SOMMAIRE AD

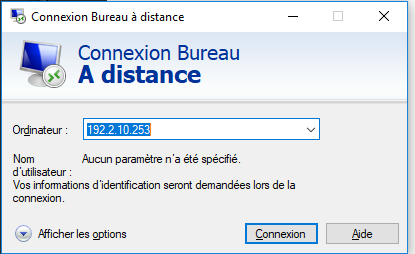
[**Installation Logiciel par GPO**](#_heading=h.fs8d3bwsua5r) **2**

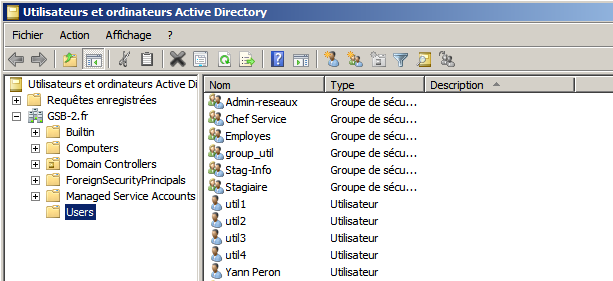
[**Création Utilisateurs et Groupe Via Powershell**](#_heading=h.d8weqojepphd) **6**

[**Création Radius**](#_heading=h.4sb8xj2nhp5q) **9**

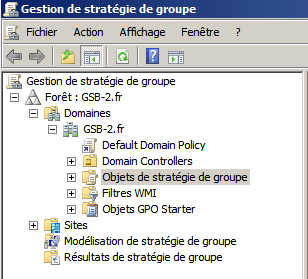
# Installation Logiciel par GPO

1- Connexion via le bureau à distance au serveur AD

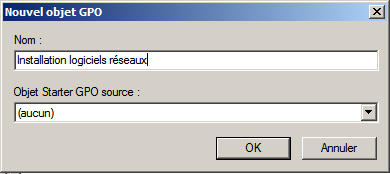




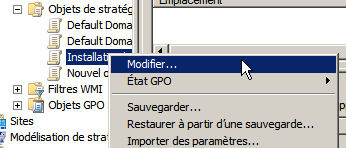
Se rendre ensuite dans “Gestion de Stratégie de Groupe”



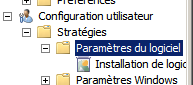
Dans “Objet de Stratégie de Groupe” faire clique droit et “Nouveau”



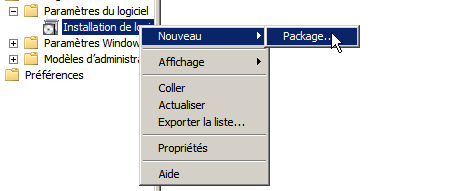
Choisir ensuite “Modifier”



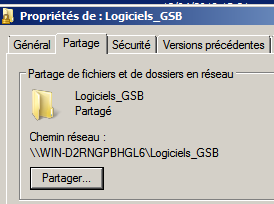
Choisir “Installation du Logiciel” dans la configuration utilisateur

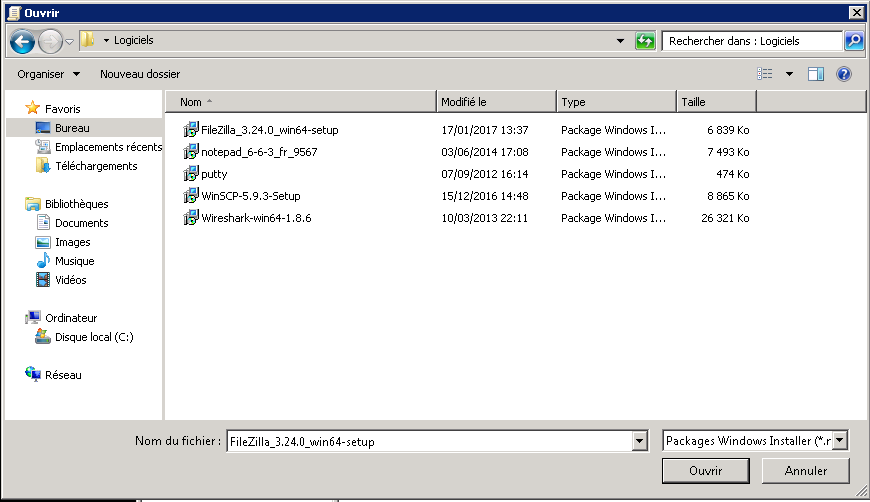


Choisir “Nouveau Package”

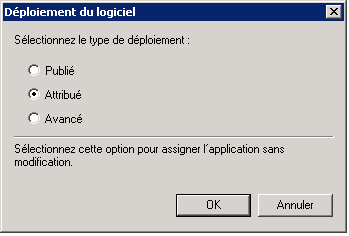


L’on met ensuite le chemin réseau du dossier qui contient les fichiers d’installation ( l’on aura préalablement partager le dossier avec les utilisateurs



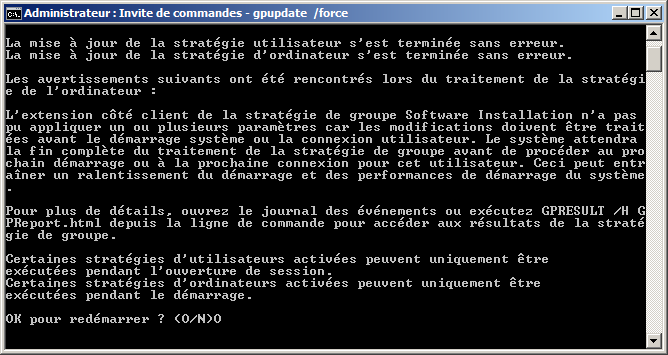


Une fois le fichier sélectionné, on choisi l’installation voulu



• Publié : l’utilisateur doit initier l’installation du logiciel  
• Attribué : Le logiciel s’installera à la prochaine ouverture de session  
• Avancé : permet d’accéder directement aux paramètres de déploiement

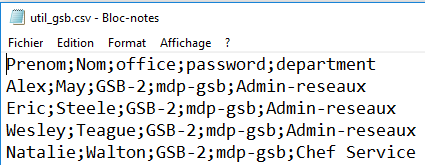
Pour appliquer les stratégies sur le serveur et les postes, on utilise la commande :  
  
**gpupdate /force**

****

# Création Utilisateurs et Groupe Via Powershell

On doit créer une hiérarchie d’utilisateurs et de groupes sera à mettre en place avec des caractéristiques définies en fonction du profil.  
Sont à créer :   
10 chefs de services  
3 administrateurs réseaux  
63 employés  
2 sessions “invités”  
1 session stagiaire informatique.  
1 session stagiaire.

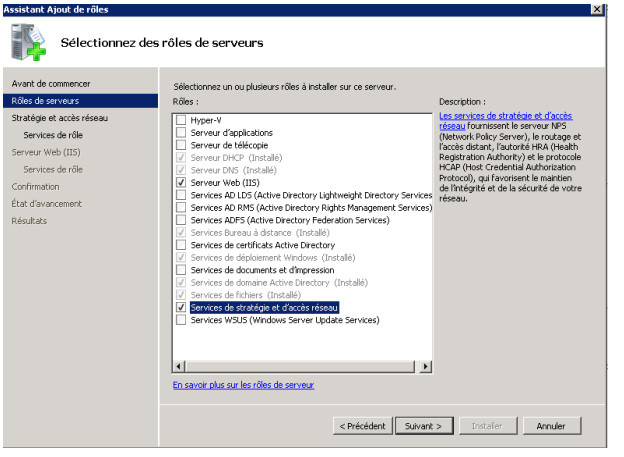
Extrait du Fichier CSV qui contient les informations Utilisateur



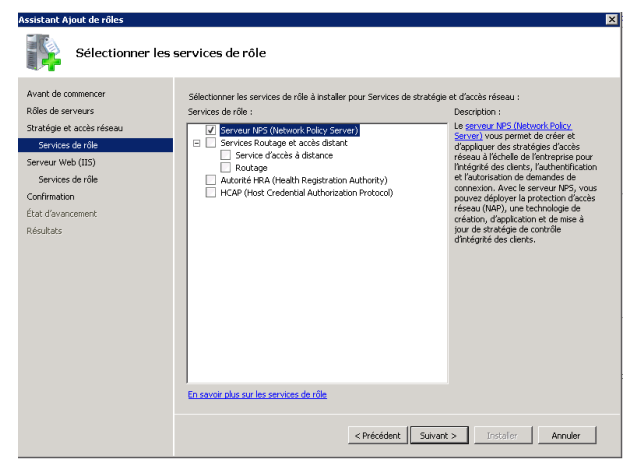
| Import-Module ActiveDirectory  $MonDomaine="dc=GSB-2,dc=fr" $AD=[ADSI]"LDAP://$MonDomaine"  $users = Import-Csv -Path "C:\Users\Administrateur\Desktop\PPE-GSB\util\_gsb.csv" -Delimiter ";" $users  foreach ($user in $users){  $name = $user.Prenom + " " + $user.Nom  $fname = $user.Prenom  $lname = $user.Nom  $login = $user.Prenom + "." + $user.Nom  $Uoffice = $user.office  $Upassword = $user.password  $dept = $user.department    switch($user.office){  "Employes" {$office = "dc=GSB-2,dc=fr"}  "Invites" {$office = "dc=GSB-2,dc=fr"}  default {$office = $null}   }    try {  New-ADUser -Name $name -SamAccountName $login -UserPrincipalName $login -DisplayName $name -GivenName $fname -Surname $lname -AccountPassword (ConvertTo-SecureString $Upassword -AsPlainText -Force) -Description $Uoffice -Department $dept -Enabled $true  echo "Utilisateur ajouté : $name"   } catch{  echo "utilisateur non ajouté : $name"  }  #\*\*\*\*\*\*\*\*Ajout des utilisateurs dans leurs groupes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  if ($Uoffice -eq "GSB-2" -and $dept -eq "Admin-reseaux"){   Add-ADGroupMember -Identity 'cn=Admin-reseaux,cn=users,dc=GSB-2,dc=fr' -Members $login  } elseif ($Uoffice -eq "GSB-2" -and $dept -eq "Stag-Info"){   Add-ADGroupMember -Identity 'cn=Stag-Info,cn=users,dc=GSB-2,dc=fr' -Members $login  } elseif ($Uoffice -eq "GSB-2" -and $dept -eq "Stagiaire"){   Add-ADGroupMember -Identity 'cn=Stagiaire,cn=users,dc=GSB-2,dc=fr' -Members $login  } elseif ($Uoffice -eq "GSB-2" -and $dept -eq "Chef Service"){   Add-ADGroupMember -Identity 'cn=Chef Service,cn=users,dc=GSB-2,dc=fr' -Members $login  } elseif ($Uoffice -eq "GSB-2" -and $dept -eq "Employes"){   Add-ADGroupMember -Identity 'cn=Employes,cn=users,dc=GSB-2,dc=fr' -Members $login }     } | permet la gestion des services d'annuaires avec PowerShell.  L’on renseigne les informations propre à son domaine  Import du fichier CSV  L’on fait correspondre les informations du fichier à des variables  L’on dispatche les utilisateurs entre le groupe invité ou Employes  L’on ajoute l’utilisateur suivant les informations dans les variables  Cas ou l’utilisateur n’est pas ajouté  Si l’utilisateur correspond aux 2 paramètres alors il est ajouté au groupe |
| --- | --- |
| Création des Groupes  Import-Module ActiveDirectory  $MonDomaine="cn=Users,dc=GSB-2,dc=fr"  $AD=[ADSI]"LDAP://$MonDomaine"  $nouveaugr=$AD.create("Group","cn=Admin-reseaux")  $nouveaugr.invokeSet("SamAccountName","Admin-reseaux")  $nouveaugr.setInfo()  $nouveaugr=$AD.create("Group","cn=Stag-Info")  $nouveaugr.invokeSet("SamAccountName","Stag-Info")  $nouveaugr.setInfo()  $nouveaugr=$AD.create("Group","cn=Stagiaire")  $nouveaugr.invokeSet("SamAccountName","Stagiaire")  $nouveaugr.setInfo()  $nouveaugr=$AD.create("Group","cn=Chef Service")  $nouveaugr.invokeSet("SamAccountName","Chef Service")  $nouveaugr.setInfo()  $nouveaugr=$AD.create("Group","cn=Employes")  $nouveaugr.invokeSet("SamAccountName","Employes")  $nouveaugr.setInfo() | Ajout du module AD  Informations sur le domaine  Création des groupes  Application des groupes |

# Création Radius

Sur le serveur l’on choisit d’ajouter le rôle

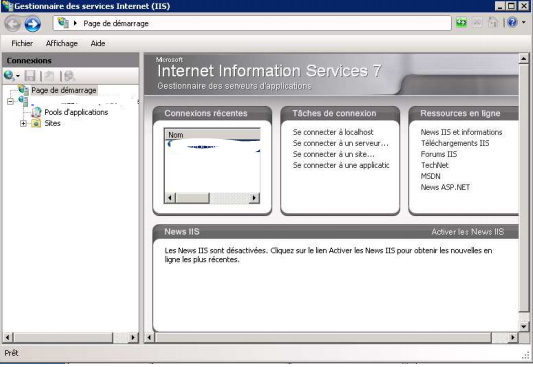


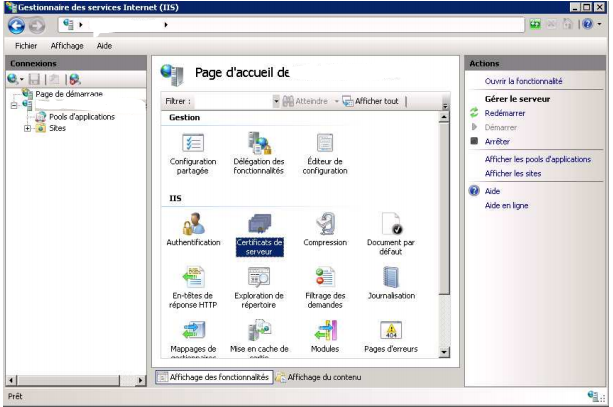
Le serveur IIS nous servira à gérer les certificats (recevoir les certificats Radius)

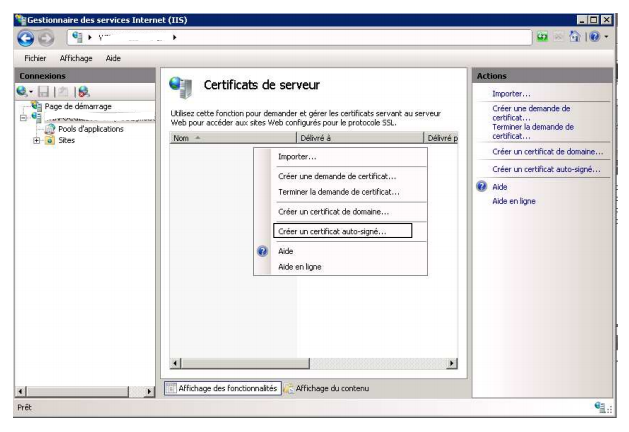


On choisit serveur NPS qui sera le serveur d’authentification (Radius)

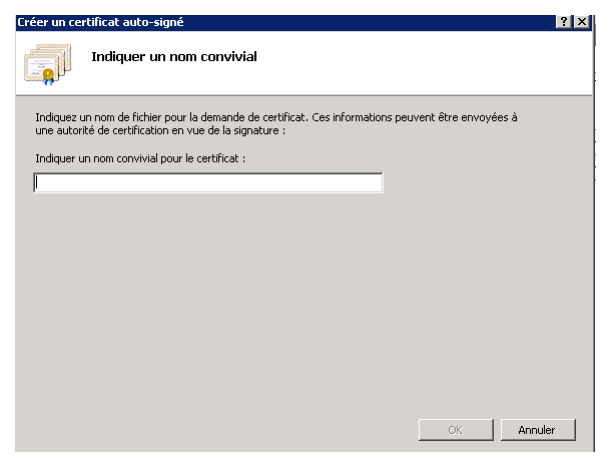
Ensuite pour pouvoir créer un certificat auto-signé, on utilise les outils d’administration du serveur IIS

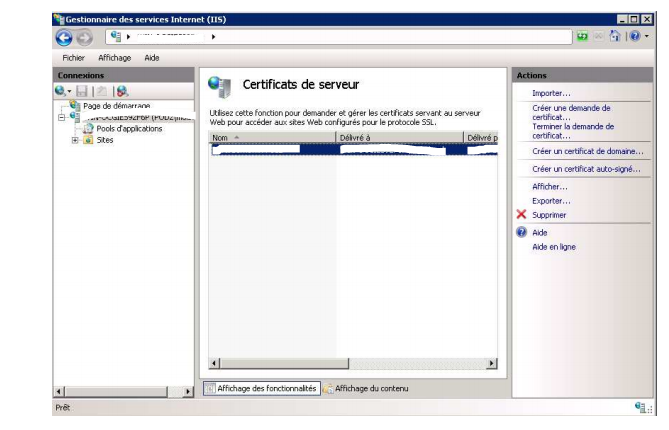






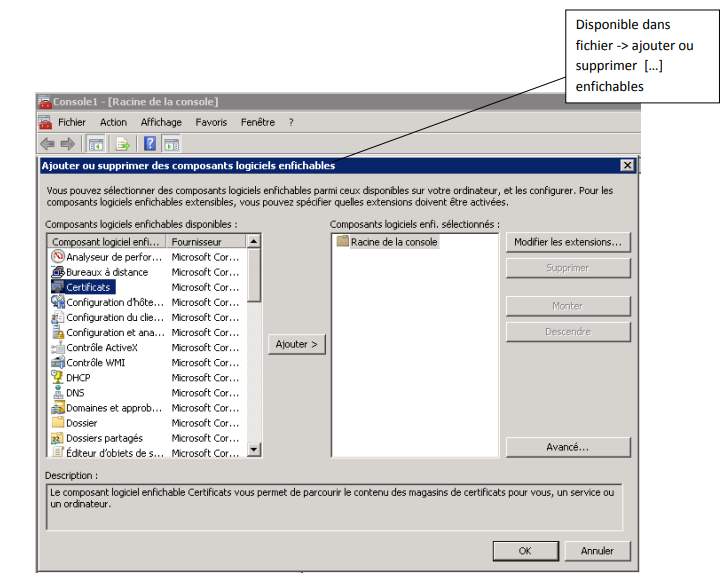
L’on crée un certificat auto-signé, par défaut car l’on ne dispose pas d'autorité de certification



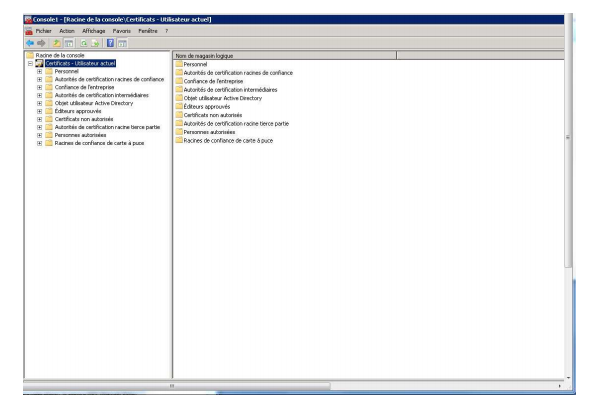


Une fois le certificat créé, on utilise le programme mmc ( tapermmc dans la barre de recherche des programmes sur le serveur )

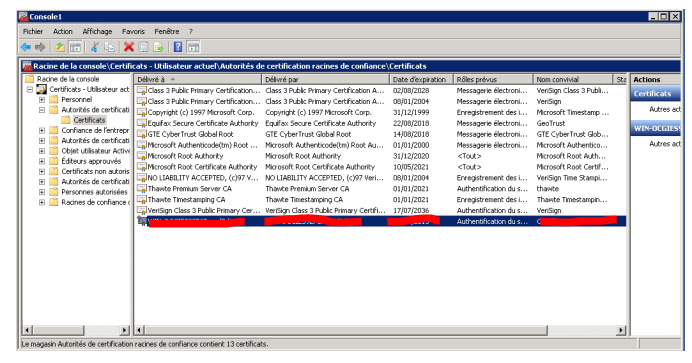
Cela permet d’utiliser des outils d’administration afin de gérer des ordinateurs, des réseaux, des services..



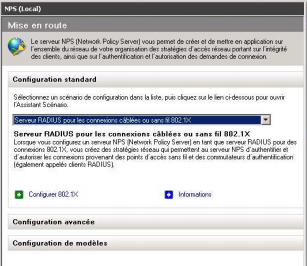
On rajoute certificats dans les composants



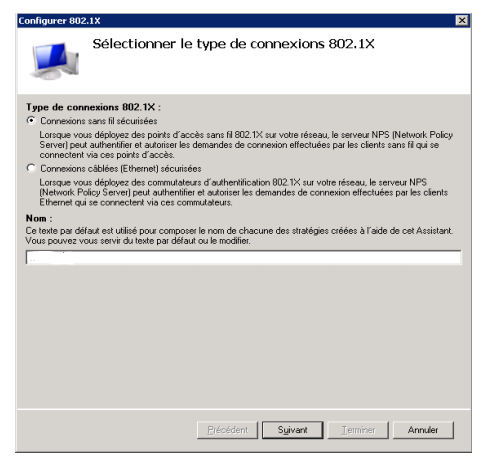
L’on peut voir notre certificat auto-signé dans la liste



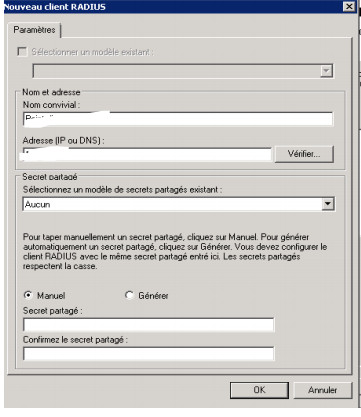
Maintenant on configure le serveur NPS en 802.1X



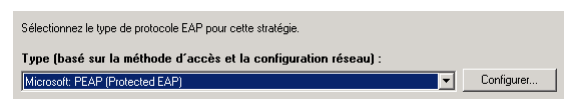
L’on choisit “Configurer en 802.1X”



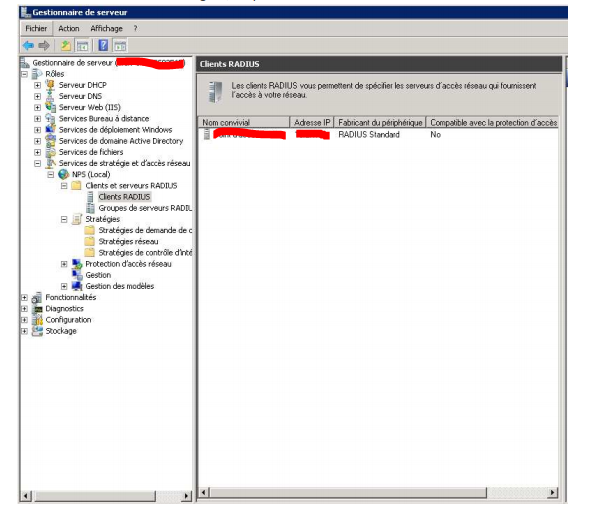
En poursuivant, on créer un client Radius, on rentre donc dans le point d’accès



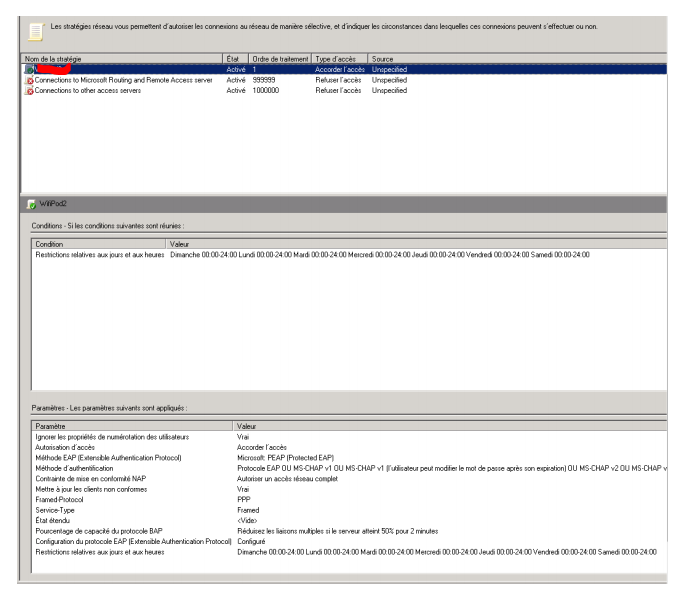
On choisit le PEAP comme mode de sécurité



le 802.1X est configuré, on peut maintenant le vérifié dans le serveur NMS

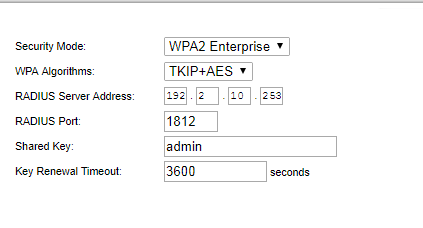


Il faut ensuite créer une stratégie d’accès réseau dans l’onglet correspondant sur le serveur NPS, il faut configurer la stratégie pour que le client ait un accès constant au réseau. On peut régler cette option dans l’onglet “Conditions ” de création de la stratégie, on peut modifier d’autre paramètres ensuite



On peut voir tous les paramètres et conditions sur le screen, on peut voir que la seule condition active est l’accès pour les utilisateurs à n’importe quelle heure pour n’importe quel jour.

Configuration de la borne wifi



Il suffit de créer un compte sur le domaine pour accéder au wifi