

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from this bar, containing the date.

29/03/2016

# Procédure de mise en place d'un serveur RADIUS

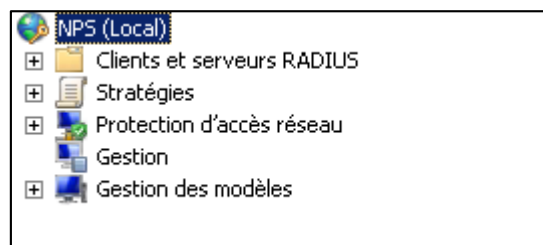
Several thin, curved lines in dark blue and light grey originate from the bottom left and sweep upwards and to the right.

LAMBERT Kevin

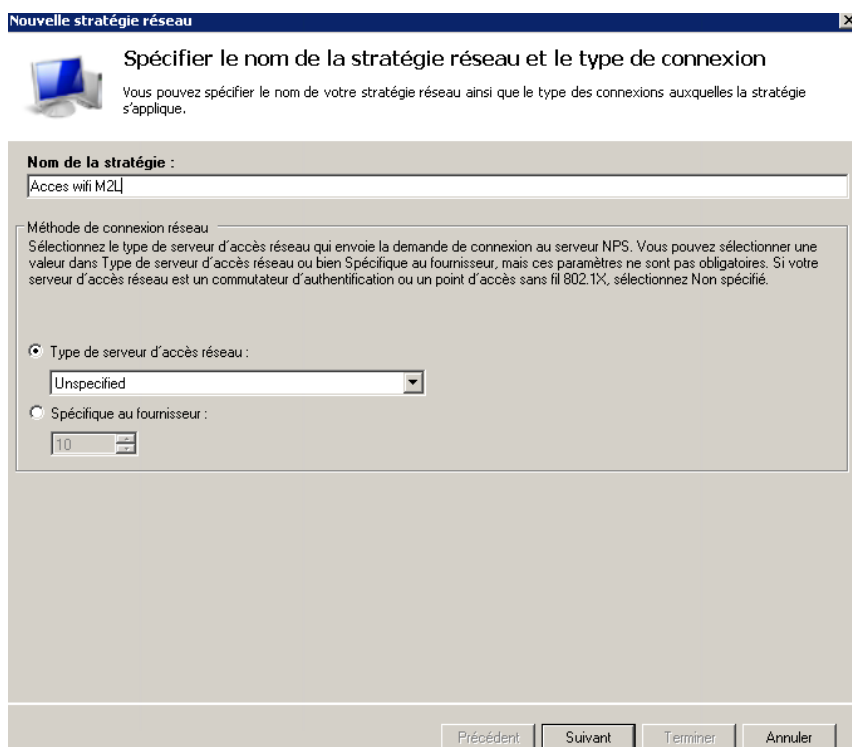


# Procédure de paramétrage d'un serveur Radius

Après l'installation de du rôle, il faut se rendre dans « Outils d'administration » et ouvrir « Serveur NPS ».

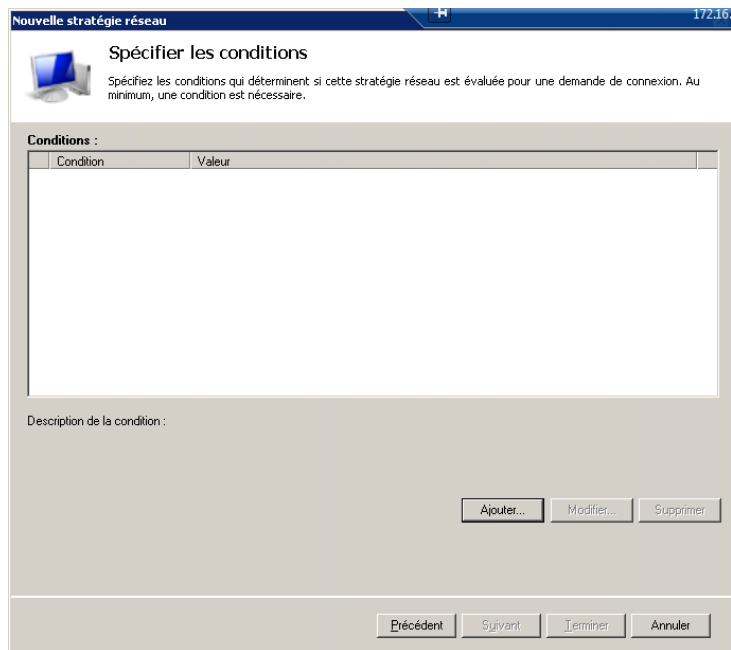


Dans « Stratégies », « Stratégies Réseau » :

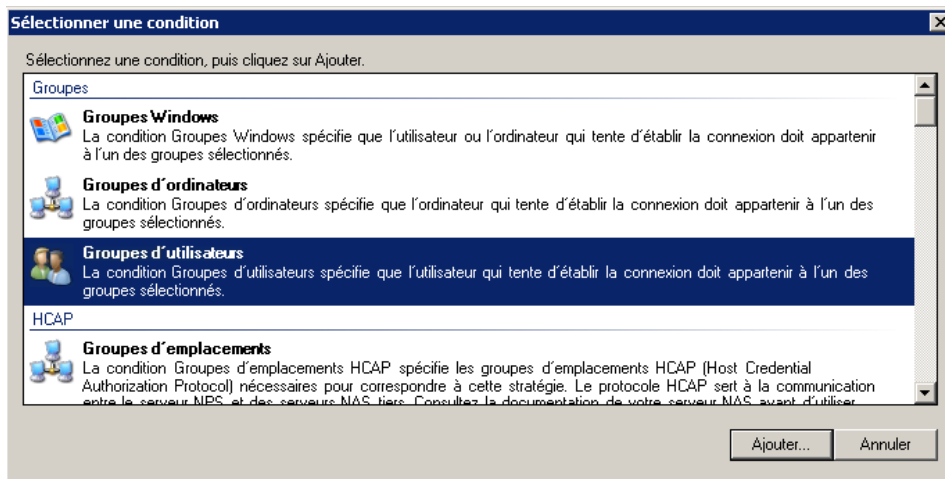
A screenshot of the 'Nouvelle stratégie réseau' (New Network Policy) wizard. The window title is 'Nouvelle stratégie réseau'. The main heading is 'Spécifier le nom de la stratégie réseau et le type de connexion'. Below this, a text box says: 'Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.' The 'Nom de la stratégie' field contains the text 'Accès wifi M2L'. Below this is the 'Méthode de connexion réseau' section. It contains a radio button for 'Type de serveur d'accès réseau' which is selected, and a dropdown menu showing 'Unspecified'. There is also a radio button for 'Spécifique au fournisseur' which is not selected, and a text box containing '10'. At the bottom of the window are four buttons: 'Précédent', 'Suivant', 'Terminer', and 'Annuler'.

Indiquer le nom de la stratégie, ici « Accès wifi M2L », et choisir « Unspecified » pour le type de serveur d'accès réseau.

Cliquer sur « Suivant ».



Cliquer sur « Ajouter ... »



Cliquer sur « Groupes d'utilisateurs » pour choisir a quels utilisateurs s'appliquera cette stratégie.

Cliquer sur « Suivant ».

**Nouvelle stratégie réseau**

### Spécifier l'autorisation d'accès

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

☒ **Accès accordé**  
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ **Accès refusé**  
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ **L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)**  
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

Laisser la case « Accès accordé » cochée et cliquer sur « Suivant ».

**Nouvelle stratégie réseau**

### Configurer 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) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.

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

**Types de protocoles EAP :**

**Ajouter des protocoles EAP**

Méthodes d'authentification :

- Microsoft : Carte à puce ou autre certificat
- Microsoft : PEAP (Protected EAP)
- Microsoft : Mot de passe sécurisé (EAP-MSCHAP version 2)**

OK Annuler

Ajouter... Modifier... Supprimer

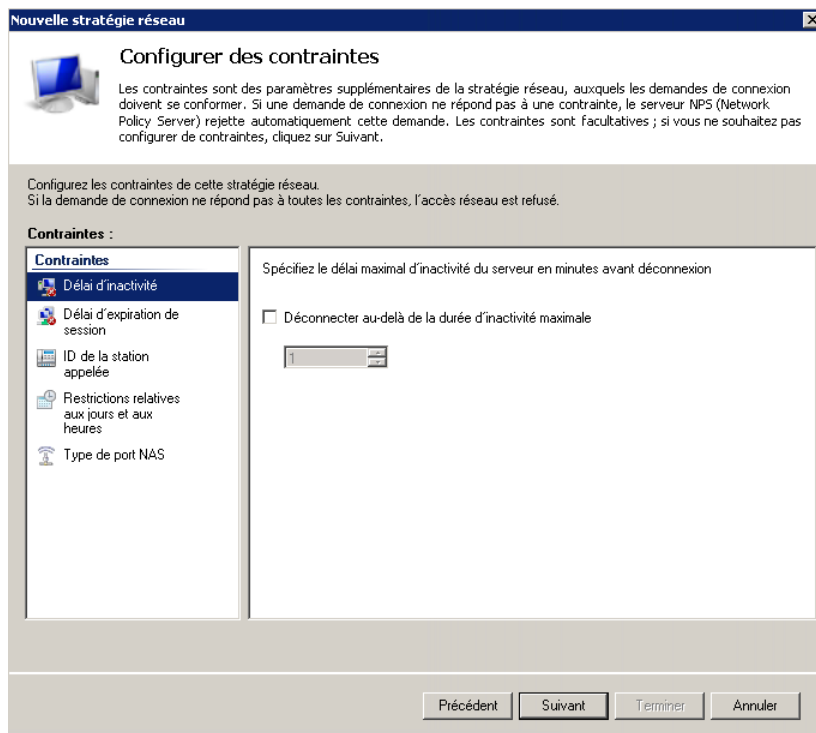
**Méthodes d'authentification moins sécurisées :**

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
  - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
  - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.
- ☐ Vérifier uniquement l'intégrité de l'ordinateur

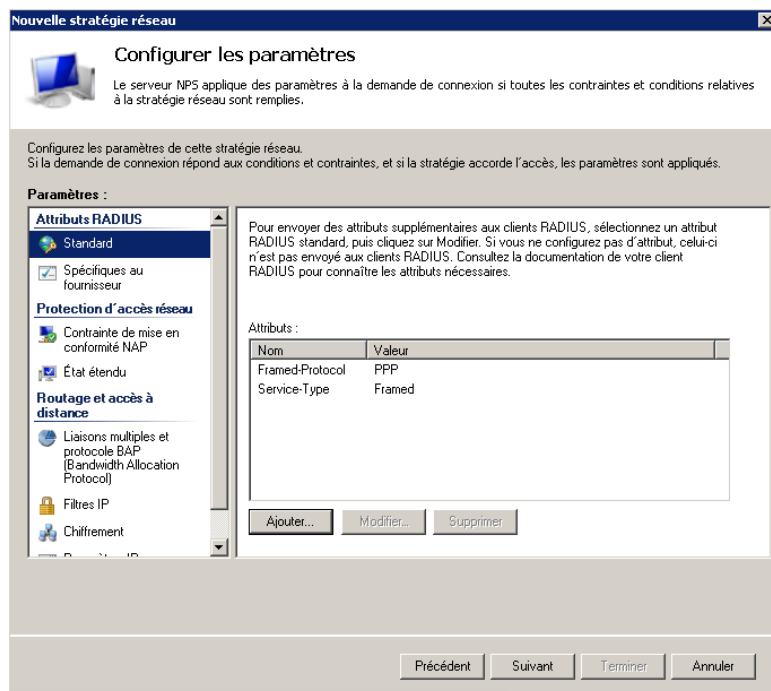
Précédent Suivant Terminer Annuler

Cliquer sur « Ajouter » puis sélectionner l'authentification « EAP- MSCHAP Version 2 ». Laisser les autres paramètres sans y toucher.

Cliquer sur « Suivant ».



Des contraintes peuvent être paramétrées mais ces paramètres pourront être modifiés ultérieurement.



De même, les options présentes ici ne seront pas configurées maintenant.

Cliquer sur suivant.

**Nouvelle stratégie réseau**

**Fin de la configuration de la nouvelle stratégie réseau**

Vous avez correctement créé la stratégie réseau suivante :

**Stratégie wifi M2L**

**Conditions de la stratégie :**

Condition	Valeur
Groupes d'utilisateurs	M2L\Tennis OU M2L\Foot OU M2L\Rugby OU M2L\Techniciens OU M2L\Administrateurs M2L

**Paramètres de la stratégie :**

Condition	Valeur
Méthode d'authentification	Protocole EAP OU MS-CHAP v1 OU MS-CHAP v1 (l'utilisateur peut modifier...)
Autorisation d'accès	Accorder l'accès
Mettre à jour les clients non conformes	Vrai
Contrainte de mise en conformité NAP	Autoriser un accès réseau complet
Framed-Protocol	PPP
Service-Type	Framed

Pour fermer cet Assistant, cliquez sur Terminer.

Précédent Suivant Terminer Annuler

Un récapitulatif des configurations apparaît. Cliquer sur « Terminer » pour valider la configuration.

**Propriétés de Stratégie wifi M2L**

Vue d'ensemble Conditions Contraintes Paramètres

Nom de la stratégie : Stratégie wifi M2L

**État de la stratégie**  
Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.

☒ Stratégie activée

**Autorisation d'accès**  
Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. Qu'est-ce qu'une autorisation d'accès ?

☒ Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.

☐ Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.

☐ Ignorer les propriétés de numérotation des comptes d'utilisateurs.  
Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.

**Méthode de connexion réseau**  
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :  
Unspecified

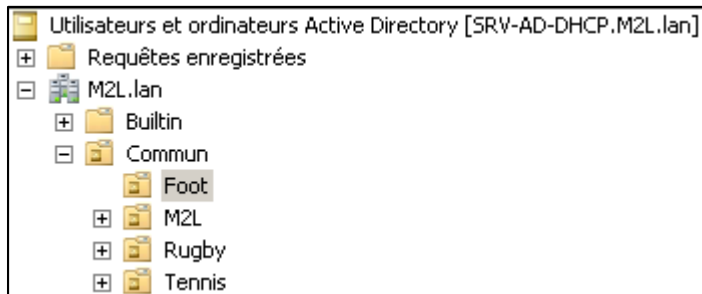
☐ Spécifique au fournisseur :  
10

OK Annuler Appliquer

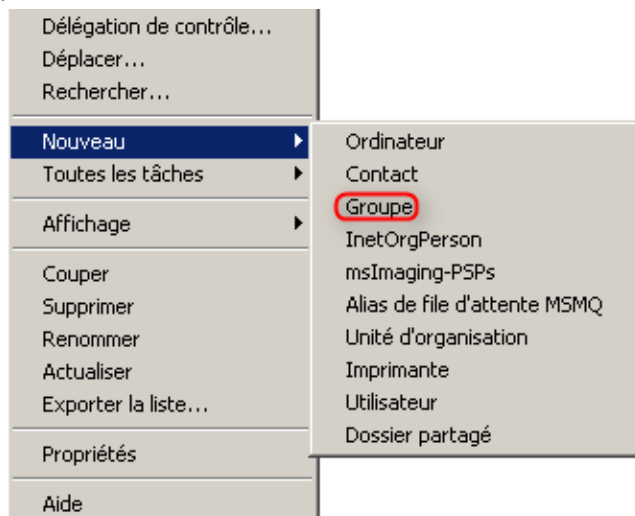
Vérifier que la case « Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie. » est cochée.

## Création de groupes dans l'AD :

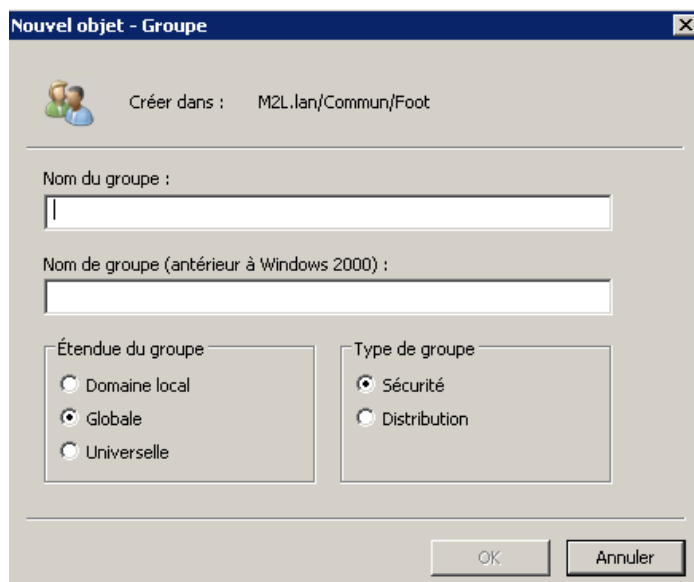
- Accéder à « Utilisateur et Ordinateur Active Directory »
- Accéder à l'OU dans laquelle sera créé le groupe.



- Cliquer droit sur l'OU et choisir « Nouveau » et sur « Groupe ».

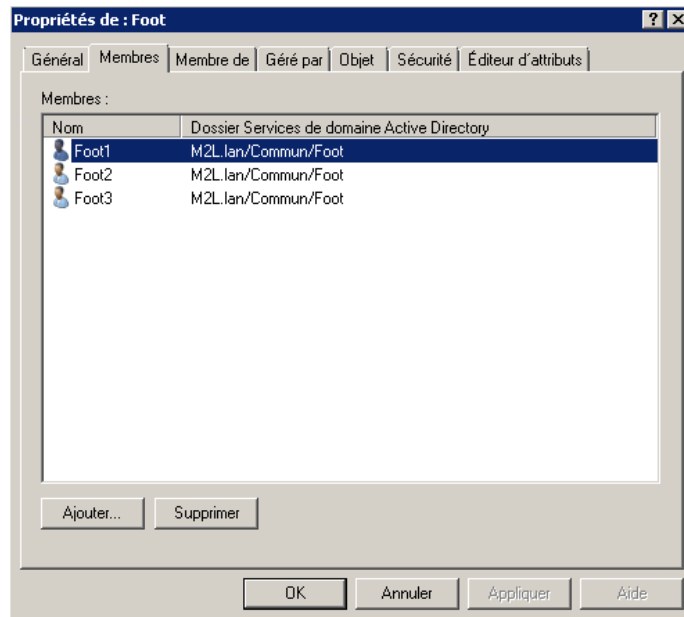


- Nommer le groupe.



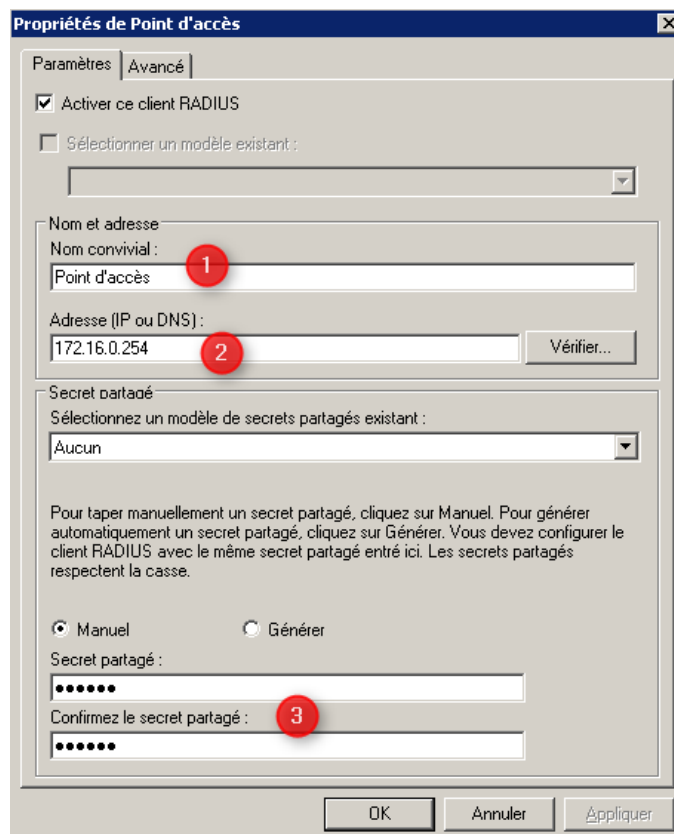
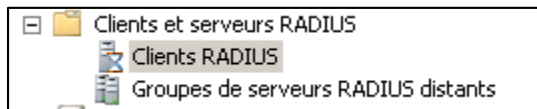


- Dans les propriétés du groupe, dans « Membre », « Ajouter » et ajouter les utilisateurs du groupe.



# Suite du paramétrage du serveur NPS

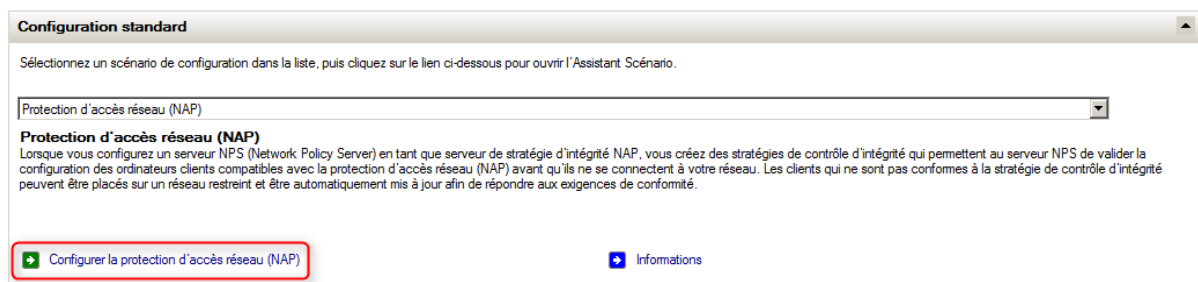
Dans « Clients et serveurs RADIUS » faire un clic droit sur « Clients RADIUS » et choisir « Nouveau ».



1. Entrer le nom du point d'accès.
2. Entrer l'adresse du point d'accès.
3. Entrer de mot de passe : SIO2016sisr

# Configuration de la protection d'accès réseau (NAP)

Pour la configuration de la protection d'accès réseau NAP, dans l'outil « serveur NPS », cliquer sur « Configurer la protection d'accès réseau (NAP) ».



Une fenêtre s'affiche, demandant une méthode de connexion réseau. Cliquer sur le menu déroulant et sélectionner « Protocole DHCP ».



La stratégie s'appellera « authent DHCP ».

Après cela, cliquer sur « Suivant ».

Ici, l'assistant de configuration demande de renseigner des clients RADIUS. Dans notre cas, le client RADIUS est le routeur du site ASSIZ. Une fenêtre nommée « Nouveau client RADIUS » s'ouvre.

**Configurer la protection d'accès réseau (NAP)**

**Spécifier les serveurs de contrainte de mise en conformité NAP exécutant Serveur DHCP**

Les clients RADIUS sont des serveurs d'accès réseau et non des ordinateurs clients. Si l'ordinateur local est un serveur DHCP, vous pouvez ignorer cette étape et cliquer sur Suivant.

Si vous souhaitez ajouter des serveurs DHCP distants en tant que clients RADIUS, cliquez sur Ajouter. Tous les serveurs DHCP distants que vous ajoutez doivent également être des serveurs NPS (Network Policy Server). En outre, les serveurs DHCP/NPS distants doivent transférer les demandes de connexion à ce serveur NPS (l'ordinateur local).

**Clients RADIUS :**

Ajouter...  
Modifier...  
Supprimer...

**Nouveau client RADIUS**

Paramètres

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial : routeur-Assiz

Adresse (IP ou DNS) : 172.25.0.25 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant : Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel ☐ Générer

Secret partagé : .....

Confirmez le secret partagé : .....

OK Annuler

Précédent Suivant Terminer Annuler

On donne donc un nom convivial au client RADIUS, ainsi que l'adresse IP de ce client. On choisit ensuite un secret partagé. C'est un mot de passe qu'il faudra renseigner dans le client RADIUS (le routeur ASSIZ) afin que celui-ci soit autorisé par le serveur.

Après avoir configuré le client RADIUS, cliquez sur « OK » puis sur « Suivant ». On peut choisir de configurer la protection NAP ou une certaine étendue d'adresse IP. Ici, on ne souhaite pas restreindre l'accès à une étendue particulière. On clique donc directement sur « Suivant ».

**Configurer la protection d'accès réseau (NAP)**

**Spécifier les étendues DHCP**

Lorsque vous spécifiez une ou plusieurs étendues NAP, le serveur NPS (Network Policy Server) évalue l'intégrité des clients et accorde l'accès aux ordinateurs clients qui demandent une adresse IP dans les étendues désignées.

Si vous ne spécifiez pas d'étendues, la stratégie s'applique à toutes les étendues NAP sur les serveurs DHCP sélectionnés. Si vous spécifiez une étendue qui ne prend pas en charge la protection d'accès réseau (NAP), vous devez activer la protection d'accès réseau (NAP) pour l'étendue souhaitée après avoir terminé l'exécution de cet Assistant.

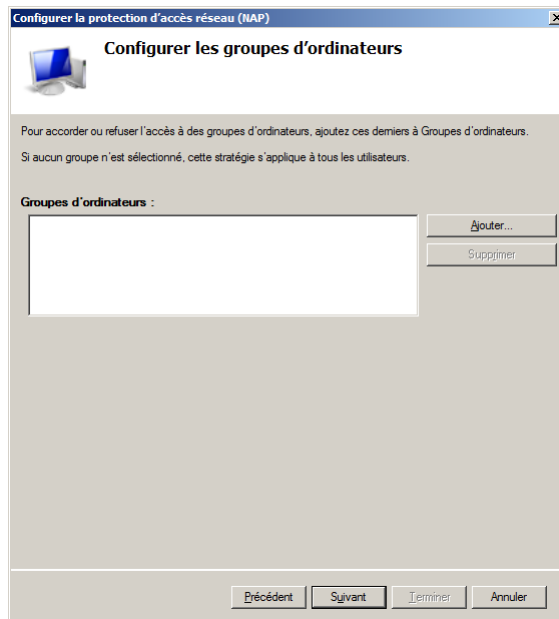
Pour spécifier une ou plusieurs étendues, cliquez sur Ajouter.

**Étendues DHCP :**

Ajouter...  
Modifier...  
Supprimer...

Précédent Suivant Terminer Annuler

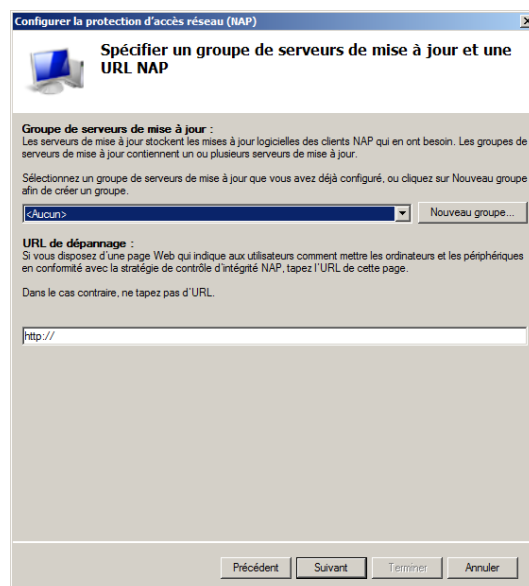
De même, la fenêtre suivante propose de restreindre l'accès à un certain groupe d'utilisateurs. On ne souhaite pas non plus ajouter cette option. Cliquer sur « Suivant ».



The screenshot shows a window titled "Configurer la protection d'accès réseau (NAP)" with a close button (X). The main heading is "Configurer les groupes d'ordinateurs". Below the heading, there is a small icon of a computer. The text explains that for granting or denying access to groups of computers, they must be added to the "Groupes d'ordinateurs" list. It also states that if no group is selected, the strategy applies to all users. There is a large empty rectangular box for the "Groupes d'ordinateurs". To the right of this box are two buttons: "Ajouter..." and "Supprimer". At the bottom of the window are four buttons: "Précédent", "Suivant", "Terminer", and "Annuler".

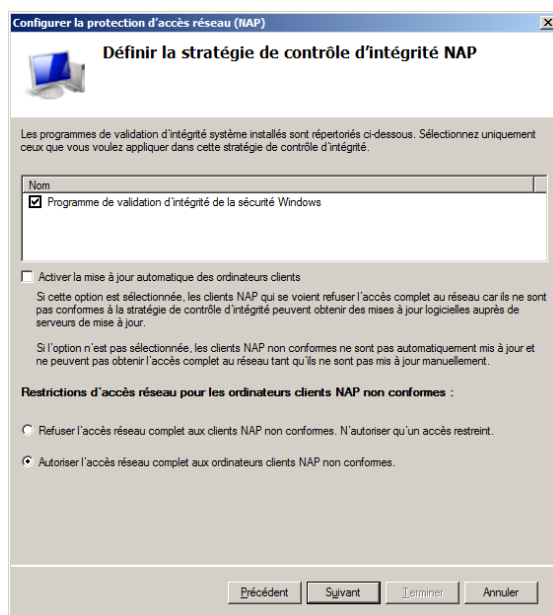
L'assistant permet aussi d'indiquer un serveur de mise à jour pour les postes qui s'authentifient sur le client RADIUS. On peut aussi indiquer une URL vers une page d'aide pour les utilisateurs.

Ne pas prendre en compte ces deux options et cliquer sur « Suivant ».



The screenshot shows a window titled "Configurer la protection d'accès réseau (NAP)" with a close button (X). The main heading is "Spécifier un groupe de serveurs de mise à jour et une URL NAP". Below the heading, there is a small icon of a computer. The text explains that NAP servers store updates for NAP clients that need them. It asks the user to select a group of servers from a dropdown menu. The dropdown menu currently shows "[Aucun]" and has a "Nouveau groupe..." button next to it. Below this, there is a section for "URL de dépannage" (troubleshooting URL), which is a text field for entering a URL. At the bottom of the window are four buttons: "Précédent", "Suivant", "Terminer", and "Annuler".

Sur la fenêtre suivante, il faut décocher la case « Activer la mise à jour automatique des ordinateurs clients ».



Il faut également sélectionner la case « Autoriser l'accès réseau complet aux ordinateurs clients NAP non conforme ». Cliquer sur « Suivant ».

La dernière fenêtre affiche un résumé de la configuration. Cliquer sur « Terminer » pour finir la configuration.

