

Projet de fin de formation

Mise en Œuvre d'un



sous

Windows Server 2008

Réalisé par :

Encadré par :

Rachid BOUHADI Sofiane DAHBI ESSAKALI El kaouri LAMTI Abdraheman BOULAL





Sommaire :

Sommaire :	1
Remerciement :	3
Introduction :	4
Partie 1	5
VPN (Virtual Private Network)	6
Qu'est-ce que VPN ?	7
Cas d'utilisation de VPN	7
Les moyens techniques de VPN :	8
Avantages et inconvénients du VPN :	8
Principe de fonctionnement :	9
Fonctionnement d'un VPN :	9
Principe de fonctionnement de l'accès à distance	10
Les protocoles de tunnelisation	11
Le protocole PPTP	12
Le protocole L2TP	12
Le protocole IPSec	12
Fonctionnalités des VPN	13
Le VPN d'accès	13
L'intranet VPN	14
L'extranet VPN	15
Bilan des caractéristiques fondamentales d'un Vpn	15
Partie 2	16
Mise en place d'un serveur VPN sous Windows 2008 Server	17
Introduction :	18
Installation des serveurs sous Windows 2008 Server :	20
DNS :	20
Active Directory :	24
DHCP :	34
Services de stratégie et d'accès réseau :	41
Création des utilisateurs et des groupe :	
NIPS (stratágias ráceau) :	50
NFS (strategies reseau)	55
Installation du client :	62
Installation de la connexion VPN cliente :	62
Phase de test du client	67 70
	/0
Bibliothèque :	71





Remerciement :

Tout d'abord, je profite de cette occasion pour exprimer toute ma gratitude à tous ceux qui ont contribué à la réalisation de ce Modest travail, tenant compte à la bonne stratégie de l'institut ISTA qui nous offre une occasion d'attaquer le secteur pratique suite à celui de la théorie, afin d'améliorer nos connaissances dans le domaine.

Nous tenons à remercier nos formateurs de l'institut, pour leur bien vaillance et leur disponibilité pour nous fournir leurs Soutiens et en plus des conseils.

Nous tenons à remercier tout particulièrement ceux qui, de près ou de loin, nous ont aidés à élaborer ce travail. Nous les remercions également pour leurs pilotages efficaces, pour leurs conseils les plus précieux, leurs commentaires les plus pertinents tout au long de cette période.

Ensuite, nous souhaitons que ce travail soit à la hauteur de nos ambitions et à l'attente de notre encadreur.





Introduction :

Les réseaux locaux d'entreprise (LAN ou RLE) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'"encapsulation" (en anglais *tunneling*, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel**(noté *RPV* ou **VPN**, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit *virtuel* car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.

Le système de *VPN* permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.





Partie 1





VPN

(Virtual Private Network)

Mise en œuvre du VPN sous Windows 2008 Server





Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau (Internet par exemple). Il permet de faire transiter des informations, entre les différents membres de ce VPN, de manière sécurisée.

VPN permet à deux bureaux distants d'être liés ensemble à travers Internet et ainsi de partager des ressources entre tous les postes faisant partie du réseau local (LAN). Il s'adresse particulièrement aux employés en déplacement qui pourront ainsi profiter des ressources de l'entreprise à distance.

Pour schématiser, on peut considérer qu'une connexion VPN revient à se connecter en LAN en utilisant Internet. On peut ainsi communiquer (ping, tous protocoles IP) avec les machines de ce LAN en appelant leurs IP locales (la plupart du temps, elles ressemblent à ça : 192.168.X.X ou bien 10.X.X.X ou bien 172.16.X.X, etc...).

Un réseau VPN repose sur un protocole appelé "protocole de 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 aux extranets d'entreprise, les réseaux privés 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 une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Cas d'utilisation de VPN

On peut trouver plusieurs cas d'utilisation d'un VPN dont :

• Le Télétravail. Il existe des entreprises sans locaux, ou les employés travaillent chez eux. Quand ce type de travail est possible, pourquoi dépenser plus pour des locaux, des problèmes de transport, etc ... ? Le VPN apporte la possibilité pour tous ses employés de travailler sur un même réseau privé virtuel. Il doit alors évidement disposé d'une connexion internet qui lui permet de travailler à distance, et d'utiliser les différents services du réseau, et même exploiter des outils de travail collaboratif.





• Connexion de sites distants. Pour en entreprise possédant plusieurs sites, il est parfois avantageux de les relier. Une première solution serait d'utiliser une LS. Mais cette solution à un coup, et le VPN ne coûte pas plus que 2 connexion d'accès à internet.

Les moyens techniques de VPN :

Le VPN est ne représente donc qu'un concept, derrière lui, plusieurs implémentations ont vu le jour, selon l'utilisation que l'on veut en faire, le niveau de sécurité, la taille du réseau, etc. ...

Plusieurs moyens techniques peuvent être utilisés et couplés pour mettre en œuvre des VPN : le chiffrement, l'authentification, le contrôle d'intégrité et les tunnels.

Chiffrement : Utilisé pour que les données traversant le réseau ne puissent pas être lu par une autre personne. On utilise pour cela notre baguage mathématique et surtout arithmétique. Les deux principaux types de cryptage utilisés sont : le chiffrement asymétrique et symétrique. Le chiffrage symétrique utilisé la même clé pour chiffrer et pour déchiffrer. L'inconvénient, est clair : chaque partie de la communication devra avoir la même clé, et la communiquer à la partie adverse sans que les autres puissent le récupérer. Plusieurs algorithmes de cryptage peuvent être utilisés : DES, AES, RC4/5. Le cryptage asymétrique n'a pas cette inconvénient la : deux clés sont utilisées : une clé publique et une clé privée. La clé public est disponible par tout le monde. Elle sert à crypter des données. Si on veut communiquer avec un autre, on doit récupérer sa clé publique et seul lui pourra la décrypter avec sa clé privé. Bien sur le cryptage et le décryptage se font de manière précise suivant la méthode utilisée.

Authentification : On veut garantir qu'a chaque instant de la communication, on parle au bon interlocuteur. Dans le cadre du VPN, on parle des deux passerelles qui sont séparé par internet.

Contrôle d'intégrité : il garantit que les données transmit entre les interlocuteur n'ont pas été modifié.

Tunnel : le tunnel consiste à établir un canal entre 2 points sans ce soucier des problématique d'interconnexion (de façon transparente). Nous verrons plus en détail cet aspect important du VPN.

Avantages et inconvénients du VPN : Les avantages :

• La possibilité de réaliser des réseaux privés à moindre coût par rapport à tout autre type de connexion, l'entreprise ne paye que l'accès à Internet, il n'est pas nécessaire de payer une communication nationale ou internationale.





- La mise en œuvre d'un Intranet étendu et homogène permettant à tous les utilisateurs d'accéder à distance à des ressources partagées ou des services de types ASP, quelle que soit leur localisation.
- L'accès de vos partenaires ou vos clients à votre réseau ainsi que la possibilité de communiquer entre eux.
- L'extension de votre réseau local en toute sécurité par l'utilisation de tunnels de communication cryptés.

Les inconvénients :

- Dépendant du réseau : a contrario des connexions à la demande, les performances de l'abonnement Internet de l'un ou l'autre des deux parties (société ou nomade) ont un impact non négligeable sur la qualité des transmissions. Tout problème chez le fournisseur d'accès de l'un ou de l'autre peut provoquer une incapacité totale à communiquer.
- **Confidentialité des données** : bien qu'utilisant des systèmes de chiffrement il n'en reste pas moins que les données transitent au travers d'Internet. Du coup, elles sont potentiellement visibles de tous et ce bien qu'elles soient chiffrées.

Principe de fonctionnement :

Fonctionnement d'un VPN :

Un réseau privé virtuel repose sur un protocole, appelé **protocole de tunnelisation** (*tunneling*), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un *VPN* établi entre deux machines, on appelle *client VPN* l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et *serveur VPN* (ou plus généralement





serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur ...

Principe de fonctionnement de l'accès à distance :

L'établissement d'une connexion d'accès à distance passe par plusieurs étapes :

- 1. Un client contacte le serveur d'accès distant et lui envoie un identifiant avec un mot de passe pour tenter de s'authentifier.
- 2. Le serveur d'accès distant commence par vérifier si l'identifiant et le mot de passe correspondent à un utilisateur de l'annuaire Active Directory : c'est la phase d'authentification.
- 3. Si l'utilisateur s'est authentifié avec succès, alors le serveur d'accès distant compare les paramètres de la demande de connexion avec toutes les stratégies d'accès distant existantes.
- 4. Si les conditions d'une stratégie d'accès distant correspondent avec les paramètres de la demande de connexion, alors le serveur d'accès distant vérifie si l'utilisateur a l'autorisation de se connecter à distance au réseau de l'entreprise : c'est la phase d'autorisation.
- 5. Si l'utilisateur est autorisé à se connecter à distance au réseau de l'entreprise, alors les conditions du profil d'accès distant de la connexion sont vérifiées.
- 6. Si toutes les conditions du profil d'accès distant sont vérifiées alors la connexion est autorisée et le client reçoit une adresse IP.







Les protocoles de tunnelisation :

Les principaux protocoles de tunneling sont les suivants :

- PPTP (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'*IETF* (RFC 2661) pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.





Le Point-To-Point Tunneling Protocol (PPTP) travaille que sur des réseaux IP.

Le principe du protocole PPTP (*Point To Point Tunneling Protocol*) est de créer des trames sous le protocole PPP et de les encapsuler dans un datagramme IP.

Ainsi, dans ce mode de connexion, les machines distantes des deux réseaux locaux sont connectés par une connexion point à point (comprenant un système de chiffrement et d'authentification, et le paquet transite au sein d'un datagramme IP.

Data	gramm	ne IP		
	Trai	me PP	P	
		Me	sage original	

De cette façon, les données du réseau local (ainsi que les adresses des machines présentes dans l'en-tête du message) sont encapsulées dans un message PPP, qui est lui-même encapsulé dans un message IP.

Le protocole PPTP consiste en deux flux de communication entre le client et le serveur, s'appuyant directement sur le protocole IP :

- Le premier flux a pour rôle la gestion du lien entre les deux parties, il s'agit là d'une connexion sur le port 1723 du serveur en TCP.
- Le second flux concerne les données échangées entre les deux parties, bien entendu ce flux peut et doit être chiffré, ce dernier transite en utilisant le protocole **GRE**.

PPTP ne concerne que le transport des données, un de ces deux protocoles intervient ensuite pour sécuriser l'authentification

- Password Authentification Protocol (PAP): consiste à mettre en place une authentification entre le client et le serveur VPN. Les informations d'authentification (nom d'utilisateur et mot de passe) transitent en clair, Ce qui n'est pas l'idéal si l'on veut sécuriser au maximum...
- Challenge Handshake Authentification Protocol (CHAP): consiste en un mécanisme d'authentification crypté, il est donc sécurisé.

Le protocole L2TP

Le protocole L2TP est un protocole standard de tunnelisation (standardisé dans un RFC) très proche de PPTP. Ainsi le protocole L2TP encapsule des trames protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS).

Le protocole IPSec

IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la





sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Le protocole IPSec est basé sur trois modules :

- *IP Authentification Header* (**AH**) concernant l'intégrité, l'authentification et la protection contre le rejeu. des paquets à encapsuler
- *Encapsulating Security Payload* (**ESP**) définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu.
- *Security Assocation* (**SA**) définissant l'échange des clés et des paramètres de sécurité. Les SA rassemblent ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP (les protocoles AH et/ou ESP, mode tunnel ou transport, les algo de sécurité utilisés par les protocoles, les clés utilisées,...). L'échange des clés se fait soit de manière manuelle soit avec le protocole d'échange IKE (la plupart du temps), qui permet aux deux parties de s'entendre sur les SA.

Fonctionnalités des VPN

Il existe 3 types standards d'utilisation des VPN. En étudiant ces schémas d'utilisation, il est possible d'isoler les fonctionnalités indispensables des VPN.



Le VPN d'accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas:

L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.





Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.

Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Nous verrons que pour pallier Ce problème certaines entreprises mettent en place des VPN à base de SSL, technologie implémentée dans la majorité des navigateurs Internet du marché.

Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.



L'intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.







Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

Bilan des caractéristiques fondamentales d'un VPN :

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
- Cryptage des données. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- Gestion de clés. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multiprotocole. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

Le VPN est un principe : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.





Partie 2





Mise en place d'un serveur VPN sous Windows 2008 Server





Introduction :

Comme nous le savons, l'internet n'a pas été créer dans un optique de confidentialité, c'est pour cela qu'ont été mis au point ces fameux VPN, ils permettent de créer une liaison entre deux points (deux pairs connectés à l'internet) tout en rendant cette connexion privé et cryptée donc inaccessible à autrui qui ne serait pas autorisé afin de protéger ces données.

Dans cette partie de ce projet en va parler sur l'installation d'un serveur VPN sous Windows 2008 Server. Exemple dans un réseau local d'une entreprise pour permet à des utilisateurs de l'entreprise d'accéder d'après l'internet en tant que client VPN au réseau local pour permet d'assurer la confidentialité des données transmises.

Et cette topologie présente l'exemple d'une entreprise qu'on va le travailler dans ce projet :



Pour installer un serveur VPN a cette entreprise il est d'abord nécessaire d'installer les serveurs suivant :

- Serveur DNS (Domaine Name Système).
- Serveur DHCP (Dynamic Host Configuration Protocol).
- Services de domaine Active Directory.



Dans notre serveur qui appartient aux système d'exploitation Windows 2008 server avec deux cartes réseau :

Propriétés de Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
O Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 200 . 200 . 1
Masque de sous-réseau : 255 . 255 . 0
Passerelle par défaut :
C Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Avancé





Installation des serveurs sous Windows 2008 Server :

Corbeille			
Gestionnaire de serveur	Administrateur Documents Ordinateur Réseau Panneau de configuration Outils d'administration Aide et support Exécuter		
Tous les programmes			
Rechercher	0 • •		
💦 Démarrer 🛛 📰 🚠		FR 🌄	

Pour l'ajoute d'un rôle on clique sur Démarrer puis Gestionnaire de serveur.

DNS:

Le serveur DNS (Domain Name System) fournit la résolution de noms pour les réseaux TCP/IP. Ce serveur est plus facile à gérer s'il est installé sur le même serveur que les services de domaine Active Directory. Si vous sélectionnez le rôle services de domaine Active Directory, vous pouvez installer et configurer le serveur DNS et les services de domaine Active Directory pour qu'ils fonctionnent ensemble.

Pour ajouter le rôle Serveur DNS on choisit le menu **Rôles** puis on clique sur **Ajouter un rôle**.

O		OFPH
Gestionnaire de serveur		
hier Action Affichage ?		
🔿 🖄 📰 🛛		
Gestionnaire de serveur (WIN-QRL	Rôles	
Configuration Configuration Configuration Configuration Configuration	Afficher l'état des rôles installés sur votre serve fonctionnalités.	eur et ajouter ou supprimer des rôles et des
	Résumé des rôles	Aide sur Résumé des rôles
	Rôles: 0 fonctionnalité(s) sur 16 installée(s)	Aiouter des rôles Supprimer des Aes

Dans l'Assistant ajout de rôles on clique sur Suivant

Assistant Ajout de rôles		×
Avant de commen	cer	
Avant de commencer Rôles de serveurs Confirmation État d'avancement Résultats	Cet Assistant aide à installer des rôles sur ce serveur. Vous devez déterminer les rôles à installer en fonction des tâches que ce serveur doit effectuer, telles que le partage des documents ou l'hébergement d'un site Web. Avant de poursuivre, vérifiez que : • Le compte d'administrateur est assorti d'un mot de passe fort. • Les paramètres réseau, tels que les adresses IP statiques, sont configurés. • Les dernières mises à jour de sécurité ont été installées par Windows Update. Si vous devez effectuer une tâche à la suite de ces vérifications, annulez l'exécution de l'Assistant, effectuez les tâches requises et relancez ensuite l'Assistant. Pour continuer, diquez sur Suivant.	
🚺	Gestionnaire de serv	20:47





On sélectionne le rôle Serveur DNS dans la liste des rôles puis on clique sur Suivant

Avant de commencer Sélectionnez un ou plusieurs rôles à installer sur ce serveur. Rôles de serveur DNS Berveur DNS Confirmation Serveur DCP État d'avancement Services AD LDS (Active Directory Lightweight Directory Services de domaine Active Directory, vous services a de dipoiement Windows) Description : Résultats Services AD RNS (Active Directory Lightweight Directory Services de domaine Active Directory, vous services de dépoiement Windows) Services de forter d'active Directory Pederation Services) Services de stratégie et d'accès réseau Services VDDI Services VDDI En servicer DUDI En servicer DUDI En servicer Vuis sur les rôles de serveur	Assistant Ajout de rôles	rôles de serveurs		× 1
	Avant de commencer Rôles de serveurs Serveur DNS Confirmation État d'avancement Résultats	Sélectionnez un ou plusieurs rôles à installer sur ce serveur. Rôles : Serveur d'applications Serveur de télécopie Serveur DHCP Services AD DS (Active Directory Lightweight Directory Services) Services AD DS (Active Directory Rights Management Services) Services ADFS (Active Directory Federation Services) Services de déploiement Windows Services de déploiement Windows Services de déploiement Windows Services de déploiement Windows Services de fichiers Services de fichiers Services de fichiers Services UDDI Image: Comparison of the services of the servic	Description : Le serveur DNS (Domain Name System) fournit la résolution de noms pour les réseaux TCP/IP. Ce serveur est plus facile à gérer s'il est installé sur le même serveur que les services de domaine Active Directory, vous pouvez installer et configurerle serveur DNS et les services de domaine Active Directory pour qu'ils fonctionnent ensemble.	

Puis on clique sur Suivant

Assistant Ajout de rôles		×
Serveur DNS		
Avant de commencer Rôles de serveurs Serveur DNS Confirmation État d'avancement Résultats	 Introduction au serveur DNS Le système DNS (Domain Name System) fournit une méthode standard d'association de noms à des adresses Internet numériques. Cela permet aux utilisateurs de référencer les ordinateurs réseau en utilisant des noms hiérarchique, ce qui permet que chaque nom d'hôte soit unique sur un réseau local ou étendu. Les services DNV Windows peuvent être intégrés aux services DHCP (Dynamic Host Configuration Protocol) sous Windows. Il n'est ains plus nécessaire d'ajouter des enregistrements DNS lorsque des ordinateurs sont ajoutés au réseau. À noter ① L'intégration du serveur DNS aux services de domaine Active Directory réplique les données DNS et d'autre données du service d'annuaire, ce qui facilite la gestion DNS. ① Les services de domaine Active Directory nécessitent l'installation d'un serveur DNS avec l'Assistant Installation des services de domaine, vous pouvez aussi installer le rôle de services de domaine Active Directory, en sélectionnant le rôle Services de domaine Active Directory, en sélectionnant le rôle Services de domaine Active Directory, en sélectionnant le rôle Services de domaine Active Directory. Informations supplémentaires Yue d'ensemble du serveur DNS avec les services de domaine Active Directory ne sélectionnant le rôle Services de domaine Active Directory. Présentation de l'intégration DNS avec les services de domaine Active Directory. Pinfication d'un déploiement DNS Présentation de la réplication d'une zone DNS 	5 55
🚺	Gestionnaire de serv	20:47

Mise en œuvre du VPN sous Windows 2008 Server 22





Pour confirmer l'installation du Serveur DNS on clique sur Installer.

Confirmer les s	élections pour l'installation
Avant de commencer Rôles de serveurs	Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, cliquez sur Installer.
Serveur DNS	1 message d'information ci-dessous
Confirmation	 Ce serveur pourrait devoir être redémarré à la fin de l'installation.
Etat d'avancement Résultats	Serveur DNS
	<u>imprimer, envoyer ou enregistrer cette information</u>
	< <u>Précédent</u> <u>Suivant</u> <u>Instater</u> Annuler
	u u
Démarrer	🚡 Gestionnaire de serv
Démarrer 📰 🏭 川 Ind l'installation term	🚡 Gestionnaire de serv) FR 🔯 🗐 🕼 2 iner on clique sur Fermer
Image: Constant and the second sec	🚠 Gestionnaire de serv) FR 🔯 🗗 🕼 2 iner on clique sur Fermer
Démarrer E La Constant Ajout de rôles	Esstionnaire de serv FR to Etallation
Démarrer E I und l'installation term Assistant Ajout de rôles Image: Comparison of the second seco	🚠 Gestionnaire de serv) FR 😡 🗐 🕼 2 iner on clique sur Fermer
Démarrer E La Commencer	Gestionnaire de serv FR to Etc. 2 iner on clique sur Fermer
Démarrer Image: Ima	Es rôles, les services de rôle ou les fonctionnalités suivants ont été installés :
Démarrer E La Commencer Róles de serveurs Serveur DNS	Gestionnaire de serv FR
Démarrer Image: Ima	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Image: A continuation of the services of the s
Démarrer E E E E E E E E E E E E E E E E E E	Image: Sestionnaire de serv FR Image: Section and the serv FR Image: Section and the section
Démarrer Image: Ima	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Image: A contract of the services of the service o
Démarrer Image: Ima	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Image: Installation Image: Installation in the installed in the in
Démarrer E E E E E E E E E E E E E E E E E E	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Image: Installation Image: Installation in the Image: Ima
Démarrer Image: Ima	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Image: Installation Image: Installation in the installe installe installe installe installe installer in
Démarrer Image: Second state of the seco	Image: Sestionnaire de serv FR
Démarrer E E E E E E E E E E E E E E E E E E	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Image: Installation Image: Installation in the installed in the installed in the installed insta
Démarrer	Image: Sestionnaire de serv Image: Sectionnaire de s
Démarrer	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : 1 message(s) d'avertissement, 1 message(s) d'information d'dessous La fonctionnalité Mises à jour automatiques de Windows n'est pas activée. Pour rechercher et configuration. Serveur DNS Vous pouvez configurer un serveur DNS avec l'Assistant Configuration d'un serveur DNS dans le Gestionnaire DNS.
Démarrer	Image: Sestionnaire de serv FR Image: Section concerning the server of the ser
Démarrer	Iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : Imessage(s) d'avertissement, 1 message(s) d'information ci-dessous
Démarrer	Restionnaire de serv iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : 1 message(s) d'avertissement, 1 message(s) d'information ci-dessous I message(s) d'avertissement, 1 message(s) d'information ci-dessous I file d'ambre s' jour automatiques de Windows n'est pas activée. Pour rechercher et installer les dernières mises à jour disponibles, utilisez Windows Update dans le Panneau de configuration. Serveur DNS Serveur DNS Vous pouvez configurer un serveur DNS avec l'Assistant Configuration d'un serveur DNS dans le Gestionnaire DNS. Imprimer, envoyer ou enregistrer le rapport d'installation
Démarrer and l'installation term Assistant Ajout de rôles Résultats de l'in Avant de commencer Rôles de serveurs Serveur DNS Confirmation État d'avancement Résultats	Image: Sestionnaire de serv Image: Sectionnaire de serve
Démarrer Image: Second sec	Retionnaire de serv iner on clique sur Fermer Installation Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : 1 message(s) d'avertissement, 1 message(s) d'information ci-dessous Image: a contrained biological de la contraine de





Active Directory :

Les services de domaine Active Directory (AD DS) stockent des informations sur les objets sur le réseau et les rendent disponibles aux utilisateurs et aux administrateurs réseau. Ces services utilisent des contrôleurs de domaine pour donner accès aux ressources autorisées aux utilisateurs réseau n' importe où sur le réseau via un processus d'ouverture de session unique.

Pour ajouter le rôle Services de domaine Active Directory on choisit le menu **Rôles** puis on clique sur **Ajouter un rôle**.

🖡 Gestionnaire de serveur		_ _ _ _ _ _
Fichier Action Affichage ?		
🗢 🔿 🖄 📊 🛛		
Gestionnaire de serveur (WIN-QRL Fonctionnalités Diagnostics Configuration Stockage	Rôles Image: Afficher l'état des rôles installés sur votre serveur et ajou fonctionnalités. Résumé des rôles Rôles : 1 fonctionnalité(s) sur 16 installée(s) Serveur DNS Serveur DNS Fournit la résolution de noms pour les réseaux TCP/IP. Statut du rôle Messages : Aucun Services système : Tout exécuter Événements : Aucun erreur(s)/événement(s) pendant 24 heures	Iter ou supprimer des rôles et des Iter ou supprimer des rôles Iter ou supprimer des rôles
	Dernière actualisation : 12/06/2012 20:49:50 Configurer l'actualis	ation

Dans l'Assistant ajout de rôles on clique sur Suivant



On sélectionne le rôle Service de domaine AD dans la liste puis on clique sur Suivant.

Assistant Ajout de rôles			×IJ
Sélectionnez des	rôles de serveurs		
Avant de commencer Rôles de serveurs Services de domaine Active Direc Confirmation État d'avancement Résultats	Sélectionnez un ou plusieurs rôles à installer sur ce serveur. Rôles : Serveur d'applications Serveur DHCP Serveur DDS (Installé) Services AD LDS (Active Directory Lightweight Directory Services Services AD LDS (Active Directory Rights Management Services) Services ADFS (Active Directory Rights Management Services) Services d'application Services d'application Services Services d'application Services Services de déploiement Windows Services de stratégie et d'accès réseau Services de stratégie et d'accès réseau Services UDDI Te neavoir plus sur les rôles de serveur Services UDDI	Description : Les services de domaine Active Directory (AD DS) stockent des informations sur les objets sur le réseau et les rendent disponibles aux utilisateurs et aux administrateurs réseau. Ces services utilisent des contrôleurs de domaine pour donner accès aux ressources autorisées aux utilisateurs réseau n'importe où sur le réseau via un processus d'ouverture de session unique. > Installer Annuler	
灯 Démarrer 🛛 📃 🚠 👘 🗍	Gestionnaire de serv	🛛 🕅 👘 🗊 🕼 21	:04





Puis cliquer sur Suivant.

Assistant Ajout de rôles		×
Services de domaine Active Directory		
Avant de commencer Rôles de serveurs Services de domaine Active Direc Confirmation État d'avancement Résultats	 Introduction aux services de domaine Active Directory Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces information de façon sécurisée et l'aclitent le partage des ressources et la collaboration entre les utilisateurs. Il sont aussi nécessaires pour certaines applications fonctionnant avec annuaire, telles que Microsoft Exchange Server, et pour d'autres technologies Windows Server, telles que les Stratégies de groupe. À noter Pour faire en sorte que les utilisateurs puissent quand même se connecter au réseau en cas de panne de servicer, installe zu n minimum de deux contrôleurs de domaine pour un domaine. Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installe, vous serez invité à installer le rôle de serveur DNS sur ce serveur. Après l'Installation des services de domaine Active Directory, utilisez l'Assistant Installation des services de domaine Active Directory installe aussi l'espace de noms DFS, la réplication DFI et les services de réplication de fichiers nécessaires au service d'annuaire. Informations supplémentaires Présentation des services de domaine Active Directory Installation des services de domaine Active Directory Installation des services de domaine Active Directory Installation des services de domaine Active Directory Configurations communes pour les services de domaine Active Directory Configurations communes pour les services de domaine Active Directory 	s - 1
	< <u>Précédent</u> <u>Installer</u> Annuler	21.05

Pour confirmer l'installation du Services de domaine Active Directory on clique sur Installer.







Puis on clique sur Fermez cet Assistant et lancez l'assistant Installation des services de domaine Active Directory (dcpromo.exe).

Assistant Ajout de rôles		
Résultats de l'ins	tallation	
Avant de commencer Rôles de serveurs Services de domaine Active Direc Confirmation État d'avancement Résultats	<image/> <text><text><image/><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text>	
i I	< <u>P</u> récédent <u>S</u> uivant > <u>Eermer</u> Annuler	l J
灯 Démarrer 🛛 📰 🚠 👘 🗍	Gestionnaire de serv 🛛 🕅 👘 😨 🕼	21:08

Assistant Installation des services de domaine Active Directory.







Cliquer sur **Suivant**.

a Assistant Installation des services de domaine Active Directory	×
Compatibilité du système d'exploitation Les paramètres de sécurité étendus dans Windows Server 2008 affectent les versions précédentes de Windows	
Les contrôleurs de domaines Windows Server 2008 offrent un nouveau paramètre sécurisé, "Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0." Ce paramètre empêche Microsoft Windows et les "clients" non-Microsoft SMB d'utiliser des algorithmes de chiffrages faibles dans des sessions sur canal sécurisé vers des contrôleurs de domaines Windows Server 2008. Désormais, les opérations et applications qui requièrent un canal sécurisé servi par un contrôleur de domaine Windows Server 2008 peuvent échouer.	
Les plates formes touchées incluent Windows NT 4.0, ainsi que les clients non- Microsoft SMB et les périphériques NAS non compatibles avec les algorithmes de chiffrement forts. Certaines opérations sur les clients Windows antérieurs à Vista avec le Service Pack 1 sont également touchées, notamment les jonctions aux domaines effectuées par Active Directory Migration Tool ou Windows Deployment Services.	
Pour plus de détails à ce sujet, voir l'article 942564 (http://go.microsoft.com/fwlink/? LinkId=104751).	
< Précédent Suivant > An	nuler

Créer un controleur de domaine dans une nouvelle forêt.







Entrez le nom de domaine complet du domaine racine de forêt .

Assistant Installatio	n des services de domaine Active Directory	×
Nommez le domaine Le premier domaine nom de la forêt.	racine de la forêt : de la forêt est le domaine racine de la forêt. Il porte également le	
Entrez le nom de do	omaine complet du nouveau domaine racine de forêt.	
Nom de domaine co	omplet du domaine racine de forêt :	
projet.ma		
, Exemple : corp.cont	toso.com	
	< Précédent Suivapt >	Annuler
Assistant Installatio	on des services de domaine Active Directory	×
Nommez le domaine Le premier domaine	e racine de la forêt e de la forêt est le domaine racine de la forêt. Il porte également le	
nom de la forêt.		
Entrez le nom de de	omaine complet du nouveau domaine racine de forêt.	
Nom de domaine c	omplet du domaine racine de forêt :	
projet.ma		
Exemple : corp.c	Vérification de la disponibilité du nouveau nom de	
	forët	
	< Précédent Suivant >	Annuler





Sélectionnez le niveau fonctionnel de la foret

assistant Installation des serv	ices de domaine Active Directory	×
Définir le niveau fonctionnel d Sélectionnez le niveau fonction	e la forêt nel de la forêt.	
Niveau fonctionnel de la forêt : Windows 2000 Windows 2000 Windows Server 2003 Windows Server 2008 En Niveau fondetominel de la fore services de domaine Active Dir vous disposez de contrôleurs de Windows Server, certaines fond ces contrôleurs de domaine tan Windows 2000. En savoir plus sur les <u>niveaux fo</u>	t vvindows 21 et once toutes les fonctionnalités des p ectory disponibles dans Windows 2000 Server. Si a domaine exécutant des versions ultérieures de tionnalités avancées ne seront pas disponibles sur t que la forêt restera au niveau fonctionnel	
	< Précédent Suivant >	Annuler
Assistant Installation des serv Options supplémentaires pour	ices de domaine Active Directory le contrôleur de domaine	×
New York Options supplémentaires pour Sélectionnez des options supplé Image: Serveur DNS Image: Contrôleur de domaine en Informations supplémentaires : Le service Serveur DNS et d Le premier contrôleur de domaine global et ne peut pas être un d En savoir plus sur les options supplémentaires et le service Serveur DNS et d	ices de domaine Active Directory le contrôleur de domaine imentaires pour ce contrôleur de domaine. lecture seule (RODC) éjà installé sur ce serveur. sine d'une forêt doit être un serveur de catalogue contrôleur de domaine en lecture seule (RODC).	

Attribution IP st	atique
Cet ordinat	eur possède une ou plusieurs adresses IP attribuées dynamiquement
Cet ordinateu statique n'a é statiques à to les protocoles Voulez-vous p	r contient au moins une carte réseau physique pour laquelle aucune adresse IP té attribuée à ses propriétés IP. Vous devez attribuer une ou plusieurs adresses I outes les cartes réseau physiques pour garantir un bon fonctionnement du DNS po IPv4 et IPv6 (lorsqu'ils sont disponibles). Consultez l' <u>Aide</u> pour plus d'informations poursuivre sans attribuer d'adresses IP statiques ?
🔶 Oui, l'o	rdinateur utilisera une adresse IP attribuée dynamiquement (non
- I 👄 NOL I /	attribueral ulle adresse in statique a toutes les cartes reseau
physic Assist	ant Installation des services de domaine Active Directory

Définir l'emplacement de la base de données et des fichiers journaux et de SYSVOL

👼 Assistant Installation des services de domaine Active Directory	1	×
Emplacement de la base de données, des fichiers journaux et o Spécifiez les dossiers qui contiendront la base de données du contrôler Active Directory, les fichiers journaux et SYSVOL.	de SYSVOL ur de domaine	
Pour de meilleures performances et une meilleure récupération, stockez données et les fichiers journaux sur des volumes séparés. Dossier de la base de données :	: la base de	
C:\Windows\NTDS	Parcourir	
Dossier des fichiers journaux :		
C:\Windows\NTDS	Parcourir	
Dossier SYSVOL :		
C:\Windows\SYSVOL	Parcourir	
En savoir plus sur le <u>placement des fichiers des services de domaine A</u>	ctive Directory	
< Précédent Su	ivant > A	nnuler





Mot de passe administrateur de restauration des services d'annuaire

sistant Installation des serv	vices de domaine Active Directory	
ot de passe administrateur o	de restauration des services d'annuaire	
Le compte d'administration de compte d'administrateur de dor	restauration des services d'annuaire est différent du maine.	
Attribuez un mot de passe au c de ce contrôleur de domaine er vous recommandons de choisir	compte d'administrateur qui sera utilisé lors du démarrage n mode Restauration des services d'annuaire. Nous r un mot de passe fort.	
Mot de passe :	•••••	
Confirmer le mot de passe :	•••••	
En savoir plus sur le <u>mot de pa</u>	sse de restauration des services d'annuaire	
	< Précédent Suivent > An	nuler
	< Précédent Suivent > An	nuler
sistant Installation des ser	< Précédent Suivent > An	nuler
sistant Installation des serv Śsumé	< Précédent Suivent > An	
sistant Installation des serv śsumé Vérfliez vos sélections :	< Précédent Suivent > An vices de domaine Active Directory	
sistant Installation des serv ésumé Vérfiez vos sélections : Configurer ce serveur en tant o d'une nouvelle forêt.		
sistant Installation des ser ésumé Vérifiez vos sélections : Configurer ce serveur en tant c d'une nouvelle forêt. Le nouveau nom de domaine e	<précédent suivent=""> An vices de domaine Active Directory que premier contrôleur de domaine Active Directory est projet ma. C'est aussi le nom de la nouvelle forêt.</précédent>	
sistant Installation des serv ésumé Vérifiez vos sélections : Configurer ce serveur en tant o d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e	<précédent suivent=""> An vices de domaine Active Directory aue premier contrôleur de domaine Active Directory est projet.ma. C'est aussi le nom de la nouvelle forêt. est PROJET.</précédent>	
sistant Installation des ser ésumé Vérifiez vos sélections : Configurer ce serveur en tant c d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e Niveau fonctionnel de la forêt :	< Précédent	
sistant Installation des serv ésumé Vérifiez vos sélections : Configurer ce serveur en tant o d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e Niveau fonctionnel de la forêt ; Niveau fonctionnel du domaine	Suivert > An vices de domaine Active Directory Image: Active Directory Ima	
sistant Installation des serv ésumé Vérifiez vos sélections : Configurer ce serveur en tant c d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e Niveau fonctionnel de la forêt : Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine Site : Default-First-Site-Name	< Précédent Suivent > An vices de domaine Active Directory que premier contrôleur de domaine Active Directory est projet.ma. C'est aussi le nom de la nouvelle forêt. est PROJET. : Windows Server 2008 e : Windows Server 2008	
sistant Installation des ser sumé Vérfiez vos sélections : Configurer ce serveur en tant o d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine Site : Default-First-Site-Name Pour modifier une option, clique sur Suivant.	< Précédent	
sistant Installation des serv sumé Vérifiez vos sélections : Configurer ce serveur en tant o d'une nouvelle forêt. Le nouveau nom de domaine e Le nouveau nom de domaine e Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine Site : Default-First-Site-Name Pour modifier une option, clique sur Suivant. Vous pouvez exporter ces para réponses pour les utiliser avec d installation sans assistance. En savoir plus sur l' <u>utilisation d'</u>	< Précédent	
sistant Installation des serv ésumé Vérifiez vos sélections : Configurer ce serveur en tant c d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e Niveau fonctionnel de la forêt : Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine Site : Default-First-Site-Name Pour modifier une option, clique sur Suivant. Vous pouvez exporter ces para réponses pour les utiliser avec d'installation sans assistance. En savoir plus sur l' <u>utilisation d'</u>	< Précédent	
sistant Installation des serv ésumé Vérifiez vos sélections : Configurer ce serveur en tant of d'une nouvelle forêt. Le nouveau nom de domaine e Le nom NetBIOS du domaine e Niveau fonctionnel de la forêt : Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine Site : Default-First-Site-Name Pour modifier une option, clique sur Suivant. Vous pouvez exporter ces para réponses pour les utiliser avec d'installation sans assistance. En savoir plus sur l' <u>utilisation d'</u>	< Précédent	





Assistant Installation des services de domaine Active Directory
L'Assistant effectue la configuration des services de domaine Active Directory. Ce processus peut durer de quelques minutes à quelques heures, en fonction de votre environnement et des options que vous avez sélectionnées.
Installation de la Console de gestion des stratégies de groupe
8
Redémarrer à la fin de l'opération

Cliquer sur Terminer.



Cliquer sur Redémarrer maintenant.







DHCP:

Le serveur DHCP (Dynamic Host Configuration Protocol) permet la configuration, la gestion et l'attribution centralisées d'adresse IP et d'informations connexes pour les ordinateurs clients.

Assistant Ajout de rôles		×
Résultats de l'ins	stallation	
Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau Paramètres DNS IPv4 Paramètres WINS IPv4 Étendues DHCP Mode DHCPv6 sans état Autorisation du serveur DHCP Confirmation État d'avancement Résultats	Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : 1 message d'avertissement ci-dessous La fonctionnalité Mises à jour automatiques de Windows n'est pas activée. Pour rechercher et installer les dernières mises à jour disponibles, utilisez Windows Update dans le Panneau de configuration. Serveur DHCP Installation réussie 	
	Imprimer, envoyer ou enregistrer le rapport d'installation	
	< <u>Précédent</u> Suivant > Fermer Annuler	
灯 Démarrer 🛛 📰 🚠 👘 🗍	a Gestionnaire de serv 📉 🛛 FR 👘 💭 🕼	21:45

Choisi le rôle Serveur DHCP dans la liste des rôles puis cliquer sur Suivant









Sélectionnez l'adresse IP privée

Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau Paramètres DNS IPv4 Étendues DHCP Mode DHCPv6 sans état Paramètres DNS IPv6 Autorisation du serveur DHCP	Assistant Ajout de rôles		×
Avant de commencer Une ou plusieurs connexions réseau avec une adresse IP statique ont été détectées. Chacune d'elles peut être utilisée pour traiter les clients DHCP sur un sous-réseau distinct. Serveur DHCP Sélectionnez les connexions réseau que ce serveur DHCP utilisera pour traiter les clients. Liaisons de connexion réseau Connexions réseau : Paramètres DNS IPv4 Adresse IP Paramètres DHCP 200.200.200.1 Mode DHCPv6 sans état IPv4 Paramètres DNS IPv6 II.0.0.0.1	Sélectionner des	liaisons de connexion réseau	
Confirmation État d'avancement Résultats	Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau Paramètres DNS IPv4 Paramètres WINS IPv4 Étendues DHCP Mode DHCPv6 sans état Paramètres DNS IPv6 Autorisation du serveur DHCP Confirmation État d'avancement Résultats	Une ou plusieurs connexions réseau avec une adresse IP statique ont été détectées. Chacune d'elles peut être utilisée pour traiter les clients DHCP sur un sous-réseau distinct. Sélectionnez les connexions réseau que ce serveur DHCP utilisera pour traiter les clients. Connexions réseau : Adresse IP Type 200.200.200.1 IPv4 10.0.0.1 IPv4	
Détails Nom : Connexion au réseau local Carte réseau : Connexion réseau Intel(R) PRO/1000 MT Adresse physique : 00-0C-29-04-68-47 2 2 2 2 2 2 Adresse physique : Quivant > 2 2 2 2 2 2 2 2 2 3 3 4 4 4 4 4 4 4 4 4 4 4 4 4 4 <t< th=""><th></th><th>Détails Détails Nom : Connexion au réseau local Carte réseau : Connexion réseau Intel(R) PRO/1000 MT Adresse physique : 00-0C-29-04-68-47 Précédent Suivant > Installer Annuler</th><th></th></t<>		Détails Détails Nom : Connexion au réseau local Carte réseau : Connexion réseau Intel(R) PRO/1000 MT Adresse physique : 00-0C-29-04-68-47 Précédent Suivant > Installer Annuler	

Donner le nom de domaine parent DNS et l'adresse IPv4 du serveur DNS préférer

Assistant Ajout de rôles		×
Spécifier les para	amètres du serveur DNS IPv4	
Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau Paramètres DNS IPv4 Étendues DHCP Mode DHCPv6 sans état Paramètres DNS IPv6 Autorisation du serveur DHCP Confirmation État d'avancement Résultats	Lorsque des clients obtiennent une adresse IP du serveur DHCP, ils peuvent recevoir des options DHCP telles que les adresses IP de serveurs DNS et le nom du domaine parent. Les paramètres que vous fournissez ici seront appliqués aux clients à l'aide d'IPv4. Spécifiez le nom du domaine parent que les clients utiliseront pour la résolution de noms. Ce nom de domaine sera utilisé pour toutes les étendues créées sur ce serveur DHCP. Domaing parent : projet.ma Spécifiez les adresses IP des serveurs DNS que les clients utiliseront pour la résolution de noms. Ces serveurs DNS seront utilisés pour toutes les étendues que vous créez sur ce serveur DHCP. Adresse IPv4 du serveur DNS préféré : 10.0.0.1 Valide Adresse IPv4 du serveur DNS secondaire : Valider	
1	En savoir plus sur les paramètres du serveur DNS < Précédent Suivant > Installer Annuler]
💵 🚺 🗾 🕹 🛛 🔤	Gestionnaire de serv	21:35





Serveur WINS n'est pas requis pour les applications sur ce réseau.

Spécifier les pa	ramètres du serveur WINS IPv4	-
Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau	Lorsque des clients obtiennent une adresse IP du serveur DHCP, ils peuvent recevoir des options DHCP telles que les adresses IP de serveurs WINS. Les paramètres que vous fournissez ici seront appliqués aux clients à l'aide d'IPv4.	-
Paramètres WINS IPv4 Étendues DHCP Mode DHCPv6 sans état Paramètres DNS IPv6 Autorisation du serveur DHCP Confirmation État d'avancement Résultats	WIN <u>S</u> est requis pour les applications sur ce réseau Spécifier les adresses IP des serveurs WINS que les dients utiliseront pour la résolution de noms. Ces serveurs WINS seront utilisés pour toutes les étendues que vous créez sur ce serveur DHCP. Adr <u>e</u> sse IP du serveur WINS préféré : <u>Adresse IP du serveur WINS secondaire : </u>	
	En savoir plus sur les paramètres du serveur WINS < Précédent Suivan Installer Annuler]

Cliquer sur Ajouter pour ajouter une plage étendue DHCP

Assistant Ajout de rôles		×
Ajouter ou modifi	er les étendues DHCP	
Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau Paramètres DNS IPv4 Paramètres WINS IPv4 Étendues DHCP Mode DHCPv6 sans état Paramètres DNS IPv6 Autorisation du serveur DHCP Confirmation État d'avancement Résultats	Une étendue correspond à la plage complète d'adresses IP consécutives possibles pour un réseau. Le serveur DHCP ne peut distribuer les adresses IP aux dients qu'une fois qu'une étendue est créée. Étendues : Nom Plage d'adresses IP Nom Plage d'adresses IP Modifier Supprimer Propriétés Ajoutez ou sélectionnez une étendue pour afficher ses propriétés. En savoir plus sur l'ajout d'étendues	
📘 💦 Démarrer 🗍 🔜 🚠 👘 🗒	<pre>< Précédent Suivant > Installer Annuler Gestionnaire de serv FR 100 100 100 100 100 100 100 100 100 10</pre>	21:36





Donner un nom à la plage et l'adresse IP de départ et fin de la plage.

Ajouter une étendue	×
Une étendue est une plage d'adresses IP p peut pas distribuer les adresses IP aux clie	ossibles pour un réseau. Le serveur DHCP ne nts tant qu'une étendue n'est pas créée.
Nom de l'étendue :	plage 1
Adresse IP de dépar <u>t</u> :	10.0.0.3
Adr <u>e</u> sse IP de fin :	10.0.0.10
Masque de so <u>u</u> s-réseau :	255.0.0.0
Passerelle par <u>d</u> éfaut (facultatif) :	
Type de s <u>o</u> us-réseau :	Câblé (bail de 6 jours)
Activer cette étendue	
	RK Annuler

Assistant Ajout de rôles Ajouter ou modifi	er les étendues DHCP	×
Avant de commencer Rôles de serveurs	Une étendue correspond à la plage complète d'adresses IP consécutives possibles pour un réseau. Le serveur DHCP ne peut distribuer les adresses IP aux clients qu'une fois qu'une étendue est créée. Ét <u>e</u> ndues :	
Serveur DHCP	Nom Plage d'adresses IP Ajouter	
Liaisons de connexion réseau	plage 1 10.0.0.3 - 10.0.0.10	
Paramètres DNS IPv4		
Paramètres WINS IPv4	Supprimer	
Étendues DHCP		
Mode DHCPv6 sans état		
Paramètres DNS IPv6		
Autorisation du serveur DHCP		
Confirmation		Γ
État d'avancement		
Résultats		
	Propriétés	
	Ajoutez ou sélectionnez une étendue pour afficher ses propriétés.	
Ī	En savoir plus sur l'ajout d'étendues	
	< <u>P</u> récédent <u>S</u> uivant <u>Installer</u> Annuler	1
灯 Démarrer 🛛 📰 🚠 👘 🗍	Gestionnaire de serv FR 😡 🕫 🕼 2	21:37

Désactiver le mode sans état DHCPv6 pour ce serveur



Autoriser le serveur DHCP pour utiliser les informations d'identification actuelles







Cliquer sur Installer pour confirmer l'installation du serveur DHCP.

Assistant Ajout de rôles			×
Confirmer les sél	ections pour l'installation		
Avant de commencer Rôles de serveurs Serveur DHCP Liaisons de connexion réseau Paramètres DNS IPv4 Paramètres WINS IPv4 Étendues DHCP Mode DHCPv6 sans état Autorisation du serveur DHCP <u>Confirmation</u> État d'avancement Résultats	Pour installer les rôles, les services de 1 message d'information ci-dess 1 message d'information ci-dess Ce serveur pourrait devoir être Serveur DHCP Liaisons de connexion réseau: Paramètres DNS IPv4 Domaine parent DNS: Serveurs DNS: Serveurs WINS: Étendues Nom: Passerelle par défaut: Masque de sous-réseau : Plage d'adresses IP: Type de sous-réseau: Activer une étendue: Mode DHCPv6 sans état: Autorisation du serveur DHCP:	rôle ou les fonctionnalités suivants, cliquez sur Installer. ous redémarré à la fin de l'installation. 10.0.0.1 (IPv4.) projet.ma 10.0.0.1 Aucun plage1 Aucun 255.0.0.0 10.0.0.3 · 10.0.0.10 Câblé (bail de 6 jours) Oui Désactivé Autoriser en utilisant les informations d'identification associées à PROJET/Administrateur	
1	Imprimer, envoyer ou enregistrer cet	<u>e information</u>	I
L L Démarrer	Gestionnaire de serv	< Précédent Suivant > Install Annuler	21:38





Services de stratégie et d'accès réseau :

Les services de stratégie et d'accès réseau fournissent le serveur NPS (Network Policy Server), le routage et l'accès distant, l'autorité HRA (Health Registration Authority) et le protocole HCAP (Host Credential Authorization Protocol), qui favorisent le maintien de l'intégrité et de la sécurité de votre réseau.



VPN O	OFPPT
Assistant Ajout de rôles Avant de commer	ncer
Avant de commencer Rôles de serveurs Confirmation État d'avancement Résultats	Cet Assistant aide à installer des rôles sur ce serveur. Vous devez déterminer les rôles à installer en fonction des tâches que ce serveur doit effectuer, telles que le partage des documents ou l'hébergement d'un site Web. Avant de poursuivre, vérifiez que : • Le compte d'administrateur est assorti d'un mot de passe fort. • Les paramètres réseau, tels que les adresses IP statiques, sont configurés. • Les dernières mises à jour de sécurité ont été installées par Windows Update. Si vous devez effectuer une tâche à la suite de ces vérifications, annulez l'exécution de l'Assistant, effectuez les tâches requises et relancez ensuite l'Assistant. Pour continuer, cliquez sur Suivant.
Démarrer	Ignorer cette page par défaut < Précédent Suiller Annuler Installer Annuler

Choisi le rôle Services de stratégie et d'accès réseau puis cliquez sur Suivant.

Sélectionnez de	s rôles de serveurs	
Avant de commencer Rôles de serveurs Stratégie et accès réseau Services de rôle Confirmation État d'avancement Résultats	Sélectionnez un ou plusieurs rôles à installer sur ce serveur. Rôles : Serveur d'applications Serveur DHCP (Installé) Servicer DNS (Installé) Services AD LDS (Active Directory Lightweight Directory Services) Services AD RMS (Active Directory Rights Management Services) Services ADFS (Active Directory Rights Management Services) Services de Certificats Active Directory Services de déploiement Windows Services de déploiement Active Directory (Installé) Services de déploiement Active Directory (Installé) Services de fichiers Services UDDI En savoir plus sur les rôles de serveur	Description : Les services de stratégie et d'accès réseau foumissent le serveur NPS (Network Policy Server), le routage et l'accès distant, l'autorité HRA (Health Registration Authority) et le protocole HCAP (Host Credential Authorization Protocol), qui favorisent le maintien de l'intégrité et de la sécurité de votre réseau.





Puis cliquer sur Suivant.

Assistant Ajout de rôles		×1
Services de stratégie et d'accès réseau		
Avant de commencer Rôles de serveurs Stratégie et accès réseau Services de rôle Confirmation État d'avancement Résultats	 Introduction aux services de stratégie et d'accès réseau vous permettent de fournir un accès réseau local et distant, ainsi que de définir et d'appliquer des stratégies pour l'authentification d'accès réseau, l'autorisation et l'Intégrité des clients à l'aide du serveur NPS (Network Policy Server), du service de routage et accès distant, de l'autorité HRJ (Health Registration Authority) et du protocole HCAP (Host Credential Authorization Protocol). À onter Vous pouvez déployer NPS comme un serveur et un proxy RADIUS (Remote Authentication Dial-In User Service), et comme un serveur de stratégie de protection d'accès réseau (NAP). Après l'Installation du serveur NPS a unoyen de cet Assistant, vous pouvez configurer NPS à partir de la page d'accueil NPAS en utilisant la console NPS. La protection d'accès réseau (NAP) vous aide à garantir que les ordinateurs se connectant au réseau sont compatibles avec les stratégies d'Intégrité du réseau et des clients de lorganisation. Après l'Installation du serveur NPS à l'aide de cet Assistant, vous pouvez configurer NAP à partir de la page d'accueil NPAS en utilisant la console NPS. Diformations supplémentaires Composants des services de stratégies et d'accès réseau Méthodes de contrainte de mise en conformité NAP. Protection d'accès réseau (NAP) dans NPS Serveur NPS (Network Policy Server) 	
上 💦 Démarrer 🛛 📰 🚠 🔹 📑	Gestionnaire de serv	22:30

Choisi le serveur NPS et le service de routage et d'accès à distance



Mise en œuvre du VPN sous Windows 2008 Server 43





Pour confirmer l'installation cliquer sur Installer.

Assistant Ajout de rôles	×
Confirmer les sél	ections pour l'installation
Avant de commencer Rôles de serveurs Stratégie et accès réseau Services de rôle Confirmation État d'avancement Résultats	Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, cliquez sur Installer. 1 message d'Information ci-dessous Ce serveur pourrait devoir être redémarré à la fin de l'Installation. Services de stratégie et d'accès réseau Services de routage et d'accès à distance Service d'accès à distance Routage
Démarrar 🗖 🗮 🗐	Imprimer, envoyer ou enregistrer cette information < Précédent Suivant > Insteller Annuler Costionnaire de sons Image: Suivant > Image: Suivant > Image: Suivant >
Assistant Ajout de rôles Résultats de l'ins	tallation
Avant de commencer Rôles de serveurs Stratégie et accès réseau Services de rôle Confirmation État d'avancement Résultats	Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés :
L	Imprimer, envoyer ou enregistrer le rapport d'installation
🖉 Démarrer 🛛 🔲 🛼 👘 🗐	< <u>Précédent</u> <u>Suivant</u> > <u>Fermer</u> Annuler Gestionnaire de serv FR Image: Constraint of the serv





Clic droit sur Routage et accès distant puis Installation d'un serveur routage et accès distant



Clique sur suivant pour continuer l'installation







Choisi Accès à distance (connexion à distance ou VPN) puis clique sur Suivant

Assistant Installation d'un serveur Routage et accès distant
Configuration Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.
 Accès à distance (connexion à distance ou VPN) Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN). NAT (Network address translation) Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique. Accès VPN (Virtual Private Network) et NAT Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique. Connexion sécurisée entre deux réseaux privés Connecter ce réseau à un réseau distant tel que celui d'une succursale. Configuration personnalisée Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.
< Précédent Suivent > Annuler

On choisit VPN puis cliquer sur Suivant

Assistant Installation d'un serveur Routage et accès distant
Accès à distance Vous pouvez configurer ce serveur pour recevoir des connexions VPN et des connexions d'accès à distance.
 VPN Un serveur VPN (aussi appelé passerelle VPN) peut recevoir des connexions à partir de clients distants via Internet. Accès à distance
Un serveur d'accès à distance peut recevoir des connexions à partir de clients distants via un équipement de connexion tel qu'un modem.
< Précédent Suivant > Annuler





Sélectionnez l'interface qui appartient l'adresse local.

Interfaces réseau :		
Nom	Description	Adresse IP
Connexion au réseau local Connexion au réseau local 2	Connexion réseau Intel(R) Connexion réseau Intel(R)	200.200.200.1
•		

Attribution d'adresse IP est automatique parce que il a un serveur DHCP.

Assistant Installation d'un serveur Routage et accès distant
Attribution d'adresses IP Vous pouvez sélectionner la méthode d'assignation des adresses IP aux clients.
Comment voulez-vous que les adresses IP soient attribuées aux clients distants ?
Automatiquement
Si vous utilisez un serveur DHCP pour attribuer des adresses, vérifiez qu'il est configuré correctement. Si vous n'utilisez pas de serveur DHCP, ce serveur générera les adresses.
A partir d'une plage d'adresses spécifiée
Plus d'informations
< Précédent Suivante Annuler





Utiliser routage et accès distant pour authentifier les demandes de connexion

Assistant Installation d'un serveur Routage et accès distant				
Gestion de serveurs d'accès à distance multiples Des demandes de connexion peuvent être authentifiées localement ou transférées à un serveur RADIUS (Remote Authentication Dial-In User Service) pour être authentifiées.				
Bien que le Routage et l'accès à distance permettent l'authentification de demandes de connexion, des réseaux de grande taille incluant plusieurs serveurs d'accès à distance utilisent souvent un serveur RADIUS pour centraliser l'authentification.				
Si vous utilisez un serveur RADIUS sur votre réseau, vous pouvez paramétrer ce serveur pour transférer les requêtes d'authentification au serveur RADIUS.				
Voulez-vous configurer ce serveur pour qu'il interagisse avec un serveur RADIUS ? • Non, utiliser Routage et accès distant pour authentifier les demandes de connexion				
O Oui, configurer ce serveur pour travailler avec un serveur RADIUS				
Plus d'infomations				
< Précédent Svivant > Annuler				

Cliquer sur terminer pour terminer l'installation.







Cette fenêtre affiche que le routage et accès à distance a créé une stratégie de demande de connexion par défaut qualifiée de stratégie du service routage et accès à distance.







Création des utilisateurs et des groupes :

Dans le service de domaine Active Directory on ajoute l'utilisateur par clic droit sur user et on fait nouveau utilisateur.

Par exemple premier utilisateur : Sofiane

ouvel objet - Util	isateur	X
🔏 Créer	dans : projet.ma/Users	
Prénom :	sofiane Initiales :	
Nom :		
Nom complet :	sofiane	
Nom d'ouverture	de session de l'utilisateur :	
sofiane	@projet.ma	
Nom d'ouverture	de session de l'utilisateur (antérieur à Windows 2000) :	
PROJET\	sofiane	
	< Précédent Suivent > Annuler	

Puis en fait un mot de passe pour l'utilisateur.

Nouvel objet - Utilisateur	×
Créer dans : projet.ma/Users	
Mot de passe :	
Confirmer le mot de passe :	
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session	
L'utilisateur ne peut pas changer de mot de passe	
Le mot de passe n'expire jamais	
Le compte est désactivé	
	_
< Précédent Suivant > Annuler	



Deuxième utilisateur : Rachid

Nouvel objet - Uti	lisateur	×
🔏 Crée	r dans : projet.ma/Users	
Prénom :	rachid Initiales :	
Nom :		
Nom complet :	rachid	
Nom d'ouverture	e de session de l'utilisateur :	
rachid	@projet.ma	
Nom d'ouverture	e de session de l'utilisateur (antérieur à Windows 2000) :	
PROJET	rachid	
	< Précédent Suivant > Annuler	





Puis en fait un mot de passe pour l'utilisateur.

louvel objet - Utilisateur	×
Créer dans : projet ma/Users	
Mot de passe :	
Confirmer le mot de passe :	
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session	
✓ L'utilisateur ne peut pas changer de mot de passe	
☑ Le mot de passe n'expire jamais	
Le compte est désactivé	
< Précédent Suivant > Annuler	
louvel objet - Utilisateur	×
Créer dans : projet.ma/Users	
Quand vous cliquerez sur Terminer, l'objet suivant sera créé :	
Nom complet : rachid]
Nom de connexion de l'utilisateur : rachid@projet.ma	
L'utilisateur ne peut pas changer de mot de passe. Le mot de passe n'expire jamais.	
	1
	_
< Précédent Terminer Annuler	





Dans le service de domaine Active Directory on ajoute l'utilisateur par clic droit sur user et on fait nouveau groupe.

On crée un groupe globale de sécurité on donne par exemple le nom VPN.

×
Annuler

On clique sur ajouter pour ajouter les utilisateurs qu'on a créé.







On écrit les noms des utilisateurs puis on clique sur ok.

Sélectionnez Utilisateurs, Contacts, Ordinateurs ou Groupes	<u>?</u> ×
Sélectionnez le type de cet objet :	
Utilisateurs, Groupes ou Autres objets	Types d'objets
À partir de cet emplacement :	
projet.ma	Emplacements
E <u>n</u> trez les noms des objets à sélectionner (<u>exemples</u>) :	
rachid (rachid@projet.ma); sofiane (sofiane@projet.ma)	Vérifier les noms
Avancé OK	Annuler

Pro	priétés de vpn		<u>?</u> ×
G	énéral Membres I	Membre de 🛛 Géré par	
1	Membres :		
	Nom	Dossier Services de domaine Active Directory	
	👗 rachid	projet.ma/Users	
	👗 sofiane	projet.ma/Users	
			_
[Ajouter	Supprimer	
		OK Annuler Appli	quer





NPS (stratégies réseau) :

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Dans NPS on ouvre le menue Stratégie puis on clic droit sur Stratégie réseau puis nouveau stratégie réseau.

📕 Gestionnaire de serveur				
Fichier Action Affichage ?				
🗢 🔿 🖄 🔂 🖬				
Gestionnaire de serveur (WIN-QRLAKF0	Stratégies réseau		Actions	
E Rôles	Les stratégies réseau yous permettent d'autoriser les	_	Stratégies réseau	-
E Serveur DNS	connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions neuvent	,	Nouveau	
 Services de domaine Active Direction Services de stratégie et d'accès 	s'effectuer ou non		Exporter la liste	
🖻 🌍 NPS (Local)	Nom de la strategie	Active	Vue	•
E Clients et serveurs RADI □	Connexions à d'autres serveurs d'accès	Active	Actualiser	
🔛 Stratégies de deman			? Aide	
Stratégies reseau		Þ		
Protection d'accès résea				
E Contage et accès distant	Conditions - Si les conditions suivantes sont réunies :	-		
		=		
	Condition Valeur	- 1		
🕀 🚰 Stockage				
	Paramètros I de paramètros evivante cont appliqués :			
	Parametres - Les parametres suivants sont appliques .	=		
	Paramètre Valeur			
		_		
		<u>-</u>	J	
				4
💦 Démarrer	Gestionnaire de serv] FR 👘 🗊	23:18

On donne un nom pour la stratégie et dans le type de serveur d'accès réseau on choisit Serveur d'accès à distance (VPN-Dial up) puis Suivant.

		OFPE
Gesti ichier	Spécifier le nom de la stratégie réseau et le type de connexion Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégi s'applique.	•
	Nom de la stratégie : vpn Méthode de connexion réseau Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou Spécifique au foumisseur.	-
	Serveur d'accès à distance (VPN-Dial up) Spécifique au foumisseur : 10	
2 2 2		
ion : e	Précédent Suivan Ierminer Annuler	1

Pour spécifier les conditions de la stratégie on clique sur ajouter.

Fichier	Spécifier Spécifiez les co minimum, une c	les conditions nditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au ondition est nécessaire.	
	<u>C</u> onditions :		•
E I	Condition	Valeur	
1 1			`
🕀 🚮 F			
ء 🚰 🗉	Description de la condition :		
		Aiouter Modifier Supprimer	
		rs,	
•			
Action : e		Précédent Suivant Terminer Annuler	
💐 Démar	rer 🛛 📃 🚠 🔹 🛓 📥	Gestionnaire de serveur 🛛 \overline 🚡 Nouvelle stratégie ré 🛛 🛛 FR 👘 😨 🕼	3 23:20





On sélectionne la condition groupe d'utilisateurs puis clique sur ajouter.

Fichier	Spécifier les conditions Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.	
	Conditions :	•
i i j	Sélectionner une condition	
± 1	Sélectionnez une condition, puis cliquez sur Ajouter.	
	Groupe	•
	Groupes Windows La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
	Groupes d'ordinateurs La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
	Groupes d'utilisateurs La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
E 🔁 🚺	HCAP	
	Groupes d'emplacements La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication entre le serveur NPS et des serveurs NAS tiers. Consultez la documentation de votre serveur NAS avant d'utiliser	
	Ajout <u>e</u> r Annuler	
•		
Action : e	Précédent Suivant Terminer Annuler	
灯 Démar	irrer 🛛 📃 🚠 🔰 📕 Gestionnaire de serv 🔚 Nouvelle stratégie réseau 🖉 👘 👘 👘	23:20

Cliquer sur ajouter des groupes pour ajouter le groupe dans la condition.

Groupes d'uti	lisateurs	ľ
Spécifie <u>z</u> l'ap	opartenance aux groupes nécessaire pour correspondre à cette	
stratégie.		
Groupes		_
1	Alexandra and an and an	
	Ajouter des groupes	
	OK Annuler	





On écrit le nom de groupe qu'on a crèè.

électionnez G	roupe		<u>? ×</u>
Sélectionnez le t	ype de cet objet :		
Groupe			Types d'objets
À partir de cet er	mplacement :		
projet.ma			Emplacements
E <u>n</u> trez le nom de	e l'objet à sélectionner (<u>exe</u>	mples) :	
vpn			Vérifier les noms
A	1		
Avance			Annuler
oupes d'util Spécifie <u>z</u> l'ap stratégie.	isateurs partenance aux group	es nécessaire pour com	espondre à cette
oupes d'util Spécifie <u>z</u> l'ap stratégie.	lisateurs partenance aux group	es nécessaire pour com	≥ espondre à cette
Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\v	isateurs partenance aux group	es nécessaire pour com	≥ espondre à cette
oupes d'util Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	isateurs partenance aux group pn	es nécessaire pour com	≥ espondre à cette
oupes d'util Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	isateurs partenance aux group pn	es nécessaire pour com	espondre à cette
oupes d'util Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	isateurs partenance aux group pn	es nécessaire pour com	spondre à cette
oupes d'util Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	isateurs partenance aux group pn	es nécessaire pour com	spondre à cette
oupes d'util Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\v	isateurs partenance aux group pn	es nécessaire pour com	spondre à cette
Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	isateurs partenance aux group pn	es nécessaire pour com	≥ espondre à cette
Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	partenance aux group pn Ajouter des group	es nécessaire pour com	espondre à cette
Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\v	isateurs opartenance aux group pn Ajouter des gro <u>u</u> r	es nécessaire pour com	espondre à cette
Spécifie <u>z</u> l'ap stratégie. Groupes PROJET\w	isateurs partenance aux group pn Ajouter des gro <u>u</u> s	es nécessaire pour com	espondre à cette

Puis on clique sur suivant

Y		
		FPPT
Fichier	Spécifier les conditions Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.	
	Conditions :	•
	Condition Valeur Groupes d'utilisateurs PROJET\vpn	
•	Description de la condition : La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés. <u>Ajouter</u> <u>Modifier</u> Supprimer	
Action : e	Précédant SuivaN Terminer Annular	
灯 Démar	rer 📃 📠 🔚 Gestionnaire de serveur 🔚 Nouvelle stratégie ré 🖌 FR 👘 🖡	23:22

Autorisation d'accès aux réseau est accordé

Fichier	Spécifier l'autorisation d'accès Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.	
	 Accès accordé Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie. Accès refusé 	^
	Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie. L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS) Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie	
Action : e	Précédent Suitont Jerminer Annuler	23:22





On choisi la methode d'authentification moins sécurisée MS-CHAP v2

Fichier Image: Configure les méthodes d'authentification Image: Configure les méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP. Si vous déployez la protection d'accès réseau (NAP) avec une connexion 802.1X ou VPN, vous devez configurer le protocole PEAP (Protected EAP) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.	
Honer Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP. Si vous déployez la protection d'accès réseau (NAP) avec une connexion 802.1X ou VPN, vous devez configurer le protocole PEAP (Protected EAP) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.	
Protected EAP) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.	
	•
Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.	
Types de protocoles EAP :	
<u>Monter</u> <u>Descendre</u> <u>Ajouter</u> <u>Modifier</u> <u>Supprimer</u>	
Cc Methodes a authentification moins securisees :	
Authentification chiffrée Microsoft (MS-CHAP)	
L'utilisateur peut modifier le mot de passe après son expiration	
Authentification confirme (CHAP)	
Autoriser les clients à se connecter sans négocier une méthode d'authentification.	
Vérifier u <u>n</u> iquement l'intégrité de l'ordinateur	
Action : en Précédent SuivNat Terminer Acquier	
🎝 Démarrer 📃 🚠 🛛 🔓 Gestionnaire de serveur 🛛 🙀 Nouvelle stratégie ré 🕅 FR 🔯 👘	00:21
	9(
Configurer des contraintes	
Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion	
doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives : si yous ne souhaitez pas	
Configurer de contraintes, cliquez sur Suivant.	
E Configura las contraintes de cotte statégia résolu	
Fil a domande de contexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.	
Contraintes :	
Contraintes : Contraintes Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion	
Contraintes : Contraintes Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion	
Contraintes : Contraintes Cont	
Contraintes : Contraintes Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session D de la station D d	
Contraintes : Contraintes : Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session Délai d'expiration de session ID de la station appelée Délai train appelée Restrictions relatives aux juri jours et aux Image: Contraintes avant déconnexion	,
Contraintes : Contraintes : Contraintes Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité maximale Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité maximal d'inactivité maximale	
Contraintes Contraintes Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Délai d'inactivité Délai d'inactivité Déconnecter au-delà de la durée d'inactivité maximale Déconnecter au-delà de la durée d'inactivité maximale Image: Déconnecter au-delà de la durée d'inactivité maximale Poise Restrictions relatives aux jours et aux Image: Die general de la durée d'inactivité maximale Poise Station Image: Die general de la durée d'inactivité maximale Poise Station Image: Die general de la durée d'inactivité maximale Poise Station Image: Die general de la durée d'inactivité maximale Poise Station Image: Die general de la durée d'inactivité maximale	
Contraintes Spécfiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécfiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session Délai d'astation appelée ID de la station appelée Restrictions relatives aux jours et aux Propie Die Cc ID de port NAS Type de port NAS	
Contraintes Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session Délai d'anactivité ID de la station appelée Déconnecter au-delà de la durée d'inactivité maximale Restrictions relatives aux jours et aux Type de port NAS	
Contraintes Contraintes Délai d'inactivité Spécfiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session Délai d'astation appelée D de la station appelée Propelée Restrictions relatives aux jours et aux Type de port NAS	
Contraintes Spécfiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Spécfiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session Délai d'astation appelée Image: Die station appelée Restrictions relatives aux jours et aux Image: Die Station appelée Type de port NAS	
Contraintes Spécfiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'expiration de session Délai d'expiration de session Image de la station appelée Restrictions relatives aux jours et aux Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale Image de la connecter au-delà de la durée d'inactivité maximale	
Contraintes : Contraintes : Contraintes : Délai d'inactivité Délai d'expiration de session appelée D de la station appelée Restrictions relatives aux jours et aux Type de port NAS	
Contraintes : Contraintes Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai d'inactivité Délai d'aractivité Délai d'aractivité Délai d'aractivité Déconnecter au-delà de la durée d'inactivité maximale Dele Restrictions relatives aux jours et aux Type de port NAS Type de port NAS	
Contraintes : Contraintes : Contraintes : Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion Délai dinactivité Délai dinactivité Délai dinactivité Déconnecter au-delà de la durée d'inactivité maximale Délai Di de la station appelée Péconnecter au-delà de la durée d'inactivité maximale Restrictions relatives aux jours et aux Type de port NAS Type de port NAS Précédent Suitivation	

Fichier	Configurer le	es paramètres
← →	Le serveur NPS appli à la stratégie réseau	que des paramètres à la demande de connexion si toutes les contraintes et conditions relatives sont remplies.
⊡ ∰ Rĉ ⊕ ∰ ⊕ ∰	Configurez les paramètres de cette stra Si la demande de connexion répond a	stégie réseau. ux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.
E 👯	Para <u>m</u> ètres :	
	Attributs RADIUS	Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
	Protection d'accès	
	Contrainte de mise en conformité NAP	Attributs : Nom Valeur
	🕎 État étendu	Framed-Protocol PPP Service-Type Framed
	Routage et accès à distance	Service Type Thanieu
🕀 🚰 St	Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)	
	General Filtres IP	Ainuter Modifier Supprimer
	🛃 Chiffrement 👻	Caracterization contraction contractions

A la fin de la configuration de la nouvelle stratégie réseau en clique sur terminer

Fichier	Fin de la configuratio	n de la nouvelle stratégie réseau	<u>- ×</u>
🖃 🖥 Rô	Vous avez correctement créé la stratégie réseau sui	ivante :	•
🗉 🗄	vpn		
E 🚼	Conditions de la stratégie :		
	Condition Valeur		•
	Groupes d'utilisateurs PROJET\vpn		
	Paramètres de la stratégie :		
E Dia	Condition	Valeur	
🕀 👬 Co	Méthode d'authentification	MS-CHAP v2 OU MS-CHAP v2 (l'utilisateur peut modifier le mot de passe a	
🕀 🚰 Sti	Autorisation d'accès	Accorder l'accès	
	Mettre à jour les clients non conformes	Vrai	
	Contrainte de mise en conformité NAP	Autoriser un accès réseau complet	
	Framed-Protocol	PPP	
	Service-Type	Framed	
	Pour fermer cet Assistant, cliquez sur Terminer.		
Action : en		Précédent Suivant Teminer Annuler	
灯 Démarre	er 🛛 💻 🚠 🚽 🚊 Gestionnaire de serve	eur 🛛 🔚 Nouvelle stratégie ré 🦒 🕅 FR 👘 🕫 🕻	00:23





Installation du client :

Client est un ordinateur Windows XP courante avec SP3 qui fonctionne comme un client

d'accès distant pour le domaine projet.ma

La configuration client consiste dans les étapes suivantes :

- **4** Installez le système d'exploitation.
- **↓** Configuration TCP/IP.
- **4** Création de la connexion VPN.

Installation de la connexion VPN cliente :

Dans favoris réseau en clic droit propriété puis on clique sur Créer une nouvelle connexion.





Dans le type connexion réseau on choisit connexion au réseau d'entreprise.

Assistant Nouvelle connexion	
Type de connexion réseau Que voulez-vous faire ?	Ì
○Établir une connexion à Intern	et
Permet d'établir une connexion à Int lire des courriers électroniques.	ernet afin de pouvoir naviguer sur le Web et de
Onnexion au réseau d'entreprise	ise
Permet d'établir une connexion à un virtuel ou l'accès réseau à distance) de votre domicile ou de tout autre er	réseau d'entreprise (en utilisant un réseau privé afin de vous offrir la possibilité de travailler à partir nplacement.
🔘 Configurer une connexion avai	ncée
Permet d'établir une connexion direc série, parallèle ou votre port infrarou, ordinateurs puissent s'y connecter.	te à un autre ordinateur en utilisant votre port ge, ou configure cet ordinateur afin que d'autres
	< Précédent Suivant > Annuler





Puis on crée une connexion réseau privé virtuel.

Assistant Nouvelle connexion
Connexion réseau Comment voulez-vous vous connecter au réseau à votre bureau ?
Crée la connexion suivante :
Connexion d'accès à distance
Permet d'établir une connexion en utilisant un modem et une ligne téléphonique standard ou RNIS.
Connexion réseau privé virtuel
Permet d'établir une connexion réseau en utilisant une connexion réseau privé virtuel (VPN) via Internet.
< Précédent Suivant > Annuler

Puis on donne un nom pour cette connexion.

Assistant Nouvelle connexion
Nom de la connexion Spécifiez un nom pour cette connexion à votre lieu de travail.
Entrez un nom pour cette connexion dans la case suivante. Nom de la société projet.ma
Par exemple, vous pouvez entrer le nom de votre lieu de travail ou le nom du serveur auquel vous allez vous connecter.
< Précédent Suivant > Annuler





Puis on donne le nom du serveur ou lors adresse IP.

Assistant Nouvelle connexion
Sélection de serveur VPN Quel est le nom ou l'adresse du serveur VPN ?
Entrez le nom d'hôte ou l'adresse IP (Internet Protocol) de l'ordinateur auquel vous voulez vous connecter. Nom d'hôte ou adresse IP (par exemple, microsoft.com ou 157.54.0.1) :
200.200.200.1
< Précédent Suivant > Annuler

Assistant Nouvelle connexion
Réseau public Windows peut s'assurer que le réseau public est connecté d'abord.
Windows peut utiliser la numérotation automatique pour établir la connexion initiale à Internet ou à un autre réseau public, avant d'établir la connexion virtuelle.
💿 Ne pas établir la connexion initiale.
Établir cette connexion initiale automatiquement :
< Précédent Suivant > Annuler





On créer cette connexion pour Mon utilisation uniquement.

Assistant Nouvelle connexion
Disponibilité de connexion Vous pouvez rendre la nouvelle connexion accessible à tous les utilisateurs ou bien uniquement à vous-même.
Une connexion qui est créée pour votre utilisation uniquement est sauvegardée dans votre compte d'utilisateur est n'est pas disponible tant que vous n'avez pas ouvert de session.
Créer cette connexion pour :
🔿 Tous les utilisateurs
 Mon utilisation uniquement
< Précédent Suivant > Annuler

A la fin de l'assistant nouvelle connexion on clique sur terminer







Phase de test du client

Pour connecter au connexion réseau privé virtuel qu'on a créé on fait double clic sur la

connexion qu'on a créé.



On donne le nom d'utilisateur et le mot de passe d'un utilisateur qu'on a créé puis on se connecte.



Puis il se connecte après un vérification de la stratégie et le groupe et l'utilisateur.







Dans le menu clients d'accès distant qui se trouve dans Routage et accès distant on voit l'utilisateur qui a accès distant au réseau de l'entreprise et on peut voir la durée de la connexion et le nombre de ports et le statut.

틡 Gestionnaire de serveur						<u>- 0 ×</u>	
Fichier Action Affichage ?							
Gestionnaire de serveur (WIN-QRLAKF0WDIF)	Clients d'accès distant (1)					Actions	
E 🔐 Rôles	Nom d'utilisateur 🔻	Durée	Nombre de ports	Statut		Clients d'acc ▲	
	PROJET \sofiane	00:10:33	1	Non comp		Autres 🕨	
🗉 对 Services de domaine Active Directory							
Services de stratégie et d'accès réseau							
Poutage et accès distant							
Interfaces réseau							
🚊 Clients d'accès distant (1)							
😐 Ports							
Connexion et strategies d'acce T							
⊞ B IPv6							
🕑 🗃 Fonctionnalités							
Diagnostics							
Configuration Stockage							
	,						
🖉 Démarrer 🛛 📃 🐁 🛛 🖡 Gest	ionnaire de serv			,	FR 🕝	n 🗊 (n 19:12	
						N C W	





Conclusion :

A travers ce dossier, nous avons vu un aperçu des différentes possibilités afin de déployer un VPN, et particulièrement la solution que représente IP Sec. Nous avions en effet pour objectif de vous donner les concepts qui tournent autour de cette solution et de vous montrer un exemple de déploiement. Mais également que le terme de VPN ne se référençait pas qu'a la solution IP Sec. Certes cette solution est la plus utilisée et est une référence. Mais le VPN est avant tout un concept et ne précise rien concernant ses moyens. Ainsi s'achève notre étude sur les VPNs. On se rend compte que derrière ce concept, une multitude de protocoles, techniques et architectures existent pour leur déploiement.

Néanmoins, le choix d'une solution pour votre VPN dépendra évidement de l'utilisation que vous en ferez et de l'investissement financier que vous y mettrez.

Le VPN à pris une dimension proportionnelle au développement d'internet. A l'origine pour déployer les réseaux privés, une nouvelle utilisation voit le jour aujourd'hui avec l'arrivée des technologies sans file. En effet, dès les premières mises en place du 802.11 (WIFI), on nous à démontré ses failles en matière de confidentialité et de sécurité. Un risque parmi d'autres, est de voir ses données transitant dans le réseau être Lues par un « homme du milieu ». Ses problèmes de sécurité sont une grande problématique quand des données sensibles sont communiquées. Les solutions VPN offre une possibilité de garantir cette sécurité et on peut alors penser à la possibilité d'allier le confort d'utilisation d'un réseau sans file à la sécurité des données qu'on transmet.





Bibliothèque :

http://free.korben.info/index.php/VPN

http://www.frameip.com/vpn/

http://telecomix.ceops.eu/DeReynal-DeRorthais-Tan-VPN.pdf

http://www.commentcamarche.net/contents/initiation/vpn.php3

http://www.labo-microsoft.org/articles/win/ras2003/