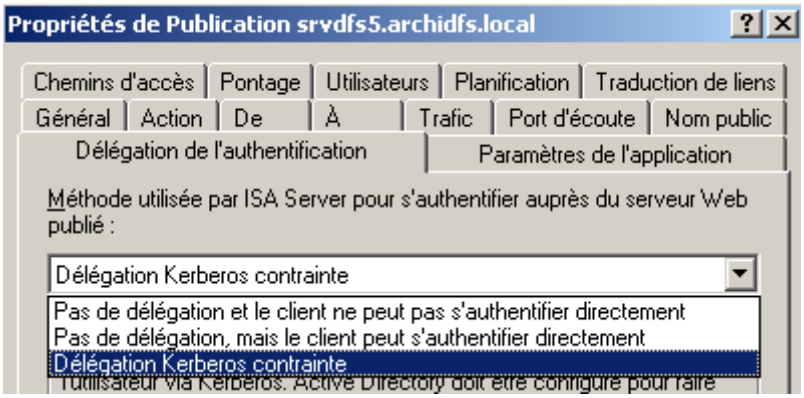
1 OBJECTIFS DE CE DOCUMENT :

Déterminer et valider la configuration d'Isa Server pour publier un serveur SharePoint sur Internet avec utilisation de certificats clients (carte à puce) avec les contraintes suivantes :

- Le client doit s'authentifier à l'aide d'une carte à puce (certificat utilisateur).
- Le serveur Isa Server doit authentifier la demande de connexion tout comme le serveur web.
- Le serveur web doit être configuré avec de l'authentification intégré.
- Les utilisateurs ne doivent pas avoir besoin de s'authentifier (il insère uniquement leur carte à puce).

2 ACTIONS A EFFECTUER SUR ISA SERVER :

On va configurer Isa Server pour accepter l'authentification avec des certificats de type « *Utilisateur* ». Cela nécessite d'utiliser la « *Délégation Kerberos contrainte* ». Il n'est pas possible d'utiliser de la délégation NTLM avec les certificats client (certificat de type « Utilisateur ») comme le montre la capture ci-dessous :



Les prérequis suivants doivent être respectés pour la mise en œuvre de la « *Délégation Kerberos contrainte* » :

- Le domaine doit être en mode natif 2003.
- Le serveur Isa Server 2006 et le serveur web doivent être dans le même domaine. **Le correctif suivant (inclus dans le SP1) semble supprimer cette limitation mais en pratique cela ne marche pas : http://support.microsoft.com/kb/942637/en-us.**
- Il faut autoriser la fragmentation IP dans Isa Server 2006.

Les articles ci-dessous expliquent comment configurer la délégation contrainte :

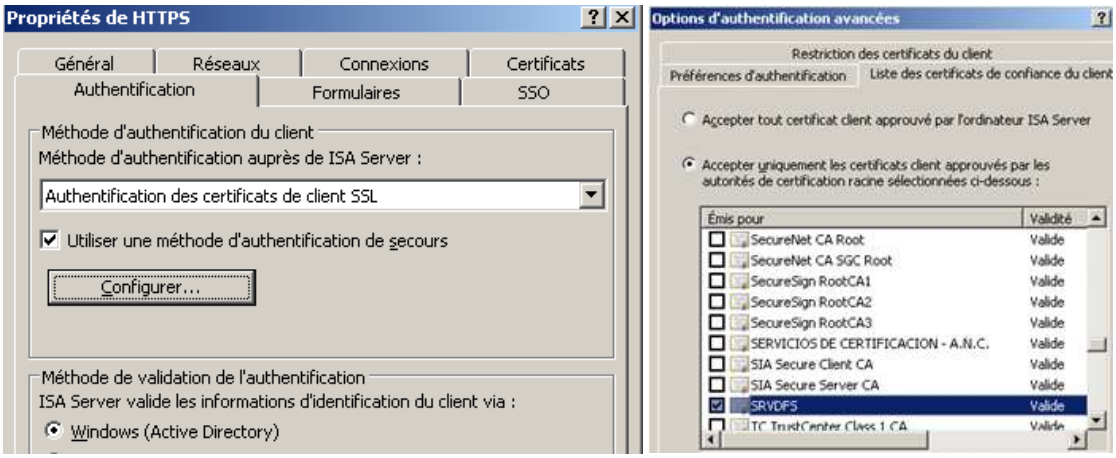
- http://technet.microsoft.com/en-us/library/bb794858.aspx
- http://technet.microsoft.com/fr-fr/library/bb794751.aspx (Exemple avec Publication OWA)
- http://technet.microsoft.com/fr-fr/library/cc786828(WS.10).aspx

Remarque :

- Il est préconisé d'installer le dernier pack de correctif Isa Server 2006 (POST SP1) : http://support.microsoft.com/kb/960148/en-us
- Pour contrôler le format de saisi du champ login / mot de passe : http://support.microsoft.com/kb/960146/en-us
- Autre problème avec la « *délégation Kerberos contrainte* » : http://support.microsoft.com/kb/947124/en-us

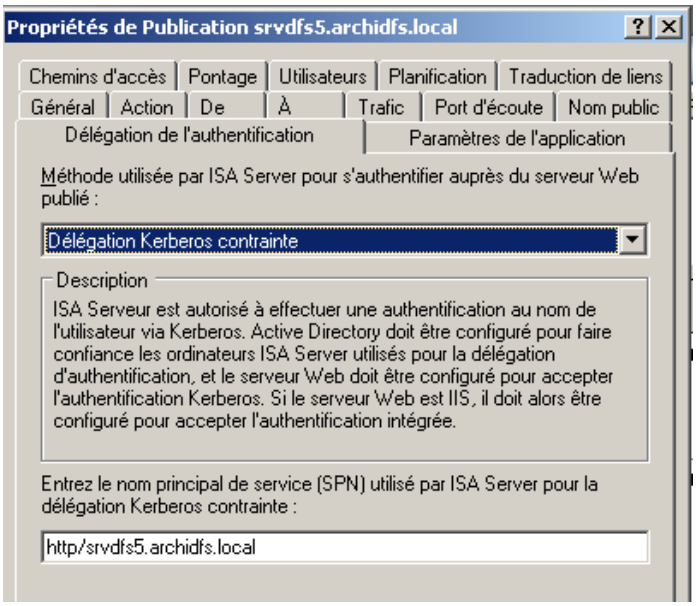
2.1 CONFIGURATION DU PORT D'ECOUTE :

Il faut configurer le port d'écoute Isa Server au niveau de la règle de publication WEB avec la méthode d'authentification « *Authentification de certificats de client SSL* ». Il faut ensuite autoriser le certificat de l'autorité de certification qui a émis les certificats clients (SRVDFS dans l'exemple).



2.2 CONFIGURATION DU PORT DE LA DELEGATION D'AUTHENTIFICATION :

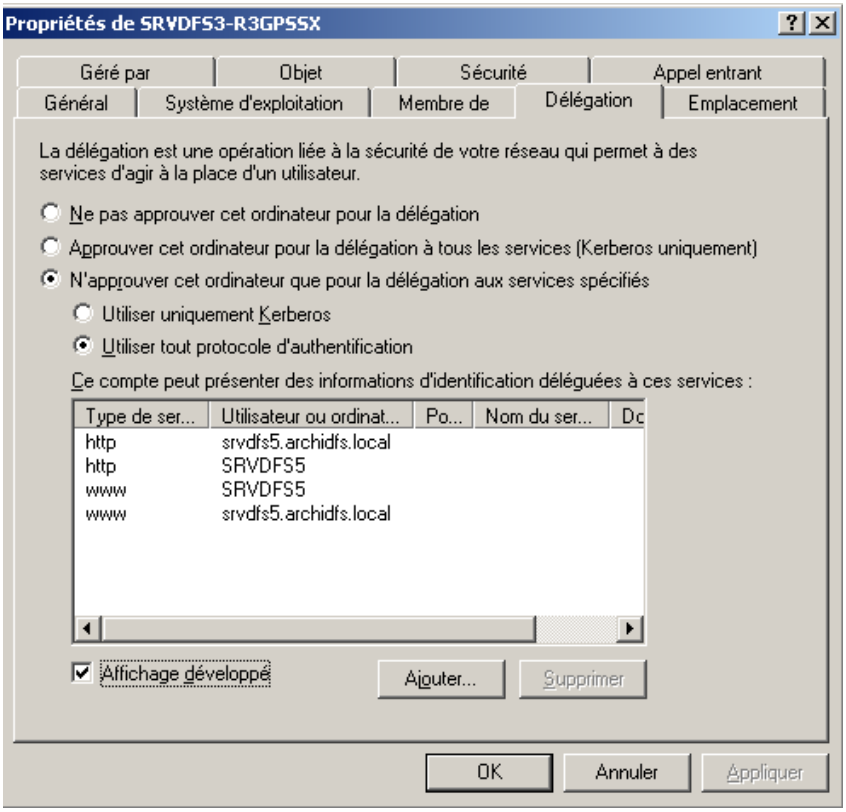
Il faut ensuite configurer la délégation d'authentification sur « *Délégation Kerberos contrainte* ».



Il sera nécessaire de créer le SPN (Service Principal Name) au niveau du serveur web (même valeur que dans la capture ci-dessous).

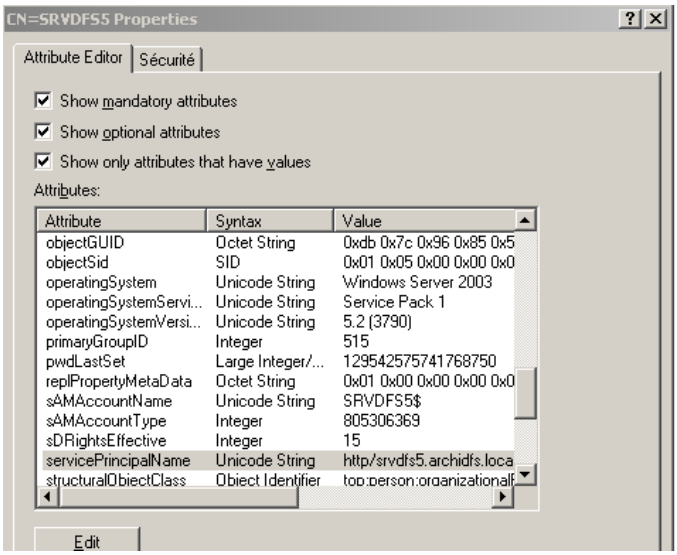
2.3 CONFIGURER LE COMPTE ORDINATEUR DU SERVEUR ISA :

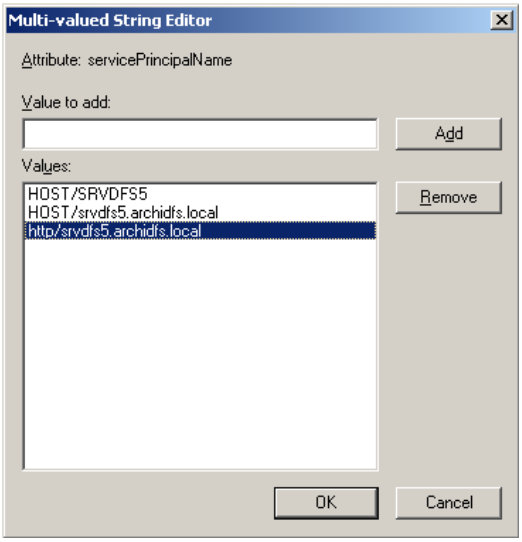
Il faut approuver la délégation au niveau du compte ordinateur du serveur ISA (SRVDF3-R3GPSSX dans l'exemple).



2.4 AJOUTER LE SERVICE PRINCIPALNAME (SPN) AU NIVEAU DU COMPTE ORDINATEUR DU SERVEUR WEB :

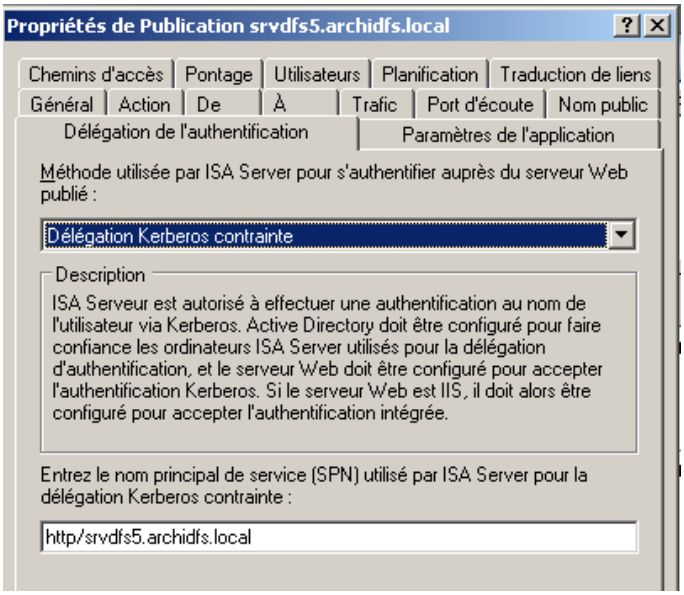
Il faut ajouter le Service Principal Name (SPN) au niveau du serveur web.
Cela peut être fait via ADSIEDIT ou via la commande SETSPN.





Le SPN doit être identique à celui indiqué dans la règle Isa Server 2006.

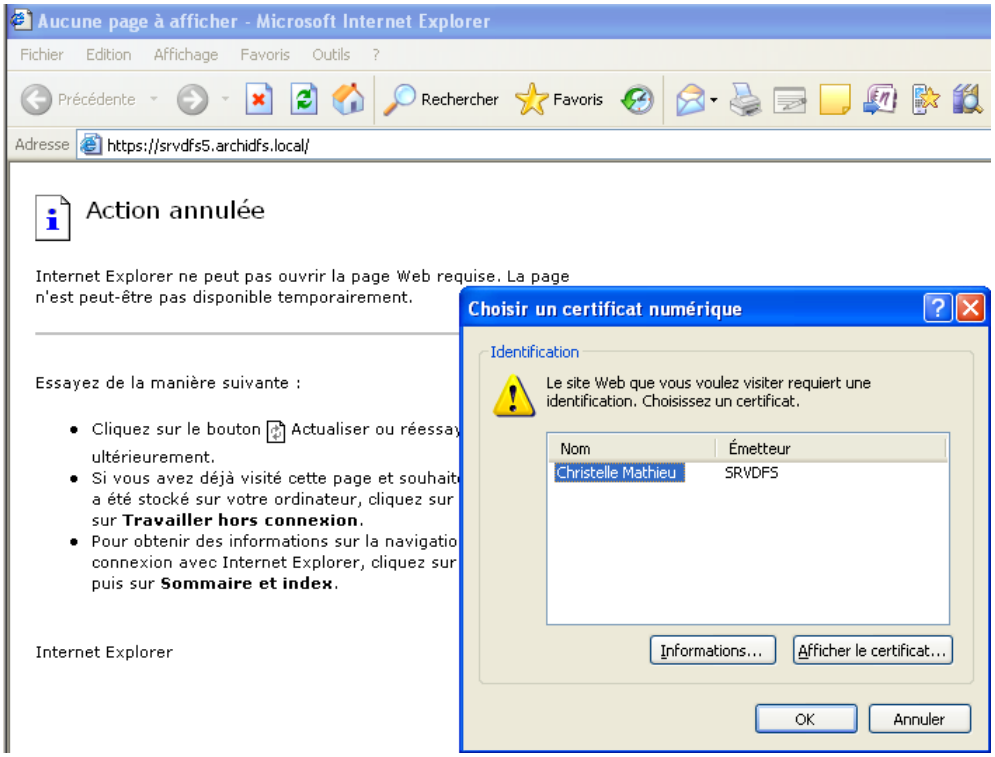
Guillaume MATHIEU – MSREPORT (http://msreport.free.fr)
La connaissance s'accroît quand on la partage



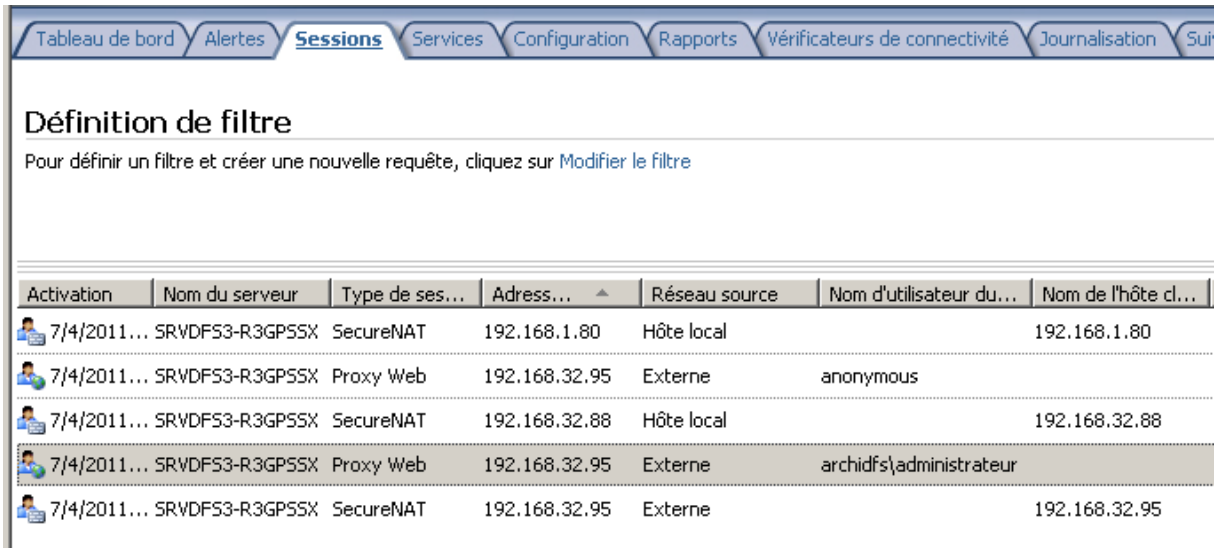
2.5 RESULTATS ET PROBLEMES RENCONTREES :

2.5.1 TESTS CONNEXION AVEC UN COMPTE UTILISATEUR SITUE DANS LE MEME DOMAINE QUE LE SERVEUR WEB ET ISA SERVER :

Si un utilisateur essaie de se connecter depuis Internet, il voit cette fenêtre :



Au niveau d'Isa Server 2006, on voit que la connexion est authentifiée et que c'est bien le module proxy qui est utilisé.



2.5.2 TEST CONNEXION AVEC UN COMPTE SITUE DANS UN AUTRE DOMAINE :

Cela échoue si utilisation d'un compte d'un autre domaine de la forêt (pas dans le même domaine que le serveur ISA et le serveur web). On a l'erreur ci-dessous.

Event Type: Error
Event Source: Microsoft ISA Server Web Proxy
Event Category: None
Event ID: 21315
Date: 7/5/2011
Time: 2:58:30 PM
User: N/A
Computer: SRVDFS3-R3GPSSX
Description:
ISA Server n'a pas pu déléguer d'informations d'identification au site Web publié par la règle Publication srvdfs5.archidfs.local à l'aide de la délégation Kerberos contrainte. Vérifiez que les noms principaux du service : http/srvdfs5.archidfs.local configurés dans ISA Server correspondent à ceux d'Active Directory.

Le correctif suivant (inclus dans le SP1) semble supprimer cette limitation mais en pratique cela ne marche pas : http://support.microsoft.com/kb/942637/en-us.