Authentification réseau : Documentation Radius

Extrait de notre infrastructure 802.1x - Client final : Windows 11 - Commutateur : Cisco SF300 - Serveur RADIUS NPS sur Windows Server

Utilisateur :

VLAN 60 IT

VLAN 3 handball -

Ports 1 à 23 contrôlés

Le serveur RADIUS a pour adresse IP 172.20.100.2 et communique dans le VLAN 60 avec le

commutateur Cisco RDC qui a pour adresse IP 172.20.70.11

Domaine de l'Active Directory : leidoscope.local

1. Installation de deux nouveaux services sur le serveur Windows 2022

 Installation d'une autorité de certification

 Installation du service NPS - Serveur RADIUS

2. Paramétrage du service NPS

 Déclaration d'un client RADIUS : le commutateur

 Déclaration d'une stratégie de connexion

 Déclaration d'une stratégie d'accès réseau

3. Paramétrer le commutateur Client RADIUS

 Paramétrage général 802.1x - déclaration du serveur RADIUS

 Paramétrage des ports contrôlés 802.1x

4. Configurer le client final en 802.1x

 Service Configuration automatique de réseau câblé

 Onglet "Authentification" des propriétés de la carte réseau

 Réglage des paramètres avancés

Installation du serveur RADIUS-NPS

Situation de départ - Un Serveur Windows avec Active Directory (AD) qui a pour adresse IP

172.20.100.2 - Un domaine AD "leidoscope.local" - Pare-feu désactivé dans un premier temps pour ne pas compliquer les tests

Dans l'Active Directory : - groupe existant : "IT" ;

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.

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

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

➔ On laisse la période de validité par défaut ainsi que l'emplacement d'installation de la base de données de certificats

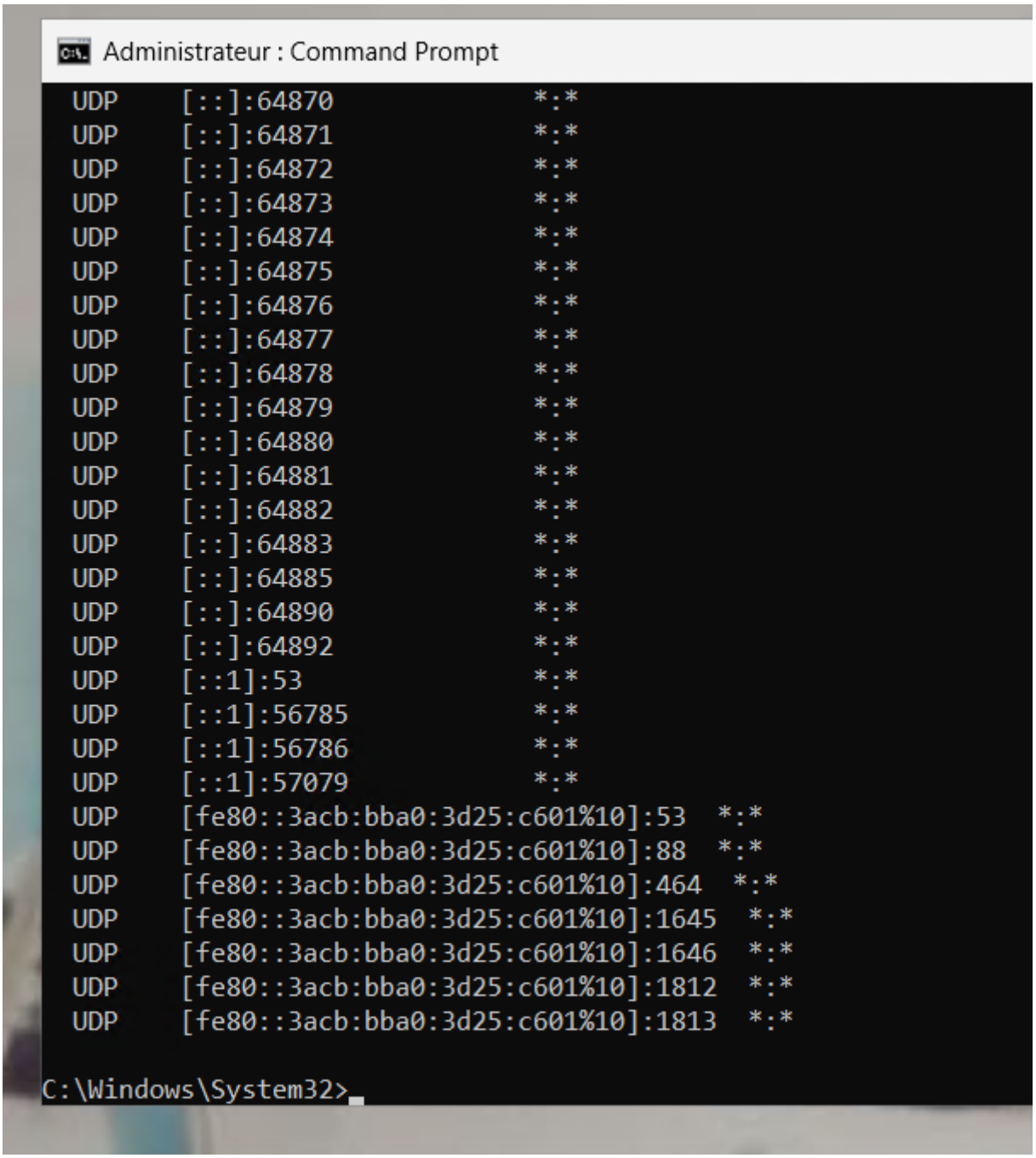
Installation du serveur RADIUS - NPS (Network Policy Server)

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

➔ ATTENTION

Si l'adresse IP du serveur est changée après l'installation de NPS, il sera impératif de redémarrer le service.

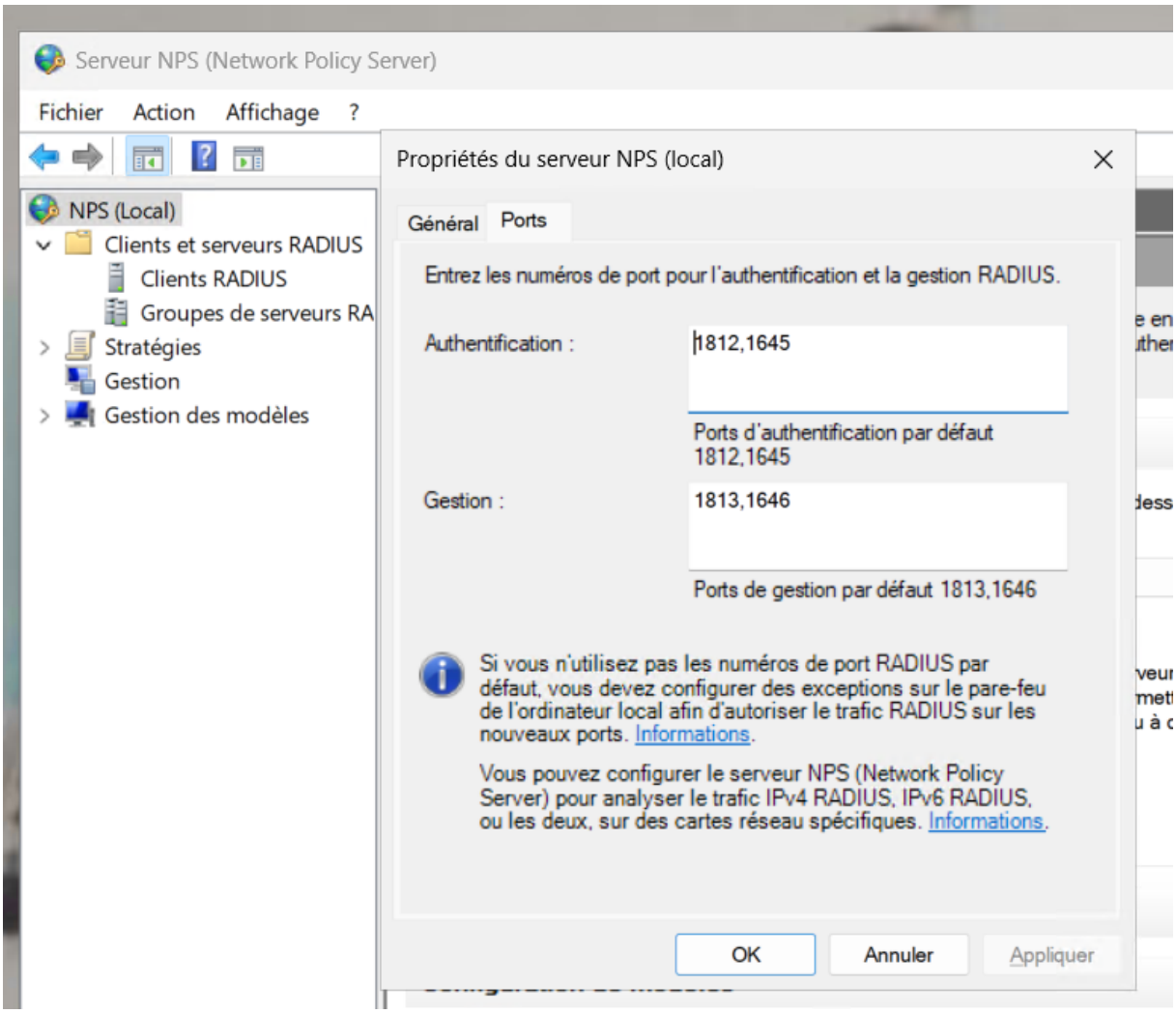
Note : Pour vérifier le bon fonctionnement du service NPS sur le serveur, vous pouvez afficher les ports en écoute sur celui-ci avec la commande netstat -a



Résultat de la commande nestat -a : voir les 4 dernières lignes.

NPS écoute sur les ports suivants par défaut : - 1812, 1645 pour l'authentification. - 1813,1646 pour la gestion.

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

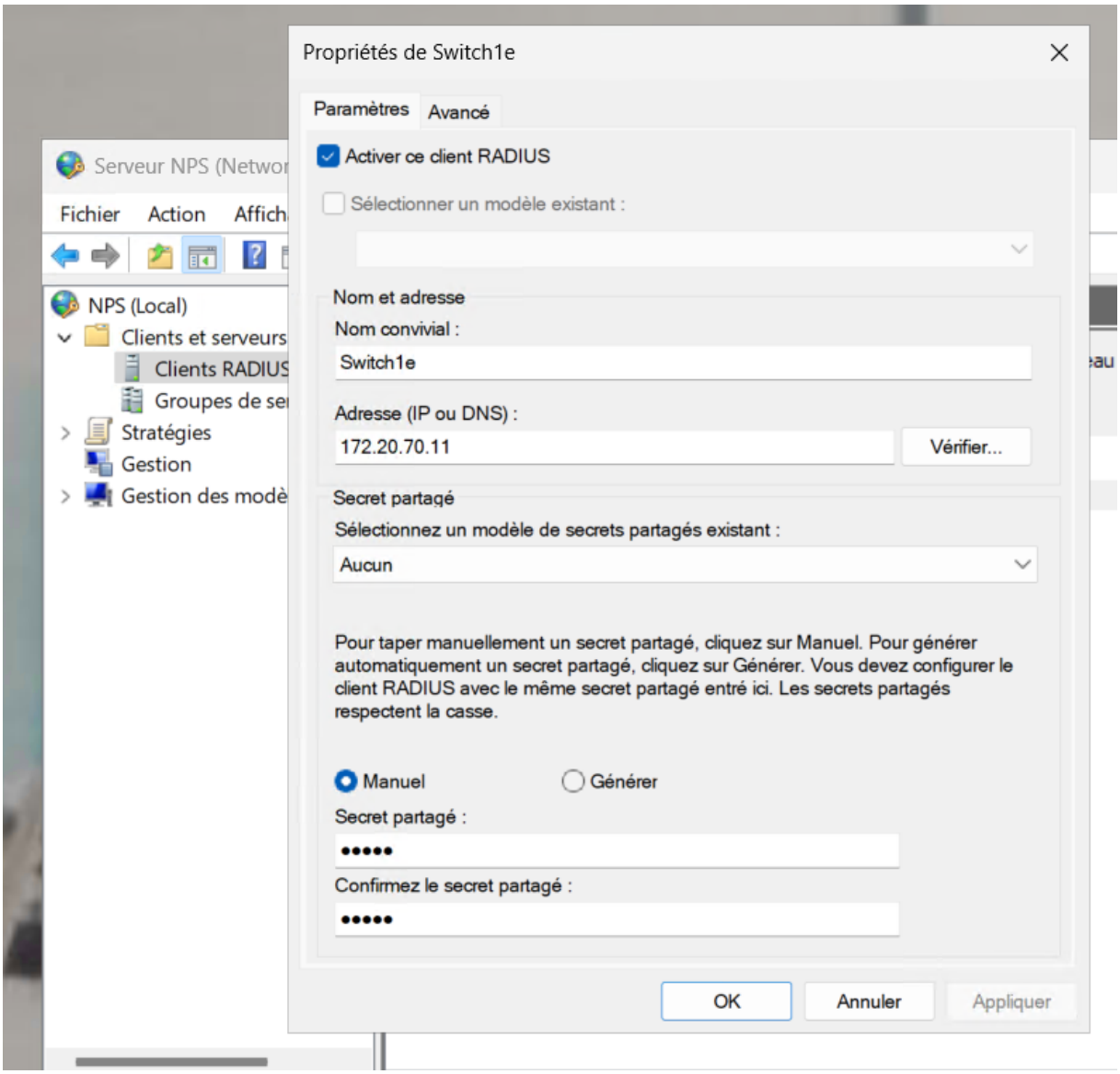


CONFIGURATION DU SERVEUR RADIUS NPS

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

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.



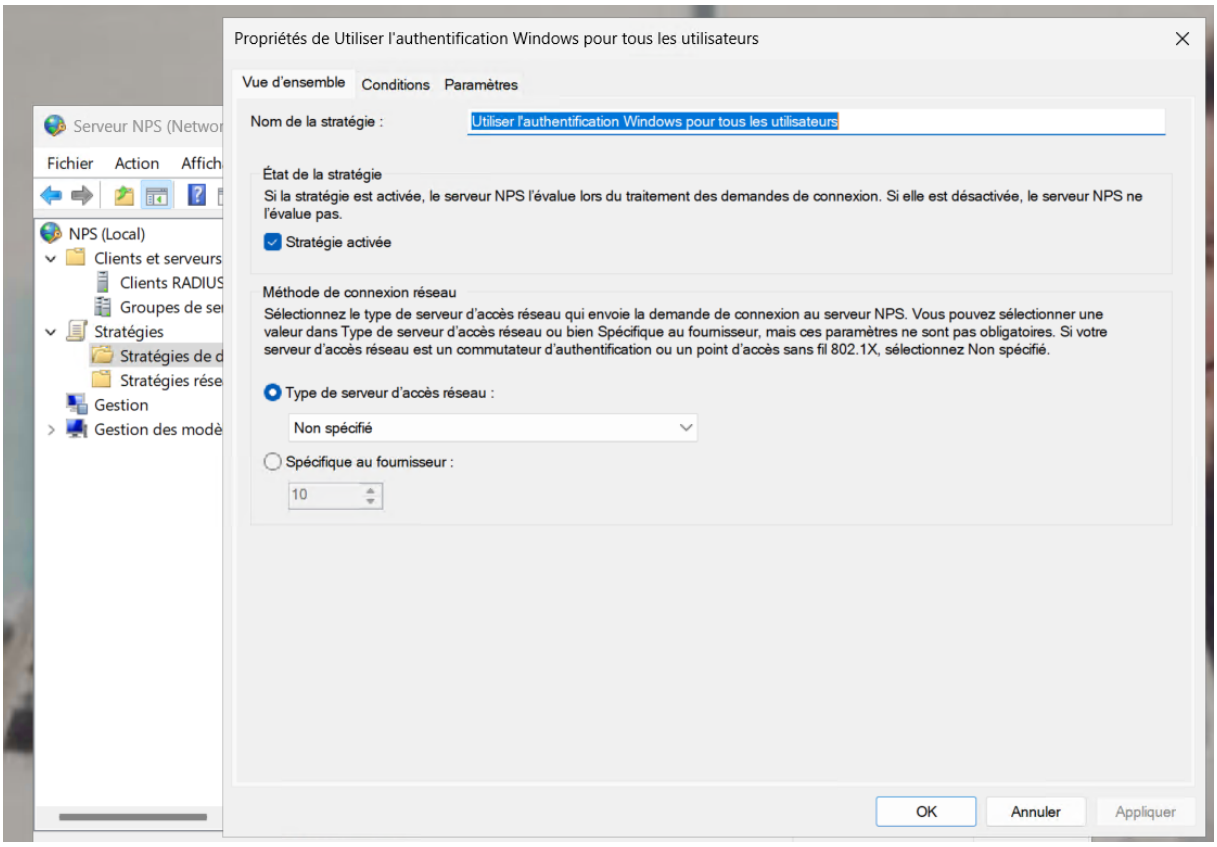
Attention : Cette chaîne doit évidemment être identique à celle déclarée dans le client radius, c'est-à-dire le commutateur Cisco. Il s'agit d'un secret partagé entre deux éléments d'infrastructure, avec une exigence de sécurité moins importante qu'un accès "depuis un poste client". Il y a peu de chance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

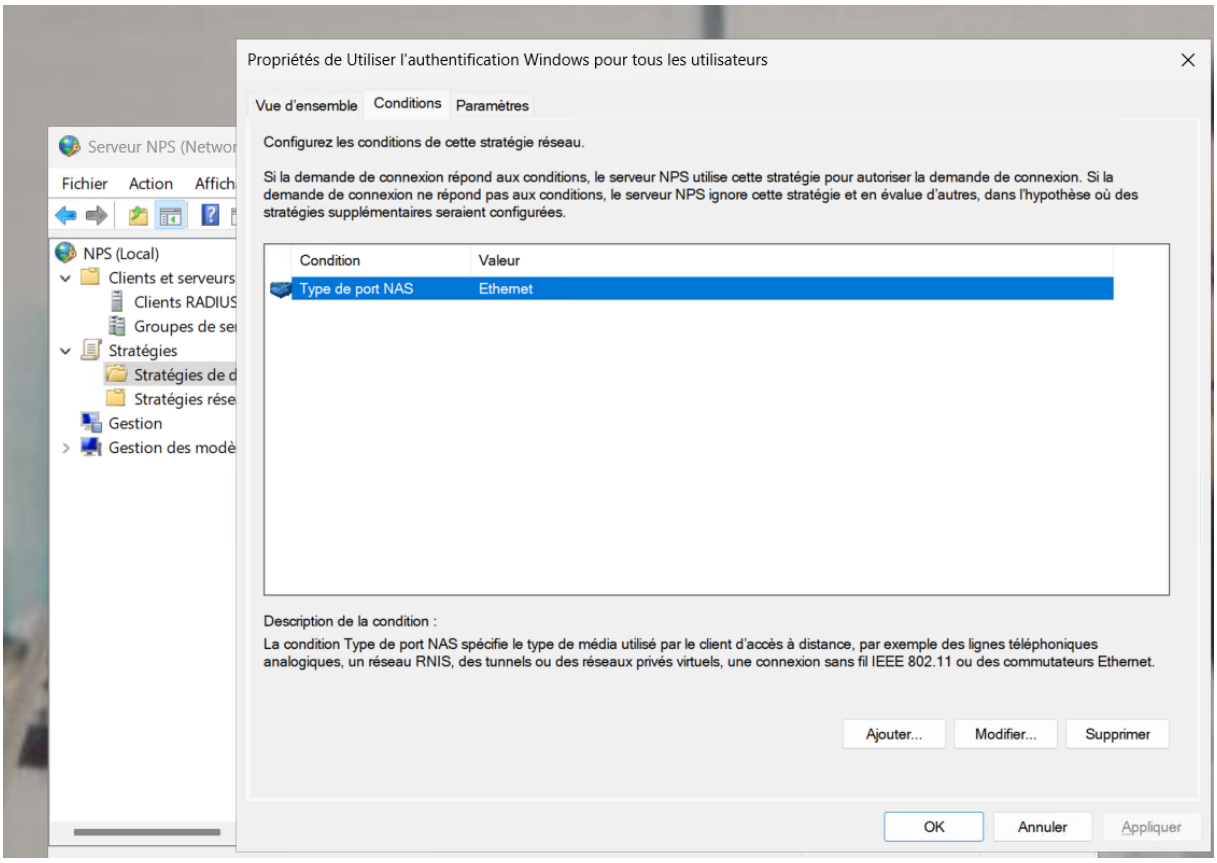


On choisit ensuite d'indiquer un type de port NAS (type de media concerné)

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.

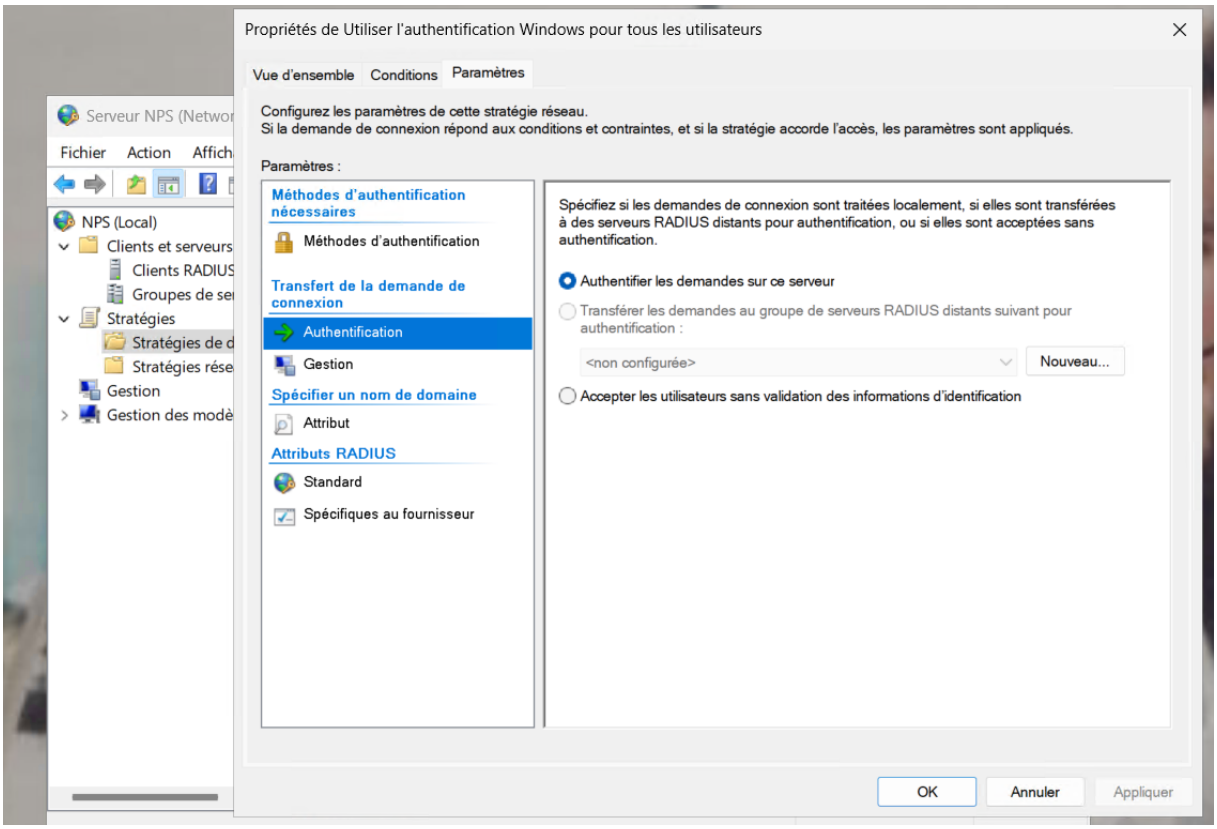


Récapitulatif :

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

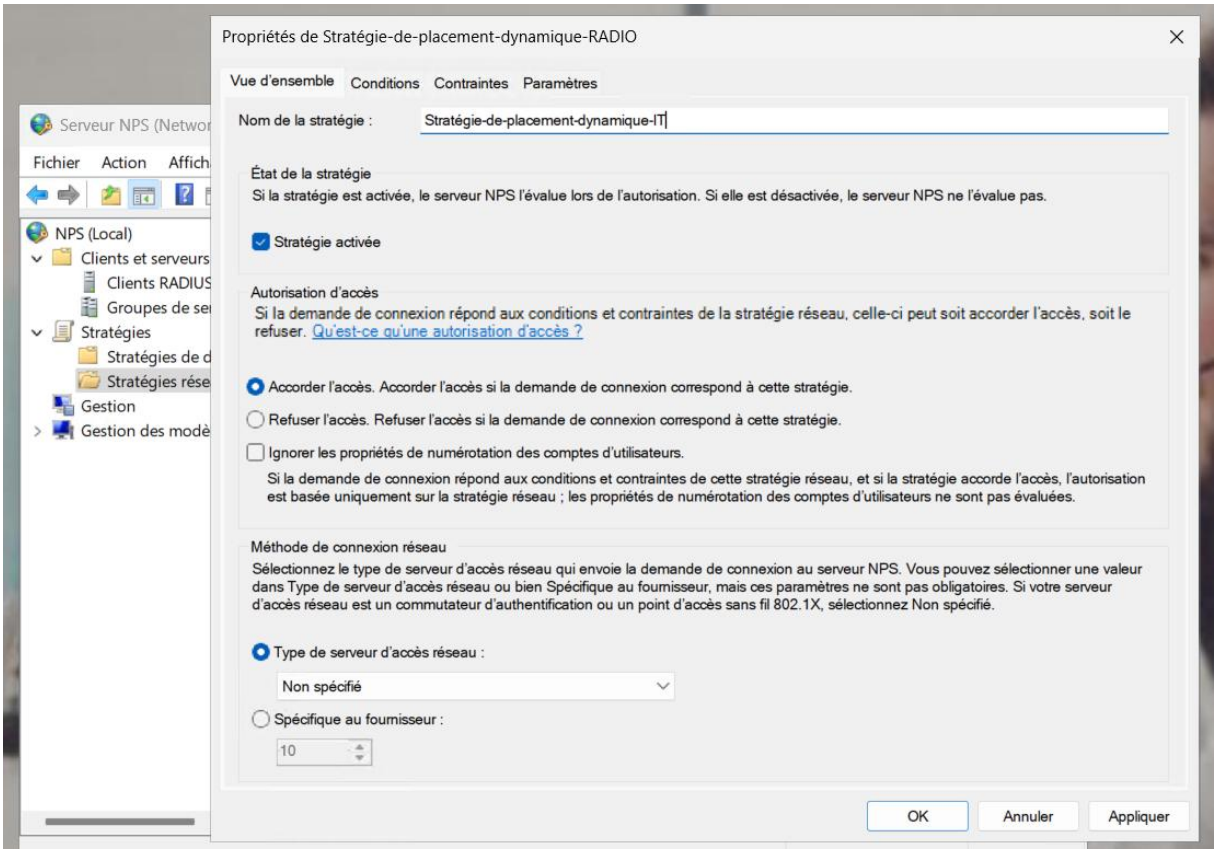
Les demandes seront traitées sur ce serveur et non sur un autre. Ce qui veut dire que ce NPS pourrait jouer un rôle de "PROXY NPS" s'il relayait les demandes à un autre serveur.

Cet écran est laissé tel quel. C'est la stratégie d'accès réseau que l'on va maintenant déclarer qui va primer.



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

On veut mettre en place une stratégie de placement dynamique dans le VLAN 60 pour les membres du groupe d'utilisateurs "IT".

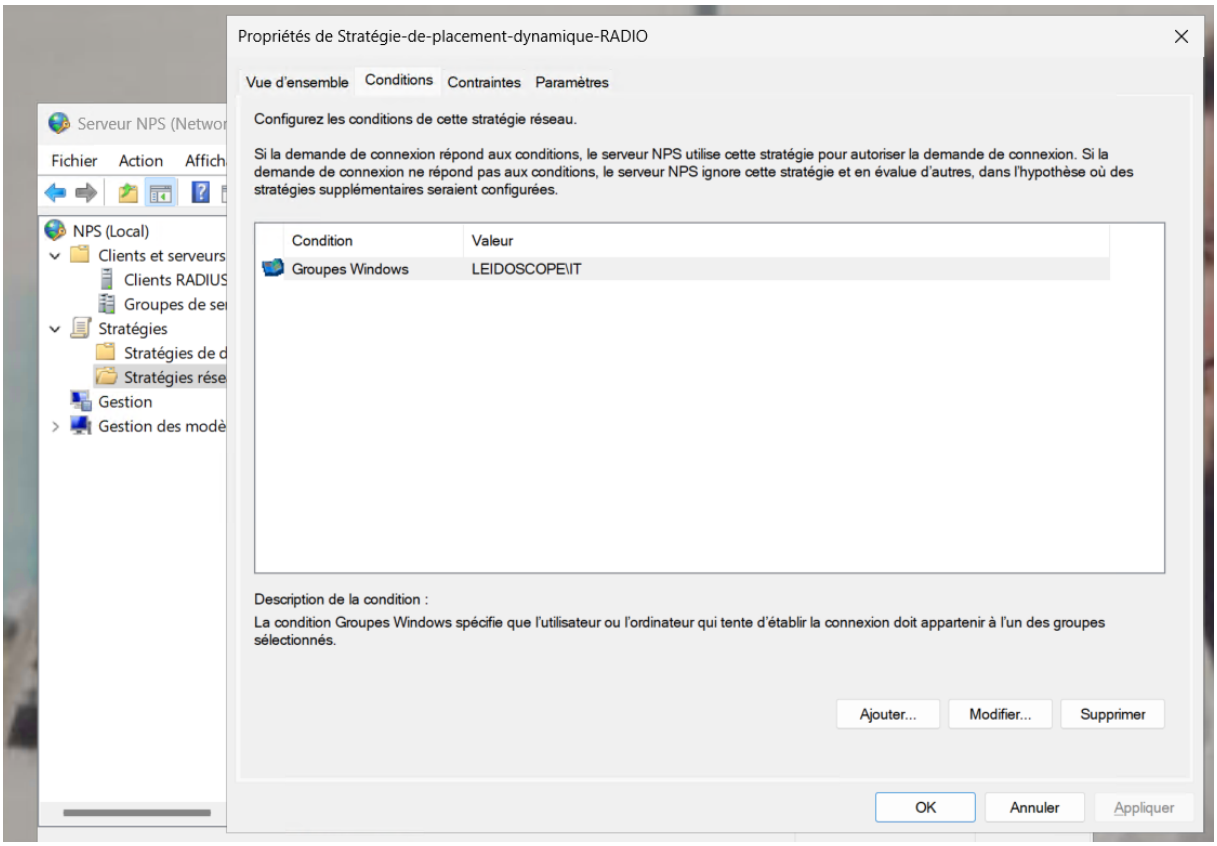


Note : Si on veut placer les membres d'un autre groupe d'un VLAN, on créera une autre stratégie d'accès réseau. On peut donc avoir un catalogue de stratégies d'accès réseau, pour une seule stratégie de demande de connexion.

Sur l'entrée Stratégie Réseau, faire un clic droit ➔ Nouvelle Stratégie réseau

➔ On reste sur un type non spécifié car il s'agit d'une authentification via un commutateur 802.1x

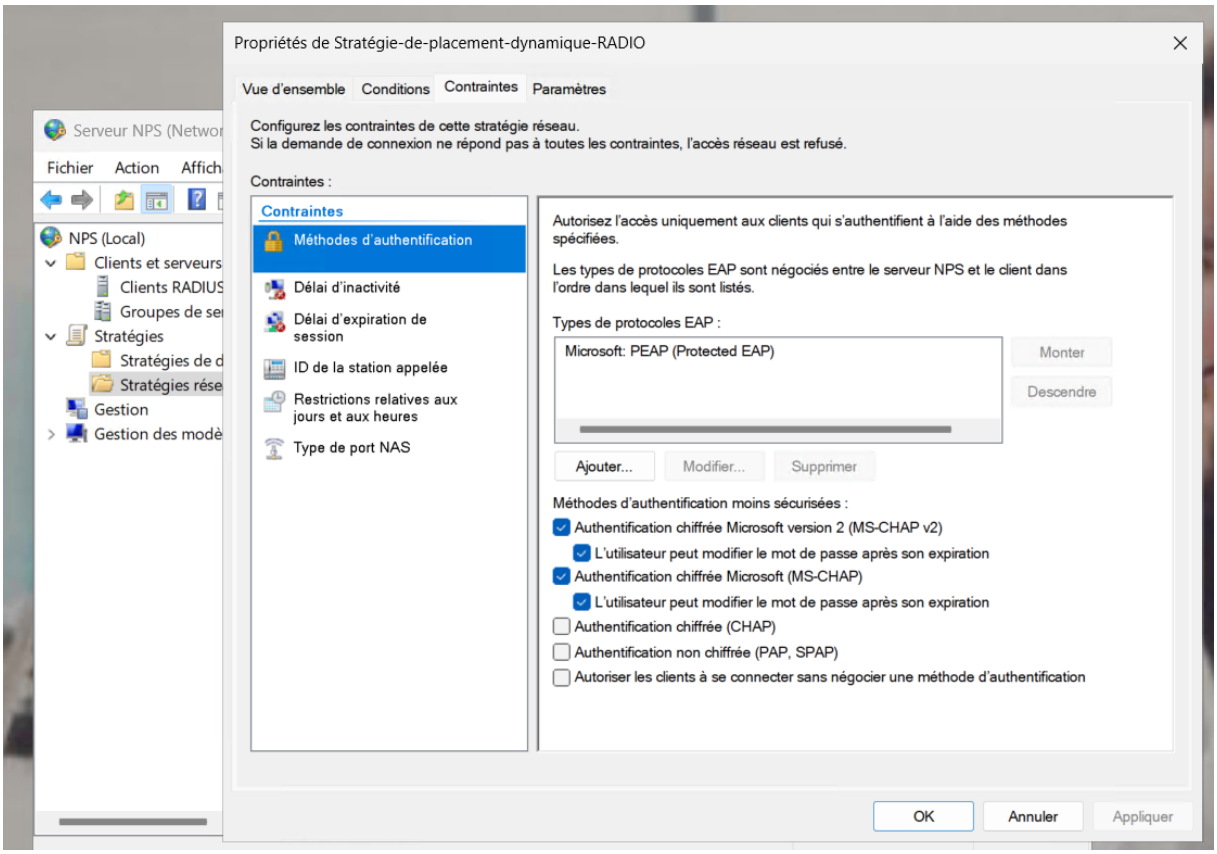
On ajoute une condition à la validation de la stratégie : que l'utilisateur soit membre d'un groupe AD qui s'appelle "IT". Pour les membres de ce groupe, on accorde l'accès. Choisir Groupe Windows et non Groupes d'utilisateurs.



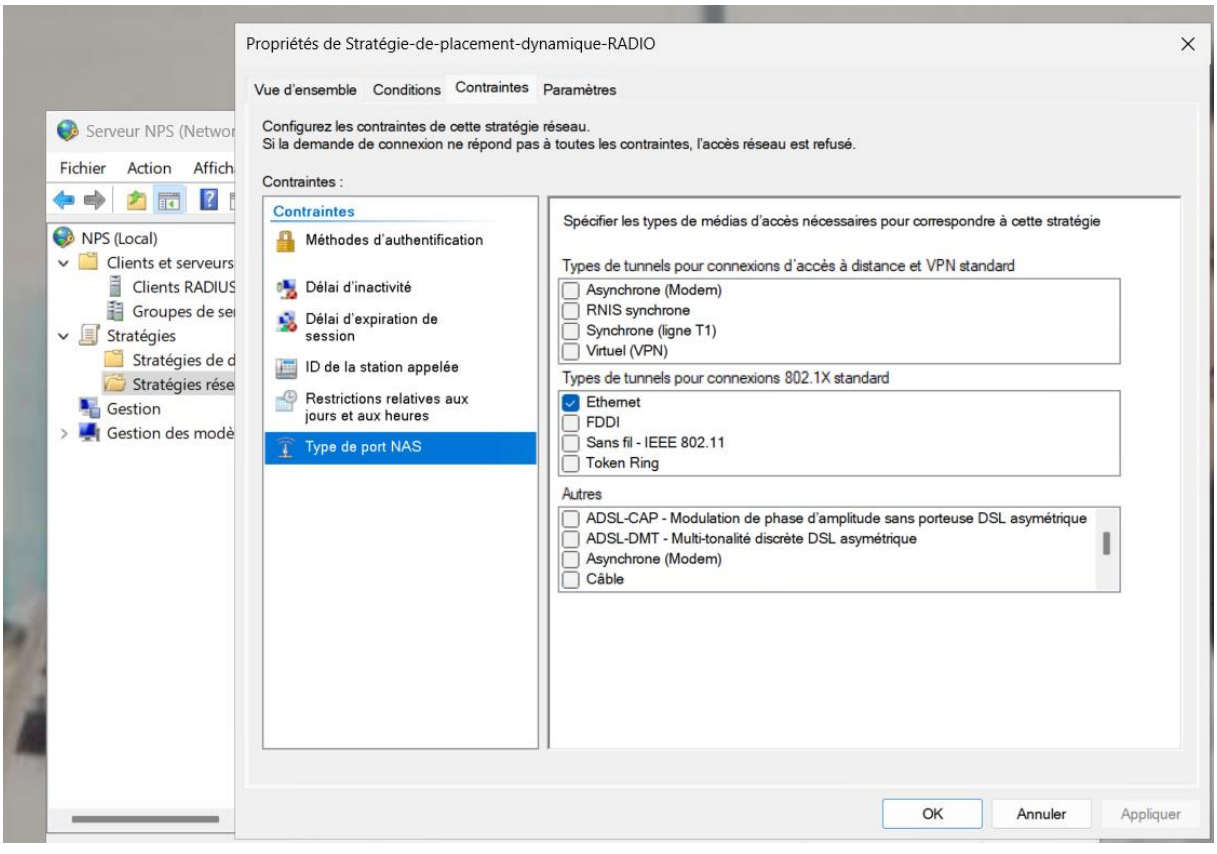
Récapitulatif du choix des groupes Windows

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.

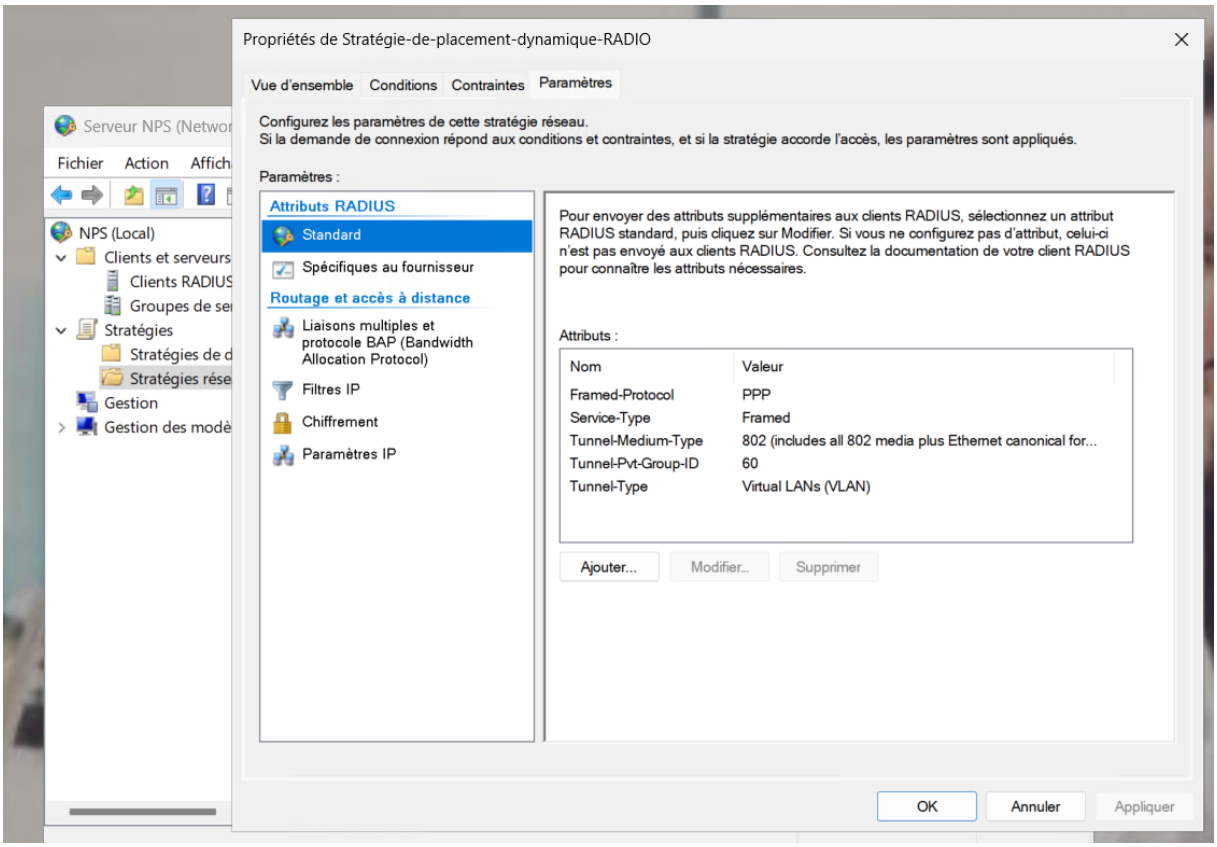
On va maintenant ajouter des attributs de contrôle de trafic en cliquant sur [AJOUTER]

 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.

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

Enfin "Tunnel-Pvt-Group-ID" sur le numéro de VLAN dans lequel on veut positionner les membres du groupe d'utilisateurs "IT" : pour nous le VLAN 60.



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

Paramétrage réalisé sur notre commutateur Cisco

Mise en place de l’authentification 802.1x sur le commutateur

A - Définir un nouveau modèle d’authentification

(config)#aaa new-model

(config)#aaa authentication dot1x default group RADIUS

(config)#aaa authorization network default group RADIUS

(config)#dot1x system-auth-control

B - Définir les informations d’accès au serveur RADIUS

(config)#RADIUS-server host IpRADIUS auth-port 1812 acct-port 1813 key

PwdClientRADIUS

Dans notre cas :

(config)# RADIUS-server host 172.20.100.2 auth-port 1812 acct-port 1813 key

Configuration des ports

Définir l'authentification 802.1x sur un port (mode configuration d'interface).

A noter qu'il est également possible de paramétrer plusieurs ports en même temps.

(config-if)#switchport mode access

(config-if)#authentication port-control auto

(config-if)#dot1x pae authenticator

(config-if)#authentication host_mode multi-host

(config-if)#spanning-tree portfast trunk

Remarque :

Si le poste ne supporte pas le 802.1x, Éventuellement, affecter le port à un VLAN invité

(config-if)#authentication event no-response action authorize vlan xx

Afficher des informations sur l'authentification 802.1x (Utile pour les tests)

Switch#dot1x initialize interface f0/1

Switch#dot1x test eapol-capable interface f0/1

Switch#show dot1x all

Switch#show authentication interface f0/1

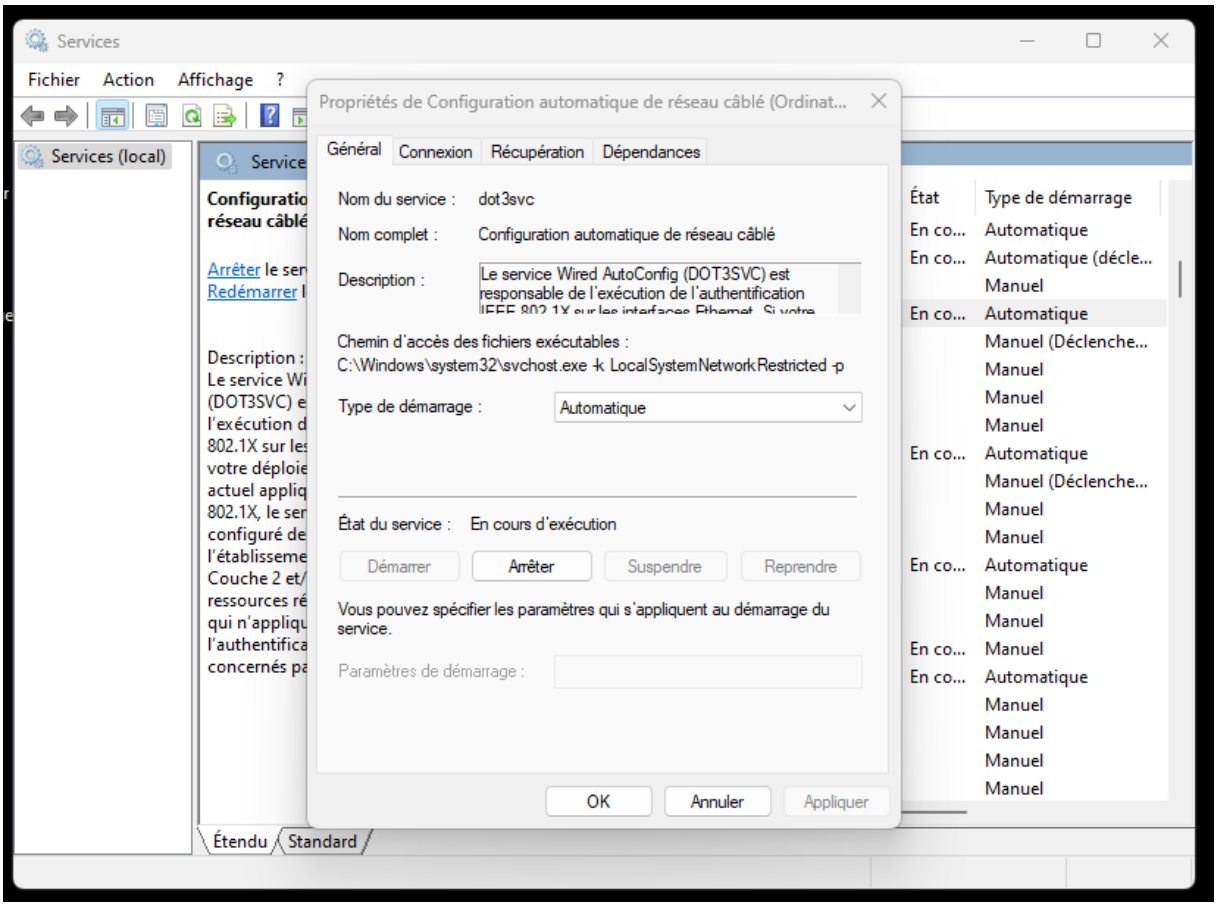
Relancer l'authentification sur un port particulier (en cas de problème) - Relancer la phase d'authentification 802.1x sur un port

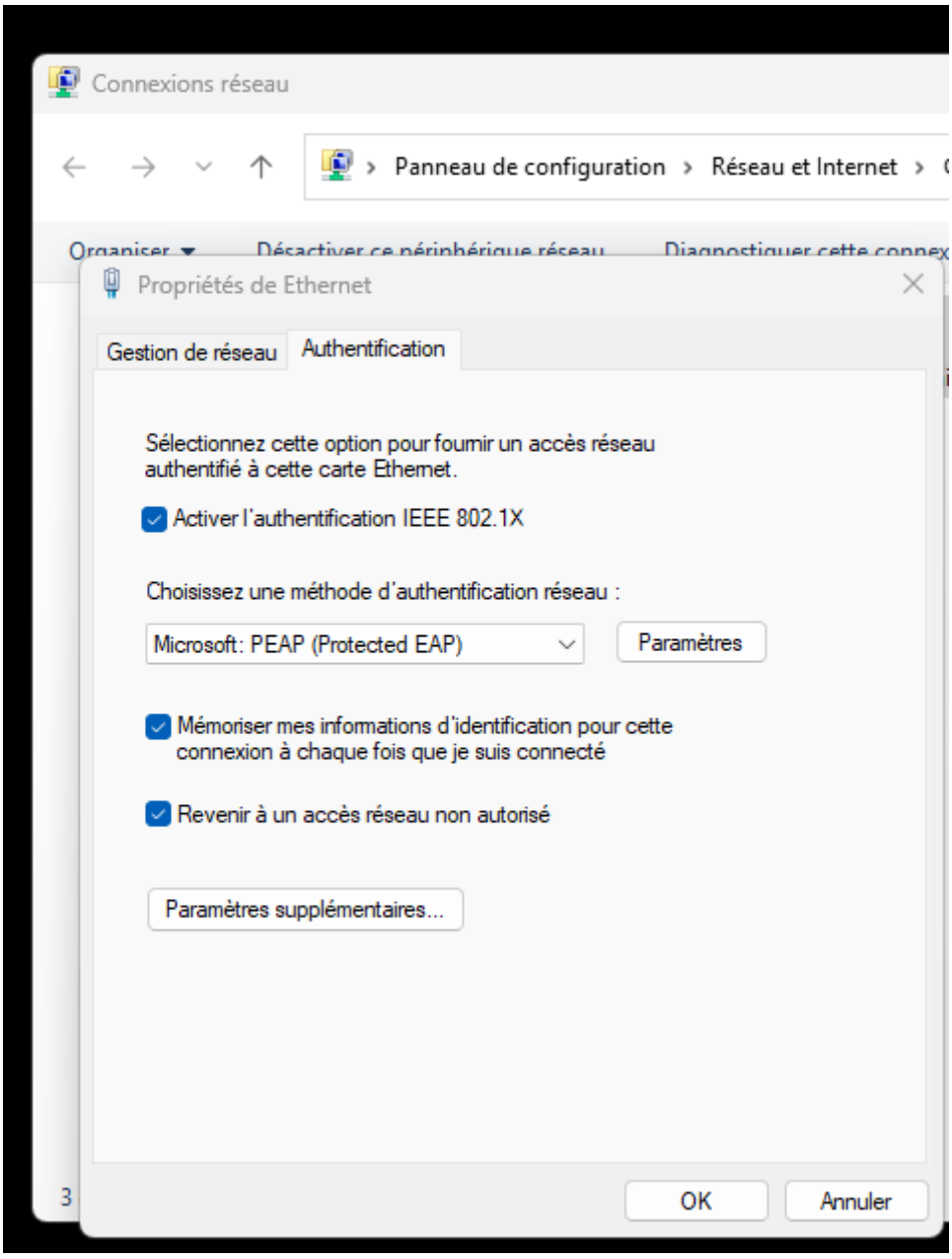
Switch#dot1x re-authenticate interface f0/1

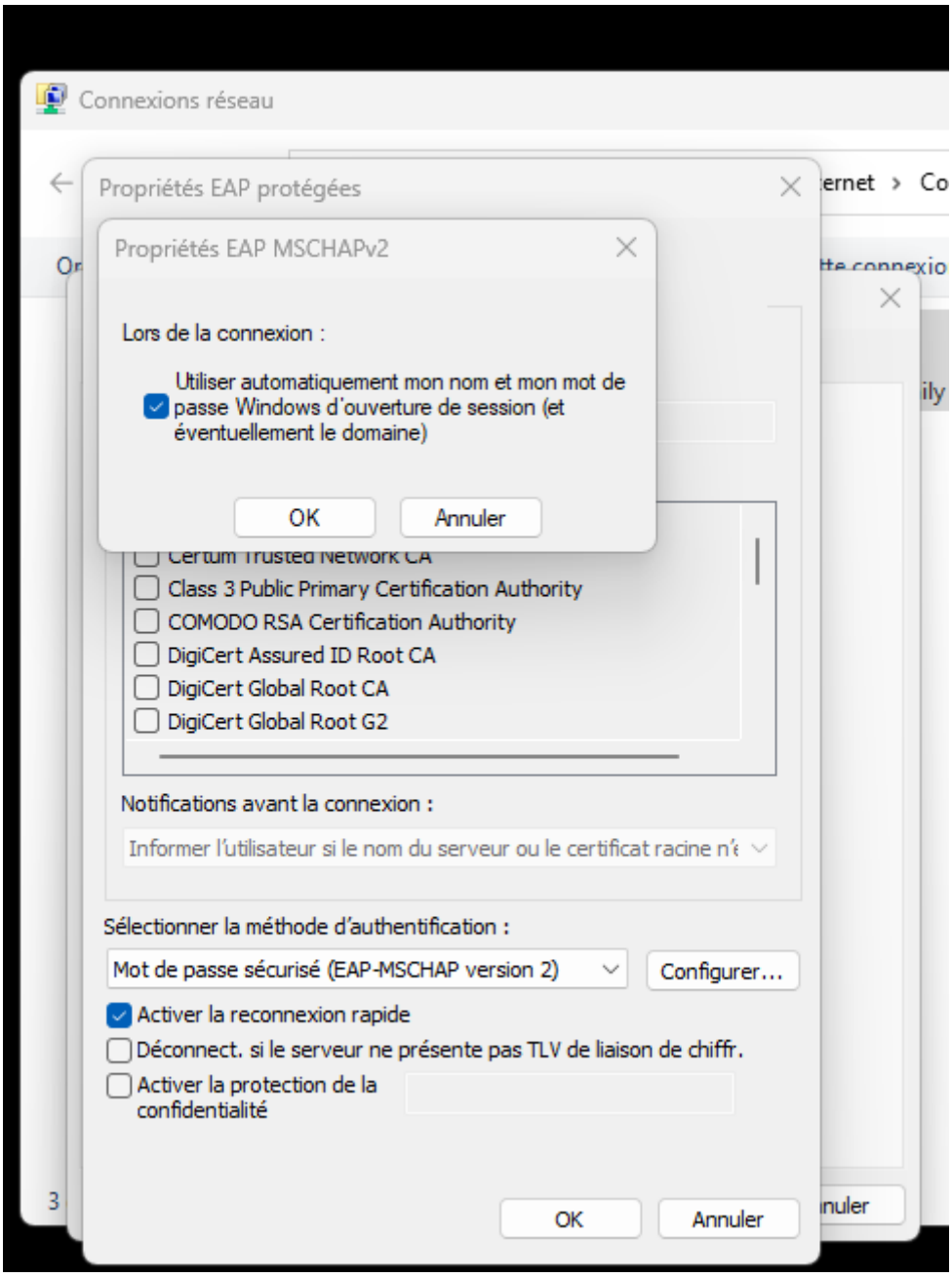
```
aaa new-model
!
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

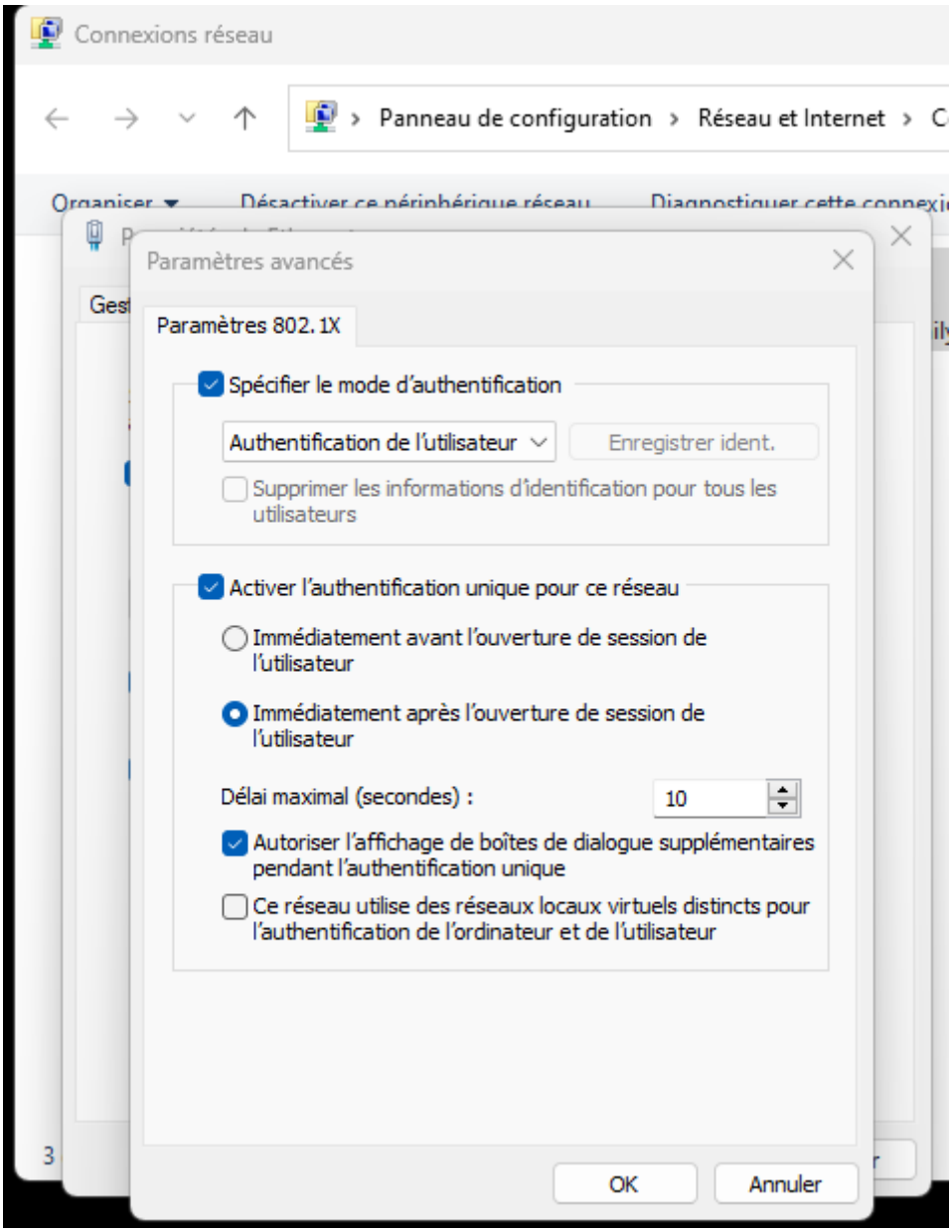
```
Nov 20 14:13:32.793: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (fc34.9780.4fd3) on Interface Fa0/3 AuditSessionID AC14460B0000001F0134C647
Nov 20 14:13:32.793: %AUTHMGR-5-VLANASSIGN: VLAN 60 assigned to Interface Fa0/3 AuditSessionID AC14460B0000001F0134C647
Nov 20 14:13:33.187: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (fc34.9780.4fd3) on Interface Fa0/3 AuditSessionID AC14460B0000001F0134C647
```

Configuration d'un client final - Dans services : Démarrer le service « Configuration automatique de réseau câblé » et régler le type de démarrage sur « automatique » - Dans l'onglet Authentification de la carte réseau, cocher l'option « Activer l'authentification IEEE 802.1X » - Toujours dans l'onglet Authentification : - cliquer sur « Paramètres » puis dans la partie méthode d'authentification, cocher uniquement la case « Appliquer la protection d'accès réseau » puis cliquer sur « configurer » et cocher l'option permettant d'utiliser automatiquement le nom et le mot de passe Windows - cliquer sur « Paramètres supplémentaires » cocher la case « Activer l'authentification unique pour ce réseau » puis sélectionner l'option « immédiatement après l'ouverture de session de l'utilisateur.




Connexions réseau
Panneau de configuration
Réseau et Internet
Organiser
Désactiver ce périphérique réseau
Diagnostiquer cette connex
Propriétés de Ethernet
Gestion de réseau
Authentification
Sélectionnez cette option pour fournir un accès réseau authentifié à cette carte Ethernet.
Activer l'authentification IEEE 802.1X
Choisissez une méthode d'authentification réseau :
Microsoft: PEAP (Protected EAP)
Paramètres
Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté
Revenir à un accès réseau non autorisé
Paramètres supplémentaires...
OK
Annuler
3


Connexions réseau
Propriétés EAP protégées
Propriétés EAP MSCHAPv2
Lors de la connexion :
Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)
OK
Annuler
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
Notifications avant la connexion :
Informer l'utilisateur si le nom du serveur ou le certificat racine n'
Sélectionner la méthode d'authentification :
Mot de passe sécurisé (EAP-MSCHAP version 2)
Configurer...
Activer la reconnexion rapide
Déconnect. si le serveur ne présente pas TLV de liaison de chiffr.
Activer la protection de la confidentialité
OK
Annuler


Connexions réseau
Panneau de configuration
Réseau et Internet
Organiser
Désactiver ce périphérique réseau
Diagnostiquer cette connexi
Paramètres avancés
Paramètres 802.1X
Spécifier le mode d'authentification
Authentification de l'utilisateur
Enregistrer ident.
Supprimer les informations d'identification pour tous les utilisateurs
Activer l'authentification unique pour ce réseau
Immédiatement avant l'ouverture de session de l'utilisateur
Immédiatement après l'ouverture de session de l'utilisateur
Délai maximal (secondes) :
10
Autoriser l'affichage de boîtes de dialogue supplémentaires pendant l'authentification unique
Ce réseau utilise des réseaux locaux virtuels distincts pour l'authentification de l'ordinateur et de l'utilisateur
OK
Annuler