MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention du Diplôme de Master en Electronique

Option : Télécommunication et Réseaux

Thème :

Implémentation d'une solution d'interconnexion entre deux forêts différentes avec une relation d'approbation et VPN site à site

Mme. LAHDIR .L

Mr. KIBOUH.M

M^{elle} .SADOUD Lila

M^{elle} .SADDEDINE Malika

Année universitaire 2012/2013

Remerciement

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

Nos premiers remerciements vont à nos chères parents, que Dieu les protège et leurs procure une longue vie.

Nous tenons à exprimer nos plus sincères remerciements à notre promotrice ***Mme.LAHDIR*** *qui nous a aidées tout au long du travail.*

Nos plus vifs remerciements vont aussi à ***Mr. LAHDIR*** *pour l'aide précieuse qu'elle nous a apportée.*

Un grand merci à notre Co-promoteur ***Mr.KIBOUH*** *pour ses encouragements et ses orientations qui nous ont beaucoup aidées au cours de notre projet.*

Nos remerciements les plus vifs s'adressent aussi à messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de Notre cycle universitaire.

Un grand merci également à nos familles et nos amis pour leurs aides considérables.

Remerciement

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

Nos premiers remerciements vont à nos chères parents, que Dieu les protège et leurs procure une longue vie.

Nous tenons à exprimer nos plus sincères remerciements à notre promotrice ***Mme.LAHDIR*** *qui nous a aidées tout au long du travail.*

Nos plus vifs remerciements vont aussi à ***Mr. LAHDIR*** *pour l'aide précieuse qu'elle nous a apportée.*

Un grand merci à notre Co-promoteur ***Mr.KIBOUH*** *pour ses encouragements et ses orientations qui nous ont beaucoup aidées au cours de notre projet.*

Nos remerciements les plus vifs s'adressent aussi à messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de Notre cycle universitaire.

Un grand merci également à nos familles et nos amis pour leurs aides considérables.

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents à qui je dois tout, je profite de les remercier pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et le sacrifice qu'ils ont fait pour moi, que Dieu les protège et les entoure de sa bénédiction ;

Mes très cher frère ***Mohamed, Djilali, Toufik, Hassan, Anis*** *à qui Je Souhaite le succès dans leurs vies.*

Mes adorables sœurs : ***Djedji et Safia.***

A nana ***Fatma*** *et mes très chère cousin et cousine et à toute la famille*

SADDEDINE.

A ma grand-mère qui j'aime beaucoup et toute mes ancles et tantes.

A ma très chère copine et binôme ***LILA*** *à quelle que je souhaite la réussite dans toute sa vie et à toute sa famille et particulièrement* ***Djedji.***

Ma très chère copine ***FAZIA*** *à quelle que je souhaite la réussite dans toute sa vie et à toute sa famille.*

Mes très chère amis :Houria, Nessema,Fazia,Karima,Dhrifa,Malha

Linda,Ghani,Ahmed,Sofiane,Rabeh et particulièrement ***Moh*** *et toute sa famille.*

A toute la promotion 2012/2013

A tous ceux qui m'ont aidé et tous ceux qui m'ont connu de prés et de loin.

MALIKA

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents à qui je dois tout, je profite de les remercier pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et le sacrifice qu'ils ont fait pour moi, que Dieu les protége et les entoure de sa bénédiction ;

Mes très cher frère ***Hamid*** *et* ***Saïd*** *à qui Je Souhaite le succès dans leurs vies. ;*

Mes adorables sœurs : ***Djedji et Naya.***

A nana ***Fatma*** *et mes très chère cousin et cousine :* ***Aldjia, Farida, Yazid, Saïd, Hakim, Farhat, Ali*** *et à toute la famille* ***SADOUD****.*

A ma grand-mère qui j'aime beaucoup et toute mes ancles et tantes et à toutes la famille ***BOUMEKRA.***

A ma très chère copine et binôme ***Malika*** *à quelle que je souhaite la réussite dans toute sa vie et à toute sa famille.*

Ma très chère copine ***Fazia*** *à quelle que je souhaite la réussite dans toute sa vie et à toute sa famille.*

Mes très chère amis : ***Houria, Nessema, Fazia****, Karima, Dhrifa, Malha , Djedji , Saida , Moh, Sofiane et particulièrement* ***Ghani*** *et toute sa famille.*

A toute la promotion 2012/2013

A tous ceux qui m'ont aidé et tous ceux qui m'ont connu de prés Et de loin.

LILA

A

ACE: Access Control Entries

ACL: Access Control List: liste des adresses et ports autorisés ou interdits par un pare-feu.

AD CS: Active Directory Certification Services : Il s'agit du composant d'autorité de certification.

AD LDS: Active Directory Lightweight Directory Services

AD RMS: Active Directory Right Management Services. Sont l'implémentation d'une solution de protection de l'information intégrée à l'Active Directory de Windows Server 2008.

ADAM: Active Directory Application Mode.est une version plus légère d'Active Directory spécifiquement dédiée à une utilisation au niveau applicatif.

ADDS: Active Directory Domain Services : Il s'agit du composant principal qui va gérer les utilisateurs, ordinateurs, stratégies de groupe, etc.

ADFS: Active Directory Federation Services

ADSL: Asymmetric Digital Subscriber Line.

AH: Authentication Header

C

CISCO: est une entreprise informatique américaine qui vendait, à l'origine, uniquement du matériel réseau (routeur et Switch Ethernet).

CHAP: Challenge Handshake Authentication Protocol

DHCP: Dynamics Host Configuration Protocol

DN: Distinguished Name.

DNS: Domain Name System.

E

EFS: Encrypting File System

ESP: Encapsulating Security Payload

F

FSMO: Flexible Single Master Operation

FTP: file transfert protocol.Protocole de transfert des fichiers.

G

GPO: Group Policy Object

GUID: Globally Unique Identifier Security Identifier

I

IP Sec: Internet Protocol Security

K

KDC: Key Distribution Center. Centre de distribution des clés.

L

L2F: layer Two Forwarding.

L2TP: Layer Two Tunneling Protocol. protocole d'encapsulation des données

LAC: L2TP Access Concentrator.

LAN: Local Area Network. Réseau local d'entreprise. Est un ensemble d'ordinateur appartenant à une même organisation et relié entre eux par un réseau.

LNS: L2TP Network Server.

N

NTLM : Windows NT Lan Manager est le protocole d'authentification réseau par défaut de NT4, Windows 2000,2003 et 2008 le prend encore en charge, afin de préserver la compatibilité.

NTP: Network Time Protocol

P

PAP: Password Authentication Protocol. Protocole d'authentification de mots de passe des utilisateurs.

PAT: Port Address Translation

PDC : contrôleur principale de domaine.

PKI: Public Key Infrastructure. Permet de délivrer et de gérer des certificats numériques.

PPP: Point to Point Protocol: protocole d'encapsulation de niveau 2 de modèle OSI.il garanti la sécurité des échanges.

PPTP: Point To Point Tunneling Protocol. Protocole d'encapsulation de données et de sécurité.

Q

QoS: Quality of Service .la QoS est un gestionnaire de trafic qui permet d'allouer les ressources réseau aux applications selon leur poids et leur priorité.

R

RID : Relative Identifier : distribue des paquets d'identificateurs relatifs aux contrôleurs de domaines.

RTC: Réseau telephonic commute

S

SA: Security Association : définit l'ensemble des opérations IP sec devant être appliquées aux datagrammes qui affèrent.

SAM: Security Account Manager

SID: Security identifier : est un identifiant unique utilisé dans Windows pour identifier les objets et leurs permissions sur les ressources

SNTP: Simple Network Time Protocol

SPN: Service Principal Name .Nom de service principale.

SSL: Secure Socket Layer

T

TCP/IP: Transmission contrôle Protocol/Internet Protocol

TDO: Objet de domaine approuvé. Sont des objets représentant chaque relation d'approbation dans un domaine donné.

TGT: Ticket Granting Ticket

U

UDP: User Datagramme Protocol .Protocole de transport de données en mode connecté.

UPN: User Principal Name.

V

VPN: Virtual Private Network: Ensemble de technologies permettant d'établir une communication sécurisée entre deux points distants.

SOMMAIRE

Sommaire

Liste de figures

Chapitre I :

Chapitre II :

Chapitre III :

Chapitre VI :

Liste de figures

Liste de figures

Liste de figures

La technologie de l'information d'aujourd'hui, a envahi tous les domaines de notre vie quotidienne, surtout au sein des entreprises qui doivent suivre l'évolution du phénomène informatique pour bénéficier de ses performances. La gestion et la maitrise de l'information sont devenues des préoccupations de premier ordre, pour répondre aux exigences de la clientèle, l'entreprise est tenue d'assurer des meilleures prestations de service.

De nos jours, du fait de l'essor informatique, les réseaux d'entreprises ont une certaine tendance à s'agrandir très rapidement. Ainsi au sein d'une même entreprise on arrive régulièrement à avoir plusieurs domaines avec différents sites éparpillés dans le monde entier. De plus en plus les entreprises ouvrent leurs systèmes d'information à des utilisateurs externes (partenaires, fournisseurs, membres de l'administration) au réseau local et intègrent d'autres entreprises afin d'améliorer le coût et organiser les ressources le mieux possible. Il est donc essentiel de donner l'accès à des utilisateurs d'une forêt d'accéder aux ressources d'une autre forêt et de maîtriser le contrôle d'accès, de connaître les ressources de l'entreprise à protéger et les droits des utilisateurs du système d'information.

La relation d'approbation est l'une des solutions la plus fiable pour les entreprises qui permettre à des utilisateurs authentifiées dans une forêt d'accéder de façon sécurisé aux ressources d'une autre forêt et un administrateur de pouvoir gérer les utilisateurs de l'autre forêt. Pour garantir l'échange de données entre ces deux forêts sans courir de risque on doit utiliser un VPN site à site.

Le VPN permet aux entreprises de profiter des avantages en termes de connectivité et de coût, sans compromettre l'intégrité des règles de sécurité d'entreprise.

Notre projet est réalisé au niveau de l'entreprise 2intPartners (Institue International des Nouvelles Technologie) qui est centrée sur les systèmes et réseaux, le développement d'applications, les bases de données et les environnements "Open Source". Sans oublier les formations utilisateurs spécifiques autour des Applications bureautiques et de travail collaboratif.

Notre mémoire est réparti en quatre chapitres ;

Le premier chapitre présente des généralités sur l'Active Directory sous Windows server 2008 ; fonctionnalités, différentes technologies, protocoles, etc.

Dans le deuxième chapitre nous exposerons une étude sur les relations d'approbation ; différents types d'approbation, fonctionnement, sécurité, etc.

Le troisième chapitre représente des fonctionnalités sur les VPN site à site ; différents types, fonctionnement, protocoles utilisées, etc.

Le quatrième chapitre sera consacré à une implémentation des solutions d'interconnexions ; configuration de tunnel VPN site à site, création d'une relation d'approbation entre forêts.

Nous terminerons notre projet par une conclusion générale.

I.1.Préambule

Active Directory est un annuaire d'entreprise qui existe depuis 1996 et est utilisable depuis Windows 2000 Server Edition sorti en 1999. Il s'agit donc d'un produit éprouvé par les années. Cet annuaire d'entreprise vient en remplacement des bases SAM (Security Account Manager) qui étaient exploitées avec NT4 et les groupes de travail. Ces bases présentaient notamment des limitations d'administration.

L'arrivée d'Active Directory a permis de passer des groupes de travail aux domaines Active Directory et ainsi de centraliser toute l'administration et la gestion des droits dans un annuaire de type LDAP. Tout logiciel utilisant LDAP sera capable de communiquer avec Active Directory.

Dans ce chapitre nous allons présenter les notions de bases sur l'Active Directory.

I.2.Présentation d'Active Directory

Active Directory permet de centraliser, de structurer, d'organiser et de contrôler les ressources réseau dans les environnements Windows Server 2000/2003 et Windows Server 2008. La structure Active Directory permet une délégation de l'administration très fine pouvant être définie par types d'objets.

I.2.1.Définition d'Active Directory

Active Directory est un service d'annuaire des objets du réseau, il permet aux utilisateurs de localiser, gérer, nommer, décrire, et sécuriser de manière cohérente les informations concernant les ressources réseau.

Il permet de réaliser la gestion des objets sans liens avec la disposition réelle ou les protocoles réseaux employés.

Active Directory organise l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets.

I.2.2. Objets Active Directory

Active Directory stocke des informations sur les objets du réseau. Ils existent plusieurs types :

- serveurs
- ordinateurs

- imprimantes
- utilisateurs
- sites
- domaines...

Figure I.1 : les objets Active Directory

Un objet représente une entité unique et ses attributs définis par le schéma. Chaque objet est défini par un DN (emplacement absolu), un UPN (login), un GUID (identifiant unique) et un SID (identifiant unique pour gérer les permissions).

✓ **Distinguished Name (DN)**

Tous les objets de l'AD possèdent un DN. Ce DN est utilisé pour localiser et identifier l'objet dans la base de données LDAP.

✓ **User Principal Name (UPN)**

L'UPN est créé sur base du nom d'utilisateur et du nom du domaine auquel appartient l'utilisateur. Il est utilisé pour se connecter au réseau dans le domaine. L'UPN est unique dans la forêt.

Ex: lila.clubscientifique.com

✓ **Globally Unique Identifier (GUID)**

Le GUID est un identifiant unique assigné à chaque objet de l'AD. Le GUID ne peut pas être changé (même si l'objet est déplacé ou renommé) et n'est pas réutilisable. Quand on modifie un objet, son DN et son SID sont changé mais pas le GUID.

✓ **Security Identifier (SID)**

Le SID est un identifiant unique utilisé dans Windows pour identifier les objets et leurs permissions sur les ressources.

Parmi les objets Active Directory :

I.2.2.1.Utilisateurs et ordinateurs

Chaque utilisateur dans Active Directory est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénoms, login, adresse e-mail, téléphone,

département, etc). Ces attributs peuvent permettre de trouver des utilisateurs dans un domaine. Ils peuvent par exemple être utilisés dans Exchange pour constituer des listes dynamiques de distribution d'e-mails. Ces utilisateurs peuvent se voir attribuer des autorisations sur d'autres objets d'Active Directory.

Les ordinateurs disposent également de comptes spécifiques dans Active Directory. Ces comptes existent pour gérer la sécurité pour les accès à certaines ressources comme les stratégies de groupe, l'accès au réseau.

I.2.2.2.Groupes

Un groupe est un ensemble des comptes utilisateurs auxquels sont assignés des droits et des permissions. Chaque groupe Active Directory est défini par son type et son étendue.

- **Le type de groupe**

Il existe deux types de groupes :

- **Les groupes de sécurité** : permettent de gérer la sécurité pour l'accès et l'utilisation des ressources de réseau. Ils peuvent aussi être utilisés comme groupes de distribution.
- **Les groupes de distribution** : Ce type permet simplement de gérer des listes de distribution d'e-mails dans un serveur de messagerie

- **Étendues des groupes**

- **Les groupes globaux** : ils donnent l'accès aux ordinateurs et aux ressources du domaine actif et des domaines approuvés, mais ne peuvent contenir que des comptes d'utilisateur globaux. Tout groupe global contenant un compte local est assimilé à un groupe local.
- **Les groupes locaux du domaine :** ils ne sont reconnus que par le domaine auquel ils sont associés, et dont ils permettent d'exploiter les fichiers et les ressources. Comme les utilisateurs locaux du domaine, ces groupes ne sont pas admis dans d'autres domaines.
- **Les groupes universels :** permettent d'assigner des autorisations d'accès à des ressources réparties dans plusieurs domaines de la forêt. Les membres de ce groupe proviennent de la forêt et sont disponible uniquement en mode natif.

- **Les stratégies de groupes (Group Policy Object ou GPO)**

Ils sont des autorisations ou des interdictions qui permettent de contrôler l'activité des utilisateurs. Les stratégies de groupe peuvent être « liées » à des sites, des domaines ou des unités organisationnelles.

Ces stratégies sont enregistrées dans l'annuaire Active Directory. Elles sont modifiables par l'outil d'administration « éditeur de stratégies de groupes », accessible

- sous Windows 2003 par les propriétés d'un domaine ou d'une UO.
- sous Windows 2008 par un outil spécifique de gestion des stratégies de groupe.

Il existe 2 catégories de stratégies de groupes :

- les stratégies d'ordinateur qui s'appliquent au moment du démarrage de la session.
- les stratégies d'utilisateur qui s'appliquent au moment du démarrage de la session de l'utilisateur.

I.2.3.Schéma Active Directory

Le schéma Active Directory stocke la définition de tous les objets d'Active Directory .Il n'y a qu'un seul schéma pour l'ensemble de la forêt, ce qui permet une homogénéité de l'ensemble des domaines. Le schéma comprend deux types de définition :

- **Les attributs** : Ils sont définis une seul fois et peuvent être utilisés dans plusieurs classes. Exemple: nom, prénom, e-mail.
- **Les classes d'objets** : Décrit les objets d'Active Directory qu'il est possible de créer. Chaque classe est un regroupement d'attributs. Exemple: utilisateur, ordinateur.

Le schéma est stocké dans la base de données d'Active Directory ce qui permet des modifications dynamiques exploitables instantanément.

I.2.4.Les différentes partitions d' Active Directory

La base de données Active Directory est divisée de manière logique en plusieurs partitions.

- La partition de schéma.
- La partition d'annuaire.
- La partition de la configuration.
- La partition du domaine.
- La partition d'application.

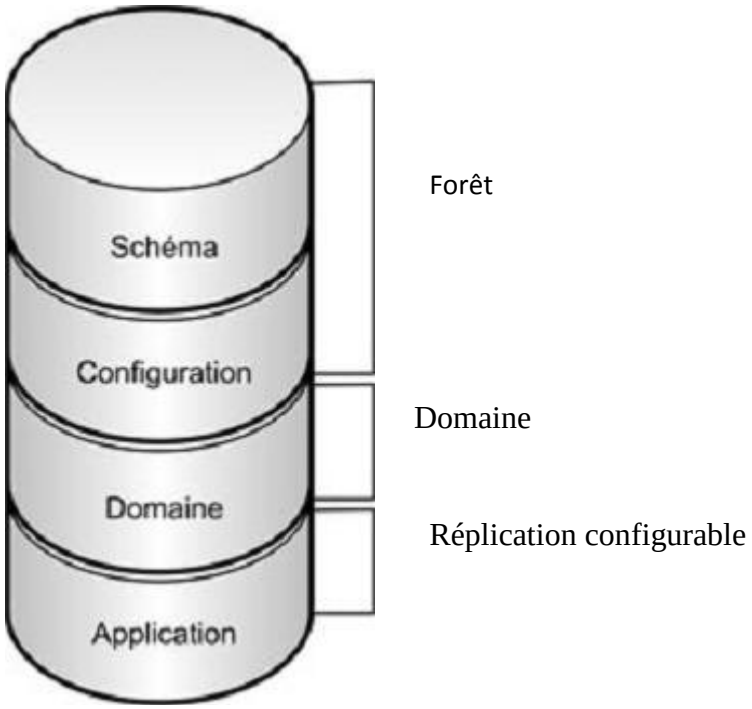


Figure I.2: les partitions d'Active Directory

- **La partition de schéma**

Chaque forêt possède une seule partition de schéma. Cette partition de schéma est stockée dans tous les contrôleurs de domaine de la même forêt. Elle contient les définitions de tous les objets et attributs créés dans l'annuaire, ainsi que les règles qui permettent de les créer et de les manipuler. Les données du schéma sont répliquées dans tous les contrôleurs de domaine de la forêt. C'est pourquoi les objets doivent être conformes aux définitions d'objet et d'attribut du schéma.

- **La partition d'annuaire**

Chaque partition est une unité de réplication et possède sa propre topologie de réplication. La réplication est exécutée entre les réplicas des partitions d'annuaire. Tous les contrôleurs de domaine de la même forêt ont au moins deux partitions d'annuaire en commun : celles du schéma et de la configuration. De plus, ils partagent une partition de domaine commune.

- **La partition de la configuration**

Chaque forêt possède une seule partition de configuration. Stockée dans tous les contrôleurs de domaine de la même forêt, la partition de configuration contient les données sur la structure Active Directory de l'ensemble de la forêt, telles que les domaines et les sites existants, les contrôleurs de domaine existants dans chaque forêt et les services disponibles. Les données de la configuration sont répliquées dans tous les contrôleurs de domaine de la

forêt.

- **La partition de domaine**

Chaque forêt peut avoir plusieurs partitions de domaine. Elles sont stockées dans chaque contrôleur de domaine d'un domaine donné. Une partition de domaine contient les données sur tous les objets propres au domaine et créés dans ce domaine, tels que les utilisateurs, les groupes, les ordinateurs et les unités d'organisation. Une partition de domaine est répliquée dans tous les contrôleurs de domaine du domaine considéré.

Tous les objets de chaque partition de domaine d'une forêt sont stockés dans le catalogue global avec un seul sous-ensemble de leurs valeurs d'attribut.

- **La partition d'application**

Les partitions d'application stockent les données sur les applications dans Active Directory. Chaque application détermine comment elle stocke, classe et utilise ses propres données. Pour éviter toute réplication inutile des partitions d'application, nous pouvons désigner les contrôleurs de domaine qui en hébergent dans une forêt. À la différence d'une partition de domaine, une partition d'application ne peut pas stocker les principaux objets de sécurité, tels que les comptes d'utilisateur. De plus, les données contenues dans une partition d'application ne sont pas stockées dans le catalogue global.

I.3.Caractéristiques d'Active directory

- **Centralisation des données**

Les données résident dans une base de données distribuée, accessible aux utilisateurs à travers le réseau. La centralisation des données réduit les coûts d'administration, évite la redondance des données et diminue les coûts de réplication.

- **Simplicité administrative**

Les domaines Active directory reposent sur des structures organisationnelles hiérarchiques. Cela facilite la localisation des ressources ainsi que le contrôle des privilèges administratifs.

- **Intégration de DNS**

-L'Active directory et DNS utilisent la même structure hiérarchique.

-Les clients Active directory utilisent le DNS pour localiser les ressources, les contrôleurs de domaines.

- Le service DNS peut utiliser l'Active directory pour stoker ses zones.

- **Gestion centralisée des clients**

Afin de diminuer les coûts d'administration des clients, Active directory offre des technologies pour la configuration des clients ou la mobilité des utilisateurs.

- **Administration basée sur des stratégies**

Les stratégies dans l'Active directory définissent les actions réalisables par les utilisateurs, facilitent le déploiement d'application, les mises à jour…

- **Réplication des informations**

Active directory utilise la réplication multi-maître pour répliquer les données qu'il stocke.Toléronce de panne, disponibilité.

- **Sécurité intégrée**

Basée sur les ACL (Access Control List) permet le contrôle d'accès aux objets, offre des mécanismes d'authentification comme kerberos.

I.4. Les différentes technologies d'Active Directory

- **ADDS (Active Directory Domain Services) (Identité)**

AD DS est conçu pour fournir un référentiel central pour gérer les identités au sein d'une organisation. AD DS fournit des services d'authentification et d'autorisation dans un réseau et prend en charge la gestion des objets au moyen de la stratégie de groupe. Il fournit également des services de gestion et de partage des informations qui permettent aux utilisateurs de trouver n'importe quel composant de serveur de fichiers, imprimantes, groupes et autres utilisateurs dans l'annuaire.

En conséquence, AD DS est la principale technologie d'Active Directory et doit être déployée dans tout réseau sous Windows Server 2008.

- **AD LDS *(*Active Directory Lightweight Directory Services) (application)**

Le rôle AD LDS auparavant connu sous le nom d'ADAM (Active Directory Application Mode), est en substance une version autonome d'Active Directory qui prend en charge les application fonctionnant avec un annuaire. En réalité, il s'agit d'un sous-ensemble d'AD DS, parce que les deux sont basés sur le même noyau de code. L'annuaire AD LDS ne stocke et ne réplique que les informations associées aux applications. Il est communément utilisé par les applications qui nécessitent le stockage d'informations dans un annuaire mais qui n'ont pas besoin qu'elles soient largement répliquées, par exemple, vers tous les contrôleurs de domaine.

AD LDS permet également de déployer un schéma personnalisé pour prendre en charge une application sans modifier celui d'ADDS.

AD LDS peut servir à fournir des services d'authentification dans des réseaux exposés comme les extranets.

- **AD CS (Active Directory Certification Services) (Approbation)**

Les organisations peuvent utiliser AD CS pour définir une autorité de certification qui émettra des certificats numériques dans le cadre d'une infrastructure à clé public (PKI, Public Key Infrastructure) qui lie l'identité d'une personne, d'un équipement ou d'un service à clé privée correspondante. Les certificats peuvent servir à authentifié des utilisateurs, des ordinateurs, des entités sur le Web et des cartes à puce, et à prendre en charge des applications notamment les réseaux sans fils sécurisés, les réseaux privés virtuels (VPN), le système de fichiers EFS (Encrypting File System), les signatures numériques, etc.

AD CS permet d'émettre et de gérer les certificats de manière efficace et sécurisée. Dans les réseaux internes, AD CS peut s'intégrer avec AD DS pour fournir automatiquement des certificats aux utilisateurs et aux ordinateurs.

- **AD RMS (Active Directory Right Management Services) (Intégrité)**

AD RMS est une technologie de protection des information qui permet de mettre en œuvre des modèles de stratégie permanents qui définissent les usages autorisés ou interdits, que ce soit en ligne, hors ligne, derrière le pare-feu ou à l'extérieur .AD RMS peut s'appuyer sur AD CS pour incorporer des certificats dans des documents ainsi que sur AD DS pour gérer les droits d'accès.

- **AD FS (Active Directory Federation Services**)

Il s'agit du composant permettant la fédération de services entre différents environnements Active Directory. Cela va nous permettre d'établir des relations de confiance avec des partenaires externes à notre entreprise (fournisseurs, fabricants, etc.) afin de leur donner un accès à certains de nos services internes de manière contrôlée et sécurisée.

I.5.Structure d'Active Directory

La structure d'Active Directory est hiérarchique et se décompose en deux parties :

La structure logique et la structure physique.

I.5.1.La structure logique

La structure logique d'Active Directory est modulaire et offre une méthode de conception hiérarchie d'annuaire cohérente, à la fois ses utilisateurs et ses administrateurs.

Les composants logiques de la structure d'Active Directory sont les suivants :

- **Domaine**

Unité fondamentale de la structure logique, un domaine peut contenir plusieurs millions d'objets qui partagent une même base de données d'annuaire et chaque domaine à un nom unique sur le réseau.

La figure ci-dessous représente le domaine Active Directory.

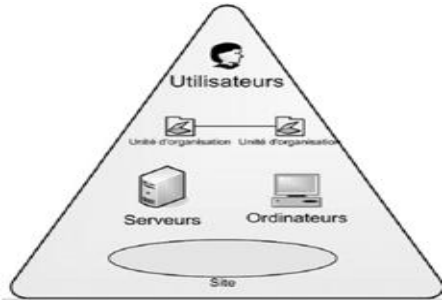


Figure I.3 : exemple de domaine

Un domaine est basé sur quatre étapes principales :

- **Limite de sécurit**é : Chaque domaine dispose de ses propres stratégies de sécurité.
- **Unité d'administration** : l'administrateur du domaine gère l'ensemble de la sécurité sur son domaine. Il est le seul à pouvoir accorder des permissions sur les objets de son domaine.
- **Unité de réplication** : les données Active Directory sont répliquées sur tous les contrôleurs de domaine.
- **Mode d'un domaine** : Active Directory peut fonctionner en deux modes, le mode Mixte et le mode Natif.

- **Arborescence**

Une arborescence (arbre) regroupe un ou plusieurs domaines partageant un même espace de nom contigu. Dans l'Active Directory, les noms des domaines correspondent à des noms DNS : le premier domaine crée appeler domaine racine n'est pas renommable et ne peut être supprimé. Les domaines ajoutés par la suite seront appelés les domaines enfants du domaine

parent. Leurs noms seront composés d'un nom relatif suivi du nom du domaine parent. Exemple : Alger est le nom relatif du domaine Alger.2int.com.

❖ **Forêt**

Une forêt est composée d'une ou plusieurs arborescences qui partagent pas un espace de nom contigu .Les arborescence d'une forêt partagent une configuration, un schéma et un catalogue globale commun. Tous les domaines d'une forêt sont liés par des relations d'approbation.

Les domaines d'une forêt fonctionnent indépendamment les uns des autres, mais la forêt autorise la communication sur l'ensemble de l'organisation.

❖ **Unité d'organisation**

Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes ainsi que d'autres unités d'organisation. Elle répond aussi à des besoins administratifs:

- Déléguer des pouvoirs à certains utilisateurs afin de leur octroyer des responsabilités sur les objets présents dans l'unité d'organisation.
- Simplifier la sécurité en limitant la visibilité des ressources dans Active Directory.

Les utilisateurs de l'unité d'organisation n'affichent alors que les objets auxquels ils ont droits.

- Définir une stratégie particulière pour les comptes utilisateurs d'une unité d'organisation

La structure de l'unité d'organisation est basée sur la localisation géographique, l'organisation fonctionnelle de l'entreprise, le type d'objet et la structure mixte.

Les unités d'organisations sont représentées dans le domaine Active Directory par des cercles qui sont montrées dans la figure ci- dessous.

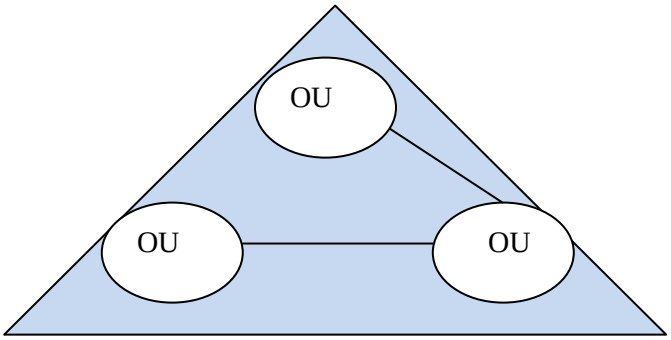


Figure I.4 : exemple d'unité d'organisation

❖ **Catalogue global**

Le catalogue global contient une partie des attributs les plus utilisés de tous les objets Active Directory. Il contient les informations nécessaires pour déterminer l'emplacement de tout objet de l'annuaire.

Le catalogue global permet aux utilisateurs d'effectuer 2 tâches importantes :

- Trouver des informations Active Directory sur toutes les forêts, quelque soit l'emplacement de ces données.
- Utiliser des informations d'appartenance à des groupes universels pour ouvrir une session sur le réseau.

Un serveur qui contient le catalogue globale est appelé serveur de catalogue global .Ce serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global et peut ainsi traiter les requêtes qui lui sont destinées. Le premier contrôleur de domaine est automatiquement le serveur de catalogue global. Il est possible de configurer d'autres contrôleurs de domaine en serveur de catalogue global afin de réguler le trafic.

❖ **Les relations d'approbation**

Les relations d'approbations permettent à des utilisateurs de domaines différents situées dans des forêts différentes de communiquer entre eux .Elles permettent à des utilisateurs d'un domaine approuvé d'être authentifiés par des ordinateurs d'un domaine d'approbation. On va donc gérer des domaines que l'on approuve et des domaines qui nous approuvent. (Une étude détaillée dans le 2eme chapitre sur les relations d'approbation).

❖ **Les niveaux fonctionnels**

Les niveaux fonctionnels sont des modes opératoires qui déterminent les versions de Windows qu'on peut utiliser sur les contrôleurs de domaine et la disponibilité des fonctionnalités d'Active Directory. On a deux types de niveaux fonctionnels :

- **Les niveaux fonctionnels de domaine**

Le niveau fonctionnel de domaine affecte les fonctionnalités Active Directory disponibles au sein du domaine et détermine les versions de Windows prises en charge par les contrôleurs de domaine du domaine .Dans les précédentes versions de Windows, les niveaux fonctionnels de domaine prenaient en charge des contrôleurs de domaine qui exécutent Microsoft Windows NT4.0. Depuis Windows Server 2008, cette prise en charge n'existe plus. Tous les contrôleurs de domaine doivent exécuter Windows 2000 Server ou ultérieur avant qu'on ne

puisse ajouter le premier contrôleur de domaine Windows Server 2008 au domaine. L'Active Directory de Windows Server 2008 prend en charge trois niveaux fonctionnels :

- ✓ Windows 2000 Natif
- ✓ Windows Server 2003
- ✓ Windows Server 2008

- **Les niveaux fonctionnels de forêt**

Les niveaux fonctionnels de forêt activent des fonctionnalités à l'échelle de la forêt et déterminent les systèmes d'exploitation pris en charge par les contrôleurs de domaine dans l'ensemble de la forêt. L'Active Directory de Windows Server 2008 prend en charge trois niveaux fonctionnels de forêt :

- ✓ Windows 2000
- ✓ Windows Server 2003
- ✓ Windows Server 2008

I.5.2.Structure physique

Dans l'Active Directory, la structure logique est séparée de la structure physique.

La structure logique utiliser pour organiser les ressources réseau mais la structure physique utiliser pour configurer, gérer le trafic réseau.

La structure physique se compose de sites et de contrôleurs de domaine.

- ❖ **Sites**

Un site est une combinaison d'un ou de plusieurs sous-réseaux IP connectés entre eux par une liaison à haut débit fiable. Un domaine peut contenir un ou plusieurs sites et un seul site peut contenir plusieurs domaines ou plusieurs parties de domaines .Un site ne contient que des objets ordinateurs et des connexions.

Le rôle d'un site est l'optimisation du trafic de réplication et permet aux utilisateurs de se connecter à un contrôleur de domaine en utilisant une connexion rapide et fiable.

- ❖ **Contrôleur de domaine**

C'est un serveur contenant une copie inscriptible de la base de données Active Directory, participant à la réplication Active Directory et contrôlant l'accès aux ressources réseau.

Les administrateurs peuvent gérer les comptes d'utilisateurs, l'accès réseau, les ressources partagées, la topologie du site et les autres objets d'annuaire à partir de n'importe

quel contrôleur de domaine de la forêt.

Les réplications entre contrôleurs du domaine sont automatiques et s'effectuent à intervalles réguliers, paramétrables et définis par l'administrateur.

Les contrôleurs de domaine peuvent contenir des informations différentes pendant un temps très court jusqu'au moment de la synchronisation.

La mise en place de plusieurs contrôleurs de domaines sur le réseau permet de faire la tolérance aux pannes.

I.6. Les rôles de maître d'opérations (FSMO)

Un maître d'opérations est un contrôleur de domaine auquel ont été affectés un ou plusieurs rôles d'opérations principales simples dans un domaine ou dans une forêt Active Directory. Les contrôleurs de domaine auxquels ces rôles sont affectés exécutent des opérations qui ne sont pas autorisées simultanément sur différents contrôleurs de domaine du réseau.

Il existe cinq rôles de maître d'opérations dans une forêt Active Directory, deux rôles au niveau de forêt et trois rôles au niveau de domaine.

I.6.1.Rôles uniques au sein d'une forêt

- **Maître de schéma**

Permet de gérer les modifications effectuées au niveau du schéma Active Directory.

- **Maître d'attribution de noms de domaine**

Valide s'il n'y a pas de conflit(s) de noms DNS au niveau des domaines de la forêt et des domaines approuvés

I.6.2.Rôles uniques dans un domaine

- **Le maître émulateur PDC**

L'émulateur PDC joue le rôle d'un contrôleur principal de domaine pour les clients Windows NT 4 et réplique les mises à jour vers le contrôleur secondaire de domaine en mode mixte.

Gère les changements des mots de passe. En mode 2000 mixte, permet aux BDC NT4 des se synchroniser avec le DC jouant le rôle d'Emulateur PDC.

- **Maître RID**

Le maître RID alloue des identificateurs relatifs à chacun des contrôleurs de domaine du domaine.

Quand un utilisateur est créé par un contrôleur de domaine, il utilise le SID du domaine auquel il ajoute un identificateur relatif qui est donc distribué par le maître RID.

- **Maître d'infrastructure**

Le maître d'infrastructure est responsable de la mise à jour des références groupe-utilisateur, après un renommage ou un déplacement par exemple d'un membre d'un groupe.

I.7. Protocoles

Active Directory supporte les protocoles standards suivants :

- **TCP/IP (Transmission contrôle Protocol/Internet Protocol)**

TCP/IP représente de certaine façon l'ensemble des règles de communications sur internet et se base sur la notion adressage IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Il est conçu pour répondre à certains nombre de critères parmi lesquels :

- ✓ Le fractionnement des messages en paquet.
- ✓ Utilisation d'un système d'adresses.
- ✓ L'acheminement des données sur le réseau (routage).
- ✓ Le contrôle des erreurs de transmission de données.

- **DNS (Domain Name System)**

Protocole permettant de résoudre un nom DNS en une adresse IP et inversement.

Le DNS a deux systèmes de résolution de noms :

- ✓ Zone de recherche directe : résout un nom en IP.
- ✓ Zone de recherche inversée : résout une IP en nom.

L'espace de noms DNS est découpé en zones DNS. Ces zones sont répartir sur des milliers de serveurs DNS.

L'interconnexion entre serveurs DNS se fait via deux mécanismes :

- ✓ **La délégation** : un serveur DNS peut déléguer une partie de l'espace de noms qu'il
- ✓ gère à un autre serveur.
- ✓ **La redirection** : un serveur DNS peut rediriger les requêtes non résolues vers un autre

serveur DNS.

Afin de fournir une tolérance de panne et de répartir la charge, un serveur DNS peut disposer d'une copie en lecture seule (zone secondaire) de la zone d'un autre serveur en lecture /écriture (zone principale).

- **DHCP (Dynamics Host Configuration Protocol)**

Est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut.

- **SNTP (Simple Network Time Protocol)**

Protocole de distribution de l'heure. Il est impératif que toutes les machines soient synchronisées sur un serveur NTP (Network Time Protocol) référence du fait de la méthode d'authentification Kerberos qui se base sur un ticket d'accès horodaté.

- **KERBEROS Version 5 :**

Le protocole KERBEROS est le protocole de sécurité pour l'authentification. Il vérifie l'identité de l'utilisateur et des services de réseau.

Avec le protocole Kerberos V5, le client demande un ticket d'un contrôleur de domaine de son domaine de compte vers le serveur du domaine d'approbation. Ce ticket est émis par un intermédiaire approuvé par le client et le serveur. Le client présente ce ticket approuvé au serveur dans le domaine d'approbation pour authentification.

- **LDIF (LDAP Data Interchange Format)**

Permet la synchronisation de l'annuaire. Protocole d'accès aux annuaires qui permet par exemple de développer le schéma à l'aide de scripts LDIF.

- **LDAP (Lightweight Directory Access Protocol)**

Protocole d'accès aux annuaires, est une norme Internet ouverte .Les services d'annuaire Active Directory prennent en charge les versions 2 et 3 du protocole LDAP pour échanger des informations entre les annuaires et les applications.

Au cours d'une ouverture de session ou lors d'une recherche dans Active Directory, l'accès aux contrôleurs de domaine et aux catalogues globaux s'appuie sur le protocole LDAP. Active Directory résout les noms d'objet à l'aide d'une requête LDAP. Il offre un moyen de communiquer avec Active Directory en attribuant un chemin d'accès unique à chaque objet. Avec LDAP on identifie deux chemins : Les chemins d'accès LDAP comprennent les

éléments suivants :

- **Les noms uniques :** le nom unique identifie le domaine dans lequel est situé l'objet, ainsi que son chemin d'accès complet.
- **Les noms uniques relatifs :** partie du nom unique qui permet d'identifier l'objet dans son conteneur.

➢ **Certificats X509 V3**

Permet l'authentification par certificats. Par exemple ils sont utilisés avec la protection EFS (Encrypting File System) des dossiers.

I.8.Active Directory et sécurité

Active Directory constitue la pièce maîtresse de la sécurisation des infrastructures réseau basées sur Windows Server 2008. Afin de garantir la sécurité de l'environnement informatique, Windows demande à vérifier l'identité de chaque utilisateur avant de l'autoriser à accéder aux ressources réseau. Les deux processus principaux qui gèrent cette vérification et l'accès aux ressources réseau sont les suivants :

- **L'authentification** : lors de l'ouverture de session, la procédure d'authentification vérifie l'identité des utilisateurs.
- **L'autorisation** : lorsque les utilisateurs réseau tentent de se connecter à des serveurs ou autres périphériques réseau, la procédure d'autorisation peut leur accorder ou leur refuser l'accès à la ressource.

À l'aide d'une seule ouverture de session réseau, les administrateurs peuvent gérer les données de l'annuaire et l'organisation de leur réseau, tandis que les utilisateurs réseau autorisés peuvent accéder aux ressources depuis n'importe quel point du réseau.

Active Directory permet de stocker de façon sécurisée les informations des comptes d'utilisateur et des groupes grâce à un contrôle d'accès sur les objets et aux informations d'identification des utilisateurs. Etant donné qu'Active Directory stocke non seulement les informations d'identification des utilisateurs mais aussi les informations de contrôle d'accès, les utilisateurs qui ouvrent une session sur le réseau obtiennent à la fois l'authentification et l'autorisation nécessaire pour accéder aux ressources du système.

Les administrateurs peuvent gérer la sécurité du système plus efficacement grâce aux comptes de groupe qu'Active Directory leur permet de créer. Par exemple, un administrateur peut autoriser tous les utilisateurs d'un groupe à lire un fichier en modifiant les propriétés de

ce dernier. Avec cette méthode, l'accès aux objets dans Active Directory repose sur l'appartenance à des groupes.

I.9.Discussion

L'Active Directory est utilisé pour gérer les utilisateurs du réseau en leur offrant différents services et droits, et l'accès aux autres domaines seront possibles grâce à la création d'une relation d'approbation entre forêts qu'on va étudier dans le 2 éme chapitre.

II.1.Préambule

De nos jours, du fait de l'essor informatique, les réseaux d'entreprises ont une certaine tendance à s'agrandir très rapidement. Ainsi au sein d'une même entreprise on arrive régulièrement à avoir plusieurs domaines avec différents sites éparpillés dans le monde entier afin d'organiser les ressources le mieux possible.

Une question se pose alors : **comment permettre à des utilisateurs authentifiés dans leur forêt d'accéder à des ressources d'une autre forêt ?**

La solution s'appelle : "**les relations d'approbation**" et c'est ce que nous allons étudier en détail dans notre chapitre.

II.2.Définition de relation d'approbation

La relation d'approbation est une relation administrative et de communication sécurisée entre des domaines, des arborescences ou des forêts. Elle permet à un utilisateur authentifié dans son forêt d'accéder aux ressources de tous les forêts approuvés et un administrateur de pouvoir gérer les utilisateurs de l'autre forêt.

II.3.Caractéristiques des relations d'approbation

II.3.1.Représentation

Il est important de savoir identifier sur un schéma une relation d'approbation. Tout d'abord elle relie forcément deux domaines (représenté sous forme d'un triangle) ou alors deux forêts comme nous le verront dans certains cas. En effet une relation d'approbation est représentée par une flèche reliant les entités qui s'approuvent. Le sens de la flèche nous informe si cette relation est unidirectionnelle ou bidirectionnelle.

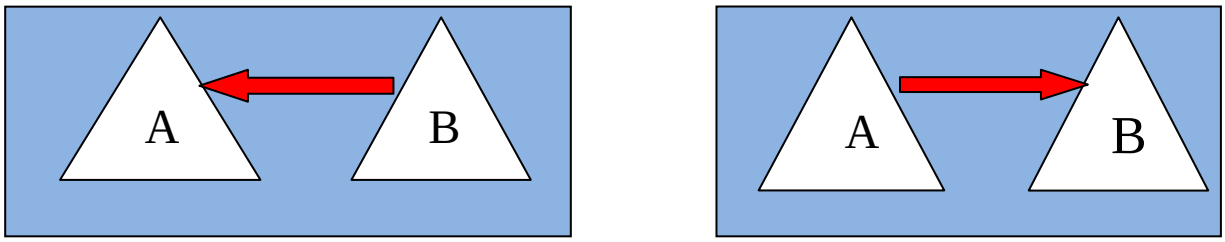
II.3.2 La direction

Il y a deux possibilité pour une relation d'approbation, soit elle est unidirectionnelle c'est à dire dans un seul sens ou alors bidirectionnelle c'est à dire dans les deux sens.

Une relation unidirectionnelle permet d'approuver un domaine à partir d'un autre domaine sans que l'inverse soit appliqué. Elle peut être unidirectionnelle entrante ou bien unidirectionnelle sortante.

Dans le cas d'une relation unidirectionnelle entrante, si un domaine A approuve un domaine B, alors un utilisateur du domaine A pourra accéder aux ressources du domaine B mais l'inverse ne serra pas possible et vice versa pour une relation unidirectionnelle sortante.

La figure suivante illustre ces deux cas :



Relation unidirectionnelle entrante **relation unidirectionnelle sortante**

Figure II.1 : relations d'approbation unidirectionnelles

L'autre possibilité est une relation bidirectionnelle. C'est à dire que les deux domaines s'approuvent mutuellement et qu'à partir de ce moment n'importe quel utilisateur d'un domaine peut accéder aux ressources de l'autre domaine. La figure ci-dessous montre cet exemple :

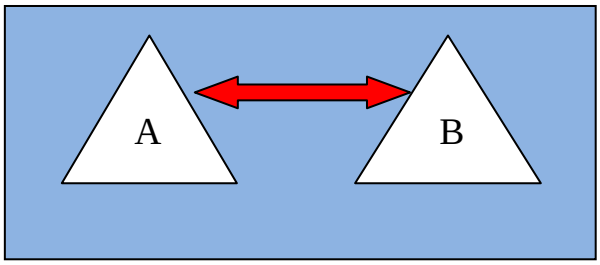


Figure II.2 : relation d'approbation bidirectionnelle

II.3.3 La transitivité

Ce terme fait référence à la notion mathématique au sens propre du terme, c'est à dire que si un domaine A approuve un domaine B et que le domaine B approuve lui même un domaine C et bien alors implicitement le domaine A approuvera le domaine C. Toutes les relations d'approbation ne sont pas forcément transitives. Cette figure montre un exemple de relation d'approbation transitive.

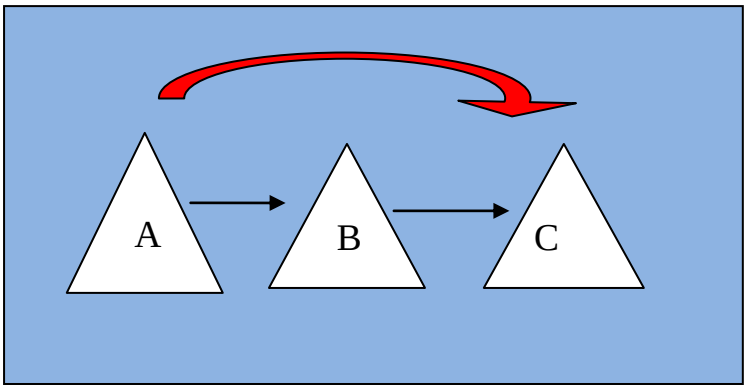


Figure II.3 : relation d'approbation transitive

II.3.4 Automatique ou manuelle

Certaine approbations sont crées automatiquement. D'autre doivent être manuellement.

Dans une forêt, tous les domaines s'approuvent mutuellement. En effet, le domaine racine de chaque arbre d'une forêt approuve le domaine racine de la forêt c'est -à- dire le premier domaine installé dans la forêt, et chaque domaine enfant approuve son domaine parent. Toutes les approbations crées automatiquement ne doivent jamais être supprimées et sont transitives et bidirectionnelles.

Les approbations vers d'autres forêts et domaines externes doivent être établies manuellement.

II.4 .Les différents types de relations d'approbation

II.4.1. Relations d'approbations prédéfinies

II.4.1.1.Approbation parent/enfant

Une approbation parent-enfant est une relation d'approbation bidirectionnelle transitive. Elle est automatiquement crée lorsqu'un nouveau domaine est ajouté à une arborescence.

Dans l'exemple ci-contre, on ajoute le sous domaine Alger.2int.com à l'intérieur du domaine 2int .com. Les deux domaines sont automatiquement reliés par une relation parent-enfant. Ainsi les utilisateurs du domaine 2int.com peuvent être authentifiés dans le domaine Alger.2int.com et vice-versa.

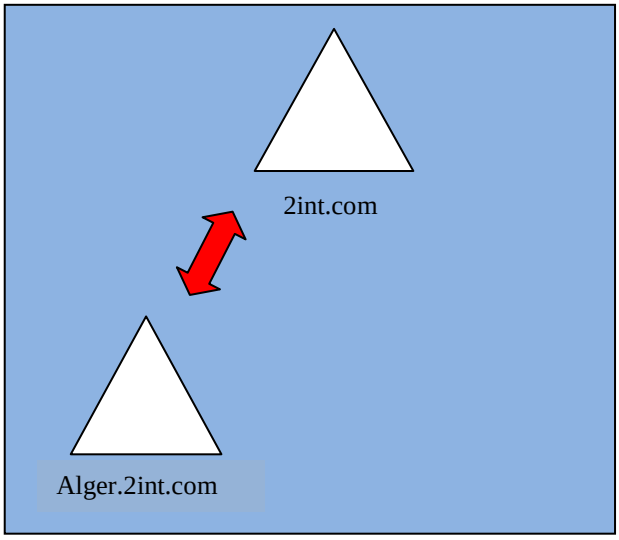


Figure II.4: approbation parent/enfant

II.4.1.2 Approbation racine d'arborescence

Lorsqu'une nouvelle arborescence est crée au sein d'une forêt, une relation d'approbation bidirectionnelle transitive lie automatiquement cette nouvelle arborescence au domaine racine de la forêt. Cela de deux arborescences de la même forêt n'est possible qu'entre les racines.

Dans l'exemple ci-contre, l'arborescence *ssnet.com* est liée à *2int.com* qui est le domaine racine de la forêt par le biais d'une relation racine/arborescence.

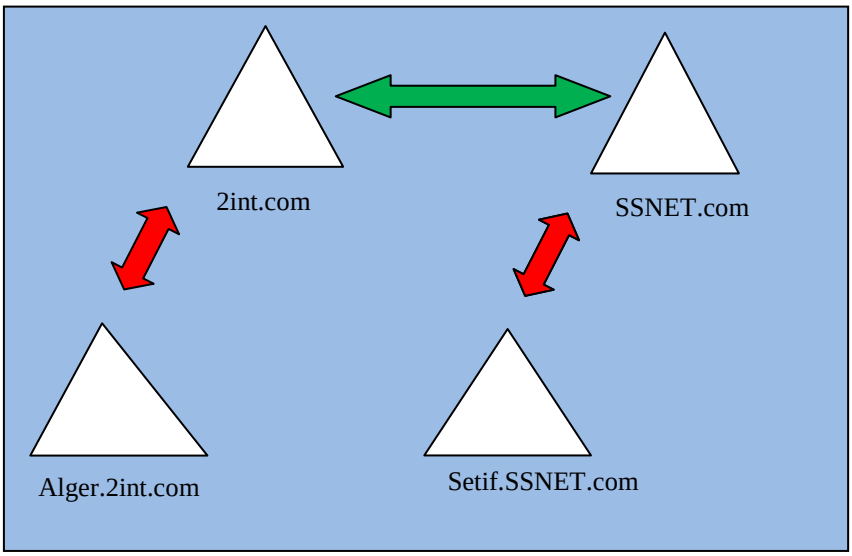


Figure II.5 : approbation racine d'arborescence

II.4.1.3 Approbations raccourcies

Il s'agit tout simplement d'approbations externes crées pour raccourcir le chemin entre deux domaines d'une même forêt lorsque les utilisateurs de l'un ou des domaines ont besoin d'un accès fréquent aux ressources de l'autre domaine. Ces relations raccourcies sont transitives et peuvent être à sens unique ou bidirectionnelles.

En créant une approbation raccourcie entre deux domaines d'une forêt, le processus d'authentification Kerberos, par lequel un accès à des ressources dans deux domaines différents est accordé à des utilisateurs, est considérablement plus court d'un point de vue du nombre de domaine à traverser, réduisant d'autant le trafic d'authentification et accélérant le processus d'authentification inter-domaine. Ce type de relations d'approbations reste utile uniquement pour les organisations possédant plusieurs niveaux de domaines.

En effet, si un utilisateur du domaine Alger.2int.com souhaite s'authentifier dans le domaine Setif.SSNET.com, il doit passer par deux approbations parent/enfant et par une approbation racine/arborescence.

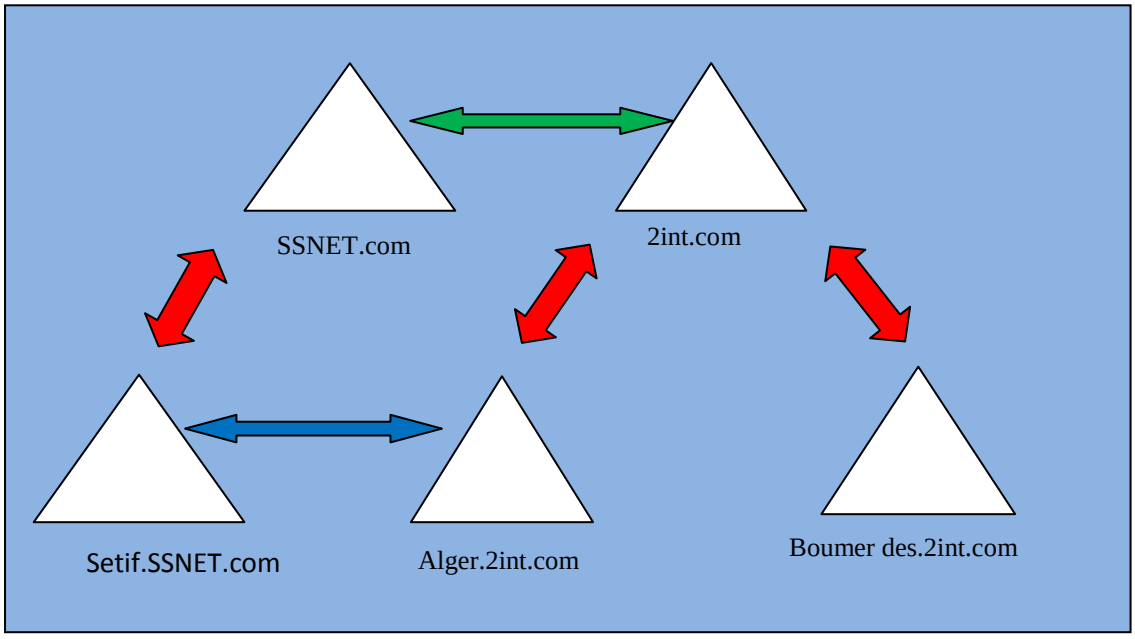


Figure II.6 : Approbation raccourcie

II.4.2.Approbations externes

Une approbation externe est une relation d'approbation non transitive. Elle doit être crée manuellement et peut avoir une direction unidirectionnelle ou bidirectionnelle.

L'approbation externe permet de relier des domaines appartenant à deux forêts distinctes. Elle permet ainsi aux utilisateurs d'avoir accès aux ressources d'une autre forêt de façon totalement transparente.

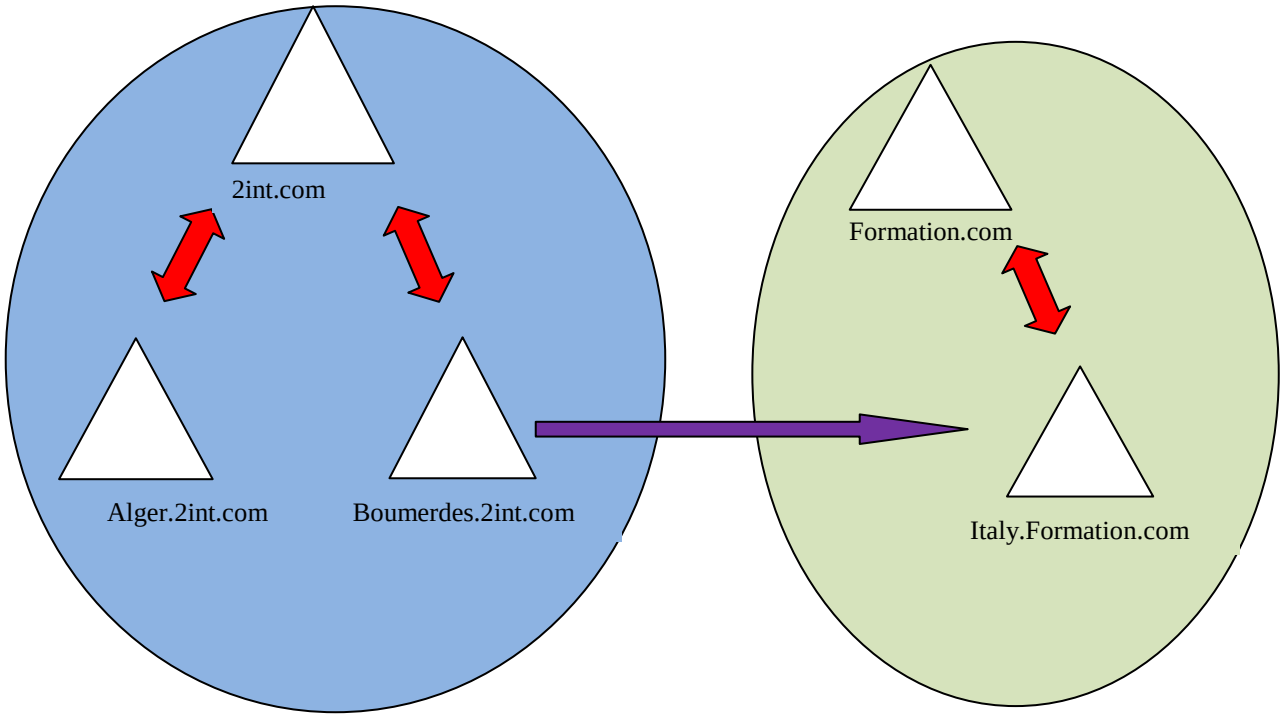


Figure II.7 : Une approbation externe vers un domaine dans une autre forêt.

II.4.3. Approbations de domaine

Une approbation de domaine est une relation d'approbation dont la transitivité et la direction doivent être paramétrées par l'administrateur. Elle peut être unidirectionnelle ou bidirectionnelle.

L'approbation de domaine permet de relier un domaine sous Active Directory avec un domaine Kerberos non Microsoft.

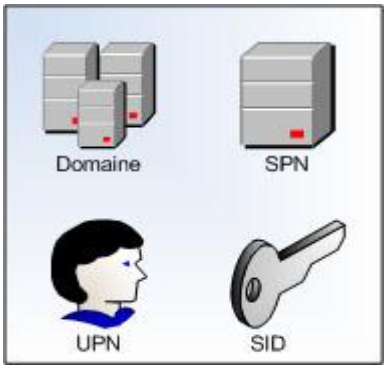
II.4.4. Approbations de forêts

Les approbations de forêt permettent aux utilisateurs d'une forêt d'accéder aux ressources d'une autre forêt en utilisant l'authentification Kerberos ou NTLM.

Les approbations de forêts sont des approbations à sens unique ou bidirectionnelle qui peuvent être créées manuellement entre les domaines racines de deux forêts. Il n'existe pas de transitivité entre les forêts, par exemple, si la forêt 1 donne son approbation à la forêt 2 et que la forêt 2 donne son approbation à la forêt 3, ceci ne veut pas dire qu'une relation d'approbation est créée entre la forêt 1 et la forêt 3.

Les approbations de forêts sont considérablement plus simples à établir, maintenir, administrer que les relations d'approbation entre chacun des domaines des forêts et elles permettent également une meilleure gestion des espaces de noms approuvés.

Les **espaces de nom Domaine**, nom d'utilisateur principal (**UPN, User Principal Name**), nom de service principal (**SPN, Service Principal Name)**, et (**SID, Security identifier)** qu'une forêt publie seront automatiquement collectés lors de la création d'une approbation de forêt et actualisés par l'interface utilisateur Domaine et approbation Active Directory.



La forêt sera ainsi approuvée comme faisant autorité pour les espaces de noms qu'elle publiera, à la condition que ces espaces de noms n'entrent pas en conflit avec des espaces de noms approuvés appartenant déjà à des relations d'approbation de forêt existantes.

Avant de mettre en œuvre une approbation de forêt, on doit remplir plusieurs exigences. Le niveau fonctionnel de forêt doit être défini à Windows Server 2003ou ultérieur. En outre, on doit posséder une infrastructure DNS spécifique qui prenne en charge une approbation de forêt.

Ces approbations de forêts sont particulièrement utiles dans des scénarios qui impliquent une collaboration entre des organisations ou au sein d'une seule organisation qui possède

plusieurs forêts, afin d'isoler les données et les services Active Directory. La figure ci-dessous illustre un exemple d'approbation de forêts.

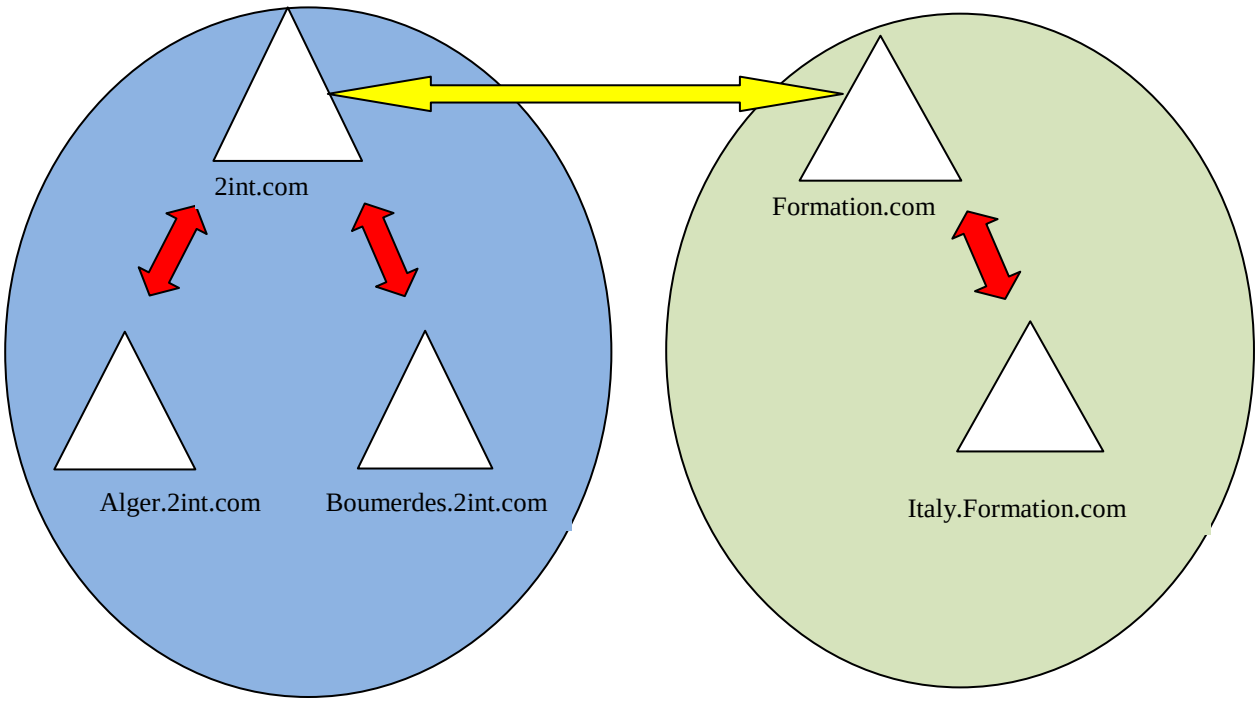


Figure II.8 : Une approbation de forêt.

II.5.Les avantages d'approbation de forêts

Les approbations de forêt peuvent apporter les avantages suivants :

- Simplification de la gestion des ressources entre deux forêts Windows Server 2008 par la réduction du nombre d'approbations externes nécessaires pour partager les ressources.
- Relations bidirectionnelles complètes avec chaque domaine de chaque forêt
- Utilisation d'une authentification par nom principal de l'utilisateur (UPN) entre deux forêts.
- Utilisation des protocoles d'authentification Kerberos V5 et NTLM, qui améliorent la fiabilité des données d'autorisation échangées par les forêts.
- Souplesse d'administration(chaque forêt peut avoir ses propres tâches d'administration)

II .6.Les protocoles d'approbation

Un contrôleur de domaine authentifie les utilisateurs et les applications à l'aide de l'un des deux protocoles suivants : Kerberos version 5 (V5) ou NTLM.

II .6 .1.Le protocole d'authentification Windows NT LAN Manager (NTLM)

Le protocole NTLM est utilisé par Windows NT 4.0 et les versions antérieures de Windows NT. Il continuera d'être pris en charge et utilisé pour l'authentification réseau "pass-through", l'accès fichier à distance et les connexions RPC authentifiées avec les versions précédentes de Windows NT.

Lorsqu'un client tente d'accéder aux ressources d'un serveur d'un autre domaine à l'aide de l'authentification NTLM, le serveur contenant les ressources doit contacter un contrôleur de domaine appartenant au domaine de compte du client afin de vérifier les informations d'identification du compte.

II.6.2.Le protocole Kerberos V5

Le protocole d'authentification Kerberos définit les interactions entre un client et un service d'authentification réseau appelé KDC (Key Distribution Center).

Lorsqu'un utilisateur se connecte au domaine, Kerberos authentifie ses informations d'identification et émet un ensemble d'information nommé ticket d'accord de ticket (TGT, Ticket Granting Ticket) avant que l'utilisateur ne se connecte au serveur pour demander le document, une requête Kerberos est envoyée au contrôleur de domaine avec le TGT qui identifie l'utilisateur authentifié. Le contrôleur de domaine envoie à l'utilisateur un autre ensemble d'informations nommé ticket de service, qui authentifie l'utilisateur auprès du serveur. L'utilisateur présente le ticket de service au serveur, qui l'accepte comme preuve que celui-ci a été authentifié.

Ces transactions Kerberos aboutissent à une connexion unique au réseau. Après que l'utilisateur s'est connecté et a reçu un TGT, il est authentifié dans l'ensemble du domaine et peut recevoir des tickets de service qui l'identifient auprès de n'importe quel service. Toute cette activité d'émission de tickets est gérée par les services et les clients kerberos intégrés à Windows, et est transparente pour l'utilisateur.

La figure suivante montre le fonctionnement de protocole kerberos

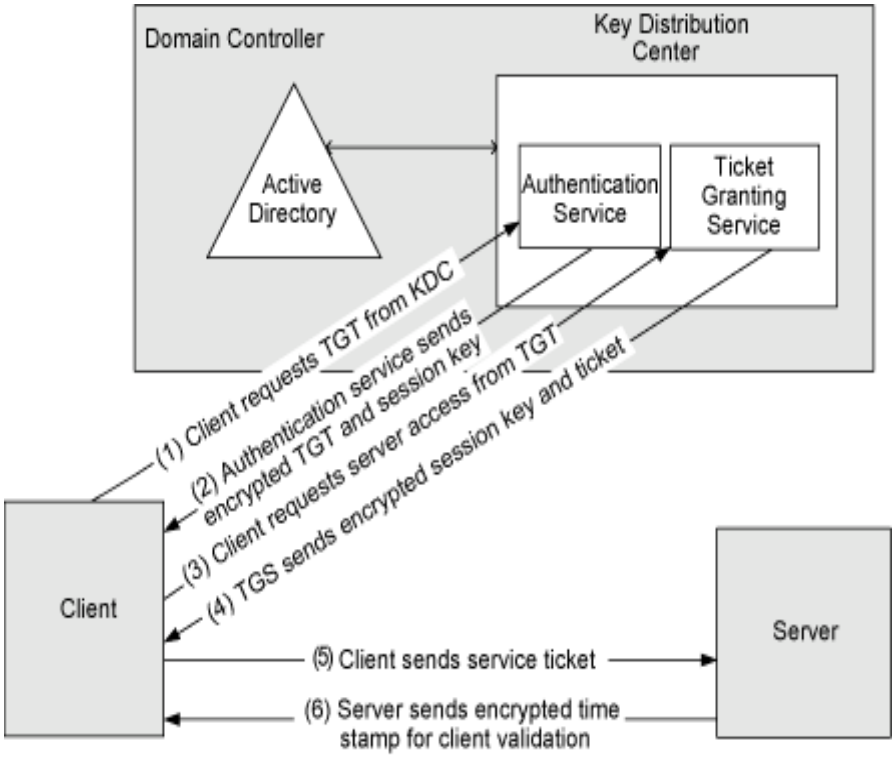


Figure II.9 : fonctionnement de protocole KERBEROS

II.7.Le fonctionnement des approbations

II.7.1.Le fonctionnements des approbations dans une forêt

Lorsqu'un utilisateur tente d'accéder à une ressource d'un autre domaine, le protocole d'authentification kerberos version 5, doit déterminer si le domaine à approuver possède une relation d'approbation avec le domaine approuvé.

Pour déterminer cette relation, le protocole kerberos version 5, suit le chemin d'approbation en utilisant le TDO afin d'obtenir une référence au contrôleur de domaine du domaine cible. Le contrôleur de domaine cible émet un ticket de service pour le service demandé. Le chemin d'approbation est le chemin d'accès le plus court dans la hiérarchie d'approbation.

Lorsqu'un utilisateur du domaine approuvé tente d'accéder aux ressources d'un autre domaine, son ordinateur contacte d'abord le contrôleur de domaine de son domaine afin d'obtenir l'authentification pour la ressource. Si la ressource ne se trouve pas dans le domaine

de l'utilisateur, le contrôleur de domaine utilise la relation d'approbation avec son parent et renvoie l'ordinateur de l'utilisateur vers un contrôleur de domaine de son domaine parent.

Cette tentative de localisation de la ressource se poursuit jusqu'au sommet de la hiérarchie, si possible vers le domaine racine de la forêt, et vers le bas de la hiérarchie tant qu'un contacte n'est pas établi avec un contrôleur de domaine du domaine dans lequel se trouve la ressource.

II.7.2. Le fonctionnement des approbations entre les forêts

Windows Server 2008 prend en charge les approbations entre les forêts, qui permettent aux utilisateurs d'accéder aux ressources d'une autre forêt. Lorsqu'un utilisateur tente d'accéder aux ressources d'une forêt approuvée, Active Directory doit préalablement rechercher les ressources. Une fois que les ressources localisées, l'utilisateur peut être authentifié et autorisé à accéder aux ressources.

- **Comment s'effectue l'accès à une ressource**

Nous prenons l'exemple d'approbation des forêts précédent : forêt 2int.com et forêt Formation.com. L'accès à la ressource s'effectue par les étapes suivantes :

- Un utilisateur qui a ouvert une session sur le domaine Alger.2int.com tente d'accéder à un à un dossier partagé de la forêt Formation.com. L'ordinateur de l'utilisateur contacte le centre de distribution de clés (KDC, Key Distribution Center) d'un contrôleur de domaine d'Alger.2int.com et demande un ticket de service en utilisant le SPN de l'ordinateur sur lequel résident les ressources. Un SPN peut être le nom DNS d'un hôte ou d'un domaine, ou le nom unique d'un objet point de connexion de service.
- Les ressources ne sont pas localisées dans Alger.2int.com, le contrôleur de domaine d'Alger.2int.com demande donc au catalogue global de voir si elles se trouvent dans un autre domaine de la forêt. Étant donné qu'un catalogue global ne contient que des informations relatives à sa propre forêt, il ne trouve pas le SPN. Il recherche alors dans sa base de données les informations relatives à des approbations de forêt qui ont été établies avec sa forêt. S'il en trouve une, il compare les suffixes de noms répertoriés dans le TDO de l'approbation de forêt par rapport au suffixe du SPN cible. S'il trouve une correspondance, le catalogue global fournit les informations de routage relatives à la manière de localiser les ressources au contrôleur de domaine d'Alger.2int.com.

- Le contrôleur de domaine d'Alger.2int.com envoie une référence à son domaine parent, 2int.com, à l'ordinateur de l'utilisateur.
- L'ordinateur de l'utilisateur contacte un contrôleur de domaine de 2int .com pour obtenir une référence à un contrôleur de domaine du domaine racine de la forêt Formation.com.
- Grace à la référence renvoyée par le contrôleur de domaine de 2int.com, l'ordinateur de l'utilisateur contacte un contrôleur de domaine de la forêt Formation.com.pour obtenir un ticket de service pour le service demandé.
- Les ressources ne se trouvent pas dans le domaine racine de la forêt Formation.com, le contrôleur de domaine contacte donc son catalogue global pour trouver le SPN .le catalogue global trouve une correspondance pour le SPN et l'envoie au contrôleur de domaine.
- Le contrôleur de domaine envoie une référence à Italy.Formation.com à l'ordinateur de l'utilisateur.
- L'ordinateur de l'utilisateur contacte le KDC sur le contrôleur de domaine d'Alger.2int.com et négocie un ticket pour l'utilisateur afin de pouvoir accéder aux ressources du domaine Alger.2int.com.
- L'ordinateur de l'utilisateur envoie le ticket de service à l'ordinateur sur lequel se trouvent les ressources partagées, il lit les informations d'identification de sécurité et crée un jeton d'accès permettant à l'utilisateur d'accéder aux ressources.

II.8. Sécuriser des relations d'approbations

Les relations d'approbations créent des points d'entrées supplémentaires pour les attaques potentielles, car un intrus peut non seulement essayer de modifier un compte utilisateur dans un domaine donné, mais également dans tous les domaines approuvés. Il est donc capital pour les administrateurs de veiller aux contrôle de sécurité lorsqu'ils créent des relations d'approbation.

- **Utilisateurs authentifiés**

Une relation d'approbation ne donne pas en soi accès à des ressources ; toutefois, il est possible qu'en créant une relation d'approbation, des utilisateurs du domaine approuvé aient un accès immédiat vers plusieurs ressources de notre domaine. En effet, de nombreuses ressources sont protégées par des ACL qui donnent des autorisations au groupe utilisateurs

authentifiés.

- **Appartenance à des groupes de domaine locaux**

La meilleure pratique pour gérer l'accès à une ressource est d'accorder des autorisations à un groupe de domaine local. Nous pouvons ensuite imbriquer des utilisateurs et des groupes de notre domaine dans le groupe de domaine local et leur accorder de ce fait un accès à la ressource. Les groupes de sécurité à étendue de domaine local peuvent également contenir comme membres des utilisateurs et des groupes globaux de domaines approuvés.

En conséquence, la façon la plus gérable d'accorder des autorisations aux utilisateurs d'un domaine approuvé est qu'ils deviennent, eux ou leurs groupes globaux, des membres d'un groupe de domaine local dans notre domaine.

- **ACL**

Les ressources partagées sur un réseau incluent des listes de contrôle d'accès (ACL) qui définissent qui peut accéder à la ressource.

Pour mieux sécuriser la relation d'approbation, nous pouvons ajouter des utilisateurs et des groupes globaux d'un domaine approuvé directement aux ACL des ressources situées dans un domaine d'approbation.

- **Transitivité**

Lorsque nous créons une approbation de domaine kerberos, celle-ci est non transitive par défaut. Si nous la rendons transitive, nous donnons la possibilité aux utilisateurs de domaines et de domaines kerberos approuvés par le domaine kerberos v5 d'accéder aux ressources de notre domaine. Il est recommandé d'utiliser des approbations non transitives, à moins qu'une raisons métier ne nous contraigne à utiliser une approbation de domaine kerberos transitive.

- **Quarantaine de domaine**

Par défaut, la mise en quarantaine d'un domaine, également appelée filtrage SID, est activée sur toutes les approbations externes et approbation de forêt.

Lorsqu'un utilisateur est authentifié dans un domaine approuvé, il présente les données d'autorisation qui contiennent les SID du compte de l'utilisateur dans les groupes auquel il appartient. En outre, les données d'autorisation de l'utilisateur s'accompagnent des identificateurs de sécurité issus d'autres attributs de l'utilisateur et de ses groupes.

Certains SID présentés par l'utilisateur du domaine approuvé peuvent ne pas avoir été

crées dans le domaine approuvé, dans ce cas il est possible qu'un administrateur malveillant utilise des informations d'identification d'administration dans le domaine approuvé pour charger des SID (dans le cas de migration d'un domaine à un autre).

La quarantaine de domaine remédie à ce problème en permettant au domaine d'approbation de filtrer les SID du domaine approuvé qui ne sont pas les SID principaux des entités de sécurité. Chaque SID contient le SID de son domaine d'origine. Ainsi, si un utilisateur d'un domaine approuvé présente sa liste de SID et ceux de ses groupes, le filtrage des SID indique au domaine d'approbation de supprimer tous les SID qui n'ont pas le SID de domaine du domaine approuvé.

- **Authentification sélective**

Lorsque nous créions une approbation externe ou une approbation de forêt, nous pouvons contrôler l'étendue de l'authentification des entités de sécurité approuvées. Il existe deux modes d'authentification pour une approbation externe ou de forêt :

- ✓ Authentification à l'échelle du domaine (pour une approbation externe) ou à l'échelle de la forêt (pour une approbation de forêt).
- ✓ Authentification sélective

Si nous choisissons l'autorisation à l'échelle du domaine ou de la forêt, tous les utilisateurs approuvés peuvent être authentifiés pour accéder aux services qui se trouvent sur tous les ordinateurs du domaine d'approbation. Les utilisateurs approuvés peuvent donc recevoir l'autorisation d'accéder aux ressources dans tous le domaine d'approbation.

Avec ce mode d'authentification, nous devons avoir confiance dans les procédures de sécurité de notre entreprise et dans les administrateurs que les mettent en œuvre afin qu'aucun accès inapproprié soit accorder à des utilisateurs approuvés.

Si toutefois, nous optons pour l'authentification sélective, tous les utilisateurs du domaine approuvé sont des identités approuvées. Ils ne peuvent authentifier que des services situés

sur les ordinateurs que nous avons spécifiés.

II.9.Discussion

Dans ce chapitre nous avons présenté l'intérêt des relations d'approbation qui permettent à des utilisateurs d'un domaine approuvé d'être authentifiés par des ordinateurs d'un domaine d'approbation ainsi leurs caractéristiques.

Nous avons présenté également les différents types d'approbation et le fonctionnement de celle-ci ainsi les sections utilisés pour sécuriser ces relations d'approbation.

Pour mieux sécuriser ces relations d'approbations de forêts et assurer l'échange de données entre eux nous devons utiliser un VPN site à site qu'on va étudier dans le troisième chapitre.

III.1.Préambule

Les entreprises se servent de réseaux privés pour communiquer avec des sites distants et d'autres entreprises. Elles utilisent des lignes louées, sécurisés mais coûteuses et les postes nomades accèdent à l'entreprise via des communications RTC qui sont faibles.

La mise en place d'un VPN doit permettre des connexions distantes (sites ou postes isolés) sécurisées et surtout moins coûteuses puisque utilisant Internet.

III.2.Définition d'un VPN

L'acronyme VPN correspond à Virtuel Private Network, c'est-à-dire un réseau privé virtuel. Dans les faits, cela correspond à une liaison permanente, distante et sécurisée entre deux sites d'une organisation. Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme Internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partagés ou publics, tels qu'Internet. Il permet d'échanger des données entre deux entités sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

III.3.Intérêt d'un VPN

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local.

Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. Nous pouvons facilement imaginer un grand nombre d'applications possible:

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades.
- Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante ;
- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet ;
- Les connexions VPN permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, tel

qu'Internet, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement ;

- Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée.
- Les connexions VPN permettent de partager des fichiers et des programmes de manière sécurisés entre une machine locale et une machine distante.

III.4.Les Caractéristiques d'un VPN

Une solution de VPN devrait fournir au moins l'ensemble des caractéristiques suivantes :

- **Authentification d'utilisateurs**: seuls les utilisateurs autorisés de la connexion VPN doivent pouvoir s'identifier sur le réseau virtuel.
- **Cryptage des données :** nécessité de cryptage des données pour protéger les données échangées entre le client et le serveur VPN.
- **Adressage :** attribuer au client VPN une adresse IP privée lors de la connexion au réseau distant et garantir que cette adresse reste confidentielle.
- **Filtrage de paquet :** mise en place de filtres sur l'interface correspondant à la connexion à Internet du serveur VPN.
- **Gestion des clés** : les clés de cryptage pour le client et le serveur doivent être générées et régénérées**.**
- **Support multi protocole :** La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

III.5.Les différentes architectures des VPN

III.5.1. De poste à poste

C'est le cas d'utilisation le plus simple. Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de bases de données entre deux serveurs d'une entreprise disposant de chaque coté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation.

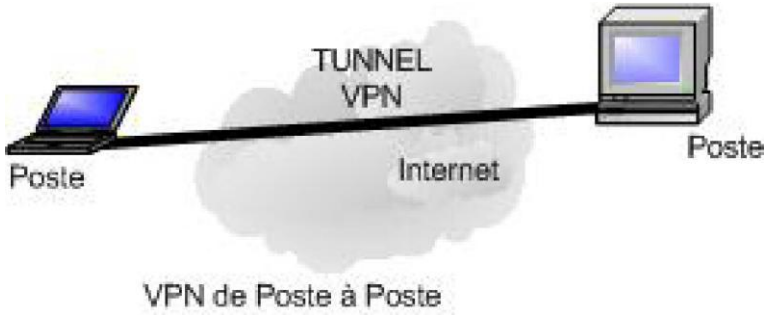


Figure III.1 : VPN de poste à poste.

III.5.2. De poste à site

Un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion Internet. Le développement de l'ADSL favorise ce genre d'utilisation.

Attention toutefois à interdire l'accès Internet depuis le poste « localement ». Pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise.

Ce point est important et rejoint la réflexion plus large de la sécurité des sites mis en relation par un VPN. Lorsque les niveaux de sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux. S'il existe une faille de sécurité sur un site (ou sur un poste nomade), celle-ci peut être exploitée

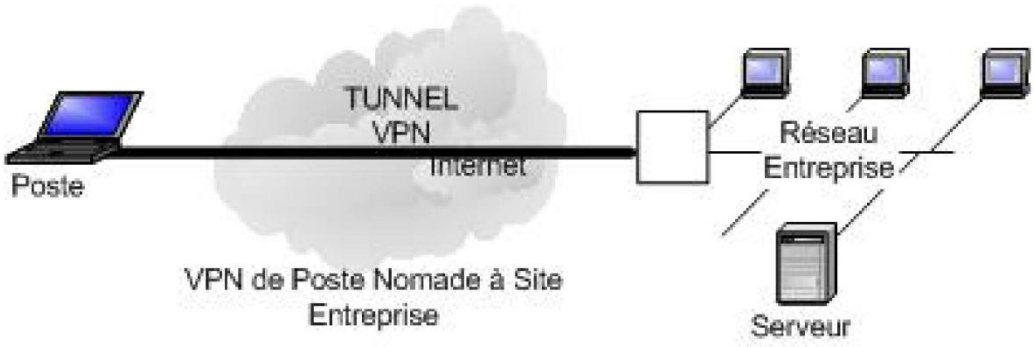


Figure III.2 : VPN de poste Nomade à site Entreprise.

III.5.3.De site à site

Elle correspond à un type d'infrastructure de réseau étendu, c'est-à-dire que l'interconnexion entre les VPN remplace et améliorent les réseaux privé existants. Elle utilise pour relier un site avec une de ses filiales, à moindre coût et en toute sécurité.

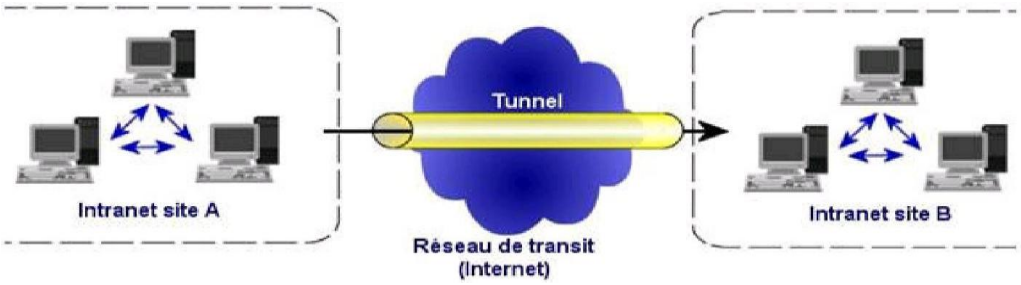


Figure III.3 : VPN de site à site.

III.6.Les différents types de VPN

III.6.1.Le VPN d'accès

Il est utilisé pour permettre à des utilisateurs d'accéder au réseau privé. Grâce à une connexion Internet, l'utilisateur établit la connexion VPN. On peut définir deux méthodes d'accès aux VPN :

- L'utilisateur demande à son fournisseur d'accès de lui établir une connexion vers un serveur dit distant. Cela lui permet de communiquer sur différents réseaux en créant plusieurs tunnels.
- L'utilisateur à son propre logiciel client pour le VPN et établit directement la connexion de manière codée vers le réseau de l'entreprise. Dans ce cas la totalité des informations est cryptée dès le début de la connexion.

III.6.2.L'intranet VPN

Il est utilisé pour relier au minimum deux intranets entre eux. C'est un réseau particulièrement utile pour une entreprise qui possède des agences à travers le monde, car il facilite la communication. Le plus important c'est qu'il garantit la sécurité des données. Des techniques d'authentification comme la cryptographie sont mises en œuvres pour assurer la validité des données et l'authentification de la source.

III.6.3.L'extranet VPN

Dans le but d'échanger et de communiquer avec ses clients et ses partenaires, l'entreprise à la possibilité de mettre en place un extranet VPN qui ouvre l'accès aux réseaux locaux pour des personnes extérieurs.

III.7.Le principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé protocole de tunnellisation (tunneling). Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à

l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou extranets d'entreprise, les réseaux privé virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

III.8. Cryptage et Authentification

III.8.1.Cryptage

La cryptographie est une méthode permettant de rendre secrètes (illisibles) des informations afin de garantir l'accès à un seul destinataire authentifié. Elle est essentiellement basée sur l'arithmétique : il s'agit de transformer les lettres qui composent le message en succession de chiffres, puis faire des calculs sur ces chiffres pour :

- D'une part les modifier de telle façon à les rendre incompréhensible.
- Faire en sorte que le destinataire saura les décryptées.

Le fait de coder un message de façon à le rendre secret s'appelle le cryptage. La méthode inverse est appelée décryptage, elle nécessite une clé de décryptage.
On distingue de types de cryptages :

- **Cryptage symétrique**

Le cryptage symétrique appelé également cryptage à clé secrète ou chiffrement conventionnel, utilise une même clé pour crypter et décrypter le message, très efficace et assez économe en ressource CUP. Les algorithmes de chiffrement les plus connus sont :

DES (Data Encryptions Standard) et 3DES et AES

Le principe problème de cette technique la distribution des clés dans un réseau étendu, nécessite de partager une seul clé avec chacun de nos correspondants.

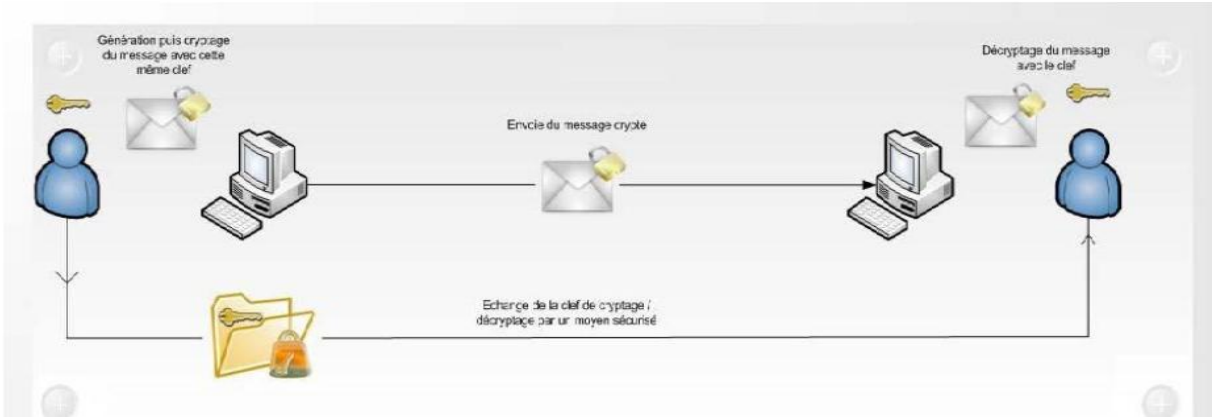


Figure III.4: Cryptage symétrique

On a un utilisateur A et un utilisateur B, lorsque l'utilisateur A veut envoyer son numéro de carte de crédit a l'utilisateur B il va le crypté avec une clé, le résultat de cryptage va transiter par Internet et lorsqu'il arrive à B il le décrypte avec la même clé et on obtient le document initial qui contient le numéro de carte de crédit.

- **Cryptage asymétrique**

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante car ces deux clés générer au même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons :

-Plus évolutif pour les systèmes possédant des millions d'utilisateurs.

- Permet de signer le message donc garantir l'Authentification et la non- répudiation.

-Supporte les signatures numériques.

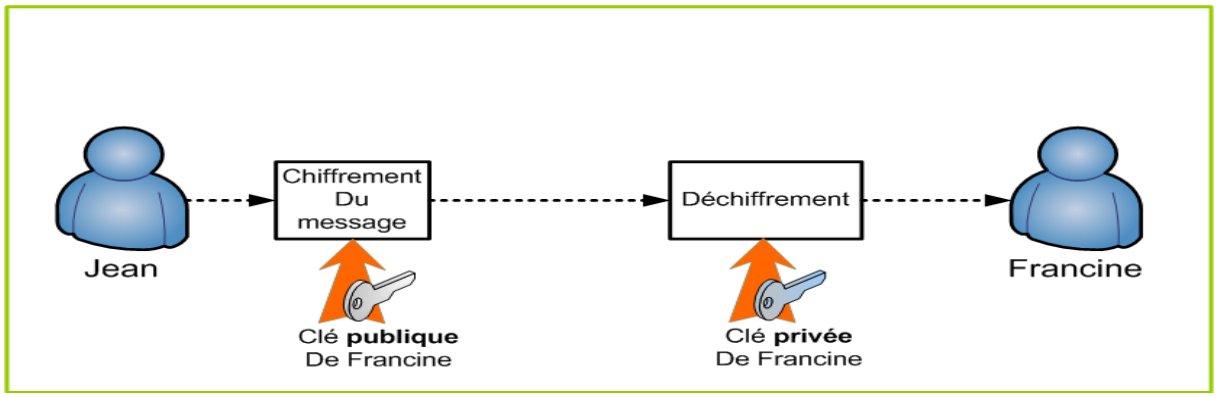


Figure III.5: Cryptage asymétrique

III.8.2.L'authentification

Permettant de vérifier les identités présumées des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle de l'authentification simple. Lorsque nécessite plusieurs facteurs on parle de l'authentification forte.

L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

-Un élément d'information que l'utilisateur connaît (mot de passe, etc)

-Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat)

-Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (ADN, empreinte digitale, fond de rétine.)

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle internet :

-Au niveau applicatif : HTTP, FTP

-Au niveau transport : SSL, SSH

-Au niveau réseau : IPSEC

-Au niveau transmission : PAP, CHAP

III.9.Protocoles utilisés et sécurité des VPN

Il existe plusieurs protocoles dit encapsulation (tunneling) qui permettent la création des réseaux VPN :

III.9.1.PPP (Point to Point Protocol)

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IPx dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau.

Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP.

III.9.2.Le protocole PPTP (Point To Point Tunneling Protocol)

PPTP (Point to Point Tunneling Protocol) est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. Ainsi, PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression.

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP.PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation).

Le tunnel PPTP se caractérise par :

- Une initialisation du client.
- Une connexion de contrôle entre le client et le serveur.
- La clôture du tunnel par le serveur.

Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établit une connexion de type PPP et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

III.9.3.L2F

L2F a été développé par Cisco Systems comme une alternative au protocole PPTP. Comme ce dernier il s'appuie sur la couche deux du modèle OSI. Il est par contre beaucoup plus souple sur les protocoles réseaux utilisés. En effet, PPTP ne peut être encapsulée que

dans des paquets IP alors que L2F peut aussi être encapsulé dans du X25 par exemple. Comme pour PPTP, L2F permet l'utilisation de différentes méthodes d'authentification.

L'authentification L2F est différente de celle de PPTP qui nécessite juste l'autorisation du RAS du LAN sur lequel on se connecte. En effet, l'authentification L2F nécessite l'approbation préalable du serveur RAS.

III.9.4.L2TP (Layer Two Tunneling Protocol)

L2TP est issu de la convergence des protocoles PPTP et L2F .Il est actuellement développé et évalué conjointement par Cisco, Microsoft, ainsi que d'autres acteurs du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (liaison de données) et 3 (réseau). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur Internet.

L2TP repose sur deux concepts :

- Les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator).
- Les serveurs réseau L2TP (LNS : L2TP Network Server).

Un élément intéressant de L2TP est l'utilisation d'UDP. Ce qui laisse entrevoir une vitesse d'acheminement supérieure. Cela implique également le fait que UDP offre des services moindres que TCP, il s'agit de les compenser ailleurs.

III.9.5. Le protocole SSL (Secure Socket Layer)

SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

SSL est le dernier arrivé dans le monde des VPN, mais il présente un gros avantages dans la mesure où coté client, il ne nécessite qu'un navigateur Internet standard. Ce protocole est celui qui est utilisé en standard pour les transactions sécurisées sur Internet

L'inconvénient néanmoins de ce type de protocole est qu'il se limite au protocole https, ce qui n'est pas le seul besoin de connexion des entreprises.

- **Les fonctionnalités de SSL**

SSL a trois fonctions:

- **Authentification du serveur**

Qui permet à un utilisateur d'avoir une confirmation de l'identité du serveur. Cela est fait par les méthodes de chiffrement à clés publiques qu'utilise SSL. Cette opération est

importante, car le client doit pouvoir être certain de l'identité de son interlocuteur à qui par exemple, il va communiquer son numéro de carte de crédit.

- **Authentification du client**

Selon les mêmes modalités que pour le serveur, il s'agit de s'assurer que le client est bien celui qu'il prétend.

- **Chiffrement des données**

Toutes les données qui transitent entre l'émetteur et le destinataire, sont chiffrées par l'émetteur, et déchiffrées par le destinataire, ce qui permet de garantir la confidentialité des données, ainsi que leur intégrité grâce souvent à des mécanismes également mis en place dans ce sens.

III.9.6.Le protocole SSH

SSH est un protocole permettant d'établir une session interactive chiffrée entre un client et un serveur. Ainsi, les flux d'informations entre ces deux entités sont cryptés ce qui garantit la confidentialité. De plus, il permet l'identification de la machine distante. L'algorithme utilisé pour la négociation des clés est RSA (dont le brevet a expiré aux USA ce qui permet une utilisation publique légale).

Une fois l'échange des clés effectué, la communication entre les deux machines se fait en utilisant un chiffrage symétrique. Les principaux algorithmes utilisés dans SSH sont triple DES (3DES) ainsi que Blowfish. La plupart des fonctionnalités cryptographiques étant implémentés dans la bibliothèque Open SSL. La version du protocole SSH utilisée est la version2, la première version de ce protocole souffrait d'une grosse faille de sécurité.

III.9.7.Le protocole IP Sec (Internet Protocol Security)

III.9.7.1.Présentation de protocole IP Sec

IP Sec (Internet Protocol Security) est un protocole de la couche 3 du modèle OSI. Les concepteurs, S. Kent et R. Atkinson de chez IETF (Internet Engineering Task Force) ont proposé une solution en novembre 1998 afin de répondre aux besoins directs du développement des réseaux en matière de sécurité. En effet, en sécurisant le transport des données lors d'échanges internes et externes, la stratégie IP Sec permet à l'administrateur réseau d'assurer une sécurité efficace pour son entreprise contre toute attaque venant de l'extérieur.

III.9.7.2.Concept de base d'IP Sec

Le protocole IP Sec est destiné à fournir différents services de sécurité. Il permet grâce à plusieurs choix et options de définir différents niveaux de sécurité afin de répondre de façon adaptée aux besoins de chaque entreprise. La stratégie IP Sec permettant d'assurer la confidentialité, l'intégrité et l'authentification des données entre deux hôtes est gérée par un ensemble de normes et de protocoles :

- **Authentification des extrémités :** Elle permet à chacun de s'assurer de l'identité de chacun des interlocuteurs. Précisons que l'authentification se fait entre les machines et non entre les utilisateurs, dans la mesure où IP Sec est un protocole de couche 3.
- **Confidentialité des données échangées** : Le contenu de chaque paquet IP peut être chiffré afin qu'aucune personne non autorisée ne puisse le lire.
- **Authenticité des données** : IP Sec permet de s'assurer que chaque paquet a bien été envoyé par l'hôte et qu'il a bien été reçu par le destinataire souhaité.
- **Intégrité des données échangées :** IP Sec permet de vérifier qu'aucune donnée n'a été altérée lors du trajet.
- **Protection contre les écoutes et analyses de trafic :** Le mode tunneling (détaillé plus loin) permet de chiffrer les adresses IP réelles et les entêtes des paquets IP de l'émetteur et du destinataire. Ce mode permet ainsi de contrecarrer toutes les attaques de ceux qui voudraient intercepter des trames afin d'en récupérer leur contenu.
- **Protection contre le rejeu** : IP Sec intègre la possibilité d'empêcher un pirate d'intercepter un paquet afin de le renvoyer à nouveau dans le but d'acquérir les mêmes droits que l'envoyeur d'origine.

Ces différentes caractéristiques permettent à l'hôte A de crypter ses données et de les envoyer vers l'hôte B via le réseau, puis à l'hôte B de les recevoir et de les décoder afin de les lire sans que personne ne puisse altérer ou récupérer ces données.

III.9.7.3.Les deux protocoles d'acheminement d'IP Sec

- **Le protocole AH (Authentification Header)**

L'Authentification Header (AH**)** est conçu pour assurer l'authenticité des datagrammes IP sans chiffrement des données (sans confidentialité).

Le principe d'AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Un numéro de séquence permet de détecter les tentatives de rejeu.

- **Le protocole ESP (Encapsulating Security Payload)**

Le premier rôle de l'ESP permet d'assurer la confidentialité mais peut aussi assurer l'authenticité des données.

Le principe d'ESP est de générer, à partir d'un datagramme IP classique, un nouveau datagramme dans lequel les données et éventuellement l'en-tête original, sont chiffrés. ESP peut également assurer l'authenticité des données par ajout d'un bloc d'authentification et la protection contre le rejeu par le biais d'un numéro de séquence.

III.9.7.4.IP sec en mode tunnel et transport

Il existe deux modes dans IP Sec, le mode Transport et le mode Tunnel.

Ces deux modes diffèrent par la méthode de construction des paquets IP des messages.

- **Mode transport**

Le mode transport protège uniquement le contenu du paquet IP sans toucher à l'en-tête, ce mode n'est utilisable que sur les équipements terminaux (postes clients, serveurs).

Le mode Transport fournit la sécurité aux couches de protocoles supérieures.

Le mode Transport protège la charge utile du paquet mais garde l'adresse IP originale en clair.

-L'adresse IP originale est utilisée pour router les paquets sur Internet.

-Le mode transport ESP est utilisé entre hosts.

- **Mode tunnel**

Le mode tunnel permet la création de tunnels par "encapsulation" de chaque paquet IP dans un nouveau paquet. Ainsi, la protection porte sur tous les champs des paquets IP arrivant à l'entrée d'un tunnel, y compris sur les champs des en-têtes (adresses source et destination par exemple).Ce mode est celui utilisé par les équipements réseau (routeurs, gardes-barrières...).

Le mode Tunnel fournit la sécurité pour tout le paquet IP.

- Le paquet IP original est crypté

-Le paquet crypté est encapsulé dans un autre paquet IP.

-L'adresse IP "outside" est utilisée pour router les paquets sur Internet

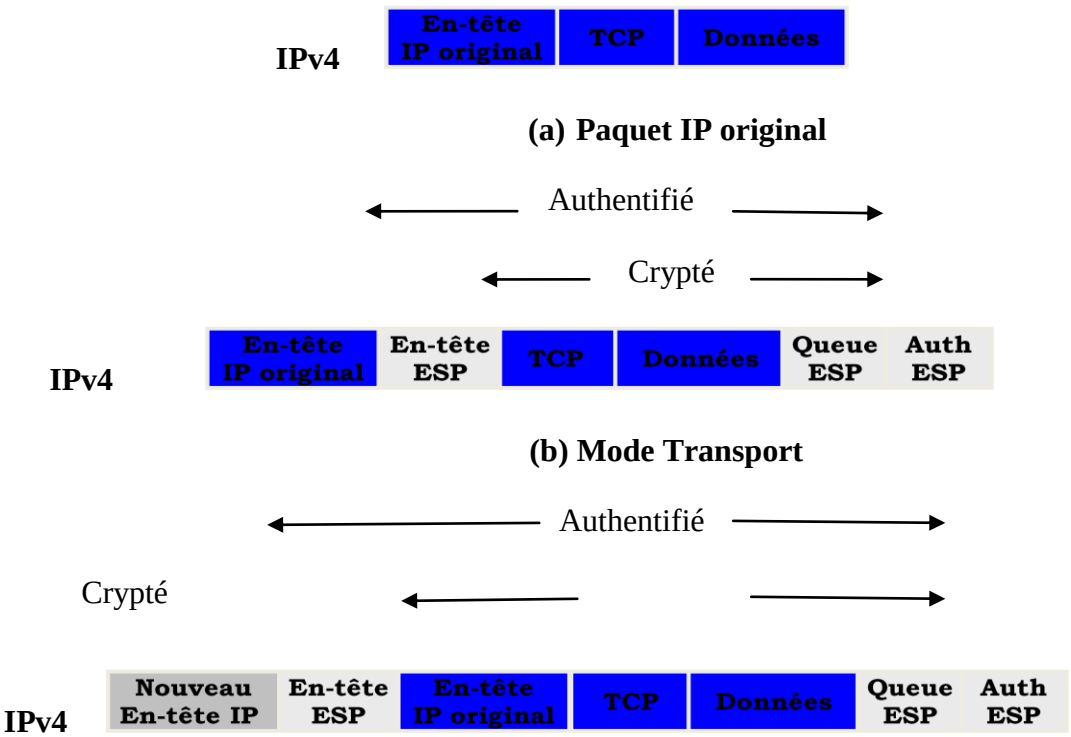


Figure III.6: les différences entre le mode tunnel et transport

III.10.SA (Security Association)

Les SAs sont des concepts de base très important dans IP Sec. Elles représentent un contrat entre deux extrémités et décrivent comment ces deux extrémités vont utiliser les services de sécurité IP Sec pour protéger le trafic. Les SAs contiennent tous les paramètres de sécurité nécessaires pour sécuriser le transport des paquets entre les deux extrémités et définissent la politique de sécurité utilisée dans IP Sec.

Une SA contient les paramètres de sécurité suivants:

- L'algorithme Authentification/Cryptage, longueurs de clés et durées de vie des clés utilisées pour protéger les paquets.
- Les clés de sessions pour l'authentification et le cryptage.
- L'encapsulation IP Sec (AH ou ESP) en mode tunnel ou transport.
- Une spécification du trafic réseau auquel s'applique la SA.

III.11. Les avantages et les inconvénients de VPN

Comme nous venons de le voir, les VPN disposent de nombreux avantages :

- Confidentialité et intégrité des données
- Forte authentification et identification des utilisateurs
- Solution simple et rapide à mettre en œuvre
- Flexible et évolutif
- Réduction des coûts d'infrastructure

Cependant ils peuvent aussi représenter quelques inconvénients :

- Faille de sécurité (si mal sécurisé).
- Utilisation de ressources matérielles importantes.
- Du matériel dédié peut être obligatoire.

III.12.Discussion

Dans ce chapitre, on a présenté la technologie récente « VPN », dont son principe est la création d'un tunnel virtuel via lequel les données transiteront sous forme cryptée, et on a décrit les protocoles les plus importants pour la création de ces tunnels. Ceci nous amène à penser que de plus en plus ces VPN entreront dans le catalogue de solutions envisagées pour une interconnexion de réseaux locaux ou alors pour la mise en place de solutions d'accès distants.

IV.1.Préambule

L'objectif de cette partie est de mettre en œuvre une solution d'interconnexion entre deux forêts avec une relation d'approbation et VPN site-à-site qui permette à des utilisateurs d'une forêt d'accéder aux ressources d'une autre forêt et un administrateur de pouvoir gérer les utilisateurs de l'autre forêt et d'assurer l'échange de données ente eux d'une façon sécurisée à travers un tunnel VPN.

IV.2.Architecture du réseau existant

Cette figure montre deux architectures réseau différentes, 2intpartners et Formationpartners, à lesquelles on apportera des améliorations et on implémentera une sécurité adéquates et garantir l'interconnexion entre ces deux forêts dans le but d'assurer le fonctionnement optimal de ses ressources réseaux et assurer à ses membres un accès sécurisé à l'information et un partage facile des données.

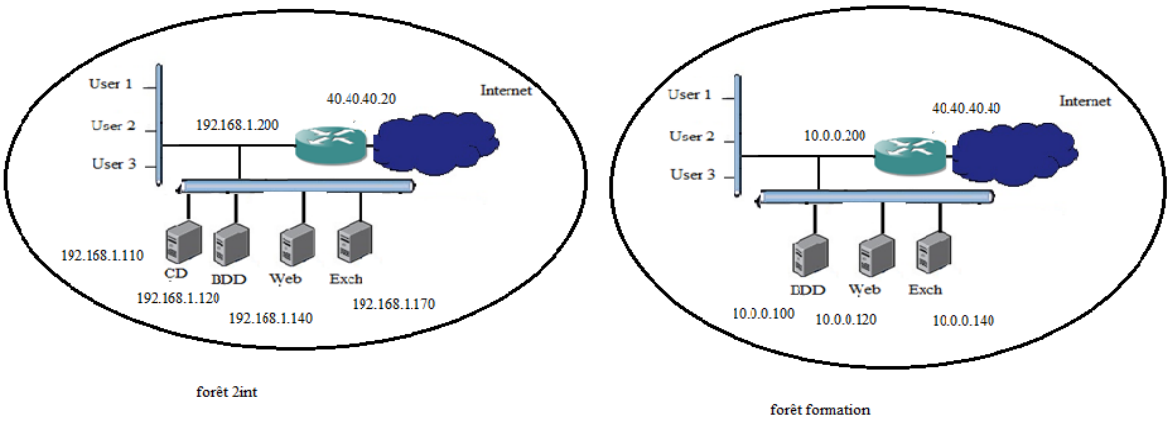


Figure IV.1 : Architecture du réseau existant

IV.3 .Les critiques du réseau existant

Une analyse du réseau d'une entreprise, nous a permis de définir un nombre de contraintes pouvant réduire ces performances voir même sa dégradation, certains de ces contraintes peuvent être un obstacle à la réalisation de la mission de cette entreprise.

- La décentralisation des administrations.
- La liaison du réseau entre les forêts est non fiable.
- Le réseau n'est pas sécuriser, il est disposé au réseau externe (internet).
- L'authentification des utilisateurs est faible.
- Le sauvegarde et le stockage des données de l'entreprise est locale.

- Absence de la redondance

IV.4.Solutions proposées

A l'issu d'une étude préalable de réseau existant nous avons opté les solutions suivantes :

- Active Directory pour la gestion et la centralisation des administrations.
- Mise en place d'un tunnel VPN site à site pour sécuriser l'échange des données entre les sites.
- Configuration d'une relation d'approbation entre forêts pour permettre à des utilisateurs d'une forêt d'accéder aux ressources d'une autre forêt.

L'architecture du réseau avec les solutions proposées est représentée par la figure suivante :

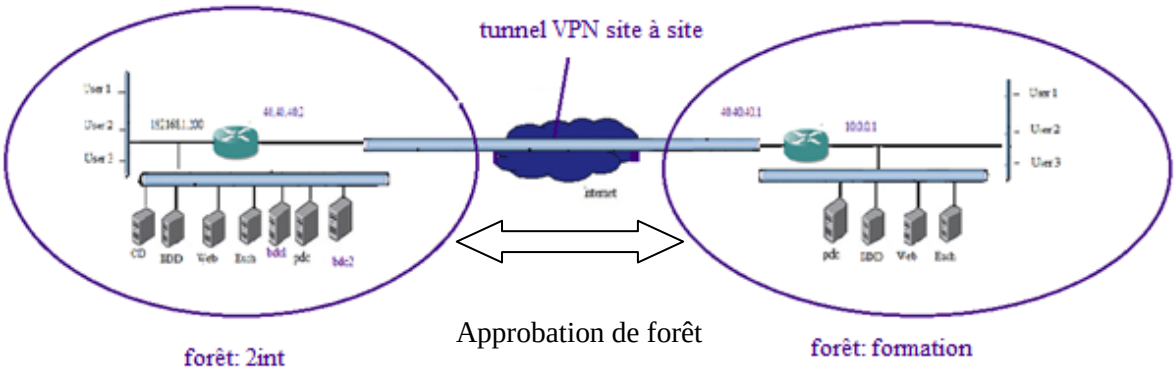


Figure IV.2 : la solution proposée

Matériels à utiliser

- Deux serveurs Active Directory (contrôleurs de domaine).
- Deux serveurs membre (domaine enfant et domaine racine d'arborescence).
- Deux routeurs Cisco 2600.
- Switch Cisco 2960.

Logiciels à utiliser

- VMware Workstation (pour la configuration des serveurs).
- GNS3 (pour la simulation graphique d'équipement réseau).
- Active Directory (installé sous Windows serveur 2008).

IV.5.La mise en place des solutions

IV.5.1.Etablissement du tunnel VPN

IV.5.1.1.La configuration des routeurs

- **Configuration des interfaces de routeur 1**

La première étape consiste à donner l'adresse IP pour chaque interface de routeur.

La configuration est la suivante :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname formation
formation(config)#interface s0/0
formation(config-if)#ip add 40.40.40.1 255.0.0.0
formation(config-if)#no shut
formation(config-if)#
*Mar  1 00:08:19.535: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
formation(config-if)#
*Mar  1 00:08:20.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
formation(config-if)#exit
formation(config)#interface f0/0
formation(config-if)#ip add
*Mar  1 00:08:43.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
formation(config-if)#ip add 10.0.0.0.1
                            ^
% Invalid input detected at '^' marker.

formation(config-if)#ip add 10.0.0.1 255.0.0.0
formation(config-if)#no shut
formation(config-if)#
*Mar  1 00:10:41.607: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:10:42.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
formation(config-if)#exit
```

- **Configuration de clock rate**

```
formation(config-if)#clock rate 64000
formation(config-if)#no shut
formation(config-if)#exit
formation(config)#exit
```

- **Configuration de protocole de routage de routeur 1**

Un routeur relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces chacune appartenant à un réseau IP différent. Lorsqu'un routeur reçoit un paquet IP sur une interface, il détermine laquelle (interface) utiliser pour transférer le paquet vers sa destination et pour cet objectif, on utilise le protocole de routage RIP et on cite les réseaux qui sont connectés directement aux deux interfaces de routeur.

La figure ci-dessous représente la configuration de RIP.

```
formation(config)#router rip
formation(config-router)#network 10.0.0.0
formation(config-router)#network 40.40.40.0
formation(config-router)#exit
formation(config)#exit
formation#
*Mar  1 00:04:37.227: %SYS-5-CONFIG_I: Configured from console by console
```

- **Configuration des interfaces de routeur 2**

La figure ci-dessous représente la configuration des interfaces de routeur 2.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname 2int
2int(config)#interface s0/0
2int(config-if)#ip add 40.40.40.2 255.0.0.0
2int(config-if)#no shut
2int(config-if)#e
*Mar  1 00:13:26.259: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
2int(config-if)#e
*Mar  1 00:13:27.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
2int(config-if)#exit
2int(config)#interface f0/0
2int(config-if)#ip add 192.168.1.220 255.255.255.0
2int(config-if)#no shut
2int(config-if)#
*Mar  1 00:14:30.679: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:14:31.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
2int(config-if)#exit
```

- **Configuration de protocole de routage (RIP) pour le routeur 2.**

```
     40.0.0.0/24 is subnetted, 1 subnets
C       40.40.40.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
2int#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2int(config)#router rip
2int(config-router)#network 40.40.40.0
2int(config-router)#network 192.168.1.0
2int(config-router)#exit
2int(config)#wr
% Incomplete command.
```

Nous allons maintenant tester les actions suivantes

- Ping de routeur formation vers l'interface (40.40.40.1) de routeur 2int.
- Ping de routeur 2int vers l'interface (40.40.40.2) de routeur formation.
- Ping de serveur 2intpartners vers le serveur formationpartners (à partir de la VMware).
- Ping de serveur formationpartners vers le serveur .2intpartners (à partir de laVMware).

Ping de routeur formation vers l'interface (40.40.40.1) de routeur 2int.

```
formation#ping 40.40.40.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.40.40.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/39/48 ms
formation#
```

Le ping de routeur 2int vers l'interface de router formation (40.40.40.2).

```
2int#ping 40.40.40.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.40.40.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/50/128 ms
2int#
```

Le ping de serveur 2intpartners vers le serveur formationpartners.

```
Microsoft Windows [version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping 10.0.0.20

Envoi d'une requête 'Ping'  10.0.0.20 avec 32 octets de données :
Réponse de 10.0.0.20 : octets=32 temps<1ms TTL=128
Réponse de 10.0.0.20 : octets=32 temps<1ms TTL=128
Réponse de 10.0.0.20 : octets=32 temps<1ms TTL=128
Réponse de 10.0.0.20 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.0.0.20:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

Le ping de serveur formationpartners vers le serveur 2intpartners

```
Administrateur : Invite de commandes
C:\Users\Administrateur>ping 192.168.1.100

Envoi d'une requête 'Ping'  192.168.1.100 avec 32 octets de données :
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.100 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

IV.5.1.2. Création d'une ACL étendue permettant l'établissement d'un tunnel VPN

Ici nous allons autoriser l'établissement d'un tunnel IPSec entre les deux routeurs :

Le routeur 1

```
formation(config)#ip access-list extended ipsecacl
formation(config-ext-nacl)#permit ahp host 40.40.40.1 host 40.40.40.2
formation(config-ext-nacl)#permit esp host 40.40.40.1 host 40.40.40.2
formation(config-ext-nacl)#permit udp host 40.40.40.1 host 40.40.40.2 eq isakmp
formation(config-ext-nacl)#exit
formation(config)#
```

Le routeur 2

```
2int(config)#ip access-list extended ipsecacl
2int(config-ext-nacl)#permit ahp host 40.40.40.2 host 40.40.40.1
2int(config-ext-nacl)#permit esp hoste 40.40.40.2 host 40.40.40.1
                               ^
% Invalid input detected at '^' marker.

2int(config-ext-nacl)#permit esp host 40.40.40.2 host 40.40.40.1
2int(config-ext-nacl)#permit udp host 40.40.40.2 host 40.40.40.1 eq isakmp
2int(config-ext-nacl)#exit
```

IV.5.1.3.Création d'une stratégie de négociation des clés et d'établissement de la liaison VPN (ISAKMP)

Paramètres ISAKMP (Internet Security Association and Key Management Protocol) est le protocole de négociation nécessaire pour que les deux hôtes se mettent d'accord sur une politique de sécurité. ISAKMP sépare la négociation entre deux phases .La première phase crée un premier tunnel, qui protégera les négociations du protocole ISAKMP.la deuxième phase crée le tunnel qui protégera les données.

Nous allons donc devoir créer une ou plusieurs politiques ISAKMP, qui regroupent les éléments suivants :

- Une méthode d'authentification (pre-share, crack, rsa-sig).
- Une méthode de cryptage (aes, aes-192, aes-256, des, 3des).
- Une méthode de hachage (md5,sha) .
- Un groupe de Diffie-Hellman (1, 2, 5,7).
- Une limite de temps pour le remplacement des clefs de cryptage (en secondes)
- Voici les commandes que nous devons exécuter pour établir une politique ISAKMP sur routeur 1.

Les commandes que nous devons exécuter pour établir une politique ISAKMP sur routeur 1

```
formation(config)# crypto isakmp policy 10
formation(config-isakmp)# authentication pre-share
formation(config-isakmp)# encryption 3des
formation(config-isakmp)# hash md5
formation(config-isakmp)# group 5
formation(config-isakmp)# lifetime 3600
formation(config-isakmp)# exit
```

Le routeur 2

```
2int(config)# crypto isakmp policy 10
2int(config-isakmp)# authentication pre-share
2int(config-isakmp)# encryption 3des
2int(config-isakmp)# hash md5
2int(config-isakmp)# group 5
2int(config-isakmp)# lifetime 3600
2int(config-isakmp)# exit
2int(config)#
```

IV.5.1.4.Création de clé pré-partagé

Nous définissons la clé pré-partagée : cisco10 ainsi que l'adresse IP du routeur distant avec lequel on communique.

Nous créons une clé pré-partagé sur chaque routeur, à l'aide de la commande suivante :

Le routeur 1

```
formation(config)# crypto isakmp key cisco10 address 40.40.40.2
```

Le routeur 2

```
2int(config)#  crypto isakmp key cisco10 address 40.40.40.1
```

IV.5.1.5. Création d'une politique IPSec (Transform set)

Lorsque nous créons un tunnel VPN, nous voudrions que des données moins sensibles soient moins bien protégées que des données très sensibles, afin d'économiser le temps du processeur et de la bande passante. C'est à cela que servent les transform set. Ils sont associés à des ACL, elles mêmes associées à des crypto map. Un transform set combine une méthode de cryptage et une méthode de hachage.

Sur chaque des routeurs, nous créons donc le transform set suivant :

Le routeur 1

```
formation(config)# crypto ipsec transform-set ipsecset esp-aes 128 esp-sha-hmac
```

Le routeur 2

```
2int(config)#  crypto ipsec transform-set ipsecset esp-aes 128 esp-sha-hmac
```

IV.5.1 .6.Création de la crypto ACL

Nous créons la crypto ACL qui est une ACL qui va identifier le trafic « intéressant » c'est à dire le trafic qui doit passer par le tunnel VPN (ici c'est le trafic depuis le LAN 2int vers le LAN formation).Voici les commandes qu'on tape sur le routeur 1 et le routeur 2.

Le routeur 1

```
formation(config)#ip access-list extended cryptoacl
formation(config-ext-nacl)#$0.0.0.1 0.255.255.255 192.168.1.220 0.0.0.255
formation(config-ext-nacl)#
```

Le routeur 2

```
2int(config)#ip access-list extended cryptoacl
2int(config-ext-nacl)#$92.168.1.220 0.0.0.255 10.0.0.1 0.255.255.255
2int(config-ext-nacl)#exit
```

IV.5.1.7.Création de la crypto map

Nous créons la crypto map qui définit le chemin qu'emprunte notre tunnel avec : la politique IPSec, la crypto ACL, le transform-set pour la politique IPSec et l'adresse IP du routeur distant avec lequel on veut communiquer.

Voici les commandes à entrer sur le routeur 1

```
formation(config)#crypto map ipsecmap 100 ipsec-iakmp
formation(config-crypto-map)#set peer  40.40.40.2
formation(config-crypto-map)#set transform-set 50
formation(config-crypto-map)#set security-association lifetime seconds 900
formation(config-crypto-map)#exit
formation(config)#
```

Sur le routeur 2

```
2int(config)#crypto map ipsecmap 100 ipsec-iakmp
2int(config-crypto-map)#set peer 40.40.40.1
2int(config-crypto-map)#set transform-set 50
2int(config-crypto-map)#set security-association lifetime seconds 900
2int(config-crypto-map)#exit
2int(config)#
```

IV.5.2. Configuration d'une relation d'approbation entre forêts

IV.5.2.1.Installation des serveurs Active Directory

Cet Active directory nous a permet de représenter et de stocker les éléments constitutifs du réseau et d'assurer une gestion centralisée dans toute l'entreprise tel que la planification des tâches.

L'installation de serveur Active Directory est subordonnée à la réalisation préalable de certaines opérations:

- Configuration d'une adresse IP statique
- Attribution de son véritable nom au serveur

➢ **Installation de domaine racine de la forêt**

Dans notre projets on va étudier deux forêts distinctes : la première forêt est « 2intpartners.com » et la deuxième est « formations partners.com » donc les étapes d'installation de domaine racine de la forêt sont les mêmes sauf quelques modifications comme :

Le nom de serveur Active Directory et le nom Net BIOS.

- **Les étapes d'installations de serveur Active Directory**

dcpromo :permet d'installer le serveur de domaine Active Directory

Dans le menu démarrer >Exécuter « dcpromo » nous lonçons l'installation d'Active Directory.

L'Assistant Installation d' Active Directory installe et configure les composants qui fournissent le service d'annuaire Active Directory aux utilisateurs et ordinateurs du réseau.On aura la figure suivante et on coche sur suivant pour continuer L'Assistant Installation d' Active Directory installe et configure les composants qui fournissent le service d'annuaire Active Directory aux utilisateurs et ordinateurs du réseau.On aura la figure suivante et on coche sur suivant pour continuer

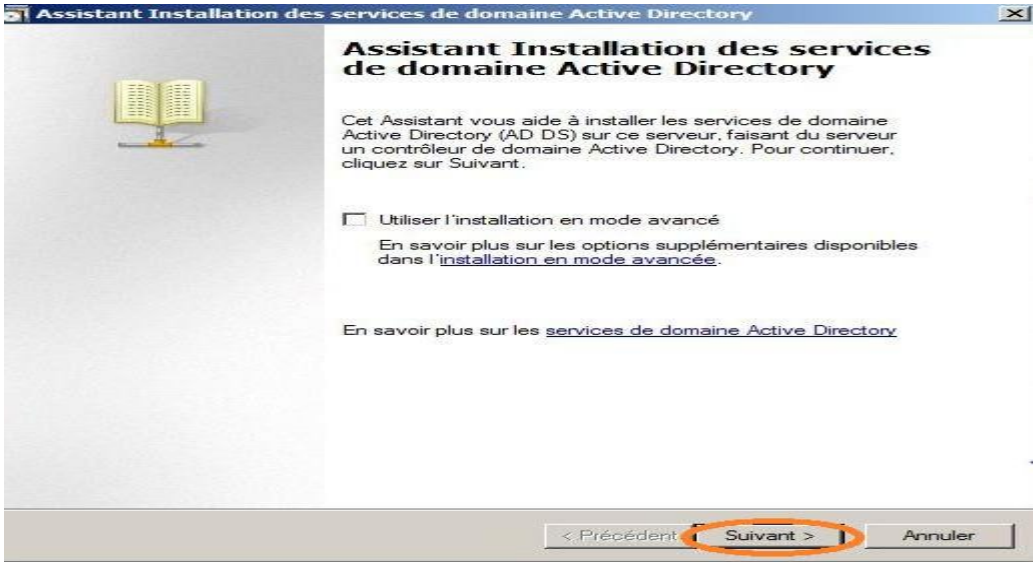


Figure IV.3: Installation des services de domaine AD.

Nous allons maintenant commencer la création d'Active Directory. On a le choix entre rejoindre une forêt existante ou créer un nouveau domaine dans une nouvelle forêt. Nous allons créer un nouveau domaine.

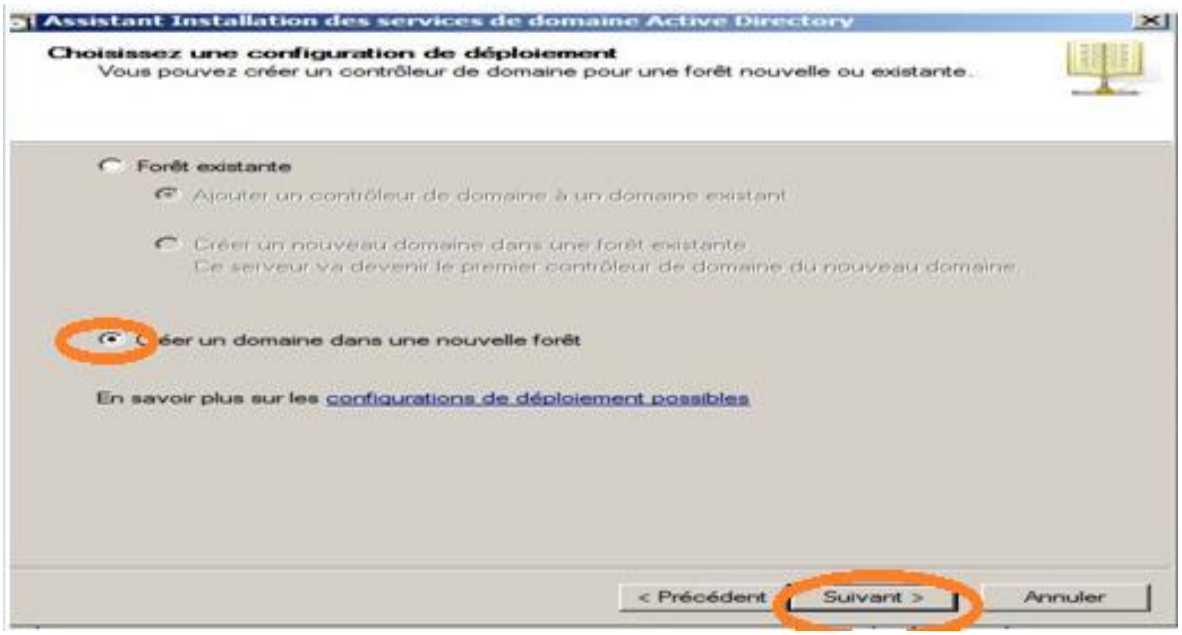


Figure IV.4: Création d'un nouveau domaine dans une nouvelle forêt

Lors de l'installation serveur de domaine Active Directory on va nommer le domaine comme suit

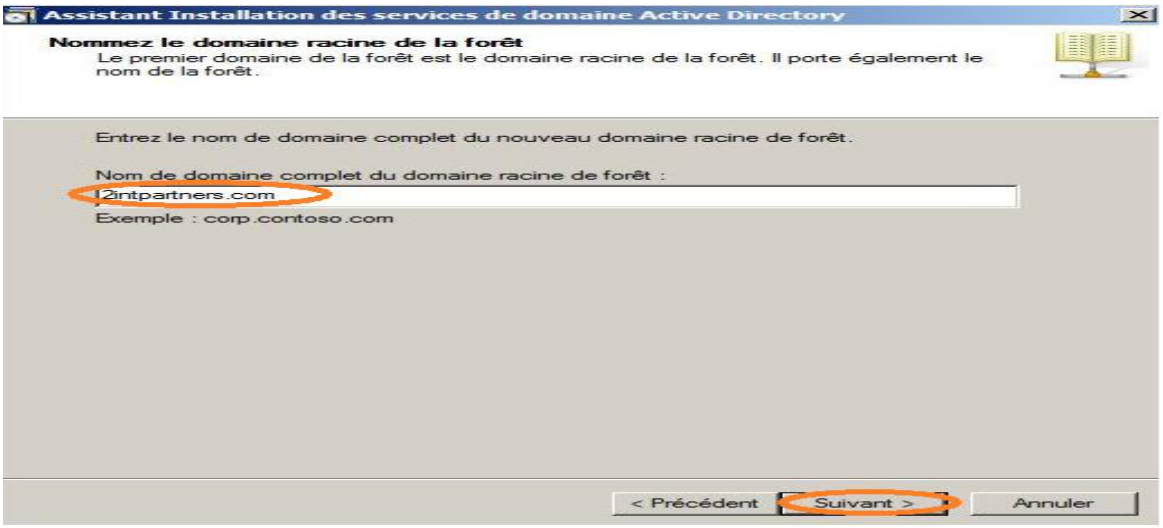


Figure IV.5 : Nom du domaine racine de la forêt

Dans la fenêtre « niveau fonctionnel », on choisit le mode Windows server 2008.

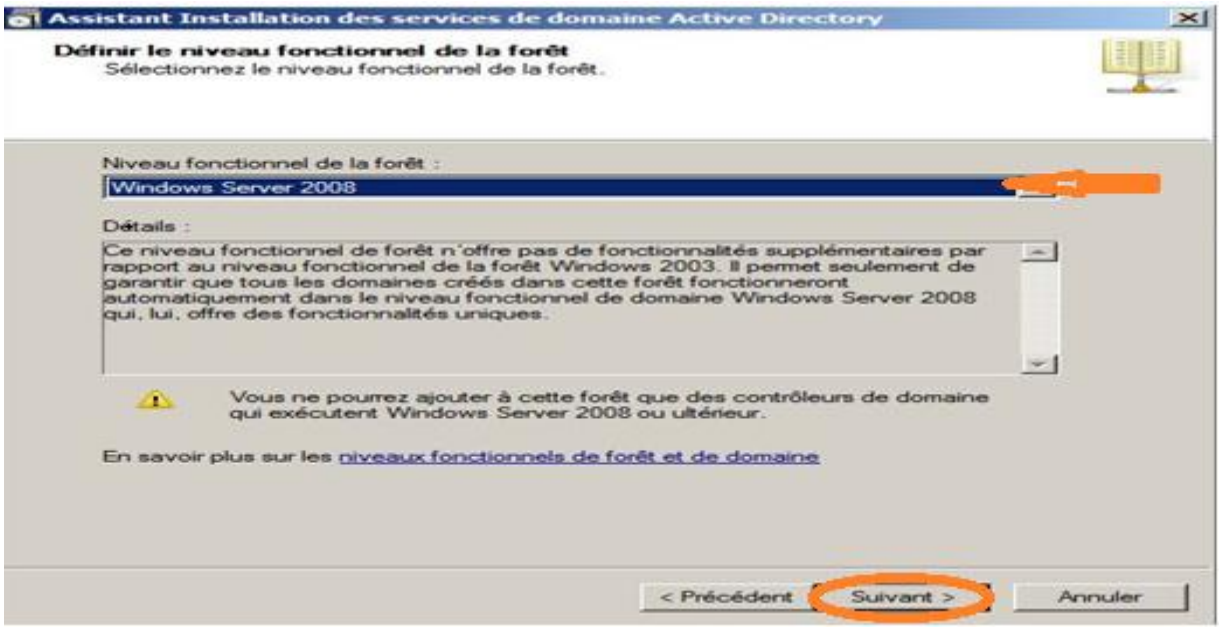


Figure IV.6 : Choix des nouvelles fonctionnalités.

On coche sur l'icône « Serveur DNS » pour continuer. DNS sera installé en même temps que l'AD

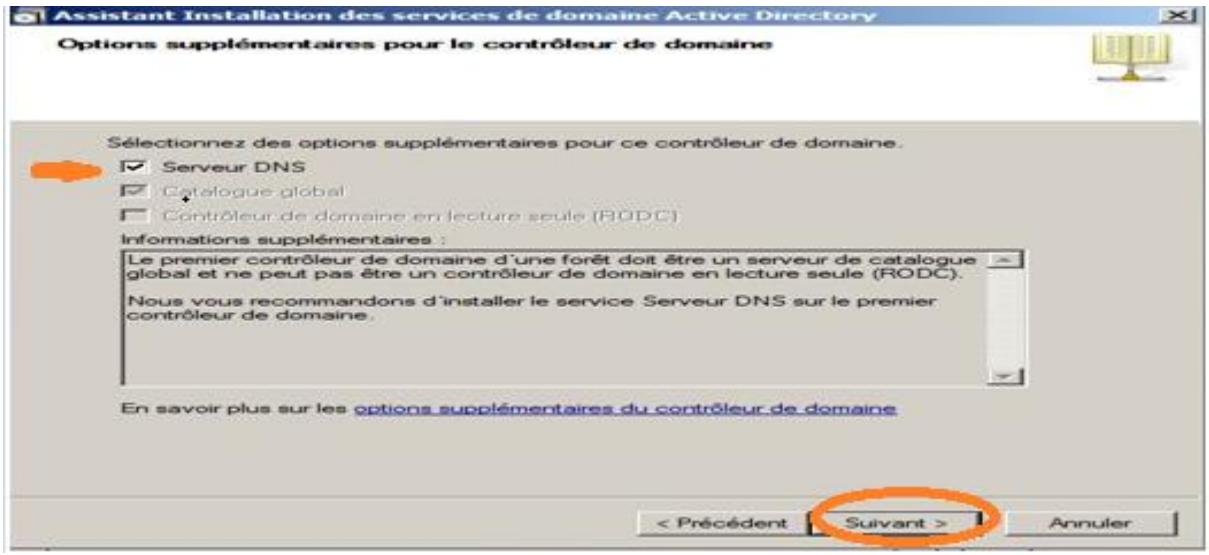


Figure IV.7 : Configuration de serveur DNS

Pour indiquer les chemins des dossiers où seront stockés les fichiers journaux et les BDD, pour une installation simple on laisse les paramètres par défaut.

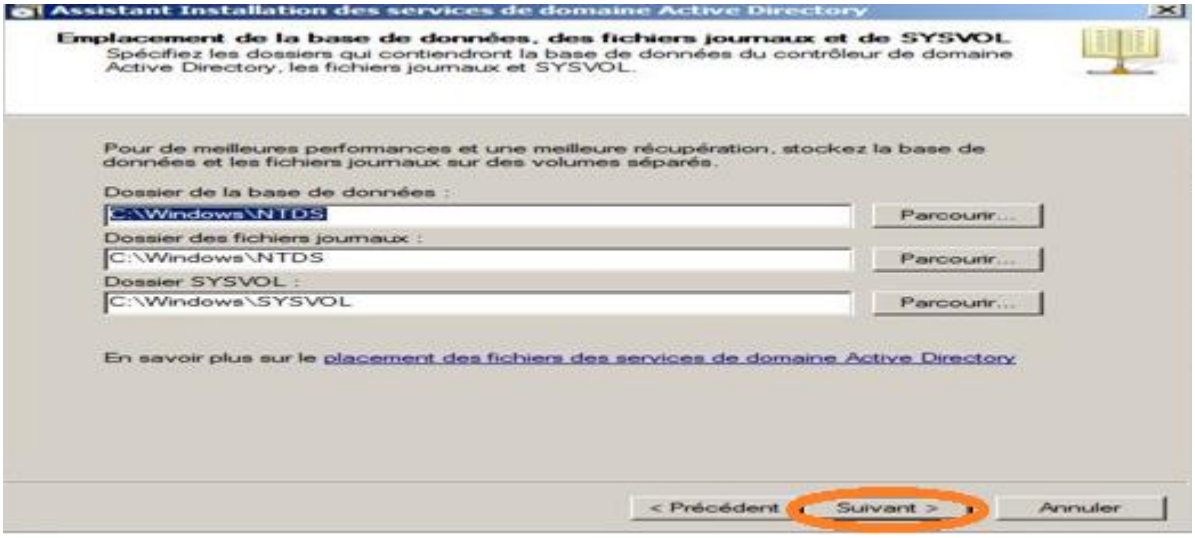


Figure IV.8: l'emplacement de la base de donnée, du journal des transactions et de partage SYSVOL

Maintenant l'assistant va vous demander de configurer un mot de passe, qui servira en cas de restauration.

On choisit le mot de passe « Pas$w0rd »

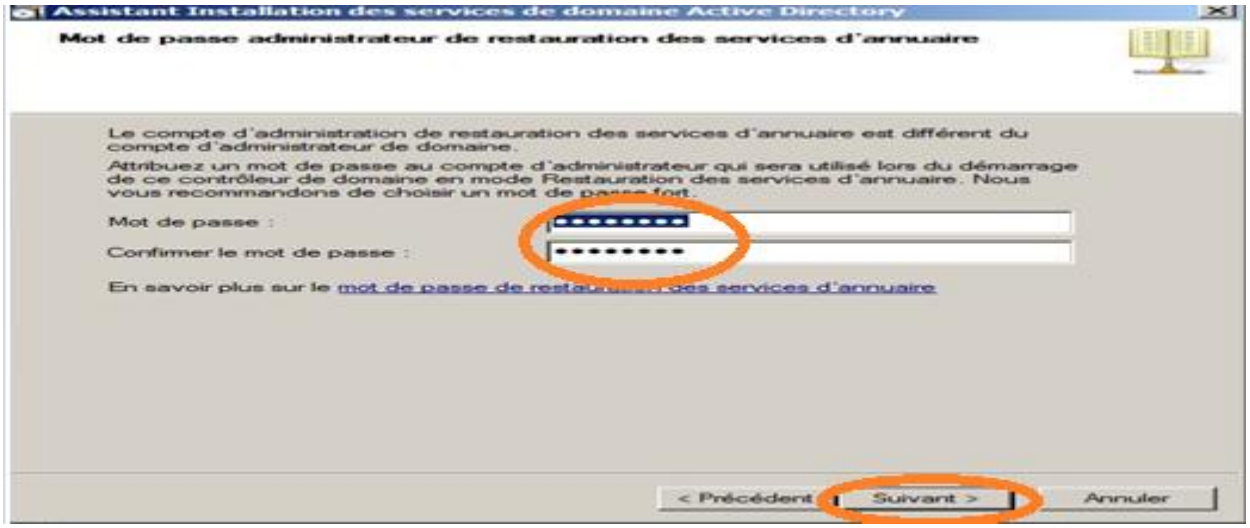


Figure IV.9 : Sécurisation des services annuaires.

Pour vérifier les paramètres on clique sur suivant

On coche la case "Redémarrer à la fin de l'opération" pour terminer l'installation.

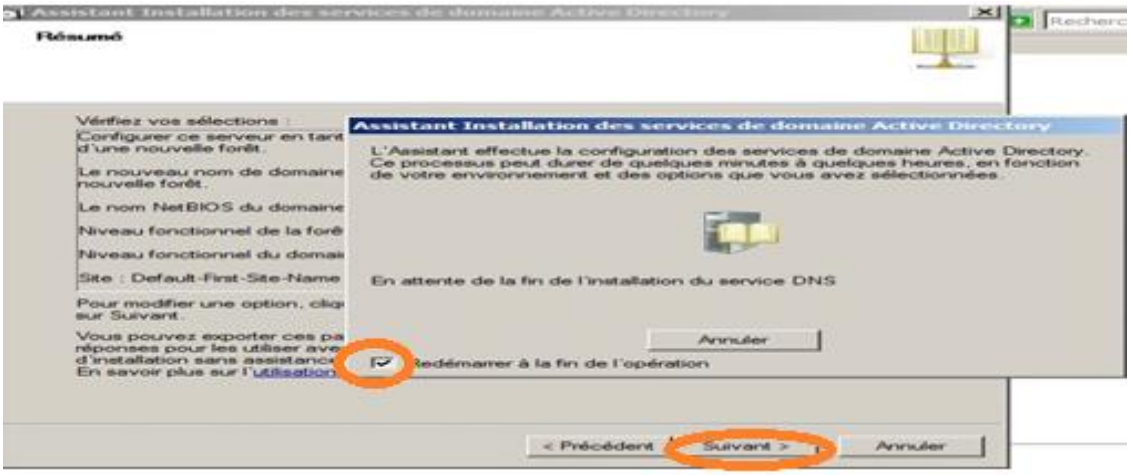


Figure IV.10 : vérification de l'installation

- **Installation de domaine enfant**

La mise en place d'un nouveau domaine enfant, le début de l'installation est le même que pour l'installation d'une nouvelle forêt.

Sur la fenêtre de l'assistant de l'installation on coche sur la case utiliser l'installation de mode avancé pour accéder à des options supplémentaires puis on clique sur Suivant.

Figure IV.11 : Installation des services Active Directory

Pour créer un domaine enfant, nous allons choisir Forêt existante puis Créer un nouveau domaine dans une nouvelle forêt existante puis nous cliquons sur suivant.

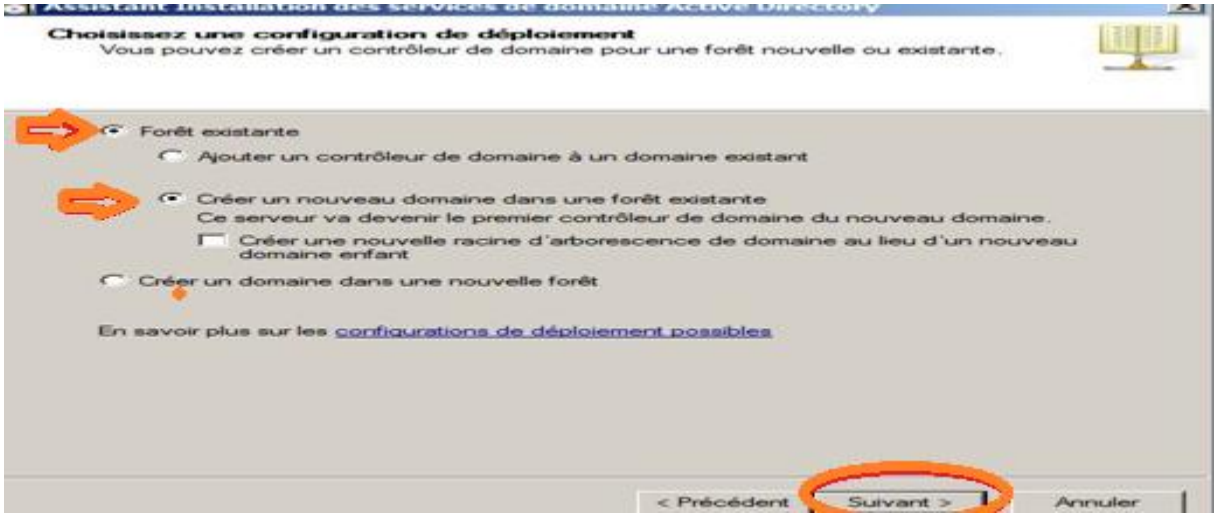


Figure IV.12 : Création d'un nouveau domaine dans une forêt existante

Nous arrivons maintenant sur la fenêtre Information d'identification réseau .On tape le nom de domaine de la forêt ou on va installer ce nouveau domaine puis on clique sur définir pour spécifier les information d'identification de compte à utiliser pour effectuer l'installation.

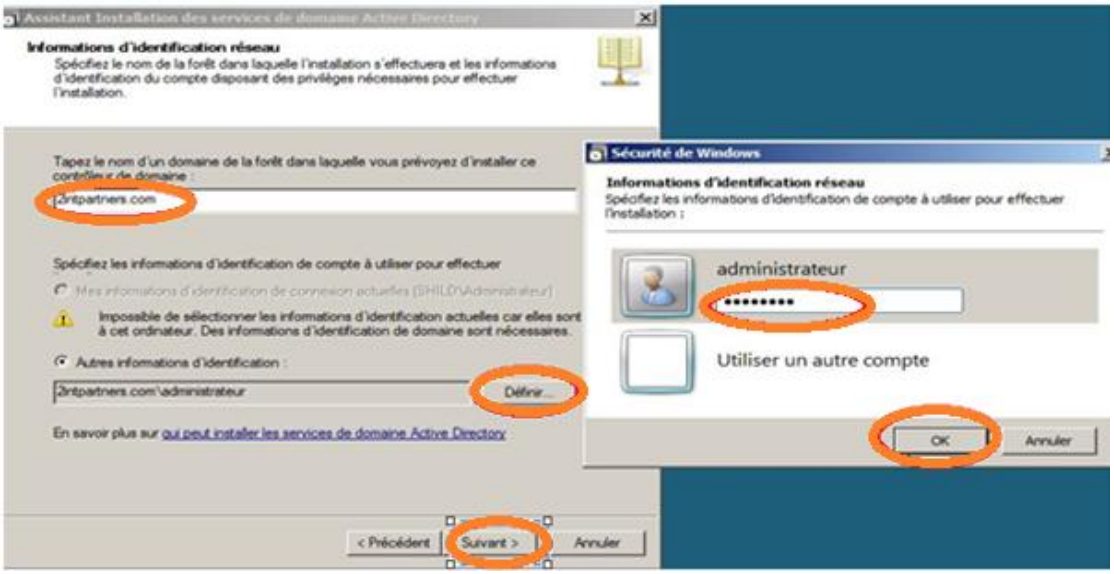


Figure IV.13 : les informations d'identification réseau.

Sur la fenêtre Nommer le nouveau domaine on donne le nom de domaine complet du domaine parent et le nom DNS en une partie du domaine enfant.

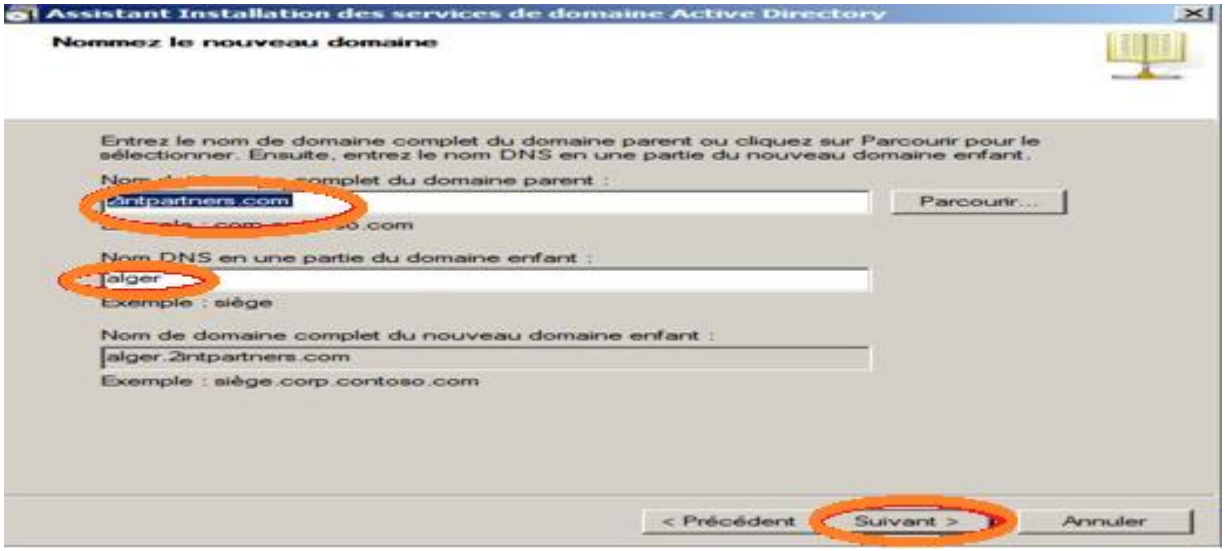


Figure IV.14 : Nommage de nom du domaine enfant.

Après avoir donné le Nom de domaine NetBIOS et le niveau fonctionnel de domaine on va sélectionner un cite sur le quel on va installer le contrôleur de domaine.

Dans la fenêtre suivante le serveur DNS est coché par défaut et l'option Catalogue Global est désactivée par défaut. On va cocher cette case pour que le contrôleur de domaine hébergera les rôles de maître d'opération et d'infrastructure au sein du domaine puis on clique sur Suivant.

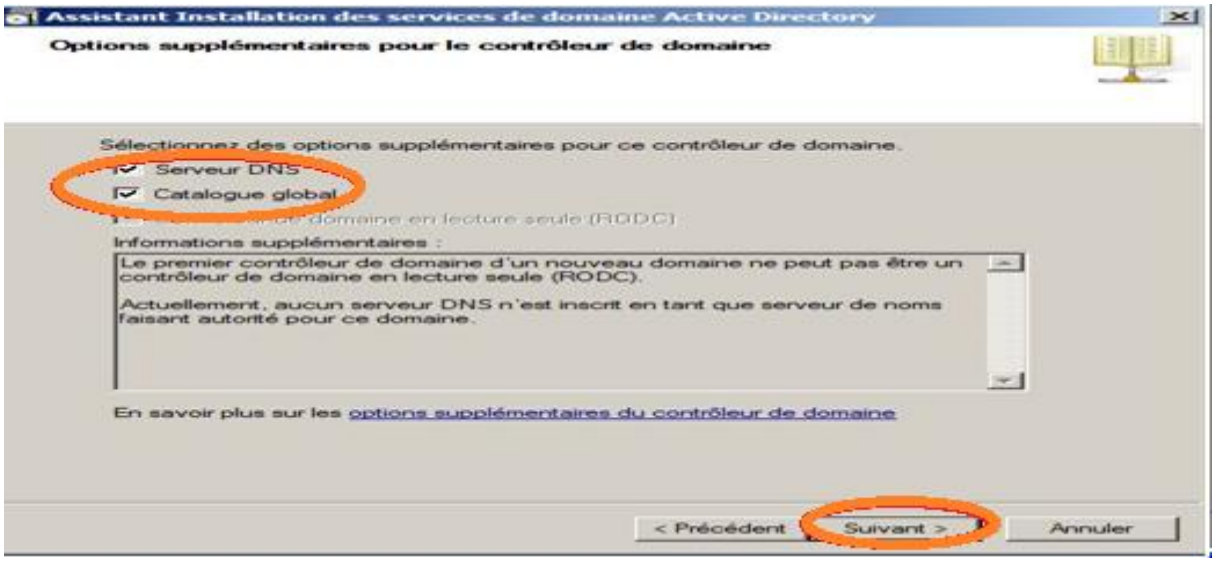


Figure IV.15 : Installation de Serveur DNS et le Catalogue Global

Après avoir choisir un mot de passe qui nous servira à démarrer les services ADDS en mode de restauration des services d'annuaire, on clique sur Suivant pour obtenir la fenêtre de fin d'installation.

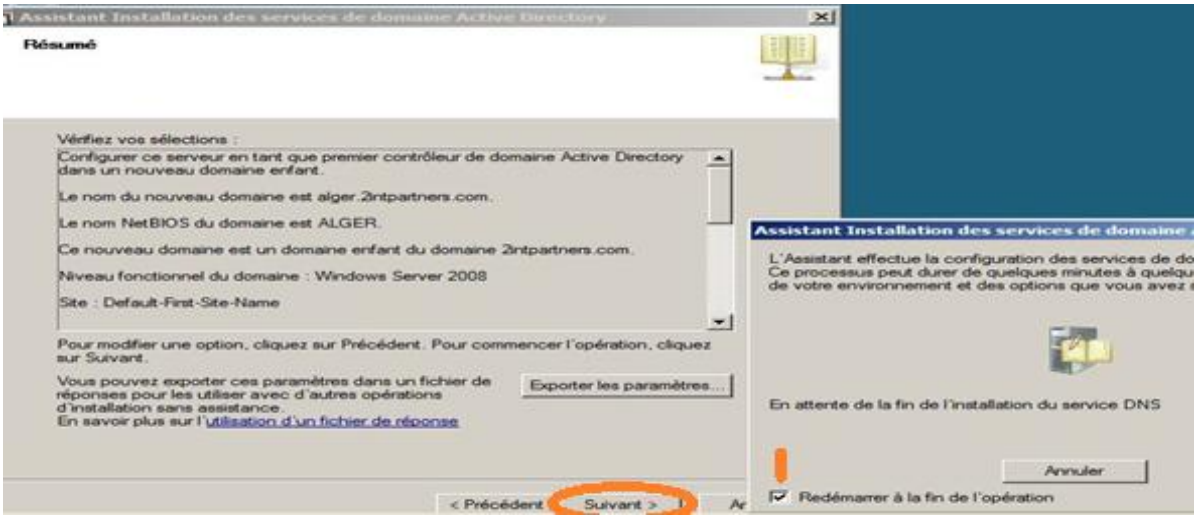
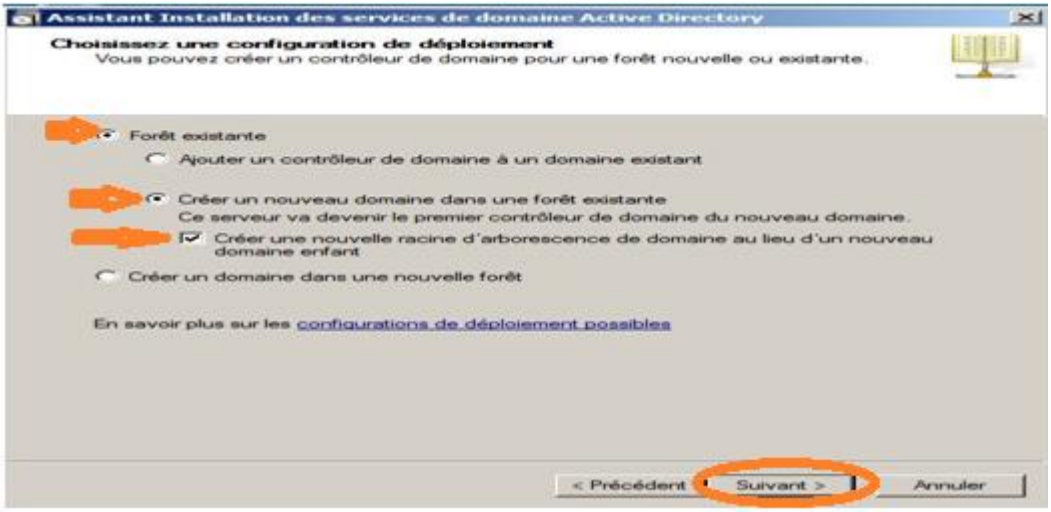


Figure IV.16 : vérification d'installation des services Active Directory

- **Installation de domaine racine d'arborescence**

Pour configurer le domaine racine d'arborescence on choisit le mode avancé.

On coche sur « Créer une nouvelle racine d'arborescence de domaine au lieu d'un nouveau domaine enfant » puis sur Suivant pour continuer.



Après avoir taper le nom de domaine de la forêt dans laquelle on vas installer ce domaine.

On vas nommer la nouvelle racine d'arborescence de domaine comme suit :

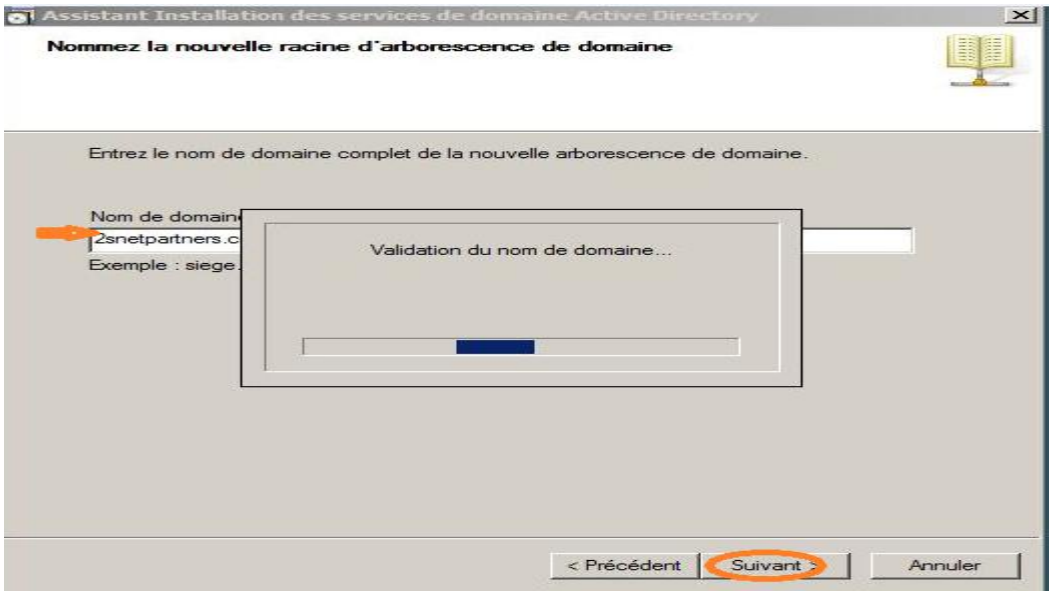


Figure IV.18 : Nom de la nouvelle racine d'arborescence

Dans la fenêtre « Sélectionnez un site » on va séléctionner un site sur le quel on installe le contrôleur de domaine.

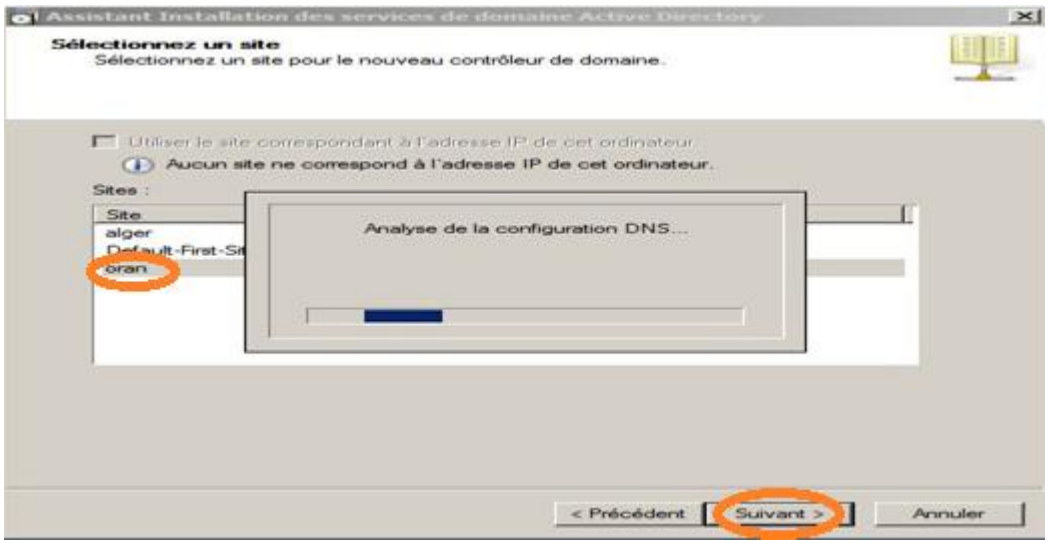


Figure IV.19 : choix du site

Les étapes qu'ils suivent sont les mêmes que les domaines précédents.

IV.5.2.2.Les étapes de configuration de la relation d'approbation entre forêts

Dans cette exemple nous allons utiliser une forêt 2intpartners.com et une forêt formationpartners.com.

Afin de mettre en place une relation d'approbation entre ces deux forêts notre infrastructure DNS devra être capable de répondre aux différentes interrogations des deux

forêts. Il nous faudra donc configurer les redirecteurs au niveau des serveurs DNS de nos forêts.

Une fois l'architecture DNS opérationnelle on peut débuter la création d'une relation d'approbation bidirectionnelle de forêt.

Sur le contrôleur de domaine de la forêt 2intpartners.com on utilise la console Domaines et approbations Active Directory**.**

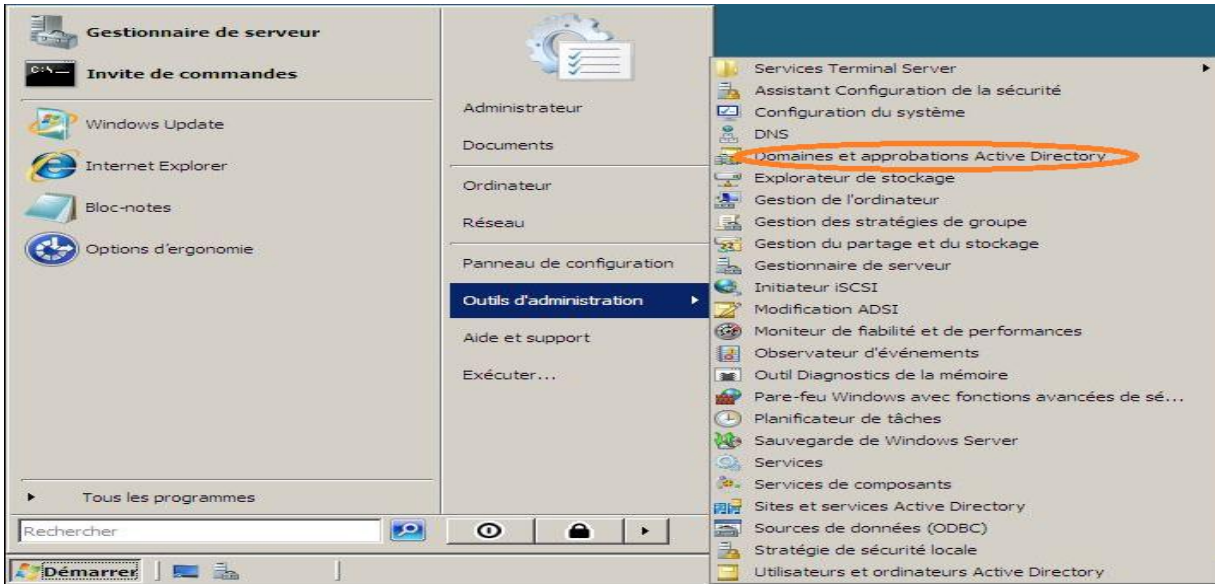


Figure IV.20 : Installation de relation d'approbation de forêt

On clique sur le nom de domaine 2intpartners.com puis sur propriétés. Dans l'onglet approbation on sélectionne sur Nouvelle approbation.

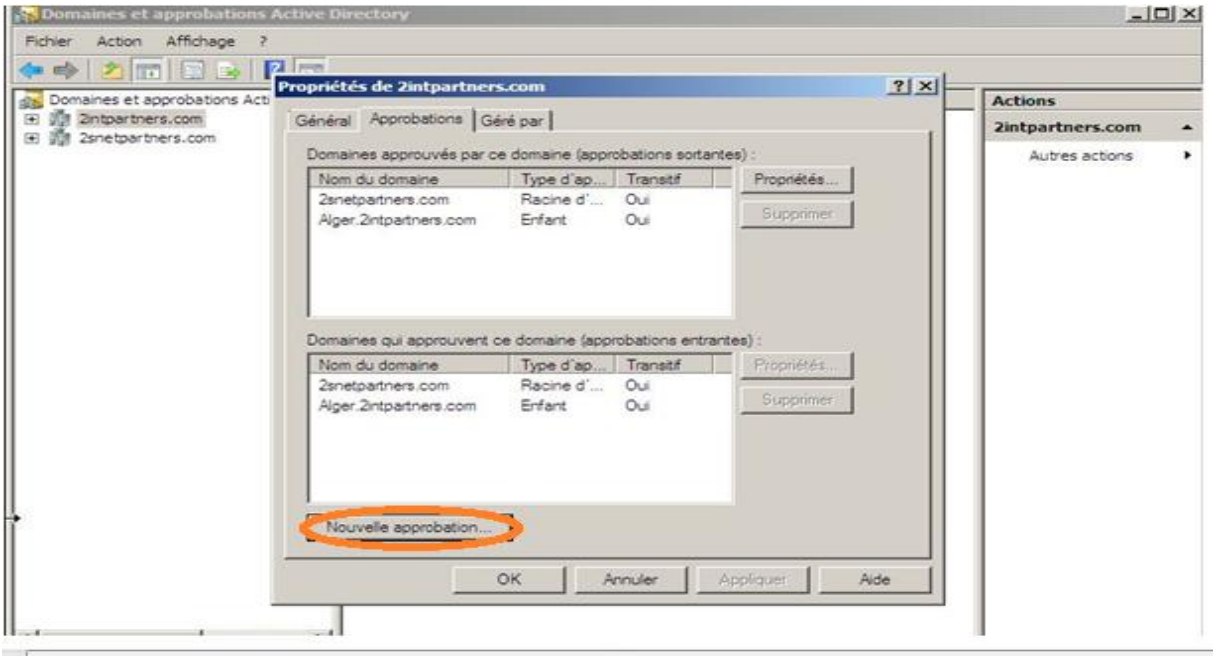


Figure IV.21: Création d'une nouvelle approbation

On entre le nom de la forêt qui sera la destination de l'approbation, dans notre cas formationpartners.com

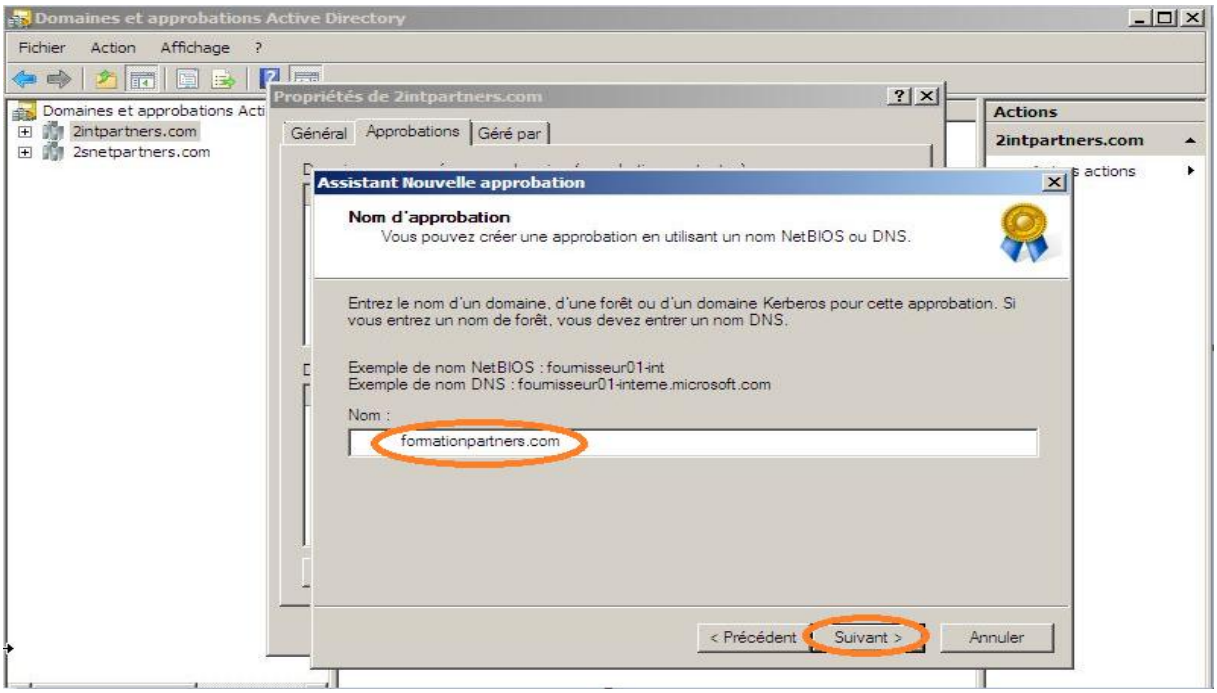


Figure IV.22: Choix du nom de forêt approuvé

Dans notre cas on va créer une relation d'approbation entre forêt donc on coche sur Approbation de forêt puis sur Suivant.

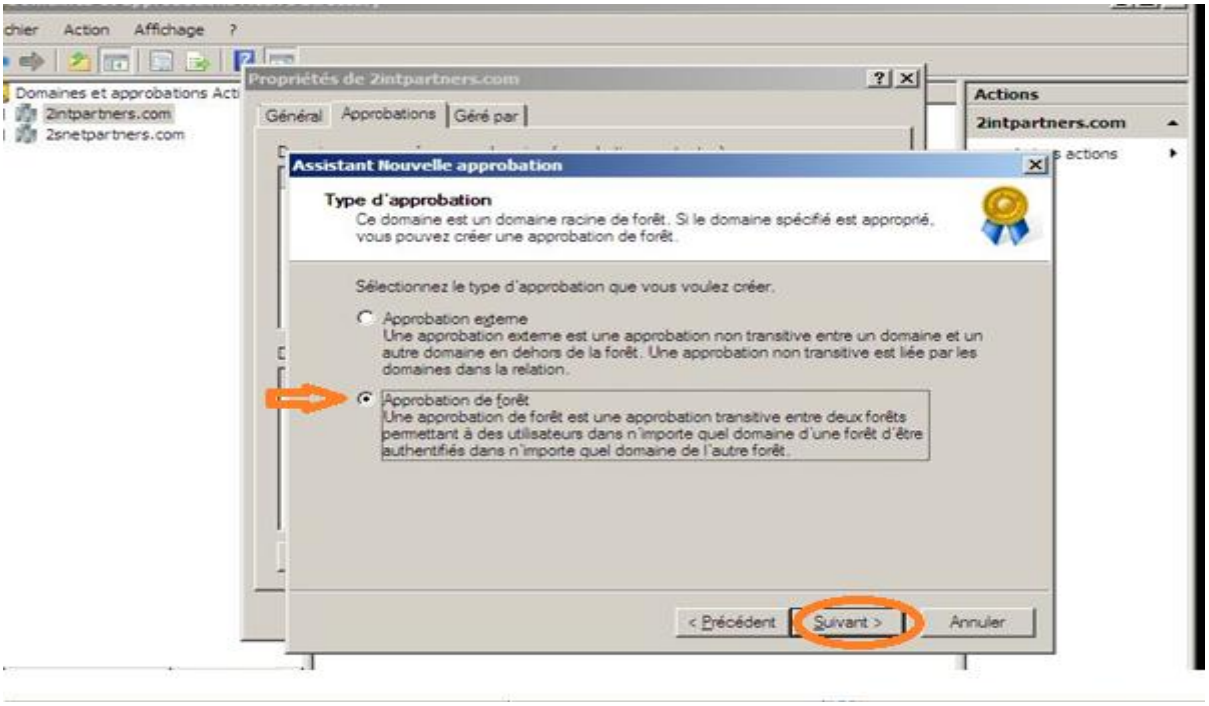


Figure IV.23 : Type d'approbation.

On veut créer une approbation de forêt bidirectionnelle, donc on clique sur Bidirectionnel cela permette à des utilisateurs dans ce domaine et les utilisateurs dans le domaine spécifié d'accéder aux ressources situées dans l'un ou l'autre domaine. Puis on clique sur Suivant pour continuer.

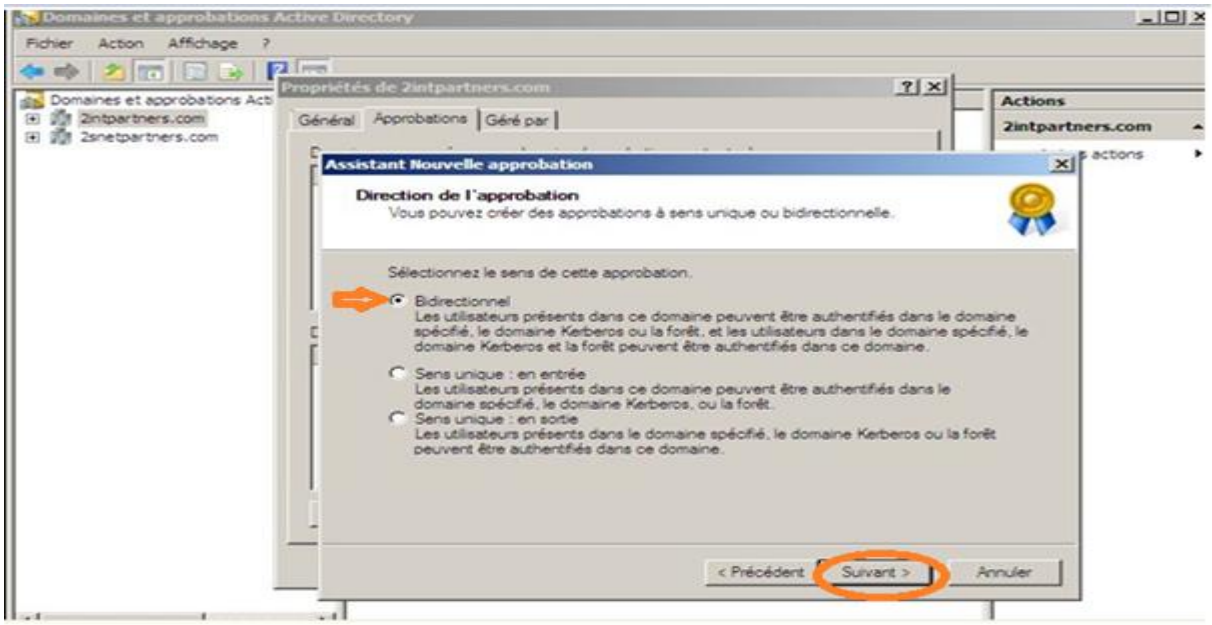


Figure IV.24: Direction de l'approbation.

Dans ce cas on sélectionne sur « Ce domaine et le domaine spécifié » cela signifie que l'approbation sera créer dans les deux forêts.

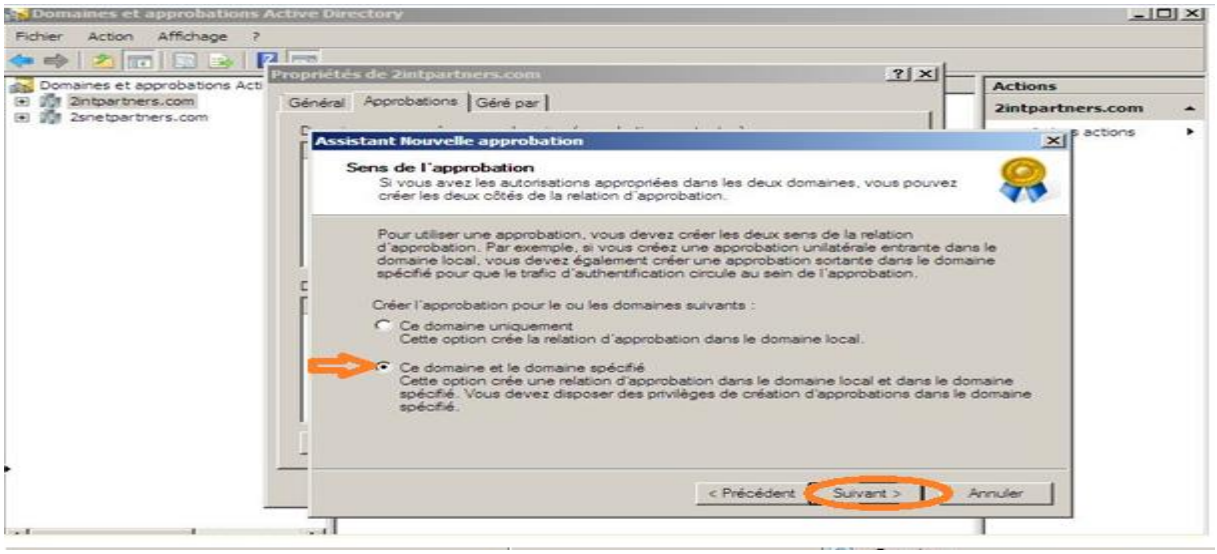


Figure IV.25: Sens de l'approbation.

Dans cette figure on donne le nom d'utilisateur et le mot de passe qui ont les droits administratifs sur la forêt formationpartners (le nom : administrateur, le mot de passe :Pas$w0rd)

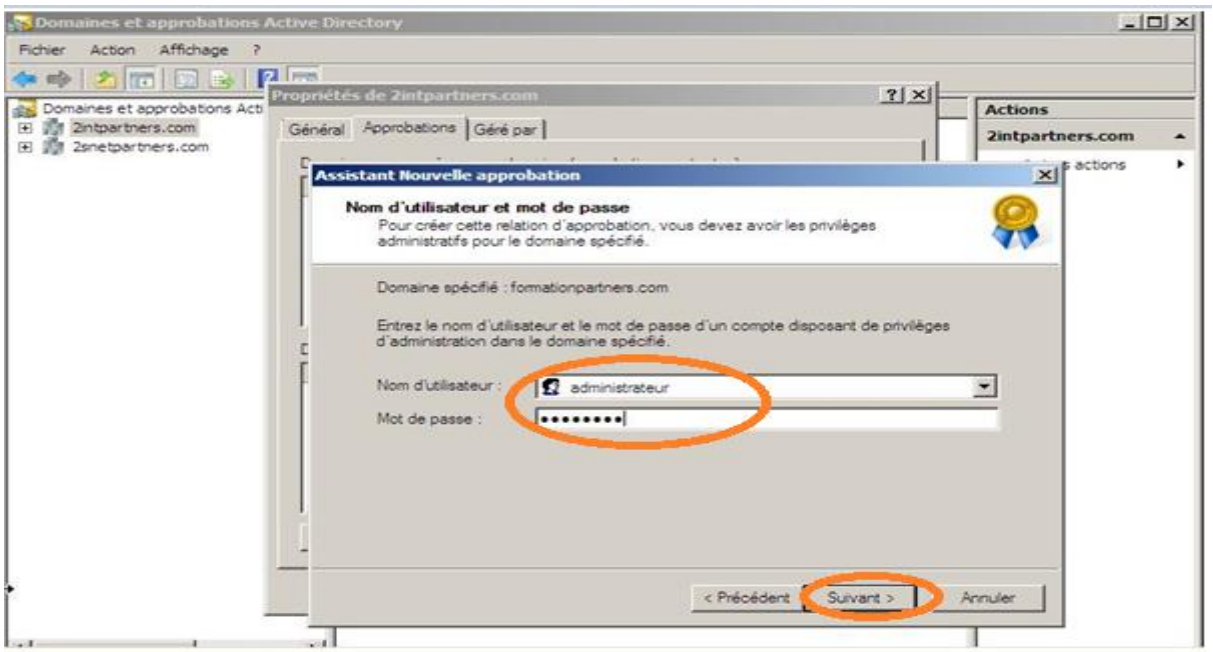


Figure IV.26: Les privilèges administratifs pour le domaine formationpartners.

On choisit « Authentification pour toute les ressources de la forêt » parceque les deux forêts appartiennent à la même organisation.

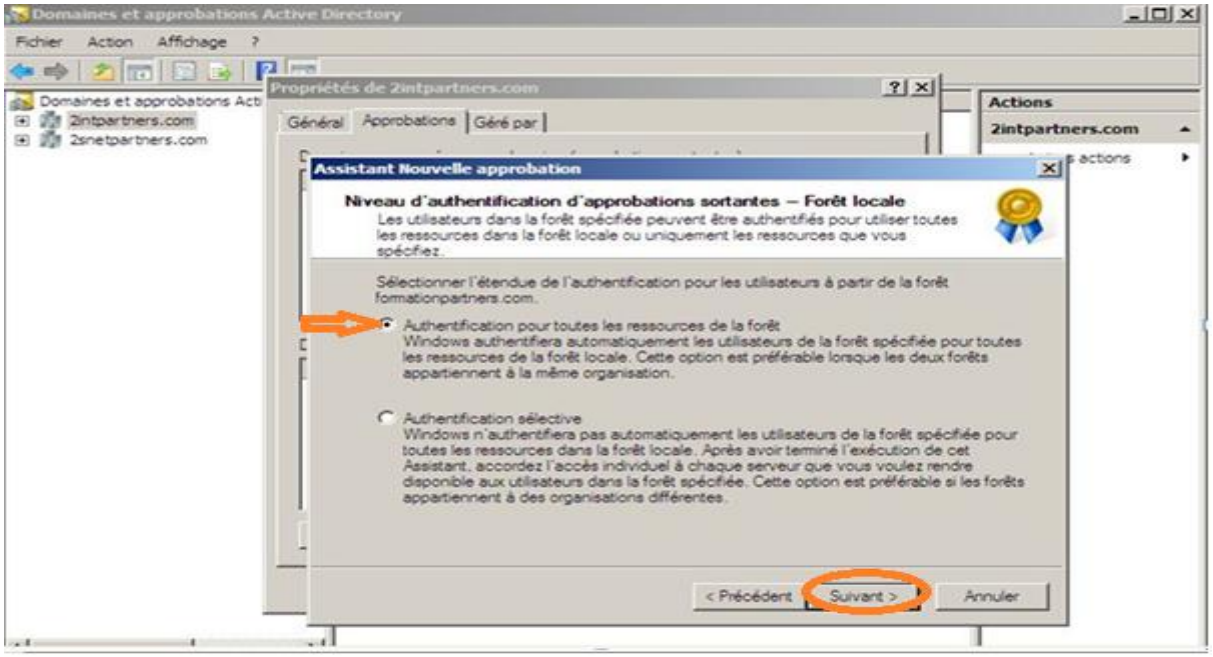


Figure IV.27 : Niveau d'authentification d'approbation.

Cette figure montre les résultats de la configuration de la relation d'approbation.

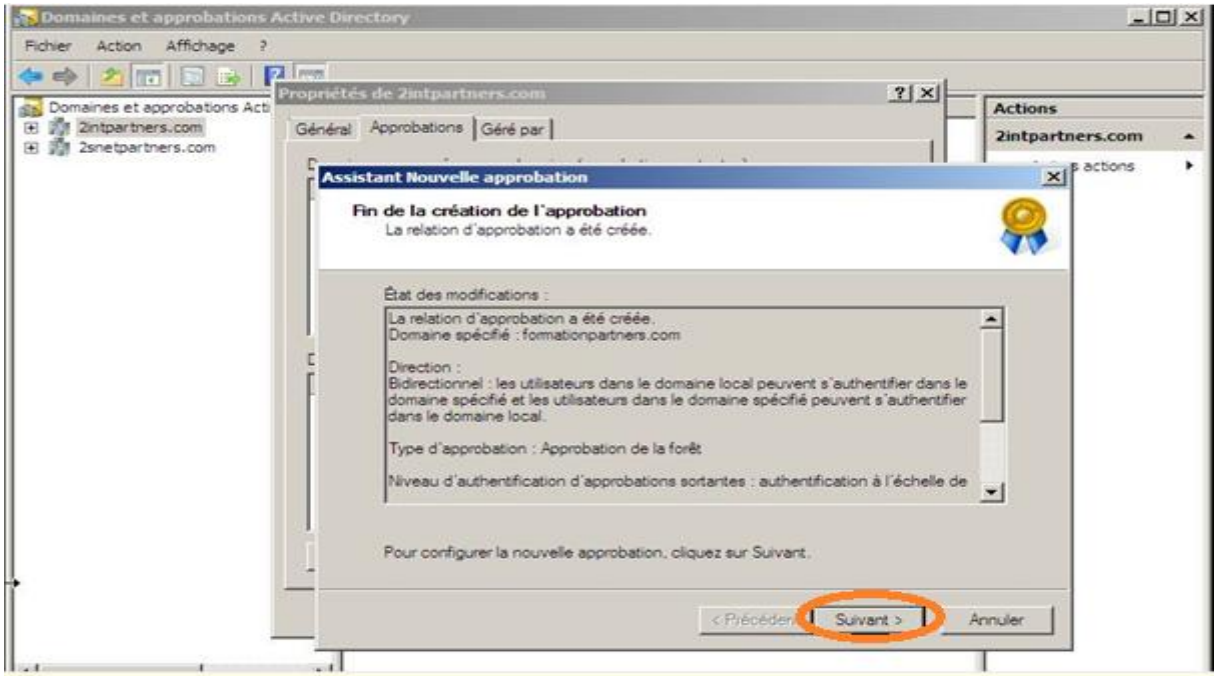


Figure IV.28: Fin de la création de l'approbation.

Cette figure montre que la relation d'approbation a été crée dans le domaine formationpartners.

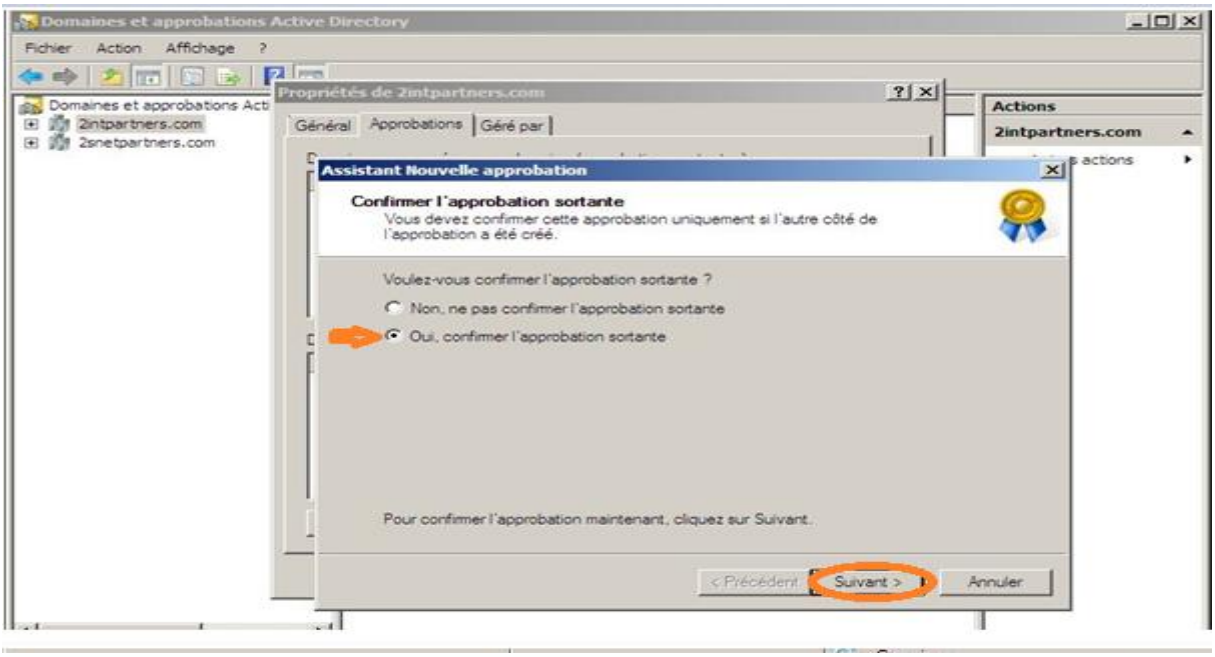


Figure IV.29 : Confirmation de l'approbation sortante.

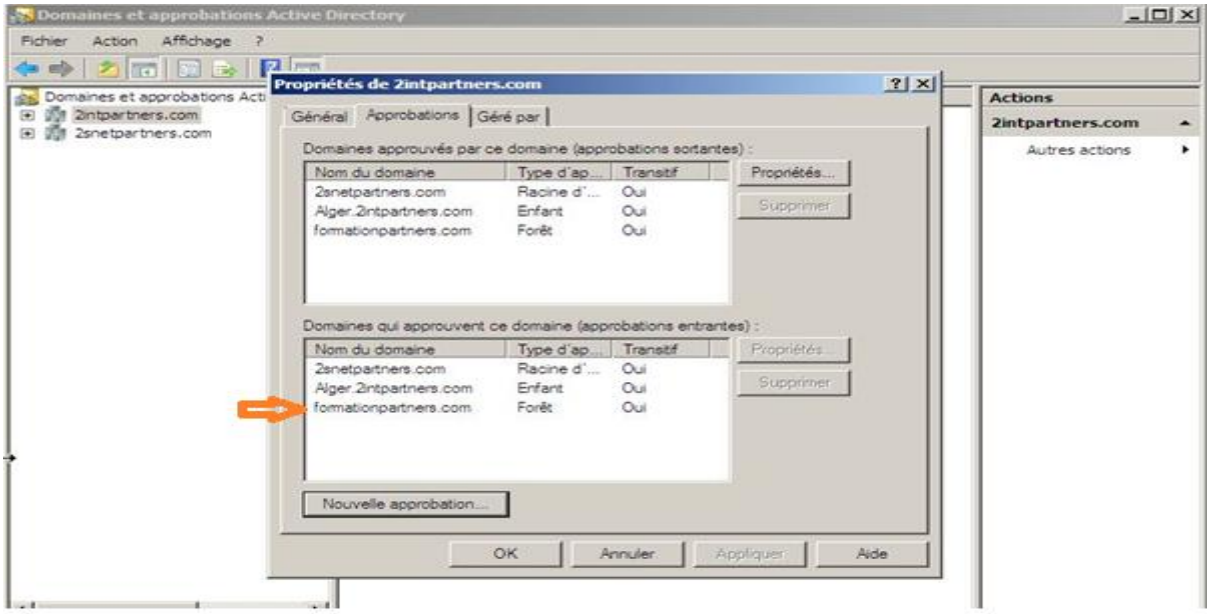


Figure IV.30 : Vérification de la création de relation d'approbation dans 2intpartners.

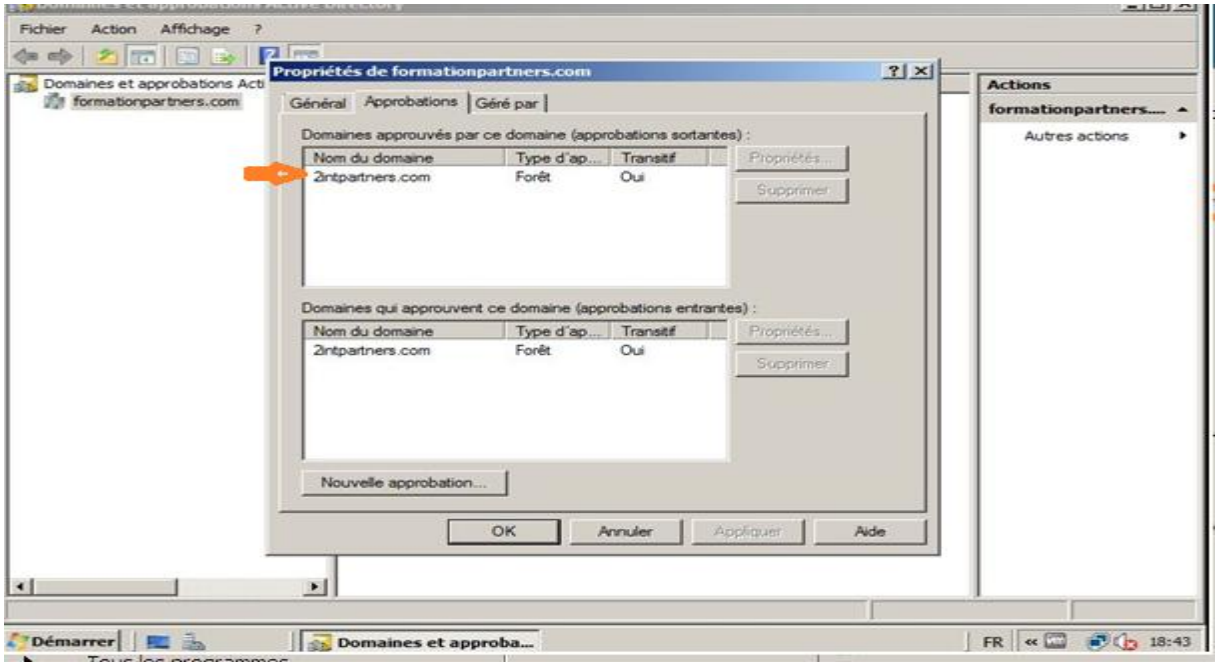


Figure IV.31: Vérification de la création de relation d'approbation dans formationpartners.

IV.6.Discussion

Notre objectif était d'interconnecter les deux forêts, par la création d'un tunnel sécurisé et de permettre à des utilisateurs d'une forêt d'accéder aux ressources de l'autre forêt par la création d'une relation d'approbation. Nous avons atteint cet objectif car nous constatons bien selon les captures ci-haut, que les sites sont bien interconnecter et les utilisateurs de la forêt 2intpartners peuvent accéder aux ressources de la forêt formationpartners et vice versa.

CONCLUSION

Dans notre mémoire, nous nous sommes intéressés à mettre en place une application permettant l'accès aux ressources de différents sites d'entreprise et de garantir un échange d'information sécurisé entre eux afin d'améliorer le rondement, la qualité de service et le temps de réponse et de satisfaire la clientèle de l'entreprise. Cette application est basée sur la configuration d'une relation d'approbation entre deux forêts distinctes et la configuration d'un tunnel VPN site à site.

Pour réaliser notre projet nous l'avons décomposé en deux parties :

Établissement d'un tunnel VPN site à site qui nécessite la configuration des routeurs Cisco, définir une politique ISAKMP, un transform set, un tunnel group, une ACL définissant le trafic à protéger et un crypto map.

Création d'une relation d'approbation entre forêts qui nécessite d'installer un serveur Active Directory sous Windows Server 2008 (un domaine racine) dans chaque forêt.

Les solutions qu'on a proposé permettre aux utilisateurs authentifiées dans une forêt d'accéder aux ressources d'une autre forêt de façon sécurisée, la maîtrise et la gestion d'accès à la base de données et d'assurer un niveau de sécurité considérable.

Nous estimons que les relations d'approbations sont des outils très puissants et faciles qui améliorent une administration réseau. Que ce soit dans le cas d'une interconnexion ou d'une création de réseaux d'entreprises, il est nécessaire de mettre en place, de façon implicite ou explicite des relations d'approbations et configurer celle-ci afin d'optimiser au mieux les capacités de réseau.

Et comme perspective à ce travail, nous proposons, le développement de l'aspect sécurité et confidentialité du système.

Ce projet nous a permis d'acquérir et d'enrichir nos connaissances et nos compétences dans de nombreux domaines, il nous a initiés au monde de la recherche sur les réseaux surtout en ce qui concerne leurs sécurisations. Il nous a également permis de découvrir les logiciels de simulation : VMware Workstation, GNS3, Windows Server 2008, service d'annuaire Active Directory.

1. La communication sur un réseau

Le fondement d'un bon réseau, c'est que le système d'exploitation soit capable :

- De gérer la transmission de données
- De fournir aux applications des interfaces standard pour leur permettre d'exploiter les ressources du réseau

C'est le cas de tous les systèmes d'exploitation à jour

A priori, rien ne devrait obliger les plates formes client et serveur à fonctionner avec le même système d'exploitation. C'était le cas pour les solutions propriétaires, c'est impensable aujourd'hui. Même si un réseau Microsoft dispose d'outils qui lui sont spécifiques, les hôtes de ce réseau peuvent tout de même dialoguer avec ceux d'un réseau Unix.

Pour arriver à cette interopérabilité, il faut que les divers protagonistes se mettent d'accord sur les fonctionnalités à implanter dans leurs applications et leurs fonctions réseau. C'est le rôle des RFC (Request For Comment) et des normes que de définir ces critères.

2. Modèle de référence OSI :

Le modèle de référence OSI se fonde sur une proposition élaborée par l'organisation internationale de normalisation(OSI) ; il est appelé modèle de référence OSI (open system interconnexion) parce qu'il traite de la connexion entre les systèmes ouverts en communication avec d'autre systèmes.

Ce modèle fonctionne de façon que, Chaque couche (n) offre un certain nombre de services à la couche (n+1) en déroulant un protocole uniquement défini à partir des services fournis par la couche (n-1). Le concept de l'OSI nécessite la compréhension de 3 concepts :

- **Le service** : Ensemble d'événements et primitives pour se rendre du niveau (n) au niveau (n-1).
- **Le protocole** : Ensemble de règles nécessaires pour réaliser un service.
- **Le point d'accès à un service** : Point situé à la frontière entre les couches (n) et (n+1).

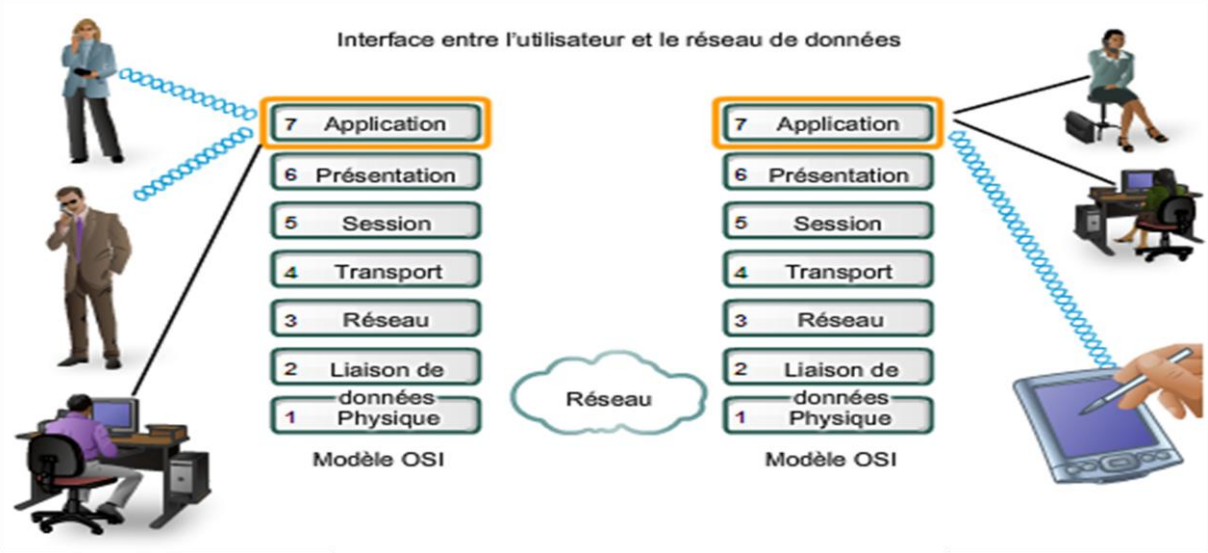
3.1. Avantages du modèle OSI

- ✓ Réduit la complexité, puisque cela subdivise la communication en plus petites couches.

- ✓ Standardise bien sur les interfaces.
- ✓ Permet un meilleur développement et une meilleure évolution, car il suffit d'interagir sur la couche qui doit être modifiée.
- ✓ Diviser les problèmes de communication sur les réseaux en problèmes plus simples et plus faciles à gérer.
- ✓ Chaque couche exerce des fonctions bien définies.
- ✓ Le nombre de couche doit être suffisamment grand pour éviter la cohabitation dans une couche de fonctions très différentes et suffisamment petit pour éviter que l'architecture devienne difficiles à maîtriser.

D'un point de vue conceptuel, chaque couche interagit avec son homologue située sur un ordinateur distant. En pratique, chaque couche communique avec la couche au dessus et en dessous d'elle.

4. 1.Description des couches OSI



Couche Application (7)

- ➢ Sert d'interface entre les applications à chaque extrémité du réseau.
- ➢ Permet d'changer des données entre les programmes s'exécutant sur les hôtes source et de destination
- ➢ Il existe de nombreux protocoles de couche application et de nouveaux protocoles sont constamment en cours de développement.

Couche Présentation (6)

- Codage et conversion des données de la couche application afin que les données issues du périphérique source puissent être bien interprétées sur le périphérique de destination ;
- Compression des données de sorte que celles-ci puissent être décompressées par le périphérique de destination ;
- Chiffrement des données en vue de leur transmission et déchiffrement des données reçues par le périphérique de destination.

Couche Session (5)

- Permet d'initier un dialogue entre les applications source et de destination.
- Initier et maintenir un dialogue
- Redémarrer les sessions interrompues ou inactives pendant une longue période

Couche Transport (4)

- Permet l'acheminement de bout en bout sans se soucier des relais intermédiaires.
- Fragmentation du message en unités plus petites dites paquets
- Multiplexage

Couche réseau (3)

- Permet l'acheminement de bout en bout en tenant compte des nœuds intermédiaires
- Routage et ordonnancement des paquets

Couche liaison de données (2)

- Structuration des données en trames
- Masquer les caractéristiques physiques
- Contrôle d'erreur à l'émission et à la réception

Couche physique (1)

- Assurer la transmission de bits entre les entités physiques
- Spécifie la nature du support de communication
- Le mode de connexion et le brochage le cas échéant
- La technique de codage des bits en signaux électriques
- Les tensions et les fréquences utilisées

3. Le modèle TCP/IP (le modèle internet)

TCP/IP représente de certaine façon l'ensemble des règles de communications sur internet et se base sur la notion adressage IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Il est conçu pour répondre à certains nombre de critères parmi lesquels :

- Le fractionnement des messages en paquet.
- Utilisation d'un système d'adresses.
- L'acheminement des données sur le réseau (routage).
- Le contrôle des erreurs de transmission de données.

4. Correspondance entre les modèles TCP/IP et OSI :

Le modèle TCP/IP des réseaux est représenté par quatre couches protocole et découle du modèle général OSI des réseaux

- Couche application : qui correspond à la couche application du modèle OSI.
- Couche transport : qui regroupe les couches présentation, session, et transport du modèle OSI.
- Couche accès réseau : qui regroupe la couche liaison de données et physique du modèle OSI.

Modèle TCP/IP	**Modèle OSI**
Couche Application (4)	Couche Application
	Couche Présentation
	Couche Session
Couche Transport (TCP) (3)	Couche Transport
Couche Internet (IP) (2)	Couche Réseau
Couche Accès réseau (1)	Couche Liaison données
	Couche Physique

Tableau : comparaison entre les deux modèle OSI et TCP/IP

La virtualisation

La virtualisation est une technique qui permet de partager et d'utiliser les ressources à partir d'un seul système informatique composé de plusieurs machines virtuelles. Chaque machine virtuelle fournit un système informatique très semblable à une machine physique. Ainsi, chaque machine virtuelle peut avoir son propre système d'exploitation, applications et services réseau.

Intérêts de virtualisation

Les intérêts de la virtualisation sont nombreux on peut citer principalement :

- Installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre, notamment dans le contexte d'une mise en production à partir d'un environnement de qualification ou de pré-production, livraison facilitée.
- Installation, tests, développements, cassage et possibilité de recommencer sans casser le système d'exploitation hôte
- Sécurisation ou isolation d'un réseau (cassage de système d'exploitation virtuels, mais pas des systèmes d'exploitation hôte qui sont invisibles pour l'attaquant, tests d'architectures applicatives et réseau).
- Isolation des différent utilisateurs simultanés d'une même machine (utilisation de type site centrale).
- Allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné.
- Diminution des risques lies au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de puissance (nouveau serveur etc) étant alors transparente.

VMware Workstation

VMware Workstation est un logiciel permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

Le logiciel «GNS3»

GNS3 est un simulateur graphique d'équipement réseaux qui nous permet de créer des topologies de réseaux complexes et d'établir des simulations. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco. L'IOS c'est le système d'exploitation des **routeurs** et **Switch et firewall** Cisco et pour entrer dans l'interface graphique de chaque éléments il faut télécharger son IOS, GNS3 est compatible avec : **Windows, Linux,…etc.**

La figure 1 est la première qui s'œuvre lorsque on click sur le logiciel «GNS3», cette figure nous présente l'emplacement des différentes icones qu'on utilise pour créer un réseau:

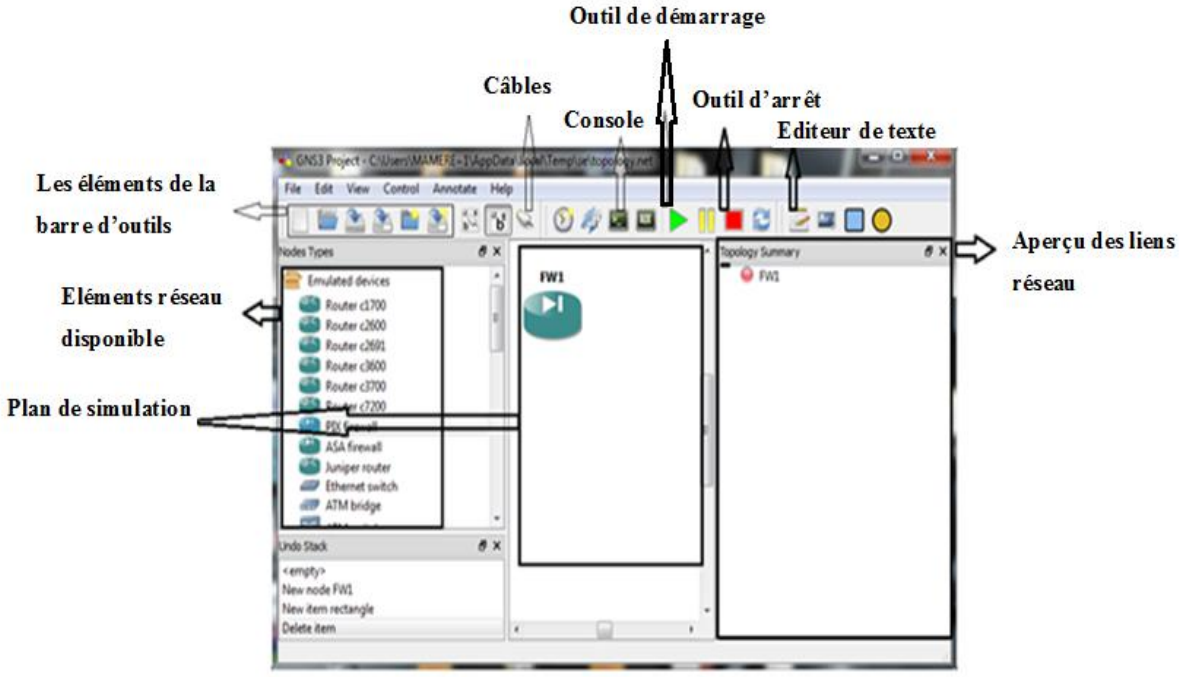


Figure 1. Détail de la fenêtre du simulateur

Pour ce qui concerne la configuration d'un firewall (ASA), On click sur EDIT puis Préférences la figure III.14 s'œuvre. Puis on suit les étapes suivantes:

- Sélectionner l'onglet **Qemu.**
- Dans le champ binary image on click sur parcourir (…) pour indiquer l'emplacement de l'IOS du ASA, on charge l'image «Initrd» et l'image «Kernel»
- On click sur « Save» puis « APPLY» et «OK»

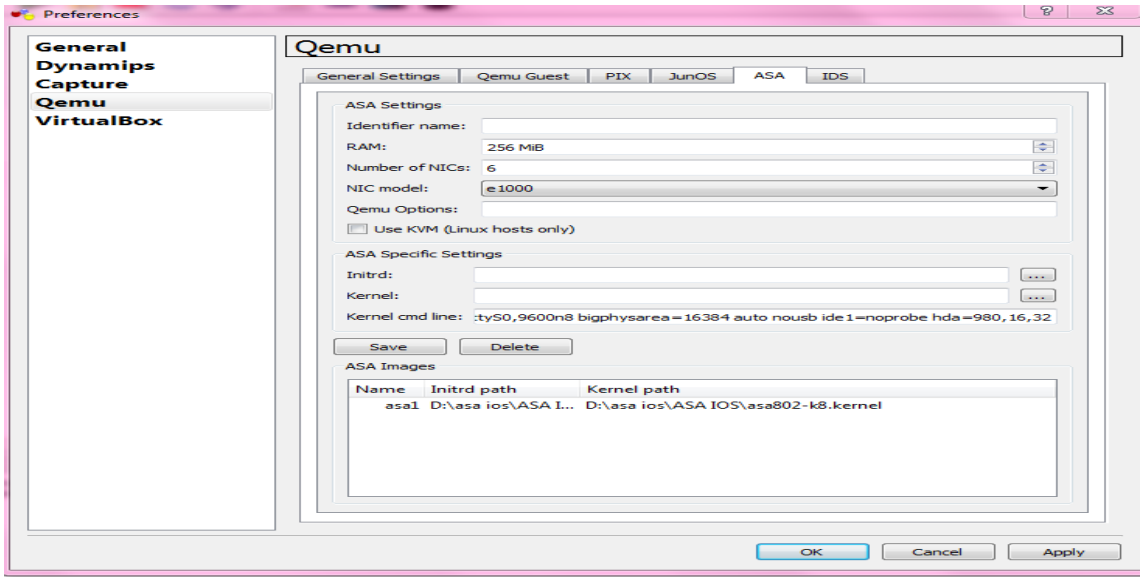


Figure 2. Localisation du binaire de Qemu

Maintenant on doit fournir notre propre IOS de Cisco à l'utilisation en GNS3.Une fois que nous avons obtenu notre propre copie d'un IOS de Cisco pour une des plateformes soutenues. Sur le menu edit on choisi IOS image and hypervisors.

Sous l'étiquette d'images d'IOS ,on click sur parcourir pour indiquer l'emplacement de notre dossier d'image IOS puis on clique save et close

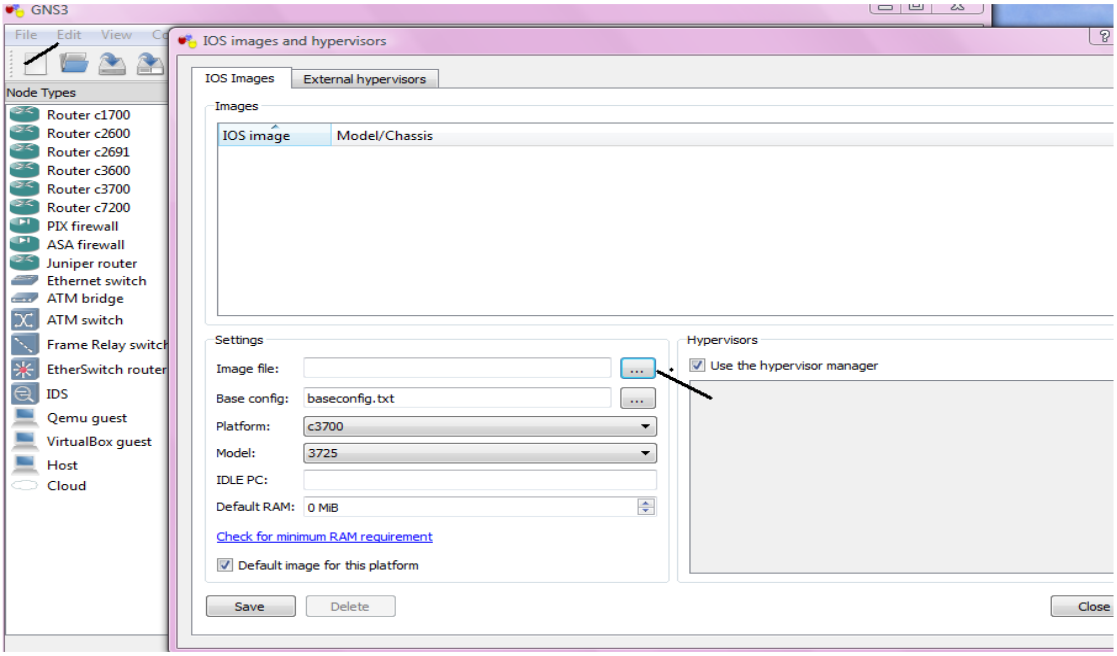


Figure 3 : localisation d'IOS and hypervisors

Enfin notre logiciel gns3 est prés pour simuler notre réseau.

Le routeur Ciscos

Un routeur Cisco est un équipement dédié aux tâches de routage des paquets IP. Les routeurs Cisco sont conçus à sur base d'une architecture de processeurs (CPU) Motorola Risc. Le CPU communique à travers un bus sur carte mère qui connecte différents types de mémoire et des interfaces de communication.

L'architecture interne du routeur Cisco prend en charge les composants qui jouent un rôle important dans le processus de démarrage. Les composants de configuration internes d'un routeur sont les suivants :

- **Mémoire RAM/DRAM** : mémoire qui stocke les tables de routage et les files d'attente de paquets. La mémoire RAM sert également de mémoire temporaire et/ou d'exécution au fichier de configuration du routeur lorsque ce dernier est sous tension. Le contenu de la mémoire RAM est perdu lors d'une mise hors tension ou d'un redémarrage.
- **Mémoire NVRAM :** mémoire non volatile (NV) qui stocke le fichier de configuration de sauvegarde/démarrage du routeur. Son contenu est conservé lors d'une mise hors tension ou d'un redémarrage.
- **Mémoire flash :** mémoire « morte » électriquement effaçable qui contient l'image du système d'exploitation. Elle permet d'effectuer des mises à niveau logicielles sans retirer ni remplacer les puces du processeur. Son contenu est conservé lors d'une mise hors tension et d'un redémarrage. Elle peut stocker plusieurs versions de la plate-forme logicielle Cisco IOS.
- **Mémoire ROM** : mémoire « morte » en lecture seule. Elle contient les diagnostics de mise sous tension, un programme d'amorçage et logiciel d'exploitation.
- **Interfaces** : connexions réseau situées sur la carte-mère ou sur des modules d'interface distincts, par lesquelles les paquets entrent et sortent du routeur. Elles sont identifiées par une adresse réseau.

Les commandes CISCO

« enable » ou « ena » ou « en » pour passer en mode administrateur sur l'équipement réseau.

Toutes les commandes indiquées ci-dessous sont à effectuer en mode administrateur.Le tableau suivant représente les différentes commandes utilisé pour la configuration d'un Switch et d'u routeur Cisco.

Commandes	Descriptions
configure terminal ou conf t ou confterm	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
Exit	Sort et remonte d'un cran dans la hiérarchie des menus
hostname ou host <hostname>	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet | fastethernet | Serial | loopback <interface>ouint e | fa | s | lo	Entre dans le mode de configuration del'interface
ip address <address><mask>ouip add	Configure l'interface avec l'ip et le masque de réseau
bandwidth ou band	Indique une bande passante
encapsulation <encap> [<type]> ou encap	Fournit l'encapsulation de l'interface
no shutdown ou no shut	Active ou Désactive l'interface
Les commandes de sauvegarde :	
copy running-config startup-configou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
copy running-configtftpou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup-configtftpou	Sauvegarde la configuration situé en
copy star tftp	NVRAM vers un serveur TFTP
copy tftp startup-configou copy tftp star	Charge un fichier de configuration d'un serveur TFTP en NVRAM
copy tftp running-configou copy tftp run	Charge un fichier de configuration d'un serveur TFTP dans la configuration courante
Commandes	***Descriptions***
erase startup-config ou erase star	Efface la configuration de la NVRAM
Configuration d'une connexion en telnet:	
router# conf t	
router(config)# line console 0	
router(config)# login	
router(config)# passwordxyz	

Les commandes de configurations du routage :	
router <xxx> [<process-id>,<autonomous system>] rip,ospf,bgp,igrp,eigrp,is-is,...	Configure le protocole de routage d'un routeur
exemple de configuration du routage RIP:	
router# conf t	
router(config)# router rip	
router(config-router)# version 1-2	la version 2 apporte le routage CIDR et l'utilisation de VLSM, un nombre de sauts à 128
router(config-router)#network *networknumber*	
exemple de configuration du routage OSPF:	
router# conf t	
router(config)# router ospf 10	
router(config-router)# network network number	
exemple de configuration du routage IGRP:	
router# conf t	
router(config)# router igrpautonomous system	
router(config-router)# network *networknumber*	
exemple de configuration du routage EIGRP:	
router# conf t	
router(config)# router eigrpautonomous system	
router(config-router)# network *networknumber*	
exemple de configuration du routage	

BGP:	
router# conf t	
router(config)# router bgp*autonomous system*	
router(config-router)# network *networknumber* [mask *network-mask*] [route-map *route-map-name*]	
D'autres commandes de routage	
ip multicast-routing	Permet de faire du routage multicast
ip rsvp bandwidth [*interface-kbps*] [*singleflow-kbps*]	Active la réservation RSVP sur une interface
Les commandes sur un Switch :	
vlan database vlan 1 name <vlan name>	Accès à la database et écriture dans le fichier vlan.dat
Exemple de configuration d'un vlan :	
switch# vlan database switch(vlan)# vlan<number><name> switch(vlan)# exit switch(config)#interface fa<iface-number> switch(config)#interface range fa... switch(config-if)#switchport mode access	affectation sur un port affectation sur un ensemble de ports on passe le mode de configuration de l'interface
Commandes	***Descriptions***
switch(config-if)# switchport access vlan <number-name>	on active le vlan sur le ou les interfaces
Activation du trunking sur l'interface	Le truncking sert dans l'extention d'un domaine VLAN sur d'autre switch, pour se faire CISCO utilise le protocole VTP VLAN Trunking Protocol
switchporttrunkencap dot1q	Il y a 2 protocoles utilisés dans l'étiquetage: le protocole ISL (CISCO) et le protocole 802.1q (IEEE)
switchport mode trunk	On active le mode trunk sur le port du

	commutateur serveur et client qui font le trunk le reste des ports sont en mode access
vlan database vtpdomain<domain-name> vtp server	Création d'un serveur VTP
vlan database vtpdomain<domain-name> vtp client	Création d'un client VTP
ip default-gateway <ip-gateway>	On peut définir une passerelle par défaut pour communiquer entre VLAN, pour se faire on utilise un routeur
encapsulation ISL | dot1q <vlan-number>	en mode interface on peut spécifier le type d'encapsulation sur le routeur
D'autres commandes communes :	
Reload	Redémarre l'équipement réseau
Setup	Passe en mode de configuration assisté
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
Les commandes show :	
show interfaces oushint	Donne une description détaillé sur les interfaces
show running-configoush run	affiche la configuration courante
Commandes	***Descriptions***
show startup-configoush star	affiche la configuration en NVRAM
show ip route ouship route	affiche la table de routage
show ip<routing-protocol> [<options>]	affiche les informations sur le protocole de routage défini
show ipprotocols	affiche des informations sur les protocoles utilisés
show ?	donne toutes les commandes show disponibles

Bibliographie

[1].MACALOU Hameye : **«** conception et réalisation d'un outil de gestion de stratégies de groupe dans un réseau active directory », Université Mouloud Mammeri Tizi-Ouzou, département informatique, thèse ingénieur, année 2009-2010.
[2].MOUSSAOUI YACINE : « conception et réalisation d'une application client/serveur d'authentification, l'autorisation et accounting dans un réseau sans fil », Université Mouloud Mammeri Tizi-Ouzou, département informatique, thèse ingénieur, année 2009-2010.

[3].BACHA DALILA : « conception et réalisation d'une application client/serveur VPN sous le protocole SSL », Université Mouloud Mammeri Tizi-Ouzou, département informatique, thèse ingénieur, année 2009-2010.

[4].N.AIT DAHMANE : « mise en place d'un tunnel VPN implémenté sur ASA Cisco » Université Mouloud Mammeri Tizi-Ouzou, département électronique, thèse master, année 2011-2012.

[5].D.HOLME : « configuration d'une infrastructure active directory avec Windows server 2008 »,Paris : dunod, 2008 : collation [VI-619] p .ill :24cm :(Kite de formation) .

[6].Jean-Georges SAURY et Silvain CAICOYA., 2007 : Windows serveur 2003 et Windows serveur 2008.1er ed, paris, 997 p.

[7].Michel de CREVOISIER « Tout sur les relations d'approbation au sein d'un domaine Active Directory (tuto de A à Z) » année 2012.

[8].Joachim GOMARD, Thomas LIAUTARD « Tout sur les relations d'approbations (Trust Relationship) » année 2012.

[9].J.C.MACKIN: « Microsoft MCITP 70-647 administrateur d'entreprise sur Windows server 2008»,Paris : dunod, 2008: collation [VI-619]p.ill; 24cm: (Kite de formation).

[10].Emmanuel Habamungu Kalume : « Etude et amélioration des performances d'un réseau informatique (LAN) cas de l'assemblée provinciale du Nord-Kivu », l'année 2010-2011 à partir de site www.mémoireonlingne.com.

[11].Xavier Lasserre, Thomas Klein et _SebF : « réseaux privé virtuels –VPN »à partir de site www.ipframe.com/vpn.

[12].William Landri : « Mise en place d'une architecture VPN MPLS avec gestion du temps de connexion et de la bande passante utilisateur », Master Européen en informatique, l'année 2009 à partir de site www.mémoireonlingne.com

[13].Philippe Latu « VPN IPsec site à site » à partir de site www.inetdoc.net

[14].M.Mostefai : « Réalisation d'un VPN SSL Host to LAN sur un ASA Cisco 5505 »université François-Rabilais à partir de site www.cisco.com/AdaptativeSécurityAppliance .