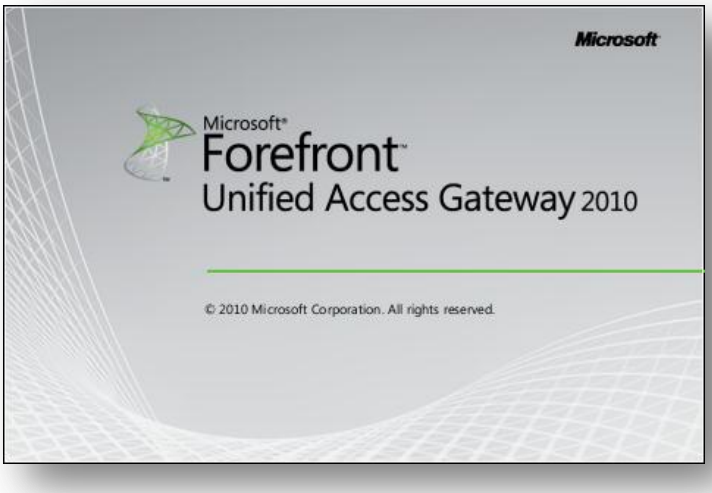
Microsoft Forefront UAG 2010 SP1

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

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

8 CONFIGURATION DE DIRECTACCESS

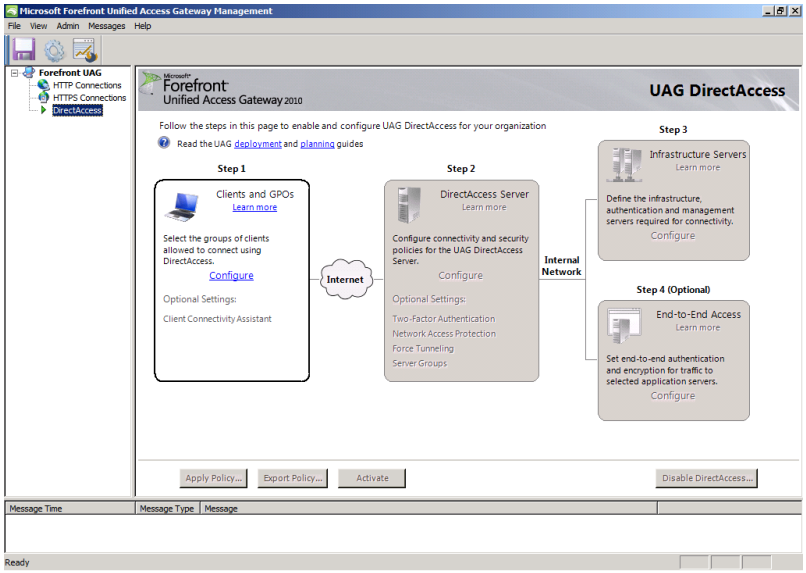
Passons maintenant au plat de résistance avec la configuration de DirectAccess. Tout se passera dans l'interface de configuration d'UAG avec une collection d'interfaces de configuration. Pour éviter de se poser des questions en cours de route, le tableau suivant résume les choix de déploiement qui seront mis en œuvre :

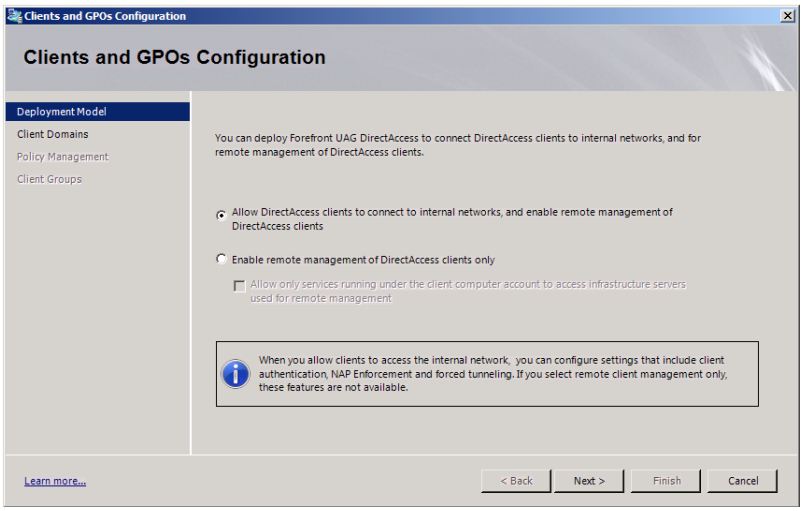
Configuration à mettre en œuvre	Valeur
Scénario de déploiement	**Autoriser les clients DirectAccess à se connecter au réseau interne et activer la gestion à distance des clients DirectAccess.**
Localisation des clients	**Dans le domaine corp.contoso.com**
Liaison des stratégies de groupe	**A la racine du domaine**
Identification des clients DirectAccess	**Dans le conteneur « Workstations » localisé à la racine du domaine**
Configuration du DirectAccess Connectivity Wizard	**Oui**
Autoriser les clients à utiliser la résolution de noms DNS locale	**Oui**
Indicateur de connectivité du DAC	**http://app1.corp.contoso.com**
Portail à présenter à l'utilisateur en cas de défaillance DirectAccess	**http://www.contoso.com/troubleshooting**
Nom du portail	**Portail d'assistance**
Adresse de messagerie du support	**Administrateur@contoso.com**
Première adresse IPv4 publique	**131.107.0.2**
Adresse IPv4 privée	**192.168.0.1**
Identification du certificat IP-HTTPS	**Friendly name « IP-HTTPS »**
Autorité de certification interne	**DC1.CORP.CONTOSO.COM**
Authentification double facteur	**Non**
Prise en charge de NAP avec DirectAccess	**Oui**
Mode de mise en œuvre de NAP	**Monitoring mode**
Localisation du serveur HRA	**Sur le serveur UAG**
URL de dépannage NAP	**http://www.contoso.com/troubleshooting.htm**
Autorité de certification délivrant les certificats System « Health Authentication »	**DC1.CORP.CONTOSO.COM\CORP-DC1-CA.**
Gabarit de certificats pour NAP	**System Health Authentication**

Gestion des flux en partance du poste client	**Split Tunneling**
Localisation des serveurs UAG	**Servers\UAGDA**
Network Location Server	**https://nls.corp.contoso.com**
Méthode de résolution des noms locaux	**Fallback to local name resolution**
Mode d'accès au réseau interne	**End-to-Edge**

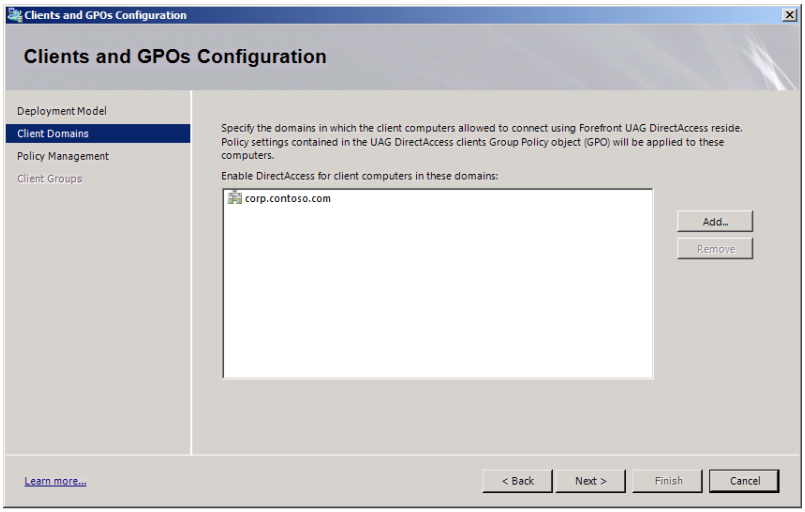
8.1 Paramétrage coté client de DirectAccess

La première étape de la configuration, c'est l'identification des clients pour lesquels DirectAccess devra être activé, le niveau d'accès de ces clients au système d'information et enfin la configuration optionnelle du DAC. Le DirectAccess Security Configuration Wizard est une interface utilisateur permettant à celui-ci d'être informé de l'état de fonctionnement de DirectAccess. C'est la partie la plus simple de la configuration de DirectAccess.

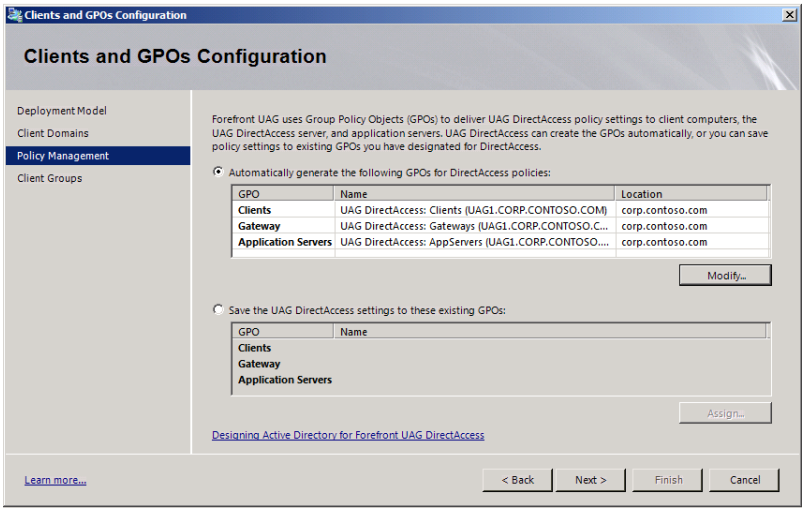
Impression écran	Description
	**L'interface de configuration ne permet de passer à l'étape suivante que si la configuration minimale a bien été renseignée.** **On distinguera des paramètres obligatoires et optionnels.**



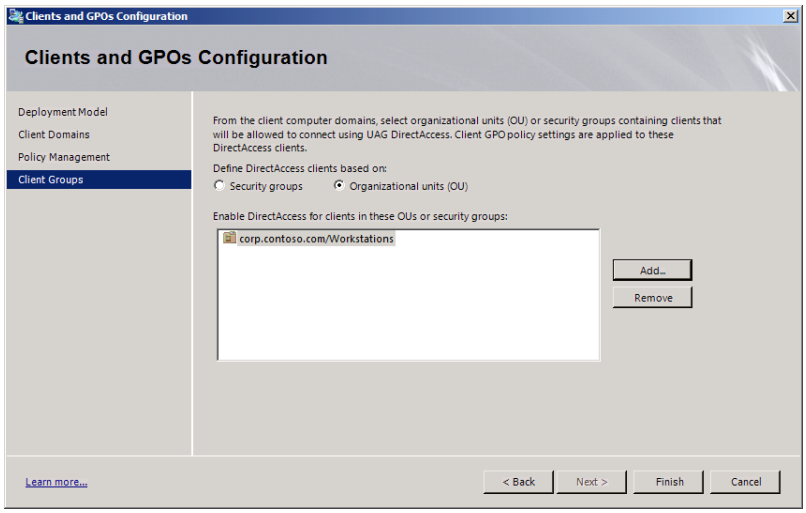
On va conserver la configuration par défaut. Par rapport à la RTM d'UAG, il y a tout de même subtilité. Il n'est plus besoin de configurer la gestion des clients en situation de mobilité. Les exceptions de pare-feu sont déjà intégrées.



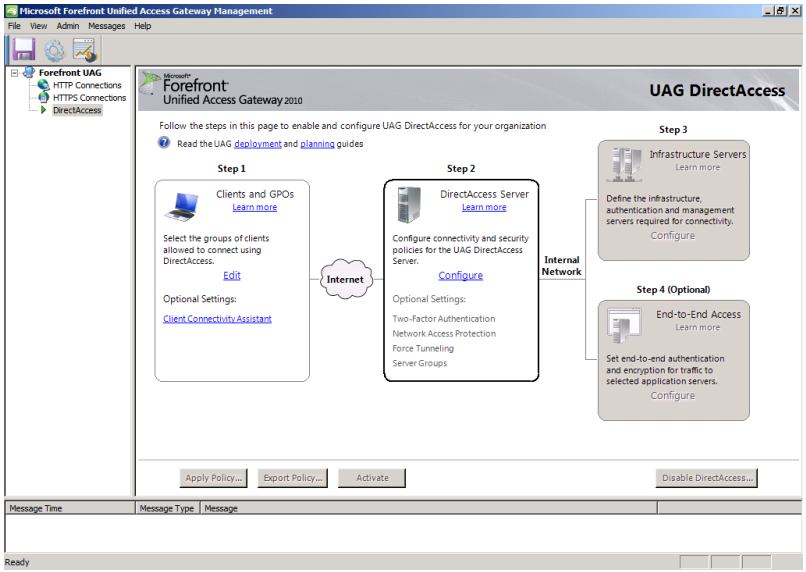
Par défaut, UAG va positionner la stratégie de groupe de configuration des postes clients dans un seul domaine. Il est donc possible de déployer UAG/DirectAccess dans un scénario de forêt de ressources.



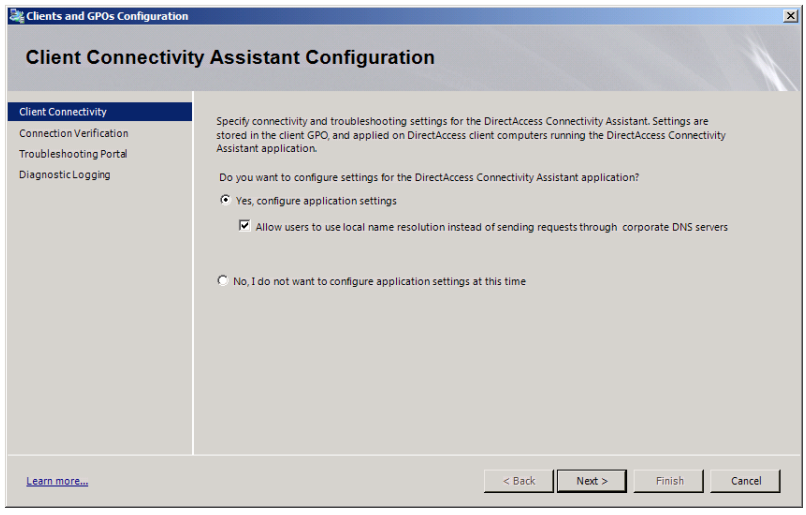
Dans la version RTM d'UAG, on n'avait pas la possibilité de configurer la liaison des stratégies de groupe. Ici encore, il sera possible de positionner le serveur UAG et les serveurs de ressources dans des forêts distinctes.



Dans la version RTM, le filtrage s'effectuait uniquement par rapport à l'appartenance à un groupe. Avec le SP1, on peut maintenant filtrer par rapport à un conteneur organisationnel.

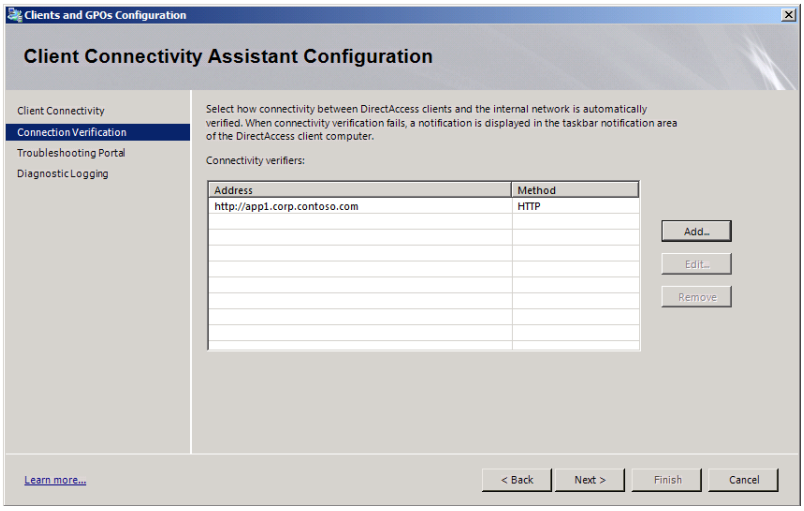


On en a fini avec la configuration obligatoire coté client, passons maintenant aux paramétrages optionnels.



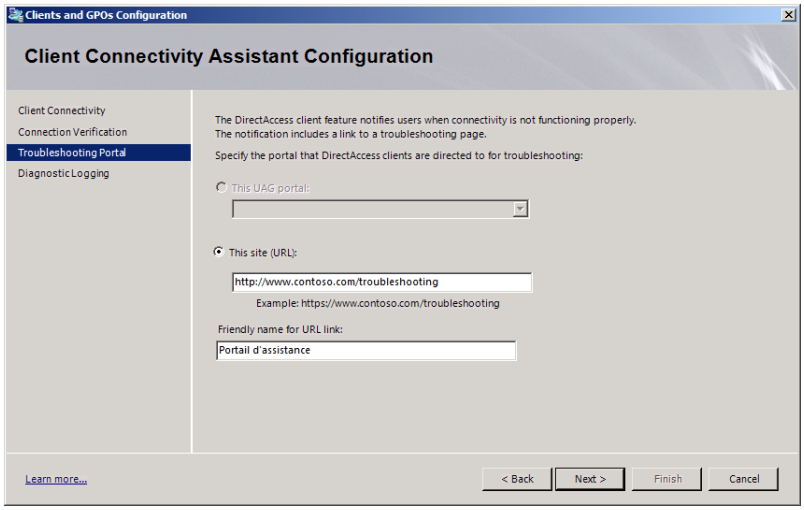
On va configurer le DirectAccess Connectivity Wizard et autoriser l'utilisateur à basculer en résolution de noms locale. L'utilisateur pourra ainsi désactiver DirectAccess si nécessaire.

La version 1.5 du client est diponible dans « c:\Program Files\ Microsoft ForeFront Unified Access Gateway\Common\Bin\Da\DAC ».



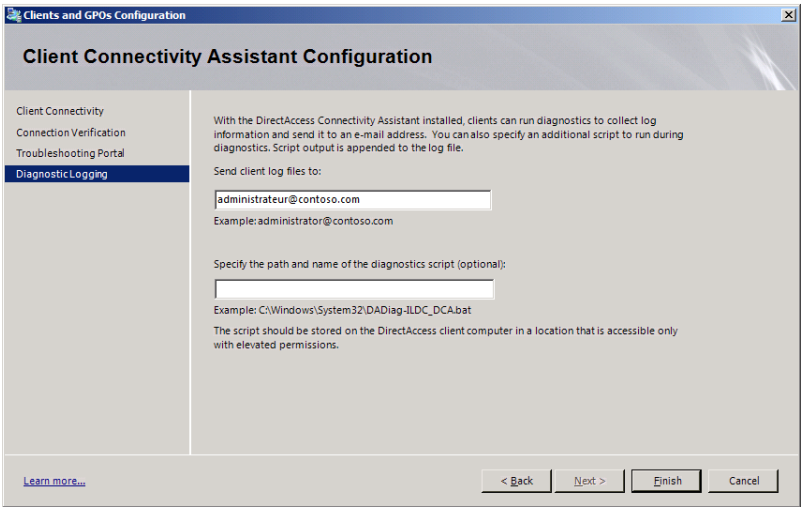
Le DAC doit être configuré pour utiliser une référence interne. Dans notre cas, j'ai retenu le site web par défaut hébergé sur le serveur APP1.

En environnement de production, je recommanderai de choisir un autre point de référence, voire même d'en référencer plusieurs.



En cas d'indisponibilité, le DAC va informer l'utilisateur et le rediriger vers un portail.

Si on a préalablement configuré le portail UAG, il est même possible de le référencer.



En cas de défaillance, l'utilisateur peut générer des traces que l'on va envoyer par messagerie à l'équipe de support.

Il est même possible d'utiliser un script de diagnostic personnalisé.

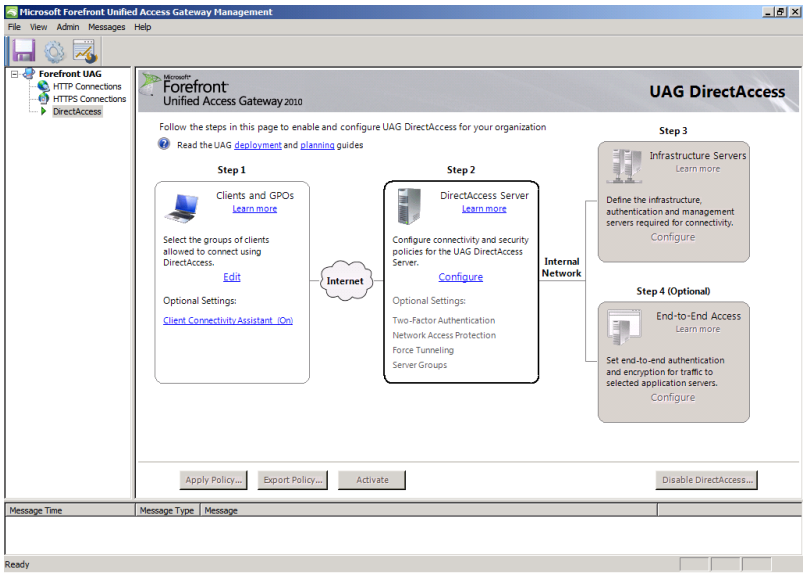
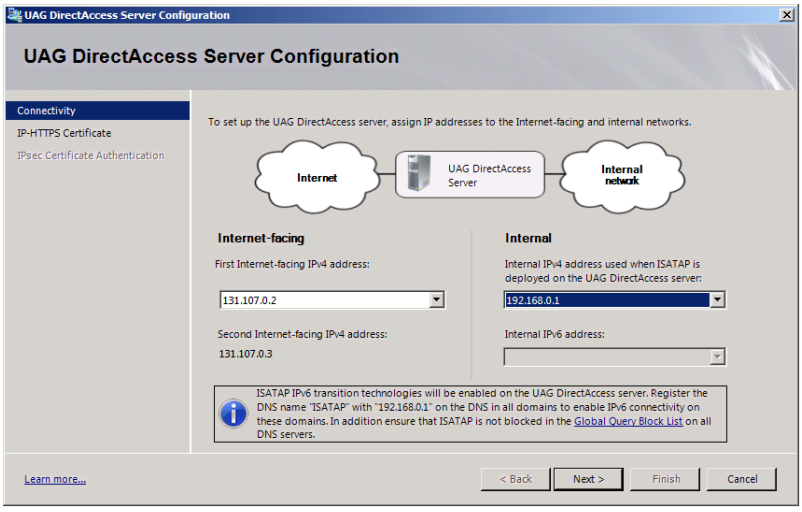
8.2 Paramétrage coté serveur de DirectAccess

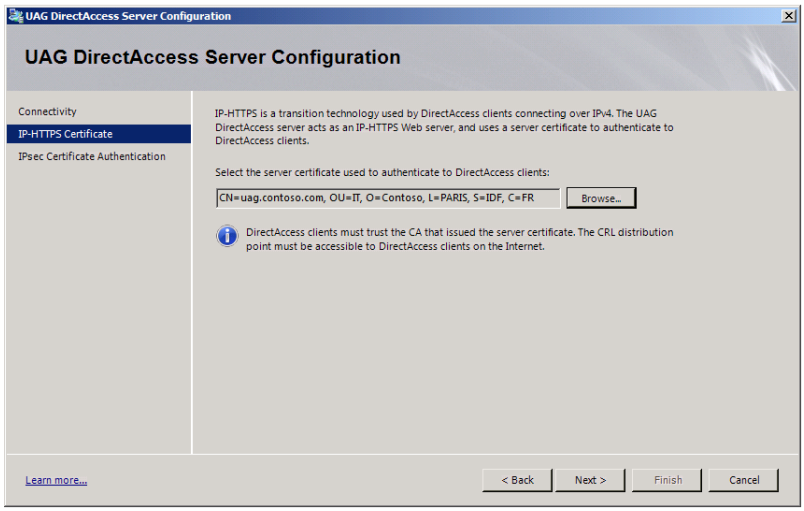
Deuxième étape, la configuration de DirectAccess à proprement parlé. A ce stade, on va :

- Indiquer à UAG quelle est l'interface interne
- Indiquer à UAG quelle est l'interface externe (avec ses deux adresses IPv4 publiques consécutives)
- Spécifier le certificat qui sera utilisé pour le protocole de transition IP-HTTPS
- Spécifier l'autorité de certification qui sera utilisée pour authentifier les tunnels IPSEC

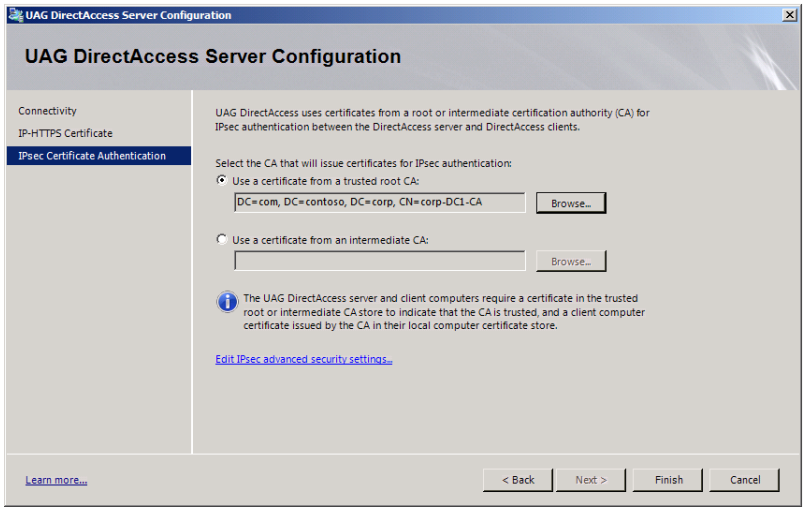
En option, on va pouvoir :

- Spécifier l'usage de la carte à puce ou d'un dispositif OTP au niveau des tunnels IPSEC
- Intégrer la prise en charge de Network Access Protection au sein de DirectAccess
- Spécifier le mode de gestion des flux sortants au niveau du client DirectAccess
- Spécifier la localisation des serveurs UAG DirectAccess

Impression d'écran	Description
	**La configuration du client est maintenant terminée. Passons à la configuration du serveur.**
	**A ce stade, pas de changement, il faut indiquer à UAG quelle est l'interface interne et l'interface externe.** **A noter que comme pour la RTM, l'interface refusera de poursuivre si les prérequis ne sont pas respectés.**

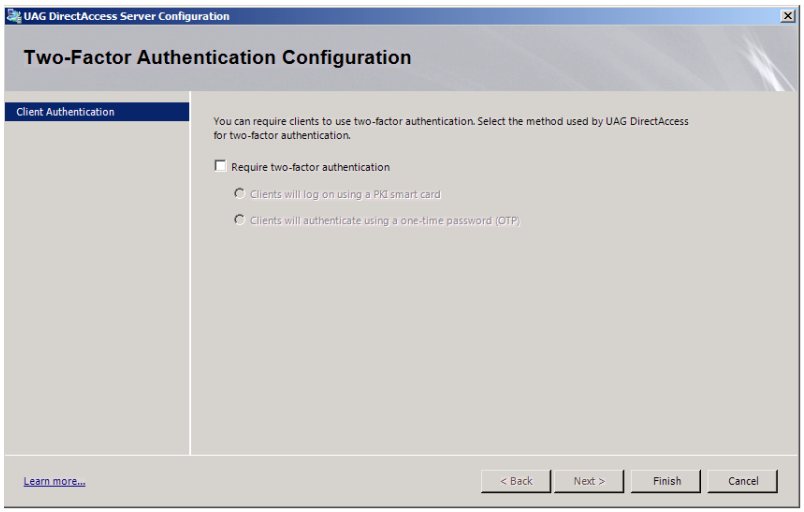


La sélection du certificat IP-HTTPS a été isolée. Pour rappel, on avait utilisé un « Friendly name ». Il sera utile pour sélectionner le bon certificat.

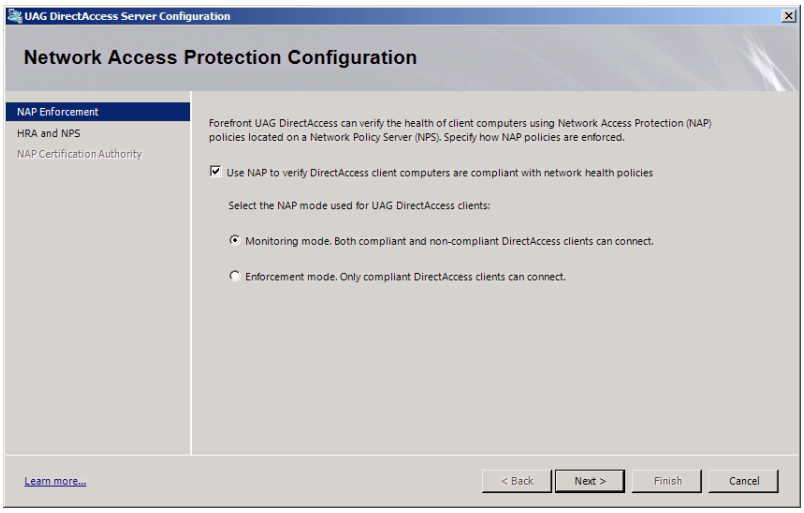


Coté autorité de certification, on va sélectionner celle que nous avons installé. C'est elle qui va distribuer les certificats d'authentification IPSEC.

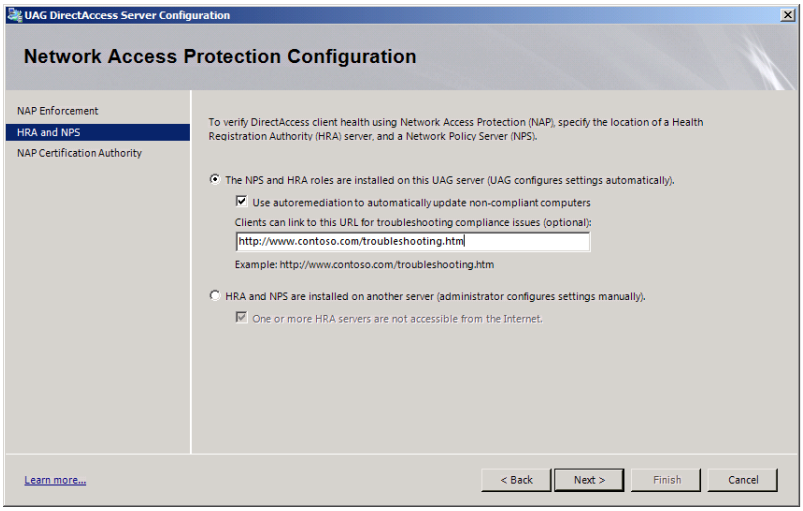
Voilà pour le paramétrage obligatoire, passons aux paramètres optionnels.



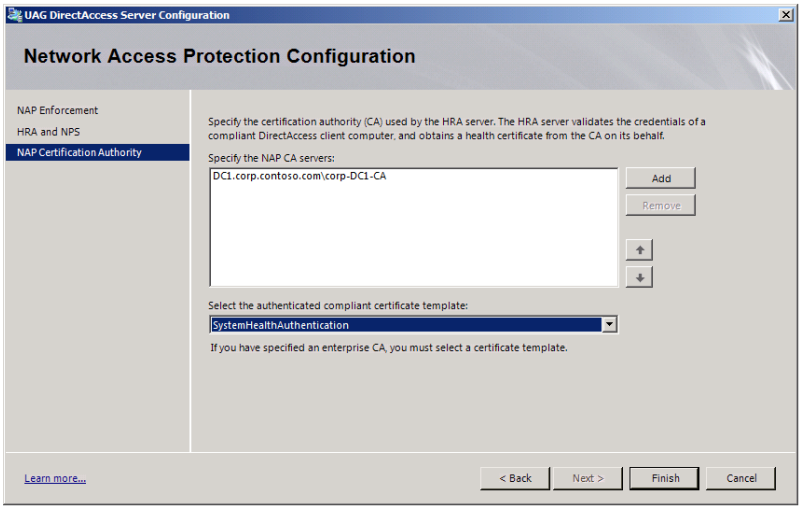
Une grande nouveauté d'UAG 2010 SP1, la prise en charge de l'authentification double facteur au niveau de l'établissement des tunnels IPSEC. Il est aussi possible de réaliser l'authentification avec une carte à puce ou un device de type OTP.



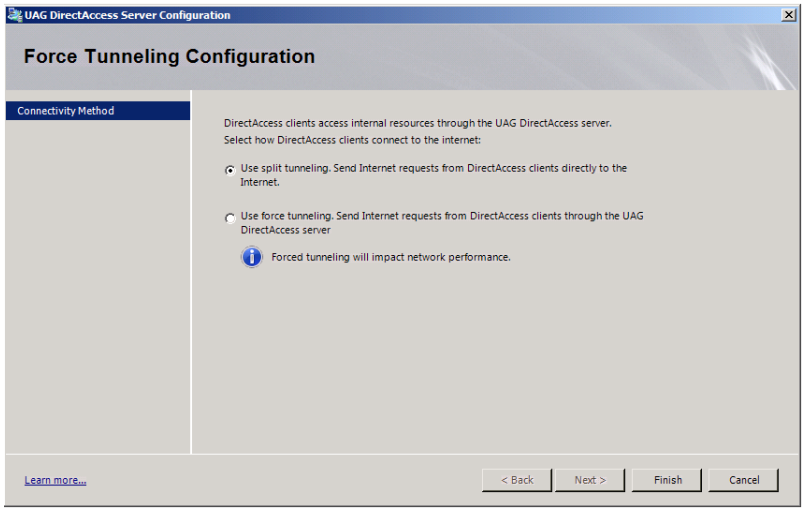
NAP était déjà intégré à la configuration de DirectAccess sauf qu'il fallait intervenir sur la stratégie de groupe coté serveur pour configurer le mode de NAP. Dans notre maquette, nous allons commencer par le mode « Monitoring ».



Dans la version RTM d'UAG, il n'était pas possible d'héberger le rôle « Health Registration Authority » sur le serveur UAG. C'est maintenant possible avec le SP1. En plus, il le configure pour nous !

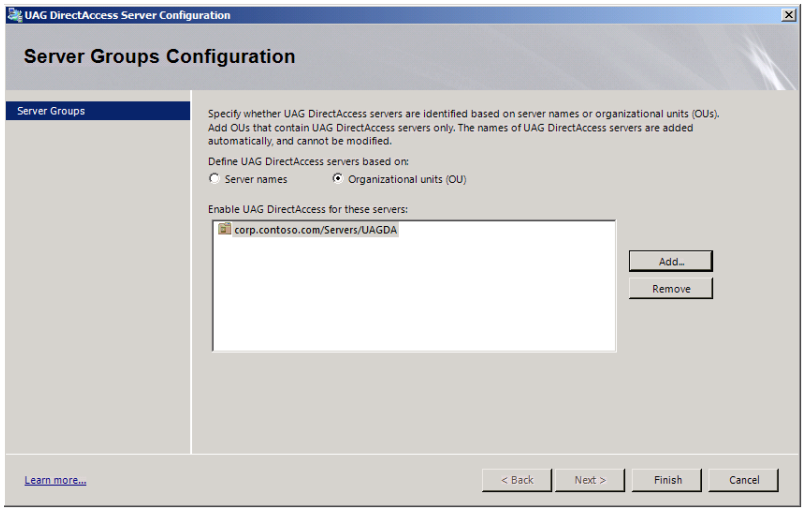


La configuration de NAP implique de désigner l'autorité de certification qui va délivrer les certificats de type System Health Authentication.



UAG RTM ne permettait pas de configurer l'encapsulation ou non des flux en partance du client. Dans notre cas, nous allons conserver le mode par défaut.

Note : Le mode « Force Tunneling » intègre des nouveautés dans le SP1 d'UAG 2010 par rapport à la version RTM.



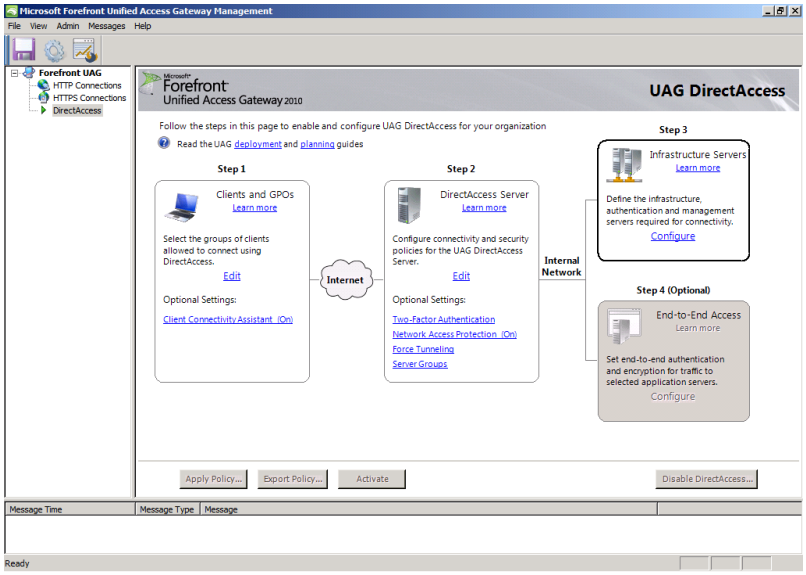
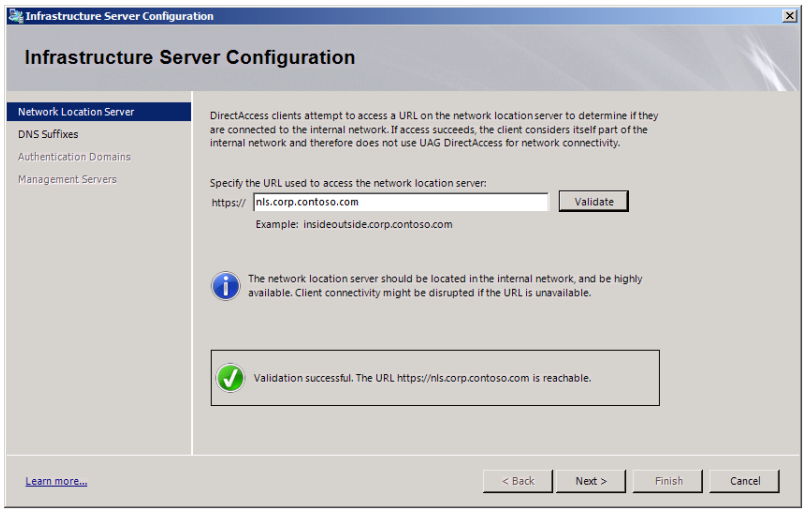
Tout comme pour les clients, il est possible de filtrer l'application de la stratégie de groupe concernant le ou les serveurs UAG à un conteneur Active Directory précis.

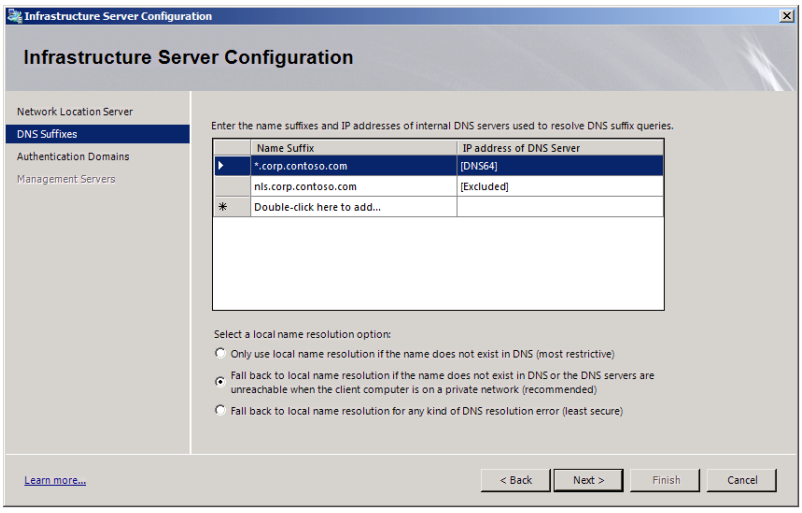
8.3 Paramétrage de la Name Resolution Policy Table

Dans cette troisième étape de la configuration de DirectAccess, on va se focaliser sur le contenu de la « Name Resolution Policy Table ». Pour rappel, cette table référence des suffixes DNS et des hôtes pour lesquels il ne faut pas utiliser la résolution de noms d'hôtes Internet. Pour chaque référence, on peut :

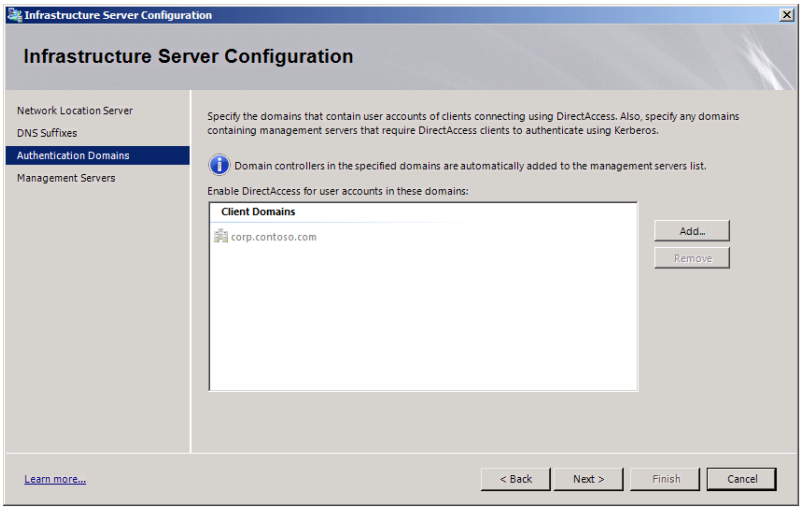
- Spécifier un ou plusieurs serveurs DNS IPv6
- Faire traiter la requête par le mécanisme de transition DNS64/NAT64
- Refuser de traiter la résolution DNS

Pour rappel, notre Network Location Server ne doit pas être accessible depuis Internet. Pour cela l'hôte DNS va être référencé comme refusé à la résolution dans la NRPT. Il est essentiel de bien référencer tous les suffixes DNS référencés dans l'entreprise. Sinon, ils ne pourront pas être adressés depuis l'extérieur.

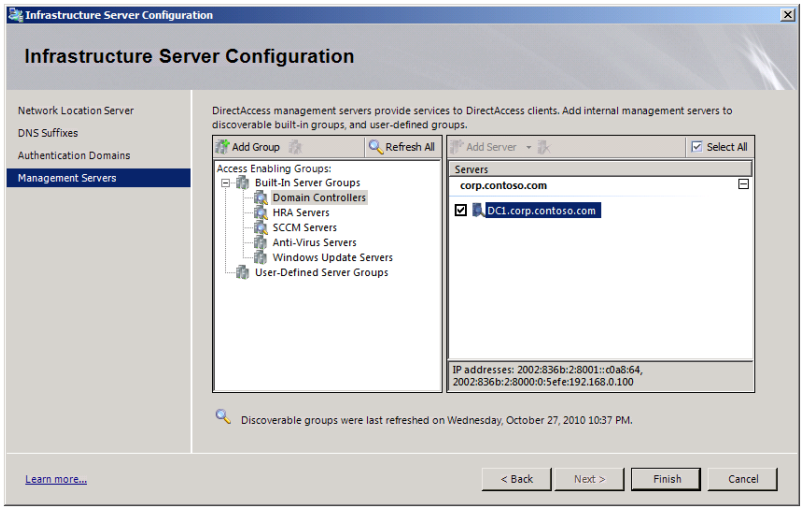
Impression d'écran	Description
	**Nouvelle étape avec la configuration des mécanismes de résolution de noms.**
	**La première étape de la configuration passe par la déclaration de l'exception de résolution lorsque l'utilisateur est en situation de mobilité. Il ne doit pas être capable de résoudre le nom du Network Location server, sinon, il serait considéré comme étant sur le LAN.**



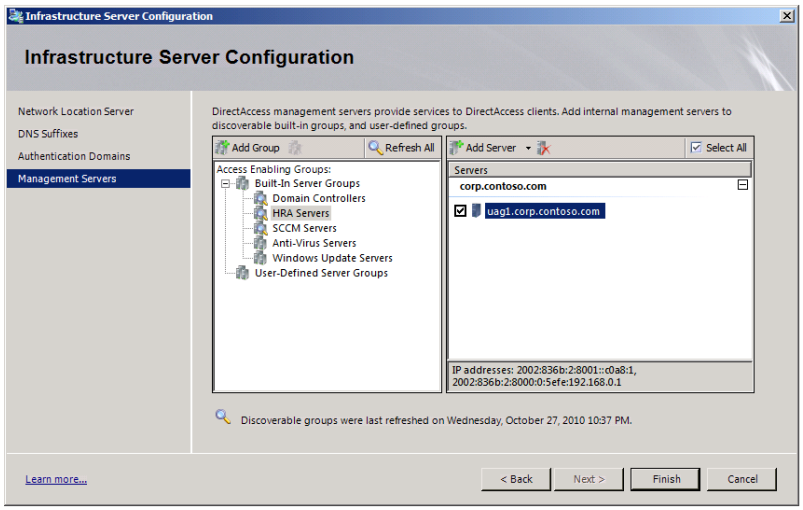
On constate bien la présence de l'exception ainsi que de la prise en charge du suffixe DNS pour la zone DNS relative au domaine Active Directory.



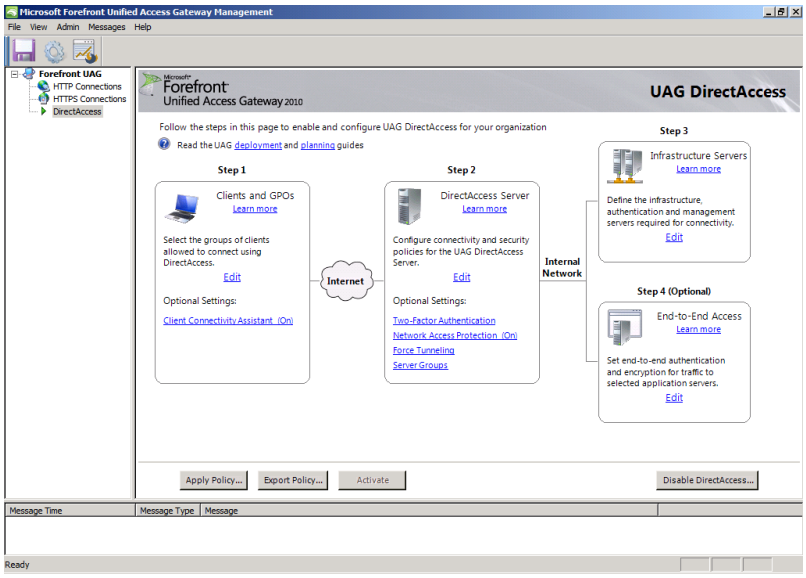
A ce stade, il est possible de spécifier les domaines Active Directory additionnels à prendre en charge, aussi bien pour les clients que les ressources auxquels ils accèdent.



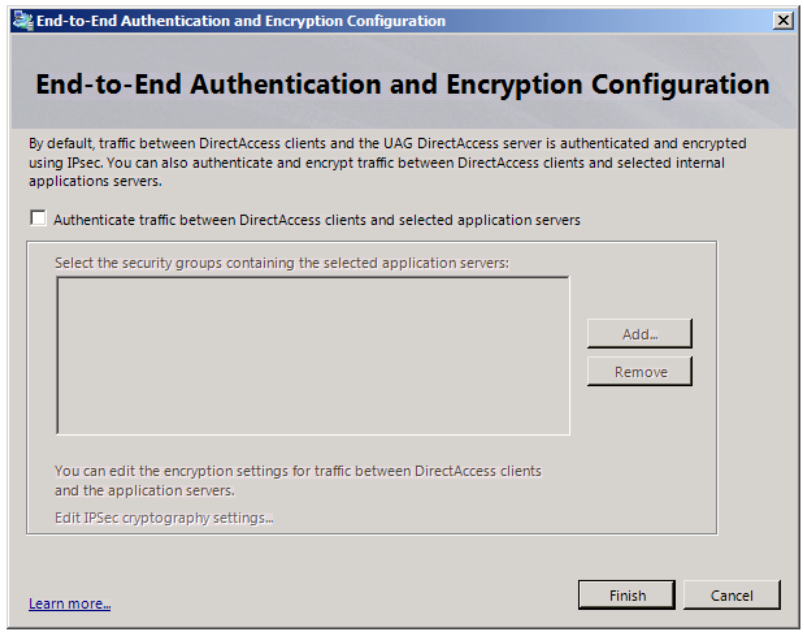
Nouveauté d'UAG 2010 SP1, la détection automatique des contrôleurs de domaine et « Health Registration Authority », à condition qu'ils soient localisés dans le même domaine que le serveur UAG.



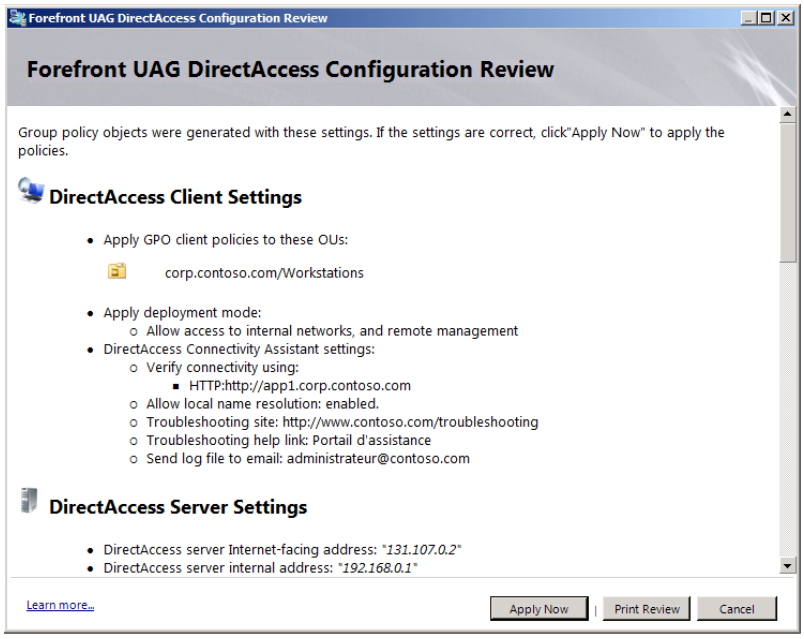
Déclarer le serveur HRA est essentiel car il doit être accessible par le client dans le tunnel infrastructure, donc avant l'ouverture de session.



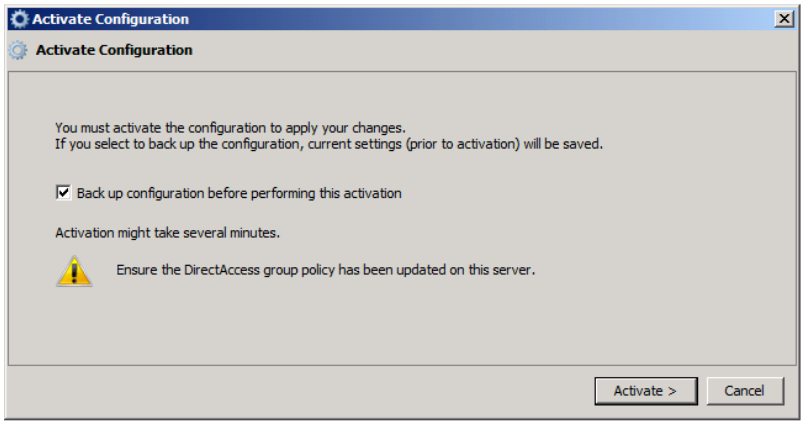
This the end, …



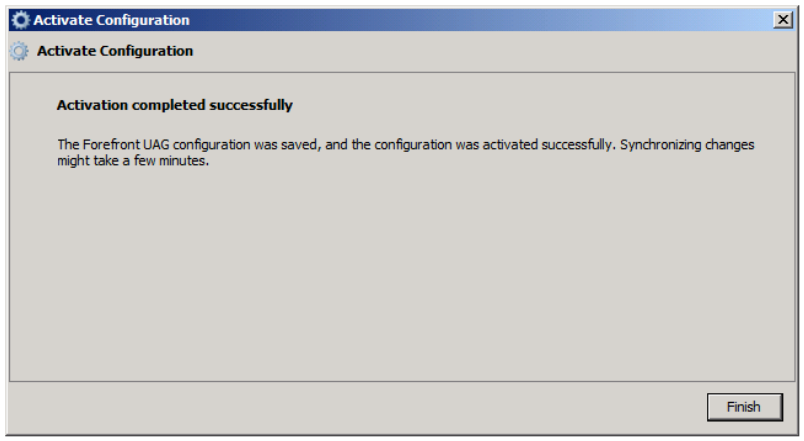
Presque car cette étape de configuration est optionnelle. Par défaut, le déploiement s'effectue en mode « End-to-Edge », ce qui signifie que l'utilisateur a accès à l'intégralité du réseau car son ou ses tunnels se terminent sur le serveur UAG.



Il ne reste plus qu'à activer la configuration. Ce n'est ni plus ni moins qu'un script Powershell qui va mettre en place l'ensemble de la configuration.



Une fois la configuration en place, reste encore à l'activer.

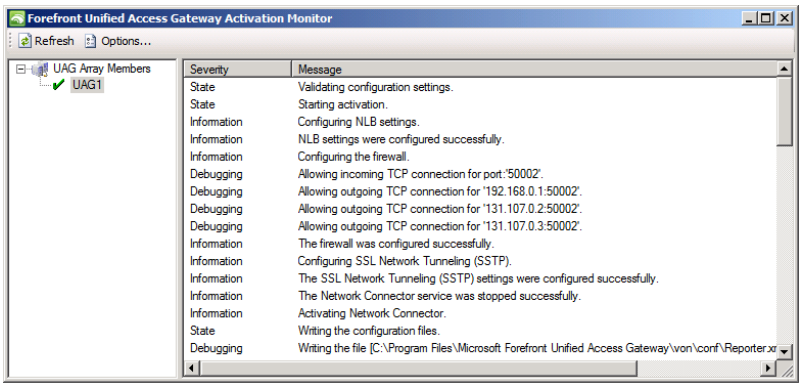
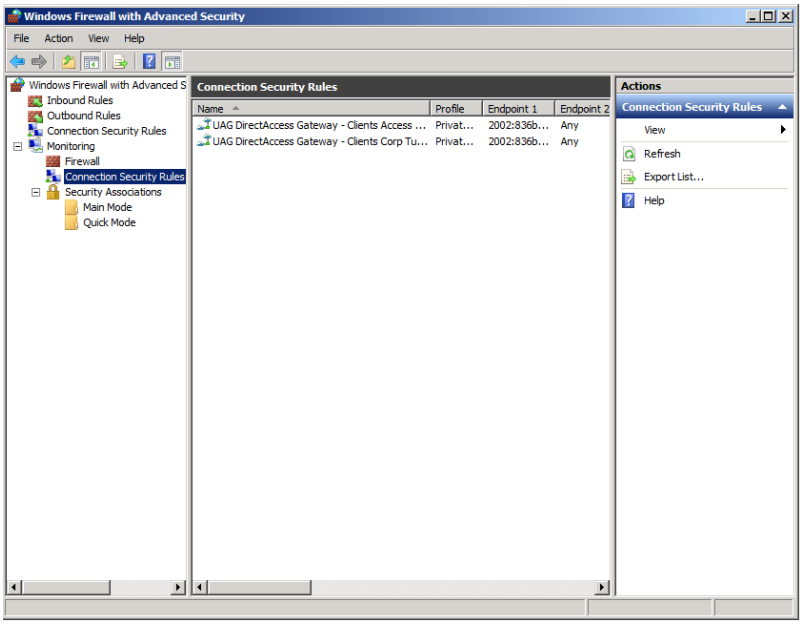


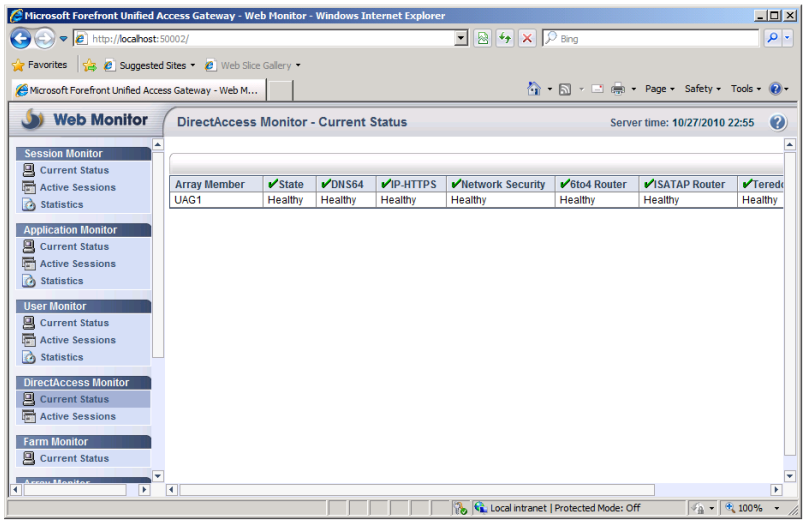
La configuration est effectivement activée. Mais est-elle propagée, ce n'est pas évident.

8.4 Checklist de bon fonctionnement

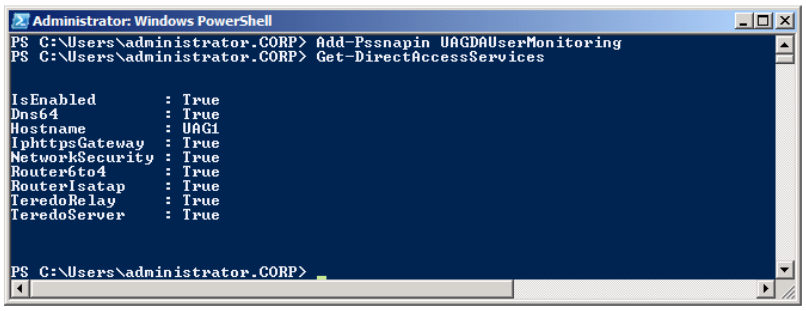
Configurer DirectAccess est certes un challenge. Maintenant, il faut que cela fonctionne. Pour cela, on va travailler à plusieurs niveaux :

- La console « UAG Activation Monitor » pour suivre l'état d'avancement de la configuration d'UAG
- La « Web Console » pour suivre l'état de santé du serveur UAG et des composants impliqués
- La « Web Console » pour suivre les sessions
- Le Snapin PowerShell livré avec UAG 2010 SP1
- La console « Pare-Feu avancé » du système d'exploitation pour suivre l'établissement des tunnels IPSEC

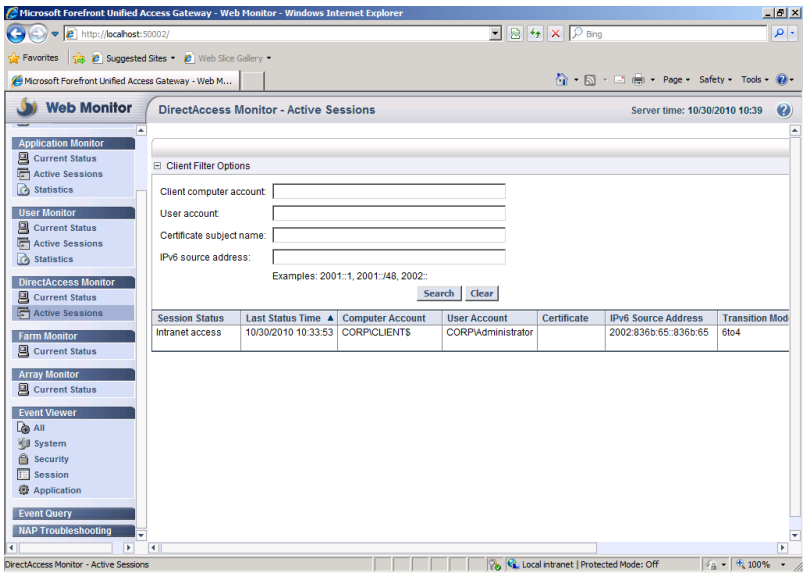
Impression écran	Description
	**La console « UAG Activation Monitor » permet de suivre l'état d'activation de notre serveur UAG. Notre serveur est bien activé mais on n'en sait pas plus.**
	**On doit pouvoir constater la présence de règles IPSEC actives dans la console de pare-feu du serveur UAG 2010. La stratégie de groupe a bien été prise en charge par notre serveur.**



Pour valider le bon fonctionnement de chaque composant, on va se référer à la console « Web Monitor » qui propose un état de santé de tous les composants impliqués. C'est une nouveauté d'UAG 2010 SP1.

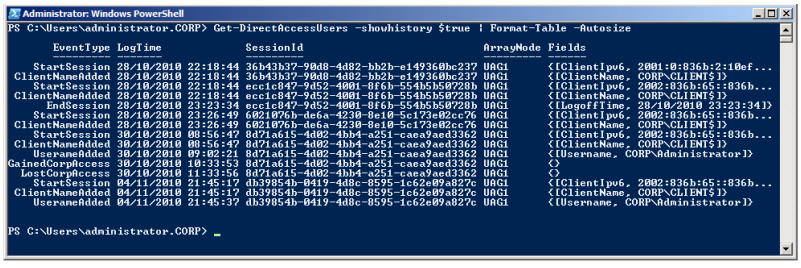


Il est aussi possible d'obtenir le même résultat en PowerShell. C'est aussi une nouveauté d'UAG 2010 SP1.



La même console permet de suivre les sessions (depuis le SP1).

Cette console présente l'intérêt de suivre les sessions de tous les serveurs UAG DirectAccess d'une même ferme.



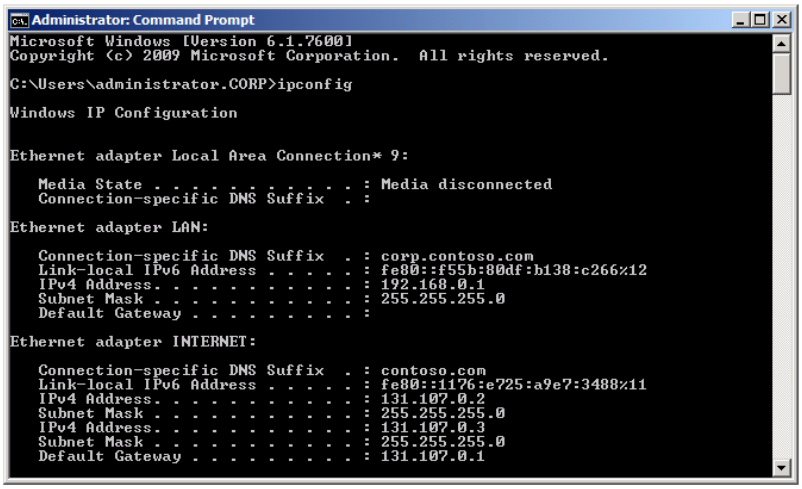
Le suivi des sessions peut aussi être réalisé en PowerShell. Depuis le SP1, on peut même demander l'historique.

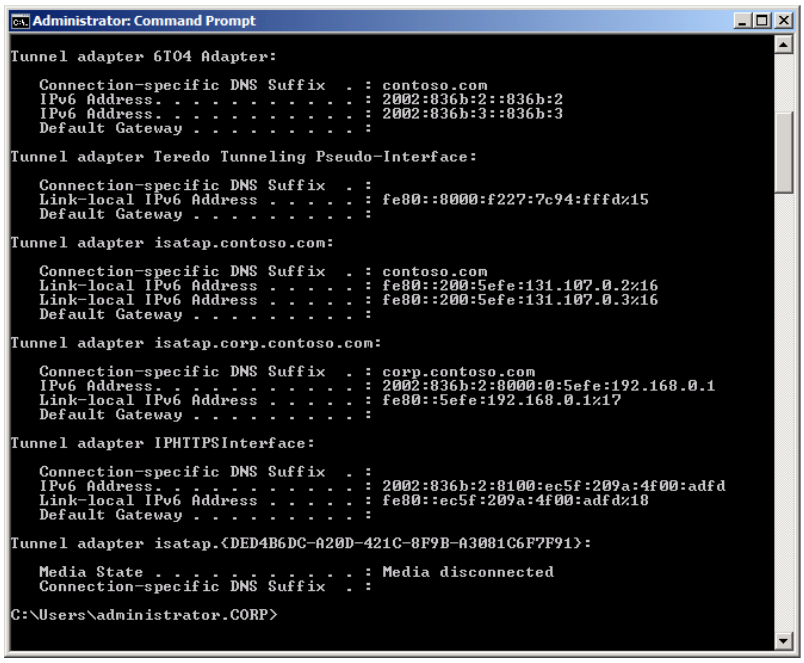
9 QU'EST CE QUI A CHANGE

La question est vaste. Coté serveur UAG, le script de configuration a effectué beaucoup de travail :

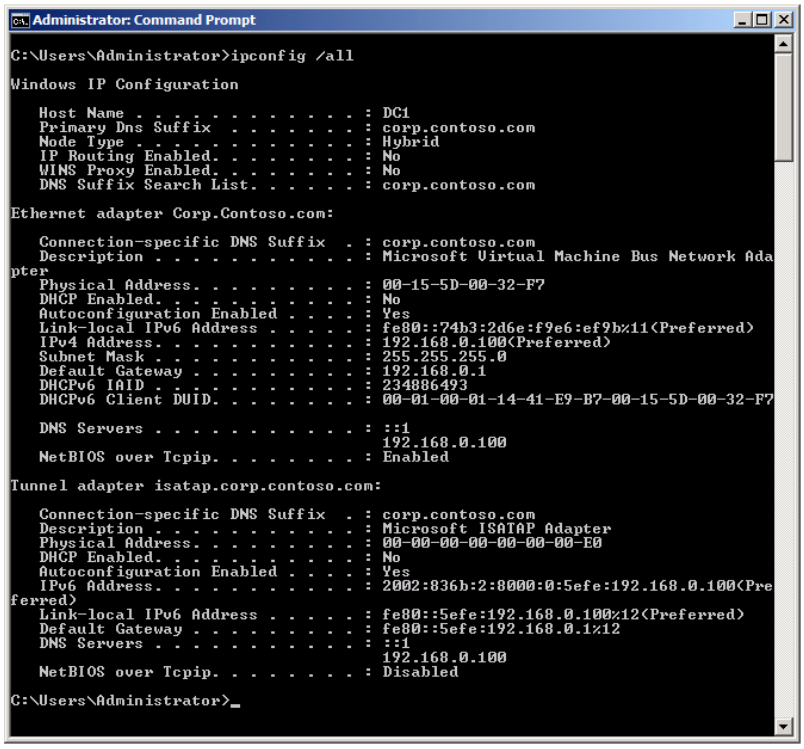
- Configuration du serveur UAG comme routeur ISATAP propageant un préfixe IPv6 dans l'organisation
- Configuration du serveur UAG comme routeur IPv6
- Configuration du serveur UAG comme routeur 6to4
- Configuration du serveur UAG comme relai et routeur Teredo
- Configuration du serveur UAG comme routeur IP-HTTPS
- Configuration du HRA sur le site web d'UAG
- Création d'une stratégie de groupe pour la configuration des clients DirectAccess
- Création d'une stratégie de groupe pour la configuration des serveurs UAG

Dès lors qu'on parle de stratégies de groupe, il ne faut pas oublier le temps nécessaire à l'actualisation. Donc un bon « GPUPDATE /Force » est nécessaire pour prendre en compte le nouveau paramétrage.

Impression écran	Description
	**Coté UAG, on pourrait penser que rien n'a changé. On ne constate même pas d'adresses IPv6 ?**

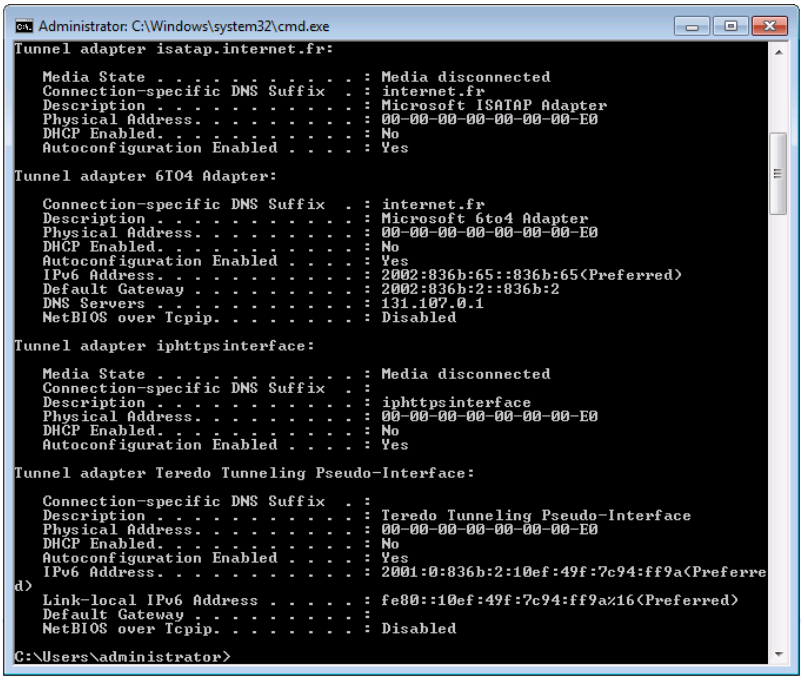


Ben non, on a bien plusieurs interfaces (6to4, Teredo, IP-HTTPS). Certaines interfaces sont désactivées car non nécessaires. C'est donc normal d'avoir une interface ISATAP désactivée coté Internet.



Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée.

Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage IPv6 d'un système d'exploitation.



Coté client, même combat. On retrouve les mêmes interfaces IPv6 (ISATAP, 6to4, Teredo, IP-HTTPS). Cependant, certaines sont désactivées car inutiles dans la situation présente.

Voilà pour les bases du DirectAccess. Pour les plus téméraires, il reste la conclusion ainsi que les possibilités pour améliorer la solution.