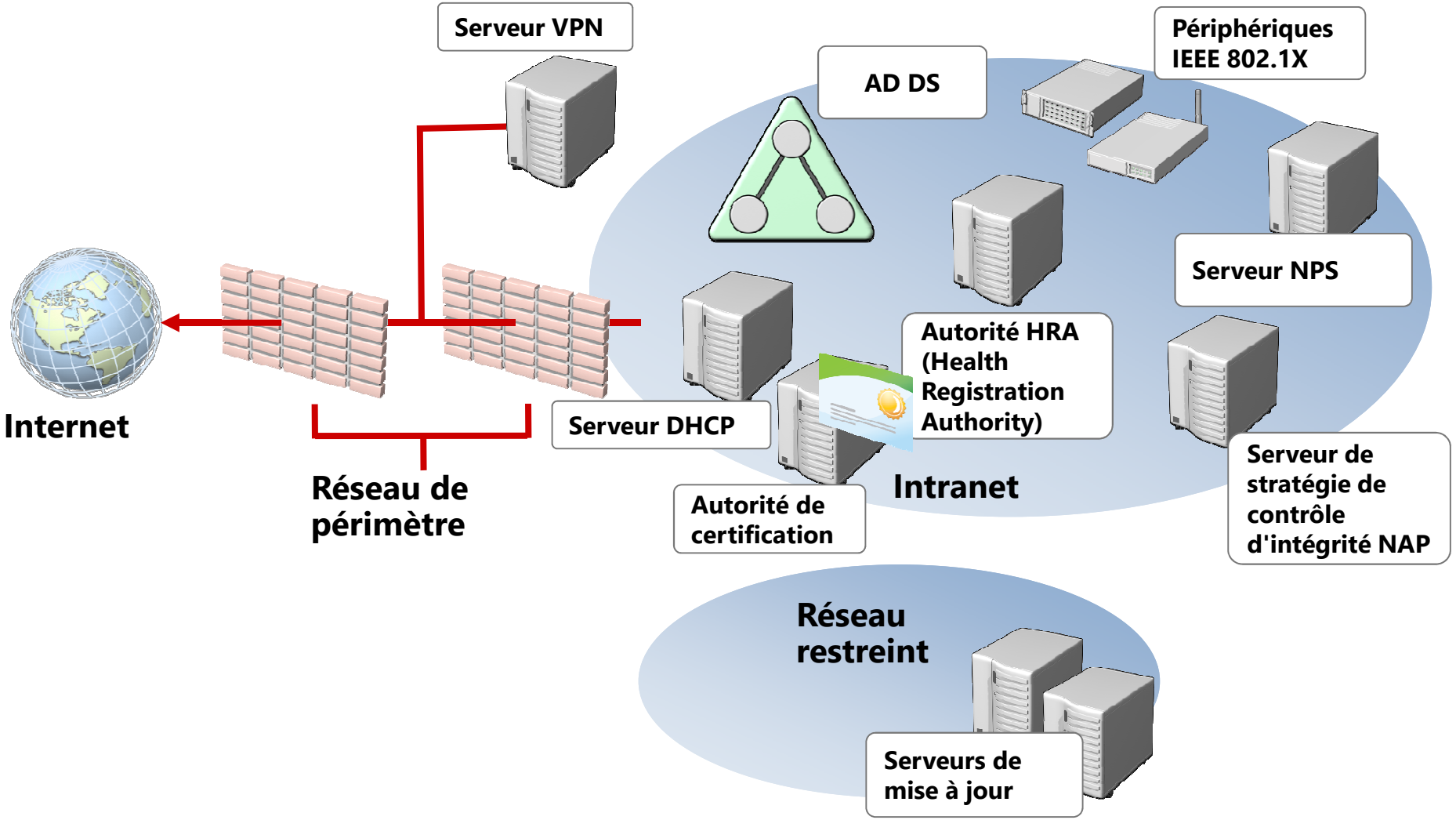
Vue d'ensemble du module

- Configuration de l'accès réseau
- Configuration de l'accès VPN
- Vue d'ensemble des stratégies réseau
- Résolution des problèmes du service de routage et d'accès à distance
- Configuration de DirectAccess

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 ?

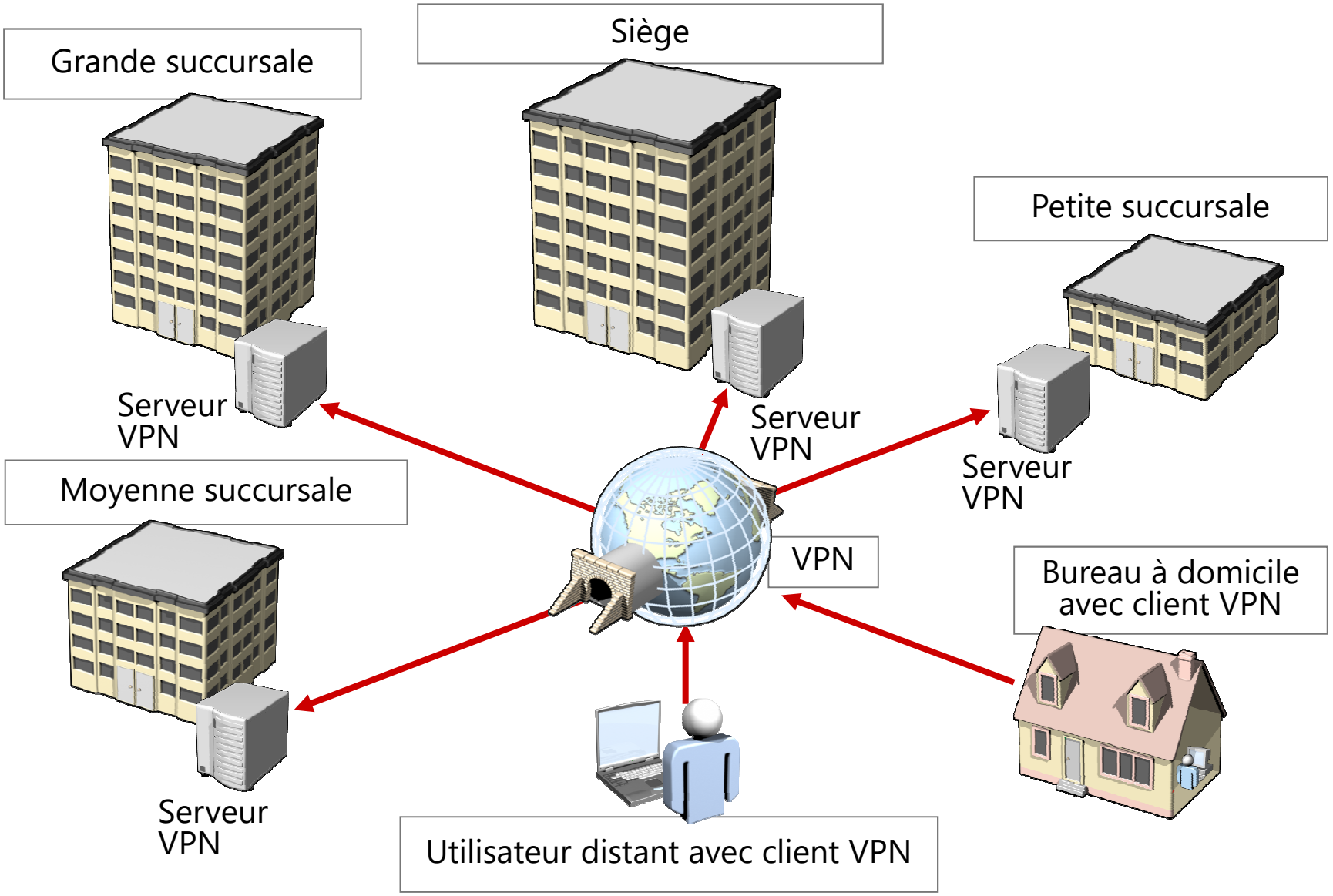
Intégration du protocole DHCP au service Routage et accès distant

- 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

Réalisation de tâches de configuration supplémentaires

Vous pourriez devoir effectuer des étapes supplémentaires pour aider à sécuriser l'installation de l'accès à distance :

- Configurer des filtres de paquets statiques
- Configurer des services et des ports
- Ajuster les niveaux d'enregistrement pour les protocoles de routage
- Configurer le nombre de ports VPN
- Créer un profil Gestionnaire de connexions pour les utilisateurs
- Ajouter les services de certificats
- Renforcer la sécurité de l'accès à distance
- Renforcer la sécurité VPN
- Implémenter la fonctionnalité Reconnexion VPN

Qu'est-ce que le Kit d'administration du 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
- Crée un fichier exécutable qui peut être exécuté sur un ordinateur client pour établir une connexion réseau que vous avez désignée
- 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

Démonstration : Procédure de création d'un profil de connexion

Dans cette démonstration, vous allez apprendre à :

- Installer les services CMAK
- Créer un profil de connexion
- Examiner le profil

Leçon 3: Vue d'ensemble des stratégies réseau

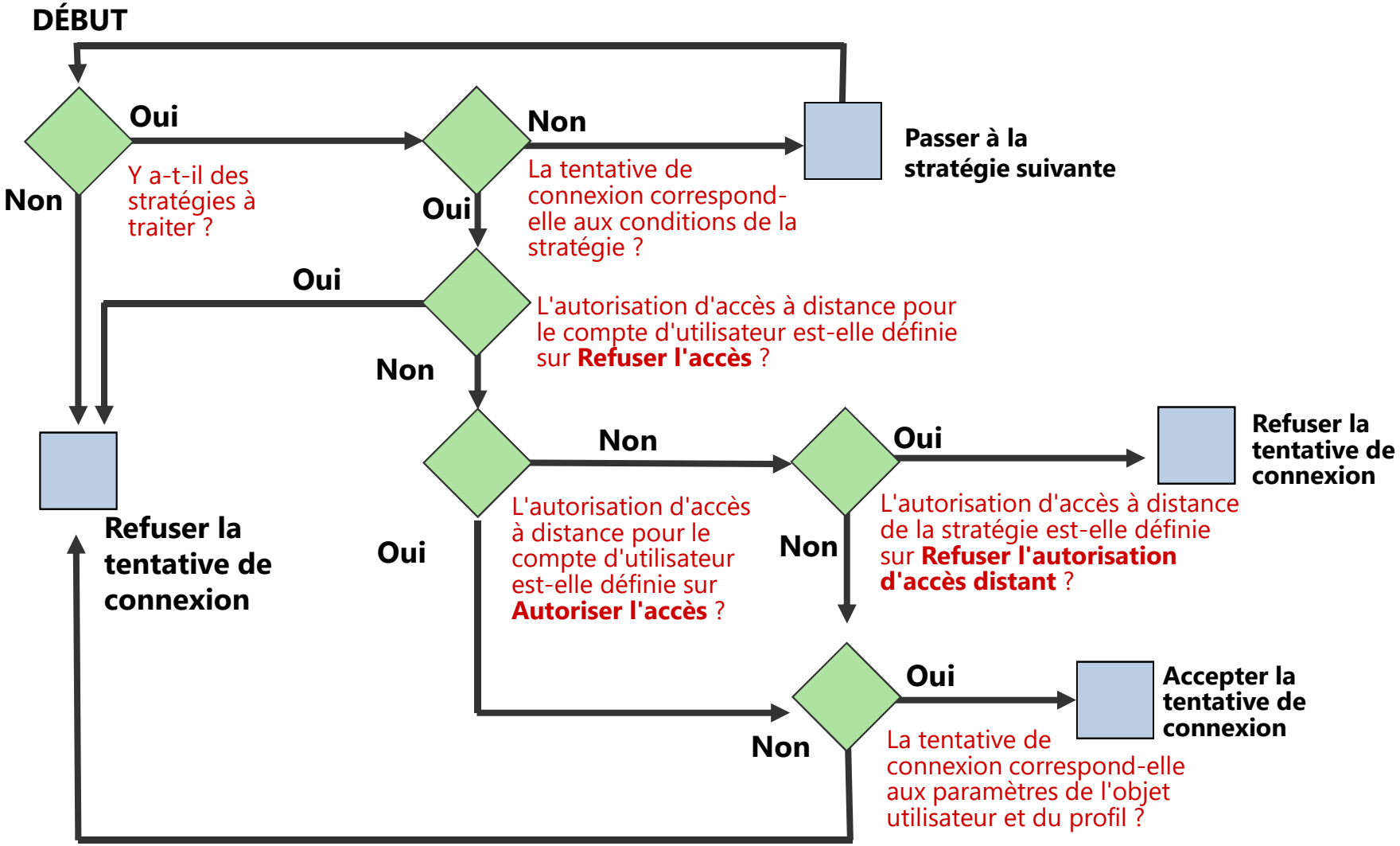
- Qu'est-ce qu'une stratégie réseau ?
- Traitement des stratégies réseau
- Processus de création et de configuration d'une stratégie réseau
- Démonstration : Procédure de création d'une stratégie réseau

Qu'est-ce qu'une stratégie réseau ?

Une stratégie réseau comporte les éléments suivants :

- Conditions
- Contraintes
- Paramètres

Traitement des stratégies réseau



Processus de création et de configuration d'une stratégie réseau

Pour créer une stratégie réseau :

- Déterminez l'autorisation par utilisateur ou groupe
- Déterminez les paramètres appropriés pour les autorisations d'accès réseau du compte d'utilisateur

Pour configurer l'assistant Nouvelle stratégie réseau :

- Configurez les conditions de la stratégie réseau
- Configurez les contraintes de la stratégie réseau
- Configurez les paramètres de la stratégie réseau

Démonstration : Procédure de création d'une stratégie réseau

Dans cette démonstration, vous allez apprendre à :

- Créer une stratégie VPN basée sur la condition Groupes Windows
- Tester le VPN

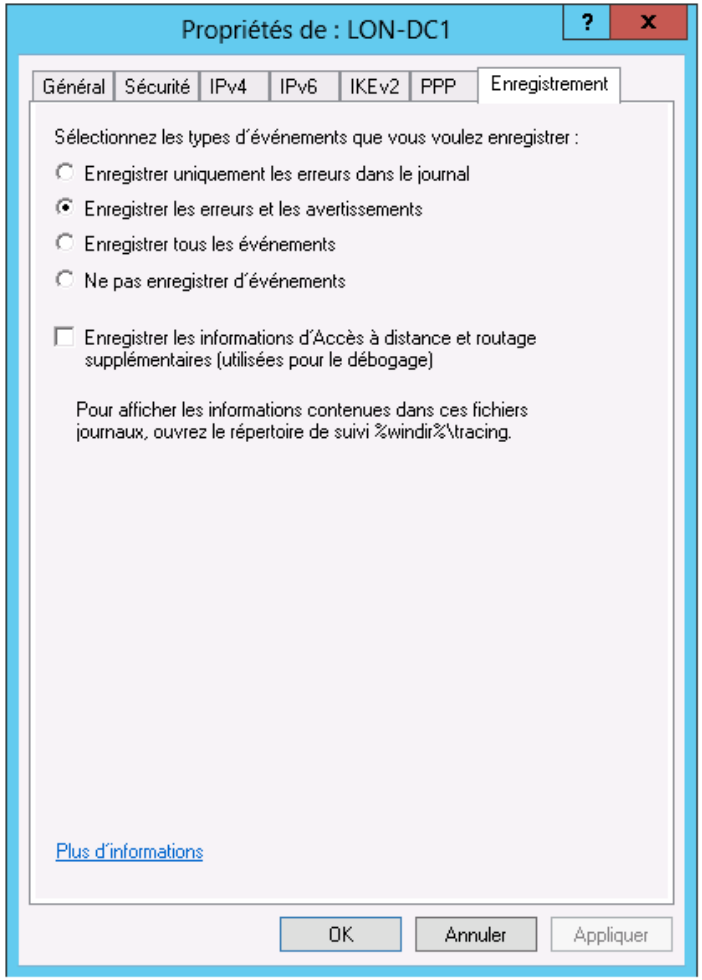
Leçon 4: Résolution des problèmes du service de routage et d'accès à distance

- Configuration de l'enregistrement des connexions d'accès à distance
- Configuration du suivi de l'accès à distance
- Résolution des problèmes VPN généraux
- Dépannage des autres problèmes

Configuration de l'enregistrement des connexions d'accès à distance

Vous pouvez configurer l'enregistrement des connexions à distance de manière à :

- Enregistrer uniquement les erreurs dans le journal
- Enregistrer les erreurs et les avertissements
- Enregistrer tous les événements
- Ne pas enregistrer d'événements
- Enregistrer les informations d'Accès à distance et routage supplémentaires



Configuration du suivi de l'accès à distance

- Vous pouvez configurer le suivi de l'accès à distance en utilisant :
  - La commande Netsh :

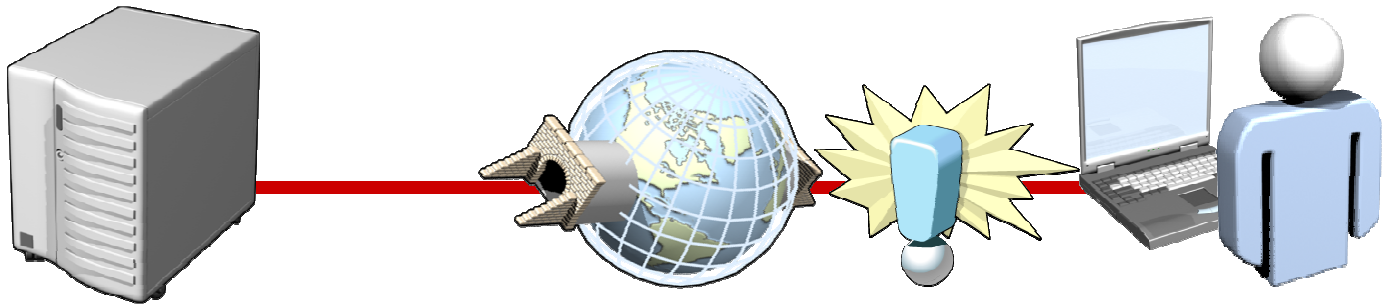
    Netsh ras diagnostics set rastracing * enabled
    (active le suivi sur tous les composants dans Accès à distance)
  - Le Registre :

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing

Le suivi utilise des ressources, vous ne devez donc l'utiliser que pour le dépannage, puis le désactiver

Résolution des problèmes VPN généraux

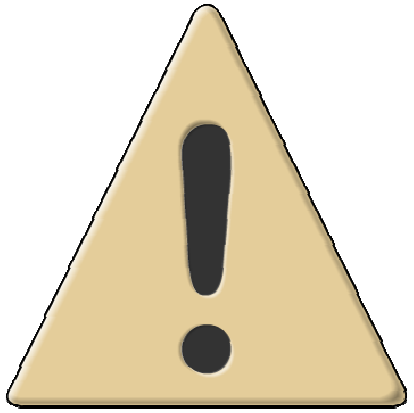
- Vérifier le nom d'hôte
- Vérifier les informations d'identification
- Vérifier le compte d'utilisateur
- Réinitialiser le mot de passe
- Vérifier que le compte d'utilisateur n'a pas été verrouillé
- Vérifier que la fonction Routage et accès distant s'exécute
- Vérifier que le serveur VPN est activé pour l'accès à distance
- Vérifier les protocoles Miniport WAN
- Vérifier la présence d'une méthode d'authentification commune
- Vérifier la présence d'au moins un niveau de chiffrement commun
- Vérifier les paramètres de la connexion



Dépannage des autres problèmes

Exemples de problèmes communs concernant l'accès à distance :

- Erreur 800 : Le serveur VPN est inaccessible
- Erreur 721 : L'ordinateur distant ne répond pas
- Erreur 741/742 : incompatibilité de chiffrement
- Problèmes L2TP/IPsec
- Problèmes EAP-TLS



Atelier pratique A : Configuration de l'accès à distance

- Exercice 1 : Configuration d'un serveur de réseau privé virtuel
- Exercice 2 : Configuration de clients VPN

Informations d'ouverture de session :

Ordinateurs virtuels:	22411B-LON-DC1
	22411B-LON-RTR
	22411B-LON-CL2
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe :	**Pa$$w0rd**

Durée approximative : 30 minutes

Scénario de l'atelier pratique A

A. Datum Corporation souhaite implémenter une solution d'accès à distance pour ses employés afin qu'ils puissent se connecter au réseau d'entreprise en dehors du bureau. Vous devez activer et configurer les services de serveur nécessaires pour établir cet accès à distance. Pour que la solution VPN soit prise en charge, vous devez configurer une stratégie réseau qui reflète la stratégie de connexion à distance de l'entreprise. Pour le pilote, seul le groupe de sécurité informatique doit pouvoir utiliser la solution VPN. Les conditions requises comprennent le besoin d'un certificat client ; les heures de connexion sont fixées à tout moment, du lundi au vendredi uniquement

Questions de révision

- Si vous utilisez la solution alternative, combien d'adresses sont allouées au serveur VPN simultanément ?
- Lors de l'atelier, vous avez configuré une condition de stratégie de type tunnel et une contrainte de restriction relative aux jours et aux heures. S'il y avait deux stratégies (celle créée ainsi qu'une stratégie supplémentaire spécifiant une condition d'appartenance au groupe Admins du domaine et des contraintes de type tunnel (PPTP ou L2TP)), pour quelle raison vos administrateurs seraient-ils dans l'incapacité de se connecter en dehors des heures de bureau ?

Leçon 5: 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

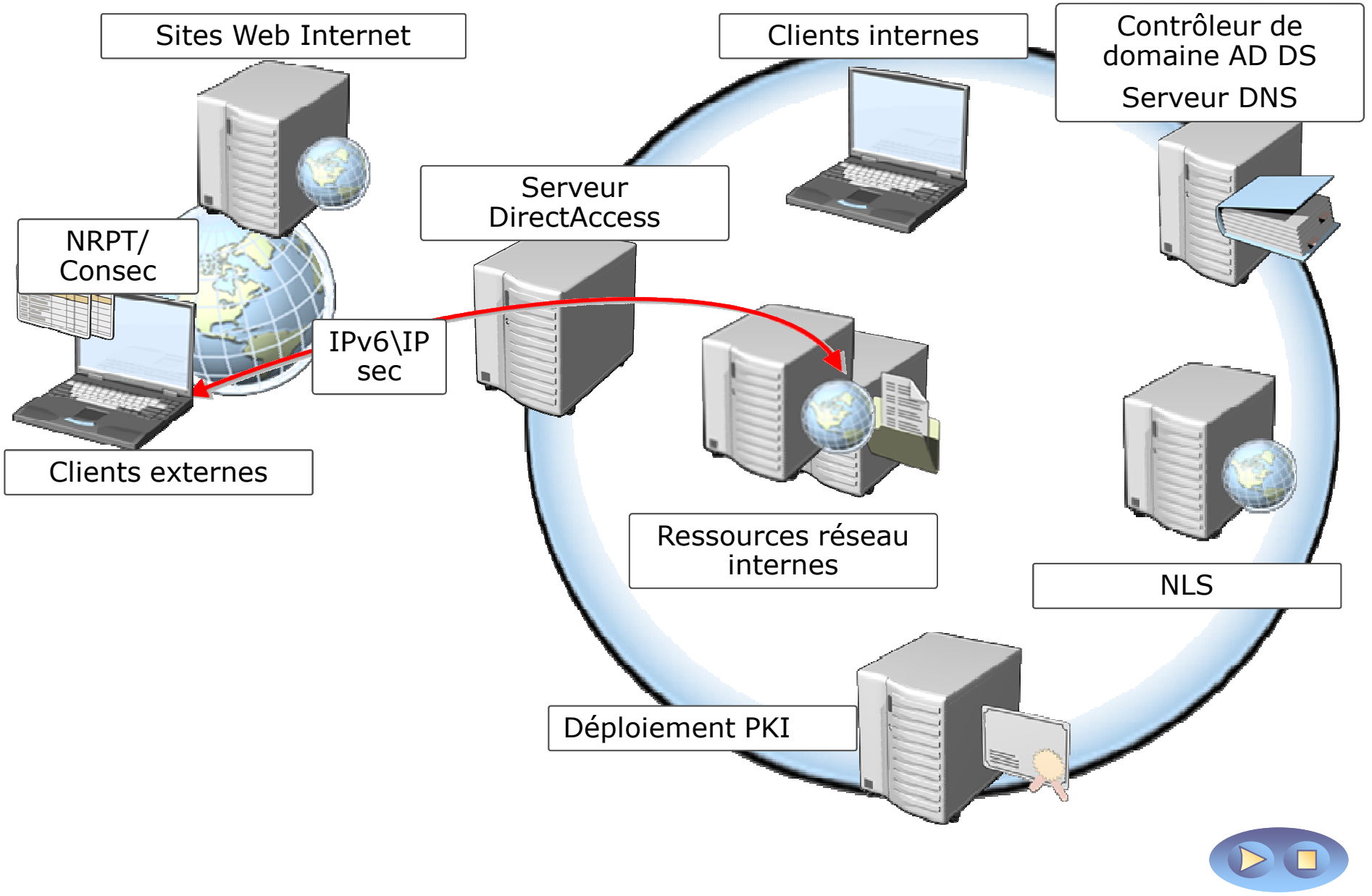
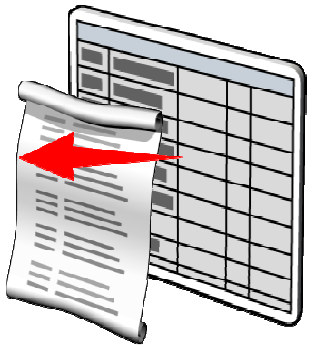


Tableau Politique de résolution de noms

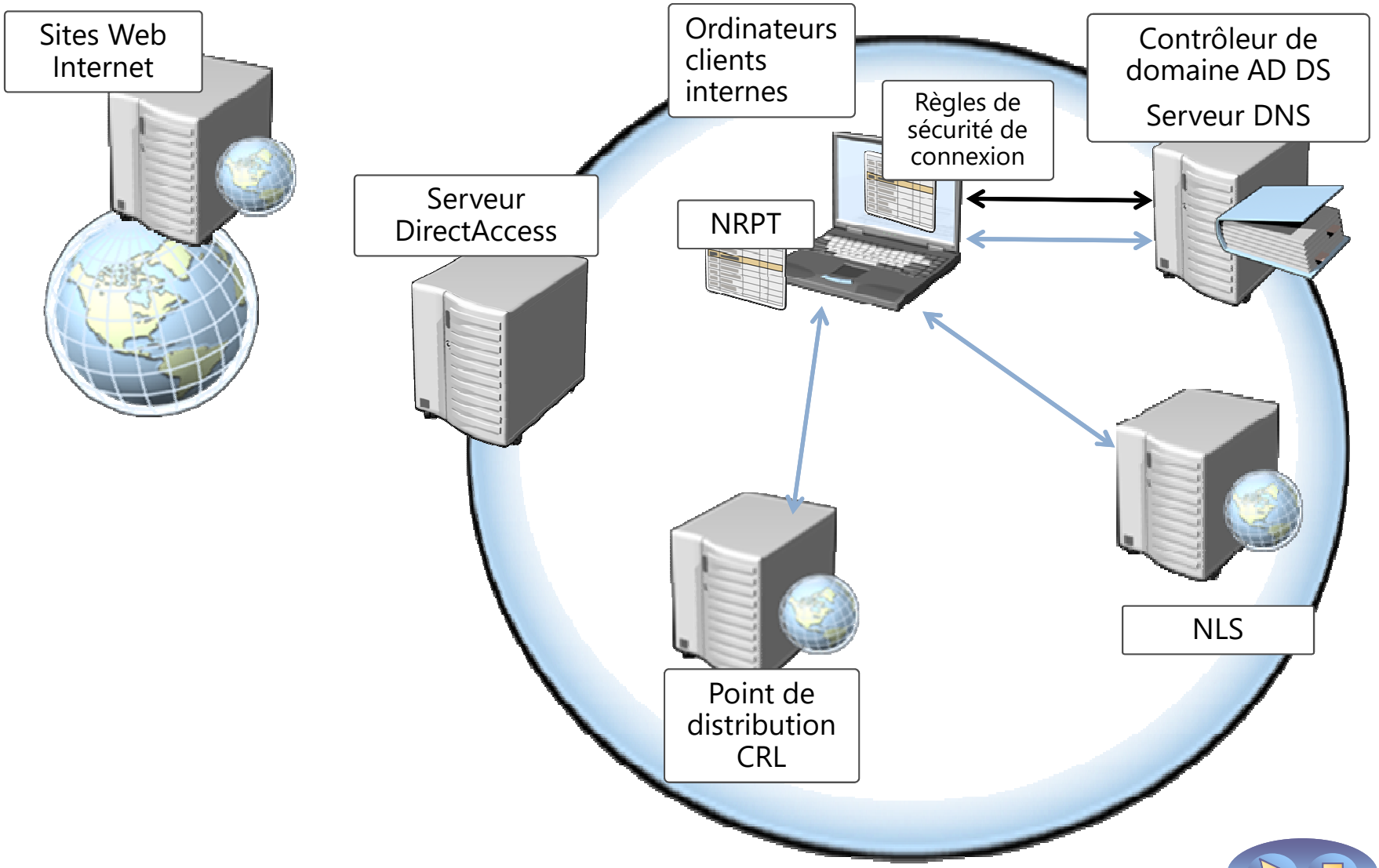
Le tableau NRPT définit les serveurs DNS pour différents espaces de noms et les paramètres de sécurité correspondants ; il est utilisé avant les paramètres DNS de l'adaptateur

Utilisation de NRPT

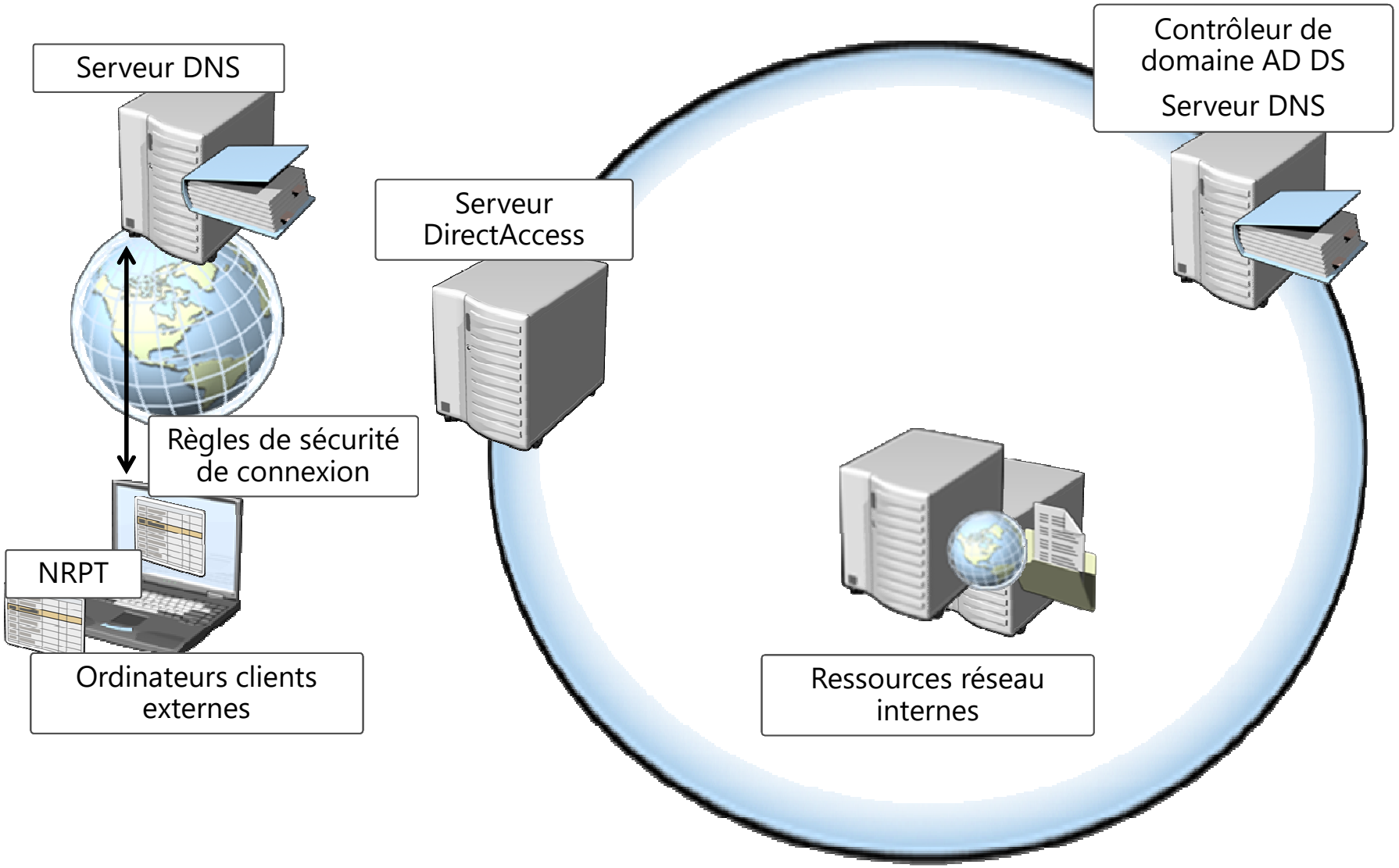
- Des serveurs DNS peuvent être définis pour chaque espace de nom DNS plutôt que pour chaque interface
- Les requêtes DNS pour des espaces de noms spécifiques peuvent éventuellement
  être sécurisées à l'aide d'IPSec



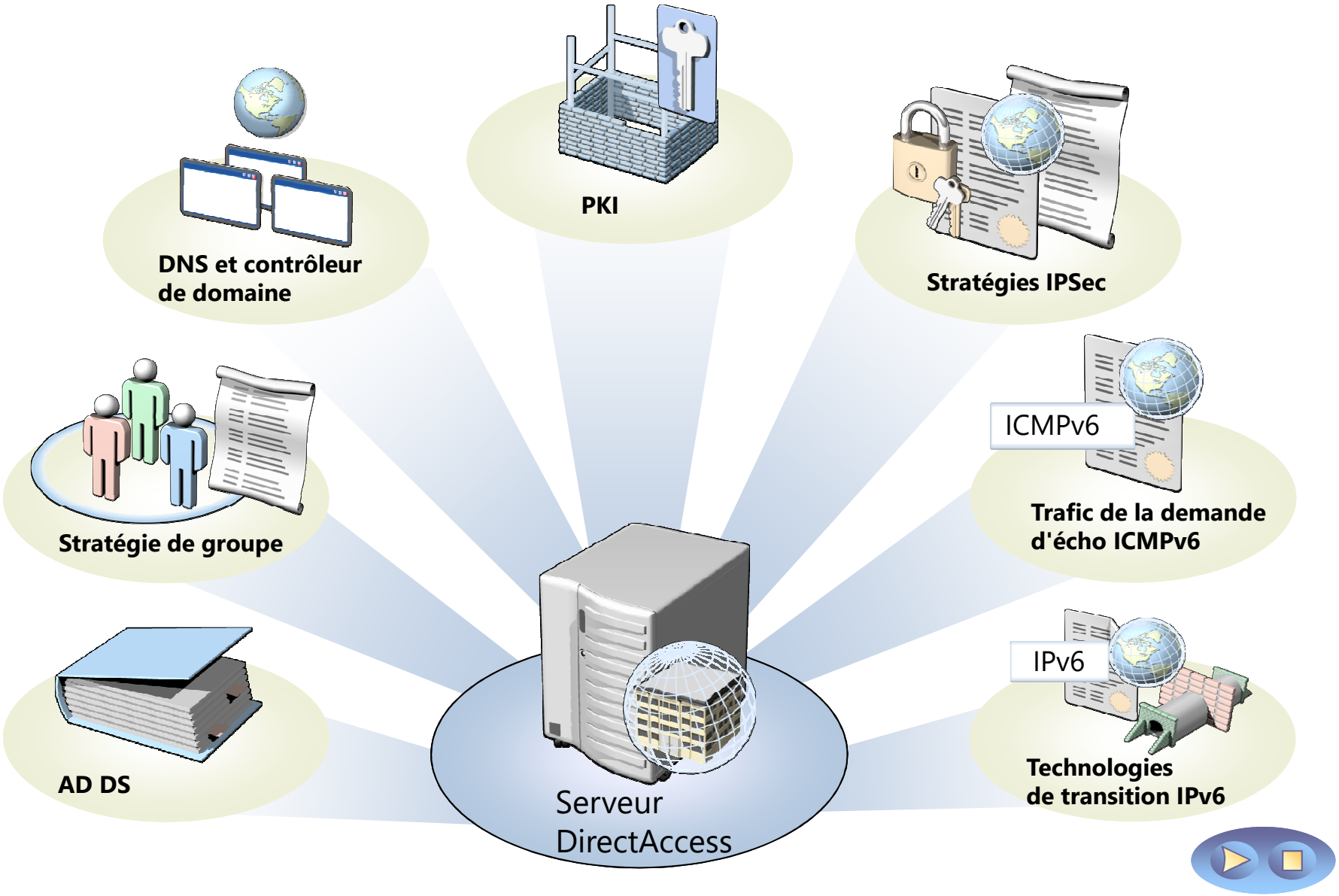
Fonctionnement de DirectAccess pour les ordinateurs clients internes



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

Atelier pratique B : Configuration de DirectAccess

- Exercice 1 : Configuration de l'infrastructure DirectAccess
- Exercice 2 : Configuration des clients DirectAccess
- Exercice 3 : Vérification de la configuration DirectAccess

Informations d'ouverture de session

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-SVR1 22411B-LON-RTR 22411B-LON-CL1
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Durée approximative : 90 minutes

Scénario d'atelier pratique

Puisque A. Datum Corporation s'est développée, plusieurs employés sont maintenant fréquemment hors du bureau, travaillant depuis leur domicile ou en voyageant. A. Datum souhaite implémenter une solution d'accès à distance pour ses employés afin qu'ils puissent se connecter au réseau d'entreprise tout en étant en dehors du bureau. Bien que la solution VPN implémentée fournisse un haut niveau de sécurité, la gestion d'entreprise est préoccupée par la complexité de l'environnement pour les utilisateurs finaux. En outre, les responsables informatiques sont également préoccupés par le fait de ne pas être en mesure de gérer efficacement les clients distants. Pour aborder ces problèmes, A. Datum a décidé d'implémenter DirectAccess en fonction des ordinateurs clients exécutant Windows 8

En tant qu'administrateur réseau senior, vous devez déployer et valider le déploiement DirectAccess. Vous configurerez l'environnement DirectAccess et validerez que les ordinateurs clients peuvent se connecter au réseau interne en fonctionnant à distance

Questions de contrôle des acquis

- Votre organisation souhaite implémenter une solution rentable qui interconnecte deux filiales avec votre siège social. De quelle façon les VPN pourraient-ils jouer un rôle dans ce scénario ?
- Le responsable informatique de votre organisation est préoccupé par l'ouverture d'un trop grand nombre de pare-feux pour faciliter l'accès à distance des utilisateurs qui travaillent à domicile via une connexion VPN. Comment pourriez-vous répondre aux attentes de vos utilisateurs distants tout en apaisant votre responsable ?
- Vous disposez d'un serveur VPN avec deux stratégies réseau configurées. La première présente une condition qui accorde l'accès aux membres du groupe Contoso, auquel chaque individu de votre organisation appartient, ainsi qu'une contrainte de restriction relative aux jours et aux heures durant les heures de bureau uniquement. La deuxième stratégie présente une condition d'adhésion au groupe Admins du domaine et aucune contrainte. Pourquoi les administrateurs se voient-ils refuser toute connexion en dehors des heures de bureau, et que pouvez-vous faire à ce sujet ?
- Comment l'ordinateur client DirectAccess détermine-t-il s'il est connecté au réseau intranet ou Internet ?
- A quoi sert une table NRPT ?

Contrôle des acquis et éléments à retenir

- Questions de contrôle des acquis
- Outils