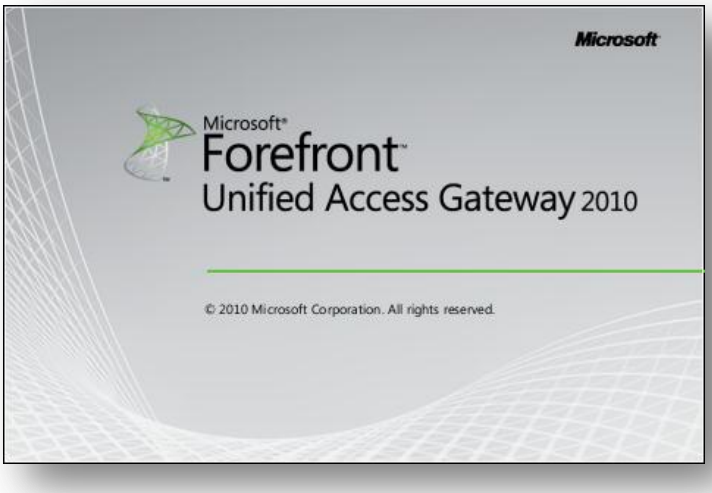
Microsoft Forefront UAG 2010 SP1

Mise en œuvre d'une plateforme DirectAccess pas à pas – Fondamentaux

Advanced architecture and Design for DirectAccess



jeudi, 14 avril 2011

Version 1.2

Rédigé par

benoits@exakis.com

MVP Enterprise Security 2010

Benoits@exakis.com

Fiche de révision et de signature

Historique des versions

Date	Auteur	Version	Modification
16/01/2011	Benoît SAUTIERE	1.2	Corrections mineures
20/11/2010	Benoît SAUTIERE	1.1	Découpage en parties
06/11/2010	Benoît SAUTIERE	1.0	Création du document

Relecteur

Nom	Version approuvée	Fonction	Date
Benoît SAUTIERE	1.2	MVP Entreprise Security	16/01/2011
Benoît SAUTIERE	1.1	MVP Entreprise Security	20/11/2010
Benoît SAUTIERE	1.0	MVP Entreprise Security	06/11/2010

Sommaire

1 INTRODUCTION

1.1 Qui suis-je ?

Benoît SAUTIERE, en poste chez Exakis comme référent technique depuis début 2008. Cette société est partenaire Gold Microsoft depuis sa création en 2001. Les services proposés couvrent un grand nombre de domaines :

- Architecture autour des produits d'infrastructure (Windows, Communications unifiées, gamme System Center)
- La sécurisation des infrastructures
- Architecture et développement de solution autour du travail collaboratif
- Le conseil au sens large sur les solutions Microsoft

Mon parcours « Microsoft » a commencé avec Windows NT 3.51 et produits associés, pour progressivement me spécialiser sur les solutions d'infrastructures Microsoft et arriver aujourd'hui à Windows 2008 R2. C'est au TechEd 2008 que j'ai découvert ce qui deviendra DirectAccess, sujet que j'ai développé tout au long de nombreux billets sur mon blog : Simple by design, signant mes articles avec la mention « Simple and Secure by Design », maintenant complétée de « and Business compliant ».

Récompensé par un « MVP Enterprise Security » en Octobre 2009, j'ai poursuivi mon bonhomme de chemin et partagé mon expérience sur DirectAccess et les sujets connexes tels que Network Access Protection, IPv6 et bien d'autres sujets très souvent orientés sur la sécurité.

1.2 Présentation du contexte

La mobilité prend de plus en plus de place au sein des entreprises. Il n'est pas rare aujourd'hui pour un cadre de disposer non plus d'un poste de travail mais bien d'un ordinateur portable connecté à Internet, disposant ainsi d'une connectivité avec le système d'information de son entreprise.

Problème, face à ce besoin de mobilité, les contraintes de sécurité telles que mises en œuvre jusqu'à maintenant montrent leurs limites. Jusqu'à maintenant, la conception de la sécurité faisait qu'on se focalisait sur la localisation de l'utilisateur pour déterminer si son accès doit être considéré comme sécurisé ou non. C'est l'approche du château fort.

Dans cette approche, on considère que par ce que l'utilisateur est connecté sur le réseau interne, il est forcément « de confiance ». L'épaisseur des murs constitue un rempart inébranlable contre tout risque en provenance de l'extérieur.

Cette approche a commencé à montrer ses limites avec l'arrivée du nomadisme. Des postes de travail sortent des murs et sont connectés à un réseau inconnu : Internet. Pire, ces postes s'y connectent pour ensuite revenir dans les murs de l'entreprise.

Pour adresser cette problématique, on a décidé qu'il fallait demander à l'utilisateur de prouver son identité avec un moyen dont il dispose ainsi qu'une information qu'il est le seul à connaître : soit une authentification à double facteurs, communément représenté par la carte à puce.

A ce stade, on ne traite qu'une partie de la problématique. On est capable de prouver son identité lorsqu'on se connecte. Cependant, rien n'est prévu concernant la sécurité du dit poste de travail. Le poste nomade ayant pour vocation de sortir de l'entreprise et être connecté à Internet, il est à la merci de toutes les menaces potentielles. Le problème, c'est quand un poste nomade infecté rentre dans l'entreprise. Par ce qu'il est dans l'entreprise, il est sécurisé!

Problème, personne à l'entrée de l'entreprise ne vérifie que le poste ne présente pas de menace pour les autres postes. C'est quand on connecte le câble réseau qu'il est souvent trop tard !

On dispose bien de mécanismes de contrôles de conformité pour les postes nomades. Toute solution de VPN/SSL qui se respecte (UAG inclus) propose ce type de solution. Cependant, celles-ci n'étant pas utilisable sur le réseau LAN de l'entreprise, on ne peut garantir la sécurité des postes. Sur le réseau LAN, on peut déployer des solutions de gestion de la conformité, mécanismes d'isolation et de remédiation. Chez Microsoft, cela se nomme Network Access Protection et c'est la même solution pour le réseau interne et les postes nomades.

Microsoft Forefront

Microsoft possède une gamme de produit orienté sur la sécurité et la gestion des identités. Cette gamme de produit a pour nom « Microsoft Forefront ».

Au travers de cette gamme de nombreux produits sont déjà disponibles et d'autres arrivent pour aider à développer les entreprises en toute sécurité. Forefront fournit une protection qui prend en compte l'ensemble des systèmes et données de votre entreprise, tout en permettant l'accès de vos employés, en tout lieu, sur la base de leur identité. DirectAccess est une nouvelle approche de la mobilité permettant de :

- Répondre aux nouveaux besoins et usages
  Il est courant aujourd'hui que l'utilisateur en entreprise dispose d'un ordinateur portable devant lui permettre d'accéder au système d'information et ce qu'il soit dans les locaux de l'entreprise ou à l'extérieur.
- Rendre les utilisateurs plus mobiles

  Dès lors que l'utilisateur est de plus en plus nomade, il faut pouvoir lui proposer un accès aux ressources de l'entreprise le plus transparent possible. Un utilisateur nomade sans accès à ses ressources ne peut pas travailler. C'est un objectif fondamental de DirectAccess.

- Se connecter depuis n'importe où

  Du point de vue de l'utilisateur final, il doit pouvoir travailler depuis n'importe où, que ce soit à son domicile, chez un client dans un hôtel, un aéroport. Les limitations techniques ont toujours bridé les utilisateurs, ne pouvant accéder qu'à certaines ressources pour cause de contraintes techniques qui ne les concernent pas. La nouvelle approche réseau de DirectAccess permet de lever ces limitations.

- Rester connecté en permanence

  Un poste nomade est complexe à administrer car lorsqu'il est à l'extérieur de l'entreprise. DirectAccess change la donne car c'est le système d'exploitation qui va assurer la connexion au système d'information et son maintien. Le poste de travail sera même capable de changer de réseau (Wifi vers 3G par exemple). DirectAccess étend le réseau

interne de l'entreprise jusqu'aux postes portables en situation de mobilité. Les postes de travail en situation de mobilité sont donc administrables de la même manière que les postes de bureau.

- Travailler plus efficacement

  Dès lors que l'utilisateur n'a pas à se soucier de comment se connecter au système d'information, il est immédiatement opérationnel, sans avoir à se soucier de la technologie sous-jacente.

Au cours de cette présentation technique, nous allons présenter un des nombreux usages de Microsoft ForeFront Unified Access Gateway 2010, à savoir DirectAccess. Cet article est basé sur la version UAG 2010 SP1 disponible depuis décembre 2010.

Même si la version Release Candidate est censée être très proche de la version RTM, je recommande vivement d'attendre cette dernière avant de passer en production. La version RTM devrait être disponible pour la fin de lannée 2010.

Etant donné que le sujet sera conséquent, cet article est donc découpé en plusieurs parties :

- Première partie : Fondamentaux
- Seconde partie : Préparation
- Troisième partie : PKI
- Quatrième partie : NLS
- Cinquième partie : UAG
- Sixième partie : DirectAccess
- Septième partie : Pour aller plus loin

Ce premier article a donc pour objectif de décortiquer toutes les briques utilisés dans DirectAccess. Par la suite, on rentrera dans la technique pure et dure et réaliserons l'assemblage du jeu de lego.

La mise en œuvre sera présentée en mode pas-à-pas et convient donc à tous les niveaux, exception peut-être de quelques digressions dans les interpréteurs MS-DOS et PowerShell☺

1.3 C'est quoi Forefront UAG 2010 par rapport à Forefront TMG 2010?

C'est une bonne question, merci de l'avoir posée. Historiquement, chez Microsoft le premier produit de la gamme ForeFront, c'était Microsoft Internet Security and Acceleration Server 2006, le pare-feu de Microsoft intégrant des fonctionnalités de filtrage avancés aussi bien au niveau réseau qu'applicatif.

C'est en 2006 que Microsoft a racheté la société Whales Communications et son produit « Intelligent Application Gateway and Application Optimizers ». Ce produit présentait la caractéristique d'embarquer ISA Server 2004 pour ses fonctions de pare-feu avancés ainsi que pour se protéger lui-même, rien de plus. Fin 2009, Microsoft a mis à disposition le successeur d' ISA Server : Forefront Threat Management Gateway 2010.

Tout naturellement, Microsoft se devait de proposer une nouvelle version d'IAG. Ce fut chose faîte fin 2009 avec ForeFront Unified Access Gateway 2010, réutilisant Forefront TMG 2010 pour se protéger. Si on doit différencier simplement TMG et UAG, on pourrait le résumer ainsi :

- Forefront TMG : Passerelle d'accès et de sécurisation
- Forefront UAG : Passerelle d'accès distant

Forefront UAG 2010 est un produit un peu différent des autres chez Microsoft car il se positionne sur plusieurs tableaux :

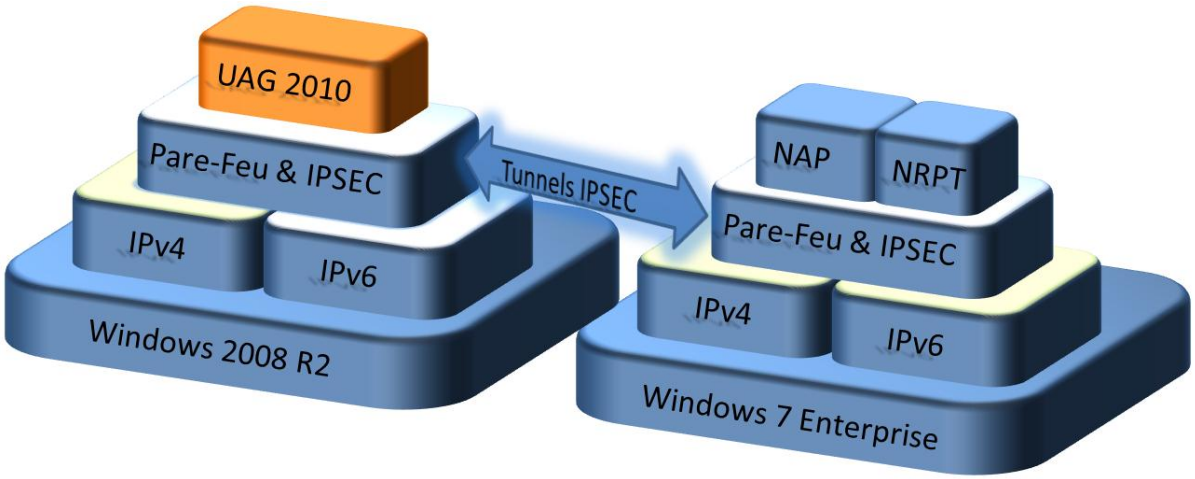
- La publication de ressources de l'entreprise à l'extérieur
- La sécurisation des accès aux ressources internes de l'entreprise

Autre caractéristique d'UAG, il est évolutif. Si une méthode d'authentification n'existe pas, rien ne nous empêche de la développer. UAG est donc d'une souplesse remarquable. Dans le cas qui nous occupe, c'est ses fonctions de sécurisation des accès aux ressources internes de l'entreprise qui nous intéressent, et plus précisément au travers de DirectAccess.

2 LE PUZZLE DIRECTACCESS

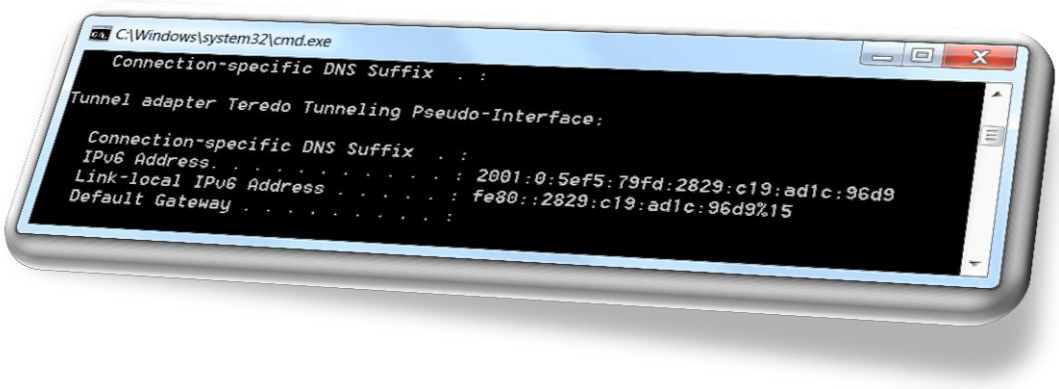
DirectAccess est un sujet à la fois simple et complexe. C'est simple car ce n'est que l'assemblage de technologies existantes, c'est complexe car il faut en maîtriser l'assemblage. Nous sommes donc en face d'un puzzle qui une fois assemblé donne entière satisfaction. Passons en revue ces pièces qui le composent :

- IPv6
- IPSec
- Pare-Feu personnel
- Systèmes d'exploitation
- Name Resolution Policy Table
- Network Location Server
- Forefront Unified Access Gateway 2010 SP1
- DirectAccess Connectivity Wizard
- Network Access Protection
- Authentification double facteur



2.1 IPv6

Commençons par ce qui fait peur, IPv6. Ça fait peur car une adresse IPv6, cela ressemble à ça!



La question, c'est pourquoi Microsoft a choisi de développer sa solution avec IPv6 :

- Proposer une solution viable répondant à la problématique de pénurie d'adresses IPv4 sur Internet
- Proposer une solution capable d'identifier les conditions de connectivité Internet et s'adapter en conséquence
- Proposer une solution reposant sur du routage et non de la publication « Reverse proxy » qui n'est pas supportée par toutes les applications

IPV6 peut faire peur. Cependant, ce qu'il faut comprendre, c'est que DirectAccess n'utilise qu'une partie d'IPv6, à savoir les technologies de transition vers IPv6 :

- ISATAP
- 6to4
- Teredo
- IP-HTTPS
- DNS64/NAT64

Tous ces protocoles sont normalisés et nativement intégrés aux systèmes d'exploitation de dernière génération. A ce stade, on peut déjà répondre à plusieurs interrogations :

- Comment va-t-on accéder à ses données depuis l'extérieur ?

  En situation de mobilité, le poste de travail va accéder aux ressources internes de l'entreprise au travers de tunnels IPSEC reposant sur la pile de protocoles IPv6

- Doit-on migrer son réseau interne en IPv6 ?

  La réponse est non. Toutes les ressources sont bien accessibles depuis l'extérieur en IPv6, y compris celles ne fonctionnant qu'en IPv4 grâce au protocole DNS64/NAT64 apporté par Microsoft Forefront Unified Access Gateway 2010 SP1

- Doit-on disposer d'une connectivité Internet en IPv6 ?

  Ici encore, la réponse est non. Dans sa version actuelle, DirectAccess ne fonctionne même pas avec une connectivité IPv6 native. Seule une banale connectivité IPv4 native est nécessaire.

- Pourquoi avoir besoin de deux adresses IPv4 publiques consécutives?

C'est un prérequis technique du protocole Teredo (RFC 4380). Dans le cas de DirectAccess, les adresses doivent nécessairement être consécutives.

- Mais alors où utilise t'on IPv6 ?
  IPv6 est principalement utilisé sur la partie Internet avec les tunnels IPSEC. Par défaut, ceux-ci sont établi entre le client Windows 7 et le serveur Microsoft Forefront Unified Access Gateway.
- N'y a-t-il pas une partie sur le LAN?

  Effectivement, on utilise aussi IPv6 sur le réseau interne de l'entreprise. Plus précisément de l'ISATAP. Cela ne concerne que les systèmes qui sont capables de faire de l'IPv6.
- Cela n'a-t-il pas un impact d'utiliser IPv6 sur le réseau LAN de l'entreprise
  L'intérêt des protocoles de transition vers IPv6, c'est leur capacité à encapsuler le trafic IPv6 dans des trames IPv4, sans impact pour les équipements réseaux actuels. De toute façon beaucoup d'équipements réseaux sont déjà prêts pour IPv6.

IPv6 intègre plusieurs technologies de transition vers IPv6 pour adresser différents scénarios :

Scénario	Protocole	Technologie
Adressage IPv6 sur le réseau interne de l'entreprise reposant sur IPv4	**ISATAP**	Encapsule le trafic IPv6 dans des trames IPv4 (Protocole IP41)
Poste de travail avec connectivité Internet publique	**6to4**	Encapsule le trafic IPv6 dans des trames IPv4 (Protocole IP41)
Poste de travail avec connectivité Internet assurée par un mécanisme de translation d'adresse (NAT)	**Teredo**	Encapsule le trafic IPv6 dans le protocole UDP 3544.
Poste de travail disposant d'une connectivité Internet limitée à HTTPS	**IP-HTTPS**	Encapsule le trafic IPv6 dans le protocole HTTPS
Résolution de noms DNS interne	**DNS64/NAT64**	Assure la résolution des noms DNS internes et met en place une translation pour les systèmes non compatibles avec IPv6.

En situation de mobilité, pour pouvoir accéder à une ressource interne, il est nécessaire de pouvoir résoudre le nom DNS de la ressource à joindre. Si la ressource n'est pas accessible en IPv6, DNS64/NAT64 assurera la translation.

2.2 IPsec

Le choix d'IPv6 est maintenant posé, passons maintenant à l'authentification et la sécurisation des flux de données échangées entre un client en situation de mobilité et le réseau interne de l'entreprise. La sécurité repose sur des tunnels IPSEC. On distinguera plusieurs types de tunnels IPSEC :

- Tunnel d'infrastructure

  Ce premier tunnel est initialisé par le système d'exploitation entre le client DirectAccess et le serveur Microsoft Forefront Unified Access Gateway 2010. L'authentification de ce tunnel repose sur le certificat « ordinateur » ainsi qu'une authentification NTLMv2. Ce tunnel est limité au système d'exploitation pour lui permettre d'accéder à des ressources d'infrastructure (DNS, Antivirus, SCCM, …) et permettre d'administrer ce poste de travail.

- Tunnel utilisateur

  Ce second tunnel est initialisé par l'utilisateur lors qu'il va tenter d'accéder à une ressource de l'entreprise. Il est initialisé entre le client DirectAccess et le serveur Microsoft ForeFront Unified Access Gateway 2010. L'authentification de ce tunnel repose sur le certificat « ordinateur » ainsi que l'authentification Kerberos de l'utilisateur. Ce tunnel est dédié à l'utilisateur pour accéder aux ressources internes de l'entreprise. Il est possible de mettre en œuvre une authentification forte à ce niveau.

- Tunnel application

  Ce dernier type de tunnel est optionnel. Il permet de configurer un groupe de serveurs de l'entreprise pour établit un tunnel IPSEC qui se terminera sur ces serveurs. L'intérêt de cette démarche est de pouvoir exiger d'appliquer de nouveaux critères pour l'authentification (utilisateur ou ordinateur appartenant à un groupe donné, authentification carte à puce obligatoire, exigence de conformité du poste de travail, …).

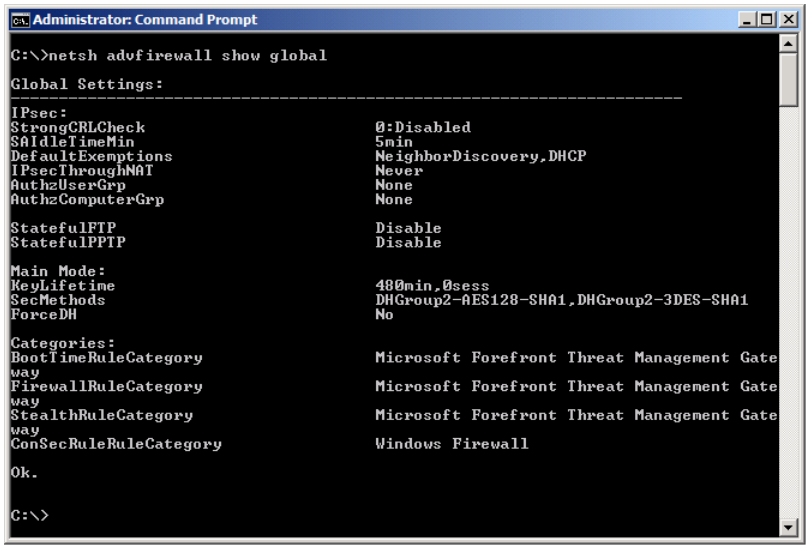
2.3 Pare-feu personnel

Depuis Windows Vista, le pare-feu personnel du système d'exploitation intègre la prise en charge d'IPSEC. Pour cette raison, il est nécessaire de conserver un pare-feu sur le poste de travail. Coté poste de travail, celui du système d'exploitation peut être conservé. Il est aussi possible d'utiliser un pare-feu tiers, tant que celui-ci est reconnu comme compatible avec Windows 7. Il doit :

- Se reposer sur l'architecture de pare-feu de Windows 7 et non la remplacer
- Ne pas remplacer le module « Windows Firewall connection Security (IPSEC)

Pour plus d'information à ce sujet, veuillez-vous référer à la rubrique Technet suivante : http://technet.microsoft.com/en-us/library/ee382257(WS.10).aspx.

Coté serveur, c'est la même chose. On conserve le pare-feu personnel de Windows Server 2008 R2. La subtilité, c'est que l'installation de Microsoft Unified Access Gateway 2010 va venir enrichir le pare-feu personnel avec Microsoft ForeFront Threat Management Gateway 2010 :



On constate que Microsoft Threat Management Gateway 2010 s'est intégré à l'architecture de pare-feu de Windows 2008 R2 en prenant soin de conserver la gestion des tunnels IPSEC au pare-feu du système d'exploitation.

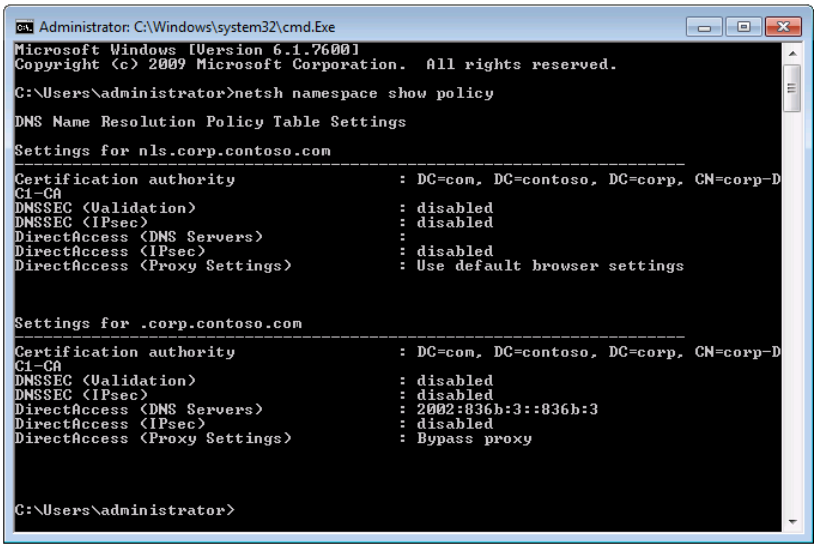
2.4 Systèmes d'exploitation

Seules les éditions Entreprise et Ultimate de Windows 7 sont éligibles à DirectAccess coté client. Les systèmes sont nécessairement membre d'un domaine. Coté serveur, les seuls systèmes d'exploitation supportés sont Windows Server 2008 R2 standard et ultérieurs.

Microsoft ForeFront Unified Access Gateway 2010 ne s'installe que sur Windows 2008 R2 éditions standard ou supérieur et uniquement en langue anglaise. La mise à niveau d'un système Windows 2008 vers R2 n'est pas recommandé.

2.5 Name Resolution Policy Table

Les fondations sont maintenant établies, ce qui manque, c'est comment accéder aux ressources internes. Des tunnels IPSEC sont mis en œuvre entre le poste de travail Windows 7 et le serveur Microsoft ForeFront Unified Access Gateway 2010, mais comment s'effectue la résolution de noms DNS? La résolution des noms DNS interne repose coté client sur la « Name Resolution Policy Table ». Celle-ci peut être affichée à l'aide de la commande suivante « NETSH.EXE NAMESPACE SHOW POLICY » :



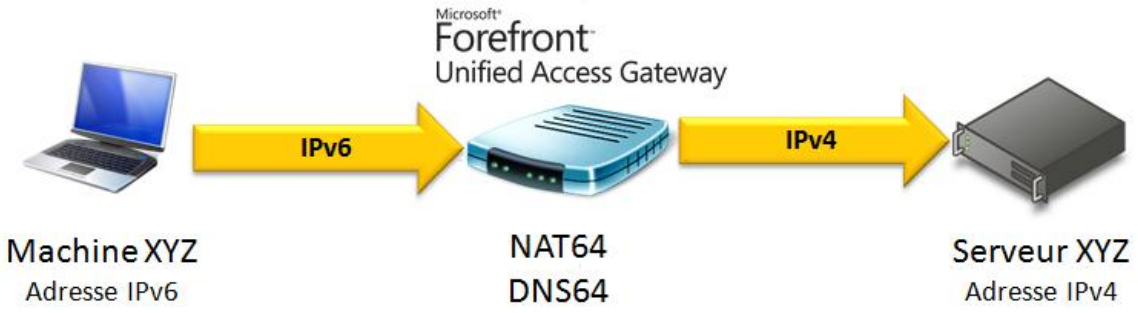
On constate tout de suite que cela associe le suffixe DNS de l'annuaire Active Directory avec une ou plusieurs adresses de serveurs DNS en IPv6. Lorsque le client est en situation de mobilité, l'ordre de résolution de nom DNS change pour devenir :

- Cache
- Host
- Name Resolution Policy Table
- DNS Internet

La configuration mise en place dans la NRPT indique que la résolution des noms DNS correspondant au domaine DNS « CORP.CONTOSO.COM » est assurée par un hôte IPv6 qui est en fait notre serveur UAG 2010. DNS64/NAT64 récupère les demandes de résolution de noms DNS et assure le traitement de la manière suivante :

- Demande de résolution du nom DNS en IPv6 et IPv4
- Si la réponse retournée est directement en IPv6 alors retourne l'information au client
- Si la réponse est uniquement IPv4 alors l'information est transmise à NAT64
- NAT64 va générer une adresse IPv6 temporaire et assurer la correspondance avec l'adresse IPv4
- Finalement, l'information IPv6 est retournée au client

La seconde référence dans la NRPT indique qu'il ne sera pas possible de résoudre un nom DNS précis : « NLS.CORP.CONTOSO.COM ». C'est normal, ce site web est utilisé comme un phare pour permettre au client d'identifier le réseau interne de l'entreprise pour lequel il n'est pas nécessaire d'utiliser la NTRP et donc DirectAccess. Ce site web ne soit donc pas être accessible de l'extérieur.



Contrairement à une implémentation de DirectAccess avec Windows 2008 R2, le serveur DNS IPv6 de l'entreprise n'est pas accessible sur Internet. Le serveur UAG joue un rôle de relais.

2.6 Network Location Server

Enfin quelque chose de simple! Dans le chapitre sur le « Name Resolution Policy Table », nous avons vu qu'il y avait une seconde entrée pour le « Network Location Server ». Ce « Network Location Server » n'est ni plus ni moins qu'un simple serveur web répondant en HTTPS avec un contenu. Ce site web est utilisé comme un phare. Lorsque le poste de travail est connecté au réseau interne de l'entreprise, celui-ci identifie le « Network Location Server » et en déduit donc qu'il n'est pas nécessaire d'utiliser la « Name Resolution Policy Table ». Il est donc normal qu'on ne puisse pas résoudre ce nom lorsque le poste de travail est en situation de mobilité. A ce stade, on peut déjà répondre à pas mal de questions sur le sujet :

- Peut-on réutiliser un site web tel que l'Intranet?

  C'est techniquement possible mais attention, ce site web ne sera pas accessible par les utilisateurs en situation de mobilité, ce n'est donc clairement pas une bonne idée.

- Doit-on acheter le certificat auprès d'un organisme tel que Verisign ou autre?

  Non, ce n'est pas nécessaire. Le certificat peut être émis par une autorité de certification interne à l'entreprise tant que celle-ci met à disposition une liste de révocation qui soit accessible par tous en interne.

- Doit-on mettre en Network Location Server en haute disponibilité?

  C'est effectivement une bonne pratique à condition de bien choisir le mécanisme de haute disponibilité. Si on se réfère à la KB968920, afin de respecter la RFC3484, le client va toujours favoriser l'adresse IP la plus proche.

- Dans les architectures de type « réseau d'agence », faut-il prévoir autant de réplique du NLS que d'agence pour couvrir l'indisponibilité du lien réseau WAN?

  Si le réseau WAN est indisponible alors le « Network Location Server » est indisponible et le client pense qu'il faut utiliser la « Name Resolution Policy Table » alors qu'il est sur le réseau LAN. C'est presque cela. En réalité, le client ne détectera la défaillance du « Network Location Server » qu'au prochain changement d'état de l'interface réseau (déconnexion, renouvellement bail DHCP, …). Si le « DirectAcess Connectivity Wizard » a bien été configuré, l'utilisateur pourra de lui-même rebasculer sur une résolution DNS standard. Une explication plus complète est disponible à cette adresse.

2.7 ForeFront Unified Access Gateway 2010 SP1

Certes, il est possible de faire du DirectAccess sans UAG. Mais alors pourquoi utiliser UAG?

- Regrouper jusqu'à huit serveurs UAG au sein d'une ferme avec une configuration centralisée
- Assurer la haute disponibilité et la répartition de charge matérielle ou logicielle au sein de la ferme UAG
- La prise en charge de NAT64/DNS64
- La capacité à réutiliser UAG pour proposer une expérience plus traditionnelle de la mobilité aux clients Windows XP, Windows Vista voire même autres
- La capacité à proposer un portail d'applications publiées avec prise en charge du SSO

2.8 DirectAccess Connectivity Assistant

C'est un composant optionnel mais tellement nécessaire pour l'utilisateur final. DirectAccess est tellement transparent pour l'utilisateur qu'il ne sait pas si cela fonctionne ou non. Pour adresser cette problématique, Microsoft a mis à disposition avec le SP1 de Microsoft ForeFront Unified Access Gateway 2010 la version 1.5 du « DirectAccess Connectivity Wizard ». Celui-ci propose une interface intuitive permettant à l'utilisateur de savoir :

- Si la connectivité Internet nécessaire pour DirectAccess est bien opérationnelle
- Si les ressources de « test » déterminant le bon fonctionnement de la solution sont bien accessibles
- S'il est nécessaire de s'authentifier avec sa carte à puce ou périphérique OTP

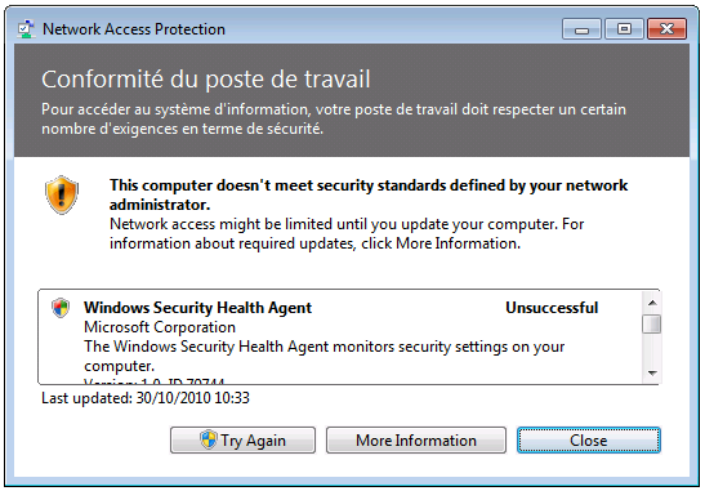
Même si UAG assure la configuration du « DirectAccess Connectivity Wizard », il n'en assure pas le déploiement.

2.9 Network Access Protection

Composant optionnel mais terriblement indispensable. Chaque constructeur qui développe une solution de nomadisme propose son propre standard. Problème, la solution n'est valable que pour les clients en situation de mobilité. Or, c'est l'ensemble qu'un faut protéger. L'approche de Microsoft consiste à proposer non pas une solution packagée complète mais un framework dans lequel Microsoft va proposer un certain nombre de composants standardisés tel que :

- Contrôle de l'état de la conformité des systèmes basés sur une ou des stratégies d'entreprise
- Correction automatique des configurations des composants de sécurité
- Isolation des systèmes en cas d'échec

Par défaut, Network Access Protection se repose sur le centre de sécurité pour déterminer le niveau de conformité. Ces critères peuvent être étendus par les solutions de sécurité (System Center Configuration Manager, ForeFront Client Security, solutions antivirus ou produits tiers) pour développer des exigences de conformité très fines. L'intégration de Network Access Protection au sein de DirectAccess permet de disposer des mêmes mécanismes de gestion de conformité pour les postes connectés au réseau LAN de l'entreprise que ceux en situation de mobilité. Le plus important reste le point de vue de l'utilisateur final. Il faut que cela reste compréhensible :



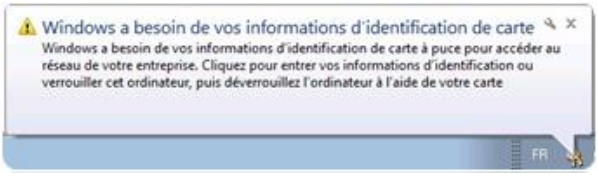
2.10 Authentification double facteur

Plus personne ne propose de solution de nomadisme sans prise en charge d'un ou plusieurs moyens d'authentification à double facteur (ce que je détiens et ce que je sais voire qui je suis). DirectAccess n'échappe pas à cette règle. Avec le Service Pack 1 de Microsoft ForeFront Unified Access Gateway 2010, les possibilités ont été accrues. L'authentification du tunnel IPSEC « utilisateur » peut désormais exploiter :

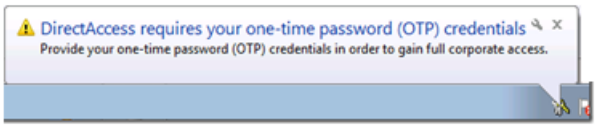
- Une authentification par carte à puce
- Un mécanisme d'authentification de type « One Time Password » (OTP)

Il est possible de pousser l'intégration jusqu'à l'ouverture de session de l'utilisateur mais dans un déploiement classique, l'utilisateur ne sera invité à s'authentifier avec sa carte à puce ou son OTP que lorsqu'il désirera accéder au système d'information. L'intégration avec la zone de notification permet de communiquer avec l'utilisateur sur ce sujet :

Carte à puce



One Time Password



Le DirectAccess Connectivity Wizard livré avec le Service Pack 1 de Microsoft Unified Access Gateway 2010 prend désormais en charge l'information de l'utilisateur quant à la nécessité de s'authentifier.

La mise en œuvre de ces mécanismes d'authentification sort du cadre de cet article. Même si c'est relativement simple du point de vue technique, l'aspect process autour de la gestion d'identité ne doit pas être négligé et nécessite une réflexion propre à chaque environnement.

2.11 Contexte matériel

J'utilise une maquette pour réaliser cette démonstration. Cette maquette n'est pas tout à fait représentative par rapport à une mise en œuvre en production mais c'est ce qu'on peut faire de plus proche. Toutes les informations présentées ci-dessous devraient vous permettre de mettre en œuvre votre propre maquette avant de nous attaquer à une mise en production. Je recommande vivement le passage par la maquette pour plusieurs raisons :

- Comprendre le fonctionnement de DirectAccess
- Appréhender IPv6
- Travailler sur la sécurité réseau
- Intégrer finement Network Access Protection
- Former vos équipes sur ces nouvelles briques

Il est vivement recommandé de vous faire conseiller par des consultants spécialisés pouvant vous assister depuis la définition de votre infrastructure, jusqu'à la mise en production. Le dossier qui va suivre couvre l'ensemble des étapes relatives à la mise en œuvre de DirectAccess, voire même aller plus loin. Les aspects réseaux n'ont pas été traités. Le découpage de dossier sera le suivant :

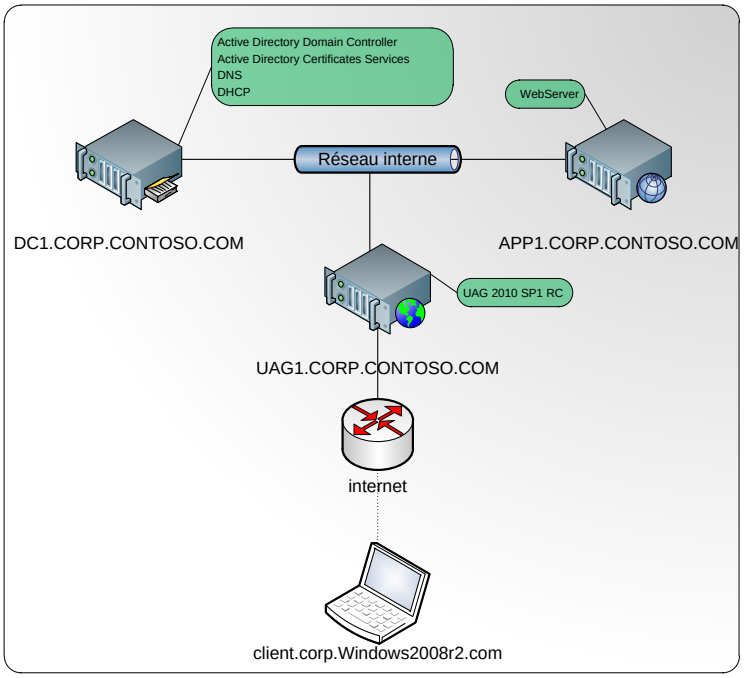
- Seconde partie : Préparation
  - Préparation de l'environnement
    - Préparation de l'infrastructure
    - Préparation réseau
    - Préparation DNS
    - Préparation Active Directory
- Troisième partie : PKI
  - Préparation Active Directory Certificates Services
    - Installation du rôle
    - Publication de la CRL
    - Sauvegarde de la clé privée
    - Configuration du rôle ADCS pour le Health Registration Authority
  - Préparation des gabarits de certificats
    - Certificats d'authentification IPSEC
    - Certificat d'état de santé
    - Certificat Network Location Server
    - Activation de l'auto-enrollment
- Quatrième partie : NLS
  - Configuration initiale du système d'exploitation
  - Installation du rôle WebServer
  - Publication de la CRL
  - Création du fichier de demande du certificat NLS
  - Soumission de la demande de certificat NLS
  - Installation du certificat NLS
- Cinquième partie : UAG
  - Configuration initiale du serveur
  - Certificat IPSEC et d'état de santé
  - Installation de Microsoft ForeFront Unified Access Gateway 2010 SP1
  - Configuration initiale UAG
  - Certificat IP-HTTPS
- Sixième partie : DirectAccess
  - Configuration de DirectAccess
  - Checklist de bon fonctionnement
- Septième partie : Pour aller plus loin

2.12 Description de l'architecture maquette

Nous utilisons ici uniquement des serveurs Windows 2008 R2 Entreprise dans cette démonstration à l'exception du de travail qui sera installé avec l'édition entreprise de Windows 7.

Détails des serveurs :

- **DC1 (512Mb)**
  - Contrôleur de domaine
  - Serveur DNS
  - Serveur DHCP
  - Serveur d'autorité racine de confiance
  - Une interface réseau connecté au LAN
- **APP1 (512Mb)**
  - Windows 2008 R2 Standard Core
  - Une interface réseau connecté au LAN
- **UAG1 (2018Mb)**
  - Windows 2008 R2 Standard Standard US
  - Serveur UAG 2010 SP1
  - Une interface réseau LAN
  - Une interface réseau Internet
- **CLIENT (512Mb)**
  - Windows 7 Enterprise
  - Une seule interface réseau



La mise en œuvre de l'annuaire Active Directory ne pose pas de problématique particulière. La mise en œuvre de l'autorité de certification fera elle l'objet de plusieurs sections. L'article se focalisant sur DirectAccess, certains sujets relatifs à l'autorité de certification ne seront pas abordés (mise hors ligne, séparation des rôles, …). Je vous invite à visiter le site Technet pour connaître les bonnes pratiques relatives au rôle ADCS. Vous pouvez consulter le portail PKI depuis ce lien http://www.microsoft.com/pki ou encore lire cet ouvrage de Brian Komar : http://www.microsoft.com/learning/en/us/Book.aspx?ID=9549&locale=en-us afin d'en savoir plus.

Coté IPv6, je conseille vivement de consulter le portail qui lui est dédié : http://www.microsoft.com/ipv6. Coté ouvrage, ce sera l'ouvrage de Joseph Davies : http://www.microsoft.com/learning/en/us/book.aspx?ID=11607&locale=en-us.

Pour finaliser la maquette, il sera nécessaire de disposer d'un certificat de type WebServer. Dans le cadre de cette démonstration, ce certificat doit être délivré par une autorité de certification reconnue comme de « Confiance » par le système d'exploitation.

2.13 Conclusion

Voilà pour les fondamentaux. J'espère que cette première partie a été assez digeste. DirectAccess repose sur des fondamentaux qu'il faut maîtriser un minimum pour l'appréhender. Prochaine étape, la préparation de notre environnement.