

TP1 – Mise en œuvre d’une infrastructure 802.1x : connexions câblées

Sommaire :

1./ Configuration Switch

2.1/ Situation de départ

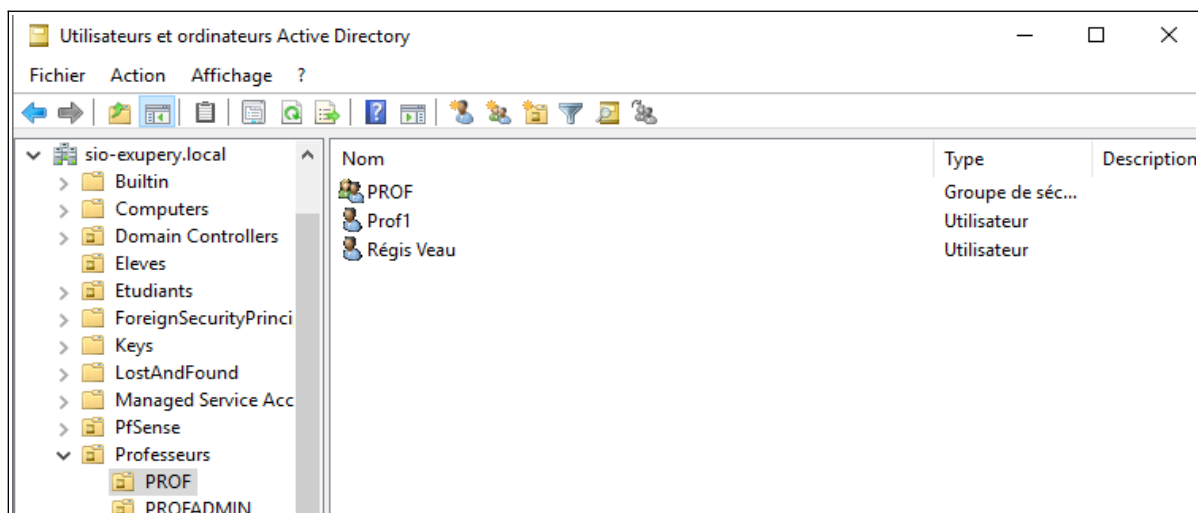
2.2/ Ajout du rôle Services de certificats Active Directory

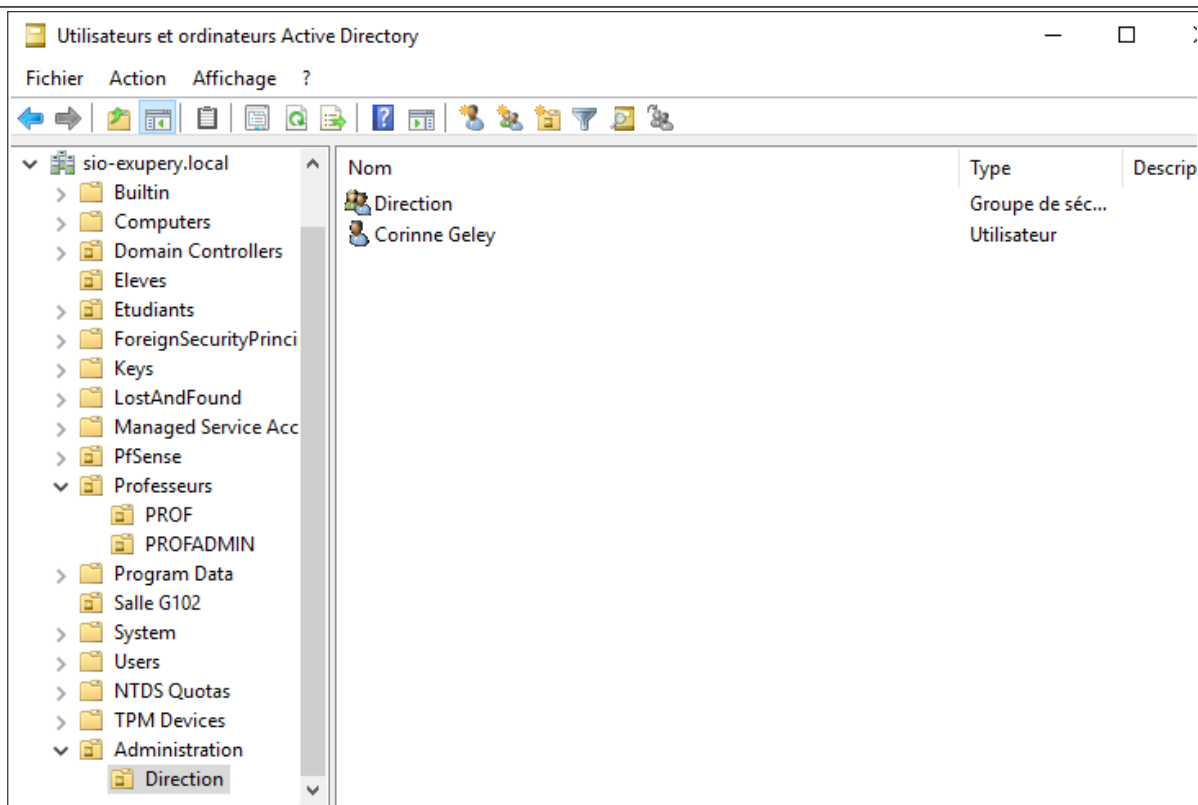
2.3/ Installation du service NPS

2.4/ Configuration du serveur RADIUS NPS

1./ Configuration Switch

```
S1(config)#aaa new-model
S1(config)#aaa authentication dot1x default group radius
S1(config)#aaa authorization network default group radius
S1(config)#dot1x system-auth-control
```





Deux unités d'organisation sont présentes :

- Professeurs/Prof avec l'utilisateur Régis Veau dans le groupe Prof.
- Administration/Direction avec l'utilisateur Corinne Geley dans le groupe Direction.

2.2/ Ajout du rôle Services de certificats Active Directory

Configuration des services de certificats Active Directory

— □ ×

Confirmation

SERVEUR DE DESTINATION
AD.sio-exupery.local

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.

⬅ **Services de certificats Active Directory**

Autorité de certification

Type d'AC :	Racine d'entreprise
Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Algorithme de hachage :	SHA256
Longueur de la clé :	2048
Autoriser l'interaction de l'administrateur :	Désactivé
Période de validité du certificat :	09/03/2028 10:24:00
Nom unique :	CN=sio-exupery-AD-CA,DC=sio-exupery,DC=local
Emplacement de la base de données de certificats :	C:\Windows\system32\CertLog
Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

— □ ×

Résultats

SERVEUR DE DESTINATION
AD.sio-exupery.local

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

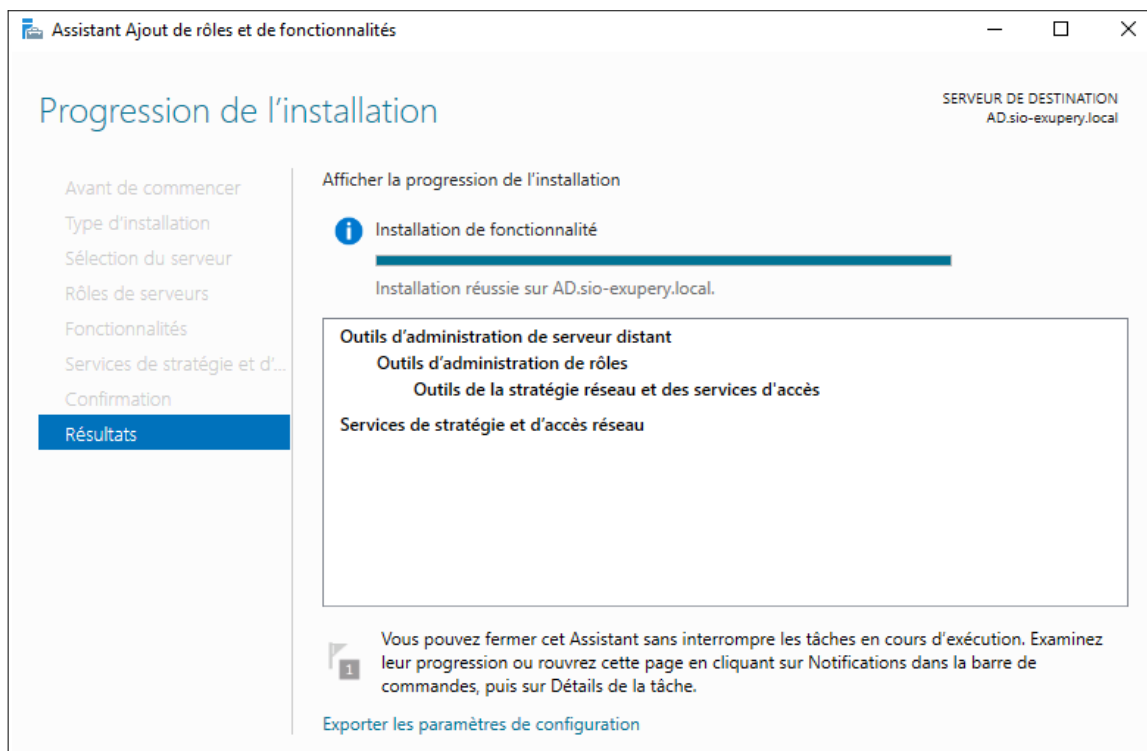
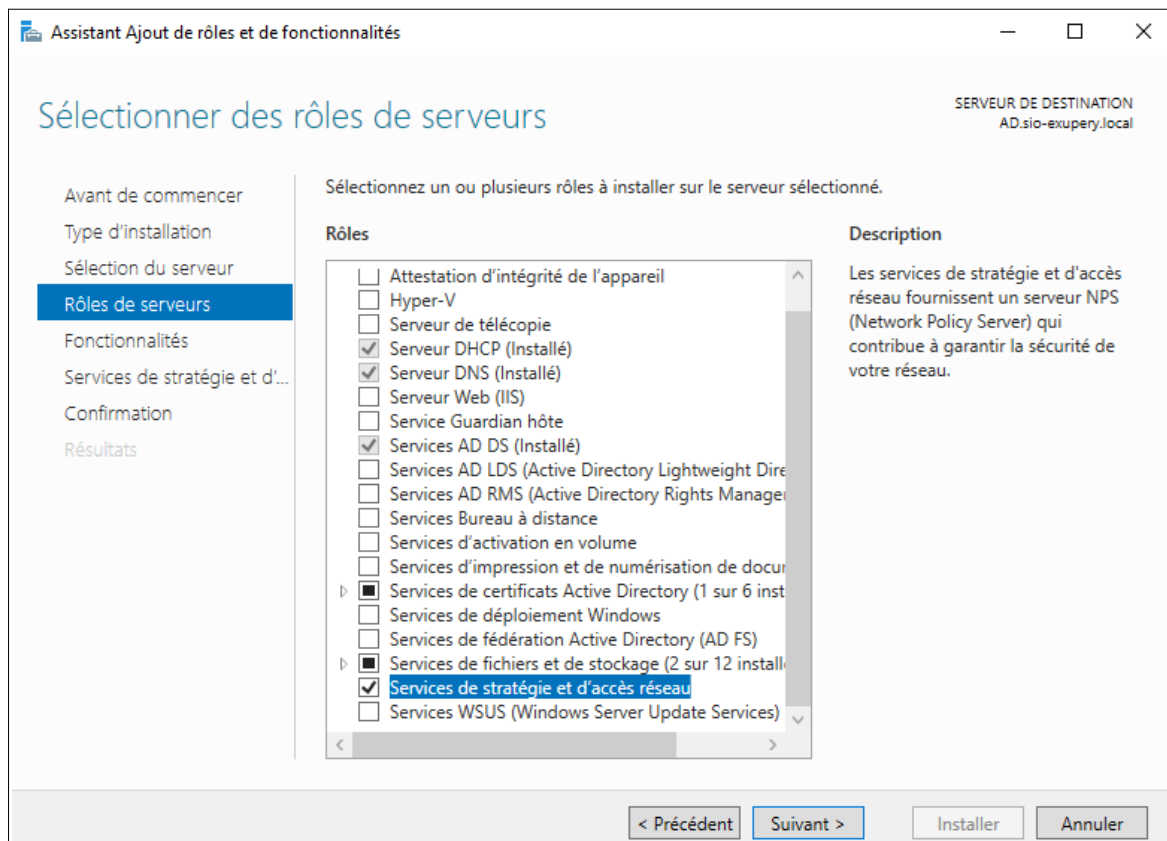
Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :

⬅ **Services de certificats Active Directory**

Autorité de certification ✔ **Configuration réussie**
[En savoir plus sur la configuration de l'autorité de certification](#)

1ère étape : Nous ajoutons le rôle **Service de certificats Active Directory**.

2.3/ Installation du service NPS



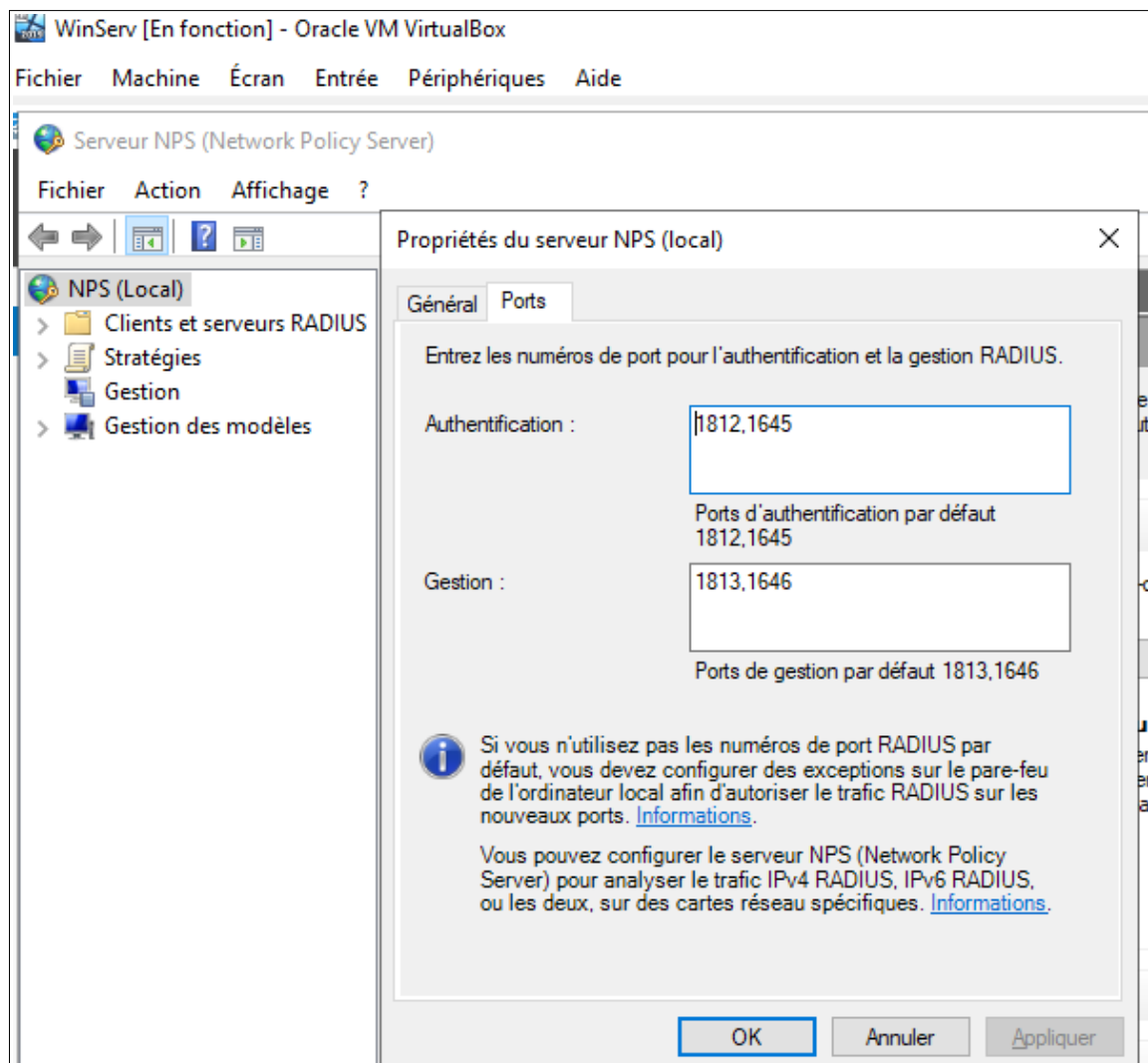
1ère étape : Nous ajoutons le rôle **Services de stratégie et d'accès réseau**.

```

UDP [fe80::7dff:791:c3aa:b7b3%8]:53 *: *
UDP [fe80::7dff:791:c3aa:b7b3%8]:88 *: *
UDP [fe80::7dff:791:c3aa:b7b3%8]:464 *: *
UDP [fe80::7dff:791:c3aa:b7b3%8]:1645 *: *
UDP [fe80::7dff:791:c3aa:b7b3%8]:1646 *: *
UDP [fe80::7dff:791:c3aa:b7b3%8]:1812 *: *
UDP [fe80::7dff:791:c3aa:b7b3%8]:1813 *: *
C:\Users\Administrateur>

```

2ème étape : Nous affichons les **ports en écoute** afin de vérifier le bon fonctionnement du service NPS.



3ème étape : Nous pouvons également retrouver ces ports dans la console **Serveur NPS**.

```
UDP 192.168.1.50:1645 *: *
UDP 192.168.1.50:1646 *: *
UDP 192.168.1.50:1812 *: *
UDP 192.168.1.50:1813 *: *
C:\Users\Administrateur>
```

4ème étape : Nous vérifions le **sockets associés** aux ports d'écoute du serveur Radius. Nous observons que l'adresse IP concorde bien.

2.4/ Configuration du serveur RADIUS NPS

Nouveau client RADIUS

Paramètres Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial : Client-Cisco-2960

Adresse (IP ou DNS) : 192.168.0.2 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

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RA
- Stratégies
- Gestion
- Gestion des modèles


Clients RADIUS

Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent votre réseau.

Nom convivial	Adresse IP	Fabricant du périphérique	État
Client-Cisco-2960	192.168.0.2	RADIUS Standard	Activé

1ère étape : Création d'un nouveau **client Radius** avec son nom convivial, adresse IP et secret partagé.

Nouvelle stratégie de demande de connexion

 **Spécifier le nom de la stratégie de demande de connexion et le type de connexion**

Vous pouvez spécifier le nom de votre stratégie de demande de connexion ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :
Connexion câblée


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 :
Non spécifié

☐ Spécifique au fournisseur :
10

2ème étape : Nous ajoutons une nouvelle **stratégie de demande de connexion** nommée « **connexion câblée** »





Nouvelle stratégie de demande de connexion

 **Spécifier les conditions**

Spécifiez les conditions qui déterminent si cette stratégie de demande de connexion est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

-  **Identificateur NAS**
La condition Identificateur NAS spécifie une chaîne de caractères qui représente le nom du serveur d'accès réseau (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les noms NAS.
-  **Adresse IPv4 NAS**
La condition Adresse IPv4 NAS spécifie une chaîne de caractères qui représente l'adresse IP du serveur d'accès réseau (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les réseaux IP.
-  **Adresse IPv6 NAS**
La condition Adresse IPv6 NAS spécifie une chaîne de caractères qui représente l'adresse IPv6 du serveur d'accès réseau (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les réseaux IPv6.
-  **Type de port NAS**
La condition Type de port NAS spécifie le type de média utilisé par le client d'accès à distance, par exemple des lignes téléphoniques analogiques, un réseau RNIS, des tunnels ou des réseaux privés virtuels, une connexion sans fil IEEE 802.11 ou des commutateurs Ethernet.

3ème étape : Nous spécifions les conditions, notamment avec **type de port NAS**.

Type de port NAS

Spécifiez les types de médias d'accès nécessaires pour correspondre à cette stratégie.

Types de tunnels pour connexions d'accès à distance et VPN standard

- ☐ Asynchrone (Modem)
- ☐ RNIS synchrone
- ☐ Synchrone (ligne T1)
- ☐ Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- ☒ Ethernet
- ☐ FDDI
- ☐ Sans fil - IEEE 802.11
- ☐ Token Ring

Autres

- ☐ ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique
- ☐ ADSL-DMT - Multi-tonalité discrète DSL asymétrique
- ☐ Asynchrone (Modem)
- ☐ Câble

OK Annuler

4ème étape : Nous cochoons par la suite **Ethernet** dans la catégorie types de tunnels pour connexion 802.1X.

Nouvelle stratégie de demande de connexion

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie de demande de connexion est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

Condition	Valeur
Type de port NAS	Ethernet

Description de la condition :

Ajouter... Modifier... Supprimer

5ème étape : Notre condition est bien présente nous pouvons désormais faire suivant.

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> Nouveau...
☐ Accepter les utilisateurs sans validation des informations d'identification

6ème étape : Nous demandons que les **demandes** soit **authentifier sur ce 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.

☐ 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.

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 :

Monter

Descendre

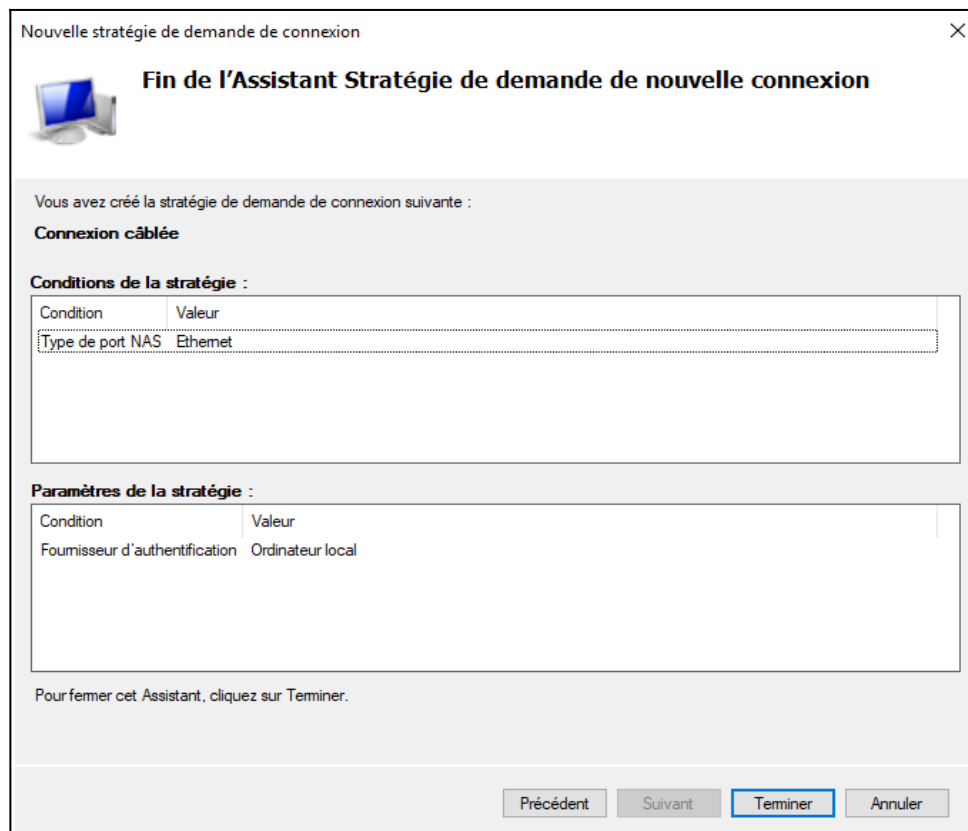
Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

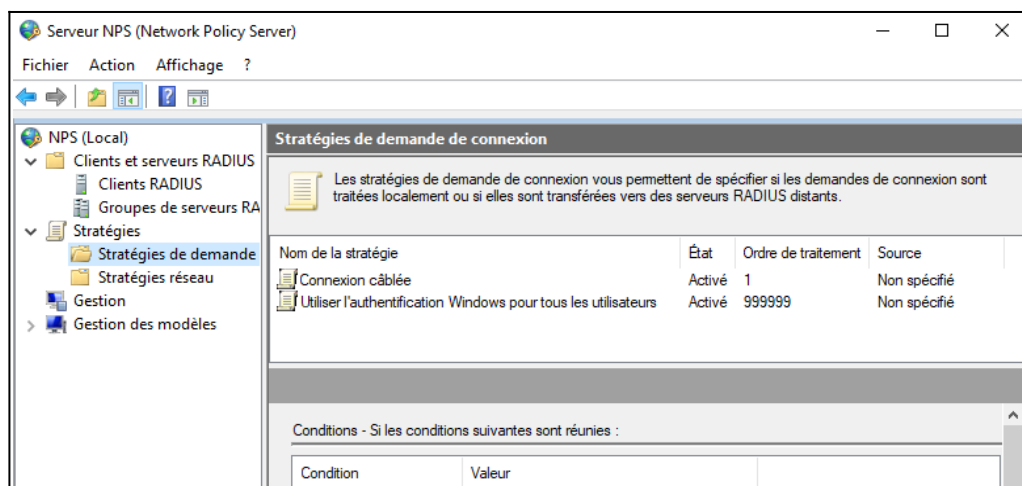
☐ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
☐ L'utilisateur peut modifier le mot de passe après son expiration
☐ Authentification chiffrée Microsoft (MS-CHAP)
☐ L'utilisateur peut modifier le mot de passe après son expiration
☐ Authentification chiffrée (CHAP)
☐ Authentification non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

Précédent **Suivant** Terminer Annuler

7ème étape : Ici nous ne modifions aucun paramètre.



8ème étape : Nous pouvons désormais terminer la **stratégie de demande de connexion**.



9ème étape : Nous observons que notre stratégie est bien présente.

Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :

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 :

☐ Spécifique au fournisseur :

10ème étape : Nous souhaitons désormais créer une nouvelle **stratégie réseau** pour les membres du **groupe Professeurs**.

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

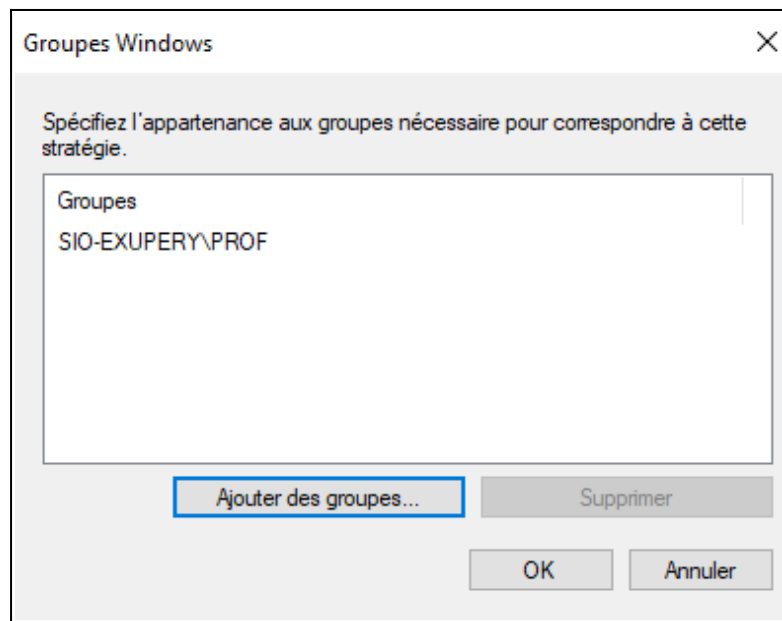
Groupes

- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

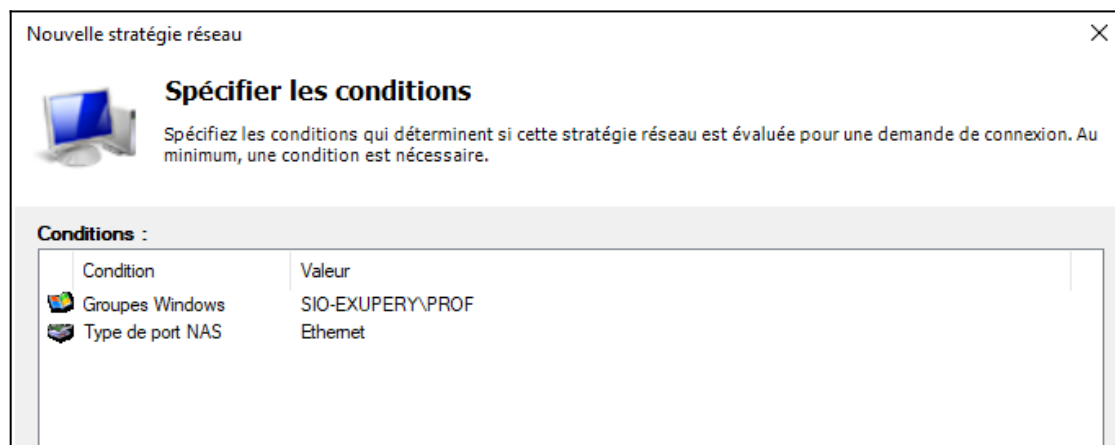
Restrictions relatives aux jours et aux heures

Restrictions relatives aux jours et aux heures
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

11ème étape : Nous ajoutons une **condition** en choisissant « **groupes Windows** ».



12ème étape : Bien évidemment dans celle-ci, le **groupe PROF** est ajouté.



13ème étape : Nous ajoutons par ailleurs une deuxième condition pour spécifier le **type de port NAS** en cochant **Ethernet**.

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.

14ème étape : Nous **accordons l'accès** pour les **membres du groupe**.

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.

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 :

Microsoft: PEAP (Protected EAP)

Monter
Descendre

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.

Précédent Suivant Terminer Annuler

15ème étape : Nous déclarons le **type de protocole EAP (PEAP)** dans l'onglet pour configurer les **méthodes d'authentification**.

Ajouter un attribut RADIUS standard

Pour ajouter un attribut, sélectionnez Spécifier les attributs :

Type d'accès : Tous

Attributs :

Nom : Tunnel-Type

Numéro de l'attribut : 64

Format de l'attribut : Enumerator

Valeurs d'attribut :

Fournisseur	Valeur
RADIUS Standard	Virtual LANs (VLAN)

Ajouter... Modifier... Supprimer Monter Descendre

OK Annuler

Informations d'attribut

Nom de l'attribut : Tunnel-Medium-Type

Numéro de l'attribut : 65

Format de l'attribut : Enumerator

Valeurs d'attribut :

Fournisseur	Valeur
RADIUS Standard	802 (includes all 802 media plus Ether...

Ajouter... Modifier...

Informations d'attribut

Nom de l'attribut : Tunnel-Pvt-Group-ID

Numéro de l'attribut : 81

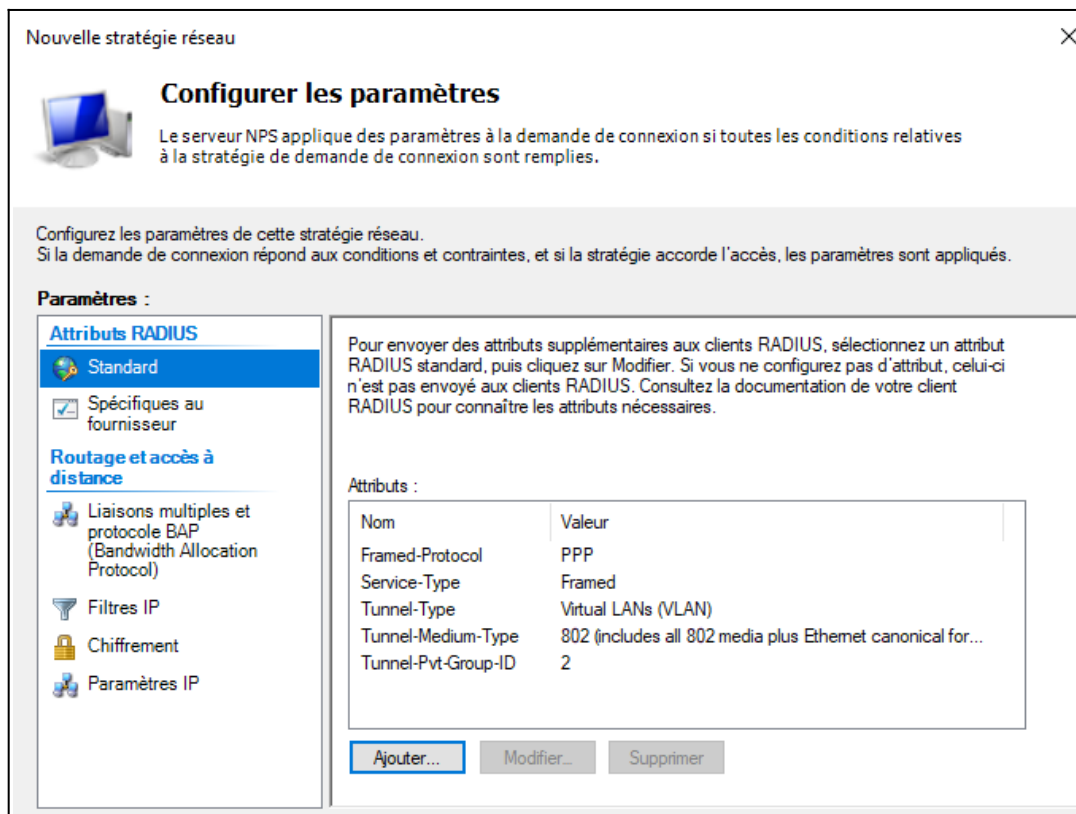
Format de l'attribut : OctetString

Valeurs d'attribut :

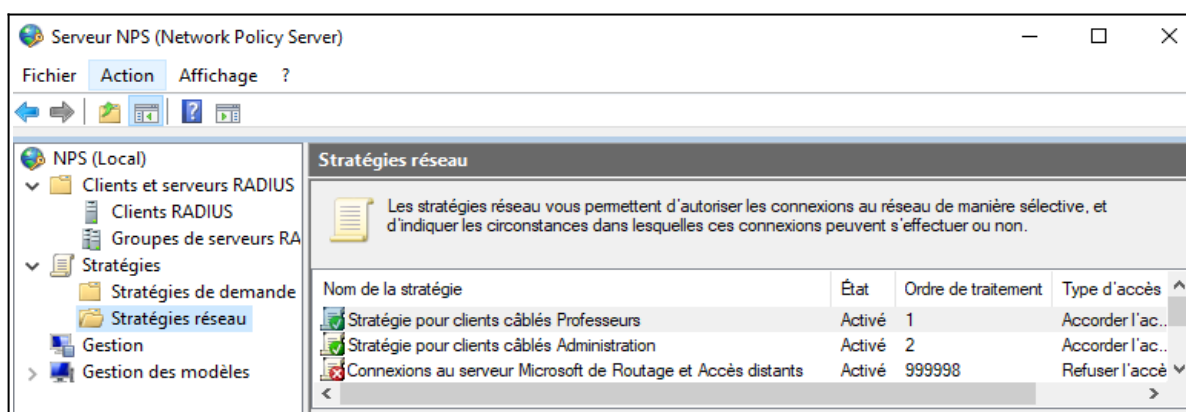
Fournisseur	Valeur
RADIUS Standard	2

Ajouter... Modifier...

16ème étape : Dans l'onglet configurer les paramètres, nous ajoutons des nouvelles valeurs d'attribut pour le client Radius.




17ème étape : Nous pouvons observer les **attributs** que nous avons ajoutés.



18ème étape : Nous définissons désormais une stratégie d'accès réseau plaçant dans le VLAN3 les membres authentifiés comme faisant partie du groupe

Nouvelle stratégie réseau



Configurer les paramètres

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.

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard
- Spécifiques au fournisseur

Routage et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Type	Virtual LANs (VLAN), Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...)
Tunnel-Pvt-Group-ID	3

Ajouter...
Modifier...
Supprimer

Précédent
Suivant
Terminer
Annuler

19ème étape : Comme visualisé au-dessus, un récapitulatif des configurations nous est fourni.