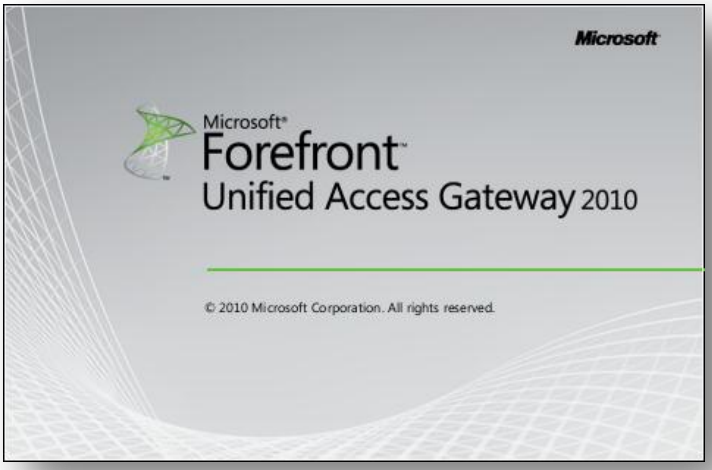
Microsoft Forefront UAG 2010 SP1

Mise en œuvre d'une plateforme DirectAccess pas à pas - UAG

Advanced architecture and Design for DirectAccess



lundi, 6 juin 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

7 CONFIGURATION DU SERVEUR UAG1

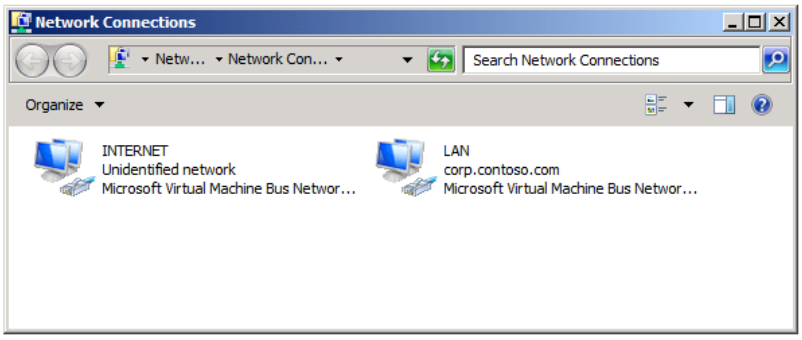
C'est la dernière ligne droite. Celle de notre serveur UAG et de sa configuration de DirectAccess. C'est la partie de cet article la plus documentée pour une raison simple : il y a beaucoup de choses à dire entre autre par rapport aux nouveautés du Service Pack 1.

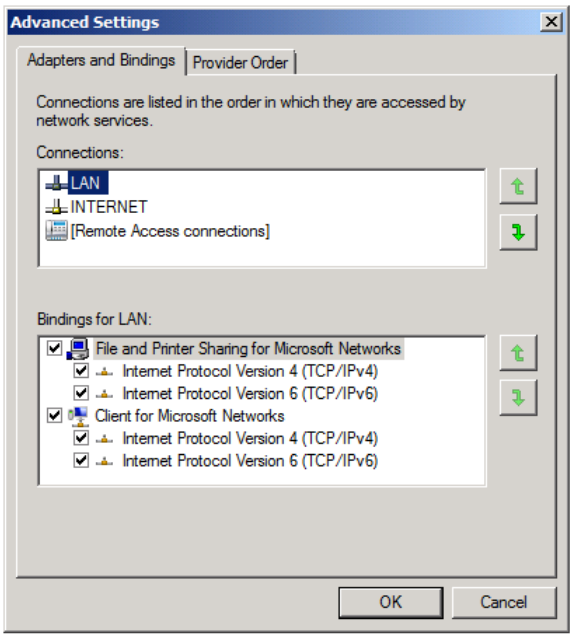
7.1 Configuration initiale du serveur

Notre serveur UAG1 dispose de deux interfaces réseau. C'est à ce niveau que vont se jouer pas mal de prérequis propres à DirectAccess. Les opérations suivantes seront réalisées :

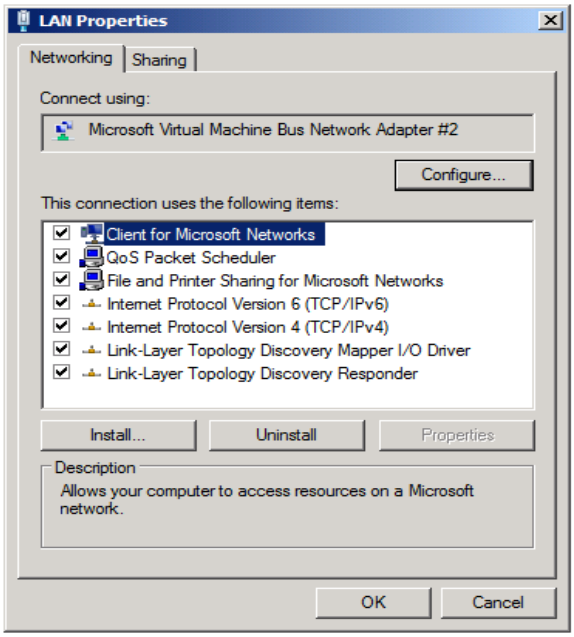
- Nommage des interfaces réseau
- Vérification de l'ordre de liaison des interfaces réseau
- Configuration de l'interface réseau LAN
- Configuration de l'interface réseau Internet
- La configuration du pare-feu
- Le déplacement du compte ordinateur

Dès lors que ces opérations auront été réalisées, il sera possible de procéder au référencement du nom DNS publique de notre serveur UAG1. Ce référencement est important car, c'est ce nom pleinement qualifié qui sera inscrit dans le certificat IP-HTTPS qui sera mis en œuvre plus tard. La recommandation est de réaliser cette demande quelques jours avant la demande de certificat afin que l'information soit bien propagée dans l'infrastructure DNS Internet.

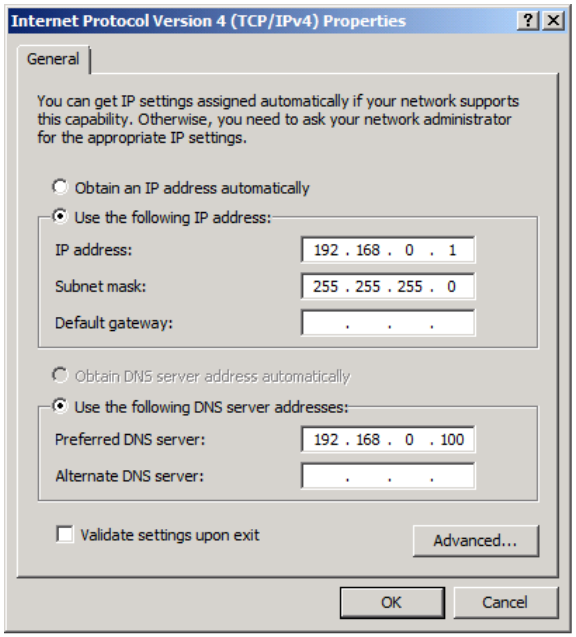
Impression écran	Description
	**Une bonne pratique pour commencer : Nommer les interfaces, c'est essentiel pour s'y retrouver plus tard.**



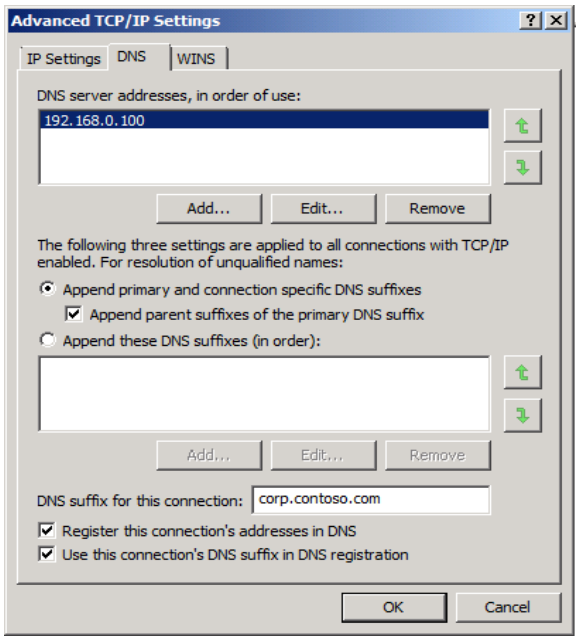
Deuxième bonne pratique, s'assurer de l'ordre de liaison des cartes réseau. La carte LAN doit être en premier car UAG (plus précisément TMG) a besoin d'accéder à sa configuration locale en passant par la carte LAN.



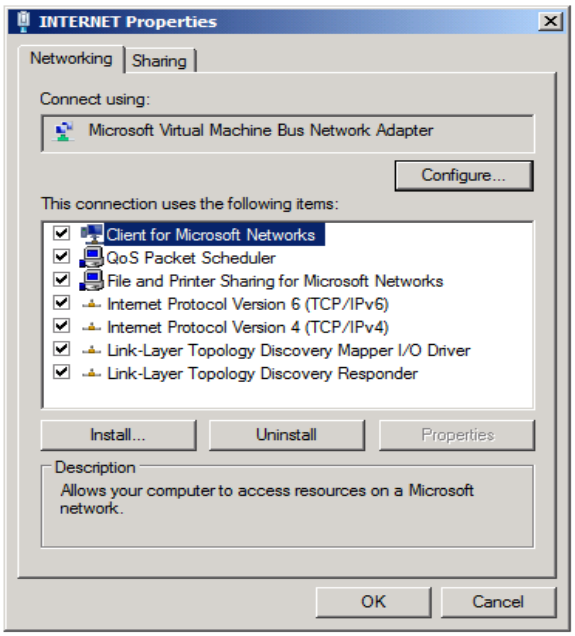
Coté Carte LAN, il est impératif de conserver IPv6.



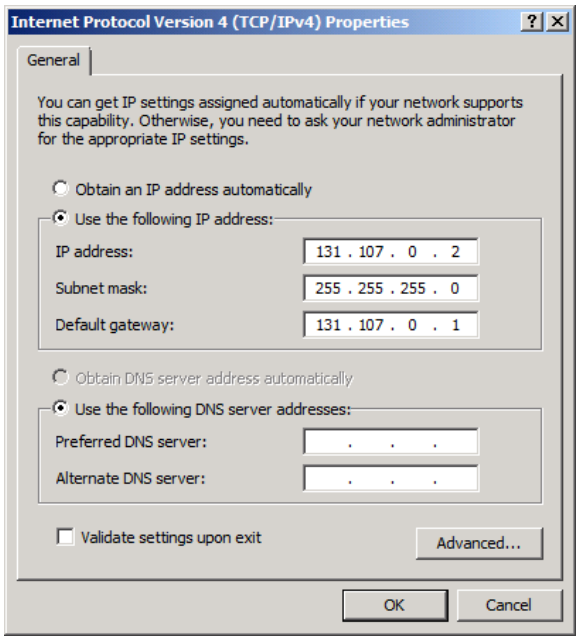
Notre carte LAN ne dispose pas de passerelle par défaut. C'est normal, la carte Internet disposera elle d'une passerelle et Windows ne sait pas traiter les passerelles sur plusieurs interfaces. Il faut passer par les routes statiques si on en a besoin.



Le référencement du suffixe DNS du domaine Active Directory sera utile pour UAG pour identifier la carte LAN sur laquelle le routage IPV6 devra être mis en œuvre.

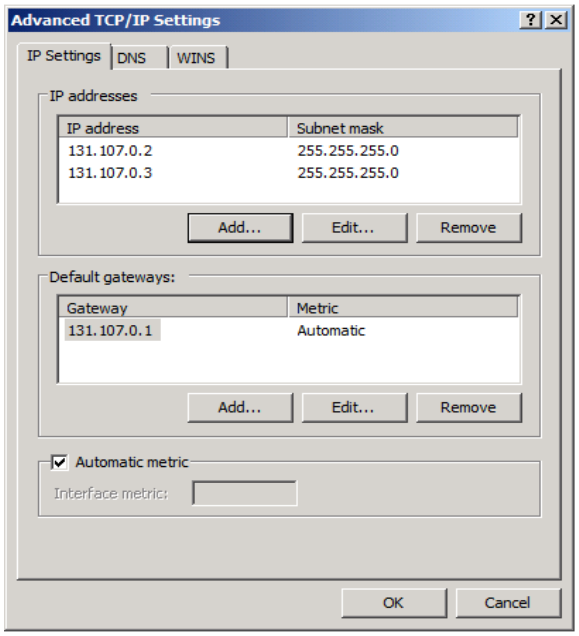


Coté Internet, même combat, on a besoin d'IPv4 et IPv6, c'est non négociable!

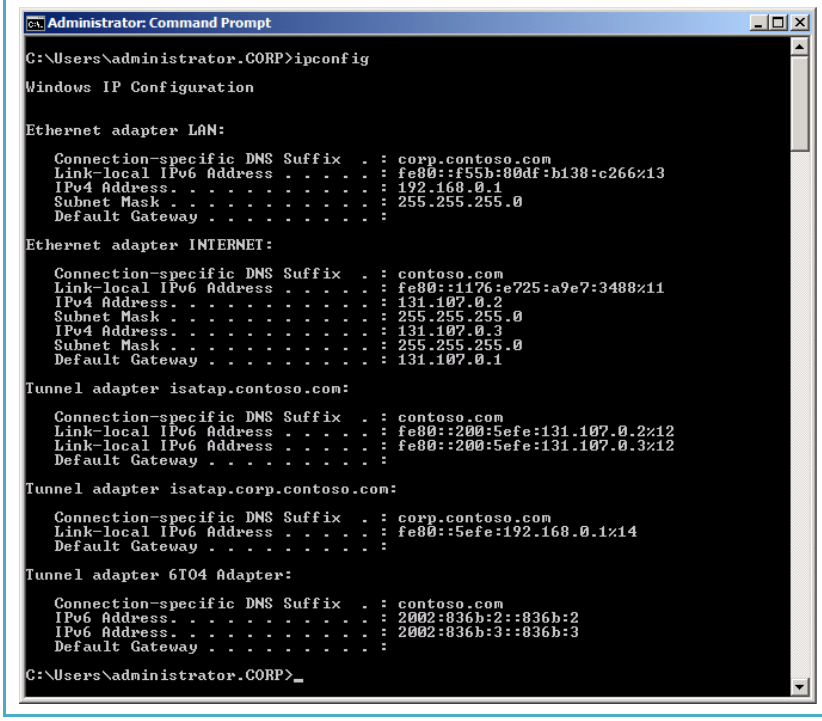


Notre interface Internet est configurée avec une passerelle par défaut. Par contre, pas de DNS à ce niveau, cela nuirait à la performance de NAT64/DNS64.

Note : Si notre serveur UAG doit pouvoir résoudre des noms sur Internet, c'est le DNS interne qui devra fournir les réponses.



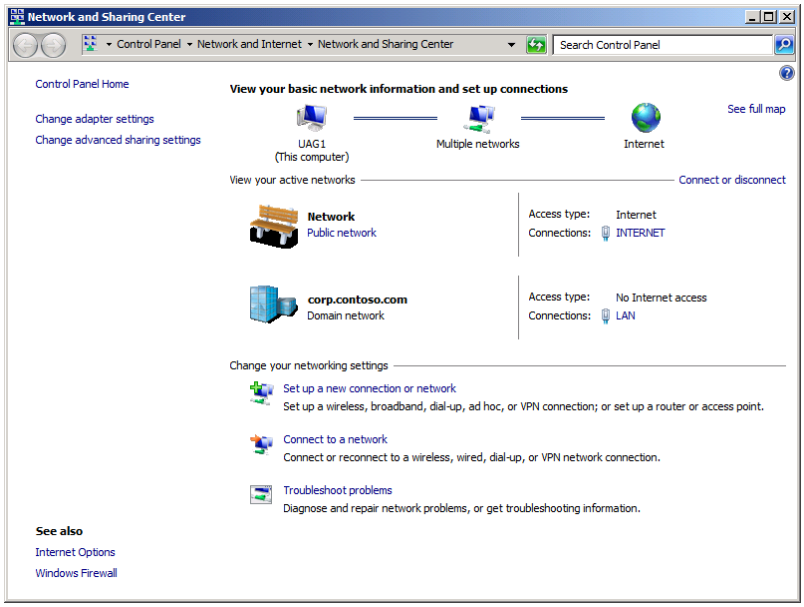
Ma carte Internet dispose bien de sa seconde adresse IPv4 publique consécutive.



Pour résumer, la configuration se présente ainsi.

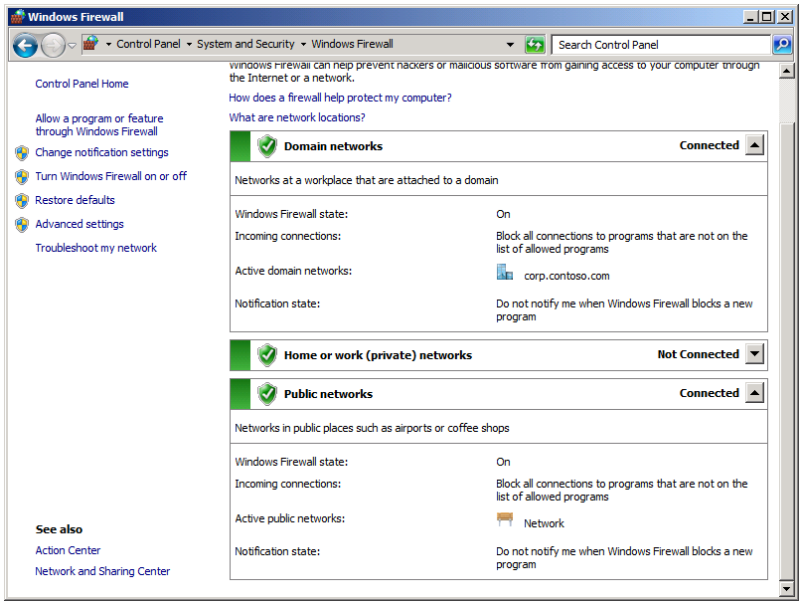
A ce stade, il existe bien des cartes réseau ISATAP mais sans configuration pour l'instant.

On constate aussi la présence d'une carte 6to4 configurée. C'est normal, le système a généré les adresses IPv6 6to4 à partir de la première adresse IPv4 publique.

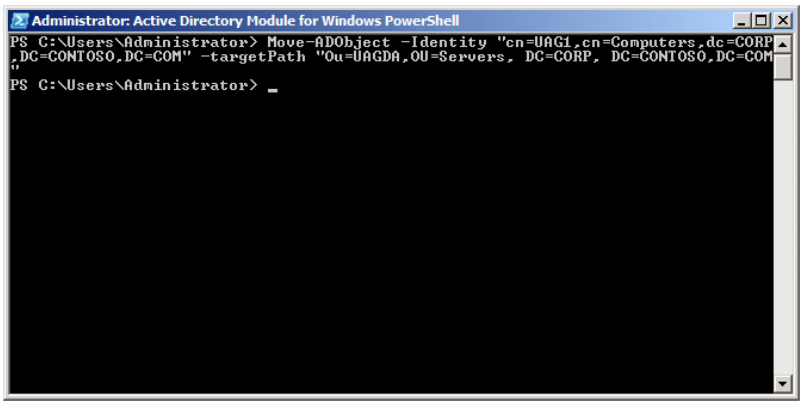


Coté connectivité, notre serveur UAG1 a bien une carte réseau connectée sur le LAN de l'entreprise et l'autre connectée à Internet.

Note : La connectivité Internet est validée car le serveur est capable de joindre le serveur www.msftncsi.com de Microsoft.



Enfin, côté pare-feu, on constate bien qu'il est actif et ce sur les deux interfaces, c'est essentiel.

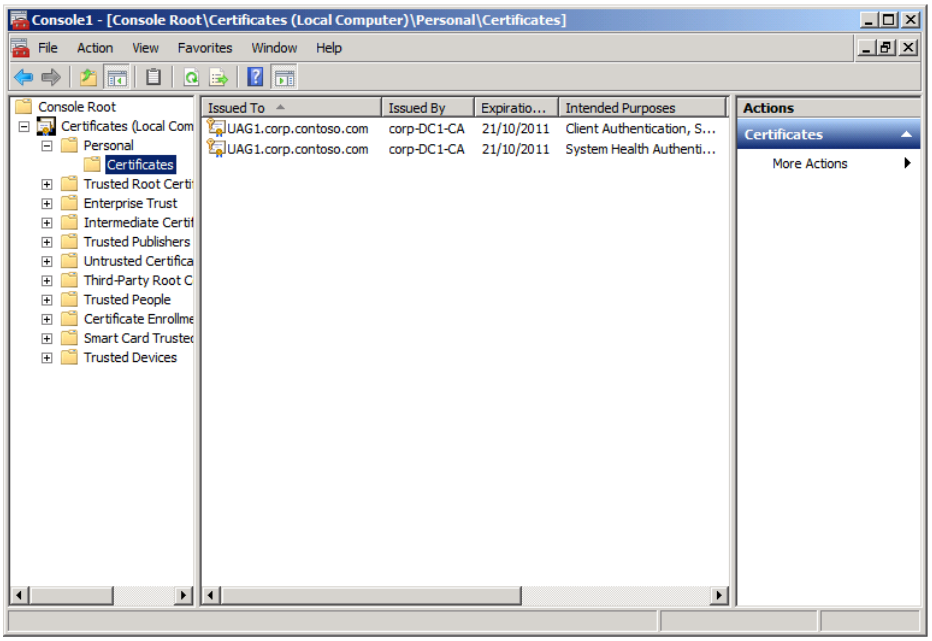


Il ne nous reste plus qu'à placer le serveur UAG1 dans le bon conteneur dans l'annuaire Active Directory, afin qu'il puisse récupérer le paramétrage qui lui sera destiné.

7.2 Certificats IPSEC et état de santé

A ce stade de la configuration, la fonctionnalité « Auto-Enrollment » de la stratégie de groupe « PKI Settings » a normalement fait son travail, à savoir la mise à disposition de certificats générés selon les gabarits suivants :

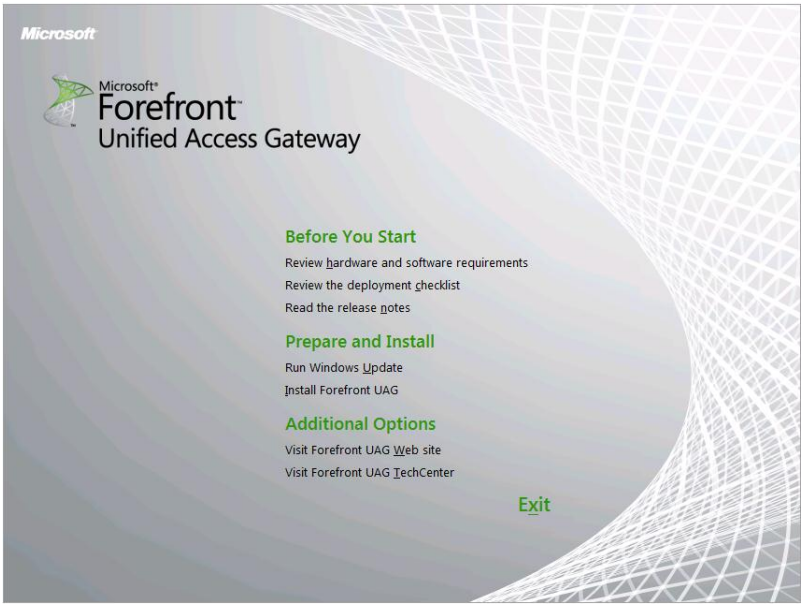
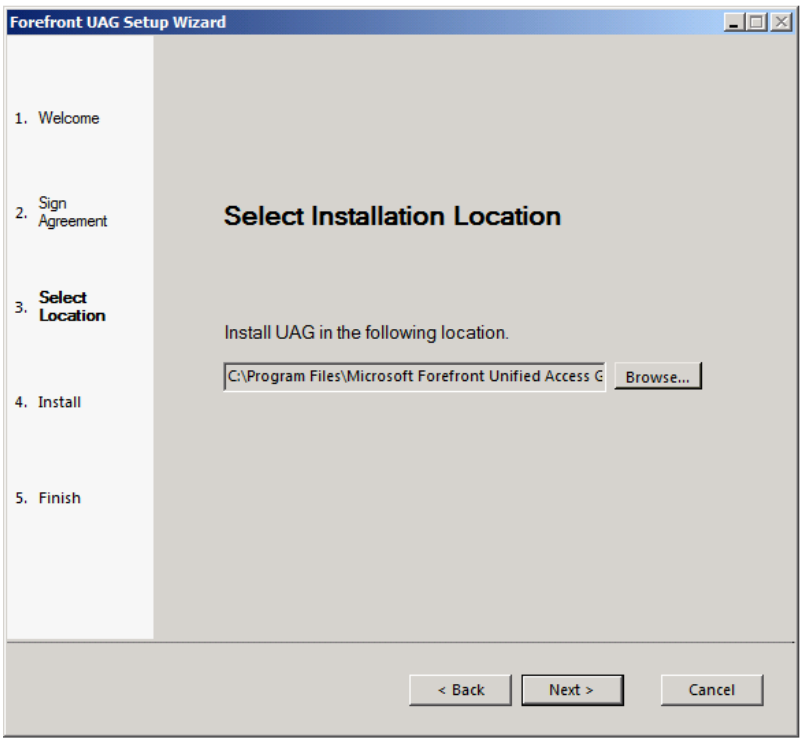
- DA certificates
- System Health Authentication

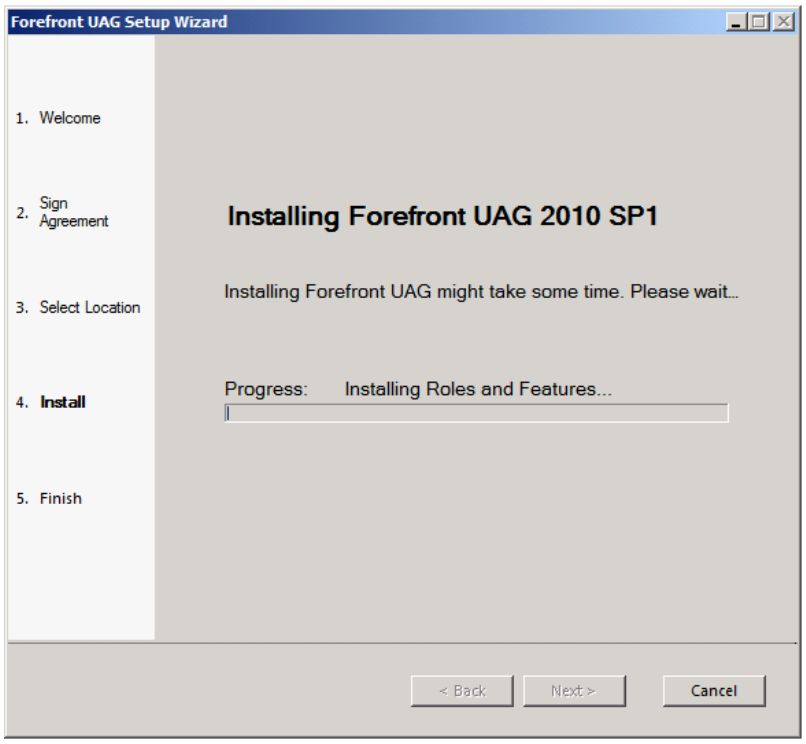


Si ces certificats ne sont pas encore présents, alors un bon « GPUPDATE.EXE /FORCE » permettra au système d'exploitation de prendre en compte la stratégie de groupe « PKI Settings ».

7.3 Installation de Microsoft ForeFront Unified Access Gateway 2010 SP1

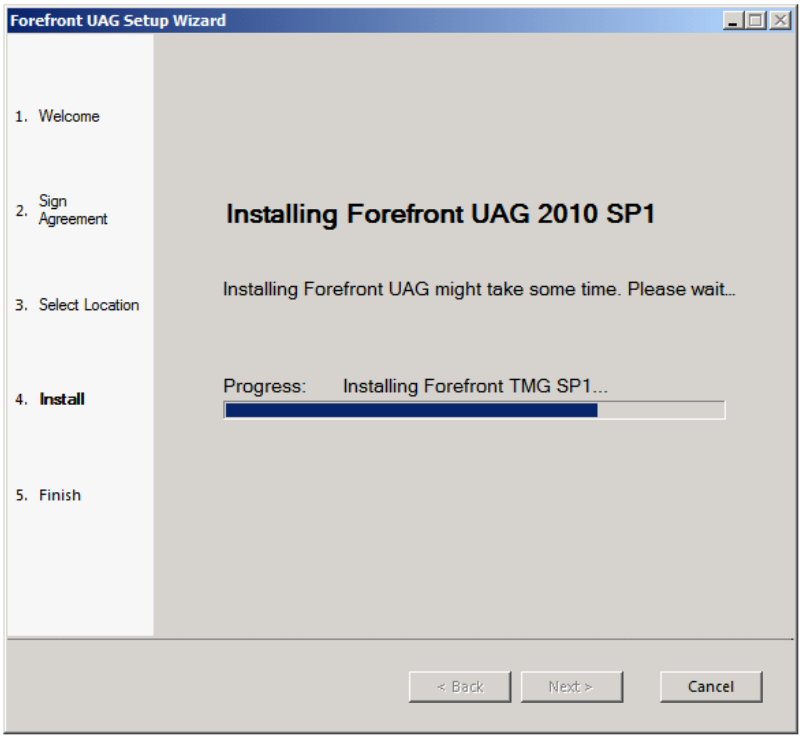
Nous y sommes enfin. A partir de maintenant, on va de focaliser sur UAG, depuis son installation, sa configuration initiale et la mise en œuvre de DirectAccess. Le plus long, c'est encore son installation. Prenez votre mal en patience, c'est très long.

Impression écran	Description
	**Avant même de commencer à installer UAG, la première chose à faire, c'est de s'assurer que notre serveur est bien à jour. Il sera connecté à Internet tout de même.**
	**Le processus d'installation en lui-même est simple, direct, sans fioriture.** **Une seule option proposée : le répertoire d'installation.**

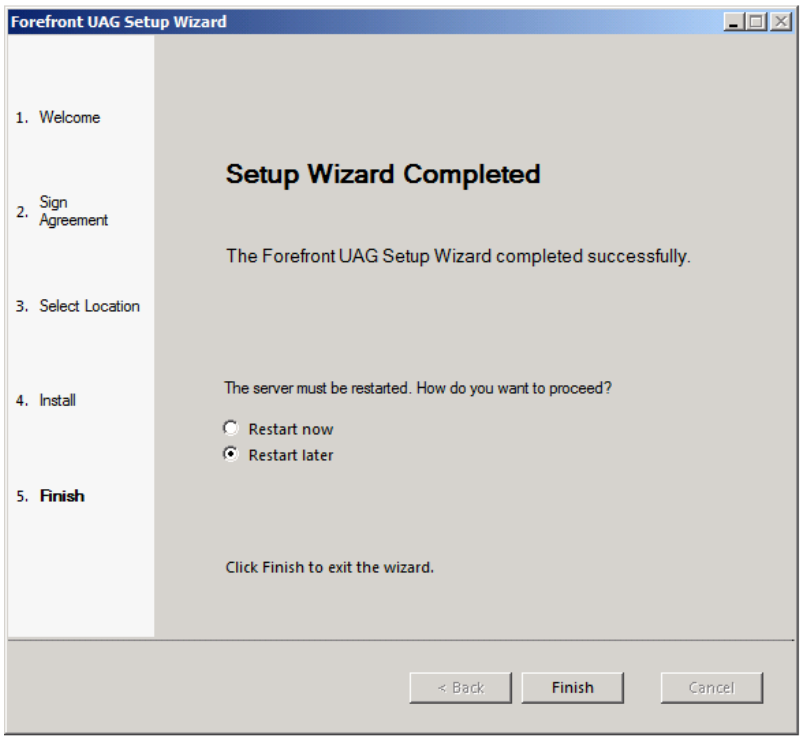


Le processus d'installation prend en charge l'installation des rôles et fonctionnalités suivants :

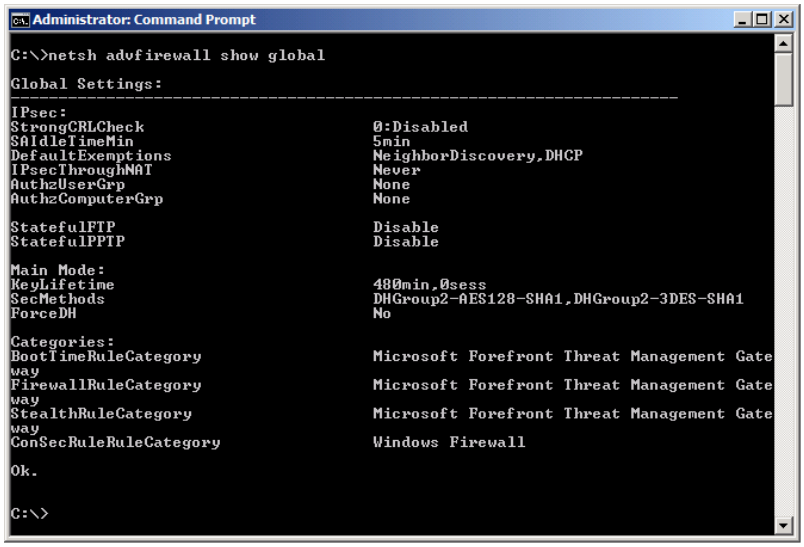
- **Network Policy Server**
- **Routing and Remote Access Services**
- **Active Directory Lightweight Directory Services Tools**
- **Message Queuing Services**
- **Web Server (IIS) Tools**
- **Network Load Balancing Tools**
- **Windows PowerShell**
- **Windows Identity Foundations (UAG 2010 SP1)**
- **Microsoft .Net Framework 3.5 SP1**
- **Windows Web Services API**
- **Windows Update**
- **Microsoft Windows Installer 4.5**
- **SQL Server Express 2005**
- **Group Policy Management Console**



L'installation d'UAG intègre bien entendu l'installation de TMG 2010, mais aussi le dernier niveau de Service Pack disponible, à savoir le premier !



Fini. A ce stade, on ne va pas encore redémarrer pour l'instant.



On va déjà mettre un point en évidence. UAG est venu se superposer au pare-feu du système d'exploitation. Pour cette raison, il est interdit de désactiver le pare-feu Windows!

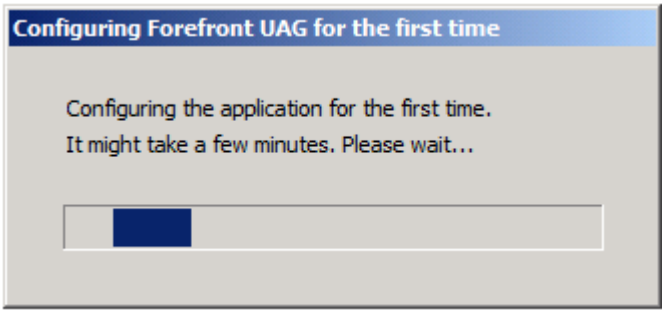
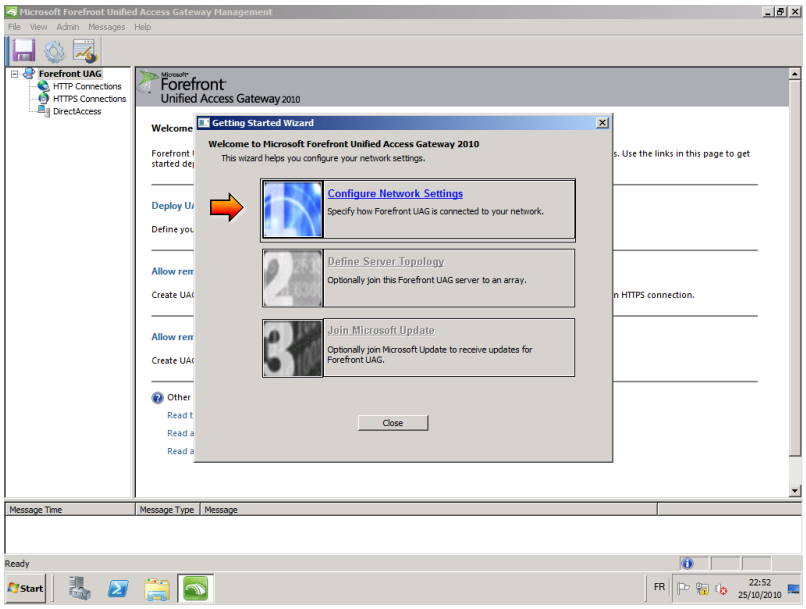
On constate aussi que la gestion des tunnels IPSEC est toujours à la charge du pare-feu du système d'exploitation.

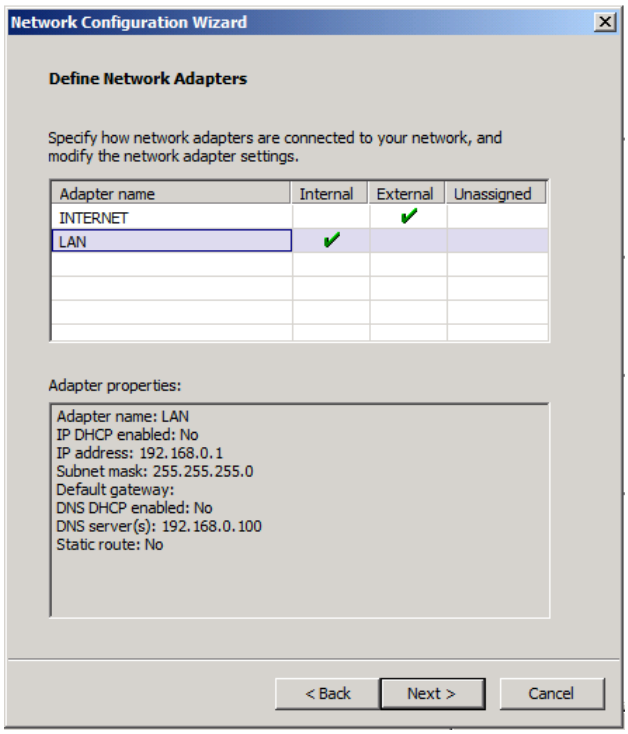
A ce stade, je recommande trois choses :

- Installer Java, c'est un prérequis pour la console « Web console » d'UAG
- Relancer Windows Update afin d'installer les correctifs correspondants aux rôles installés ainsi qu'à TMG et UAG
- Redémarrer le serveur pour intégrer toutes ces mises à jour

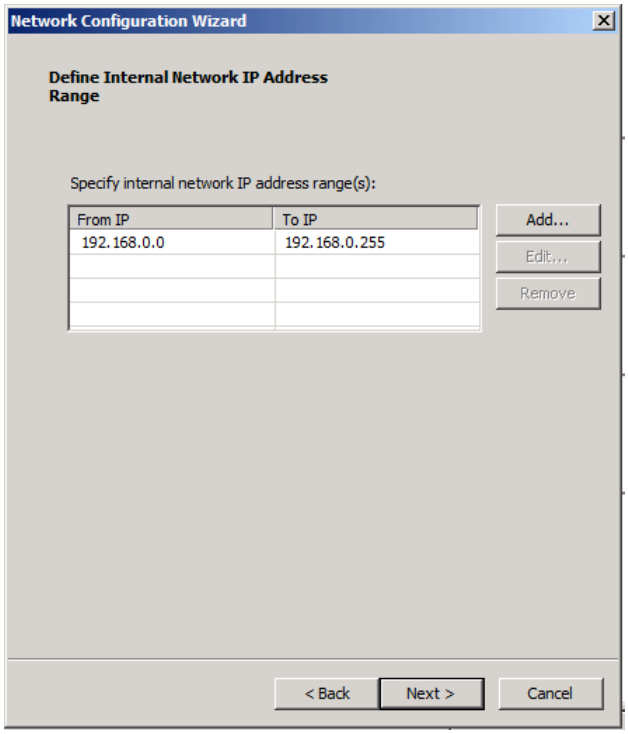
7.4 Configuration initiale d'UAG

Par défaut, un UAG sorti de sa boîte ne sait rien faire. Et pour cause, son principal composant (TMG) n'est pas encore configuré. On doit donc passer par la configuration initiale d'UAG qui est en fait quelque part celle de TMG.

Impression écran	Description
	**Toute la configuration d'UAG doit être initialisée la première fois avec la « UAG Management Console ». On va créer la configuration dans l'instance ADLDS mise en œuvre pour TMG.**
	**Première étape TMG et sa configuration réseau.**

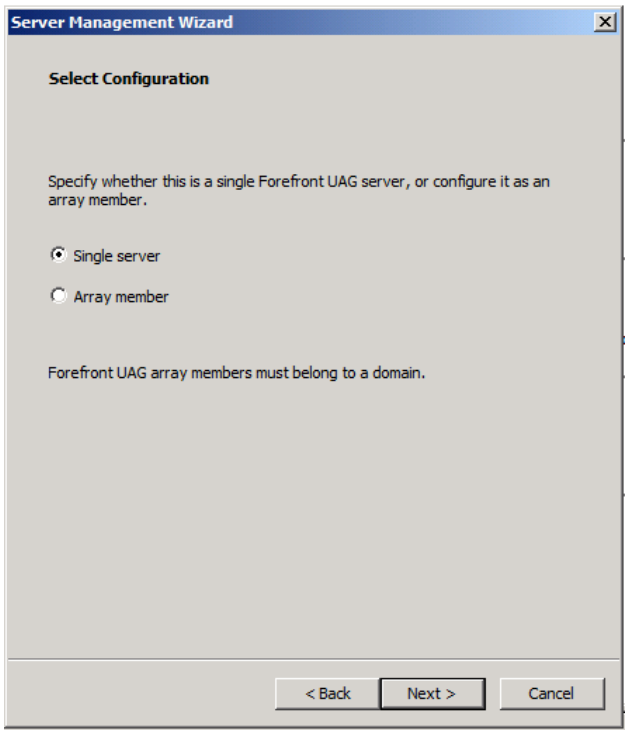


On comprend rapidement pourquoi il était intéressant de nommer les interfaces réseaux. TMG a besoin de différencier la carte LAN de la carte Internet.



Coté TMG, il a besoin d'identifier plus précisément les sous-réseaux internes de l'entreprise. Bien entendu, ceux-ci respectent la RFC 1918, …

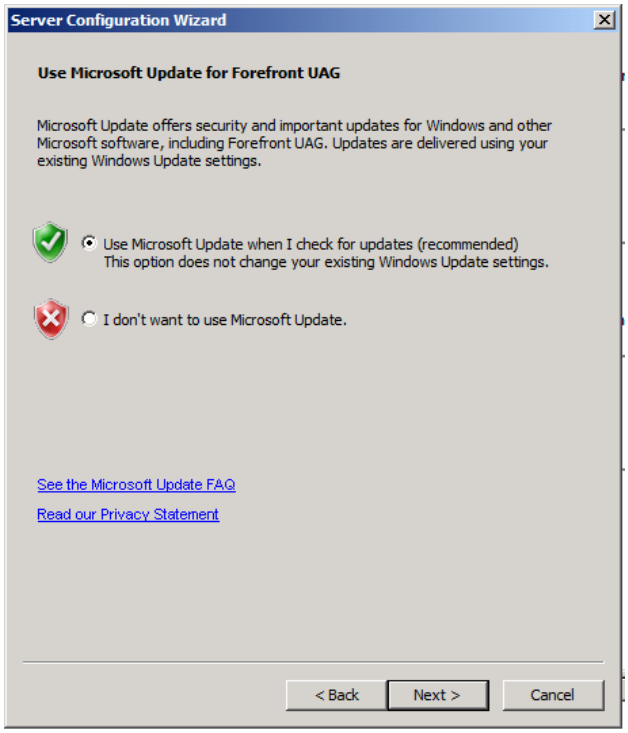
Autre possibilité, cette plage d'adresse IPv4 publique appartient à l'entreprise.



Second étage UAG. Il existe deux modes d'installation :

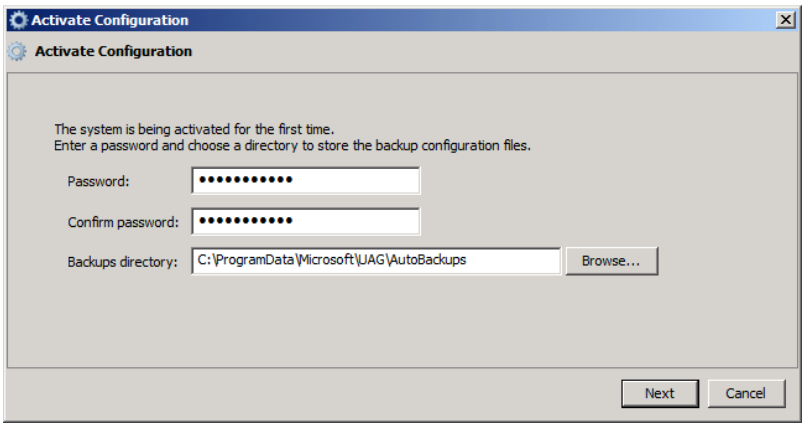
- **Standalone**
- **Ferme de serveurs (jusqu'à 8)**

Dans le cas qui nous occupe, nous partons sur un déploiement « Standalone ».

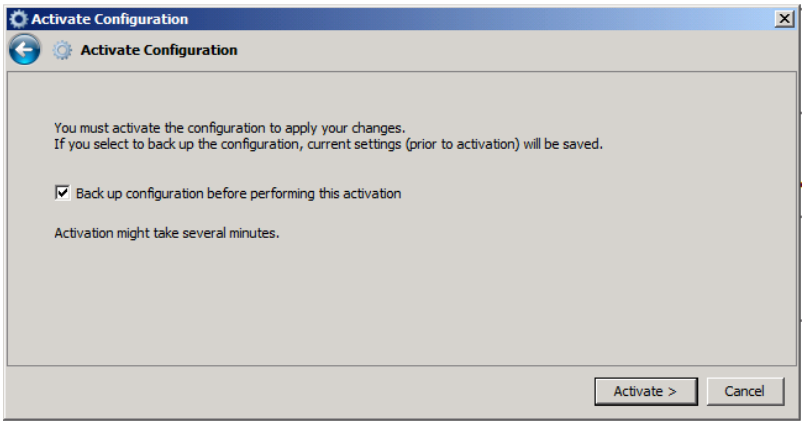


Enfin dernière étape avec la configuration de Windows Update pour TMG et UAG.

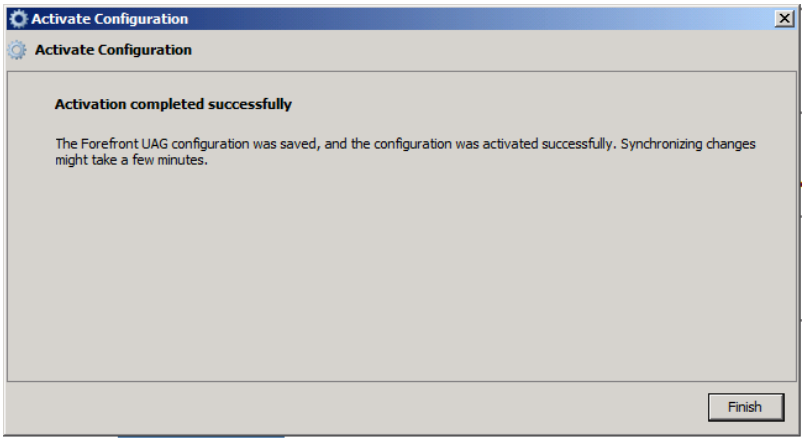
Note : Pensez à activer les catégories de TMG et UAG sur votre serveur WSUS interne.



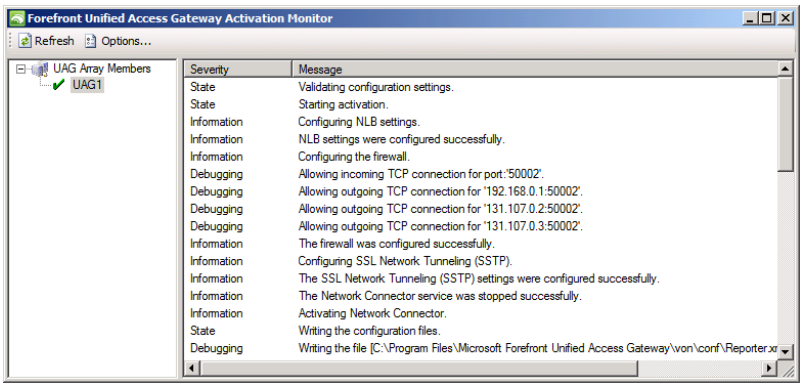
Il ne nous reste plus qu'à activer cette première configuration. Pour cela, il est nécessaire de définir un emplacement pour le stockage des configurations sauvegardées ainsi que du mot de passe qui va avec.



Par sécurité, on effectue toujours une sauvegarde la configuration précédente avant d'en active une nouvelle. C'est le seul moyen rapide de revenir en arrière.



La configuration est active oui, mais pas encore propagée.



Pour s'en assurer, le meilleur moyen reste encore de consulter le statut dans la console « Activation Monitor ».

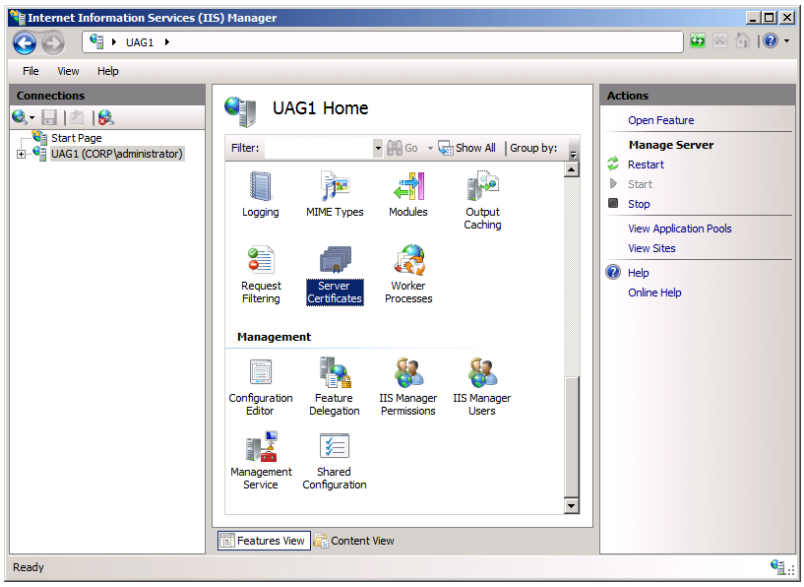
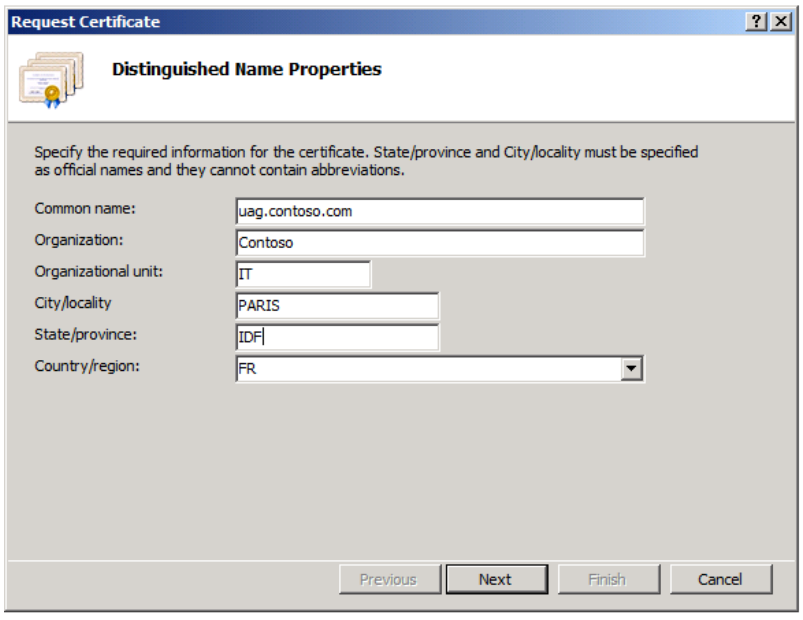
Attention, ce n'est pas immédiat.

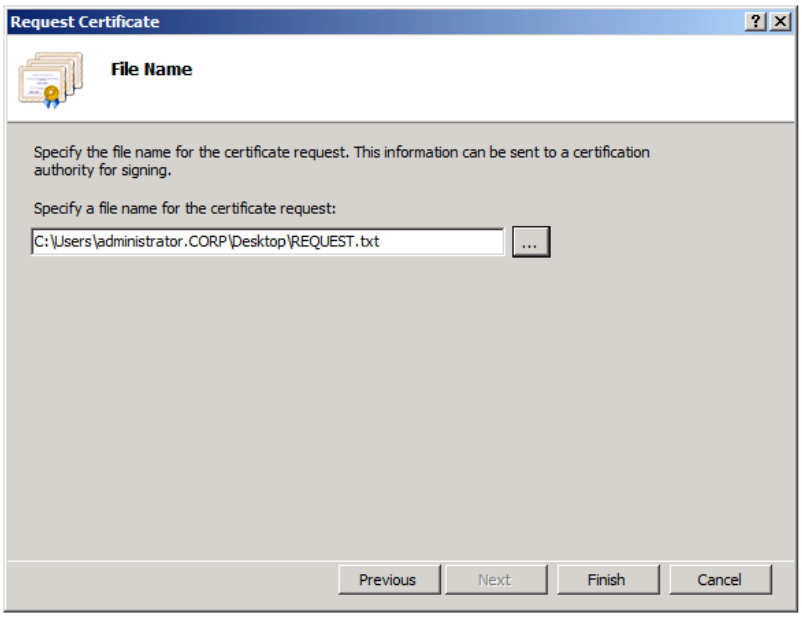
7.5 Certificat IP-HTTPS

La configuration DirectAccess de notre serveur UAG1 ne pourra s'effectuer sans disposer au préalable d'un certificat SSL pour authentifier le serveur UAG pour les accès en IP-HTTPS (encapsulation des tunnels IPSEC dans des trames HTTPS). Pour rappel, IP-HTTPS sera utilisé si :

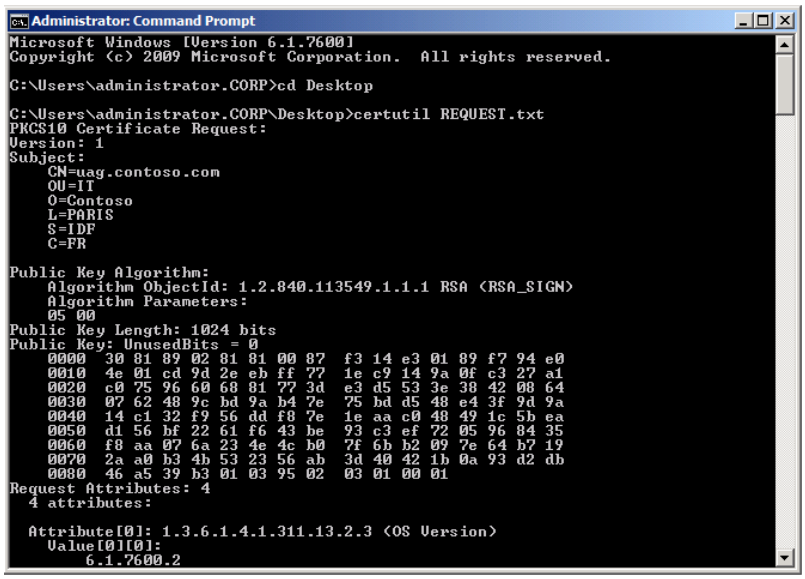
- Le client détermine qu'il est sur un réseau privé et est incapable d'utiliser Teredo
- Ou le client est configuré pour opérer en « Force Tunneling »
- Ou le client a été configuré pour ne fonctionner qu'avec IP-HTTPS

Etant donné que ce simple certificat web devra authentifier notre serveur UAG sur Internet, il est important d'avoir préalablement enregistré ce nom DNS dans la zone DNS dont on est propriétaire. Dans le cas fictif qui nous occupe, ce sera « UAG.CONTOSO.COM ».

Impression écran	Description
	**Étant donné qu'UAG a eu la gentillesse de nous installer la console IIS, on va donc l'utiliser pour l'ensemble de l'opération.**
	**La demande de certificat doit être dument remplie.**

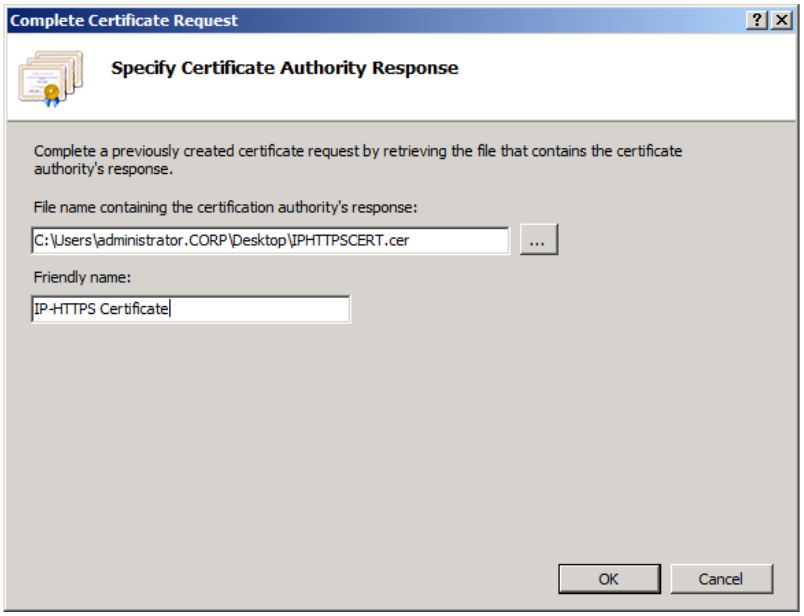


Il faut soumettre notre fichier de demande déjà codé.



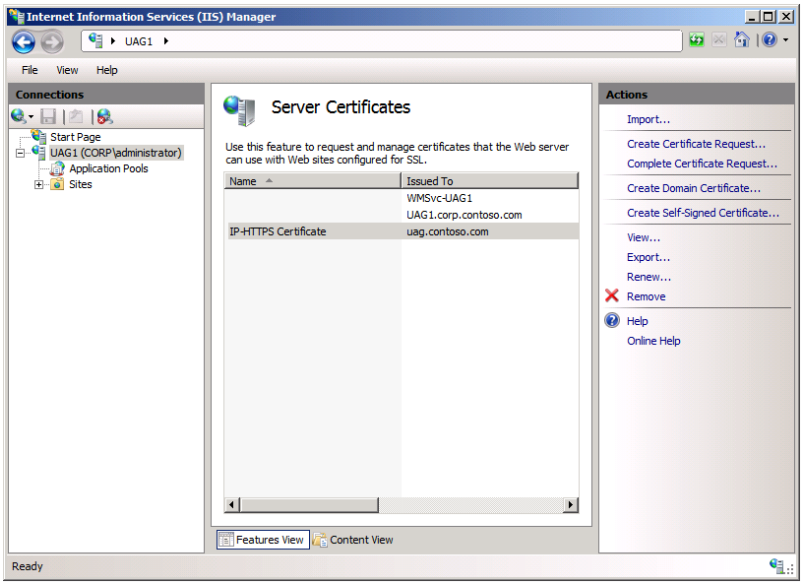
Par soucis de vérification (ca se paie un certificat public), je recommande toujours le « CERTUTIL.EXE » pour relire le contenu du fichier de demande.

C'est l'heure de sortir la carte bleue pour payer le certificat.



Dès lors qu'on a reçu notre certificat, il ne reste plus qu'à le positionner dans le magasin ordinateur pour un usage ultérieur.

Note : Je recommande vivement de nommer le certificat importé pour pouvoir le différencier des autres déjà présents dans le magasin personnel de l'ordinateur.



Notre certificat est bien présent dans le magasin Computer. Son « Friendly Name » nous permet de clairement l'identifier.

Nous sommes maintenant prêts à nous attaquer à DirectAccess. Il était important de bien poser les fondations. L'assistant de configuration d'UAG va assembler toutes nos briques pour mettre en œuvre DirectAccess. C'est l'heure de la magie!