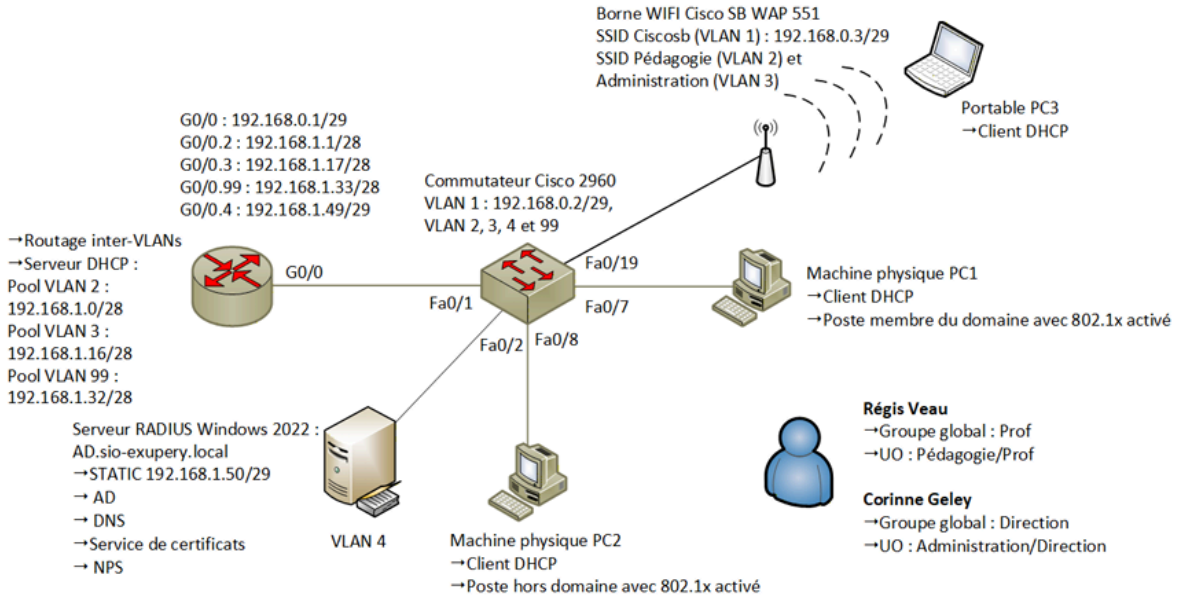
BTS 2 - Services Informatiques aux Organisations

BTS SIO SISR – Mise en oeuvre d'une infrastructure 802.1x : connexions câblées

Configuration du routeur..... 1
Configuration du commutateur..... 3
1. Le client final..... 6
2. Installation du service NPS..... 10
3. Configuration du serveur RADIUS NPS..... 11
3.1 Déclaration du client Radius :..... 13
3.2 Déclaration d'une stratégie de demande de connexion..... 14
3.3 Déclaration d'une stratégie d'accès au réseau..... 20
4. Demande de connexion des utilisateurs rveau et cgeley..... 45
Annexe :..... 47

Topologie :



Configuration du routeur

```
Router(config)#int G0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.248
Router(config-if)#no shut
Router(config-if)#
```

```
Router(config)#int G0/0.2
Router(config-subif)#encapsulation dotlq 2
Router(config-subif)#ip address 192.168.1.1 255.255.255.240
Router(config-subif)#no shut
Router(config-subif)#
```

```
Router(config)#int G0/0.3
Router(config-subif)#encapsulation dotlq 3
Router(config-subif)#ip address 192.168.1.17 255.255.255.240
Router(config-subif)#no shut
Router(config-subif)#
```

```
Router(config)#int G0/0.4
Router(config-subif)#encapsulation dotlq 4
Router(config-subif)#ip address 192.168.1.49 255.255.255.248
Router(config-subif)#no shut
Router(config-subif)#
```

```
Router(config)#int G0/0.99
Router(config-subif)#encapsulation dotlq 99
Router(config-subif)#ip address 192.168.1.33 255.255.255.240
Router(config-subif)#no shut
Router(config-subif)#
```

Visualisation de la configuration des interfaces sur le routeur :

```
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 description VLAN 2
 encapsulation dot1Q 2
 ip address 192.168.1.1 255.255.255.240
!
interface GigabitEthernet0/0.3
 description VLAN 3
 encapsulation dot1Q 3
 ip address 192.168.1.17 255.255.255.240
!
interface GigabitEthernet0/0.4
 description VLAN 4
 encapsulation dot1Q 4
 ip address 192.168.1.49 255.255.255.248
!
interface GigabitEthernet0/0.99
 description VLAN 99
 encapsulation dot1Q 99
 ip address 192.168.1.33 255.255.255.240
!
```

Configuration du commutateur

Création des vlans :

```
Switch(config)#
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#vlan 4
Switch(config-vlan)#vlan 99
Switch(config-vlan)#
```

Configuration des interfaces Fa0/2 et Fa0/19 :

```
Switch(config)#int Fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#int Fa0/19
Switch(config-if)#switchport mode trunk
Switch(config-if)#^Z
Switch#
```

Mise en place de l'authentification 802.1x :

- Activation générale de 802.1x :

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#aaa authorization network default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#
```

- Définition des informations d'accès au serveur RADIUS :

```
Switch(config)#radius-server host 192.168.1.50 auth-port 1812 acct-port 1813 k$
Switch(config)#
```

Définition de l'authentification 802.1x sur le port Fa0/2, Fa0/7 et Fa0/8 :

```
Switch(config)#int Fa0/7
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
Switch(config-if)#int Fa0/8
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

```
Switch(config-if)#int Fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control ?
  auto                PortState set to automatic
  force-authorized    PortState set to AUTHORIZED
  force-unauthorized  PortState set to UnAuthorized

Switch(config-if)#authentication port-control
% Incomplete command.

Switch(config-if)#no authentication port-control auto
Switch(config-if)#no dot1x pae authenticator
Switch(config-if)#
```

Visualisation de la configuration du commutateur :

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#do sh dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for FastEthernet0/7
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Info for FastEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60

ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Switch(config)#
```

Visualisation des informations sur l'authentification 802.1x :

```
Switch#sh dot1 all summary
Interface        PAE     Client          Status
-----------------------------------------------------------
Fa0/7            AUTH    none            UNAUTHORIZED
Fa0/8            AUTH    none            UNAUTHORIZED
Switch#
```

Configuration du serveur DHCP :

- Pour le VLAN 2 :

```
Router(config)#ip dhcp pool VLAN 2
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#network 192.168.1.0 255.255.255.240
Router(dhcp-config)#exit
Router(config)#
```

- Pour le VLAN 3 :

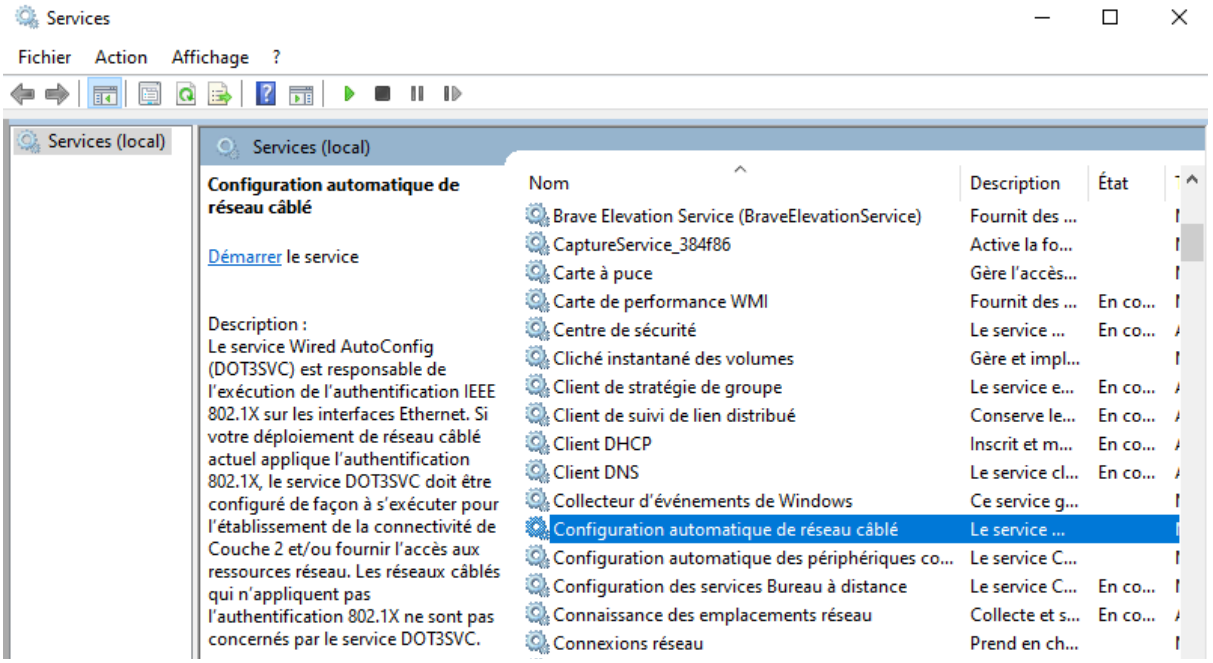
```
Router(config)#ip dhcp pool VLAN 3
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#network 192.168.1.16 255.255.255.240
Router(dhcp-config)#exit
Router(config)#
```

- Pour le VLAN 99 :

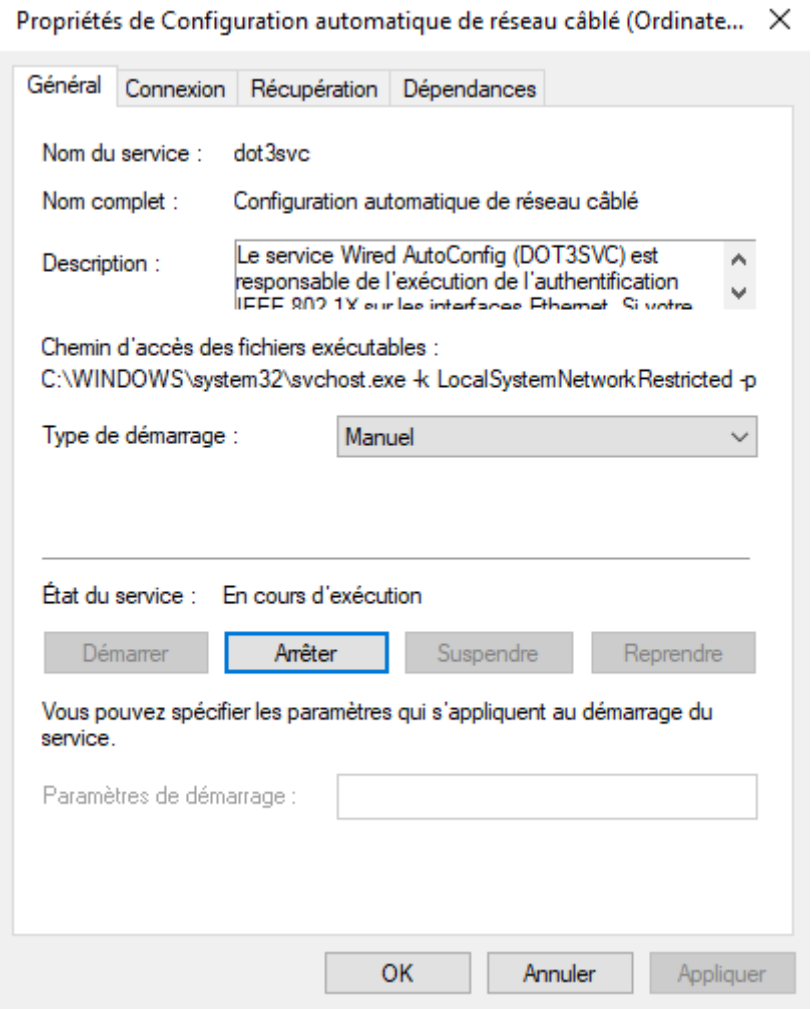
```
Router(config)#ip dhcp pool VLAN 99
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#network 192.168.1.32 255.255.255.240
Router(dhcp-config)#exit
Router(config)#
```

1. Le client final

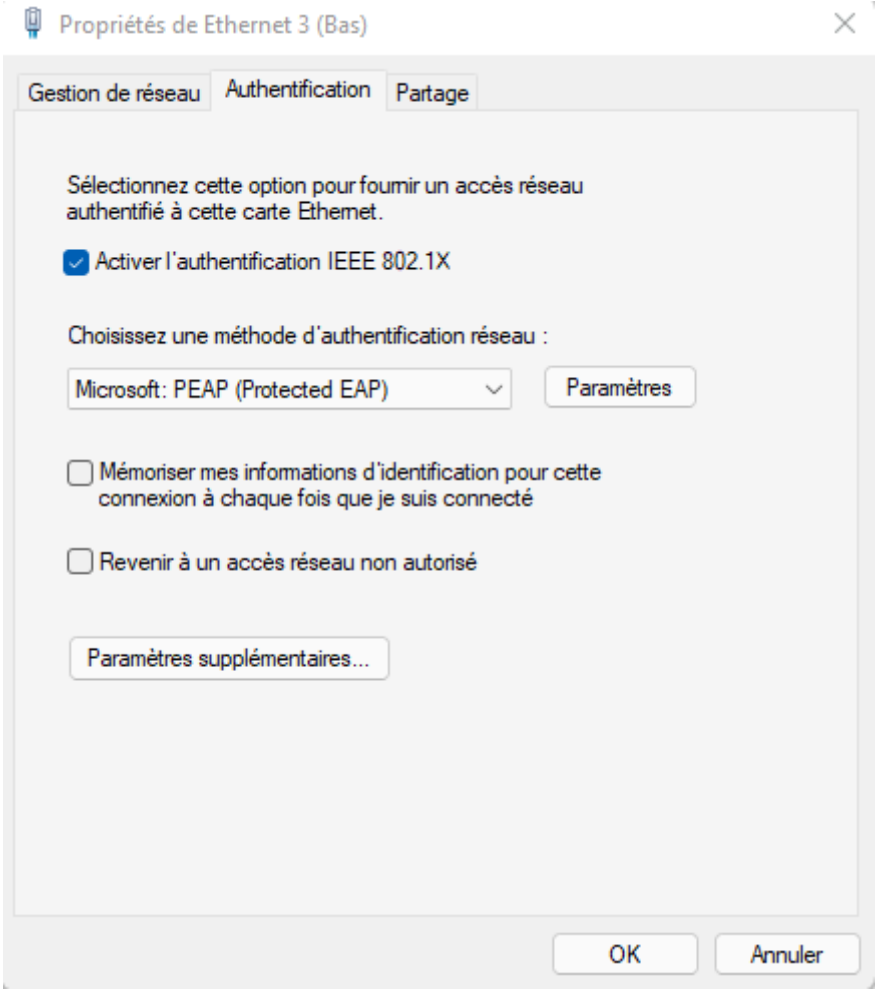
Configuration automatique de réseau câblé :



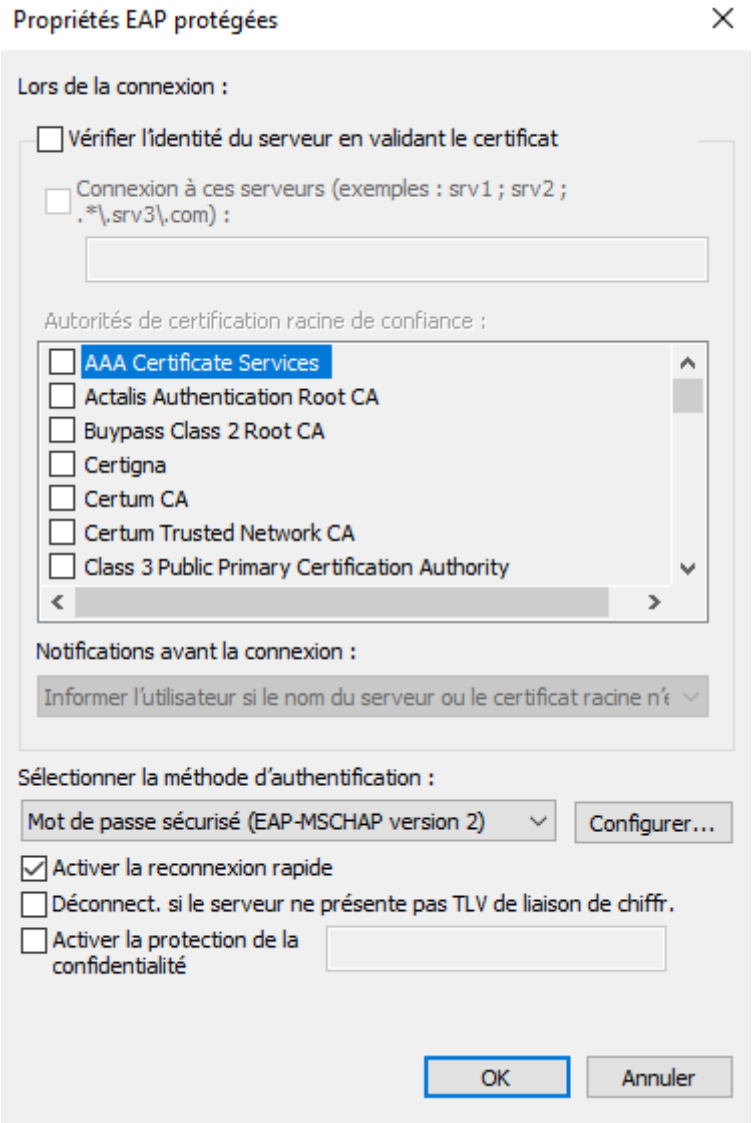
Démarrage en mode manuel du service **dot3svc** (configuration automatique de réseau câblé) :



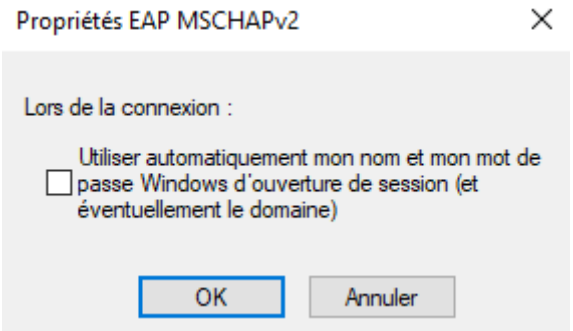
Activation de l'authentification IEEE 802.1x par la méthode d'authentification PEAP (Protected EAP) :



Méthode d'authentification par mot de passe sécurisé (EAP-MSCHAP version 2) avec l'activation de la reconnexion rapide :

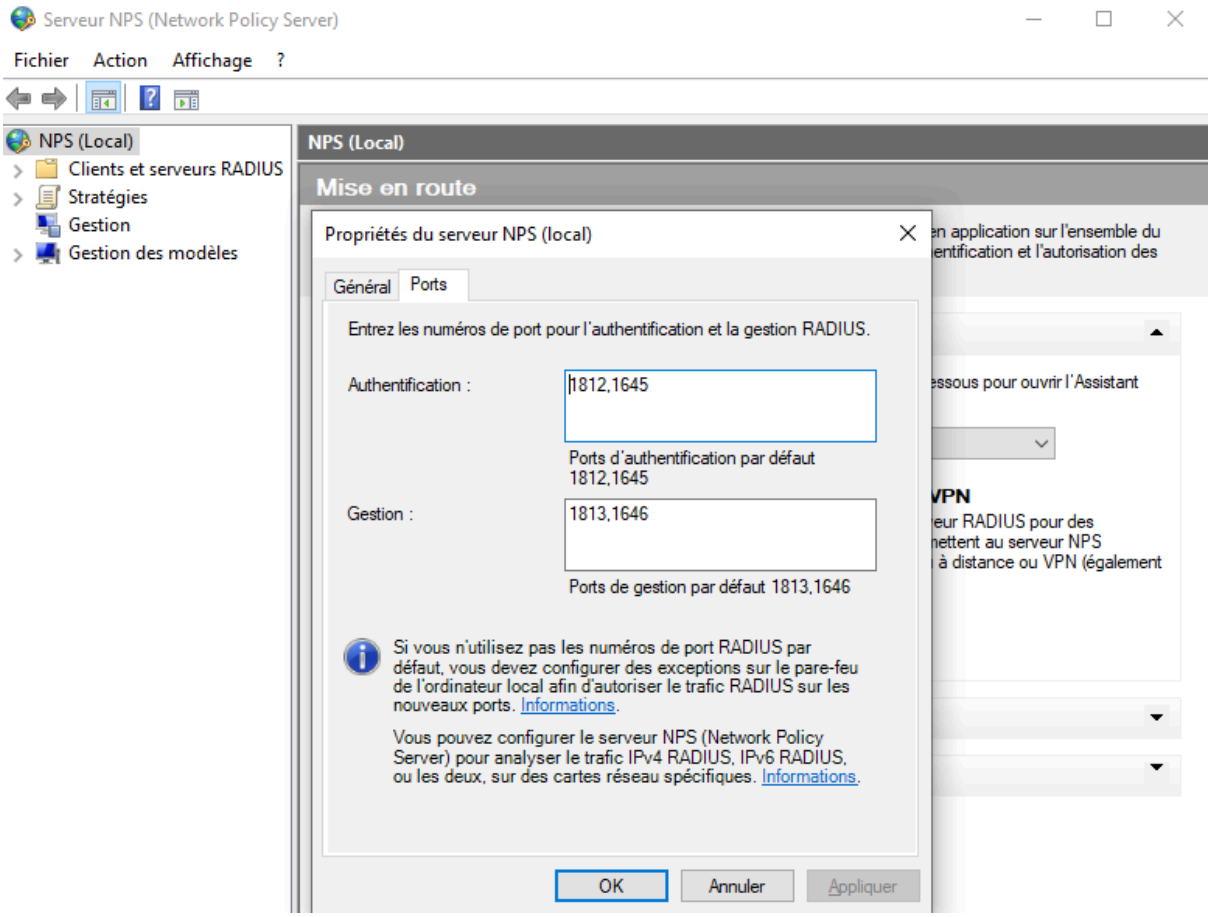


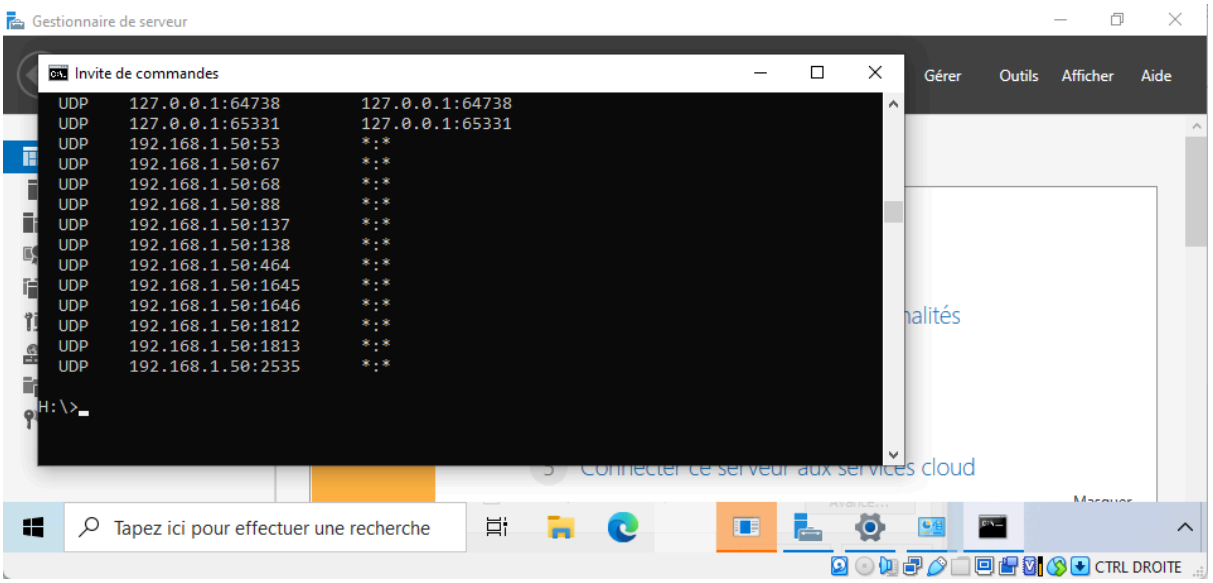
Lors de la connexion, ne pas utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session :



2. Installation du service NPS

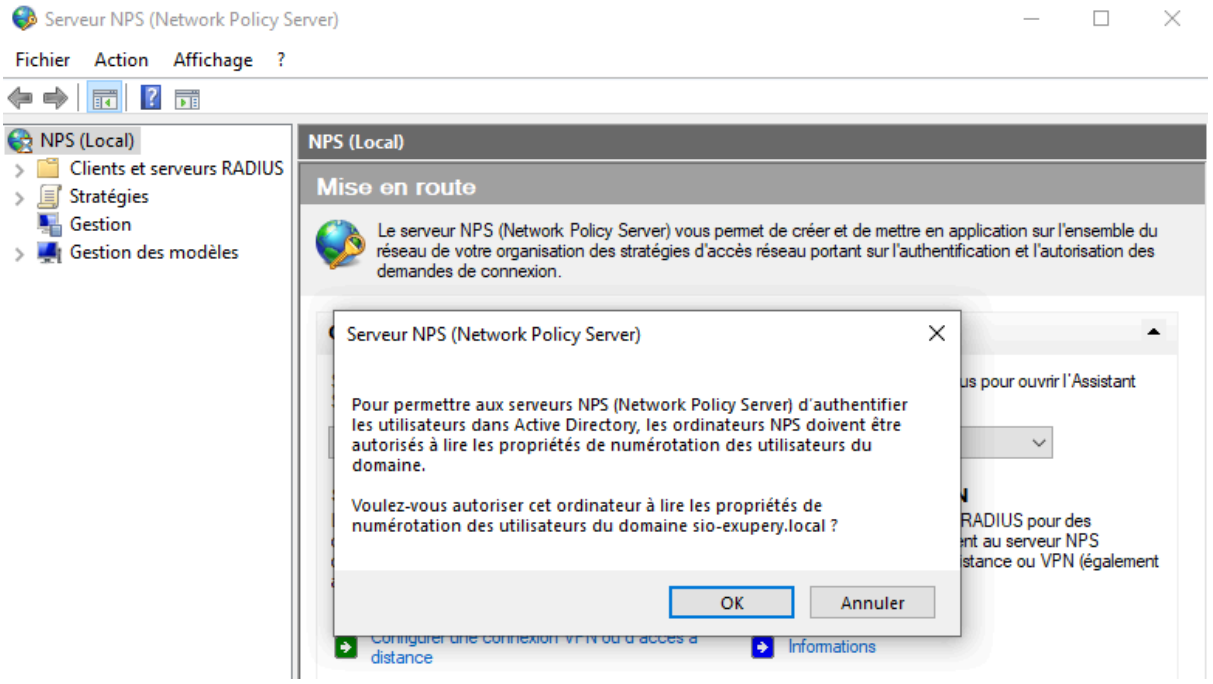
Ouverture du serveur NPS (Network Policy Server) avec les ports dans les propriétés du serveur NPS :



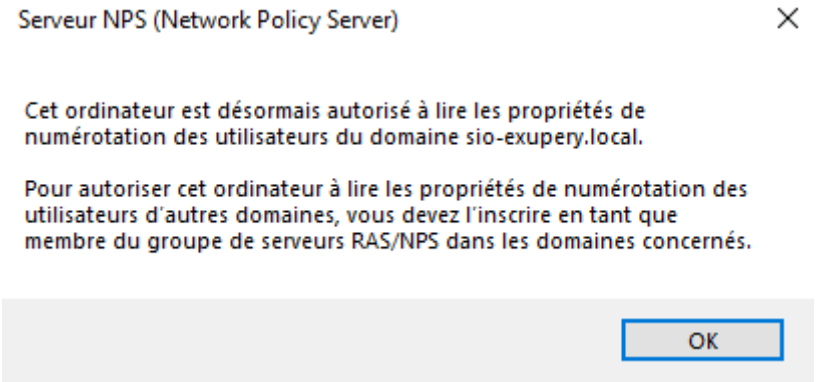


3. Configuration du serveur RADIUS NPS

Inscription du serveur dans Active Directory :
Autoriser cet ordinateur à lire les propriétés de numérations des utilisateurs du domaine sio-exupery.local. > Clique droite sur **Action** > **Inscrire un serveur dans Active Directory.**



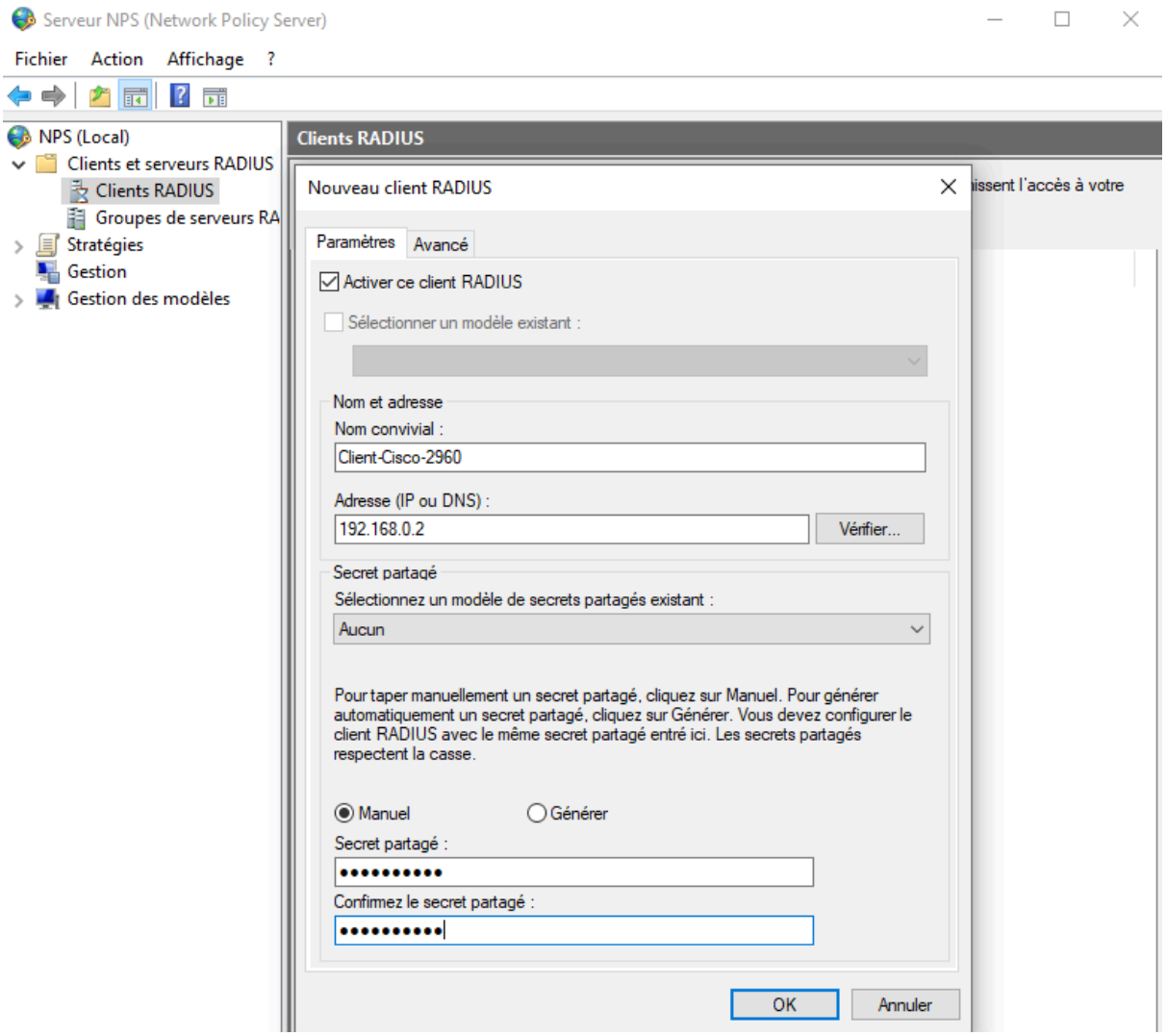
Confirmation de l'assistant global :



Mise en route du service NPS avec configuration du serveur Radius pour les connexions câblées ou sans fil 802.1x.

3.1 Déclaration du client Radius :

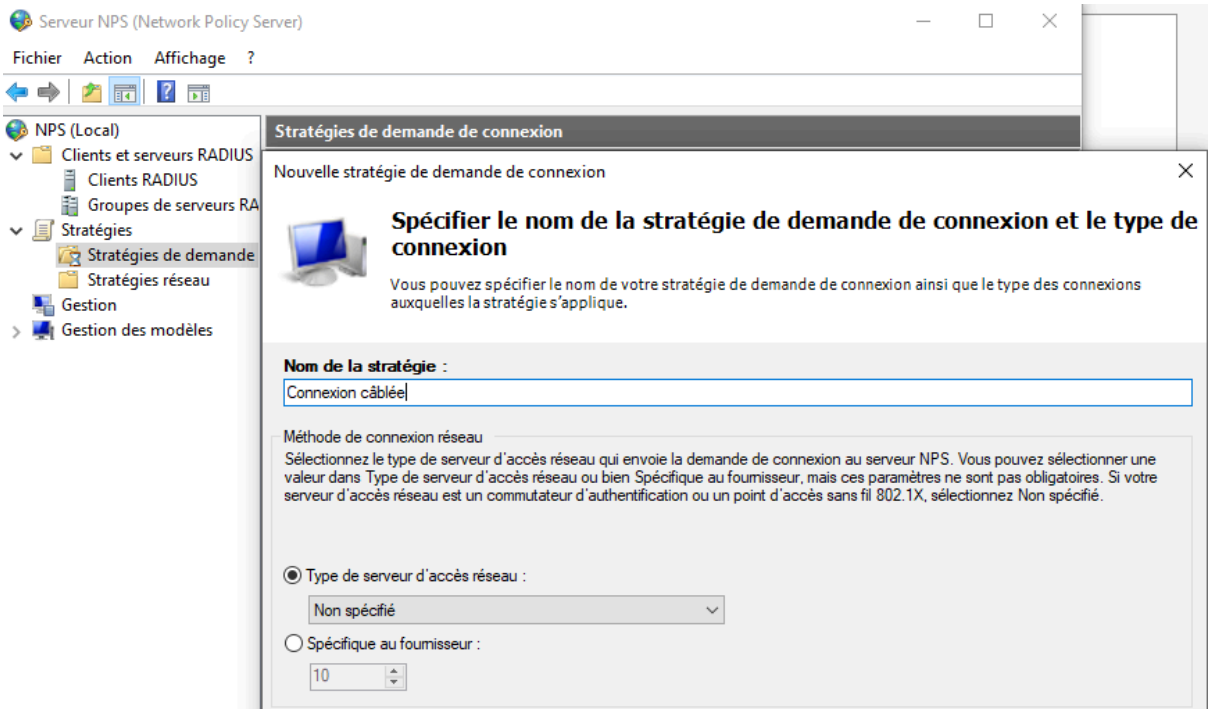
Ajout du nouveau client Radius : > Clique droit sur **Clients RADIUS** > Nouveau.



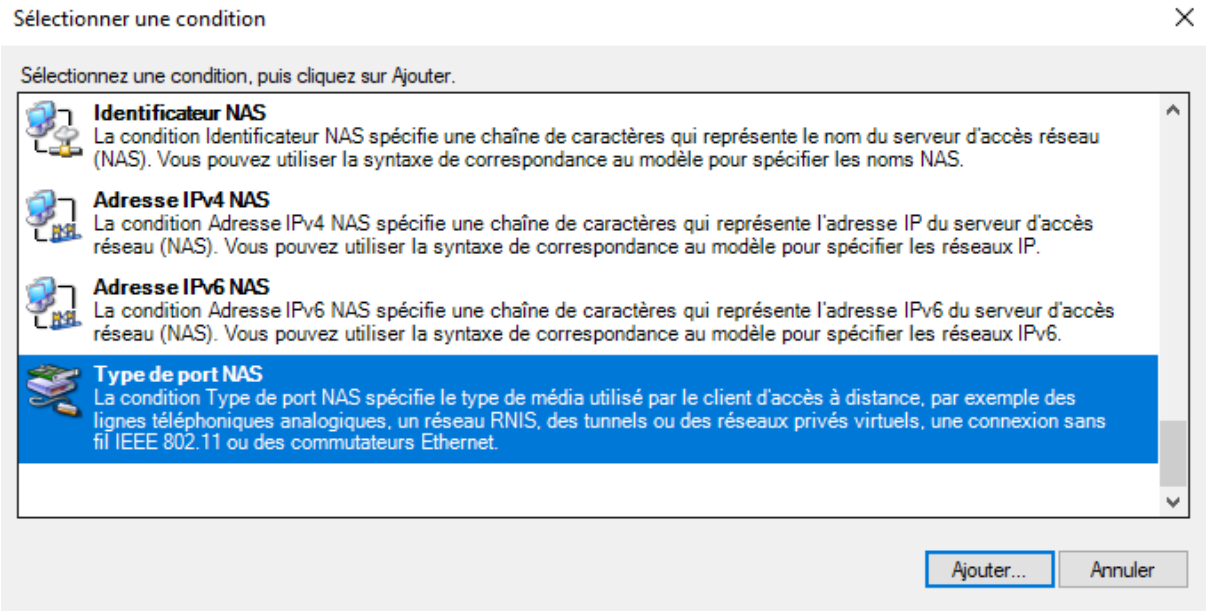
Visualisation du client Client Cisco-2960 dans la liste des clients RADIUS :

3.2 Déclaration d'une stratégie de demande de connexion

Ajout d'une nouvelle stratégie de demande de connexion : > Clique droit sur **Stratégie de demande de connexion** > Nouveau.

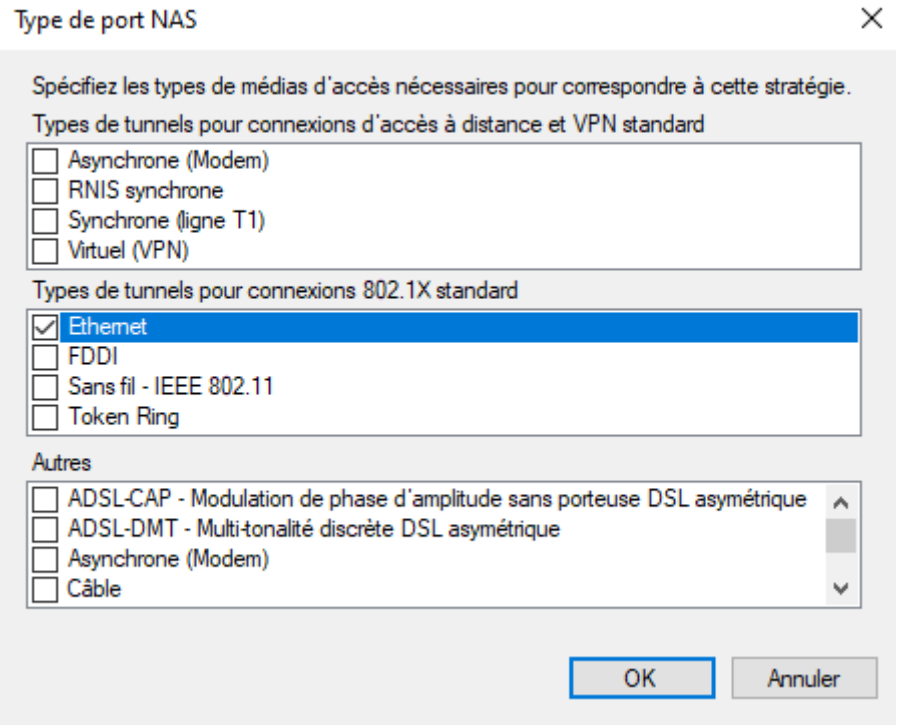


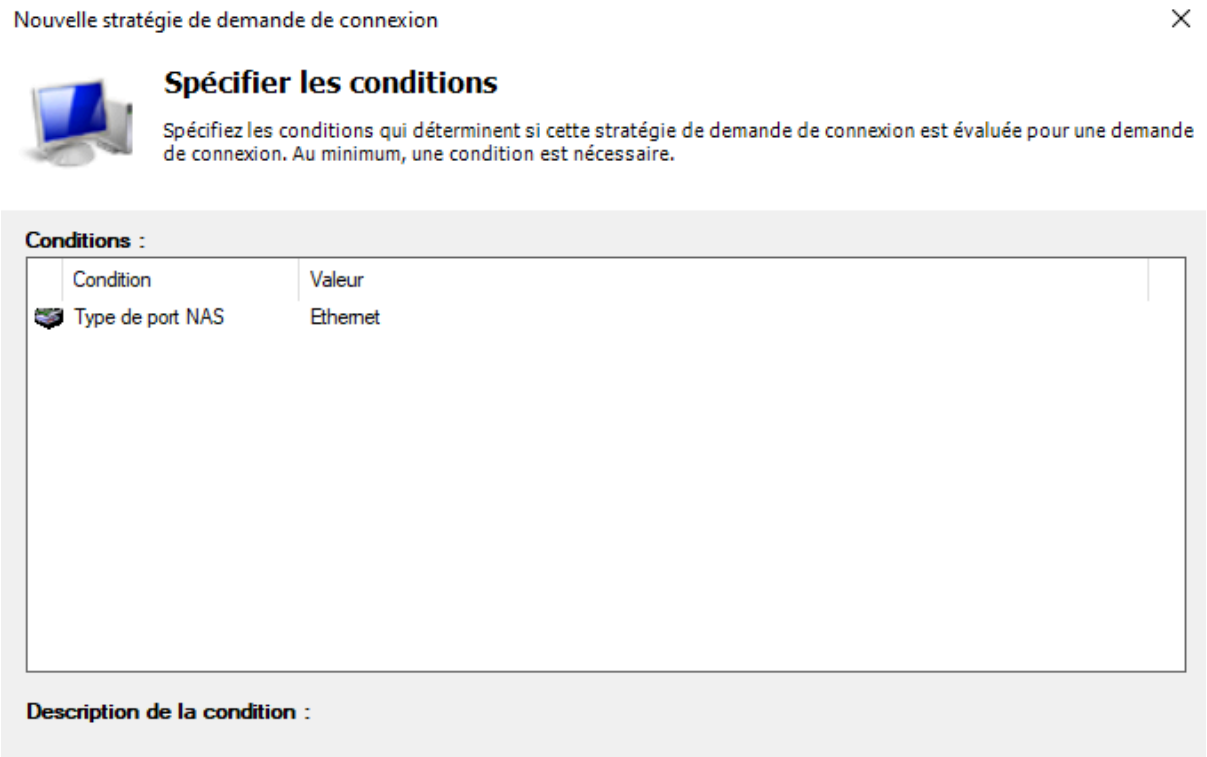
Sélection de la condition **Type de port NAS**.



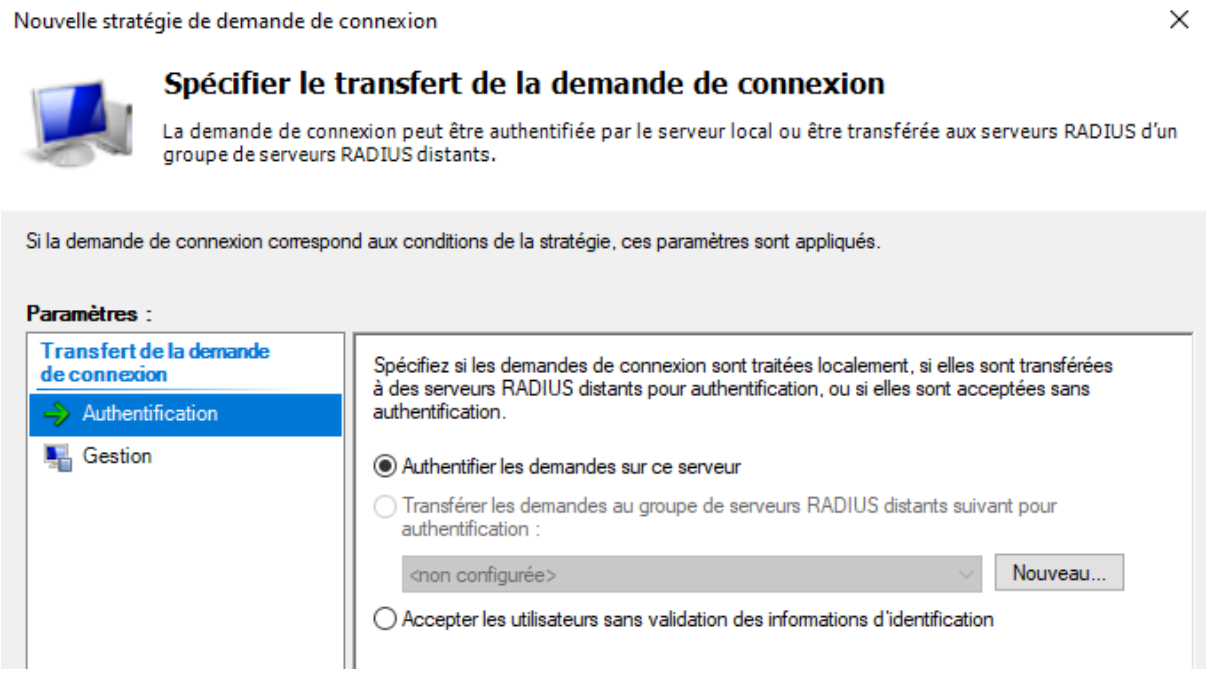
NAS est ici l'acronyme de **Network Access Server** et désigne le client RADIUS. Ne pas confondre avec **Network Authentication Server** qui désigne le serveur Radius lui-même.

Sélection du **Type de tunnels pour connexions 802.1x standard** Ethernet.

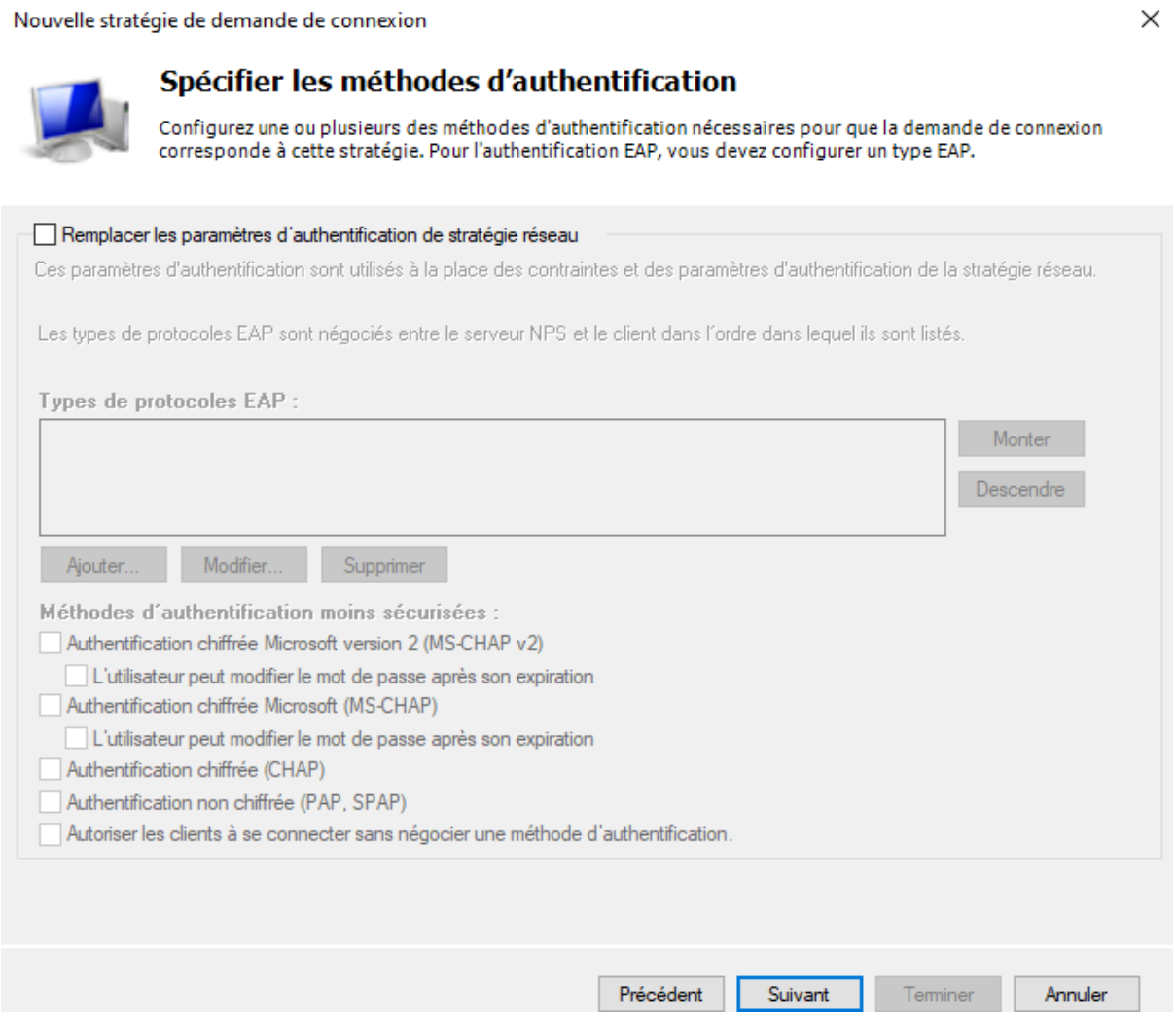




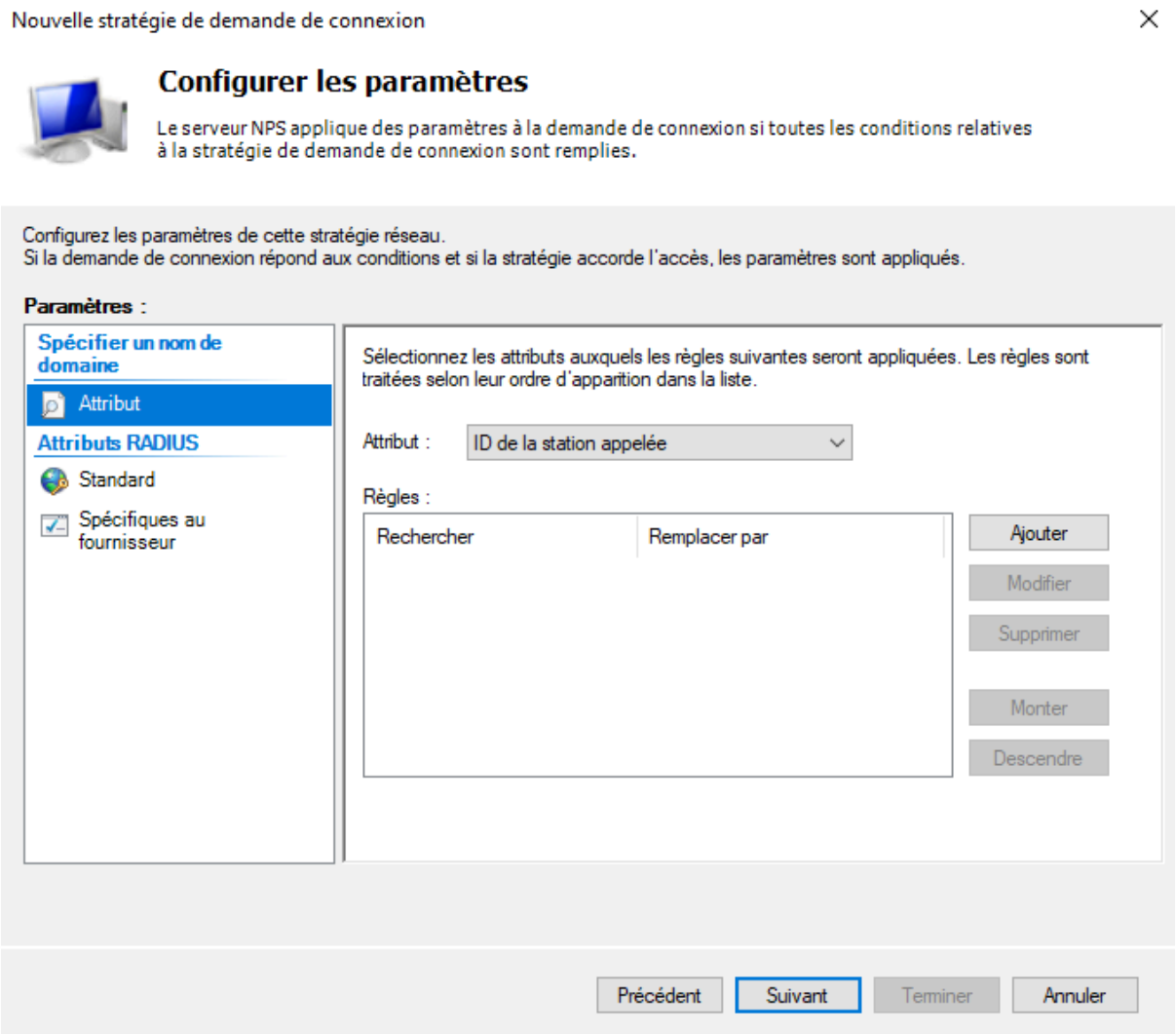
Authentification des demandes sur le serveur :

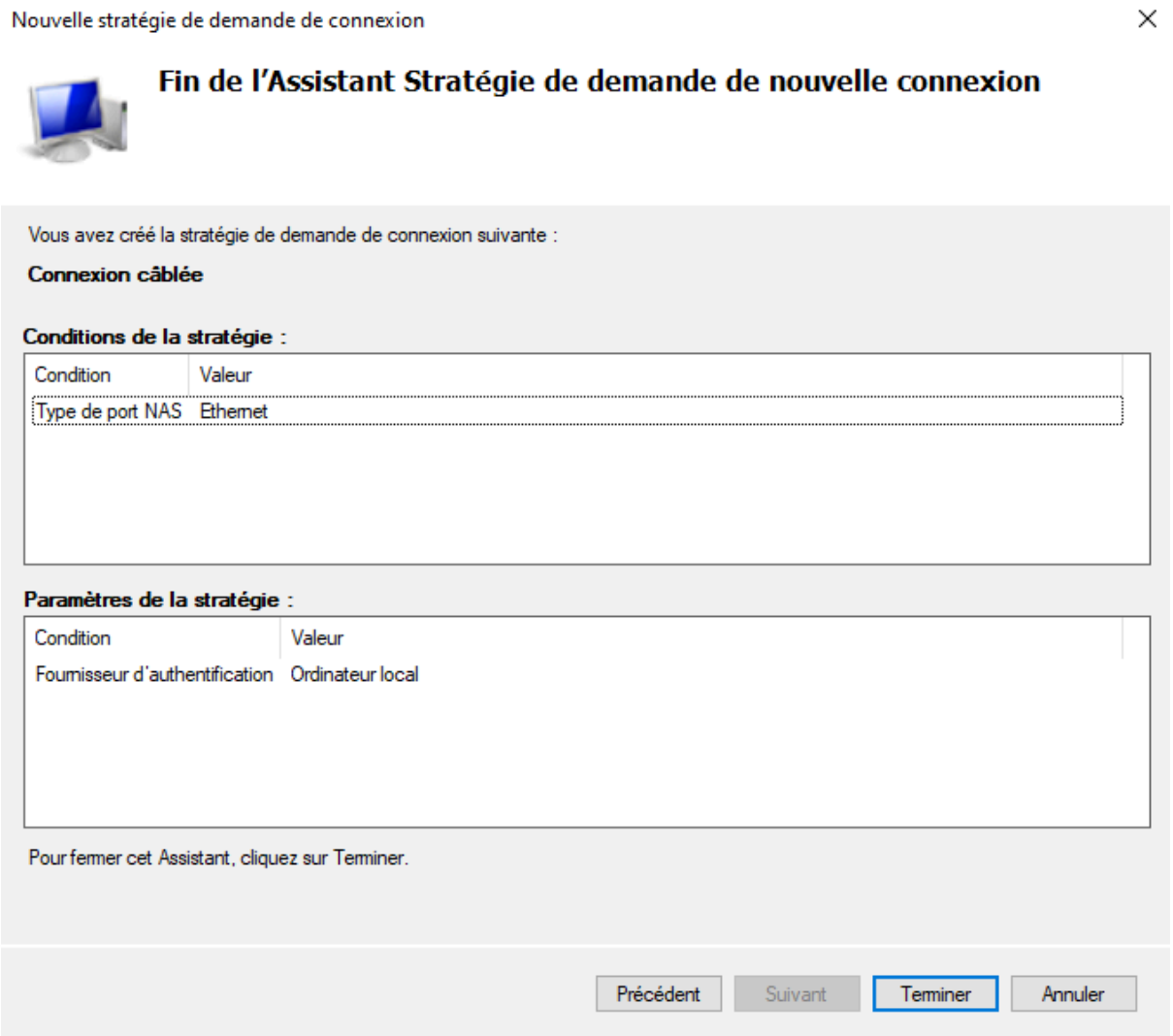


Pas de configuration des méthodes d'authentification :

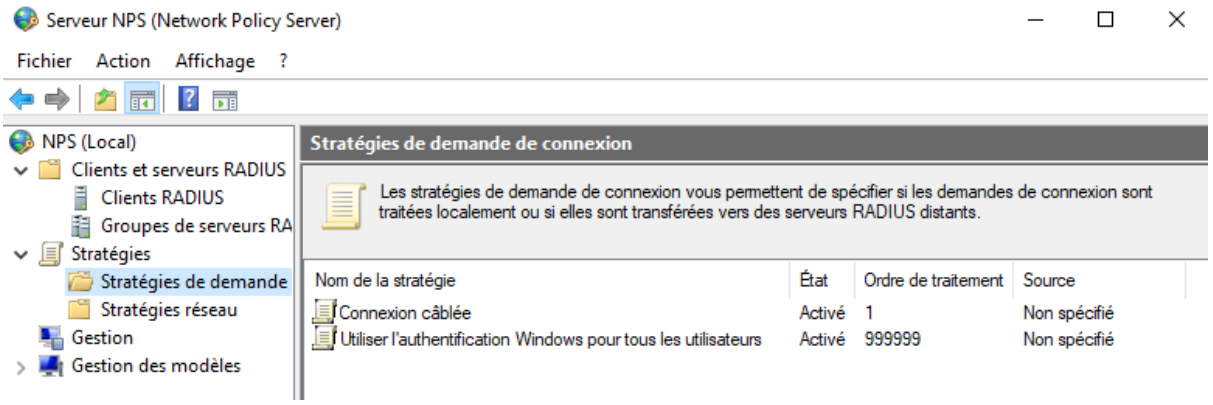


Attributs auxquels les règles suivantes seront appliquées : ID de la station appelée :



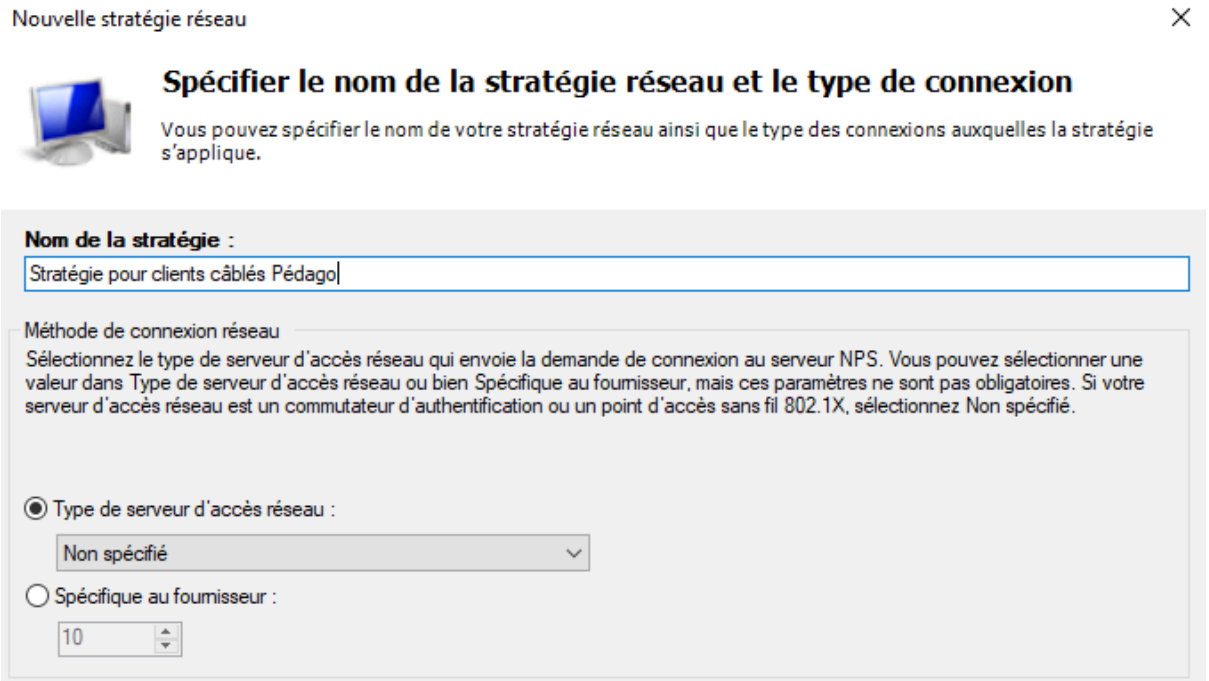


Récapitulatif de la stratégie de demande de connexion :

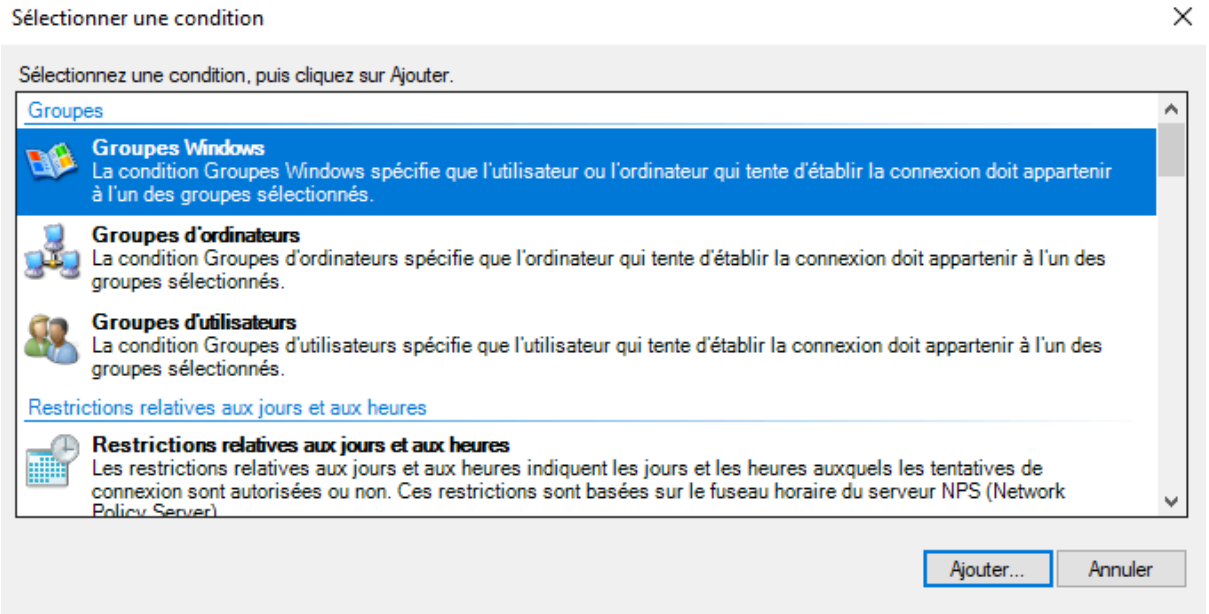


3.3 Déclaration d'une stratégie d'accès au réseau

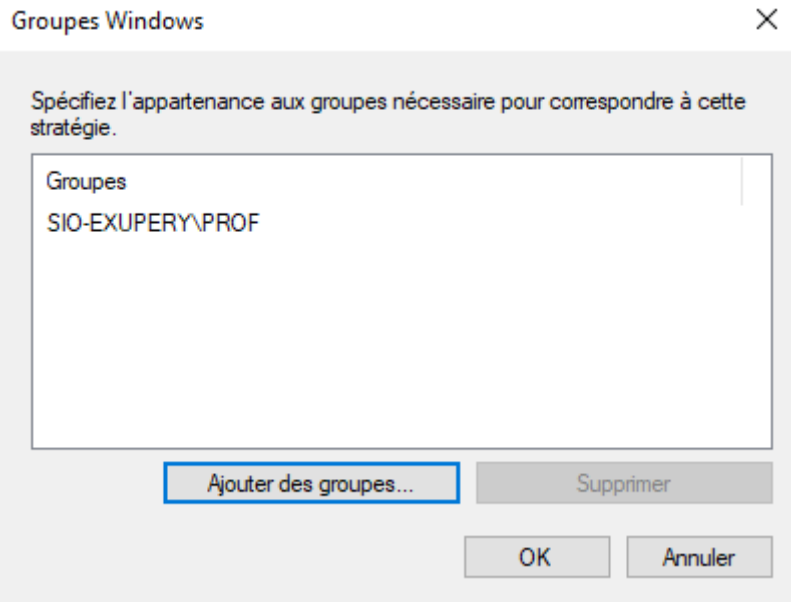
Ajout d'une nouvelle stratégie réseau : > Clique droit sur **Stratégie réseau** > Nouveau.



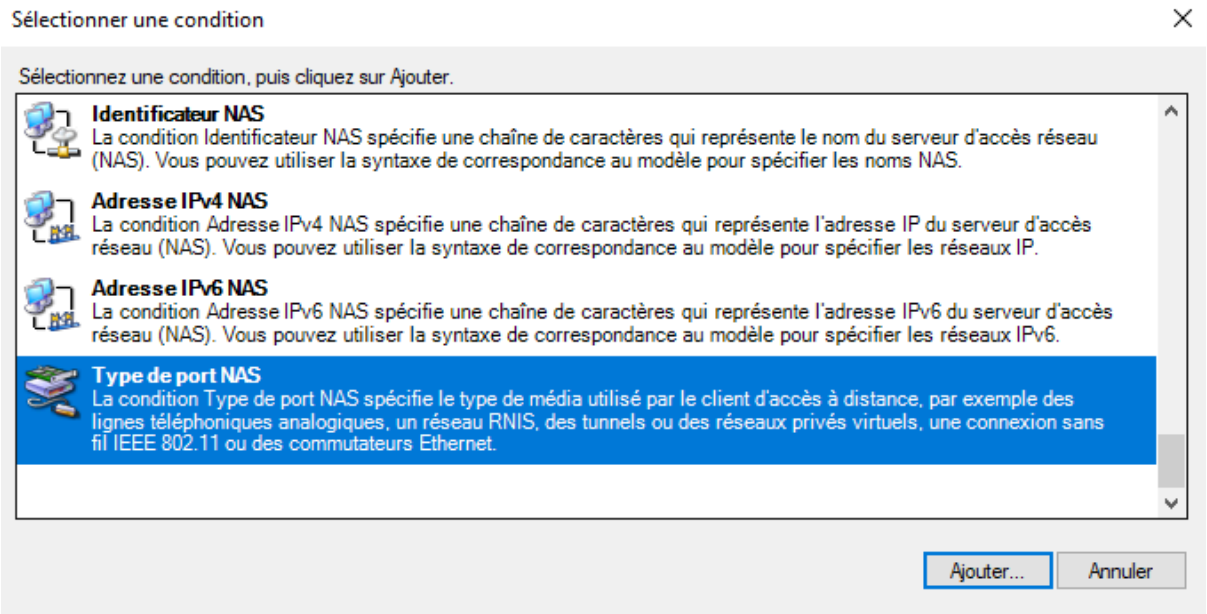
Sélection de la condition **Groupes Windows**.



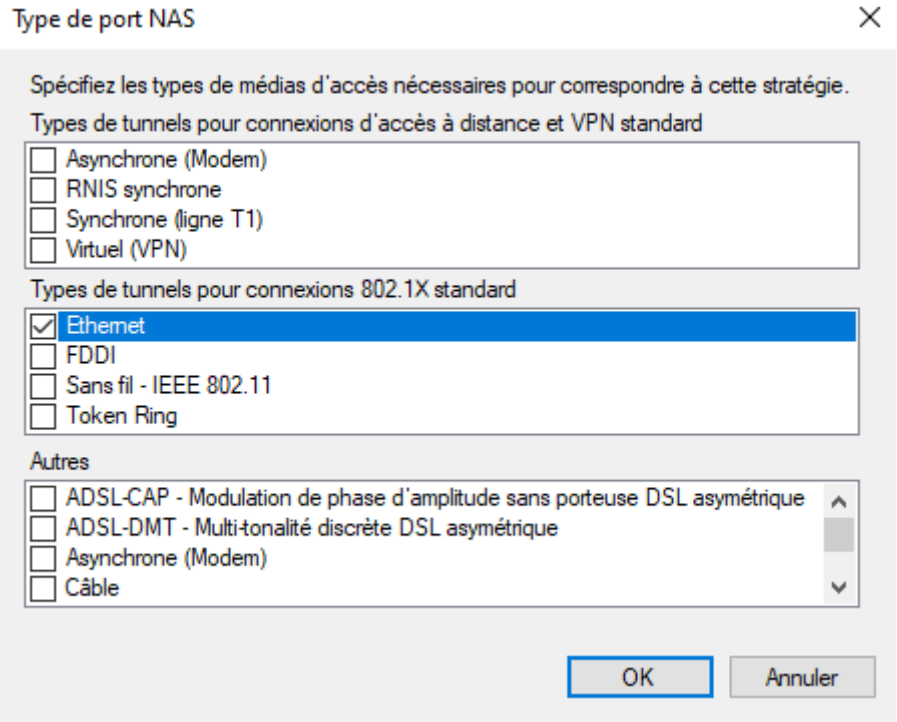
Ajout du groupe Prof à la stratégie :



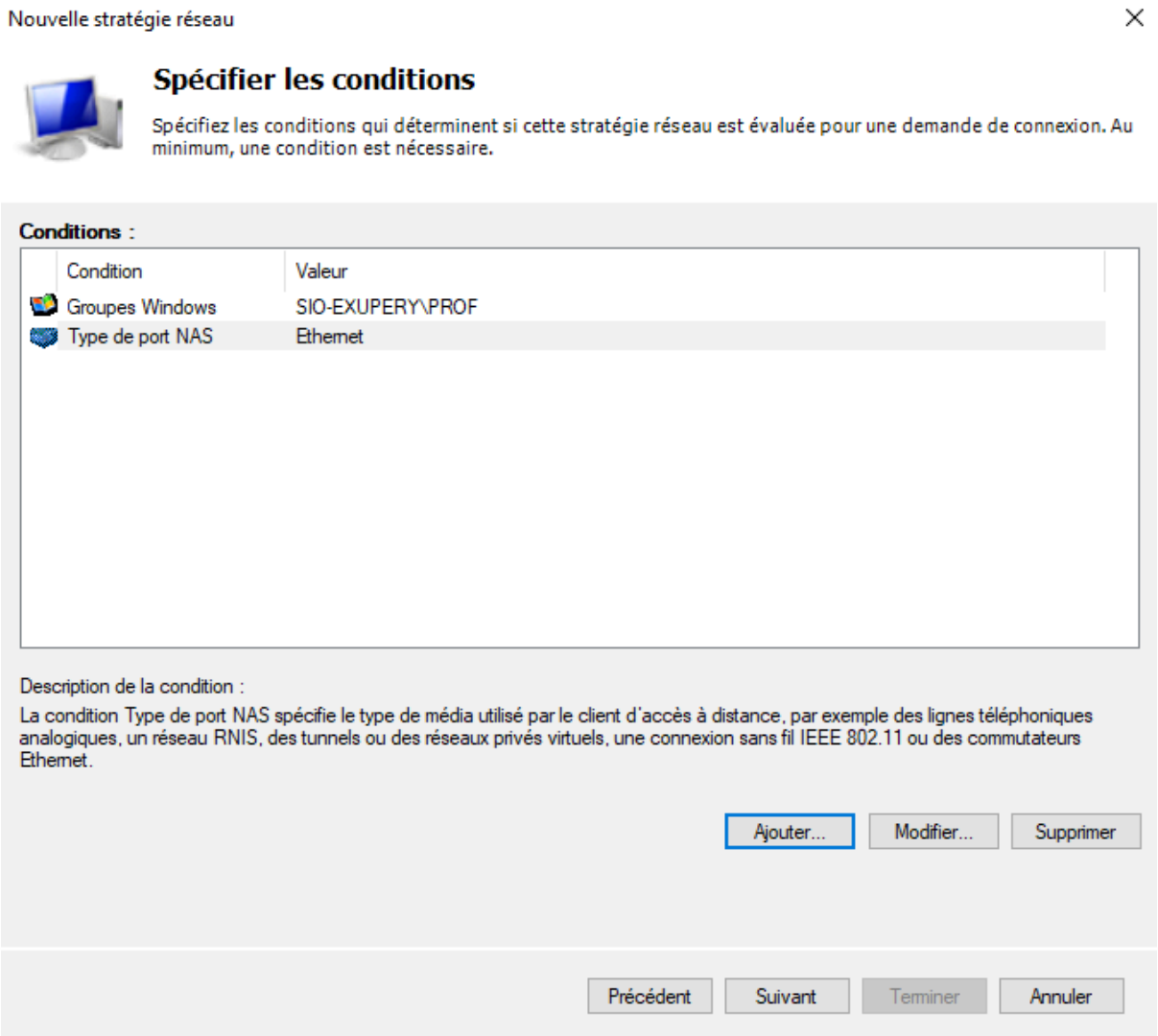
Sélection de la deuxième condition **Type de port NAS**.



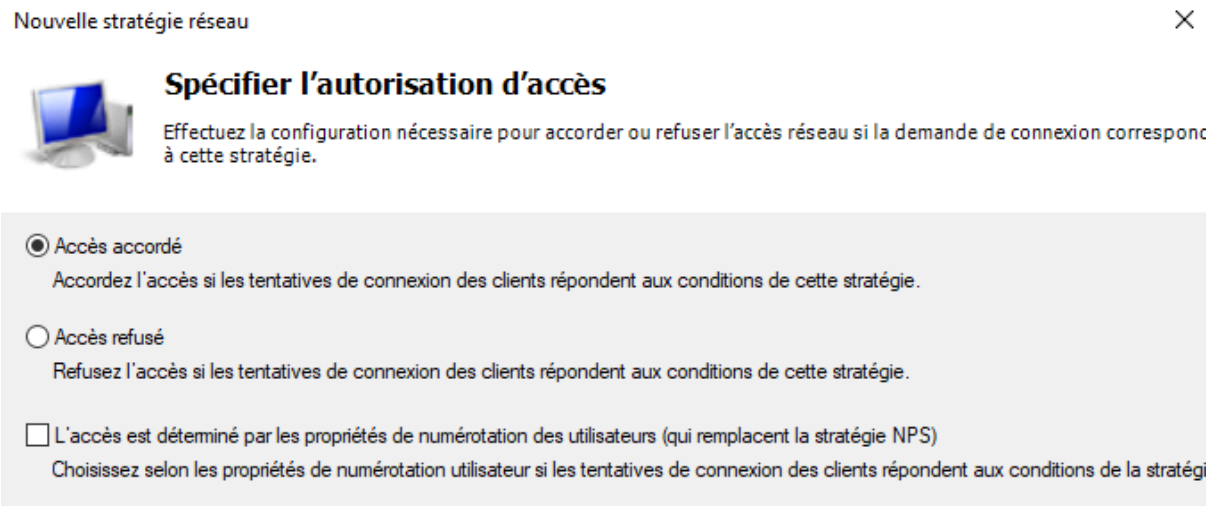
Sélection du **Type de tunnels pour connexions 802.1x standard** Ethernet.



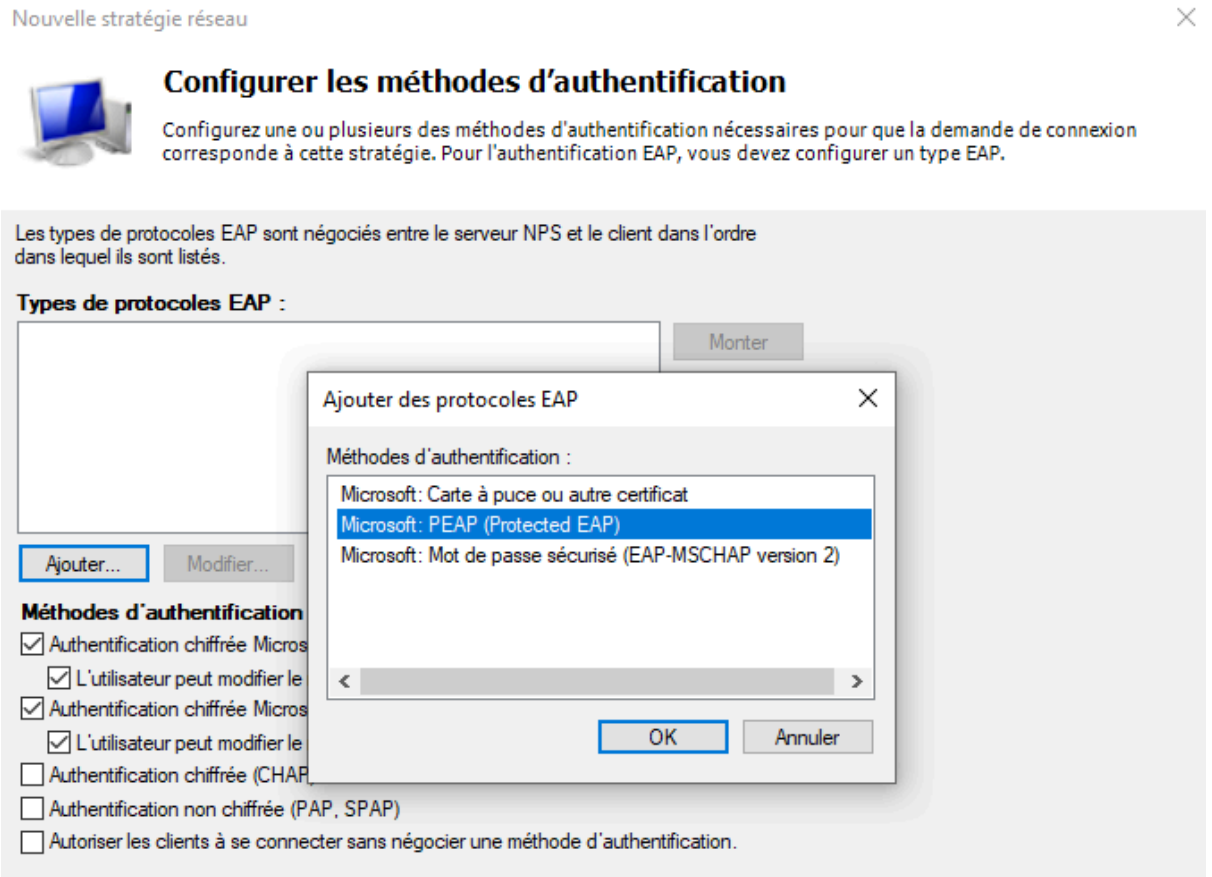
Visualisation des conditions de la stratégie réseau :



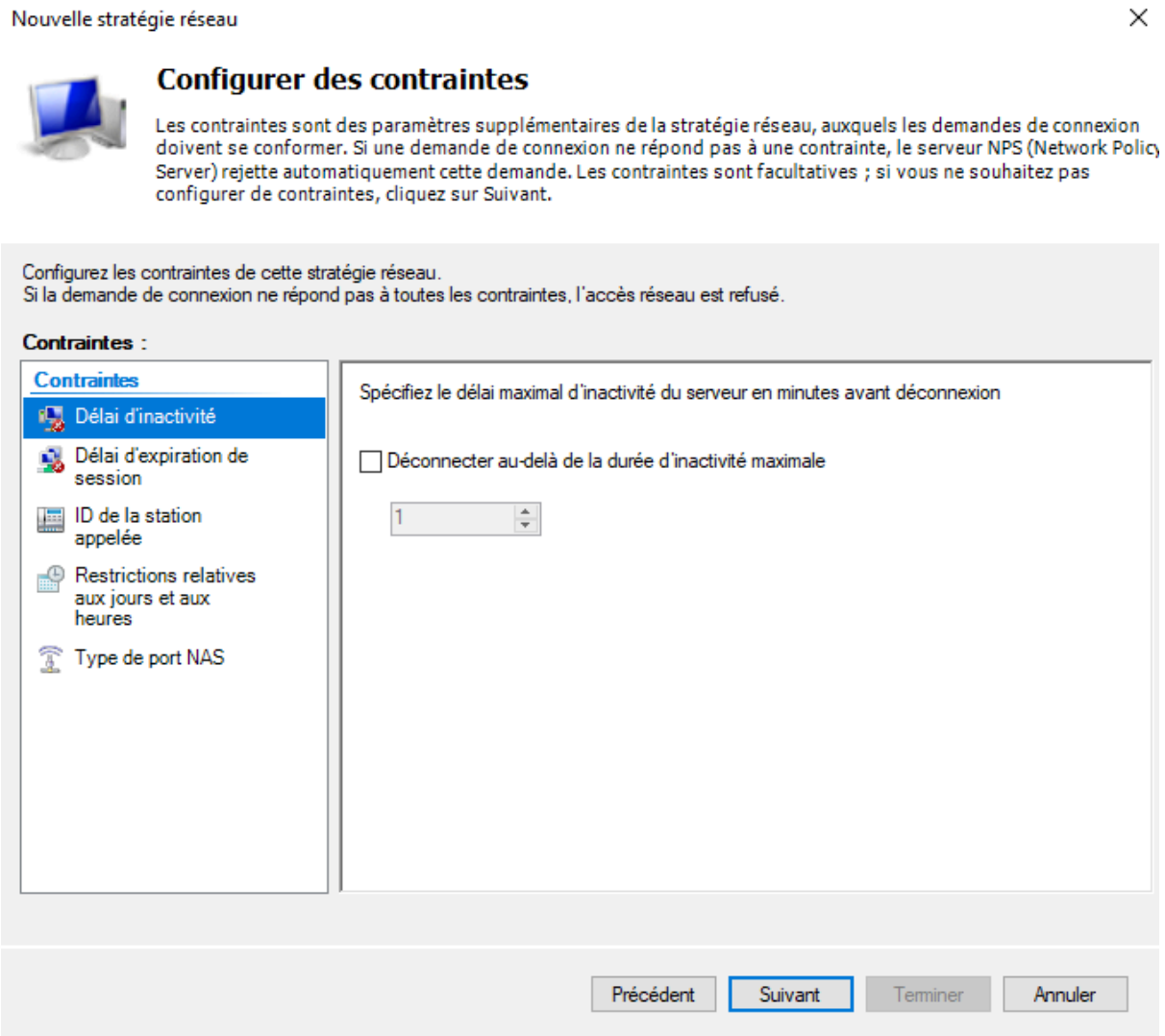
Autorisation d'accès accordé pour tous les membres du groupe Prof.



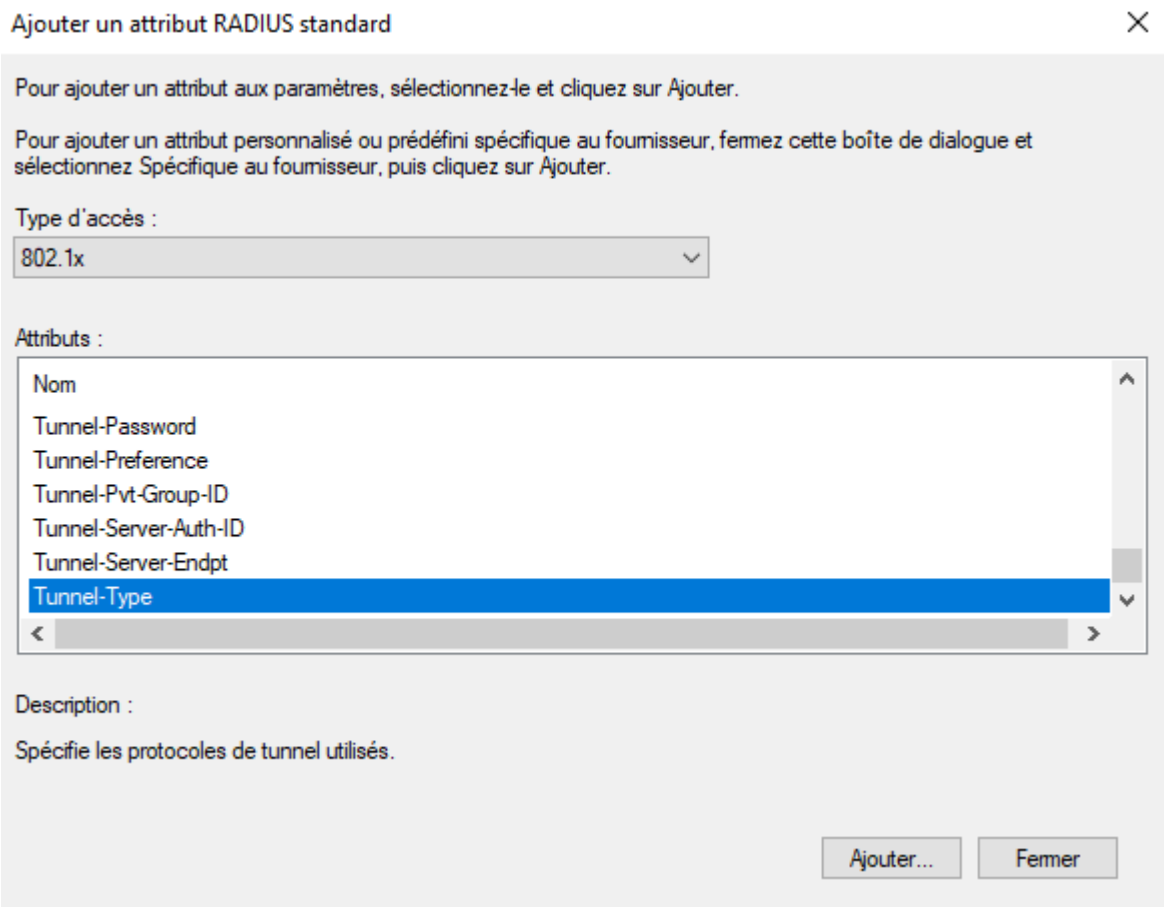
Méthode d'authentification par PEAP (Protected EAP).



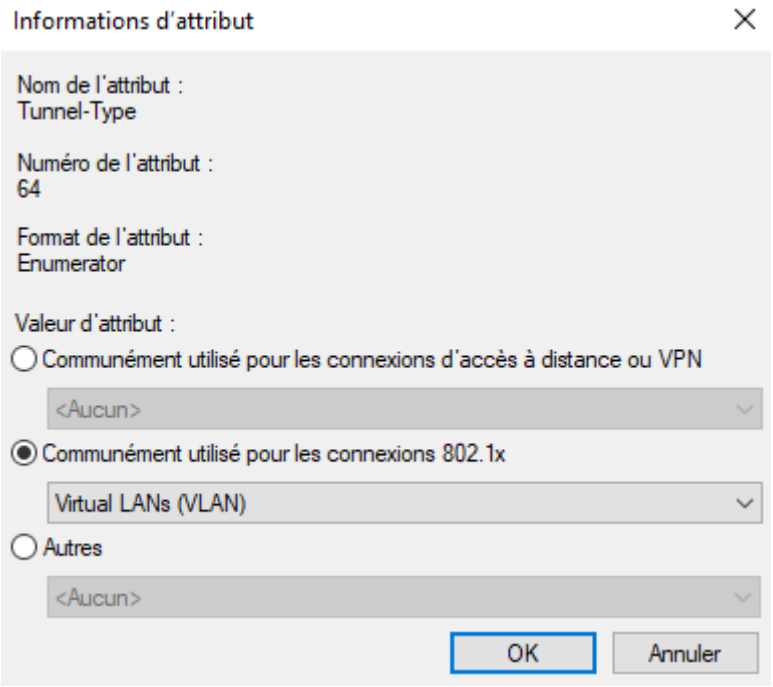
Pas de configuration des contraintes.



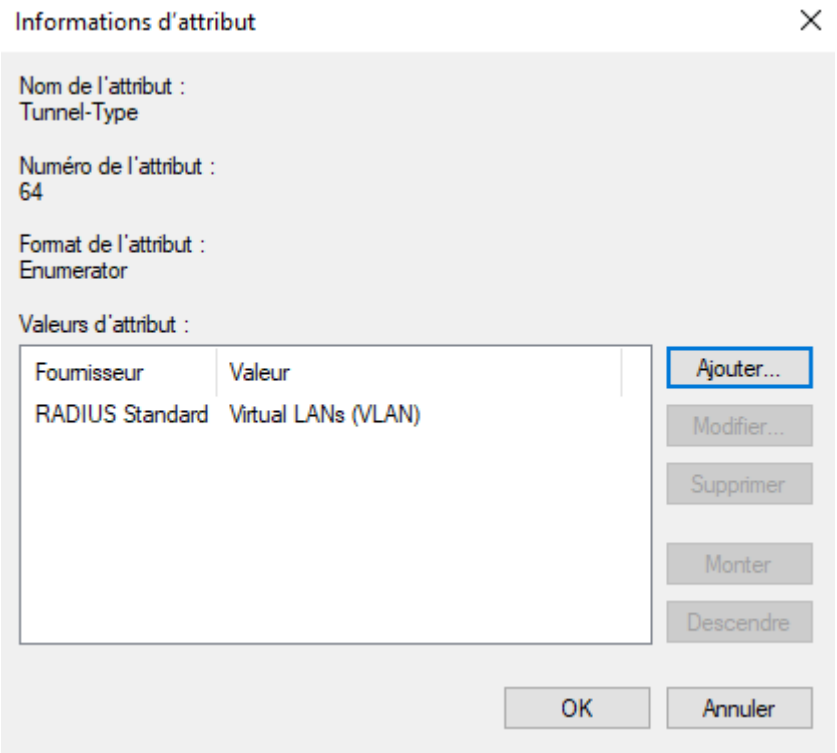
Ajout d'un attribut RADIUS standard **Tunnel-Type** en type d'accès **802.1x**.



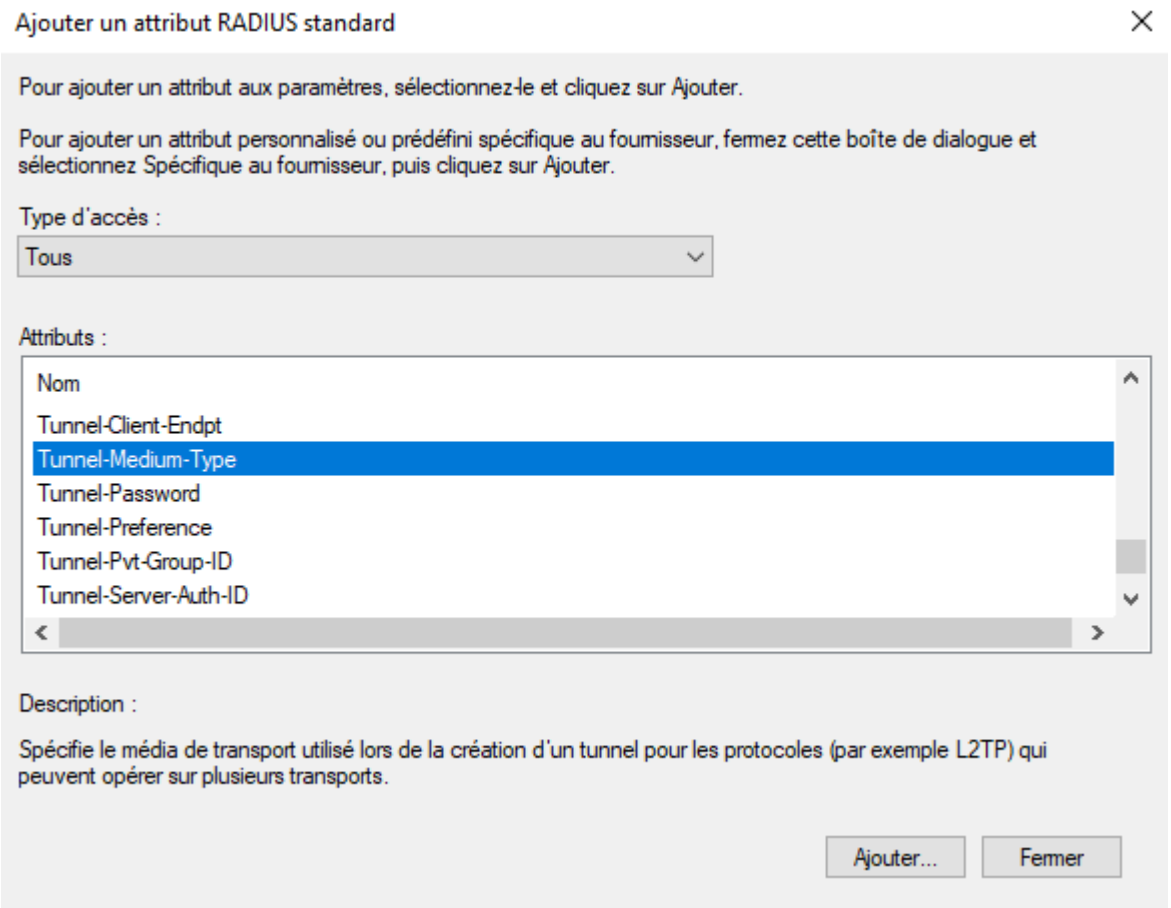
Information d'attribut communément utilisé pour les connexions 802.1x par les VLAN.



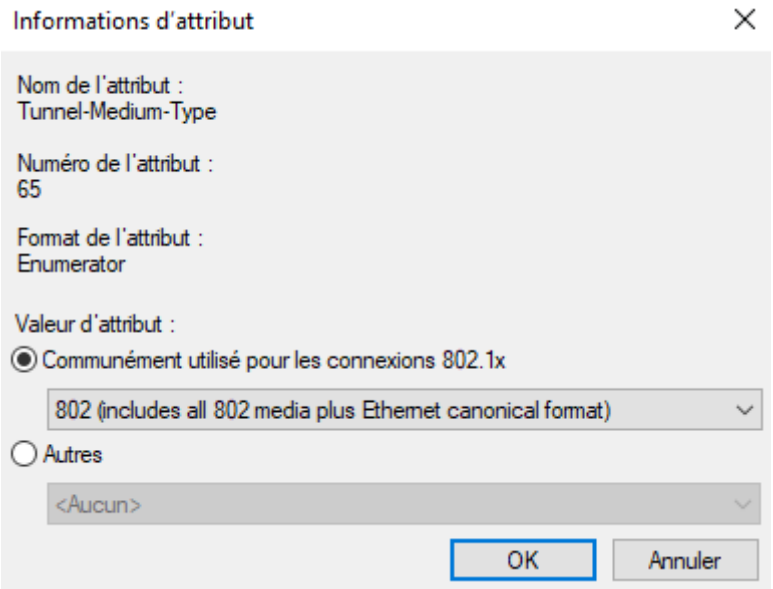
Visualisation de la valeur d'attribut :



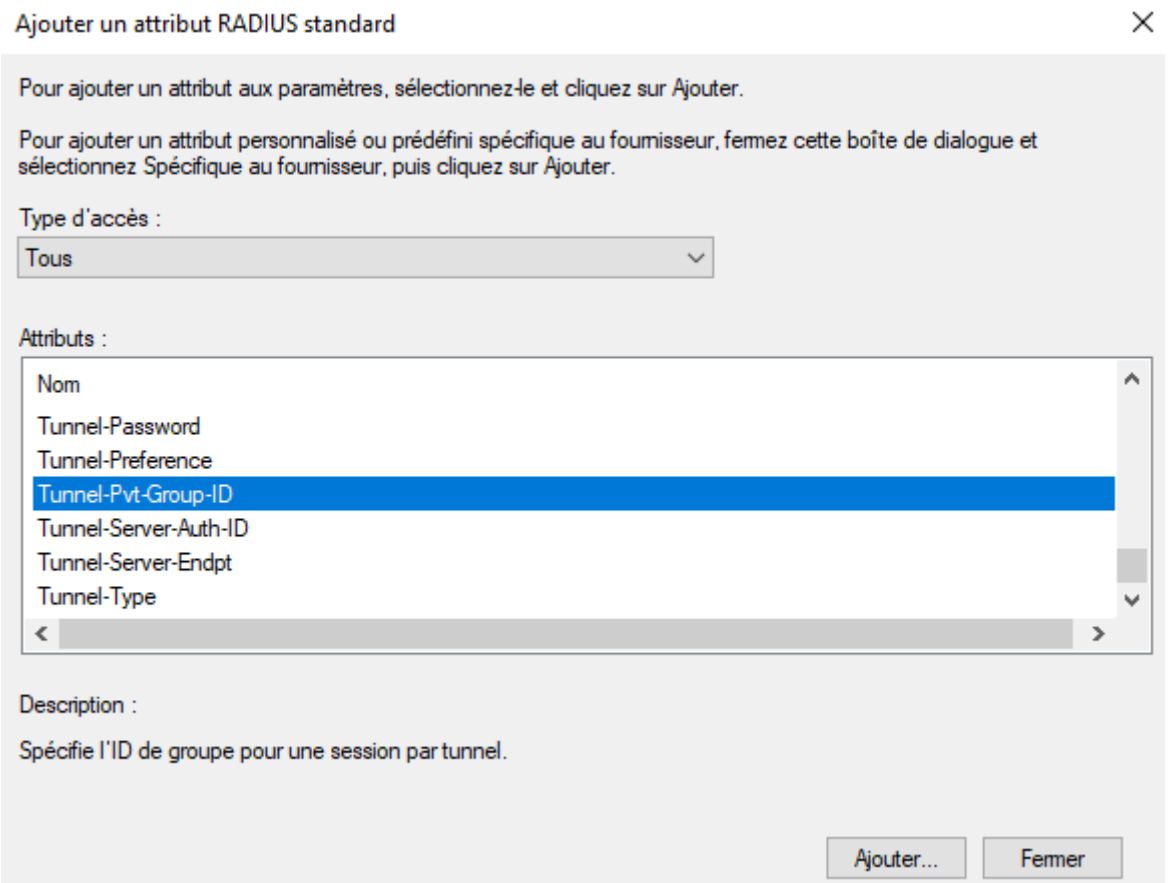
Ajout d'un attribut RADIUS standard **Tunnel-Medium-Type** en tous les types d'accès.



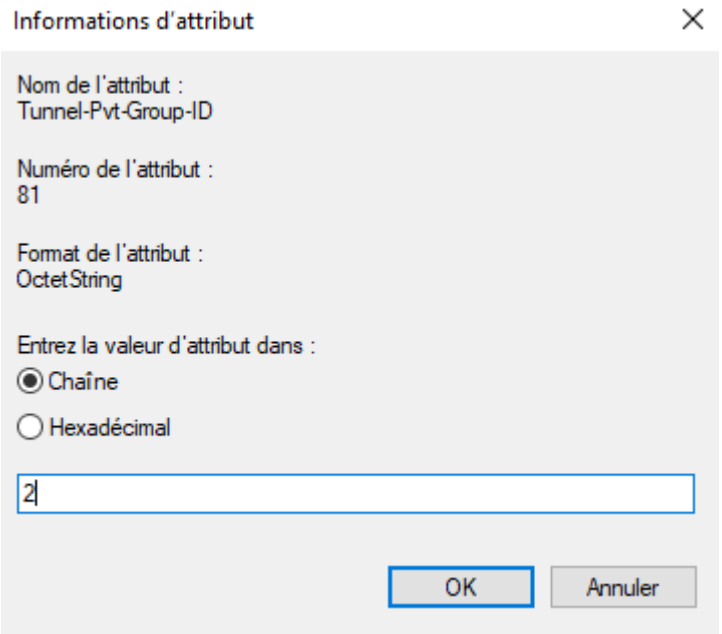
Information d'attribut communément utilisé pour les connexions 802.1x par 802 (includes all 802 media plus Ethernet canonical format).



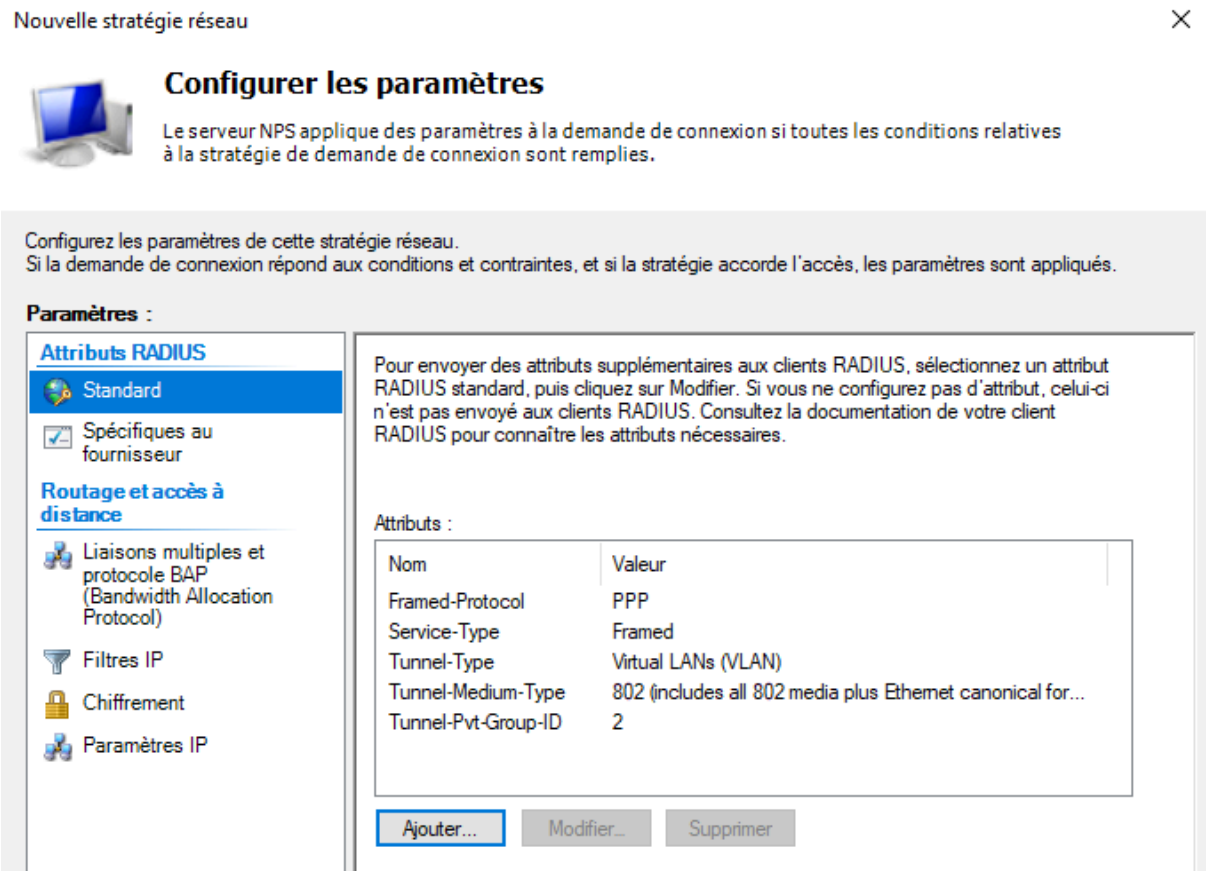
Ajout d'un attribut RADIUS standard **Tunnel-Pvt-Group-ID** en tous les types d'accès.



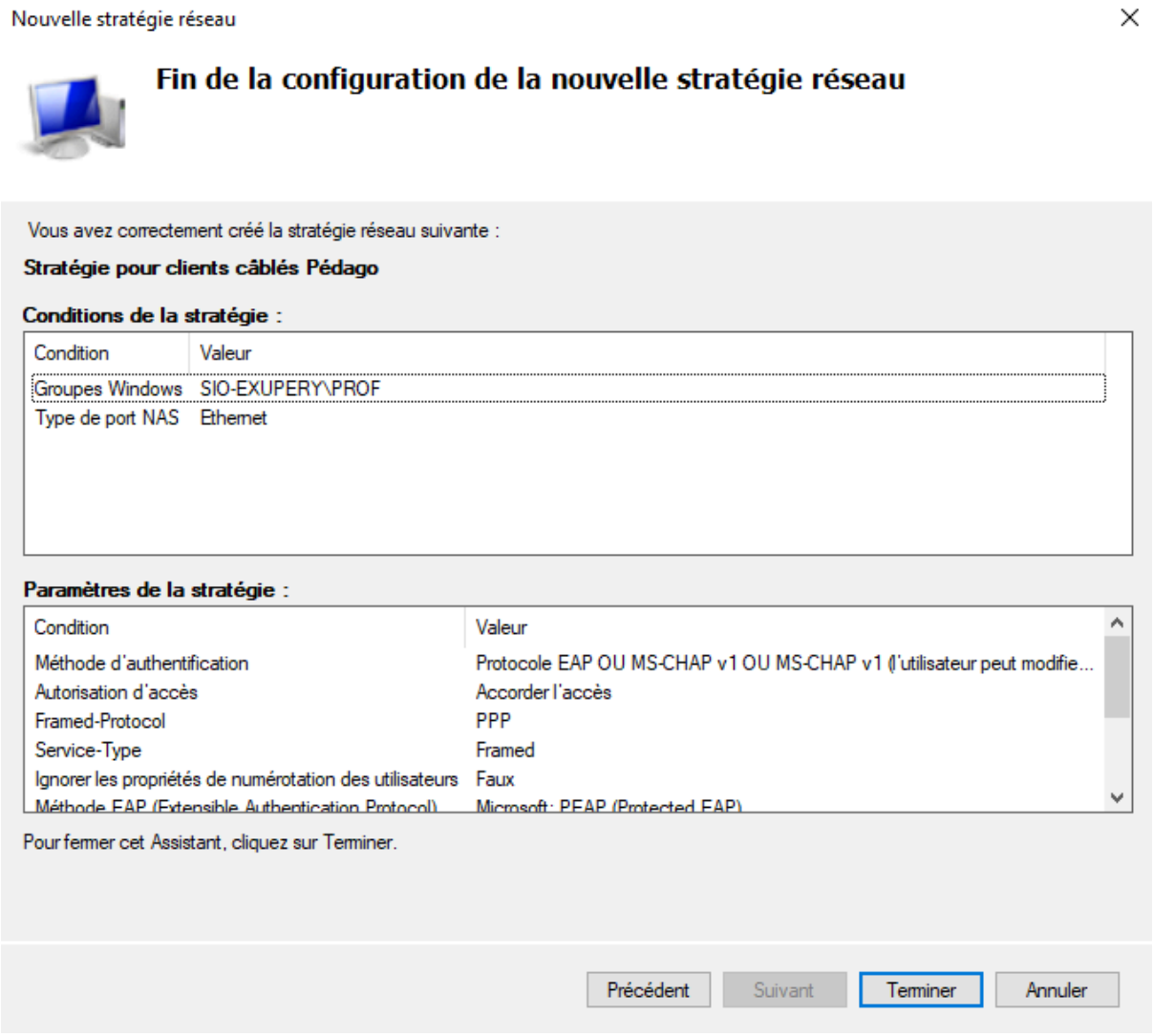
Définition du numéro de VLAN où sont positionnés les membres.

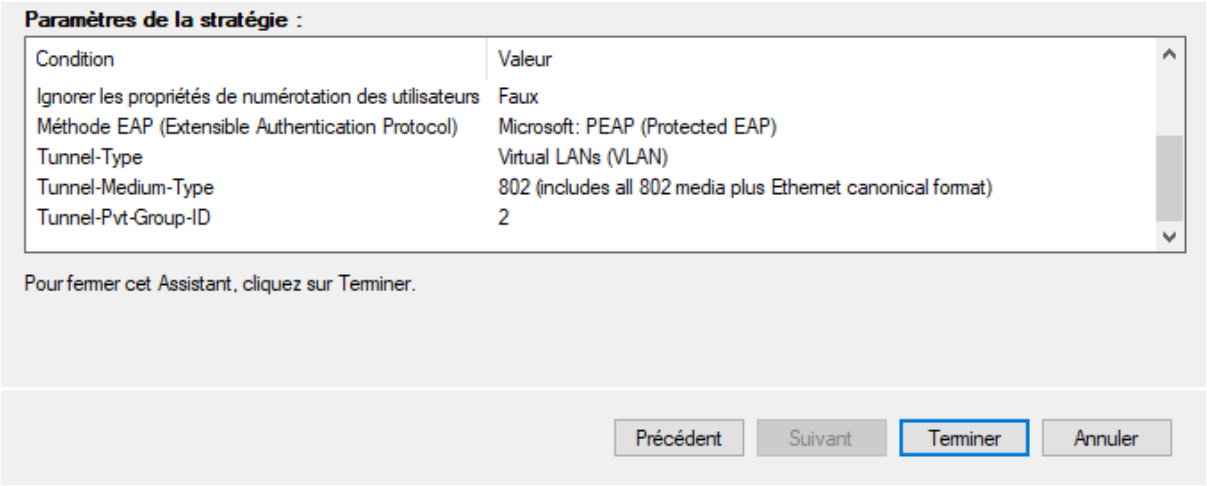


Visualisation des attributs ajoutés.

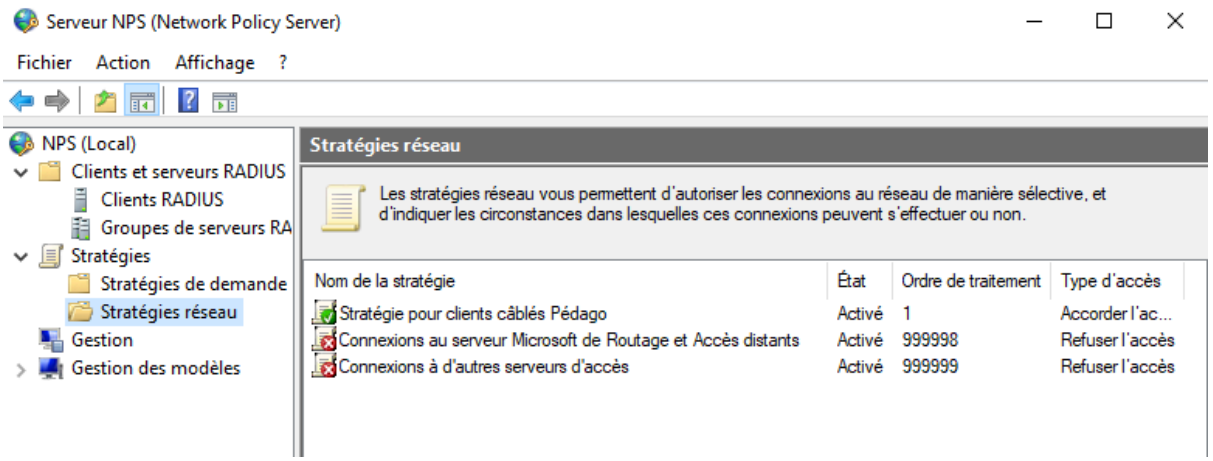


Visualisation des conditions de la stratégie.

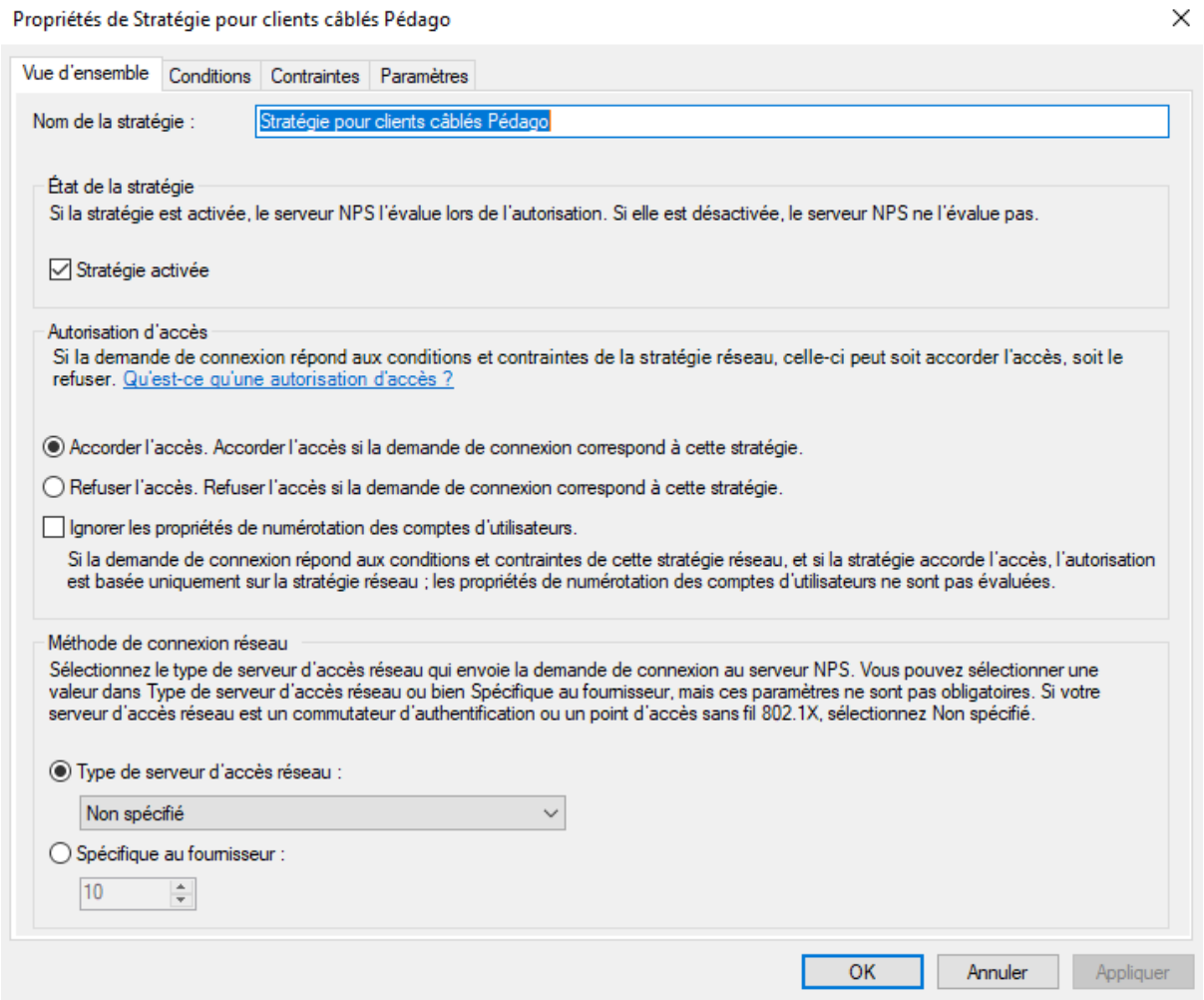




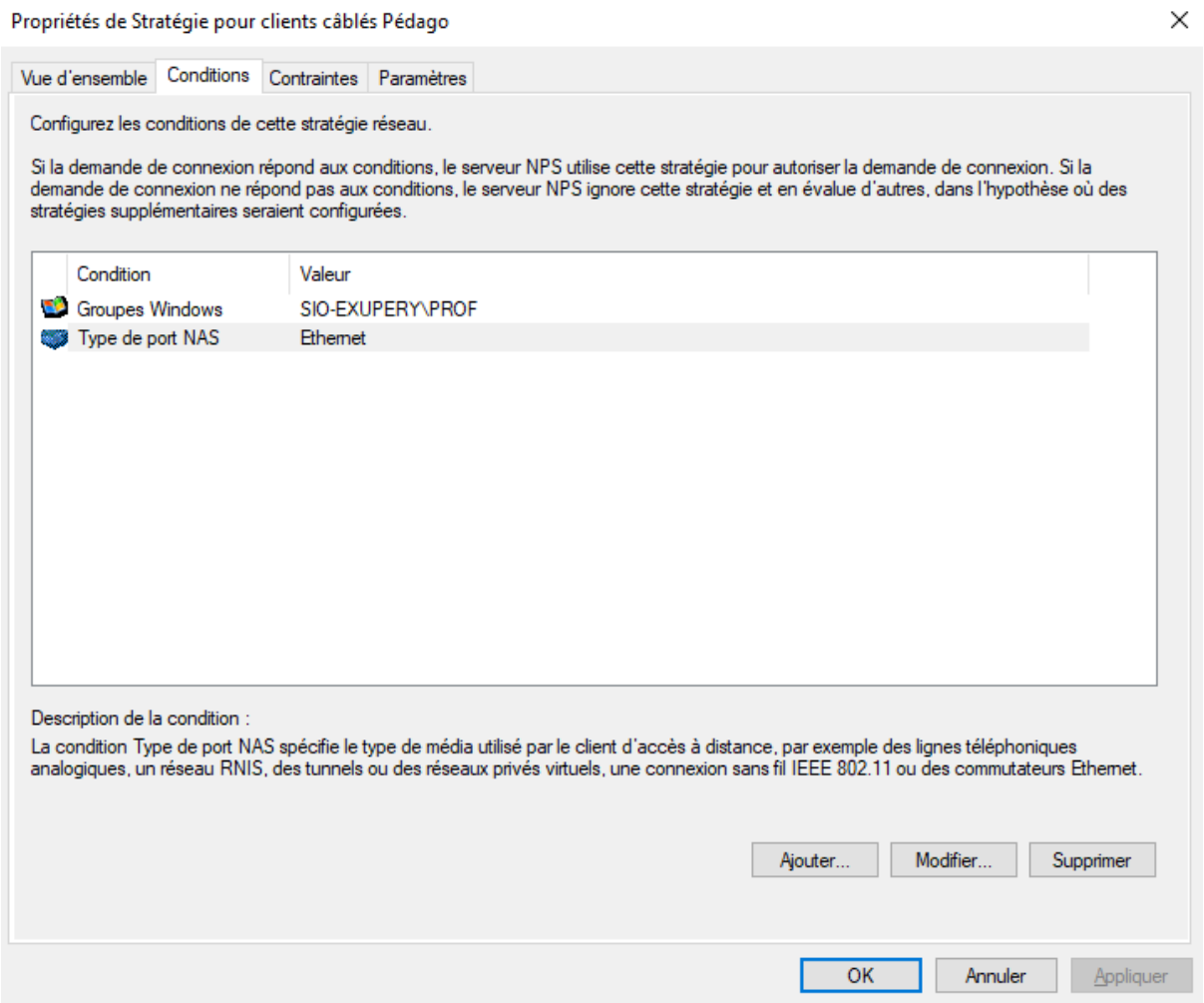
Propriété de la Stratégie réseau :



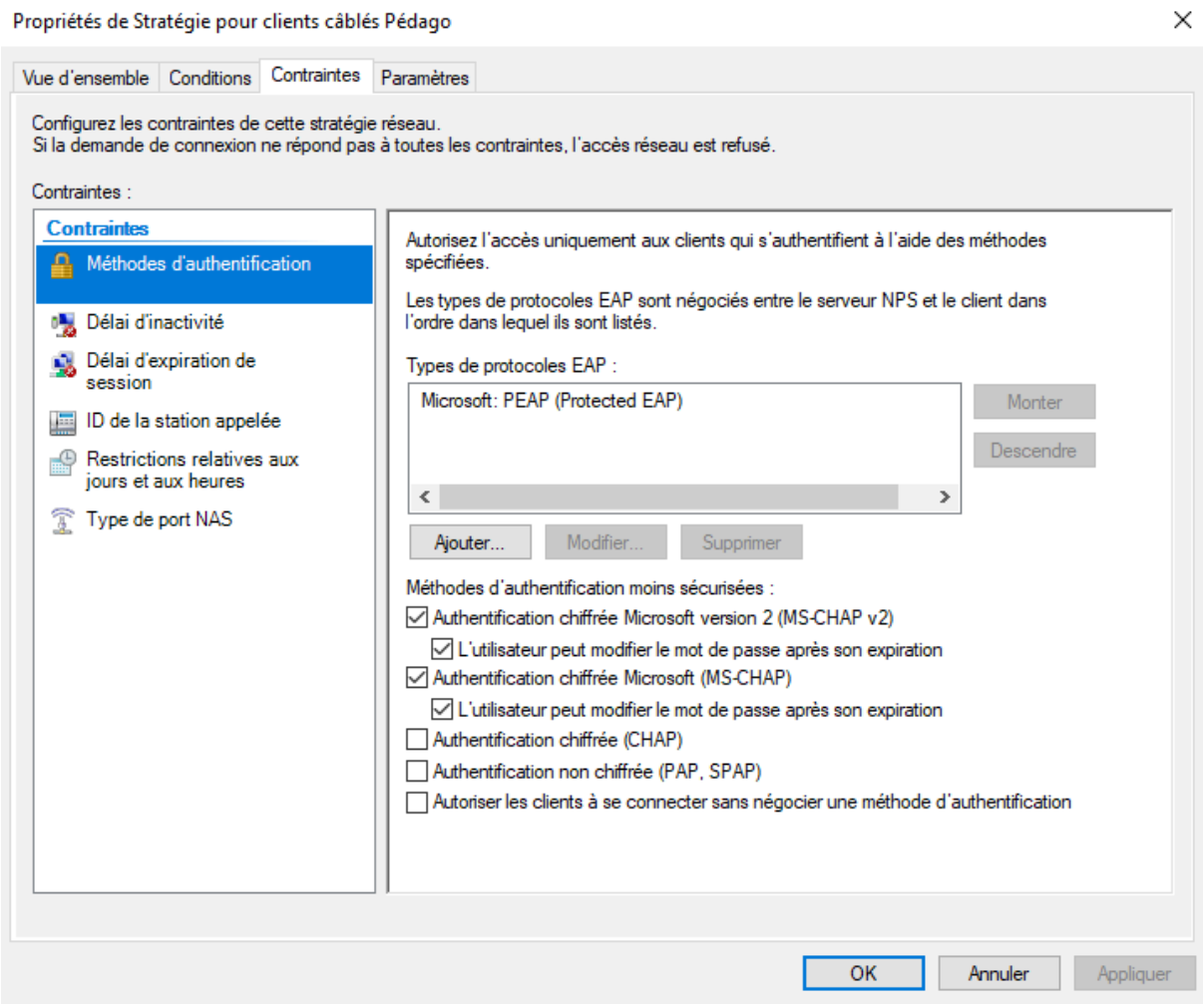
Vue d'ensemble de la Stratégie pour les clients câblés Pédago.



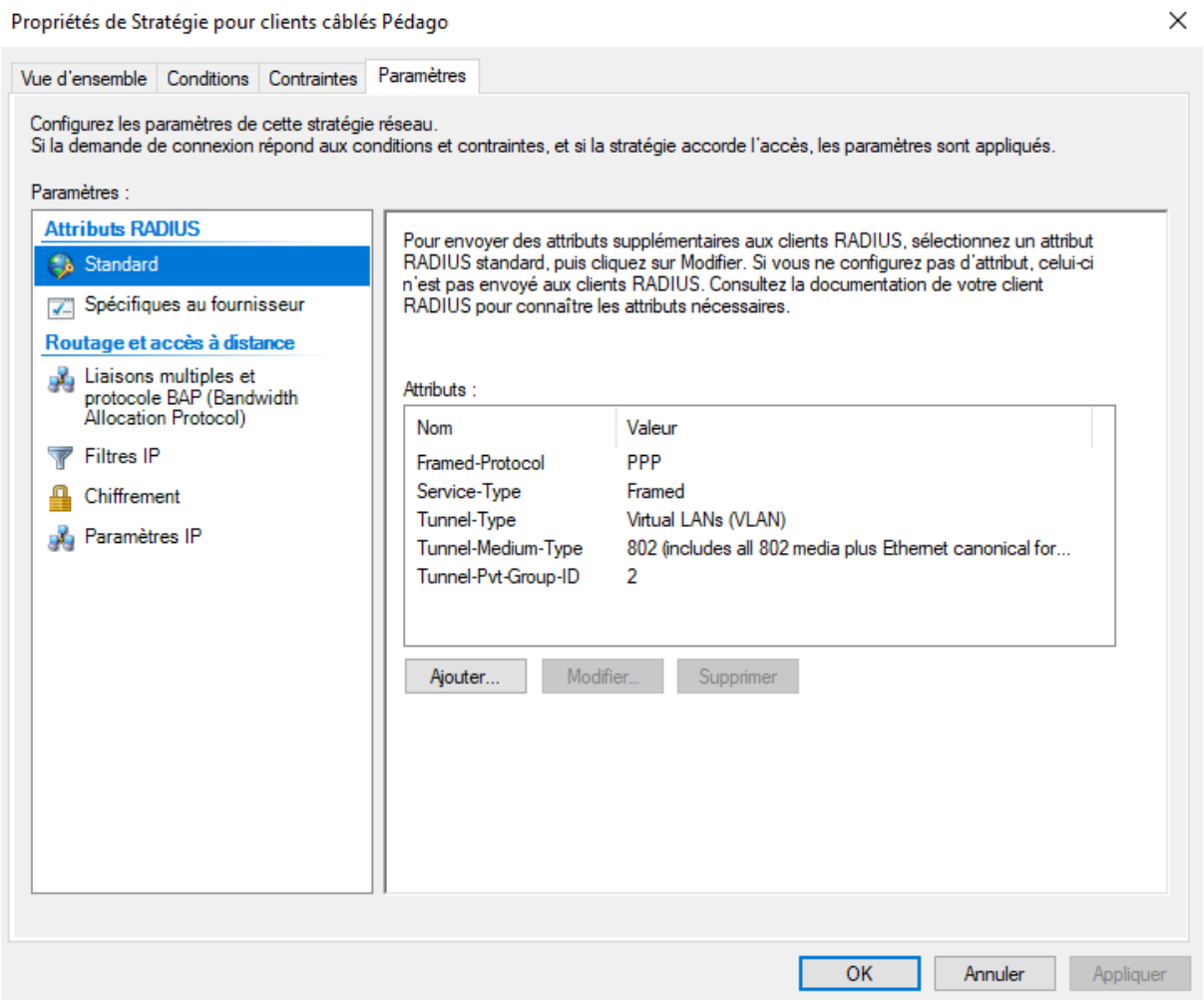
Conditions de la Stratégie pour les clients câblés Pédago.



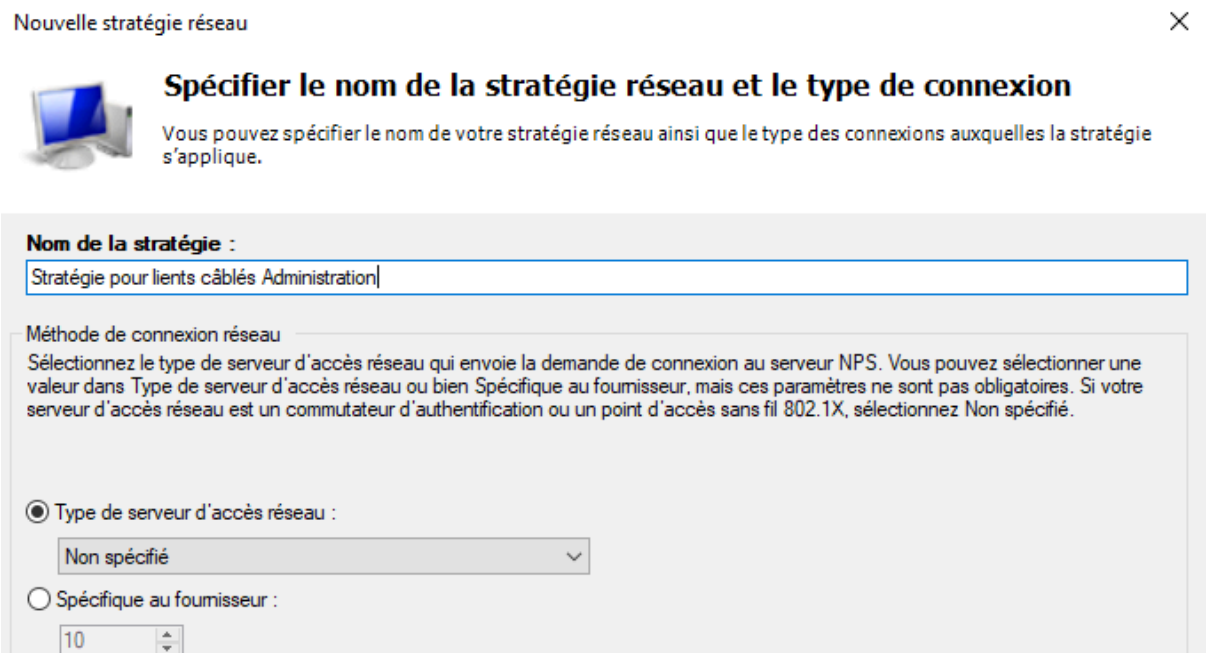
Contraintes de la Stratégie pour les clients câblés Pédago.



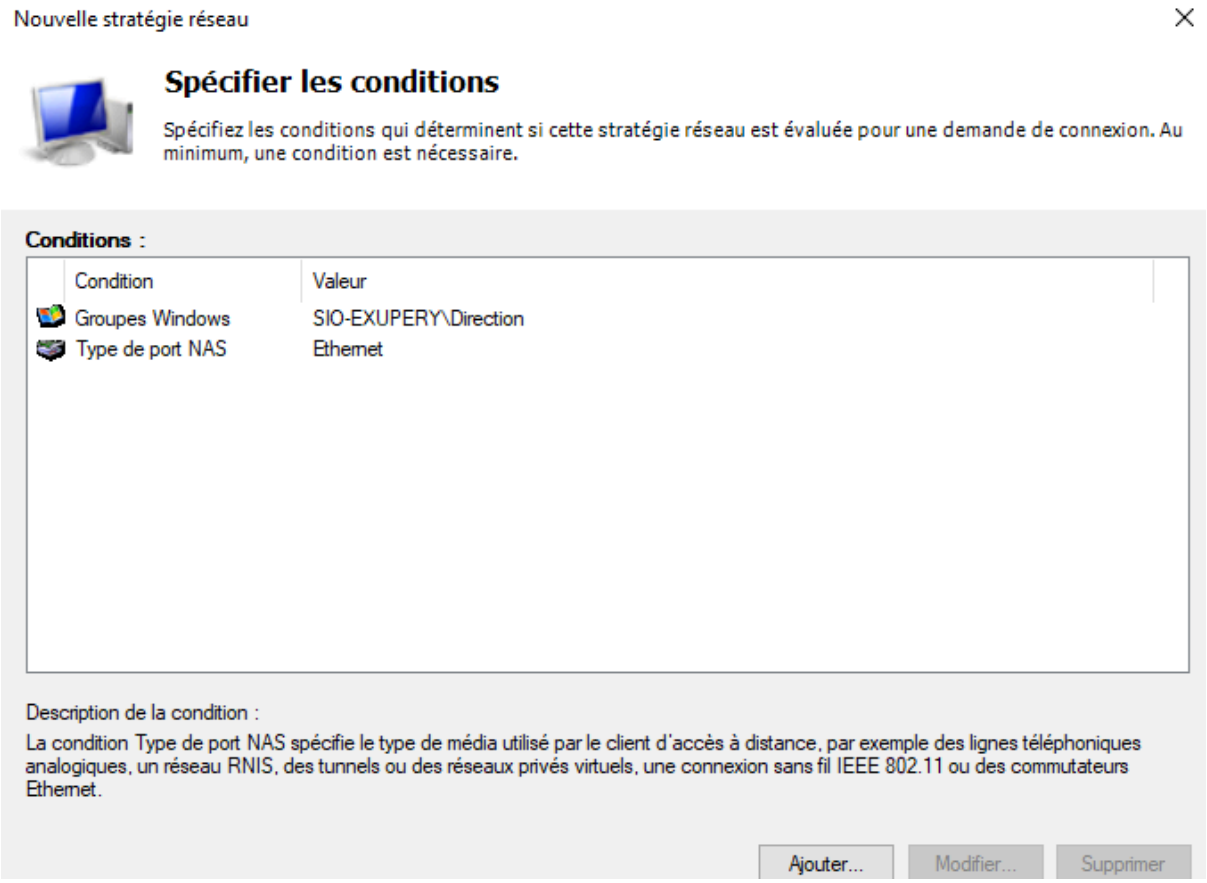
Paramètres de la Stratégie pour les clients câblés Pédago.



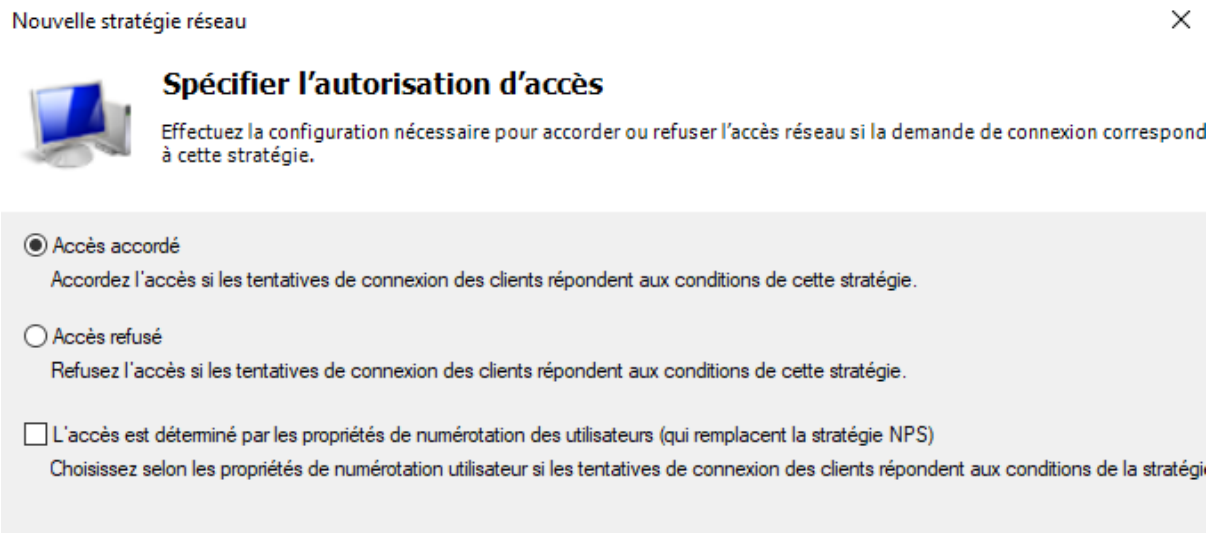
Création d'une nouvelle stratégie réseau **Stratégie pour les clients câblés Administration**.



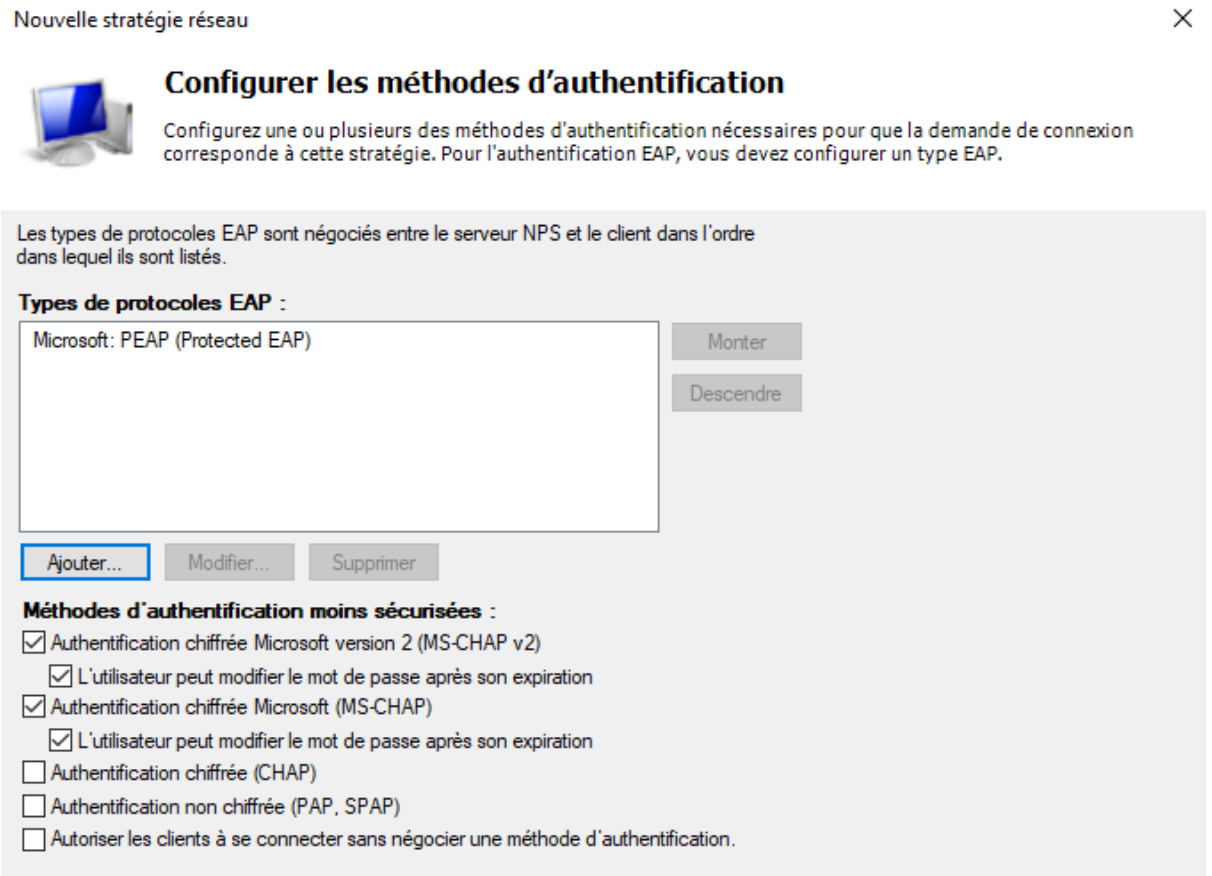
Visualisation des conditions de la stratégie réseau :



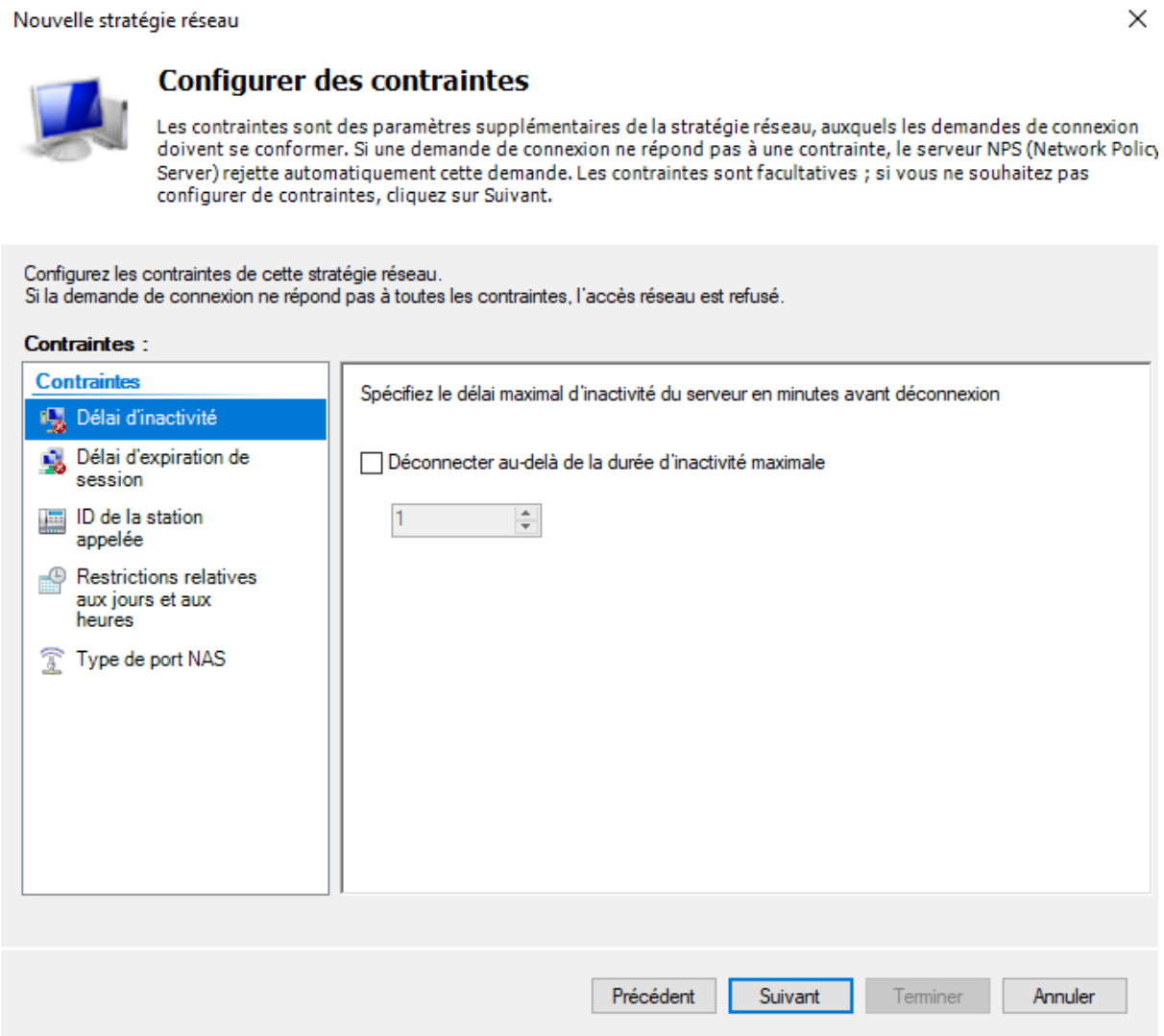
Autorisation d'accès accordé pour tous les membres.



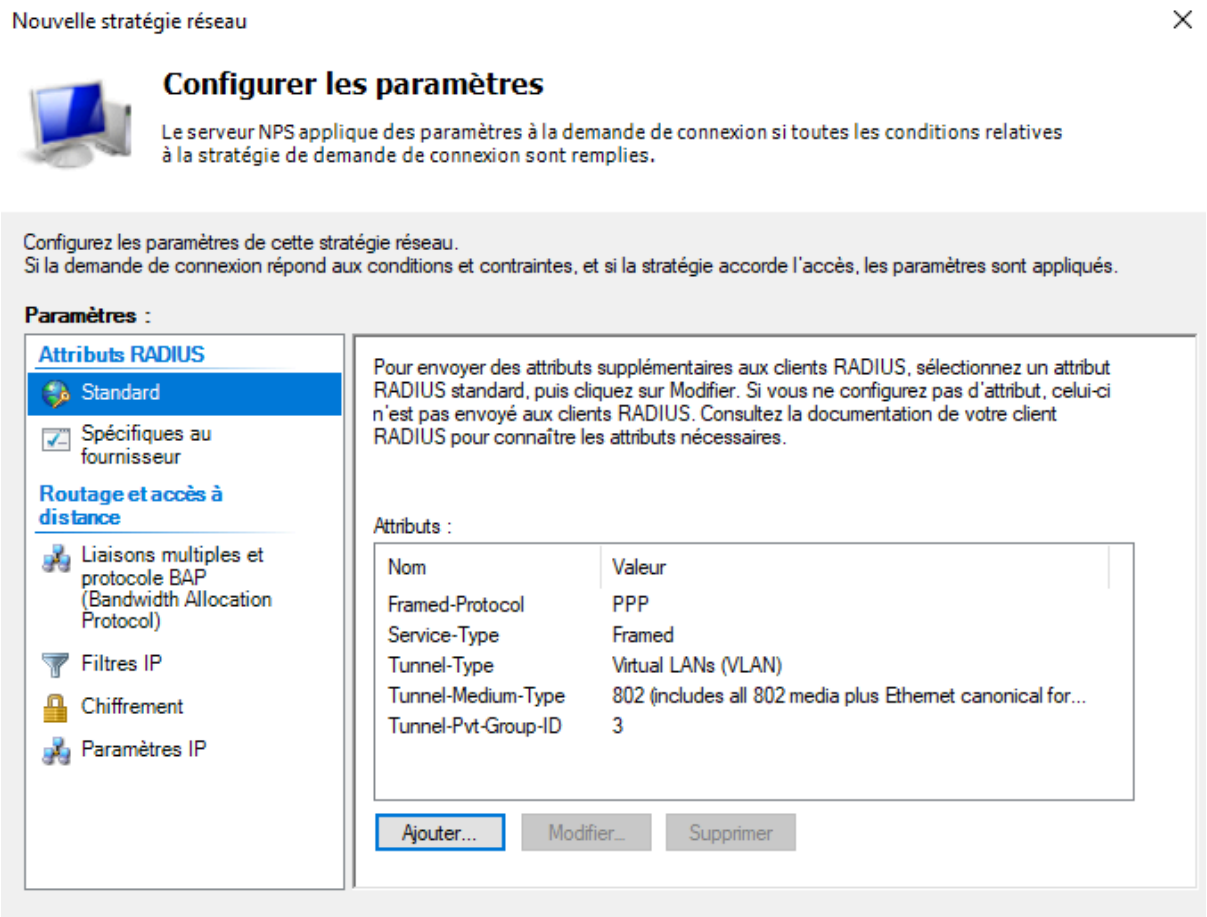
Méthode d'authentification par PEAP (Protected EAP).



Pas de configuration des contraintes.



Visualisation des attributs ajoutés.



Visualisation des conditions de la stratégie.

Nouvelle stratégie réseau

Fin de la configuration de la nouvelle stratégie réseau

Vous avez correctement créé la stratégie réseau suivante :

Stratégie pour lients câblés Administration

Conditions de la stratégie :

Condition	Valeur
Groupes Windows	SIO-EXUPERY\Direction
Type de port NAS	Ethernet

Paramètres de la stratégie :

Condition	Valeur
Méthode d'authentification	Protocole EAP OU MS-CHAP v1 OU MS-CHAP v1 (l'utilisateur peut modifie...
Autorisation d'accès	Accorder l'accès
Framed-Protocol	PPP
Service-Type	Framed
Ignorer les propriétés de numérotation des utilisateurs	Faux
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)

Pour fermer cet Assistant, cliquez sur Terminer.

Précédent | Suivant | Terminer | Annuler

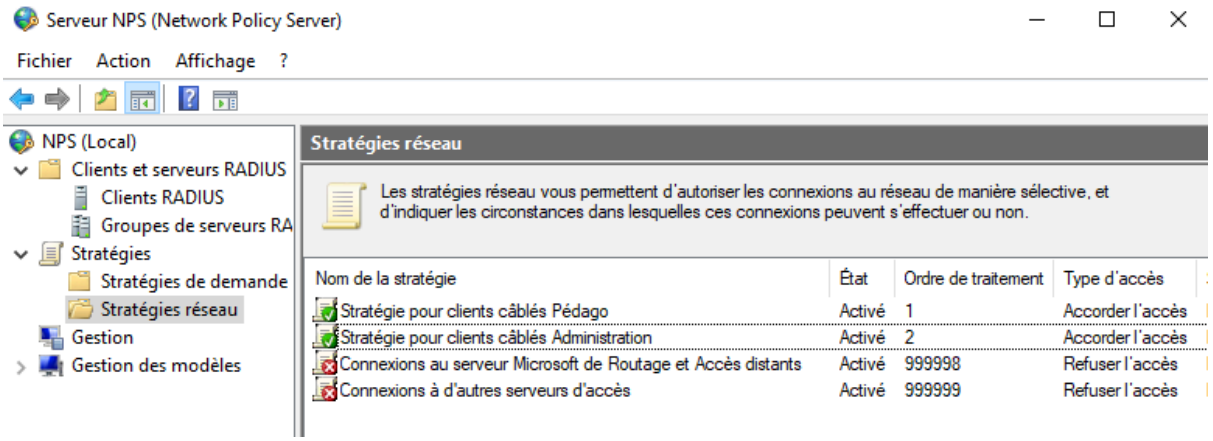
Paramètres de la stratégie :

Condition	Valeur
Ignorer les propriétés de numérotation des utilisateurs	Faux
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	3

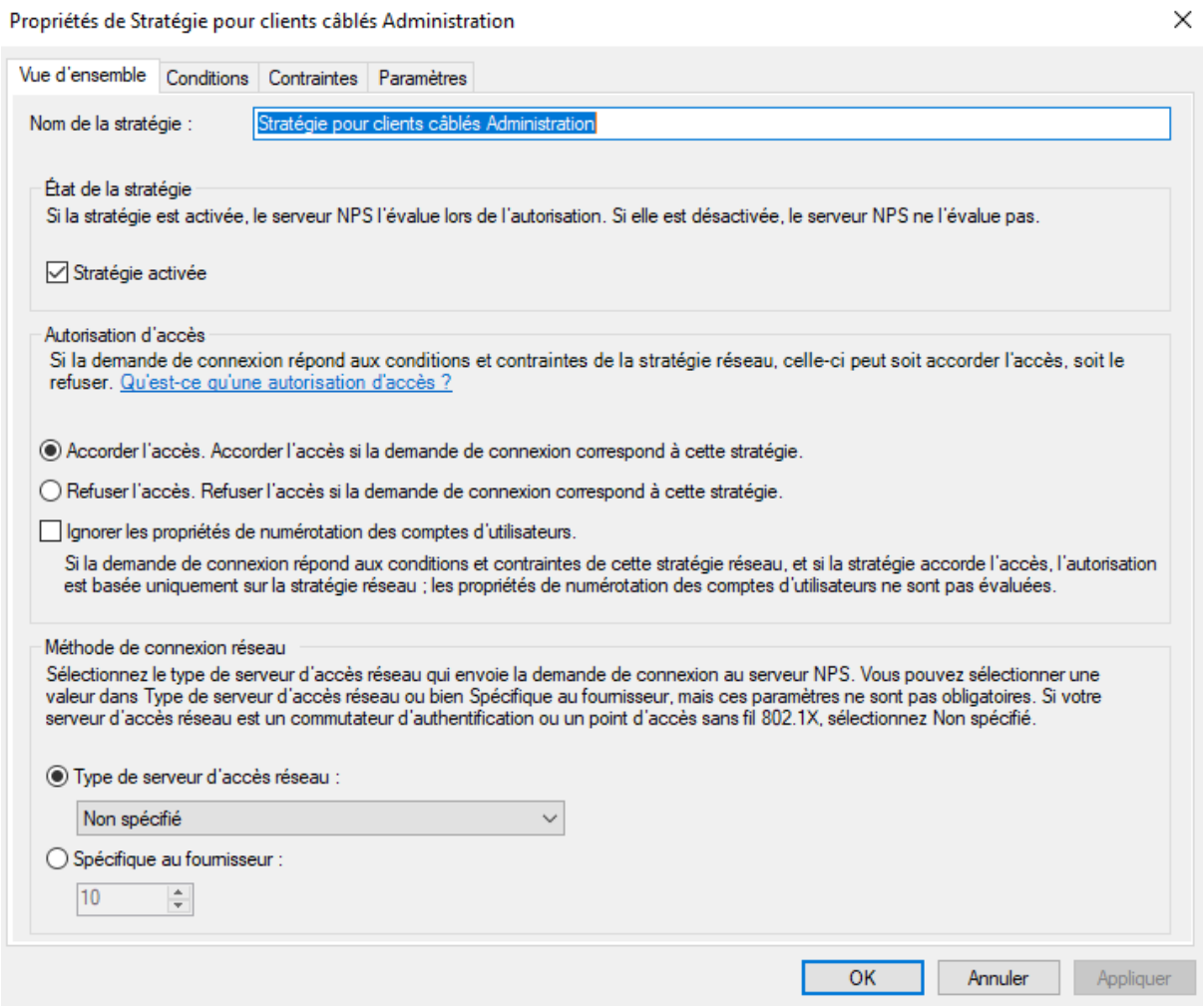
Pour fermer cet Assistant, cliquez sur Terminer.

Précédent | Suivant | Terminer | Annuler

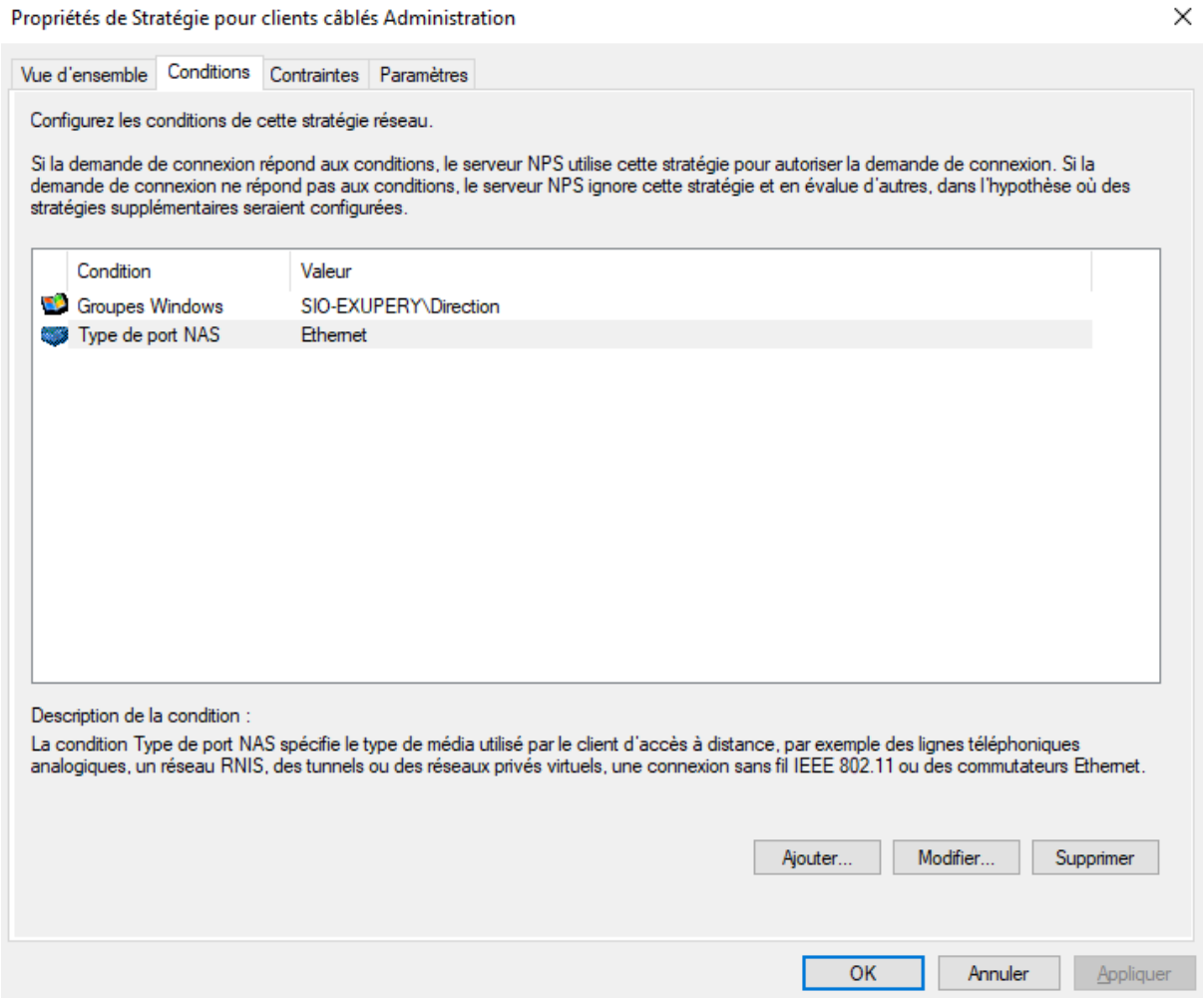
Propriété de la Stratégie réseau :



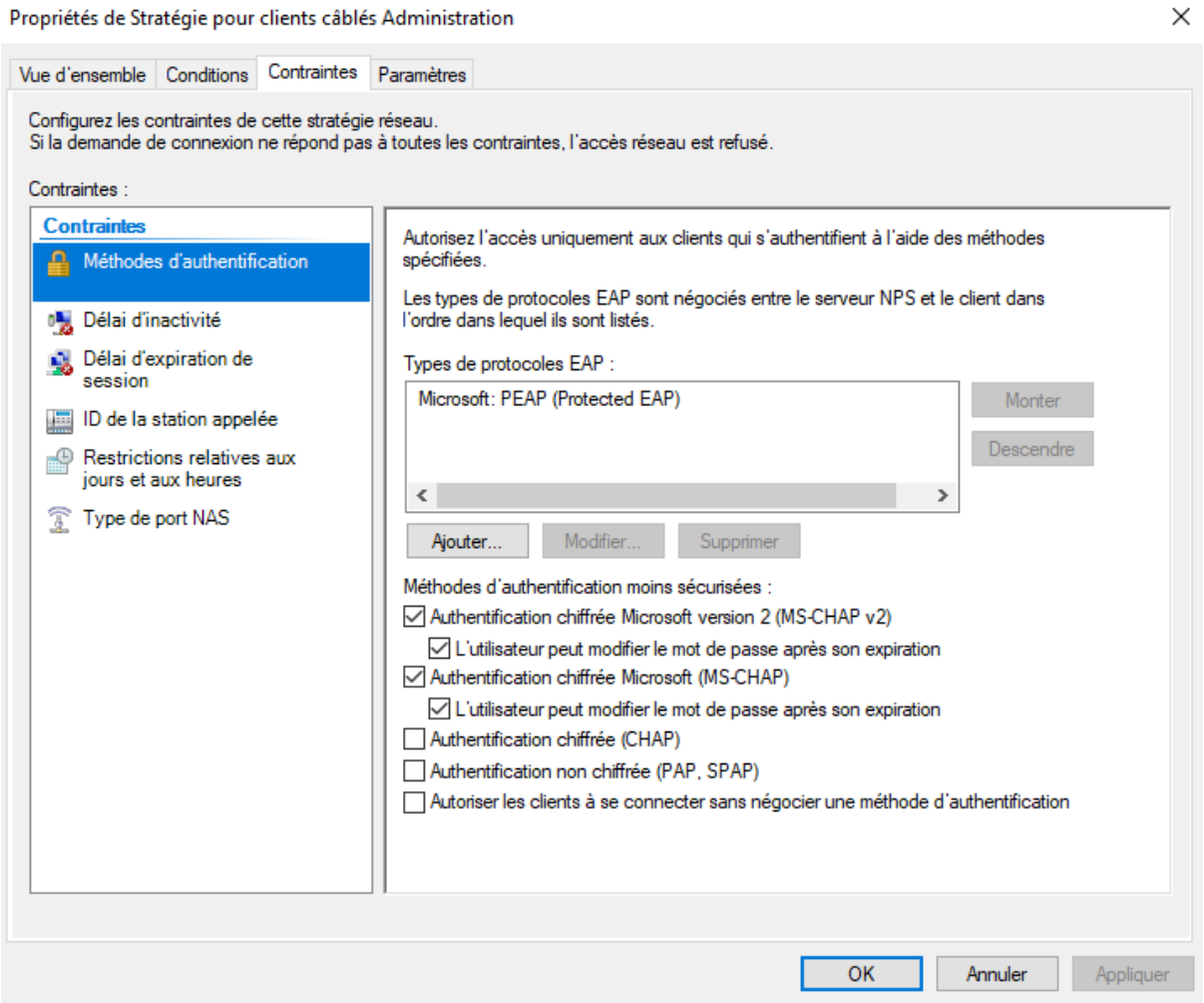
Vue d'ensemble de la Stratégie pour les clients câblés Administration.



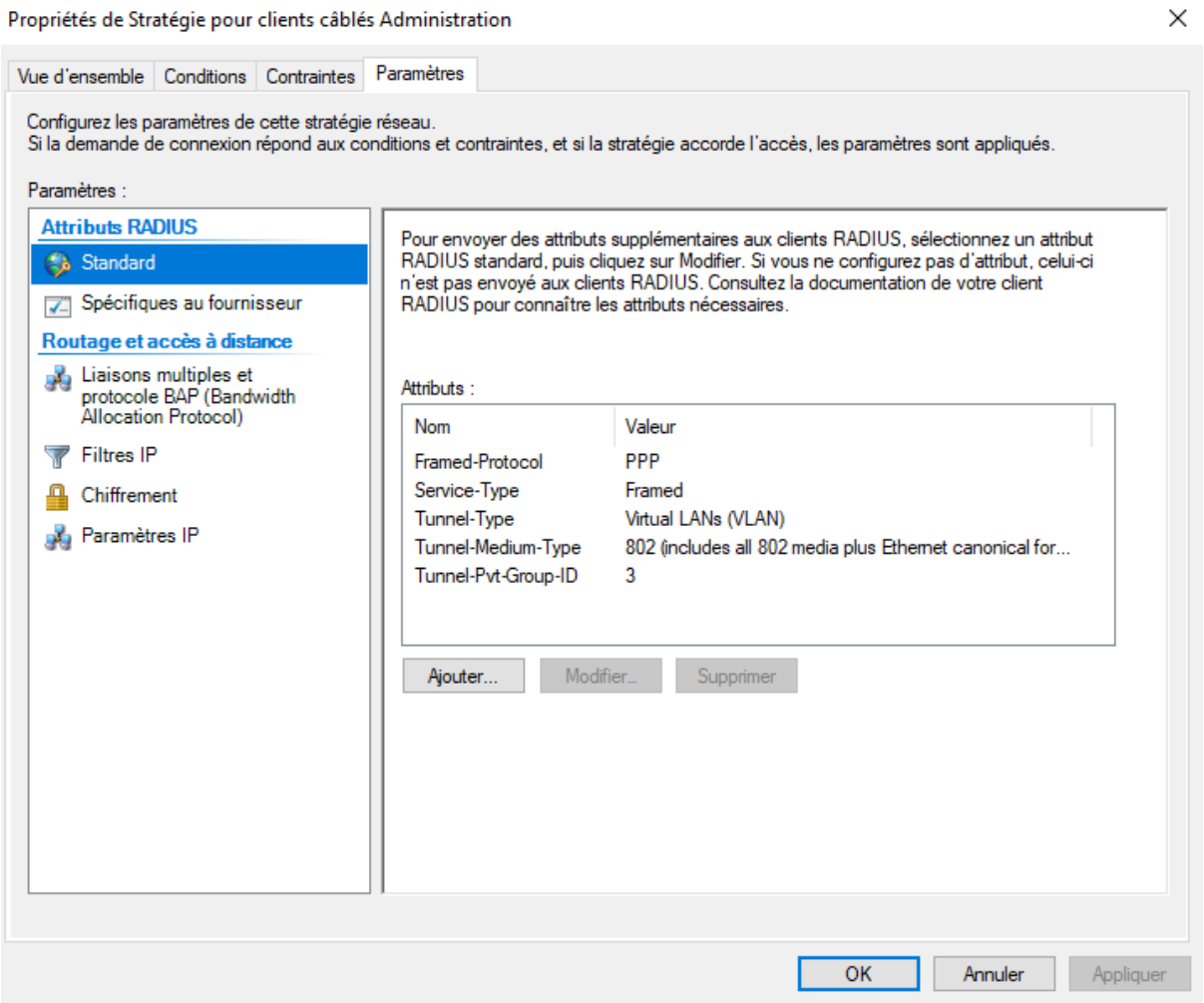
Conditions de la Stratégie pour les clients câblés Administration.



Contraintes de la Stratégie pour les clients câblés Administration.

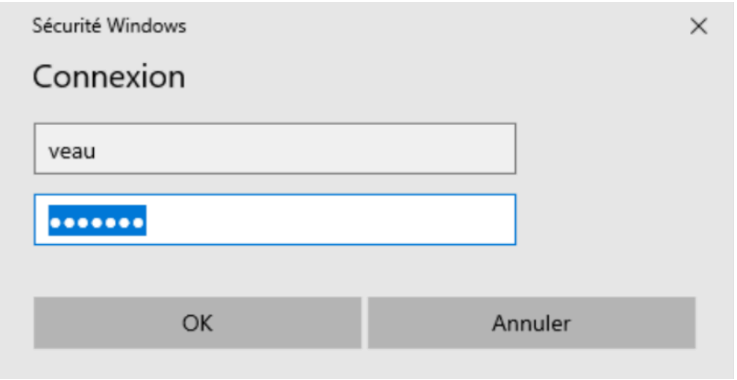


Paramètres de la Stratégie pour les clients câblés Administration.

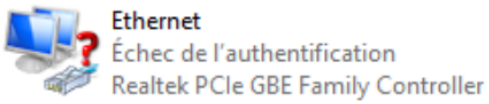


4. Demande de connexion des utilisateurs rveau et cgeley

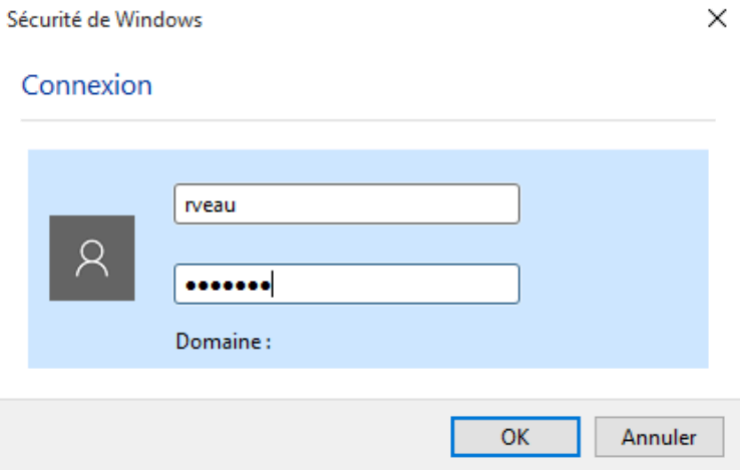
Une tentative d'authentification 802.1X est effectuée avec les identifiants utilisateur sur le poste client.

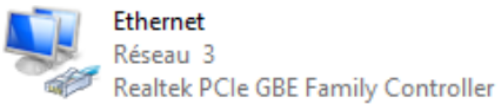


L'authentification échoue dans un premier temps sur l'interface Ethernet.



Après correction, la connexion réseau est rétablie et l'interface Ethernet devient active.





La commande **ipconfig /all** confirme l'attribution d'une adresse IP et des paramètres réseau via DHCP.

```
Invite de commandes
C:\Users\admin>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . : G101-MSI-C
   Suffixe DNS principal . . . . . . . :
   Type de noeud. . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . : Non

Carte Ethernet Ethernet Haut :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 30-9C-23-A5-90-CA
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::7c5c:f03f:366c:5a2a%6(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.2(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.240
   Bail obtenu. . . . . . . . . . . . . . : jeudi 26 mars 2026 12:10:52
   Bail expirant. . . . . . . . . . . . . : vendredi 27 mars 2026 12:10:51
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . : 523279395
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-23-3F-D2-C9-50-3E-AA-03-ED-39
   Serveurs DNS. . . . . . . . . . . . . : 192.168.1.50
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Users\admin>
```

Le switch indique que le port Fa0/7 est authentifié (AUTHORIZED) tandis qu'un autre port reste non autorisé.

```
S1#sh dot1x all summary
Interface        PAE     Client          Status
----------------------------------------------------------
Fa0/7            AUTH    309c.23a5.90ca  AUTHORIZED
Fa0/8            AUTH    none            UNAUTHORIZED
S1#
```

Le switch confirme que le port Fa0/7 est associé au VLAN "Pédagogie", confirmant ainsi l'attribution dynamique du VLAN après l'authentification 802.1X.

```
S1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
2    Pedagogie                        active    Fa0/7
3    Administration                   active
4    Serveurs                         active    Fa0/2
99   Gestion                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Annexe :

Mémo commandes pour sauvegarder la configuration sur les équipements réseaux Cisco :

- **copy running-config startup-config**: Cette commande copie la configuration en cours vers la configuration de démarrage, rendant la configuration persistante. **Lien**
- **write memory**: Cette commande enregistre la configuration dans la NVRAM, la rendant persistante. **Lien**
- **archive**: Cette commande permet de sauvegarder la configuration dans la mémoire flash, ce qui est utile pour la sauvegarde et la restauration. **Lien**