

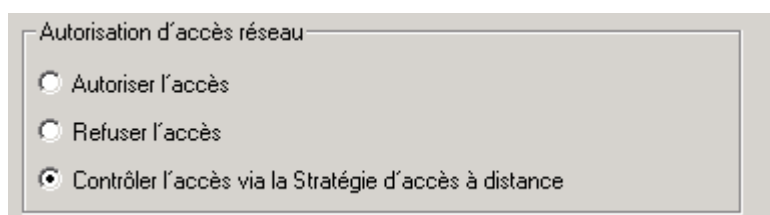
# Déroulé de l'installation du serveur RADIUS-NPS sur Windows 2008-R2 Server

## 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.

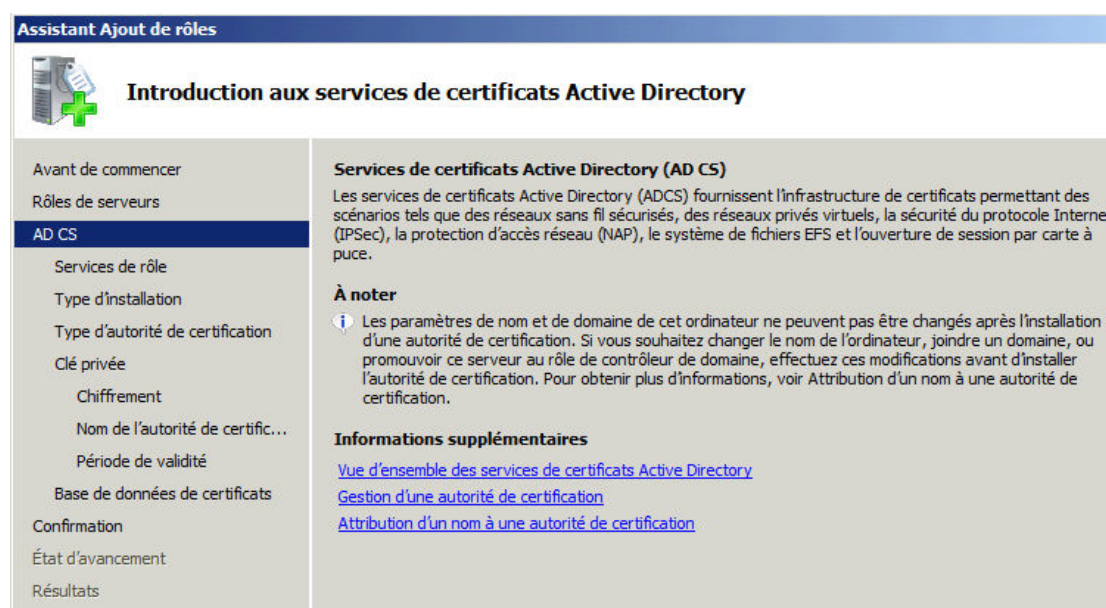


## I Ajout du rôle "Services de certificats Active Directory"

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.



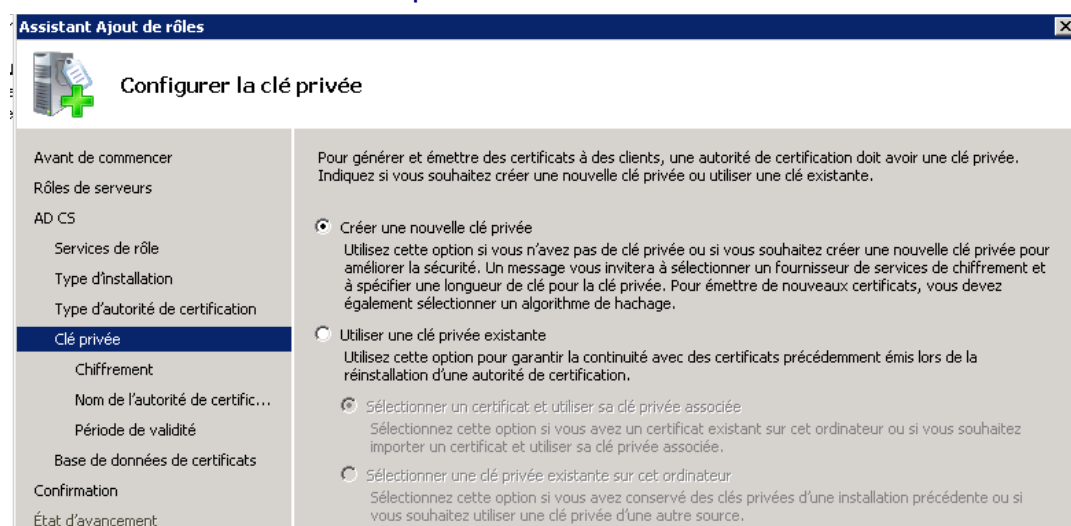
## On choisit une installation du type Autorité de certification d'entreprise...



## ... 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

**Assistant Ajout de rôles**

**Configurer le chiffrement pour l'autorité de certification**

Avant de commencer  
Rôles de serveurs  
AD CS  
Services de rôle  
Type d'installation  
Type d'autorité de certification  
Clé privée  
**Chiffrement**  
Nom de l'autorité de certific...  
Période de validité  
Base de données de certificats  
Confirmation

Pour créer une nouvelle clé privée, vous devez d'abord sélectionner un [fournisseur de services de chiffrement](#), un [algorithme de hachage](#) et une longueur de clé adaptée à l'utilisation prévue des certificats que vous émettez. La sélection d'une valeur élevée pour la longueur de clé donnera une sécurité renforcée, mais allongera les opérations de signature.

Sélectionnez un fournisseur de services de chiffrement : RSA#Microsoft Software Key Storage Provider Longueur de la clé en caractères : 2048

Sélectionnez l'algorithme de hachage pour la signature des certificats émis par cette autorité de certification : SHA256, SHA384, SHA512

☐ Autoriser l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

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

**Assistant Ajout de rôles**

**Configurer le nom de l'autorité de certification**

Avant de commencer  
Rôles de serveurs  
AD CS  
Services de rôle  
Type d'installation  
Type d'autorité de certification  
Clé privée  
Chiffrement  
**Nom de l'autorité de certific...**  
Période de validité  
Base de données de certificats  
Confirmation

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Des valeurs de suffixe de nom uniques sont automatiquement générées mais ne peuvent pas être modifiées.

Nom commun de cette autorité de certification : MARS-2008-CA

Suffixe du nom unique : DC=SIO,DC=local

Aperçu du nom unique : CN=MARS-2008-CA,DC=SIO,DC=local

## → On laisse la période de validité par défaut ...

**Assistant Ajout de rôles**

**Période de validité du certificat**

Avant de commencer  
Rôles de serveurs  
AD CS  
Services de rôle  
Type d'installation  
Type d'autorité de certification  
Clé privée  
Chiffrement  
Nom de l'autorité de certific...

Un certificat sera émis par cette autorité de certification pour sécuriser les communications avec d'autres autorités de certification et avec des clients demandant des certificats. La période de validité d'un certificat d'autorité de certification peut être basée sur un certain nombre de facteurs, notamment la fonction prévue de l'autorité de certification et les mesures de sécurité que vous avez instaurées pour sécuriser l'autorité de certification.

Sélectionnez la période de validité du certificat généré par cette autorité de certification : 5 Années

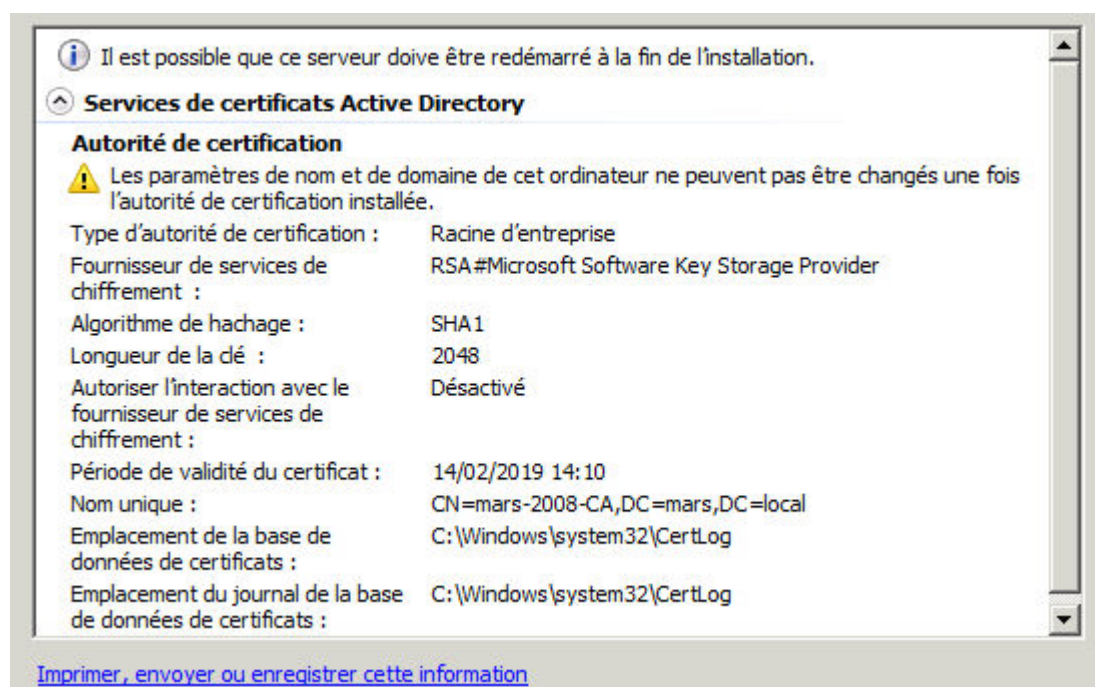
Date d'expiration de l'autorité de certification : 01/02/2019 08:41

Notez qu'une autorité de certification n'émettra des certificats valides que jusqu'à sa date d'expiration.

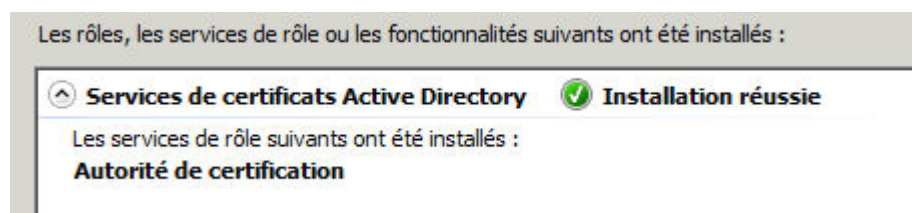
... ainsi que l'emplacement d'installation de la base de données de certificats



Écran récapitulatif des choix avant installation de l'autorité :

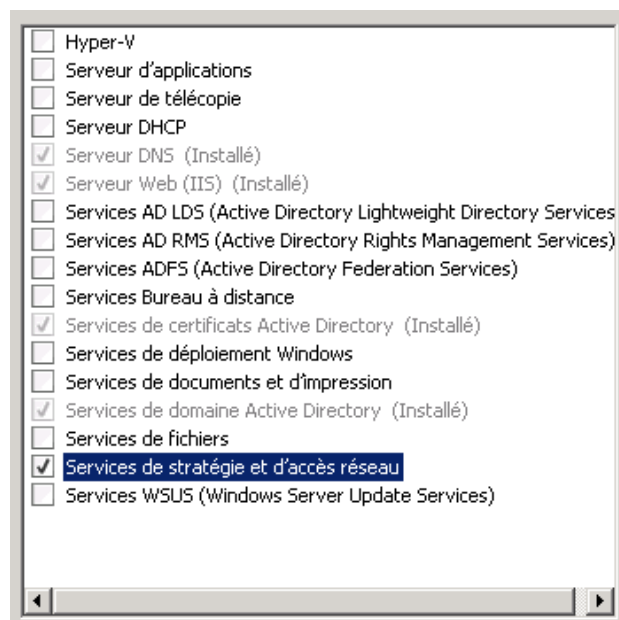


Écran témoin de la réussite de l'installation de l'autorité de certification (AC).



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

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

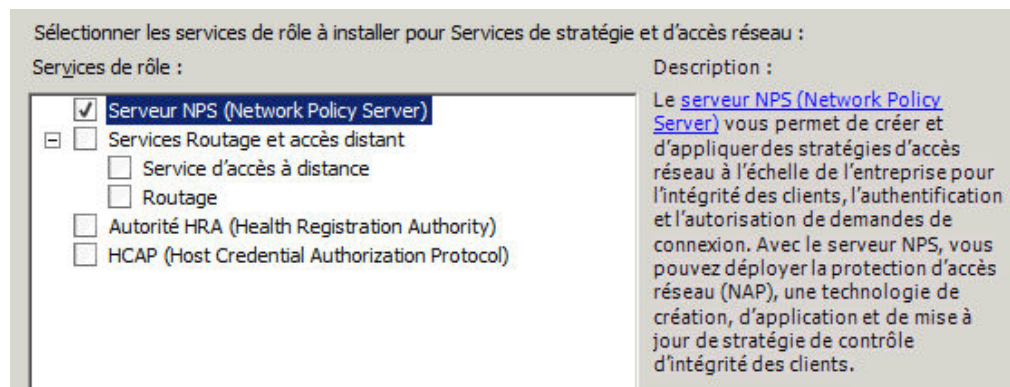


Suit un écran d'informations :

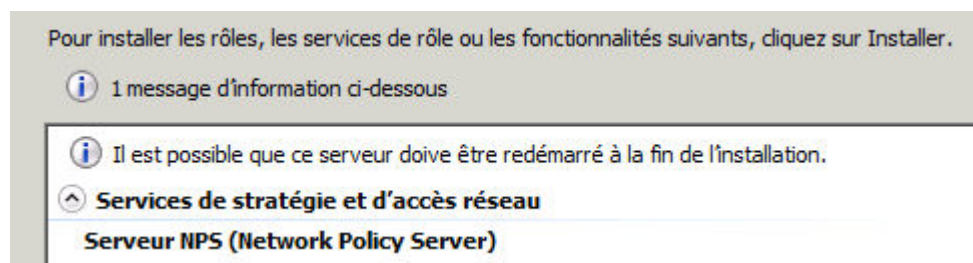
Avant de commencer	<b>Introduction aux services de stratégie et d'accès réseau</b> Les services de stratégie et d'accès réseau vous permettent de fournir un accès réseau local et distant, ainsi que de définir et d'appliquer des stratégies pour l'authentification d'accès réseau, l'autorisation et l'intégrité des clients à l'aide du serveur NPS (Network Policy Server), du service de routage et accès distant, de l'autorité HRA (Health Registration Authority) et du protocole HCAP (Host Credential Authorization Protocol).  <b>À noter</b> <ul style="list-style-type: none"><li>Vous pouvez déployer NPS comme un serveur et un proxy RADIUS (Remote Authentication Dial-In User Service), et comme un serveur de stratégie de protection d'accès réseau (NAP). Après l'installation du serveur NPS au moyen de cet Assistant, vous pouvez configurer NPS à partir de la page d'accueil NPAS en utilisant la console NPS.</li><li>La protection d'accès réseau (NAP) vous aide à garantir que les ordinateurs se connectant au réseau sont compatibles avec les stratégies d'intégrité du réseau et des clients de l'organisation. Après l'installation du serveur NPS à l'aide de cet Assistant, vous pouvez configurer NAP à partir de la page d'accueil NPAS en utilisant la console NPS.</li></ul> <b>Informations supplémentaires</b> <a href="#">Composants des services de stratégie et d'accès réseau</a> <a href="#">Méthodes de contrainte de mise en conformité NAP</a> <a href="#">Protection d'accès réseau (NAP) dans NPS</a> <a href="#">Serveur NPS (Network Policy Server)</a>
Rôles de serveurs	
<b>Stratégie et accès réseau</b>	
Services de rôle	
Confirmation	
État d'avancement	
Résultats	



Choisir les services de rôle suivants :



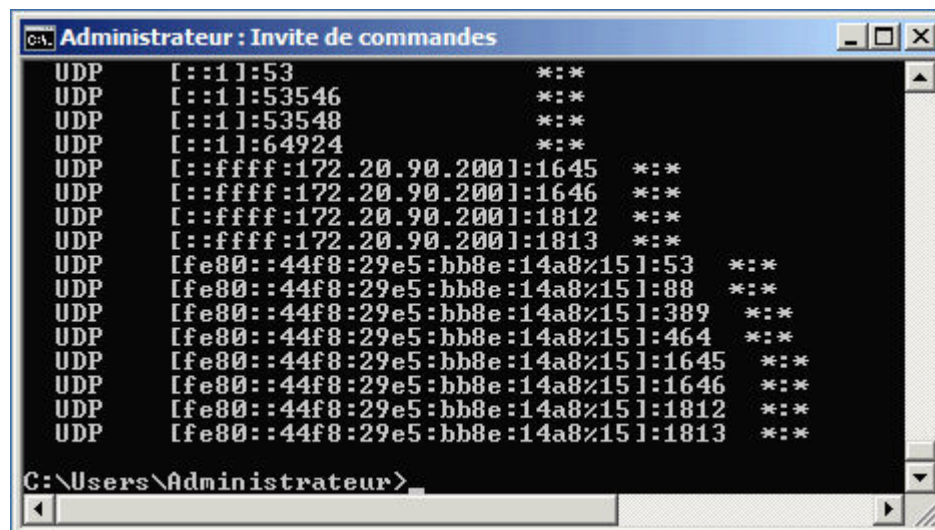
Écran récapitulatif des choix d'installation de NPS et témoin de réussite



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 `netstat -a` : voir les 4 dernières lignes.

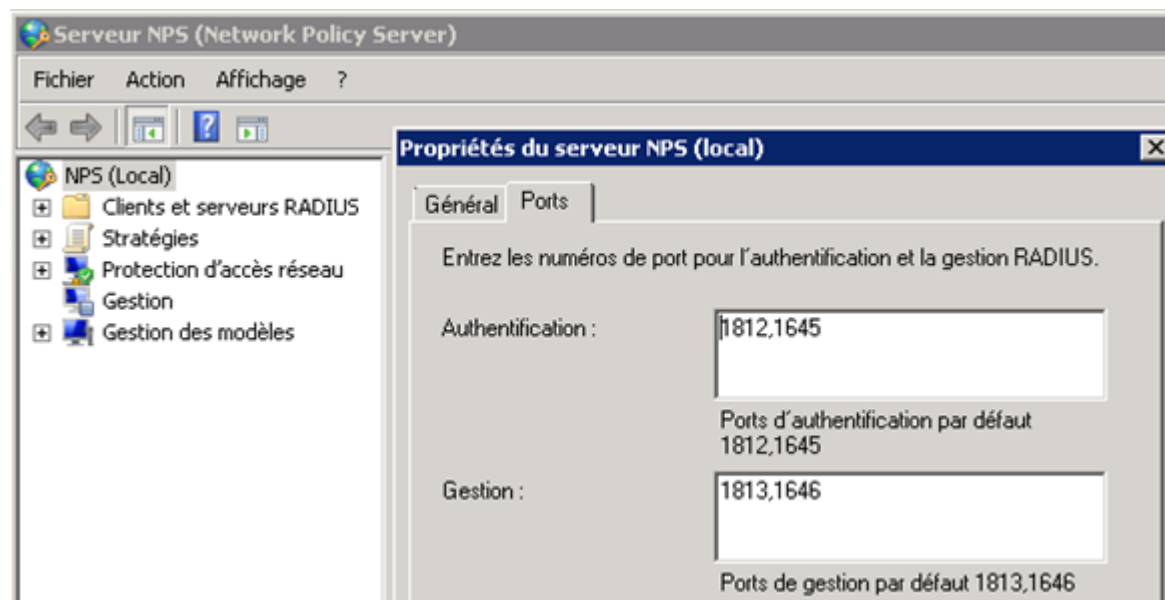


NPS écoute sur les ports suivants par défaut :

- 1812, 1645 pour l'authentification.
- 1813, 1646 pour la gestion.

Note

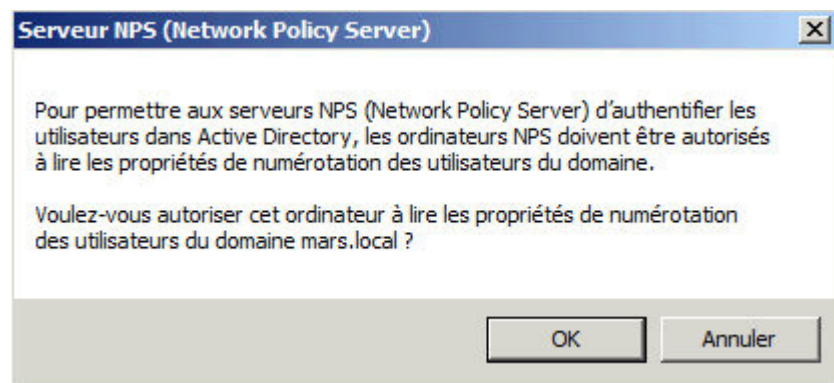
On peut retrouver ces ports dans les propriétés du serveur NPS (à chercher dans les outils d'administration ou dans le service de rôle) :



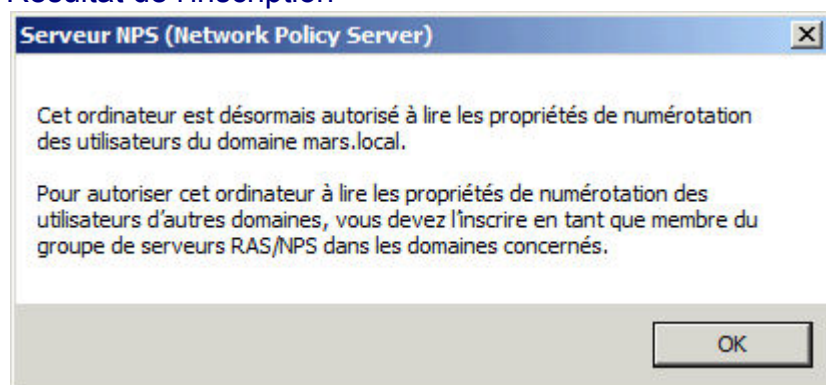


### III CONFIGURATION DU SERVEUR RADIUS NPS

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



Résultat de l'inscription



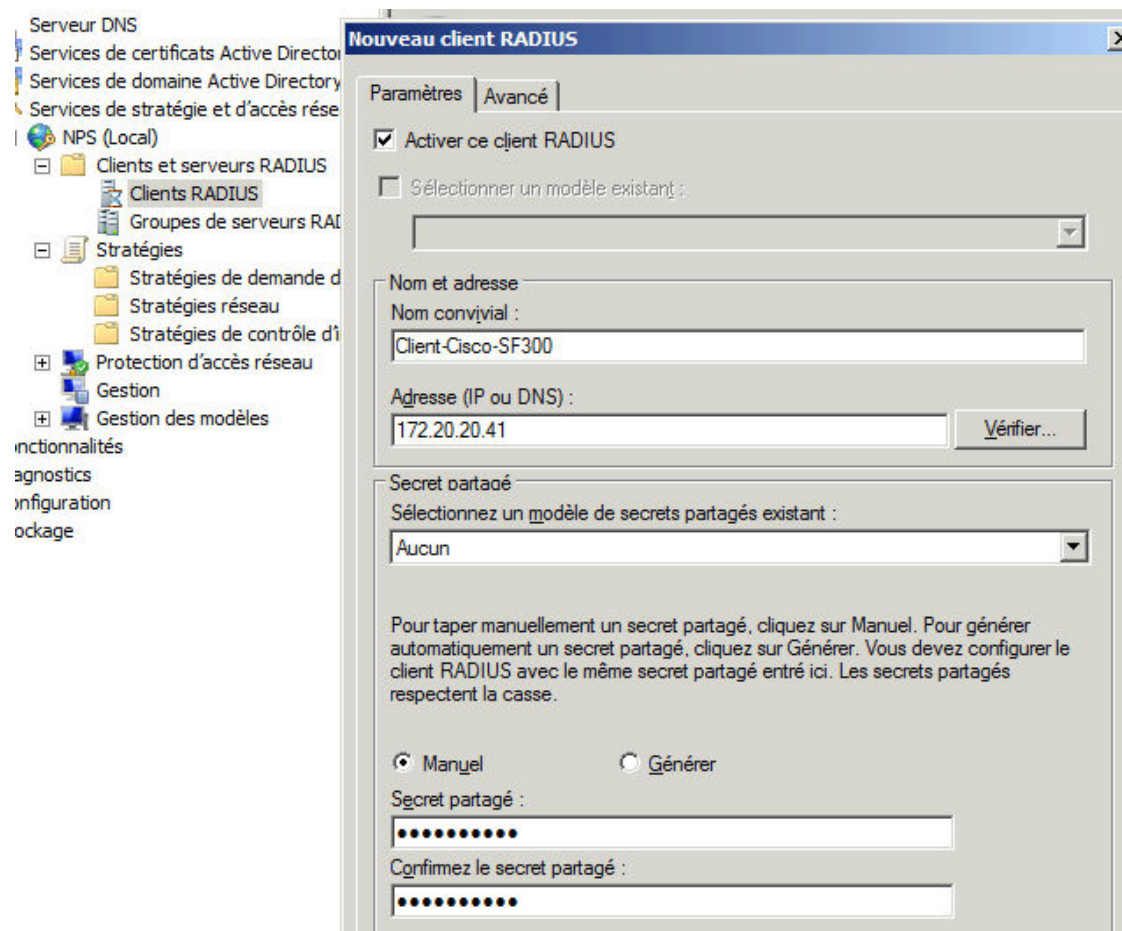
Note : un assistant global est disponible. On va plutôt détailler chaque phase.

#### 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".

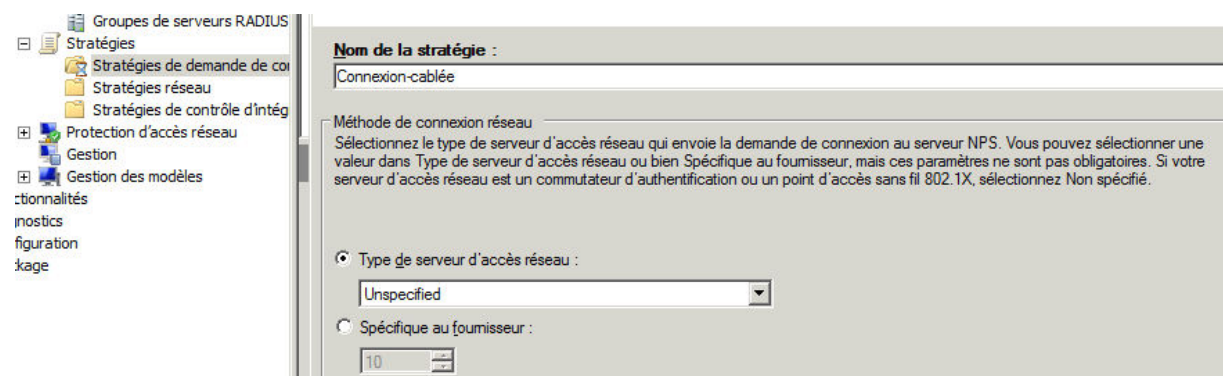
Cette chaîne doit évidemment être identique à celle déclarée dans le client radius, c'est-à-dire le commutateur Cisco. Il s'agit d'un secret partagé entre deux éléments d'infrastructure, avec une exigence de sécurité moins importante qu'un accès "depuis un poste client". Il y a peu de chance qu'un élément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

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



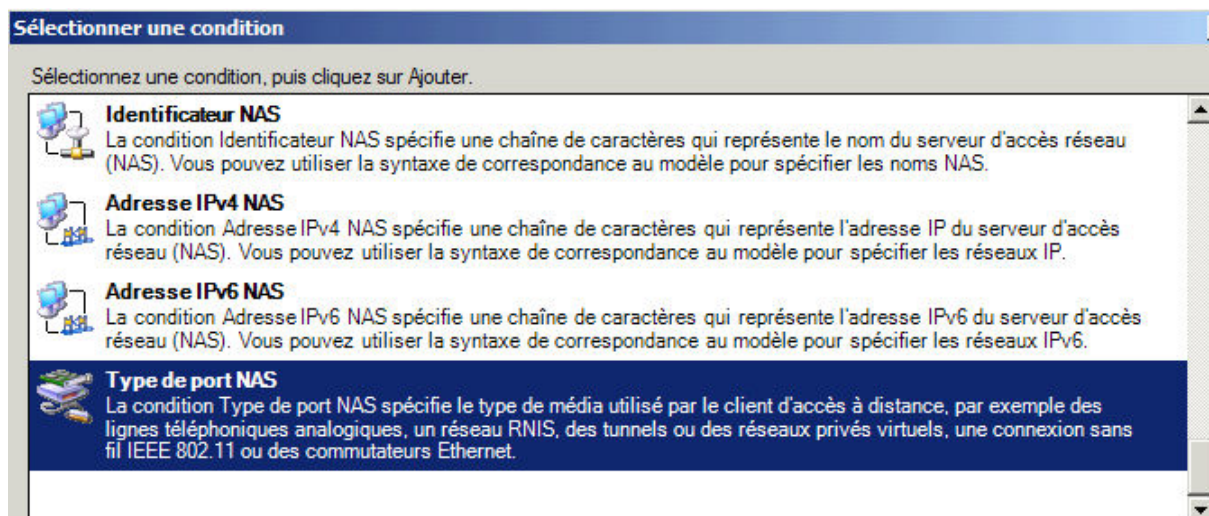
## 2. Déclaration d'une stratégie de demande de connexion

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



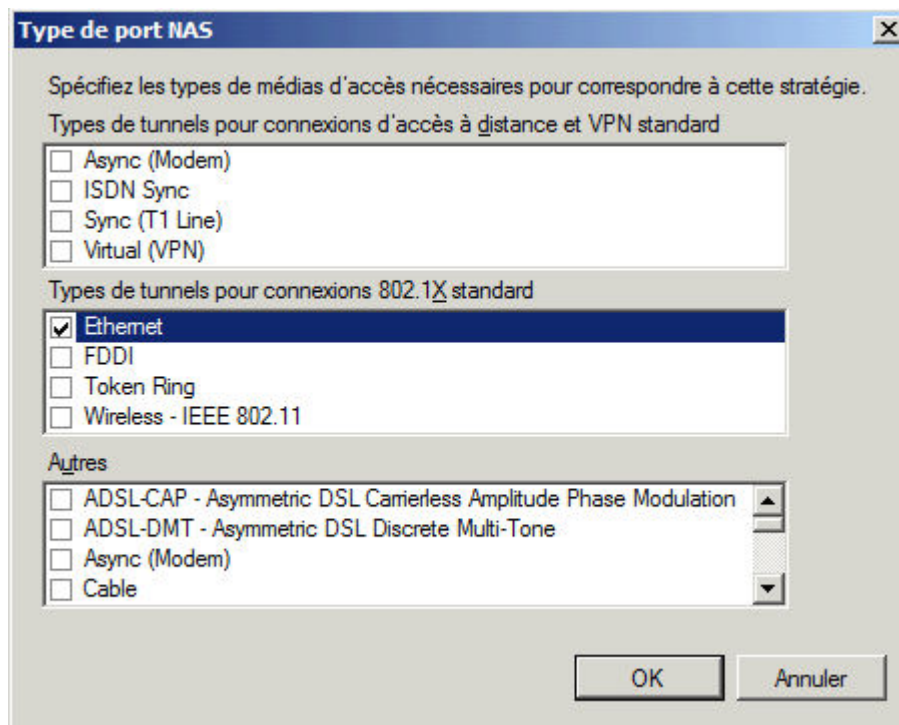
Ici, on choisit un nom de stratégie. On laisse le type de serveur sur "Unspecified" (nous utilisons un commutateur en tant que client Radius).

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 :

Conditions :	
Condition	Valeur
 Type de port NAS	Ethernet

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

**Nouvelle stratégie de demande de connexion**

 **Spécifier le transfert de la demande de connexion**

La demande de connexion peut être authentifiée par le serveur local ou être transférée aux serveurs RADIUS d'un groupe de serveurs RADIUS distants.

Si la demande de connexion correspond aux conditions de la stratégie, ces paramètres sont appliqués.

**Paramètres :**

**Transfert de la demande de connexion**

- **Authentification**
- Gestion

Spécifiez si les demandes de connexion sont traitées localement, si elles sont transférées à des serveurs RADIUS distants pour authentification, ou si elles sont acceptées sans authentification.

☒ Authentifier les demandes sur ce serveur


☐ Transférer les demandes au groupe de serveurs RADIUS distants suivant pour authentification :

<non configurée>

☐ Accepter les utilisateurs sans validation des informations d'identification

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.

**Nouvelle stratégie de demande de connexion**

 **Spécifier les méthodes d'authentification**

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP. Si vous déployez la protection d'accès réseau (NAP) avec une connexion 802.1X ou VPN, vous devez configurer le protocole PEAP (Protected EAP).

☐ Remplacer les paramètres d'authentification de stratégie réseau

Ces paramètres d'authentification sont utilisés à la place des contraintes et des paramètres d'authentification de la stratégie réseau. Pour les connexions VPN et 802.1X avec la protection d'accès réseau (NAP), vous devez configurer l'authentification PEAP ici.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

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

The screenshot shows a window titled 'Nouvelle stratégie de demande de connexion' with a sub-header 'Configurer les paramètres'. Below the title bar, there is a small icon of a computer and the text: 'Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.' Below this, a paragraph states: 'Configurez les paramètres de cette stratégie réseau. Si la demande de connexion répond aux conditions et si la stratégie accorde l'accès, les paramètres sont appliqués.'

The 'Paramètres' section is divided into two main areas. On the left, under 'Spécifier un nom de domaine', there is a tree view with 'Attribut' selected. Below it, 'Attributs RADIUS' is expanded, showing 'Standard' and 'Spécifiques au fournisseur'. On the right, there is a section for 'Sélectionnez les attributs auxquels les règles suivantes seront appliquées. Les règles sont traitées selon leur ordre d'apparition dans la liste.' Below this, there is a dropdown menu for 'Attribut' with 'ID de la station appelée' selected. Below the dropdown, there is a table for 'Règles' with columns 'Rechercher' and 'Remplacer par'. To the right of the table are buttons: 'Ajouter', 'Modifier', 'Supprimer', 'Monter', and 'Descendre'.

---

Écran récapitulatif de la stratégie de demande de connexion

The screenshot shows a window titled 'Nouvelle stratégie de demande de connexion' with a sub-header 'Fin de l'Assistant Stratégie de demande de nouvelle connexion'. Below the title bar, there is a small icon of a computer. Below the icon, there is a paragraph: 'Vous avez créé la stratégie de demande de connexion suivante :'. Below this, there is a section titled 'Connexion-cablée'. Below this, there is a section titled 'Conditions de la stratégie :'. Below this, there is a table with two columns: 'Condition' and 'Valeur'. The table contains one row: 'Type de port NAS' and 'Ethernet'. Below this, there is a section titled 'Paramètres de la stratégie :'. Below this, there is a table with two columns: 'Condition' and 'Valeur'. The table contains one row: 'Fournisseur d'authentification' and 'Ordinateur local'.

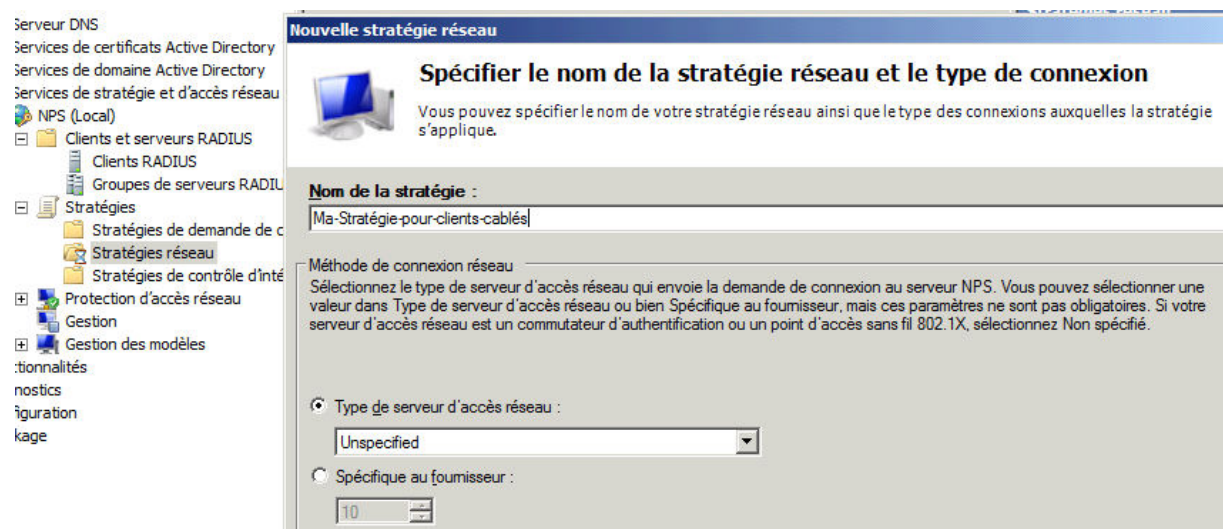


### 3. Déclaration d'une stratégie réseau (stratégie d'accès au réseau)

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.

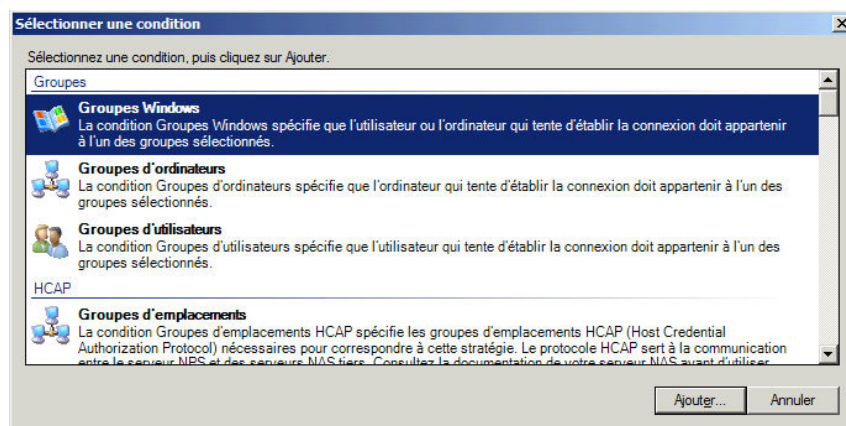
Note : Si on veut placer les membres du groupe "Handball" dans un VLAN 3, on créera une autre stratégie d'accès réseau. On peut donc avoir un catalogue de stratégies d'accès réseau, pour une seule stratégie de demande de connexion.

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.

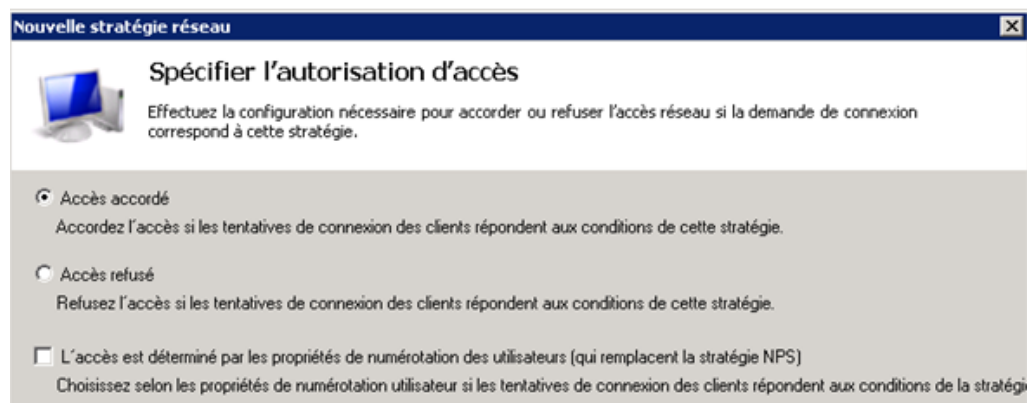


---

## Récapitulatif du choix des groupes Windows

	Condition	Valeur
	Groupes Windows	MARS\escrime

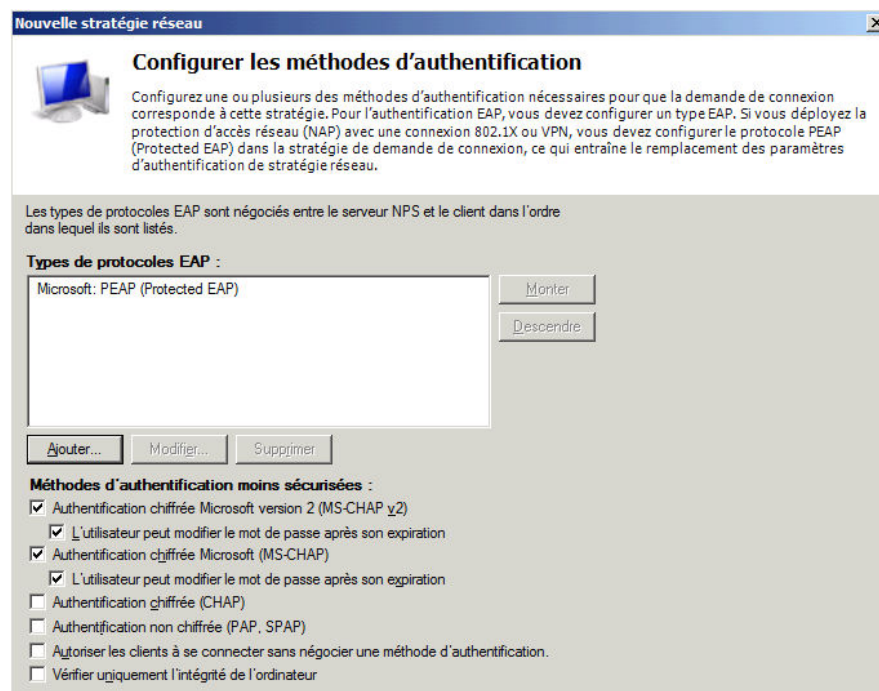
---



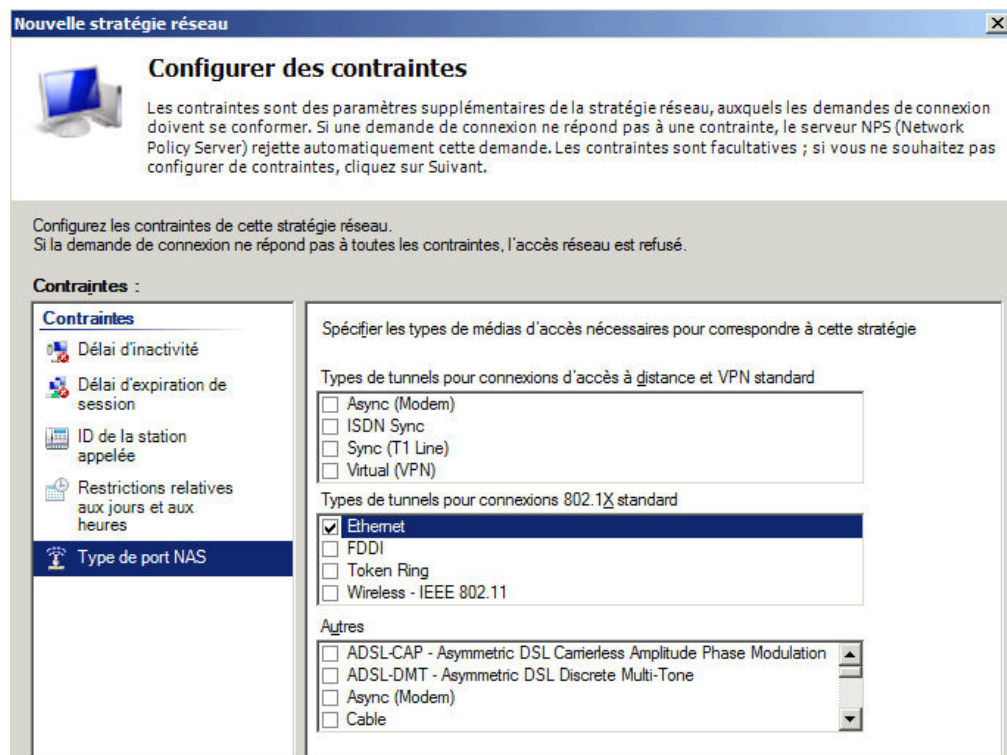
On peut définir des stratégies autorisant l'accès quand les conditions sont réunies ou, à l'inverse, interdisant l'accès lorsque les conditions sont réunies (un groupe d'utilisateur en congé par exemple).

---

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

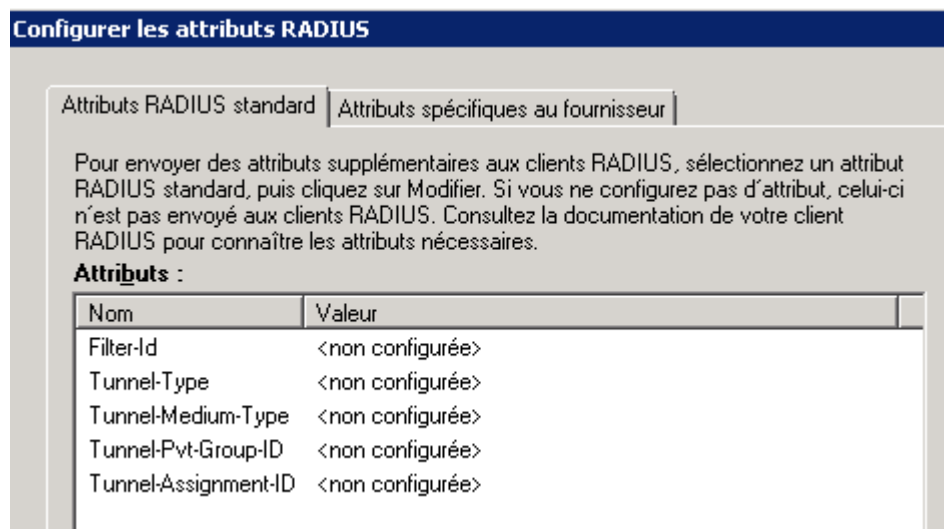


→ On accepte les Types de ports NAS Ethernet



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.

The screenshot shows a dialog box titled "Informations d'attribut". It contains the following fields and options:

- Nom de l'attribut : Tunnel-Type
- Numéro de l'attribut : 64
- Format de l'attribut : Enumerator
- Valeur d'attribut :
  - ☐ Communément utilisé pour les connexions d'accès à distance ou VPN (with a dropdown menu showing "<Aucun>")
  - ☒ Communément utilisé pour les connexions 802.1x (with a dropdown menu showing "Virtual LANs (VLAN)")
  - ☐ Autres (with a dropdown menu showing "<Aucun>")

Buttons: OK, Annuler

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

The screenshot shows a dialog box titled "Informations d'attribut". It contains the following fields and options:

- Nom de l'attribut : Tunnel-Medium-Type
- Numéro de l'attribut : 65
- Format de l'attribut : Enumerator
- Valeur d'attribut :
  - ☒ Communément utilisé pour les connexions 802.1x (with a dropdown menu showing "802 (includes all 802 media plus Ethernet canonical format)")
  - ☐ Autres (with a dropdown menu showing "<Aucun>")

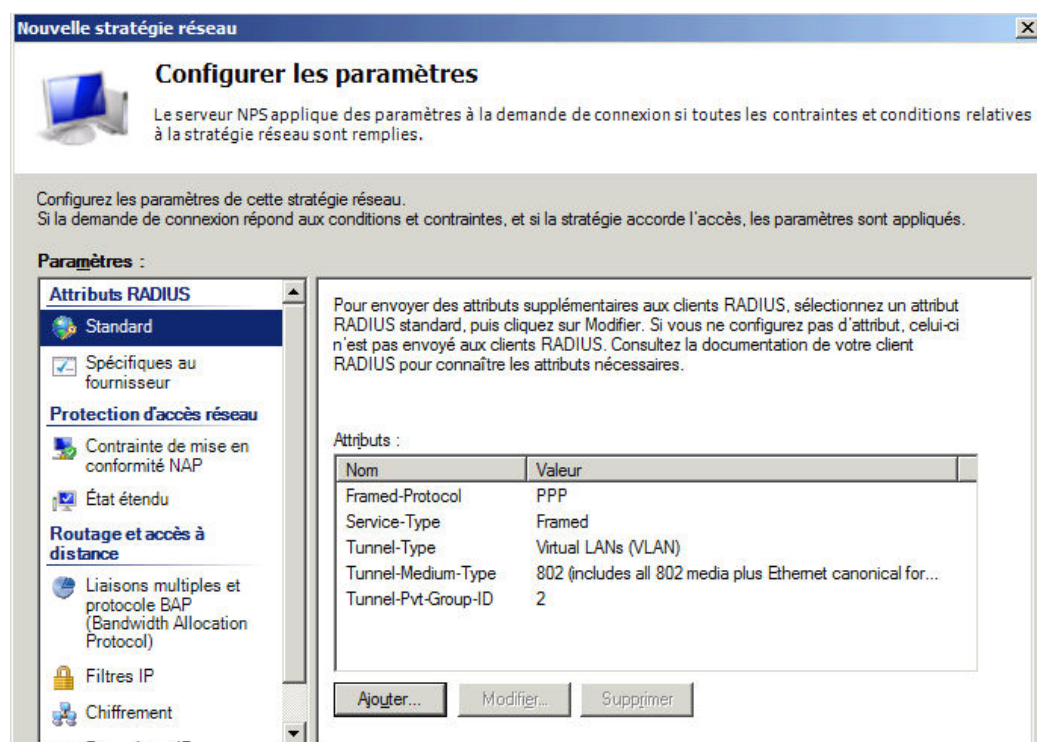
Enfin "Tunnel-Pvt-Group-ID" sur le numéro de VLAN dans lequel on veut positionner les membres du groupe d'utilisateurs "escrime" : pour nous le VLAN 2.

The screenshot shows a dialog box titled "Informations d'attribut". It contains the following fields and options:

- Nom de l'attribut : Tunnel-Pvt-Group-ID
- Numéro de l'attribut : 81
- Format de l'attribut : OctetString
- Entrez la valeur d'attribut dans :
  - ☒ Chaîne
  - ☐ Hexadécimal

Input field: 2

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



## FIN

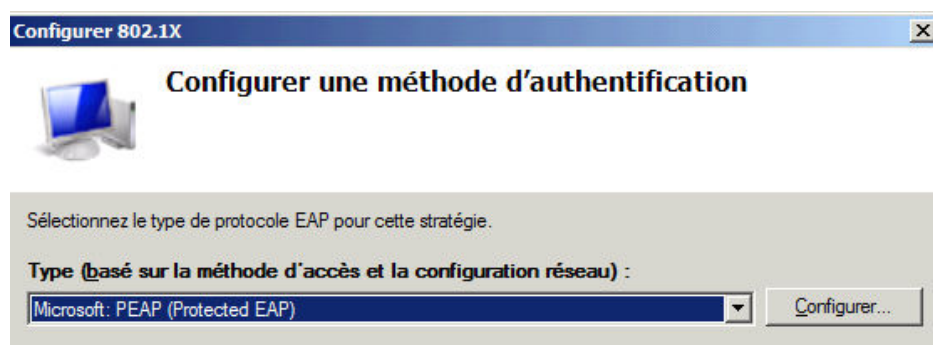
On a donc défini une stratégie d'accès réseau Ethernet 802.1x plaçant dans le VLAN2 les membres authentifiés comme faisant partie du groupe "escrime", vérifiée par la collaboration du serveur NPS avec le client RADIUS, commutateur d'IP 172.20.20.41.

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

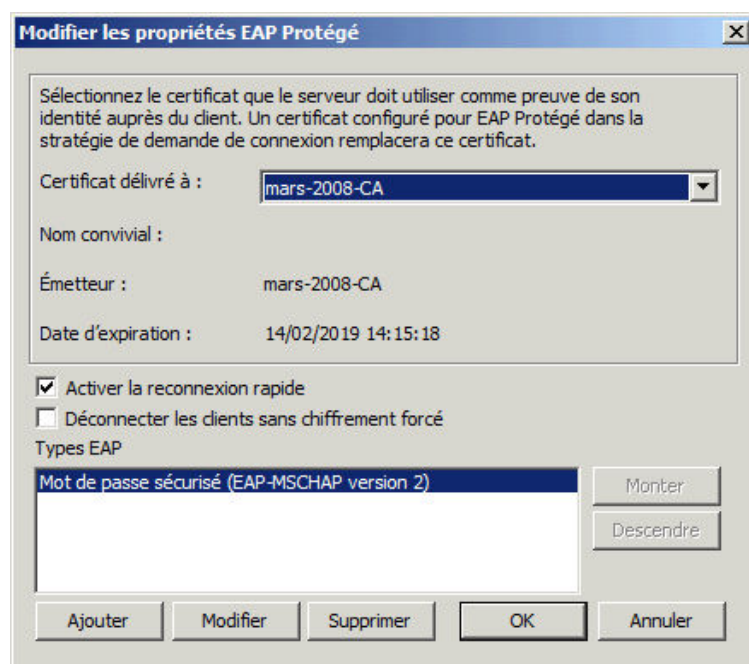
- Stratégie de demande de connexion associée aux connexions filaire Ethernet
- Stratégie réseau (accès au réseau)
- Précisant le groupe autorisé (escrime)
  - ➔ notion de conditions
- Précisant la méthode d'authentification (PEAP/MSCHAPV2)
  - ➔ notion de propriété
- Associant avec la stratégie de demande de connexion (NAS Ethernet)
  - ➔ notion de contrainte
- Précisant les paramètres renvoyés au client radius (VLAN)
  - ➔ notion d'attributs



Note : si nous avons 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'évènement : 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 :	-