# Déroulé de l'installation du serveur RADIUS-NPS sur Windows 2008-R2 Server

**Situation de départ**

- Un Serveur Windows 2008 R2 avec Active Directory (AD) qui a pour adresse IP 172.20.90.100 ;

- Un domaine AD "mars.local" ;

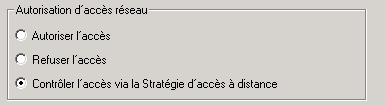
- Pare-feu désactivé dans un premier temps pour ne pas compliquer les tests.

Dans AD :

- Deux groupes existent : "escrime" et "handball" ;

- Deux utilisateurs : "valerie" dans le groupe "escrime" et "nicolas" dans le groupe "handball" ;

- Ces utilisateurs se verront accorder l'accès distant dans l'onglet "appel entrant" en fonction de la future stratégie d'autorisation d'accès. Un accès 802.1x est considéré comme un accès distant, même si cet accès se fait sur le réseau local. Si on positionne l'autorisation sur "autoriser l'accès", cela marchera également : la stratégie pourra refuser l'accès sur un autre critère.



# I Ajout du rôle "Services de certificats Active Directory"

Note : ce rôle est nécessaire pour l'utilisation de PEAP dans une stratégie d'accès réseau. On peut installer Network Policy Server (NPS) sans service de certificats, mais on ne pourra pas utiliser PEAP.



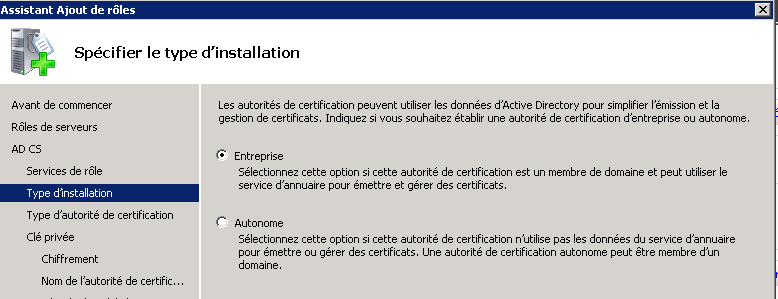
[SUIVANT] sur la page informative suivante



Choix d'installation d'une autorité de certification. Le service d'inscription de l'autorité de certification via le Web n'est pas nécessaire dans notre cas.



On choisit une installation du type Autorité de certification d'entreprise...



... de type "RACINE"



🡺 On crée une nouvelle clé privée



Cette étape va générer la clé publique présente dans le certificat.

🡺 On choisit la méthode de chiffrement par défaut



Par défaut, l'assistant nomme l'autorité de certification avec le nom de domaine suivi du nom de machine. On peut simplifier ce nom.



🡺 On laisse la période de validité par défaut ...



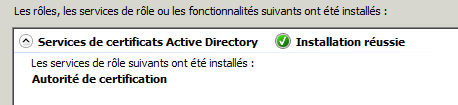
... ainsi que l'emplacement d'installation de la base de données de certificats



Écran récapitulatif des choix avant installation de l'autorité :

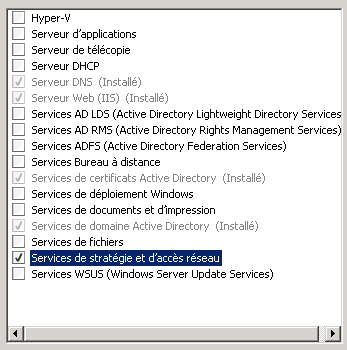


Écran témoin de la réussite de l'installation de l'autorité de certification (AC).

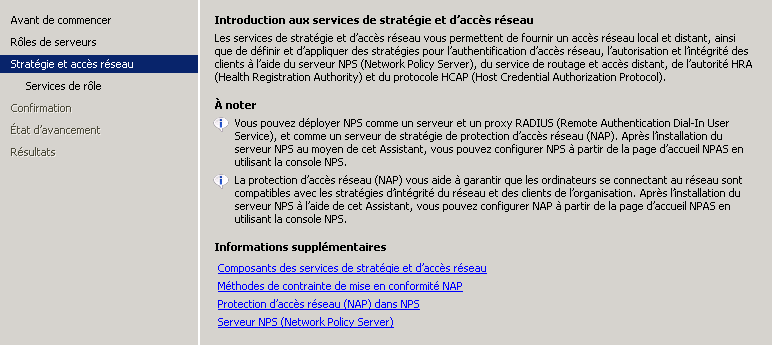


## II Installation du serveur RADIUS - NPS (Network Policy Server)

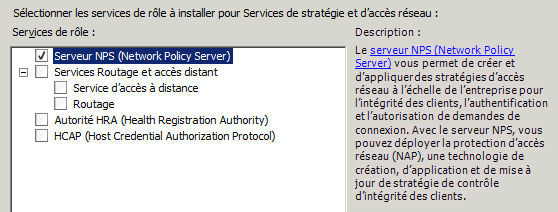
Dans l'assistant de gestion des rôles, choisir "Services de stratégie et d'accès réseau".



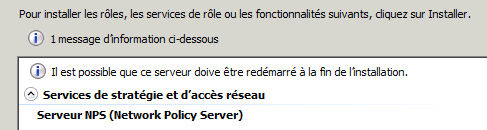
Suit un écran d'informations :



Choisir les services de rôle suivants :



Écran récapitulatif des choix d'installation de NPS et témoin de réussite



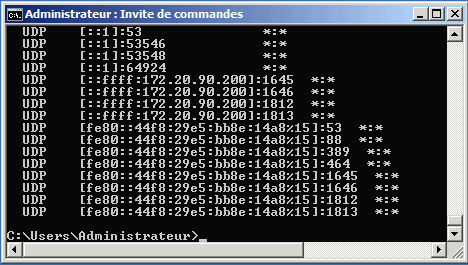


🡺 ATTENTION

Si l'adresse IP du serveur est changée après l'installation de NPS, il sera impératif de redémarrer le service.

Pour vérifier le bon fonctionnement du service NPS sur le serveur, vous pouvez afficher les ports en écoute sur celui-ci avec la commande **netstat -a**

Résultat de la commande nestat -a : voir les 4 dernières lignes.



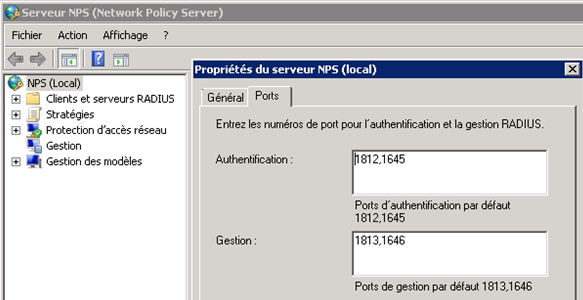
NPS écoute sur les ports suivants par défaut :

- 1812, 1645 pour l'authentification.

- 1813,1646 pour la gestion.

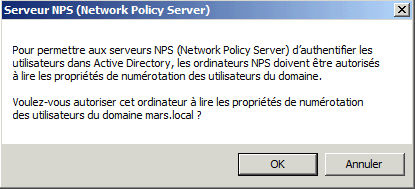
Note

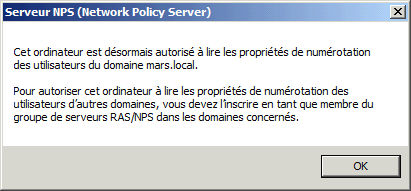
On peut retrouver ces ports dans les propriétés du serveur NPS (à chercher dans les outils d'administration ou dans le service de rôle) :



## III CONFIGURATION DU SERVEUR RADIUS NPS

Au préalable, il faut inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs. Menu Action.



Résultat de l'inscription  


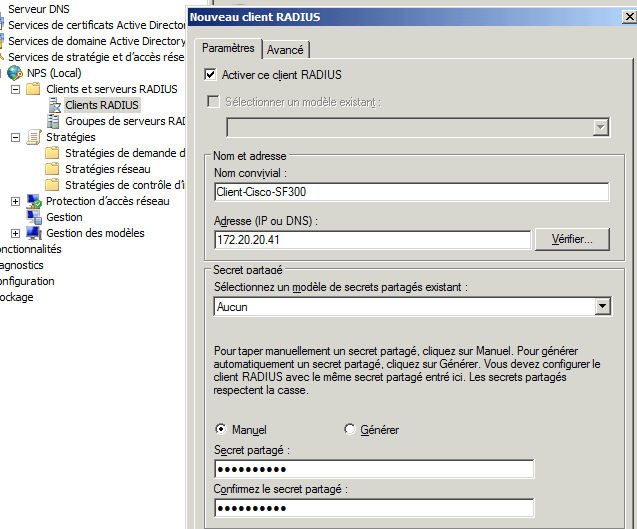
Note : un assistant global est disponible. On va plutôt détailler chaque phase.

### 1. Déclaration d'un client RADIUS

Dans notre cas, le commutateur est un Cisco SF300 compatible 802.1x. Les éléments à renseigner sont : le nom "convivial" du client-RADIUS, son adresse IP et la chaîne de caractères du "secret partagé" entre le serveur RADIUS et le client RADIUS, ici la chaîne "Sesame9999".

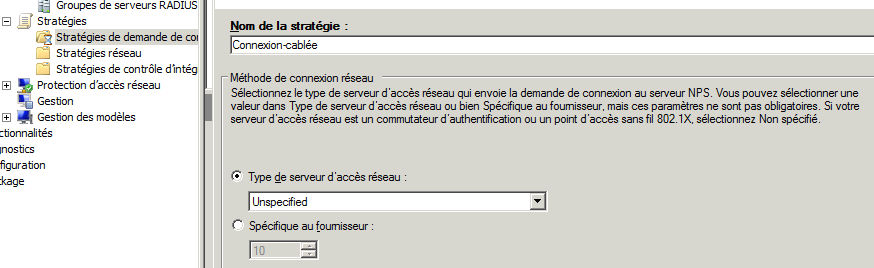
Cette chaîne doit évidemment être identique à celle déclarée dans le client radius, c'est-à-dire le commutateur Cisco. Il s'agit d'un secret partagé entre deux éléments d'infrastructure, avec une exigence de sécurité moins importante qu'un accès "depuis un poste client". Il y a peu de chance qu'un élément d'infrastructure en agresse un autre ...

Sur l'entrée *Clients RADIUS*, faire un clic droit 🡺 Nouveau Client RADIUS



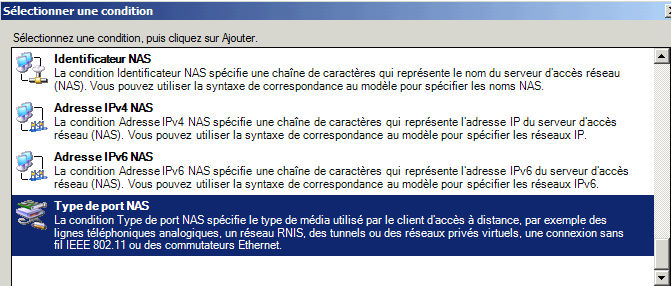
### 2. Déclaration d'une stratégie de demande de connexion

On déclare une stratégie de demande de connexion pour Ethernet. Il s'agit de la connexion physique au média.



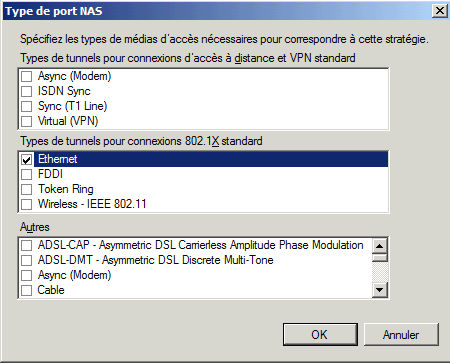
Ici, on choisit un nom de stratégie. On laisse le type de serveur sur "Unspecified" (nous utilisons un commutateur en tant que client Radius).

On choisit ensuite d'indiquer un type de port NAS (type de media concerné)

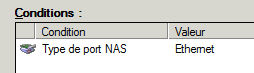


Note : NAS est ici l'acronyme "Network Access Server" et désigne le client RADIUS. Ne pas confondre avec Network Authentication Server, qui désigne le serveur Radius lui-même.

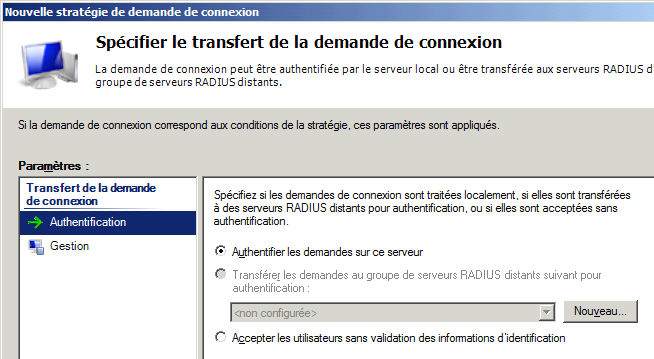
Puis on coche "Ethernet" dans l'écran suivant...



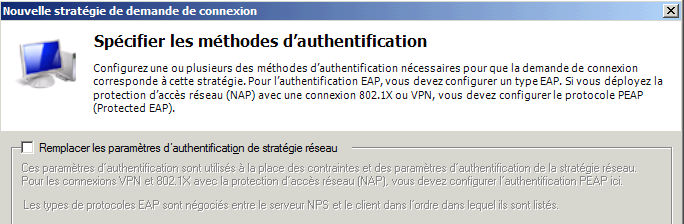
Récapitulatif :



Dans les autres écrans, on garde les choix par défaut :

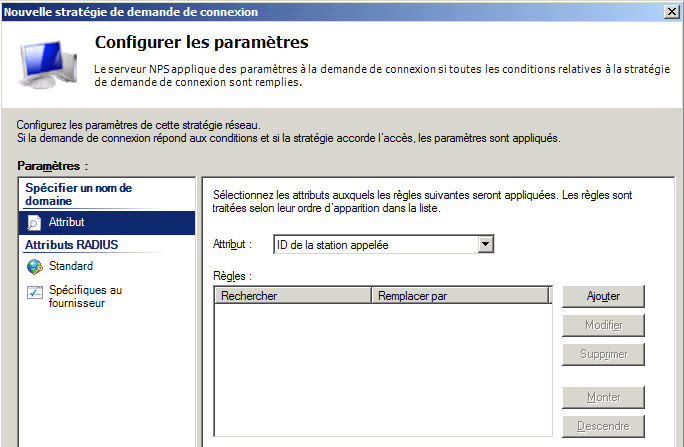


Les demandes seront traitées sur ce serveur et non sur un autre. Ce qui veut dire que ce NPS pourrait jouer un rôle de "PROXY NPS" s'il relayait les demandes à un autre serveur.

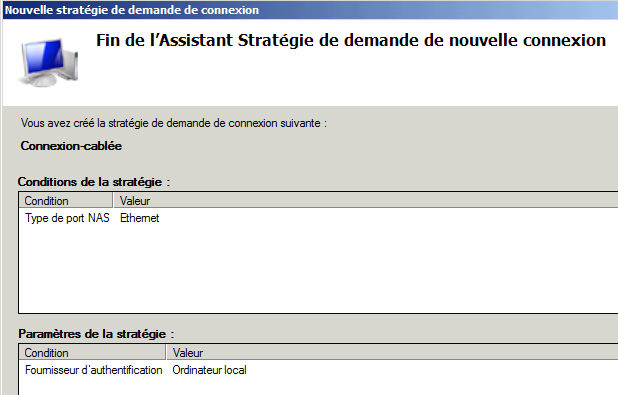


Cet écran est laissé tel quel. C'est la stratégie d'accès réseau que l'on va maintenant déclarer qui va primer.

Rien à configurer non plus dans l'écran suivant



Écran récapitulatif de la stratégie de demande de connexion

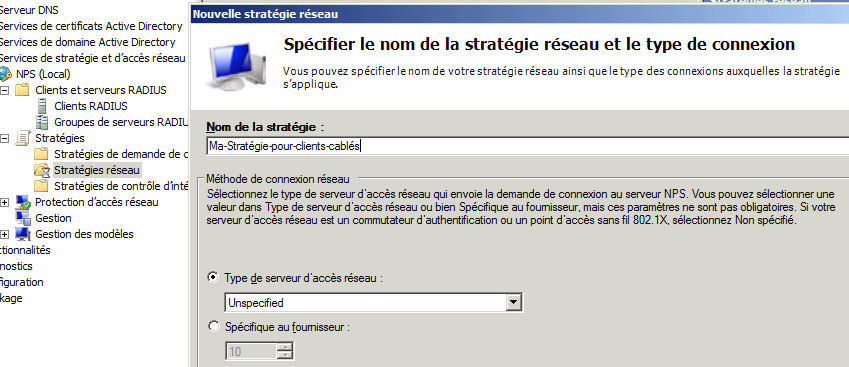


### 3. Déclaration d'une stratégie réseau (stratégie d'accès au réseau)

On veut mettre en place une stratégie de placement dynamique dans le VLAN 2 pour les membres du groupe d'utilisateurs "escrime". Le commutateur client-RADIUS se chargera lui-même du placement dans un VLAN "guest" des utilisateurs non authentifiés.

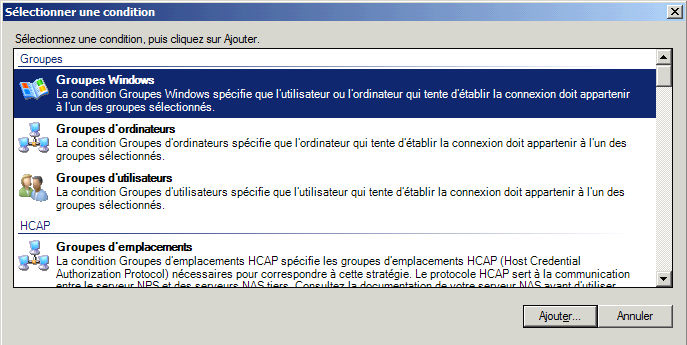
Note : Si on veut placer les membres du groupe "Handball" dans un VLAN 3, on créera une autre stratégie d'accès réseau. On peut donc avoir un catalogue de stratégies d'accès réseau, pour une seule stratégie de demande de connexion.

Sur l'entrée Stratégie Réseau, faire un clic droit 🡺 Nouvelle Stratégie réseau

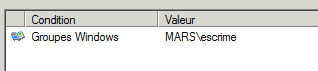


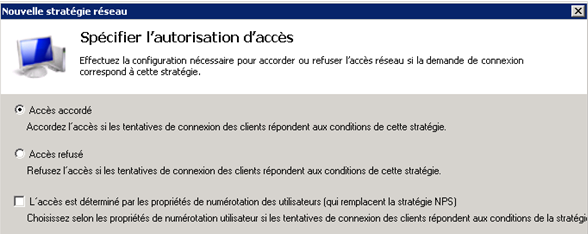
🡺 On reste sur un type non spécifié car s'agit d'une authentification via un commutateur 802.1x

On ajoute une condition à la validation de la stratégie : que l'utilisateur soit membre d'un groupe AD qui s'appelle "escrime". Pour les membres de ce groupe, on accorde l'accès. Choisir Groupe Windows et non Groupes d'utilisateurs.



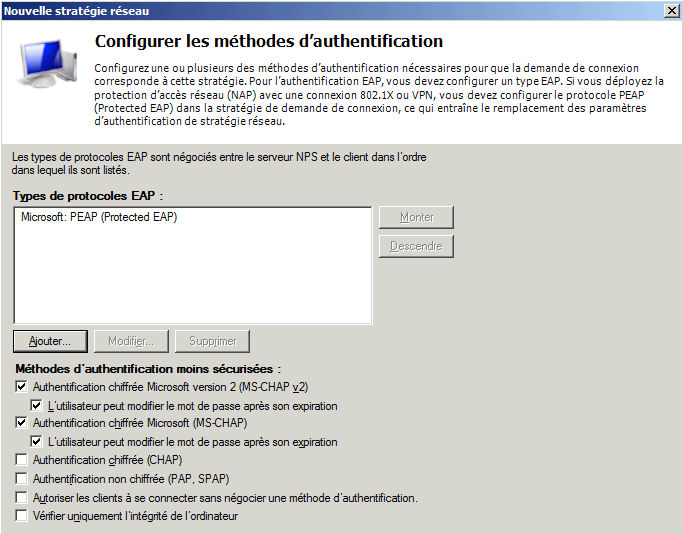
Récapitulatif du choix des groupes Windows



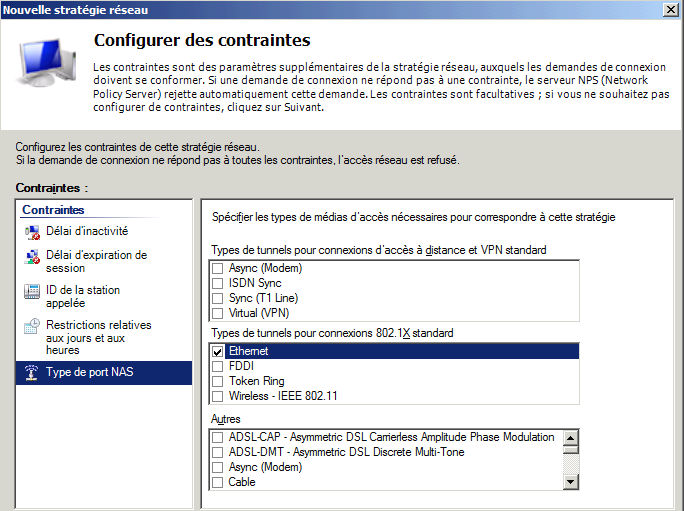


On peut définir des stratégies autorisant l'accès quand les conditions sont réunies ou, à l'inverse, interdisant l'accès lorsque les conditions sont réunies (un groupe d'utilisateur en congé par exemple).

🡺 On déclare ensuite les types de protocoles EAP accepté : PEAP

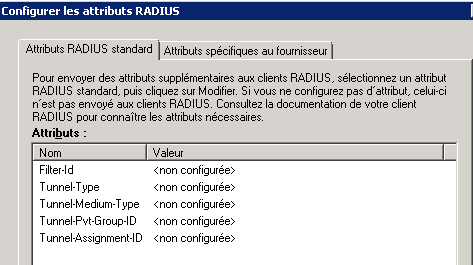


🡺 On accepte les Types de ports NAS Ethernet

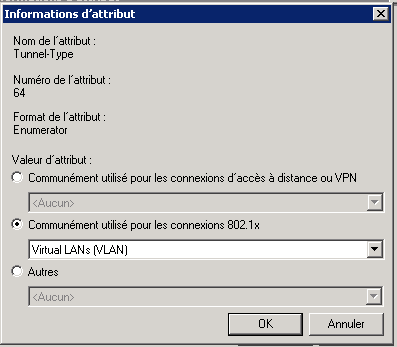


C'est ici que se fait le lien avec la stratégie de demande de connexion.

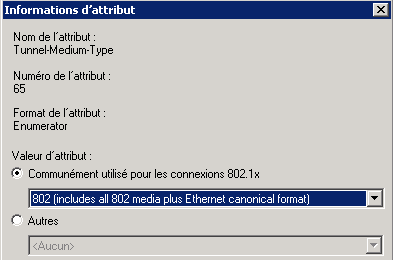
On va maintenant ajouter des attributs de contrôle de trafic en cliquant sur [AJOUTER]



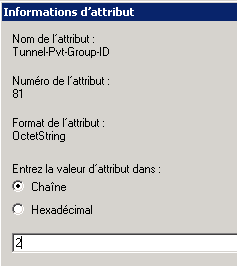
▶ Dans notre objectif d'affectation dynamique de VLAN, on va modifier les attributs Tunnel-Type, Tunnel-Medium-Type et Tunnel-Pvt-Group-ID qui vont être envoyés au client Radius pour qu'il réalise l'affectation dynamique de VLAN.



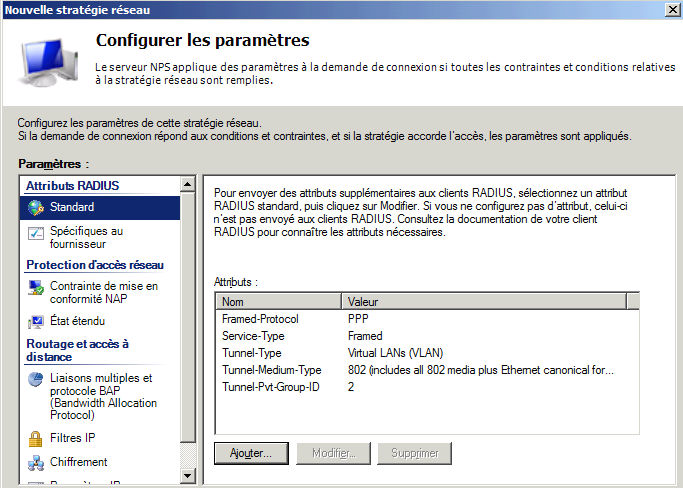
Même chose pour "Tunnel-Medium-Type" que l'on règle sur "802 (includes...)"



Enfin "Tunnel-Pvt-Group-ID" sur le numéro de VLAN dans lequel on veut positionner les membres du groupe d'utilisateurs "escrime" : pour nous le VLAN 2.

****

▶ Un écran récapitulatif des attributs est affiché par l'assistant :



**FIN**

On a donc défini une stratégie d'accès réseau Ethernet 802.1x plaçant dans le VLAN2 les membres authentifiés comme faisant partie du groupe "escrime", vérifiée par la collaboration du serveur NPS avec le client RADIUS, commutateur d'IP 172.20.20.41.

Pour cela le mécanisme de mise en place par NPS a été le suivant :

- Stratégie de demande de connexion associée aux connexions filaire Ethernet

- Stratégie réseau (accès au réseau)

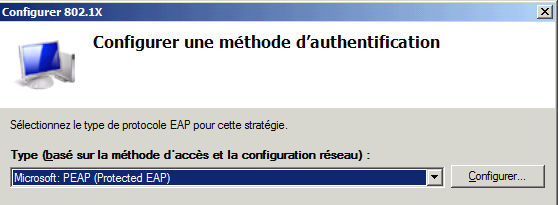
- Précisant le groupe autorisé (escrime)  
 🡺 notion de conditions

- Précisant la méthode d'authentification (PEAP/MSCHAPV2)  
 🡺 notion de propriété

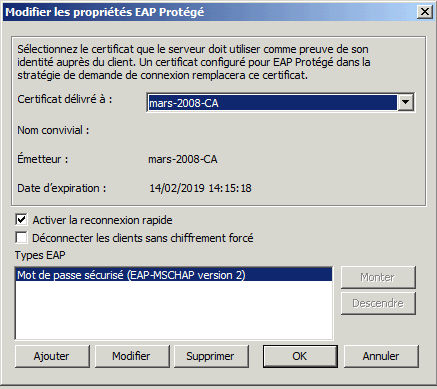
- Associant avec la stratégie de demande de connexion (NAS Ethernet)   
 🡺notion de contrainte

- Précisant les paramètres renvoyés au client radius (VLAN)   
 🡺 notion d'attributs

Note : si nous avions pris l'assistant général, dans le choix de la stratégie réseau, nous aurions rencontré les écrans suivants :



Cliquer sur [Configurer] fait apparaître l'écran suivant, dans lequel on voit la référence au certificat serveur (fait par défaut du fait de l'installation de NPS après le service de certificat et son inscription dans AD)



## Observateur d'évènements AVANT / APRES

L'Observateur d'évènement de Windows 2008 se présente sous forme fenêtrée avec du scrolling qui le rend difficile à intégrer sous forme "papier". Par contre, les exportations XML sont possibles :

🡺 dans un cas d'insuccès de l'authentification : Nicolas, du groupe "Handball"

Nom du journal :Security

Source : Microsoft-Windows-Security-Auditing

Date : 14/02/2014 15:37:34

ID de l’événement :6273

Catégorie de la tâche :Serveur NPS

Niveau : Information

Mots clés : Échec de l’audit

Utilisateur : N/A

Ordinateur : Base-2008-R2.mars.local

Description :Le serveur NPS a refusé l’accès à un utilisateur.

Contactez l’administrateur du serveur NPS pour plus d’informations.

Utilisateur :

ID de sécurité : S-1-5-21-3923959702-3099665348-2013018430-1105

Nom de compte : nicolas@mars.local

Domaine de compte : MARS

Nom de compte complet : MARS\nicolas

Ordinateur client :

ID de sécurité : NULL SID

Nom de compte : -

Nom de compte complet : -

Version du système d’exploitation : -

Identificateur de la station appelée : -

Identificateur de la station appelante : 90-2B-34-40-5F-9A

Serveur NAS :

Adresse IPv4 du serveur NAS : 172.20.20.41

Adresse IPv6 du serveur NAS : -

Identificateur du serveur NAS : -

Type de port du serveur NAS : Ethernet

Port du serveur NAS : 7

Client RADIUS :

Nom convivial du client : Client-Cisco-SF300

Adresse IP du client : 172.20.20.41

Informations détaillées sur l’authentification :

Nom de la stratégie de demande de connexion : Connexion-cablée

Nom de la stratégie réseau : -

Fournisseur d’authentification : Windows

Serveur d’authentification : Base-2008-R2.mars.local

Type d’authentification : EAP

Type EAP : -

Identificateur de la session du compte : -

Résultats de la journalisation : Les informations de suivi ont été inscrites dans le fichier journal local.

Code raison : 48

Raison : La demande de connexion ne correspondait à aucune stratégie réseau configurée.

🡺 Dans un cas de succès de l'authentification :

Nom du journal :Security

Source : Microsoft-Windows-Security-Auditing

Date : 14/02/2014 15:29:09

ID de l’événement :6278

Catégorie de la tâche :Serveur NPS

Niveau : Information

Mots clés : Succès de l’audit

Utilisateur : N/A

Ordinateur : Base-2008-R2.mars.local

Description :

Le serveur NPS a accordé l’accès total à un utilisateur car l’hôte répond aux critères définis par la stratégie d’intégrité.

Utilisateur :

ID de sécurité : MARS\valerie

Nom de compte : valerie@mars.local

Domaine du compte : MARS

Nom de compte complet : mars.local/Users/valerie

Ordinateur client :

ID de sécurité : NULL SID

Nom de compte : -

Nom de compte complet : -

Version du système d’exploitation : -

Identificateur de la station appelée : -

Identificateur de la station appelante : 90-2B-34-40-5F-9A

Serveur NAS :

Adresse IPv4 du serveur NAS : 172.20.20.41

Adresse IPv6 du serveur NAS : -

Identificateur du serveur NAS : -

Type de port du serveur NAS : Ethernet

Port du serveur NAS : 7

Client RADIUS :

Nom convivial du client : Client-Cisco-SF300

Adresse IP du client : 172.20.20.41

Informations détaillées de l’authentification :

Nom de la stratégie de demande de connexion : Connexion-cablée

Nom de la stratégie réseau : Ma-Stratégie-pour-clients-cablés

Fournisseur d’authentification : Windows

Serveur d’authentification : Base-2008-R2.mars.local

Type d’authentification : PEAP

Type EAP : Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)

Identificateur de la session du compte : -

Informations de quarantaine :

Résultat : Accès complet

Résultats étendus : -

Identificateur de la session : -

URL de l’aide : -

Résultats du validateur d’intégrité du système : -