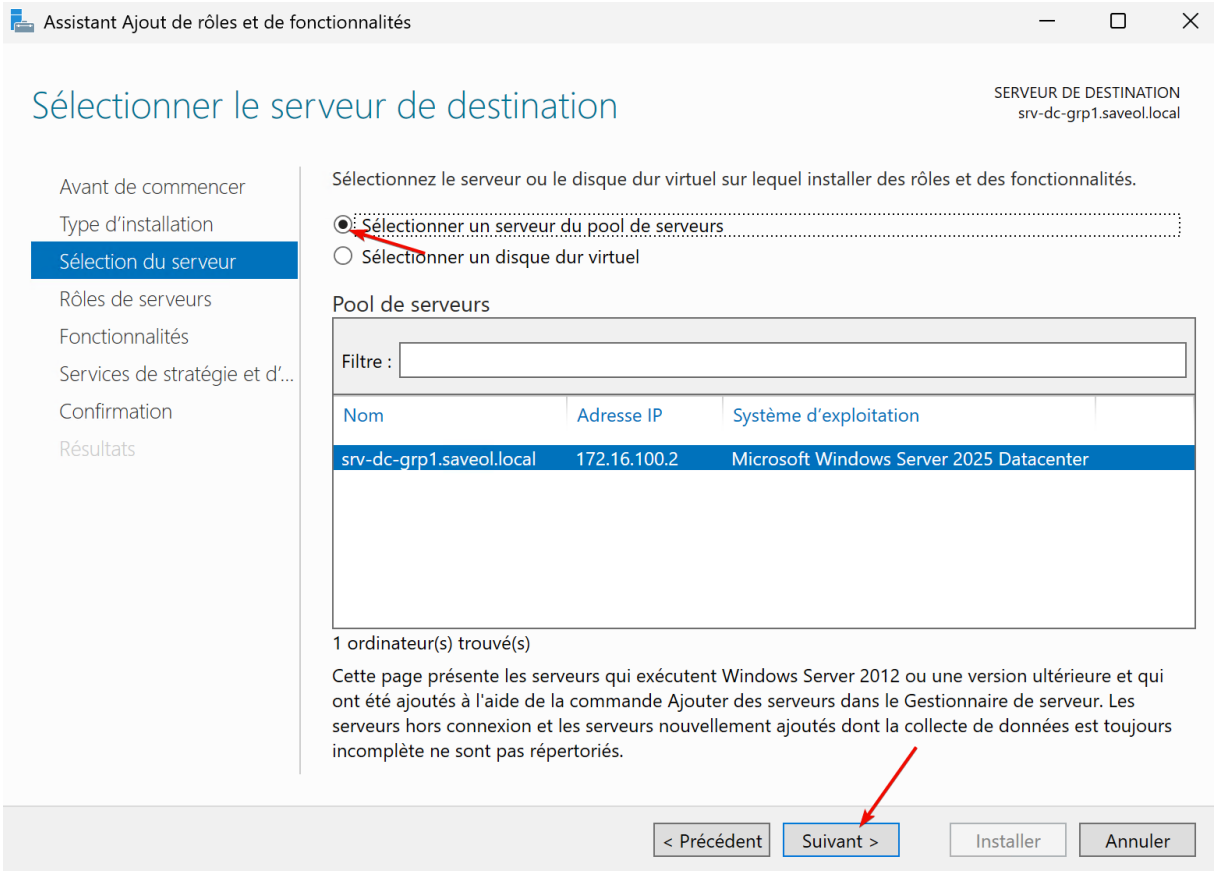
Installation NPS

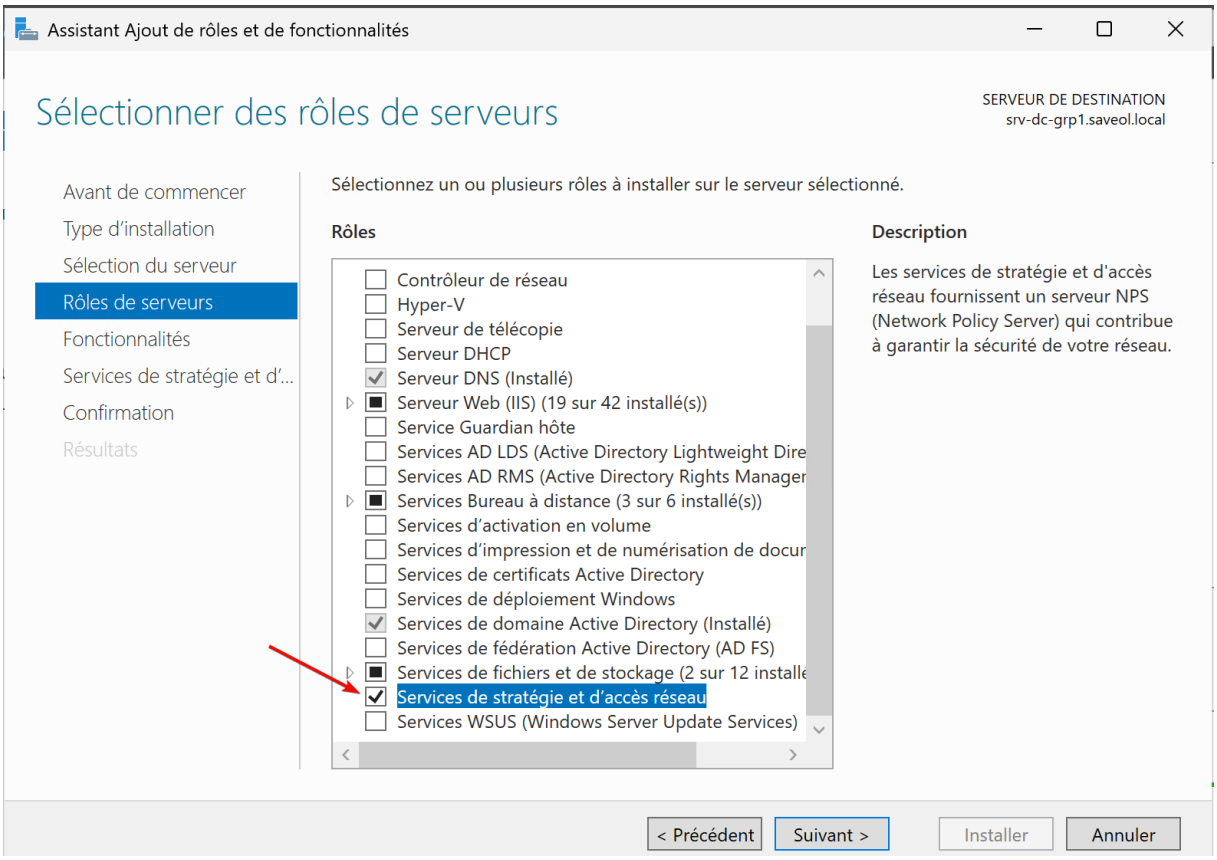
Objectif :

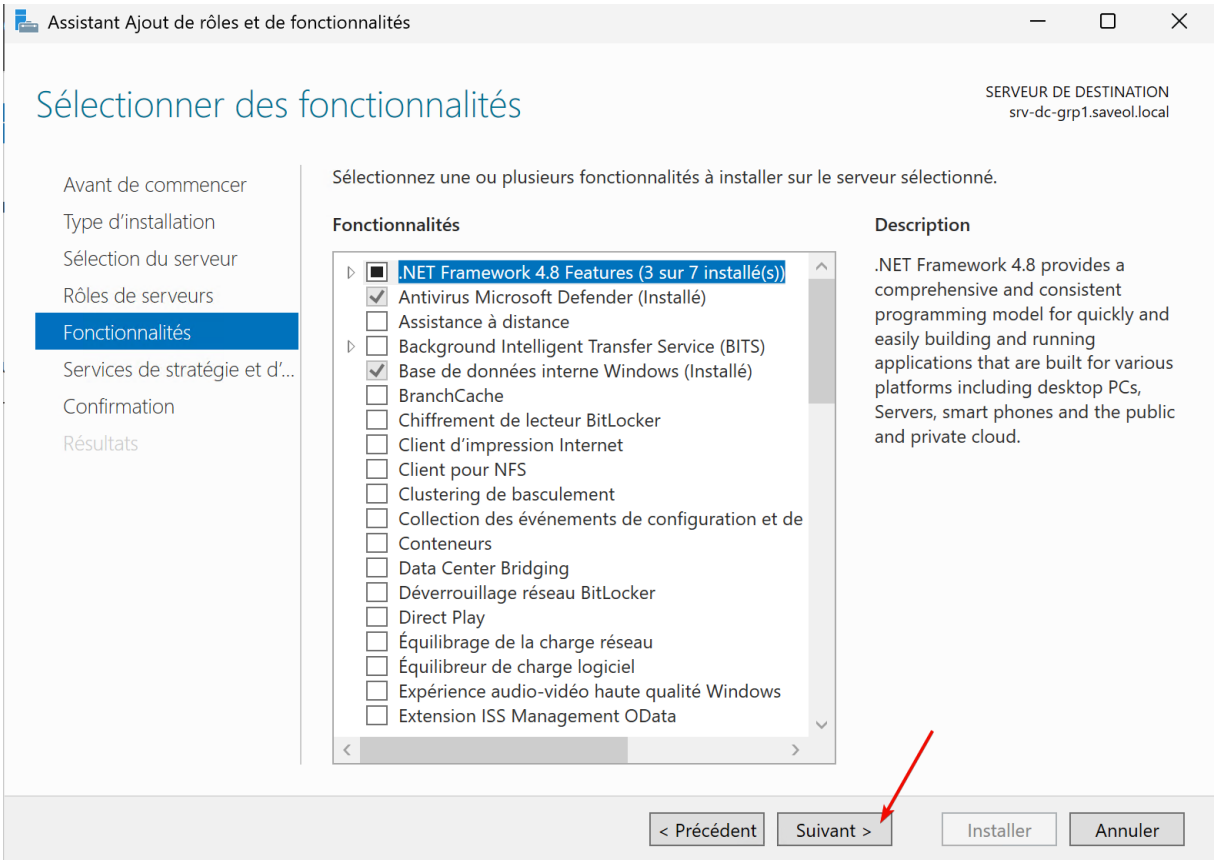
Installation et configuration d’un serveur RADIUS

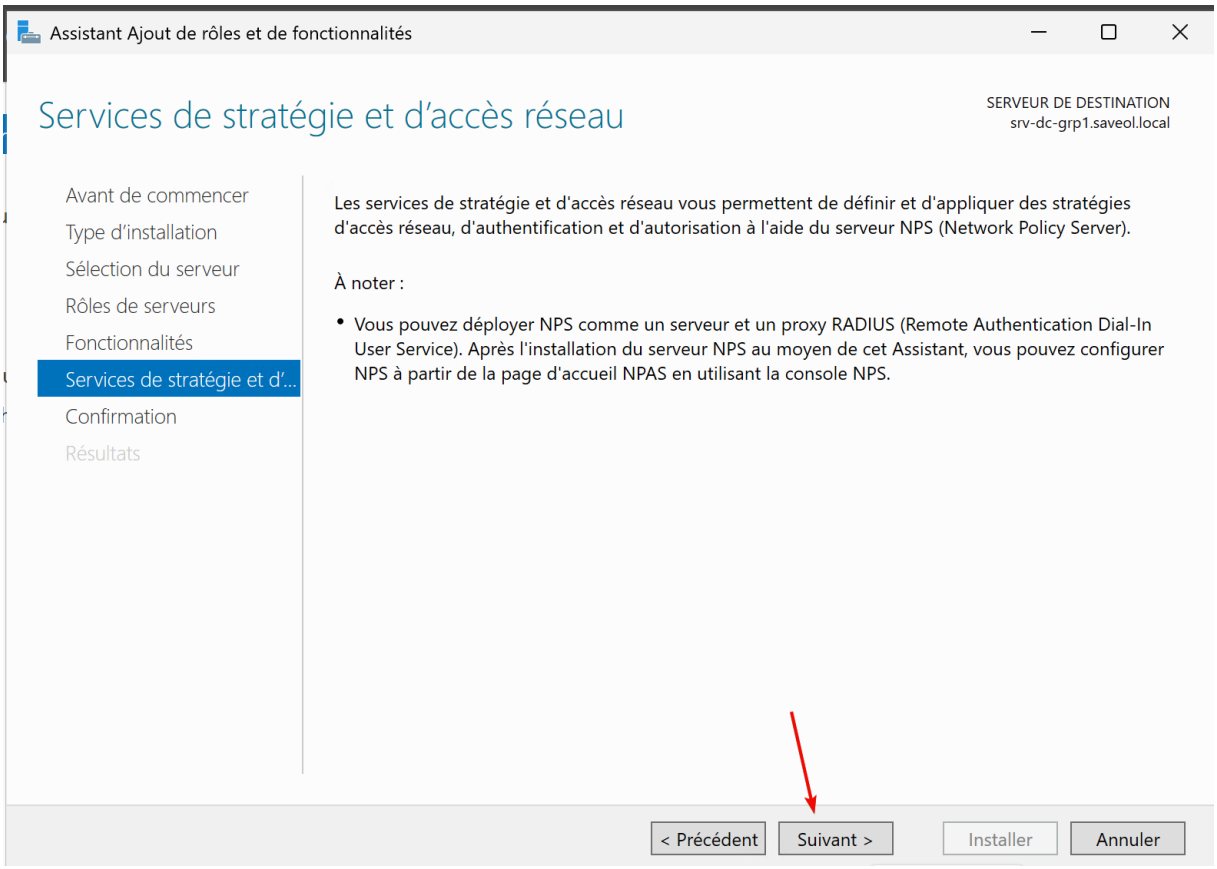
Réalisation :

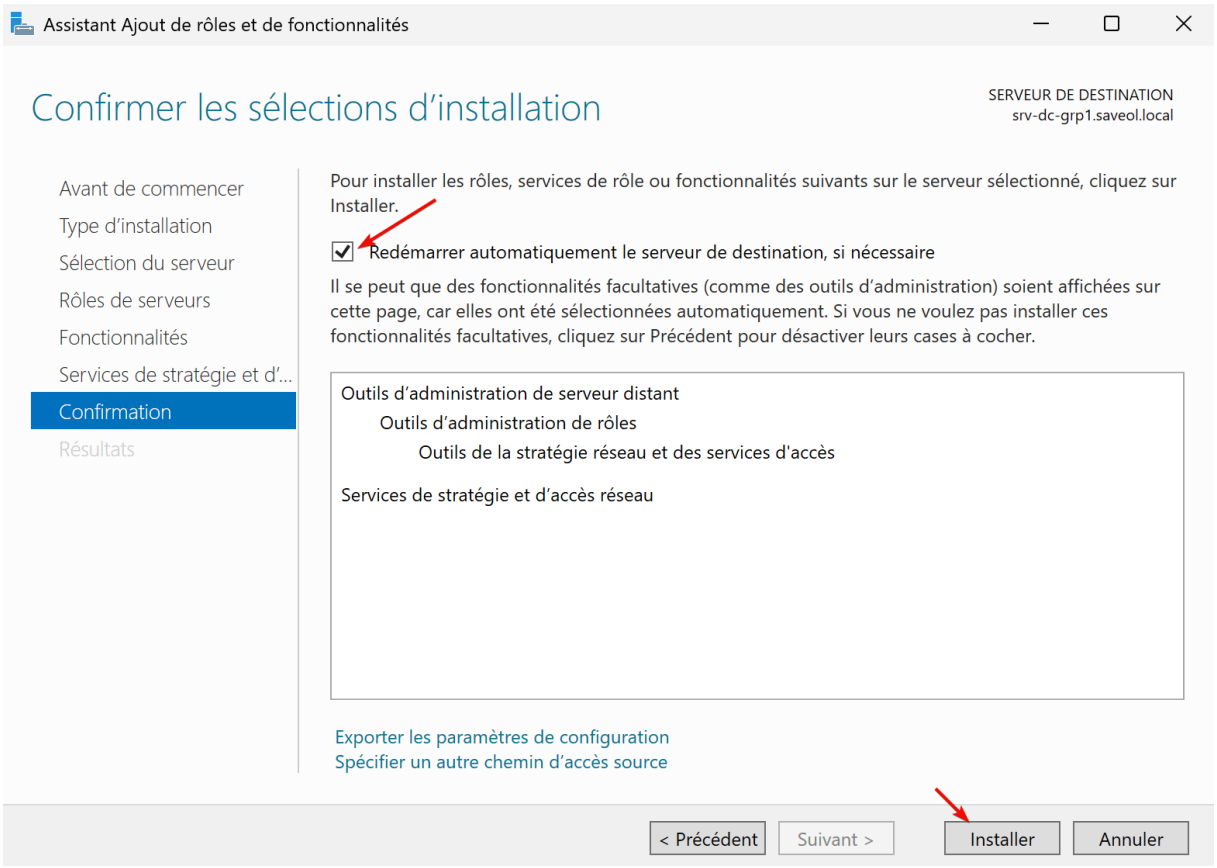
Installer le rôle NPS en vous référant aux captures d'écran.




Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
srv-dc-grp1.saveol.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS (Installé)
Serveur Web (IIS) (19 sur 42 installé(s))
Service Guardian hôte
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manager
Services Bureau à distance (3 sur 6 installé(s))
Services d'activation en volume
Services d'impression et de numérisation de docur
Services de certificats Active Directory
Services de déploiement Windows
Services de domaine Active Directory (Installé)
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (2 sur 12 installé
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
Description
Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.
< Précédent
Suivant >
Installer
Annuler

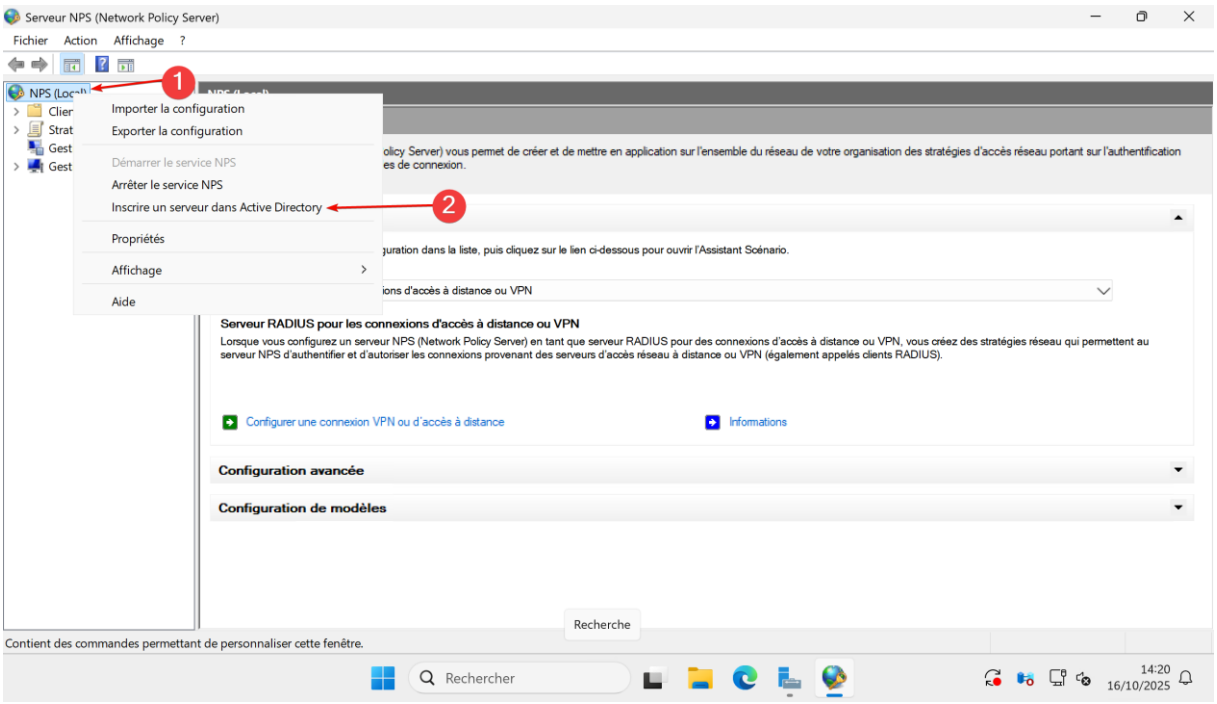

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des fonctionnalités
SERVEUR DE DESTINATION
srv-dc-grp1.saveol.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.
Fonctionnalités
.NET Framework 4.8 Features (3 sur 7 installé(s))
Antivirus Microsoft Defender (Installé)
Assistance à distance
Background Intelligent Transfer Service (BITS)
Base de données interne Windows (Installé)
BranchCache
Chiffrement de lecteur BitLocker
Client d'impression Internet
Client pour NFS
Clustering de basculement
Collection des événements de configuration et de
Conteneurs
Data Center Bridging
Déverrouillage réseau BitLocker
Direct Play
Équilibrage de la charge réseau
Équilibreur de charge logiciel
Expérience audio-vidéo haute qualité Windows
Extension ISS Management OData
Description
.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
< Précédent
Suivant >
Installer
Annuler

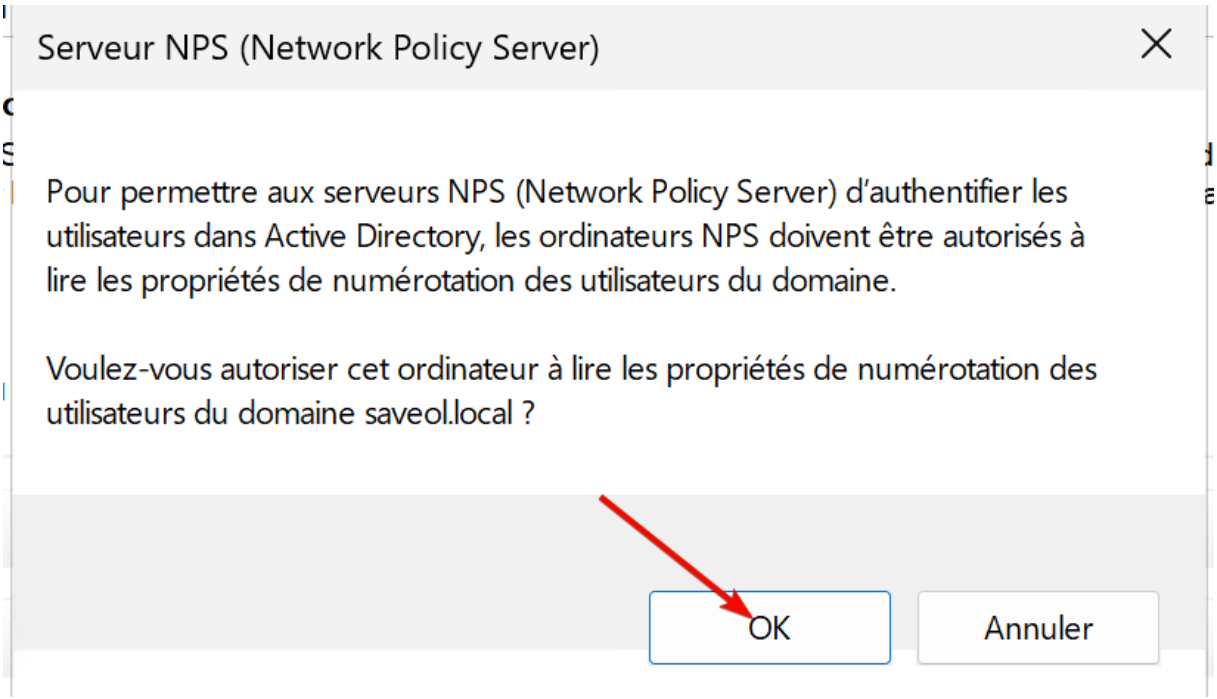

Assistant Ajout de rôles et de fonctionnalités
Services de stratégie et d'accès réseau
SERVEUR DE DESTINATION
srv-dc-grp1.saveol.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats
Les services de stratégie et d'accès réseau vous permettent de définir et d'appliquer des stratégies d'accès réseau, d'authentification et d'autorisation à l'aide du serveur NPS (Network Policy Server).
À noter :
Vous pouvez déployer NPS comme un serveur et un proxy RADIUS (Remote Authentication Dial-In User Service). Après l'installation du serveur NPS au moyen de cet Assistant, vous pouvez configurer NPS à partir de la page d'accueil NPAS en utilisant la console NPS.
< Précédent
Suivant >
Installer
Annuler

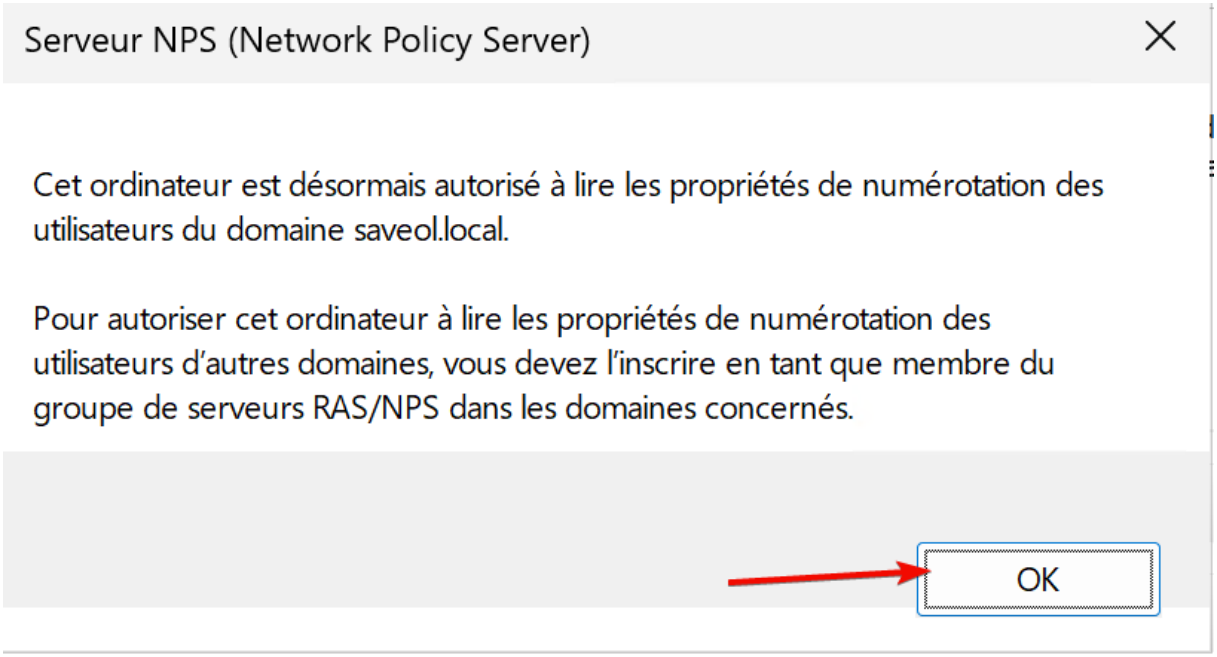

Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
srv-dc-grp1.saveol.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de la stratégie réseau et des services d'accès
Services de stratégie et d'accès réseau
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

Enregistrer NPS dans Active Directory

Une fois cela fait lier le serveur NPS a l'active directory

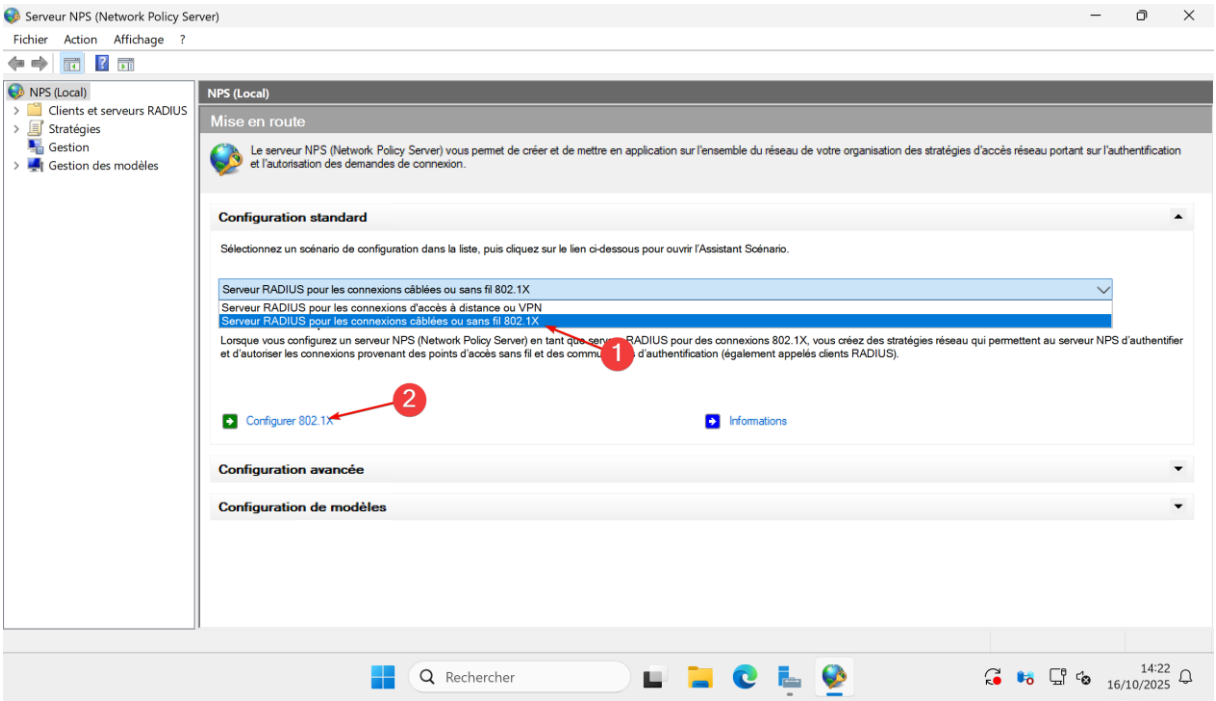




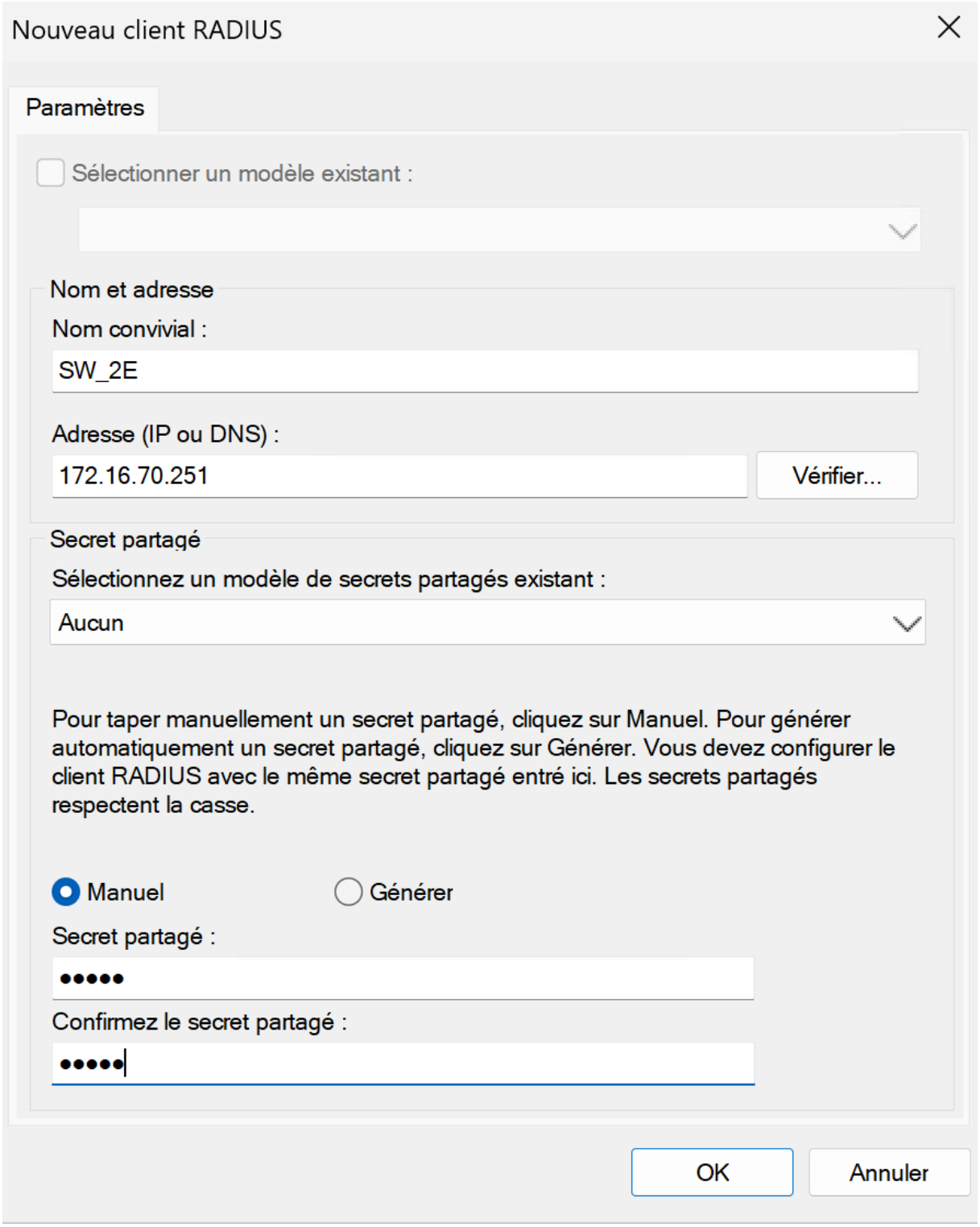


Création des clients RADIUS

Une fois cela fait il faut crée une configuration pour que les équipements puissent se connecter



Faire comme la configuration du switch SW_2E pour tous les équipements de l'infra
En définissant :
-le nom de l'appareil
-l'adresse IP de l'équipement
-defnir le mot de passe


Nouveau client RADIUS
Paramètres
Sélectionner un modèle existant :
Nom et adresse
Nom convivial :
SW_2E
Adresse (IP ou DNS) :
172.16.70.251
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

Configurer 802.1X

Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X(clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

SWRC	RNET1
SW_1E	RNET2
SW_2E	
SWCOEUR	
ZYXEL	
SW_DMZ_INTERMEDIAIRE	
SW_DMZ_INTERNE	
SWNET	

Ajouter...

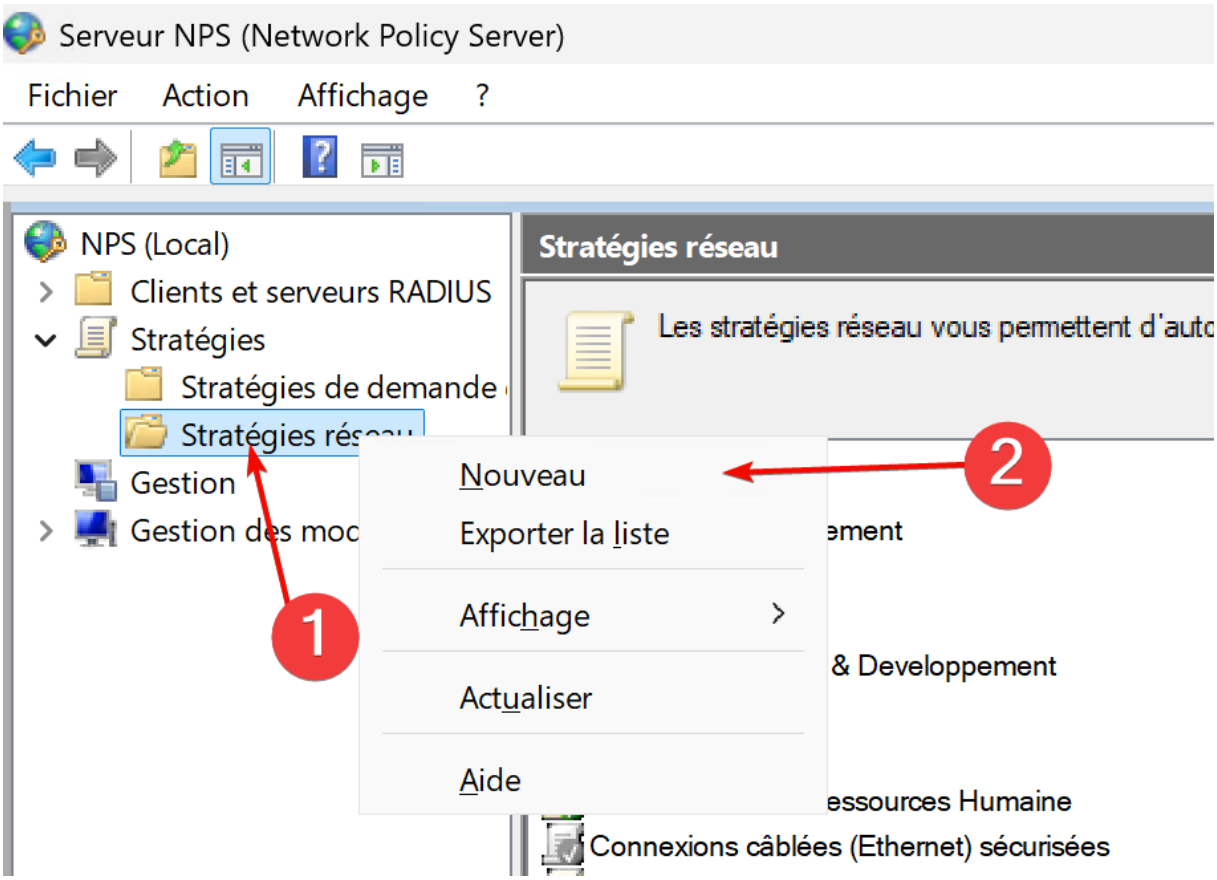
Modifier...

Supprimer

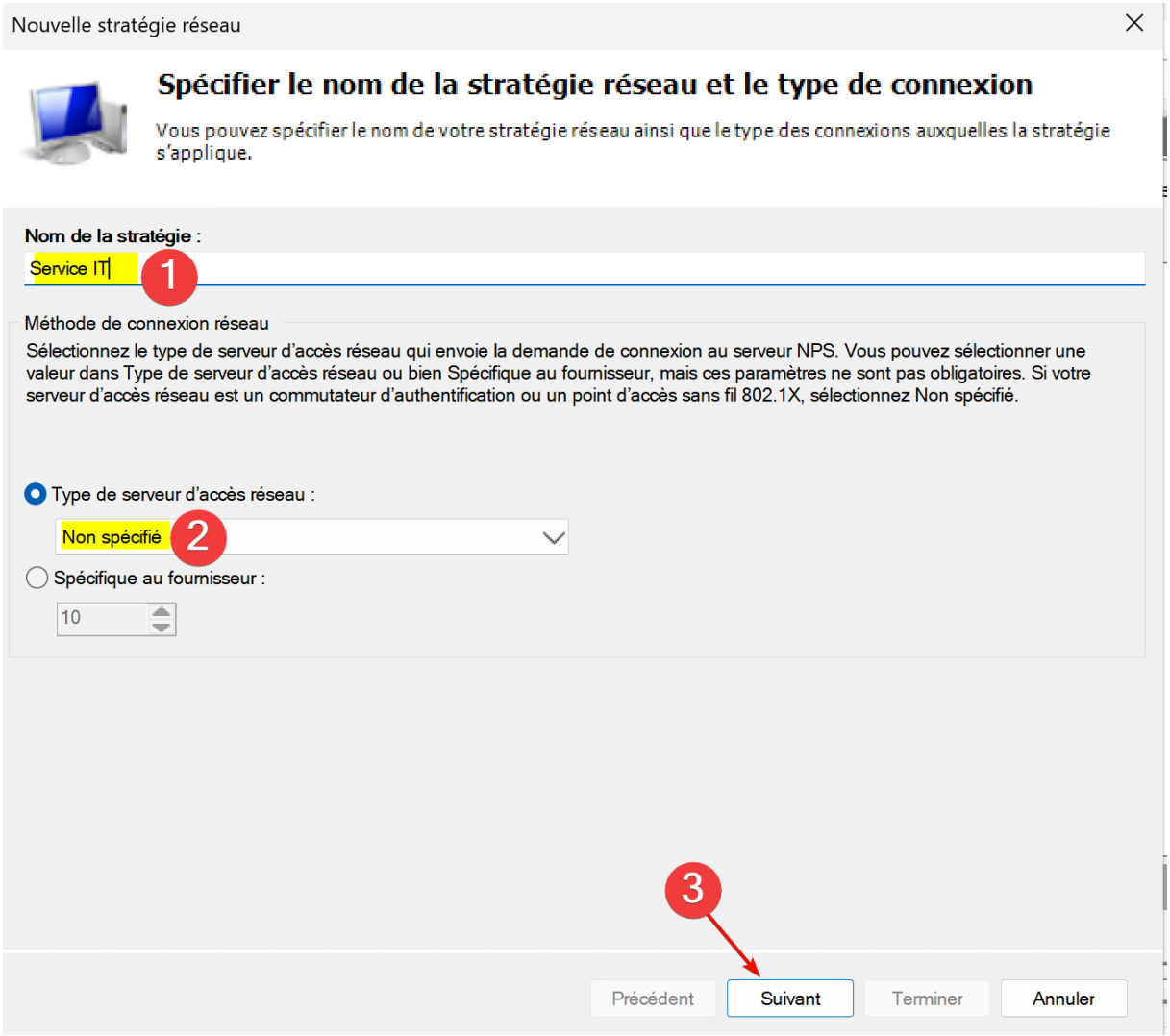
Précédent | Suivant | Terminer | Annuler

Configuration des Stratégies réseaux

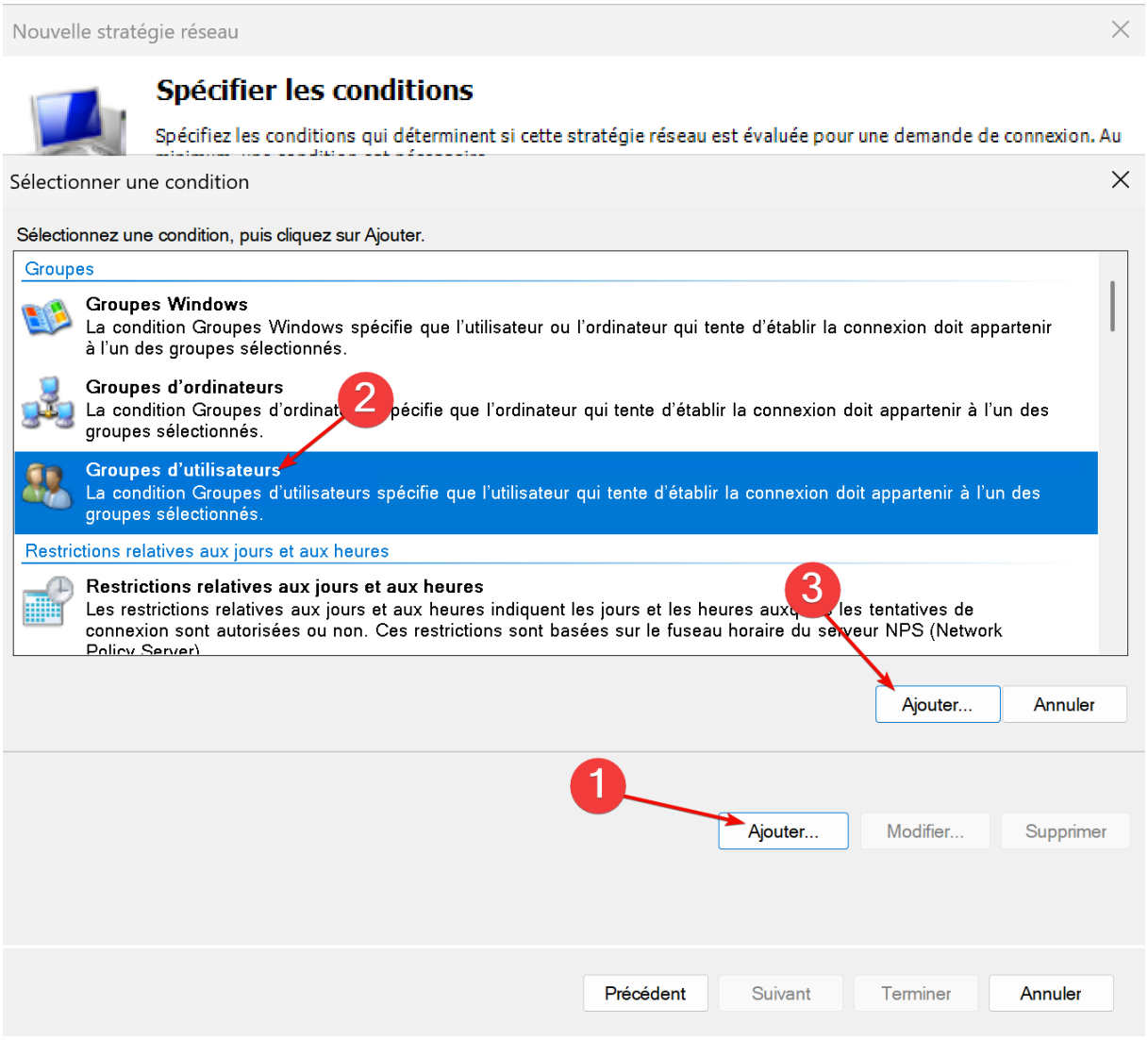
Faite un clique droit sur : Stratégies réseau -> Nouveau

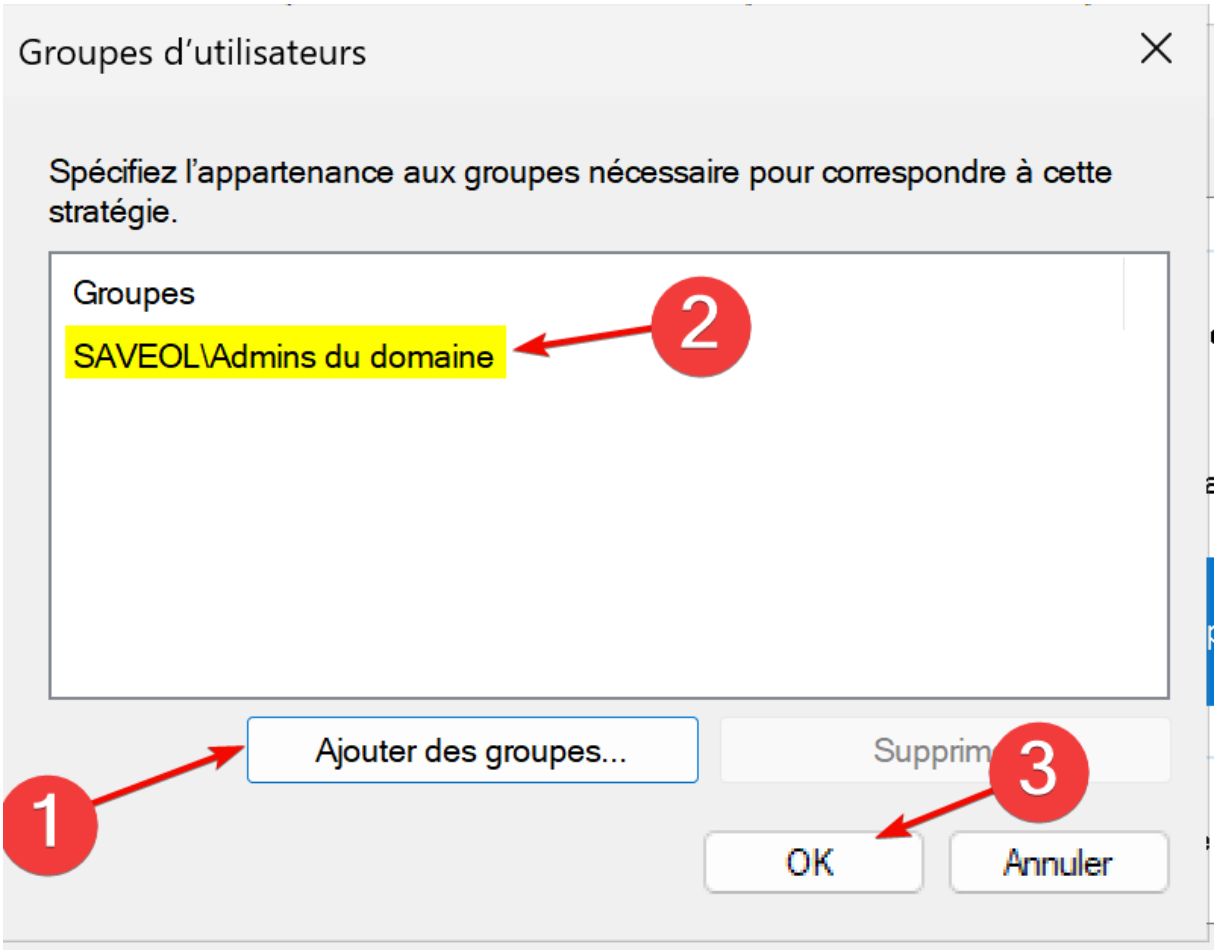


Nommé la stratégie en fonction du VLAN a assigner pour ma part « Service IT », puis laisser le type de serveur d'accès réseau dans « non spécifier », cliquer sur suivant

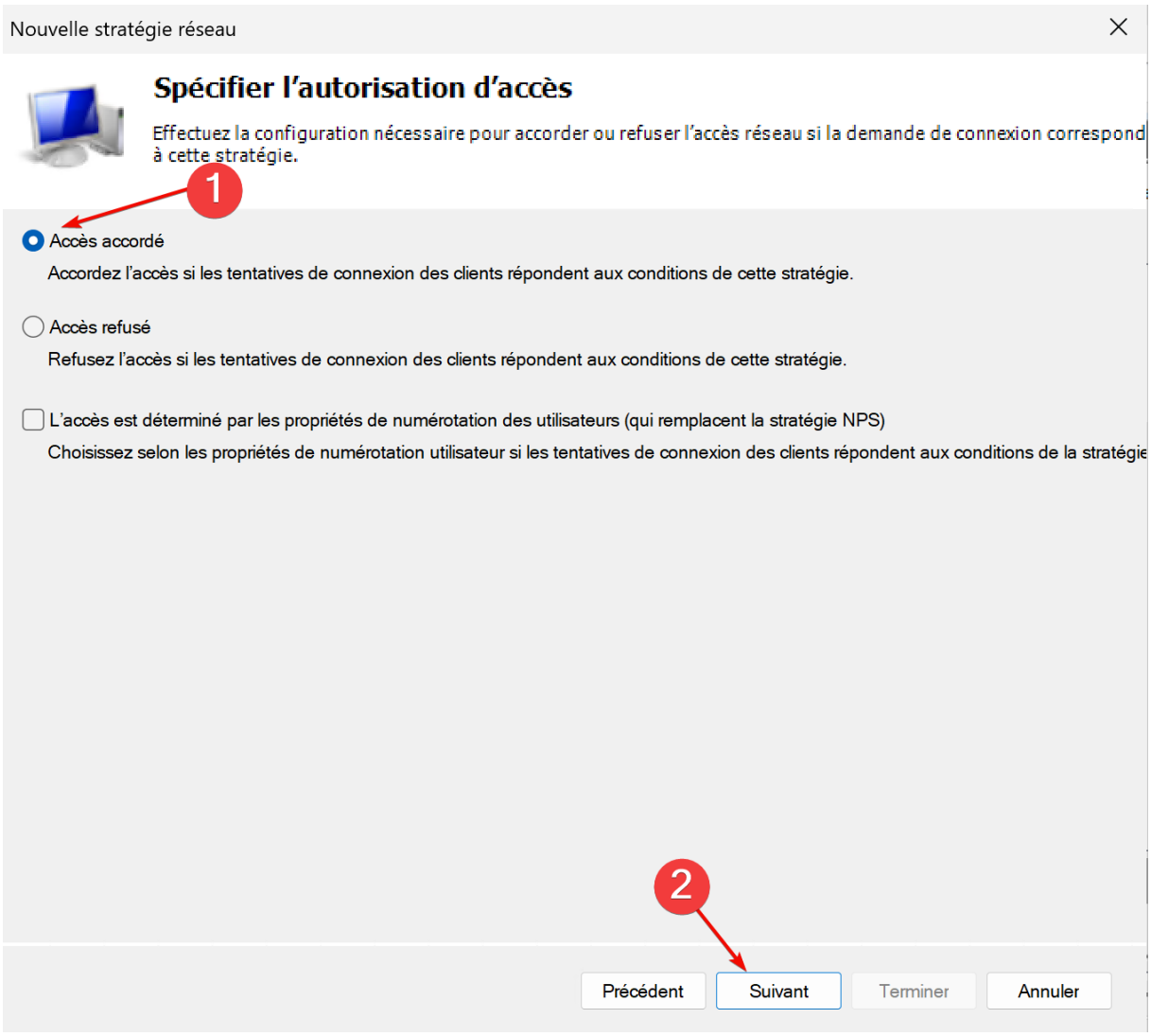


Sélectionne le groupe d'uttilisateur -> Ajouter -> sélectionner le groupe des user -> ok -> suivant

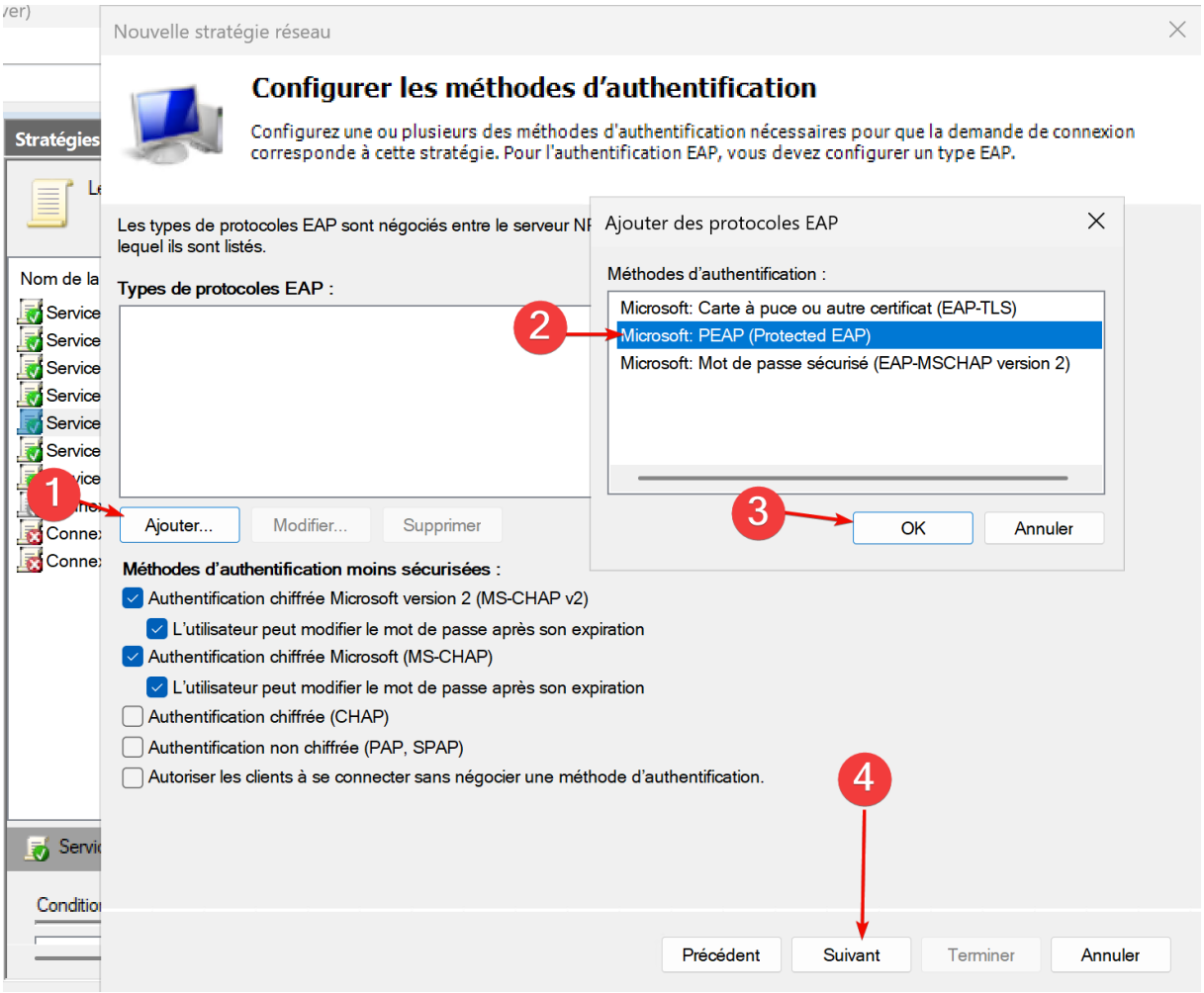

Nouvelle stratégie réseau
Spécifier les conditions
Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au
Sélectionner une condition
Sélectionnez une condition, puis cliquez sur Ajouter.
Groupes
Groupes Windows
La condition Groupes Windows spécifie 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'ordinat pécifie 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 auxq les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server)
Ajouter...
Annuler
1
2
3
Ajouter...
Modifier...
Supprimer
Précédent
Suivant
Terminer
Annuler



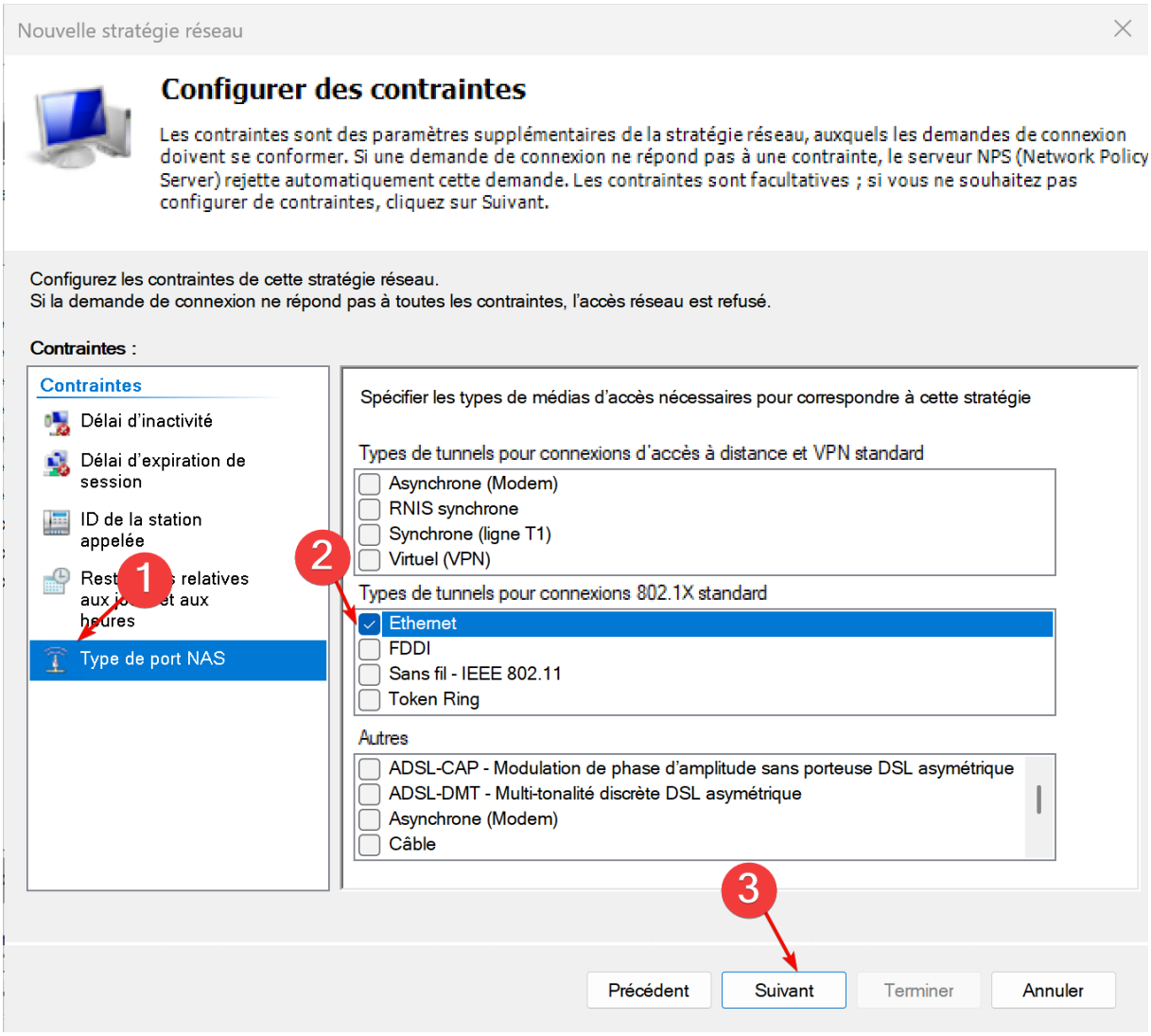
Sélectionner « accès accordé » -> Suivant



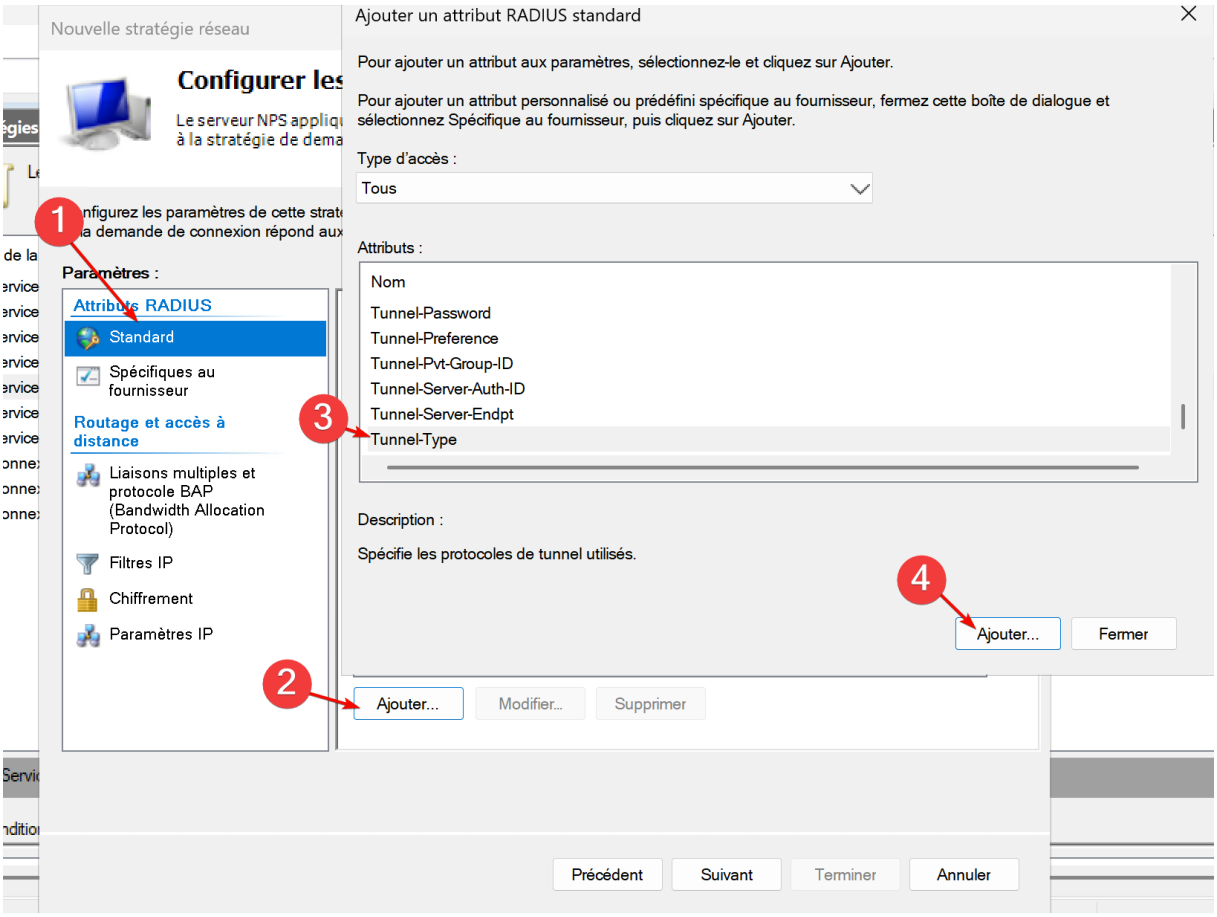
Sélectionne Ajouter -> sélectionner le protocole PEAP -> ok -> suivant

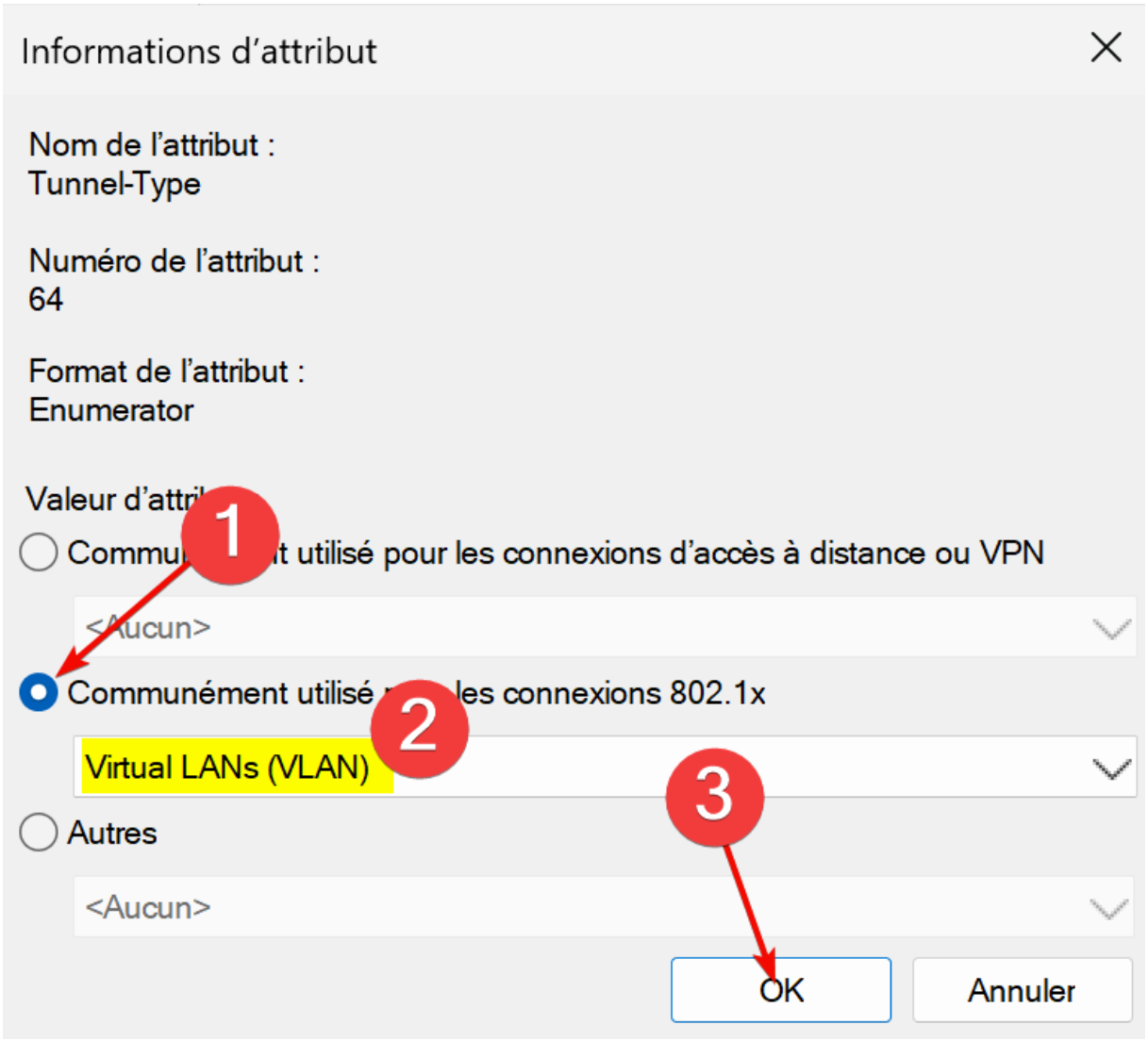


Aller dans « Type de port NAS » -> Cocher la case « Ethernet » -> suivant

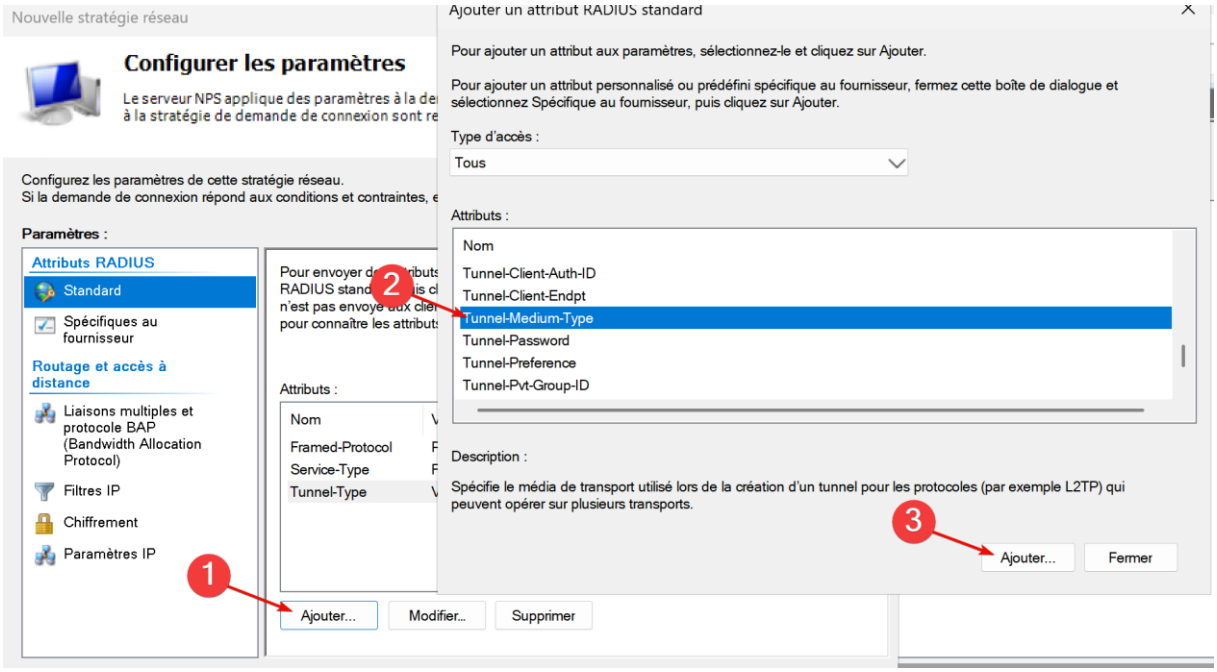


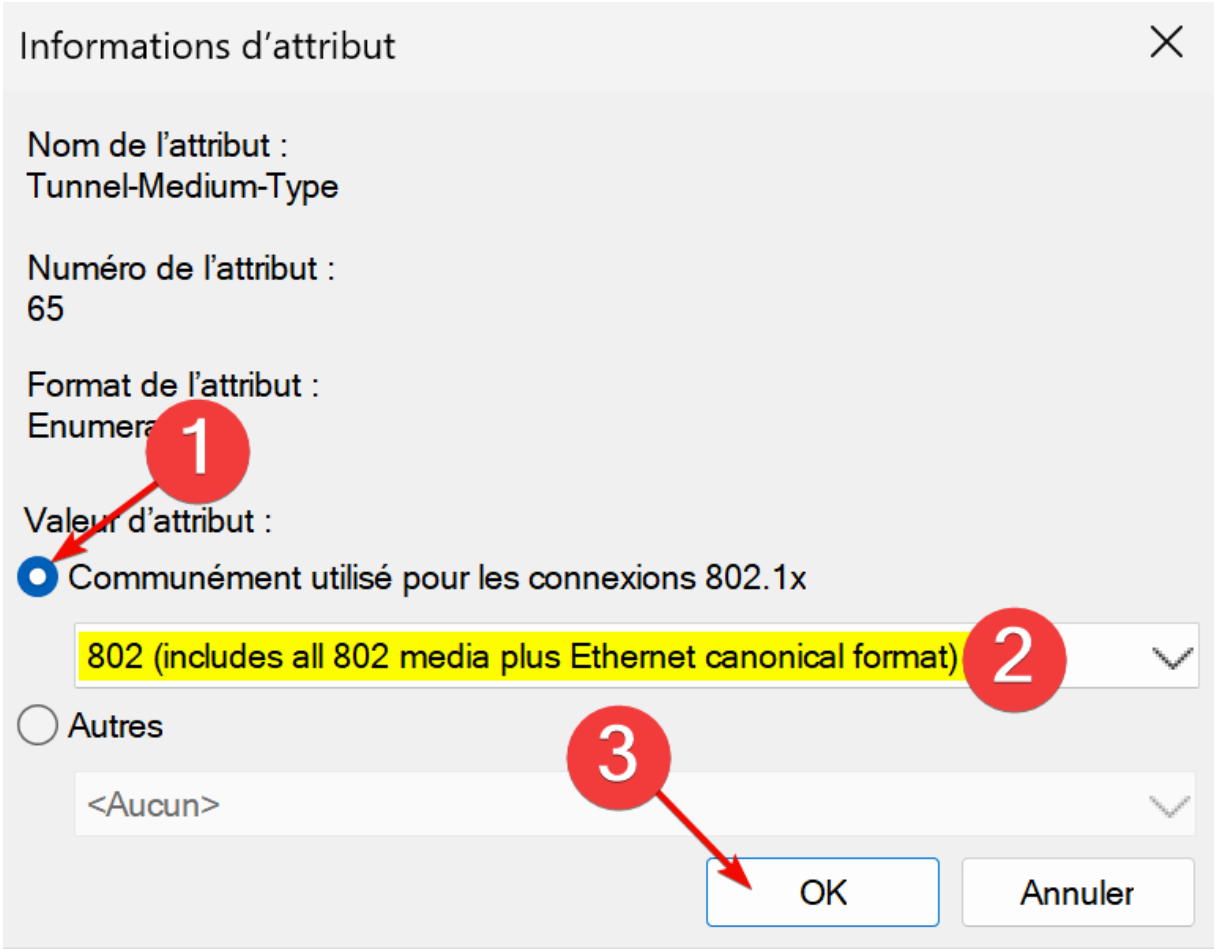
Cliquer sur attributs radius -> Ajouter -> Tunel-Type -> Ajouter -> Sélectionner « communément uttilisé pour les connexions 802.1X » -> Selectionner « VLAN » -> OK


Nouvelle stratégie réseau
Configurer les
Le serveur NPS appliqu
à la stratégie de dema
nfigurez les paramètres de cette strat
la demande de connexion répond aux
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
Ajouter...
Modifier...
Supprimer
Précédent
Suivant
Terminer
Annuler
Ajouter un attribut RADIUS standard
Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.
Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.
Type d'accès :
Tous
Attributs :
Nom
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type
Description :
Spécifie les protocoles de tunnel utilisés.
Ajouter...
Fermer
1
2
3
4

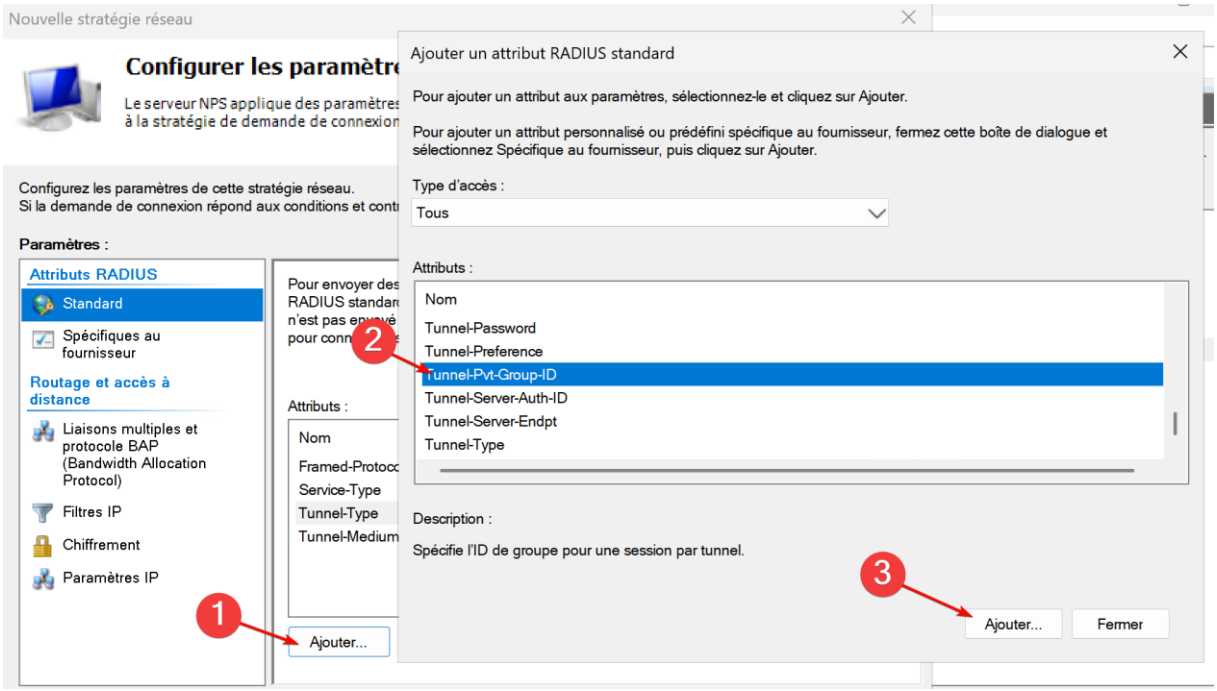


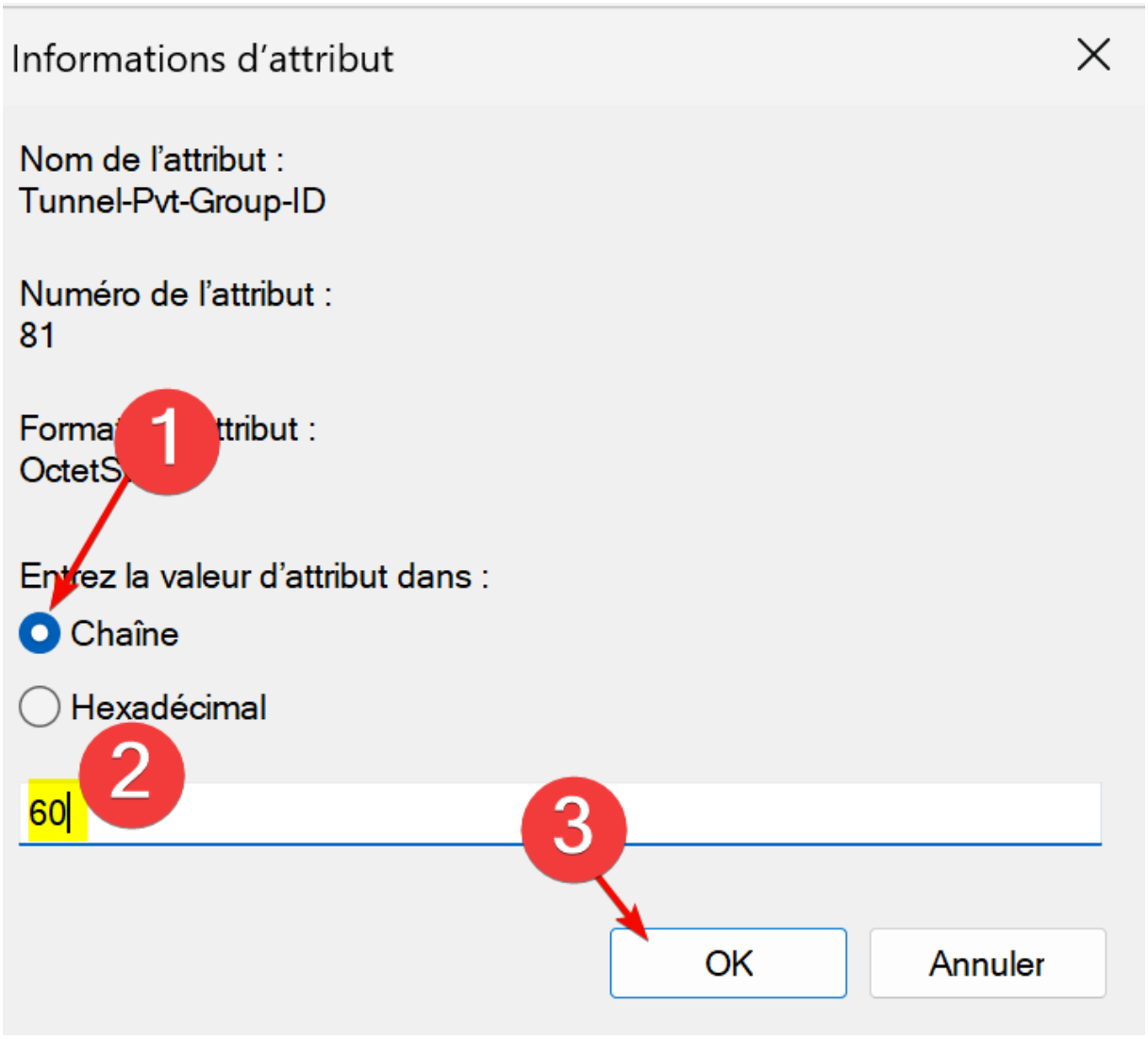
Cliquer sur attributs radius -> Ajouter -> Tunel-Medium-Type -> Ajouter -> Sélectionner « communément uttilisé pour les connexions 802.1X » -> Selectionner «802 » -> OK

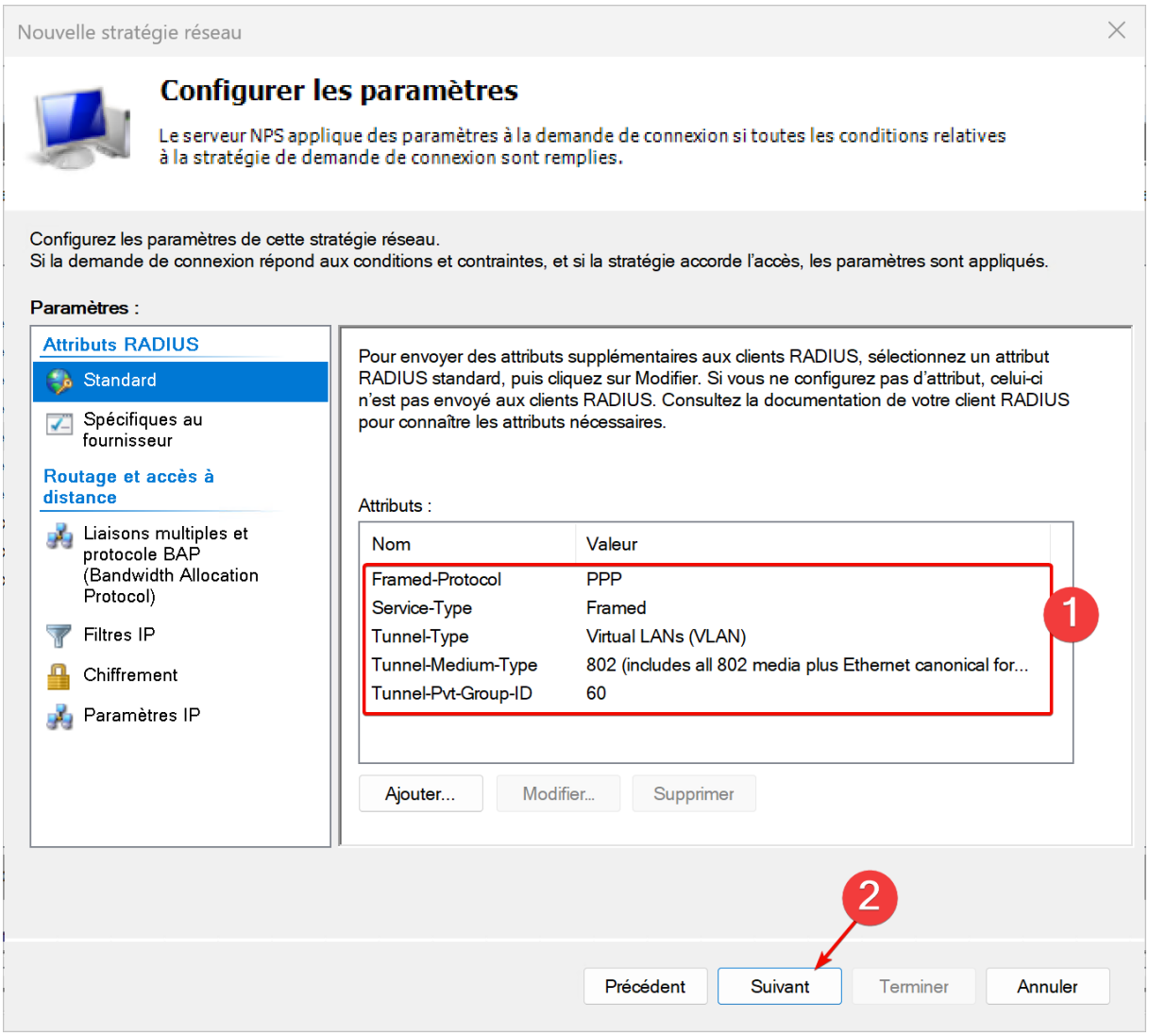




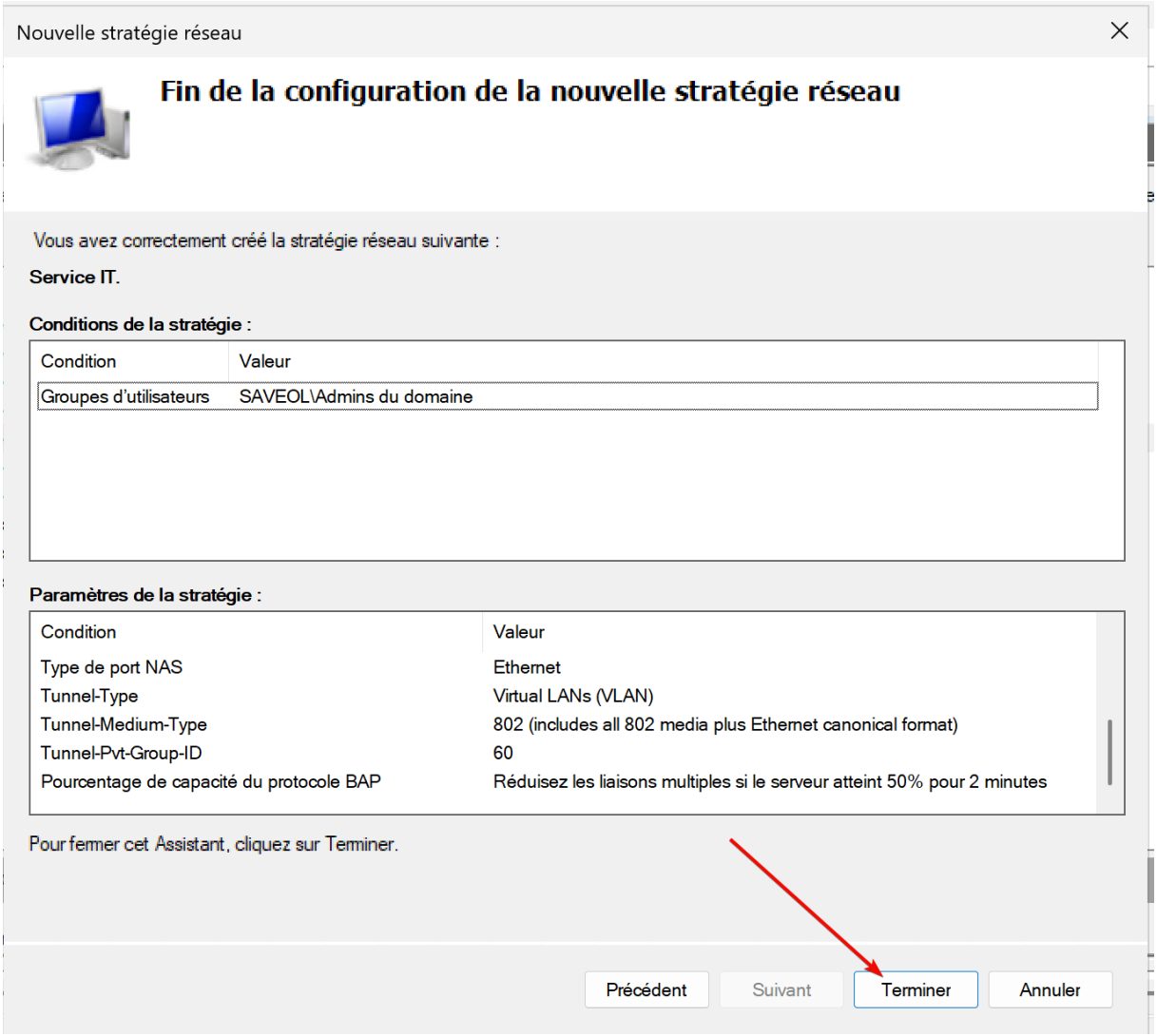
Cliquer sur attributs radius -> Ajouter -> Tunel-Pvt-Groupe-ID -> Ajouter -> Sélectionner « chaîne » -> rentré le numéro du vlan -> OK


Nouvelle stratégie réseau
Configurer les paramètre
Le serveur NPS applique des paramètres
à la stratégie de demande de connexion
Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contr
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
RADIUS standar
n'est pas envoyé
pour conn
Attributs :
Nom
Framed-Protocc
Service-Type
Tunnel-Type
Tunnel-Medium
Ajouter...
1
Ajouter un attribut RADIUS standard
Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.
Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.
Type d'accès :
Tous
Attributs :
Nom
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type
2
Description :
Spécifie l'ID de groupe pour une session par tunnel.
3
Ajouter...
Fermer


Informations d'attribut
Nom de l'attribut :
Tunnel-Pvt-Group-ID
Numéro de l'attribut :
81
Forma ttribut :
OctetS
1
Entrez la valeur d'attribut dans :
Chaîne
Hexadécimal
2
60
3
OK
Annuler

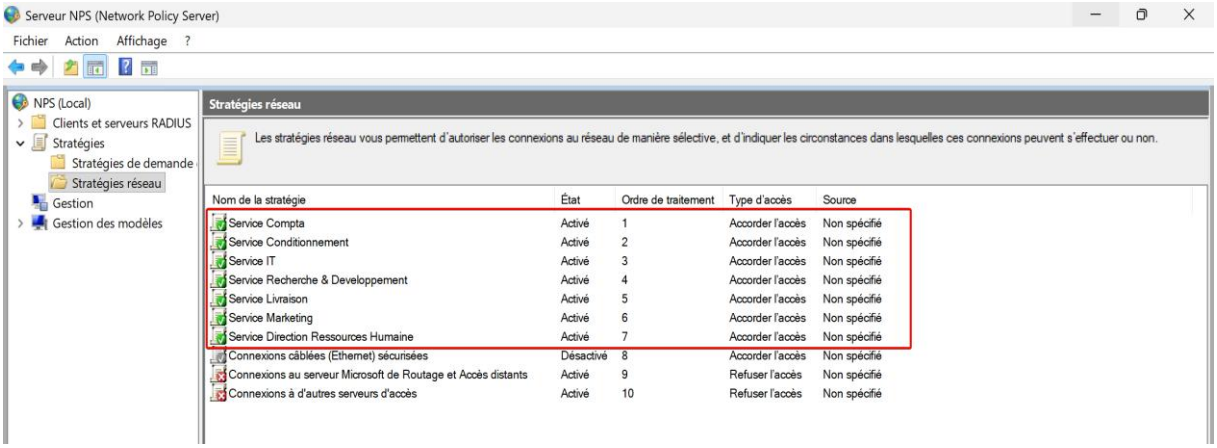


Cliquer sur attributs radius -> Vérifier que la configuration soit identique au screen -> Suivant -> Terminer



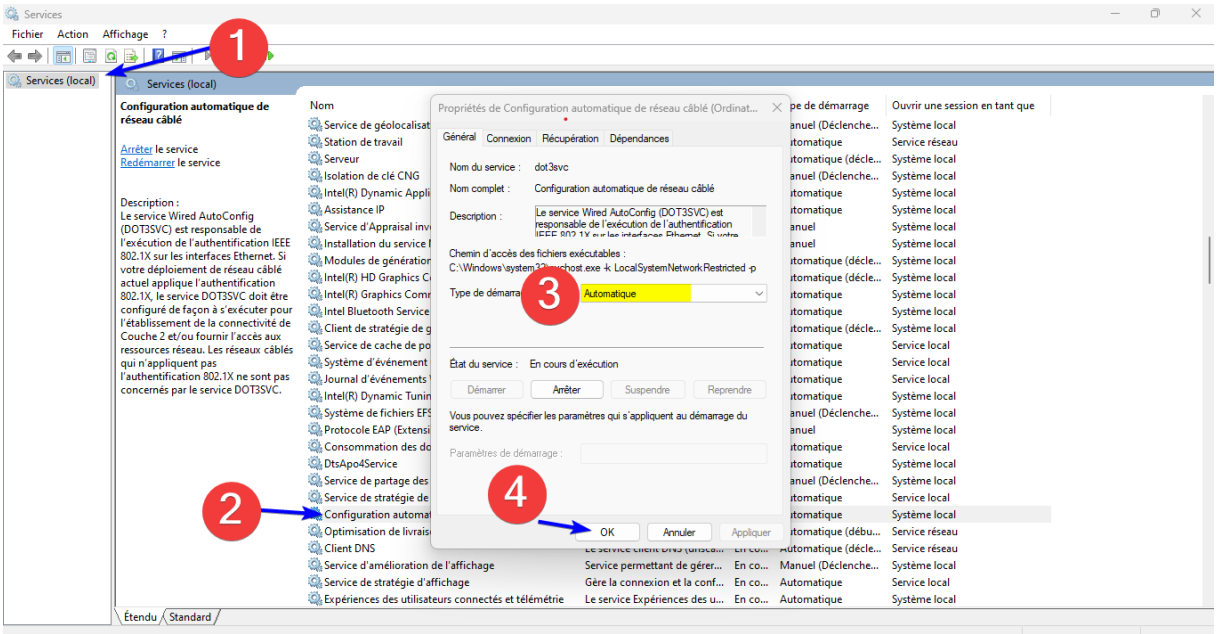
Reproduisez la stratégie réseau en ajustant les paramètres du groupe et le numéro du VLAN pour chaque stratégie, en vous basant sur les informations du tableau.

Nom de la stratégie	***Nom du groupe***	***Numéro du vlan***
Service Compta	Comptabilité	10
Service Marketing	Marketing	20
Service Conditionnement	Conditionnement	30
Service Livraison	Livraison	40
Service R&D	Recherche	50
Service IT	Admins du domaine	60
Service Direction RH	Direction	80



Paramétrage du 802.1X sur le PC client

Ouvrer « Service » -> cliquer sur « Configuration de configuration automatique de réseau câblé » -> sélectionner comme type de démarrage « Automatique » -> cliquer sur « ok »



Configuration des switches

Configuration des switches :

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

```
(config)#RADIUS-server host 172.16.100.2 auth-port 1645 acct-port 1646 key admin
(config)#RADIUS-server host 172.16.100.2 auth-port 1812 acct-port 1813 key admin
```

```
aaa group server radius DC1
 server 172.16.100.2 auth-port 1645 acct-port 1646
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
```

Configuration des ports du switch :

```
interface FastEthernet0/1
 switchport mode access
 authentication host-mode multi-host
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast trunk
!
interface FastEthernet0/2
 switchport mode access
 authentication host-mode multi-host
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast trunk
!
interface FastEthernet0/3
 switchport mode access
 authentication host-mode multi-host
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast trunk
!
```

Configuration des switches pour mettre en place l'authentification en mode radius :

```
aaa new-model
aaa group server radius DC1

server 172.16.100.2 auth-port 1645 acct-port 1646
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization exec default group radius local

aaa authorization network default group radius
dot1x system-auth-control
radius-server host 172.16.100.2 auth-port 1645 acct-port 1646 key admin
radius-server host 172.16.100.2 auth-port 1812 acct-port 1813 key admin
```