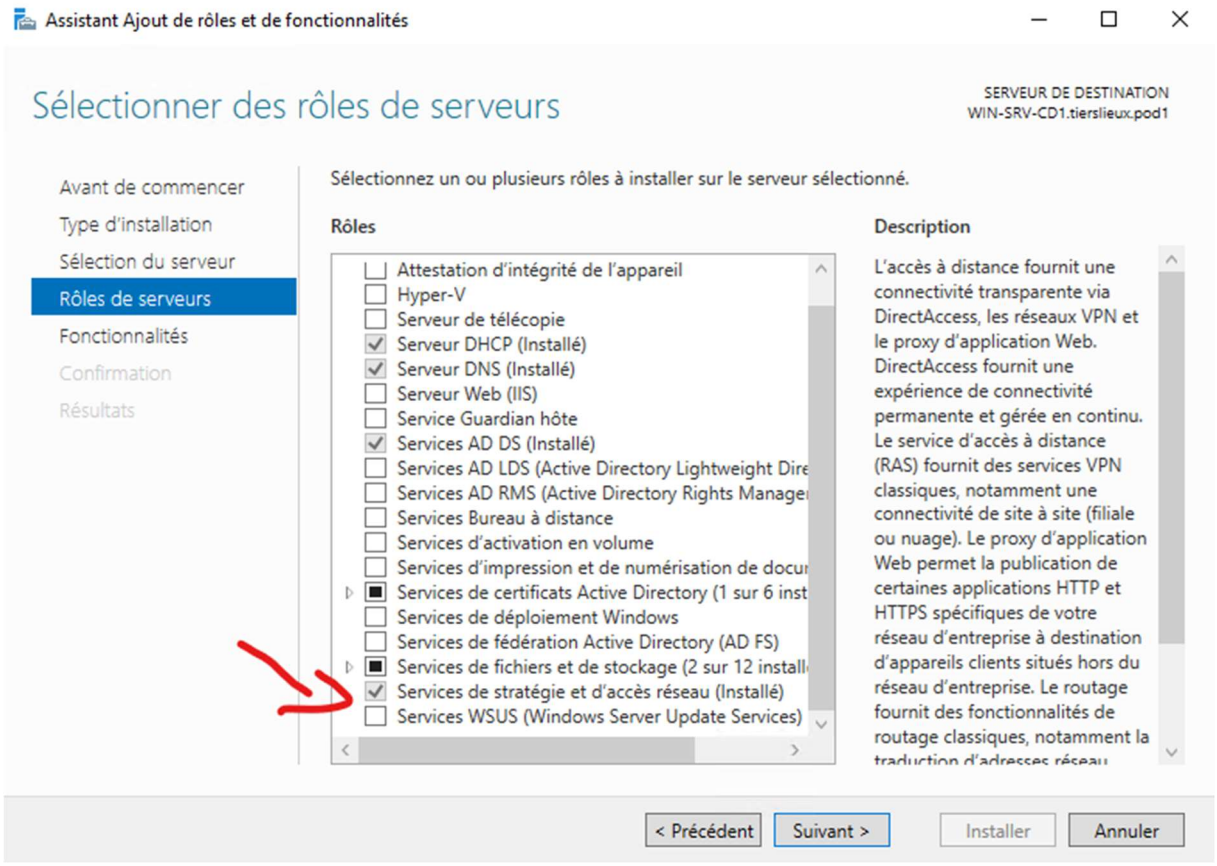
Mise en place d’une infrastructure radius

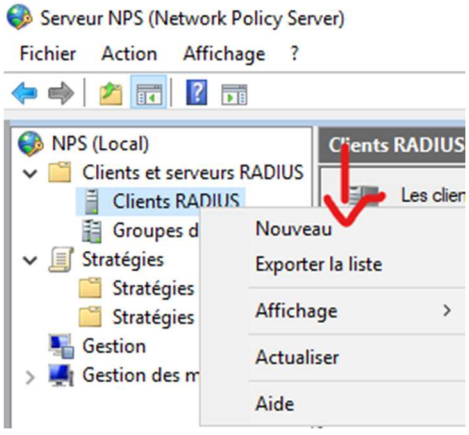
Table des matières

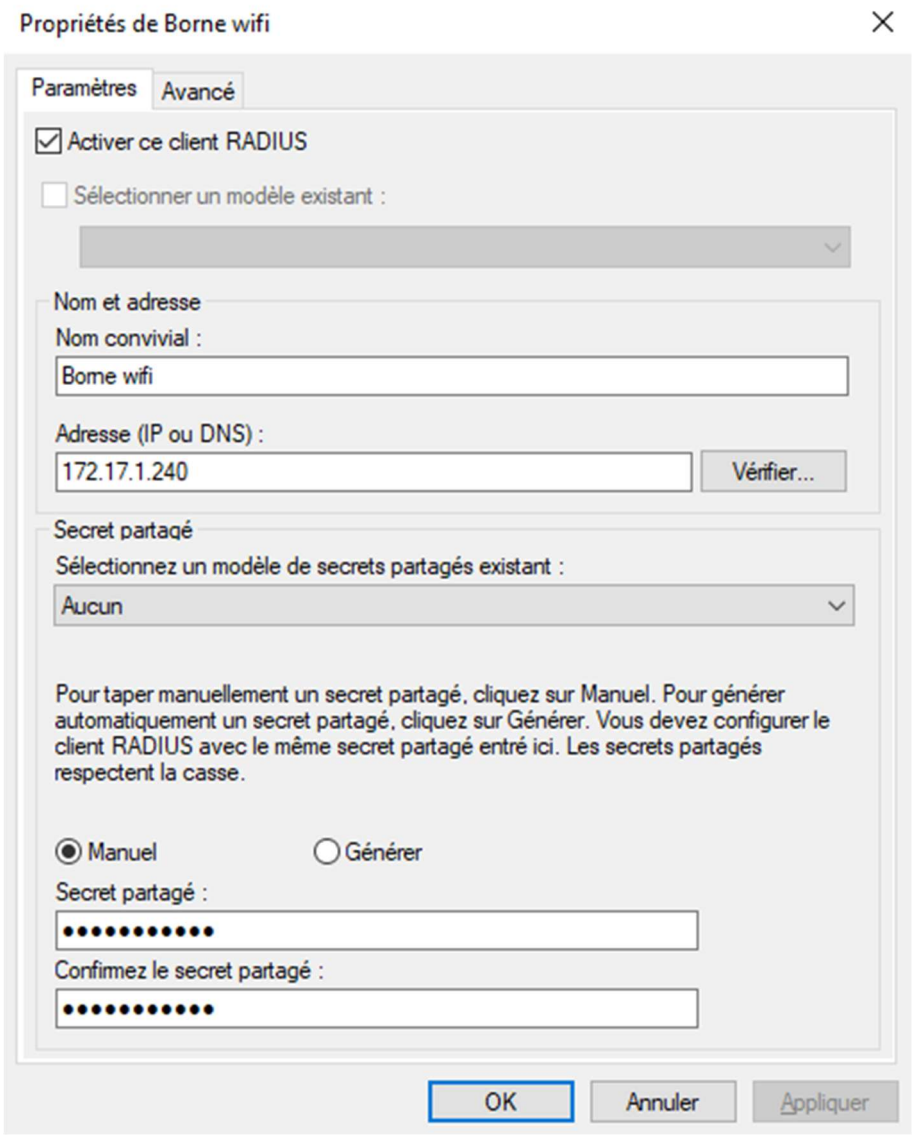
Installation du serveur NPS (radius)

Installer le serveur nps

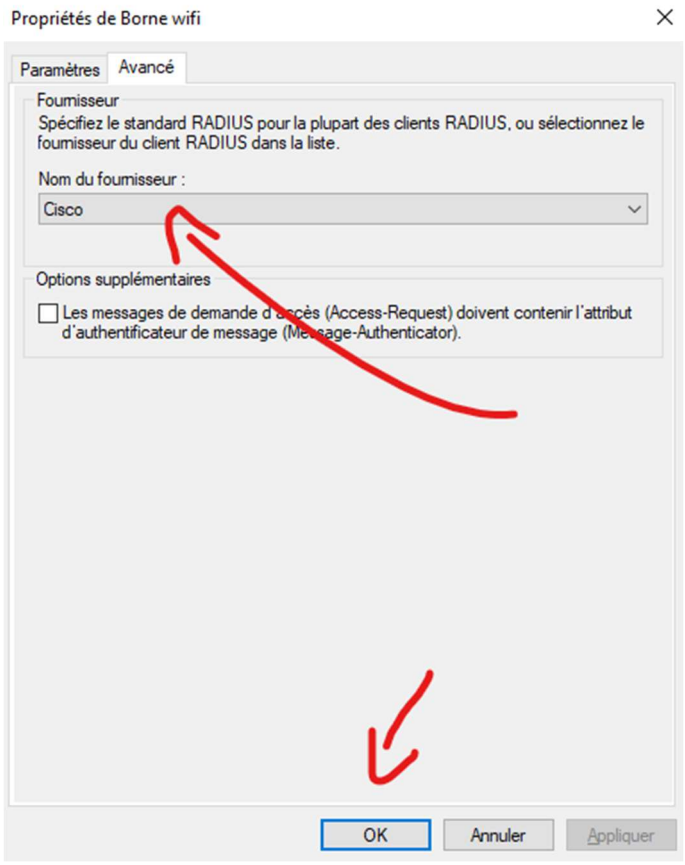


Ajouter un nouveau client

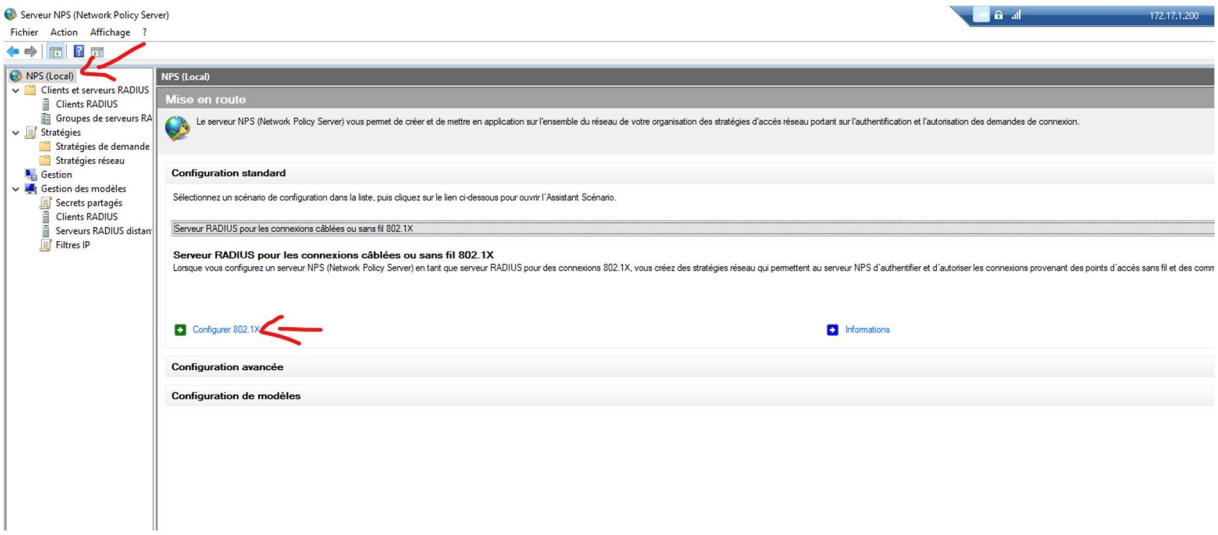


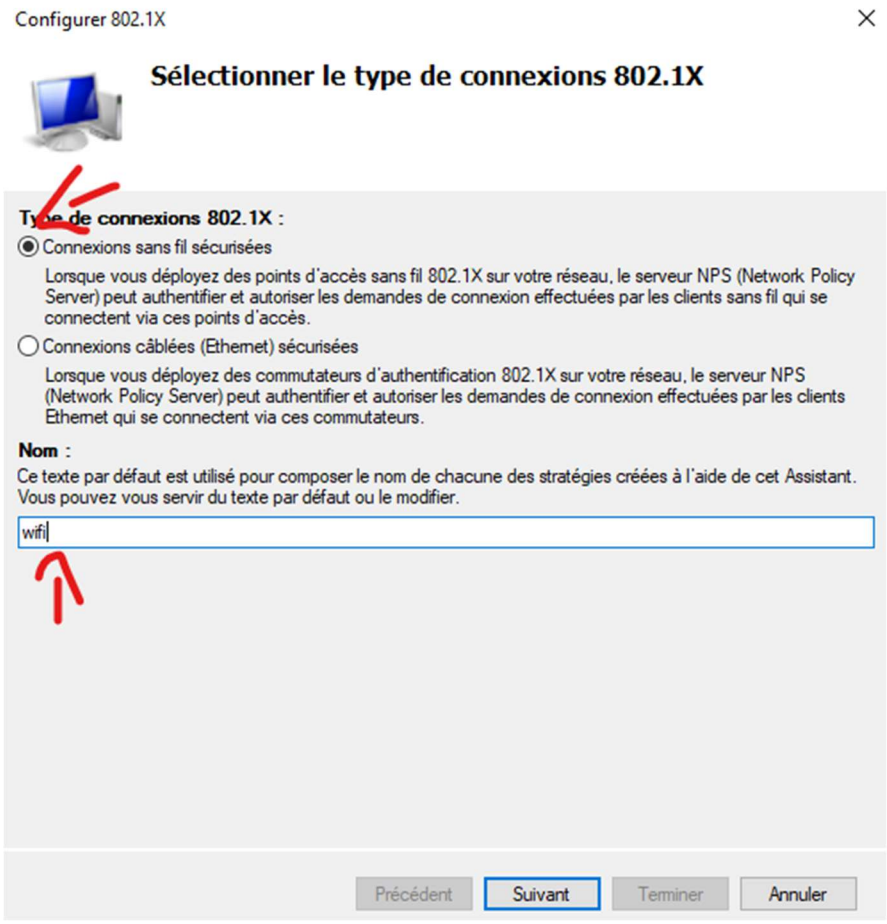


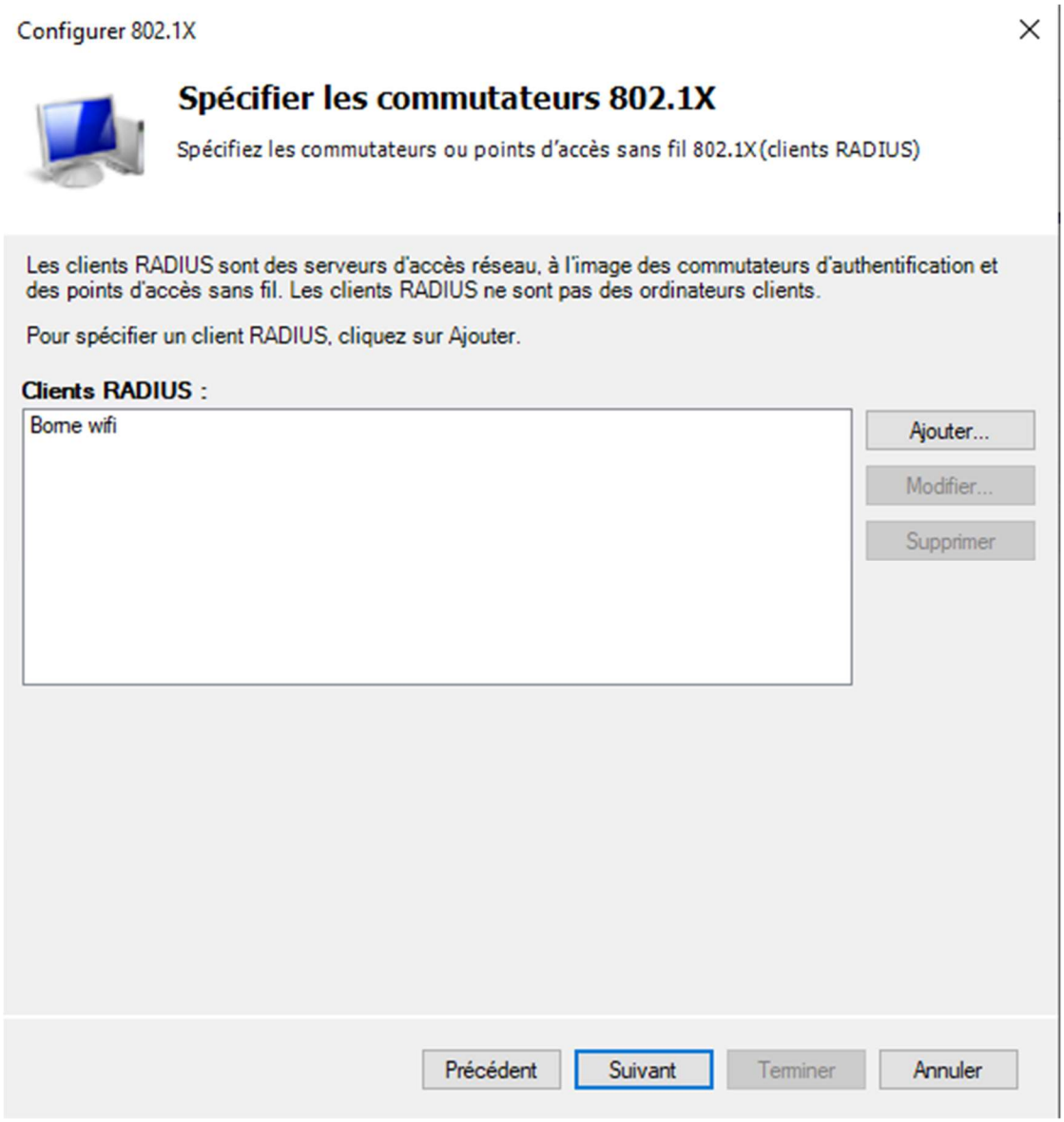
Ajouter le fournisseur Cisco si le client est de la marque Cisco

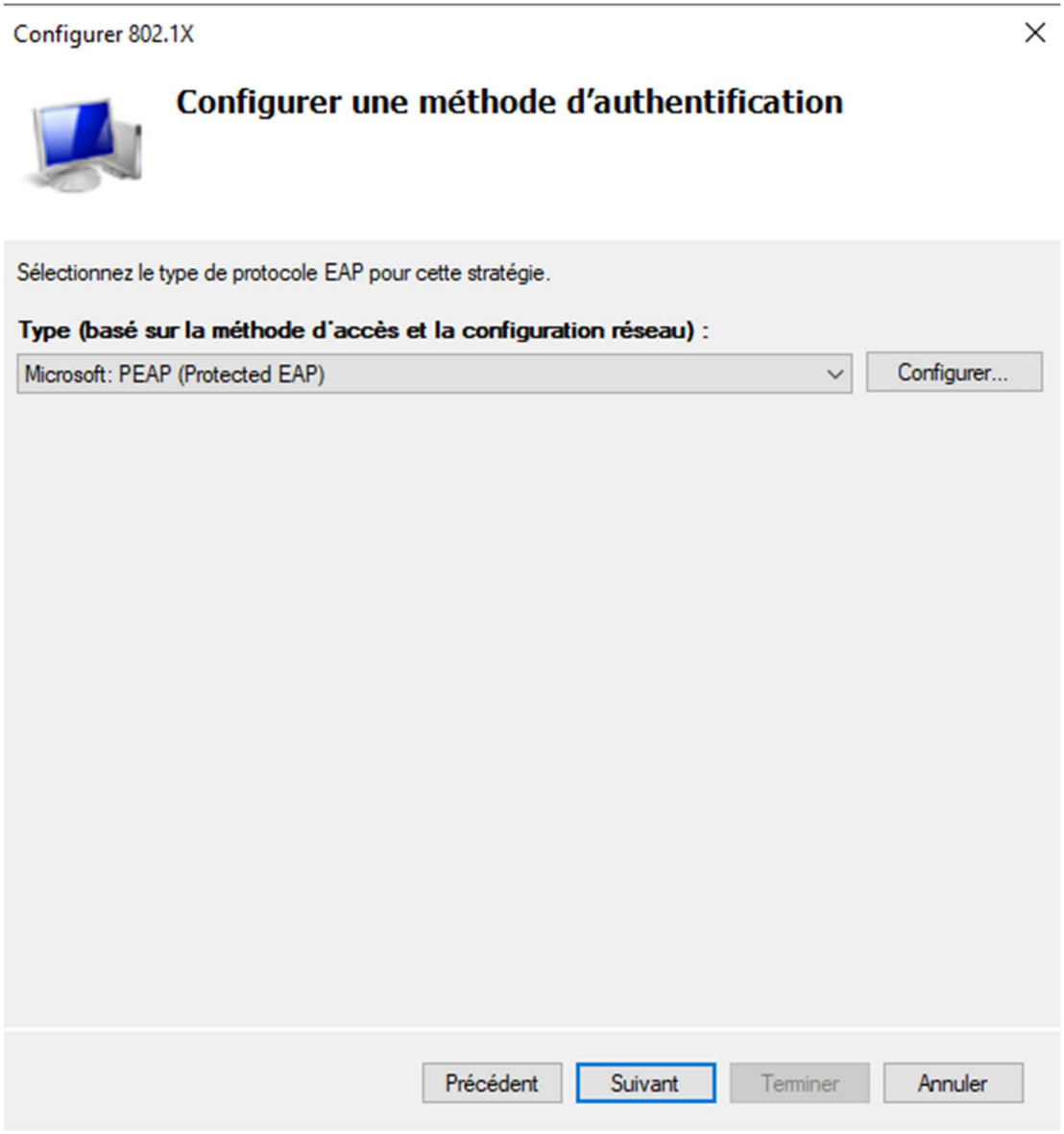


Ajouter la règle des autorisations

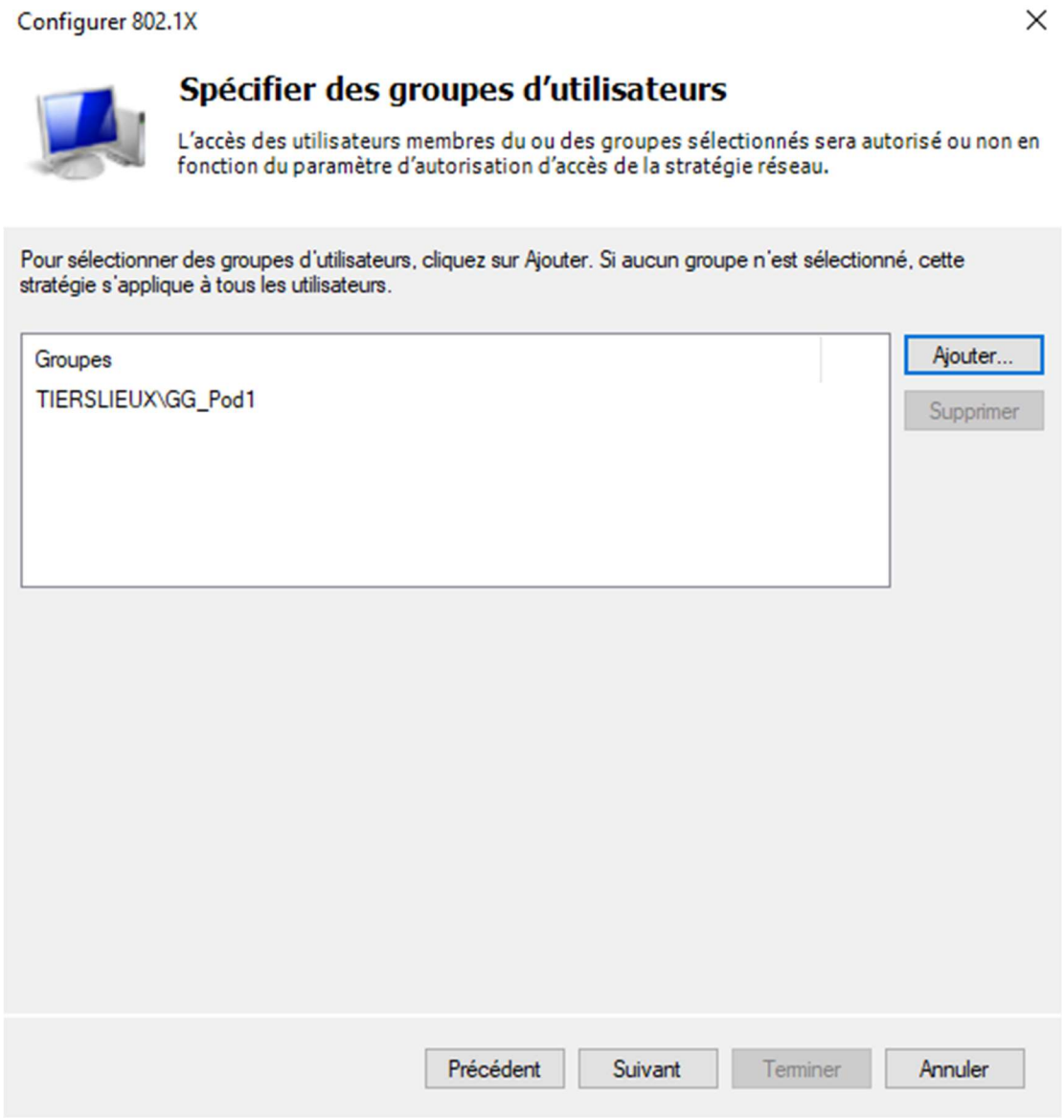



Configurer 802.1X
Sélectionner le type de connexions 802.1X
Type de connexions 802.1X :
Connexions sans fil sécurisées
Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.
Connexions câblées (Ethernet) sécurisées
Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.
Nom :
Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.
wifi
Précédent
Suivant
Terminer
Annuler

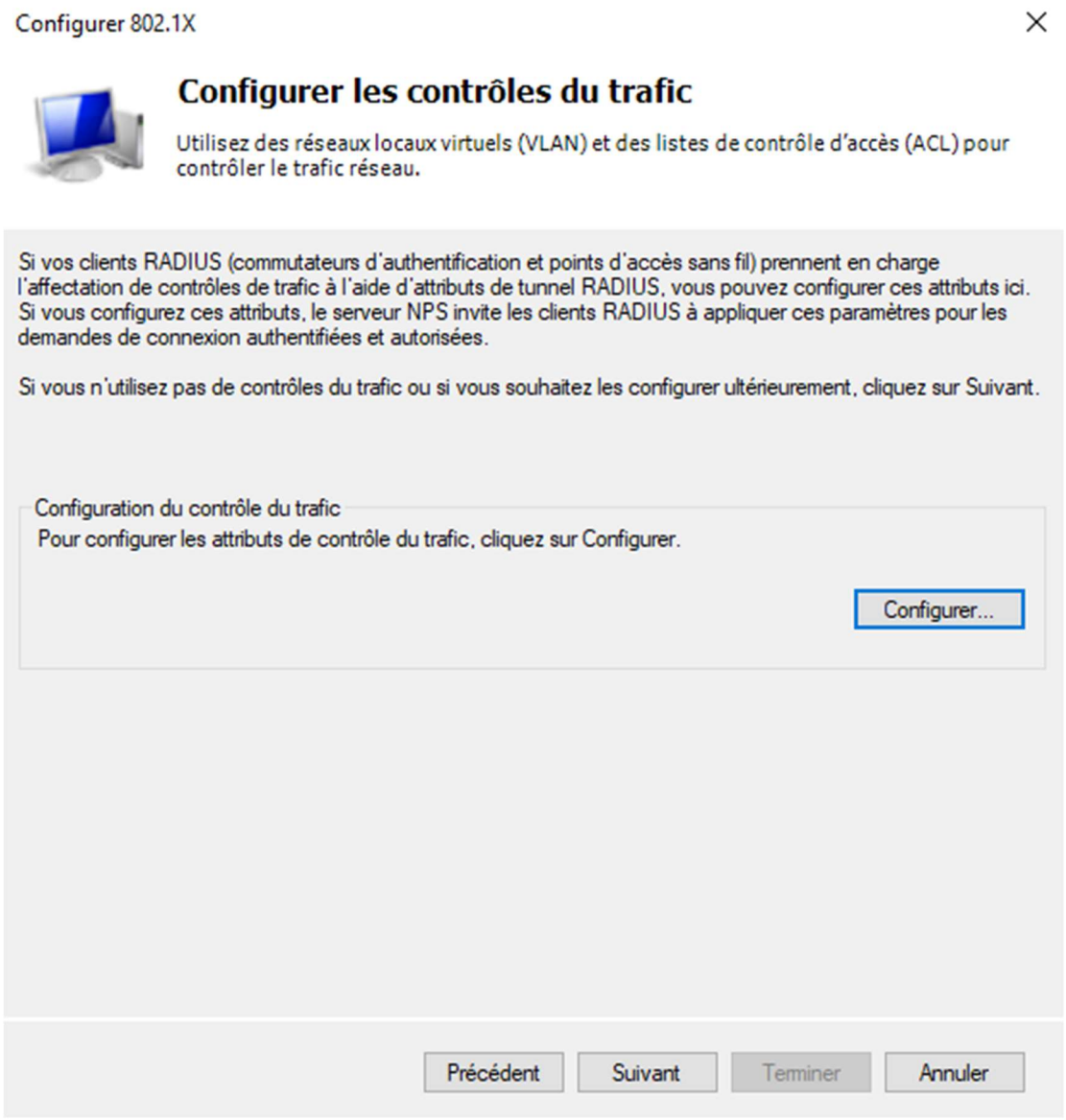

Configurer 802.1X
Spécifier les commutateurs 802.1X
Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)
Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.
Pour spécifier un client RADIUS, cliquez sur Ajouter.
Clients RADIUS :
Borne wifi
Ajouter...
Modifier...
Supprimer
Précédent
Suivant
Terminer
Annuler



Ajouter le groupe d'utilisateur ou d'ordinateur pouvant se connecter au réseau

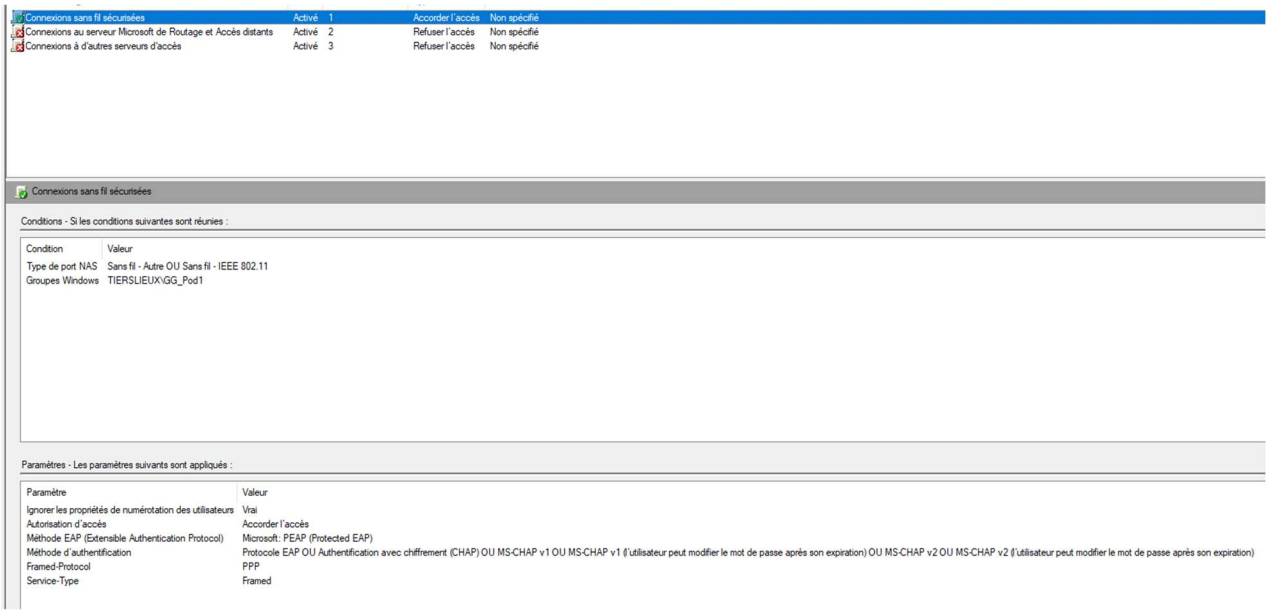


Configuration Optionnel



Puis cliquer sur terminer

Voici le résultat attendu



Pour faire l'association user vlan il faut rajouter ces trois paramètre

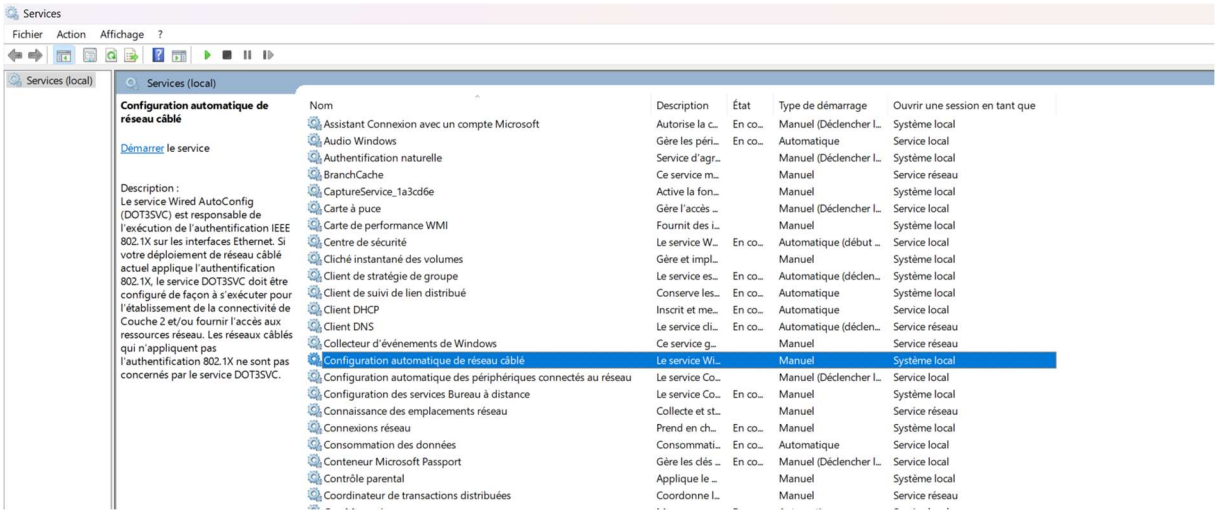
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Pvt-Group-ID	101
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...

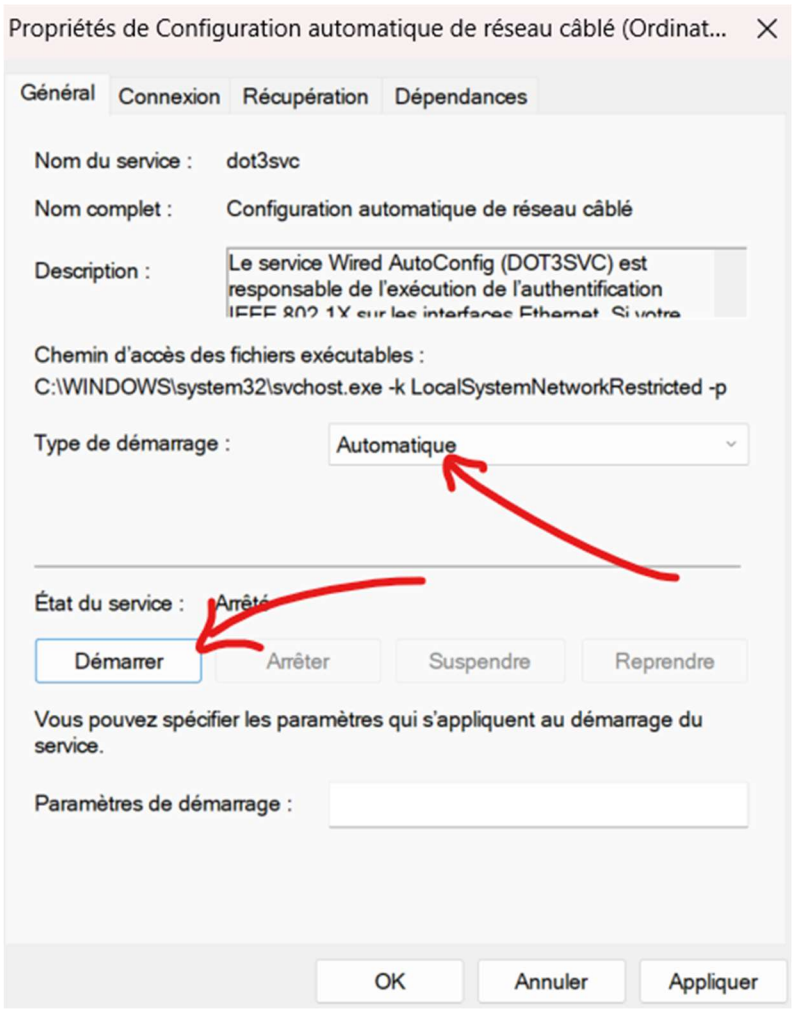
Pare-feu du serveur NPS

Rajouter 2 règles de pare-feu en trafics entrant

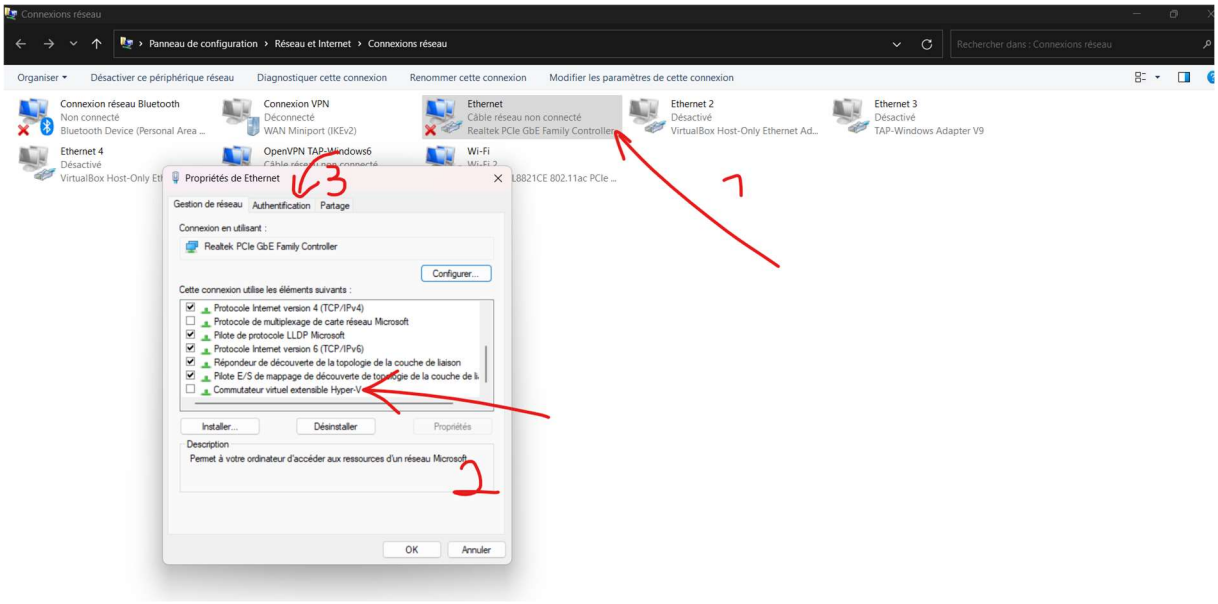
RADIUS	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	UDP	1812	Tout	Tout	Tout
RADIUS	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	UDP	1813	Tout	Tout	Tout

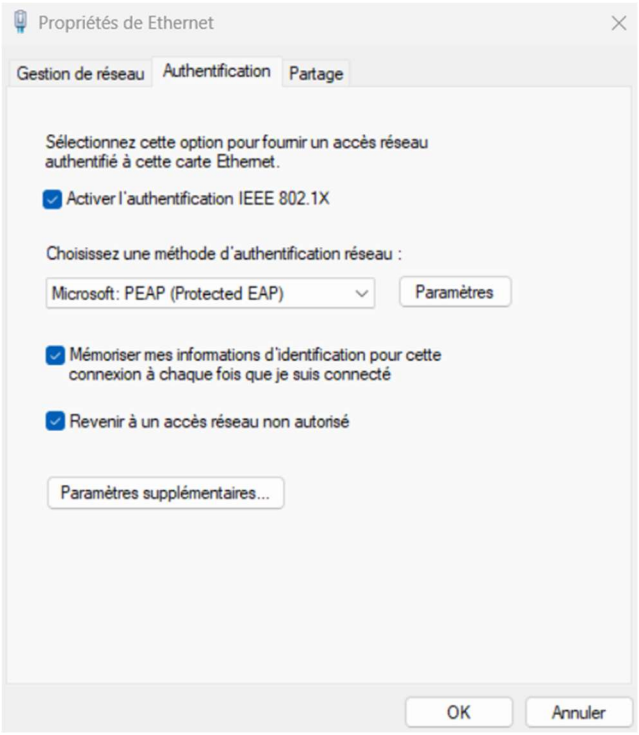
Configuration du client Windows



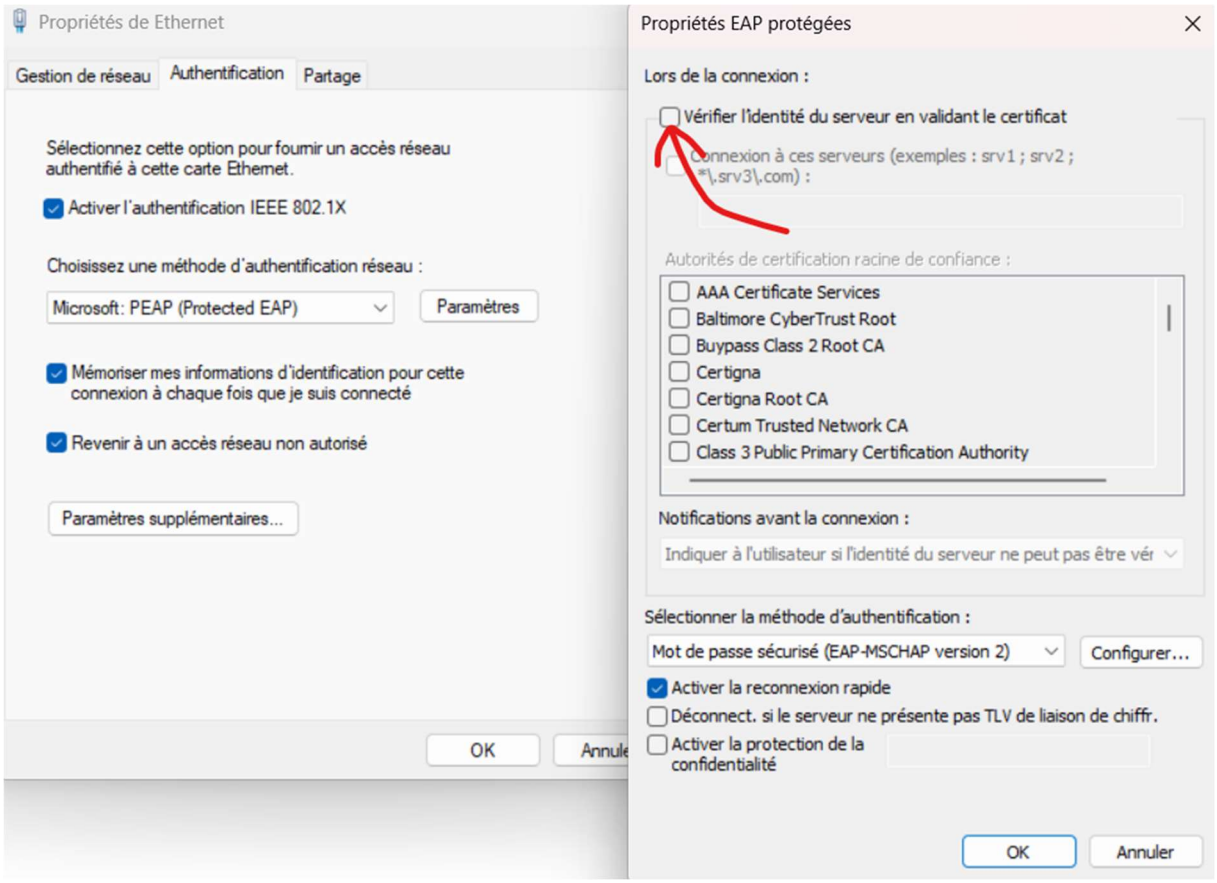


Dans les propriétés de la carte réseau désactivé « le commutateur virtuel extensible hyper-v »

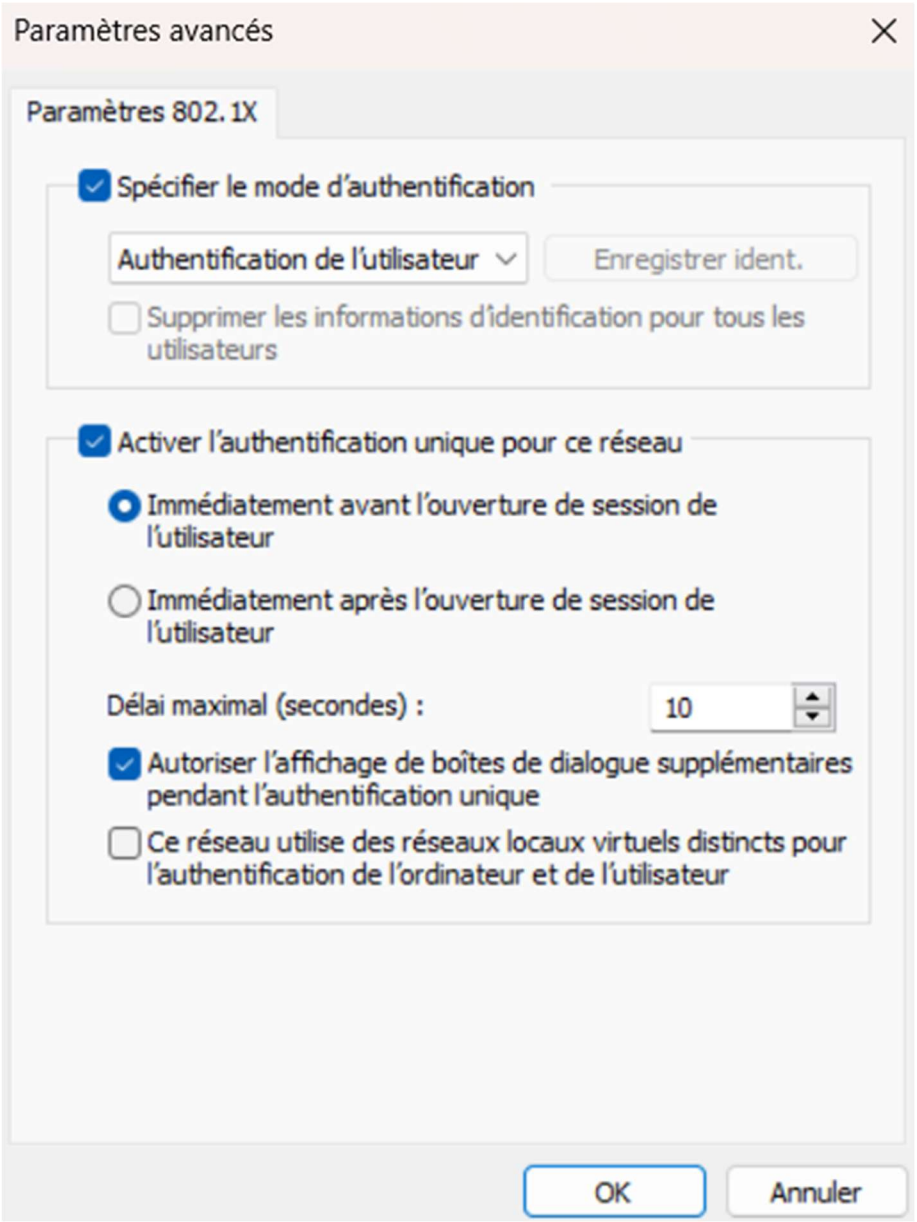




Désactivé la vérification de certificat



Et l'authentification avant l'ouverture de session


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

Configuration du switch

(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 172.16.0.1 auth-port 1812 acct-port 1813 key toto

(config)# interface f0/1

(config-if)#switchport mode access

(config-if)#authentication port-control auto

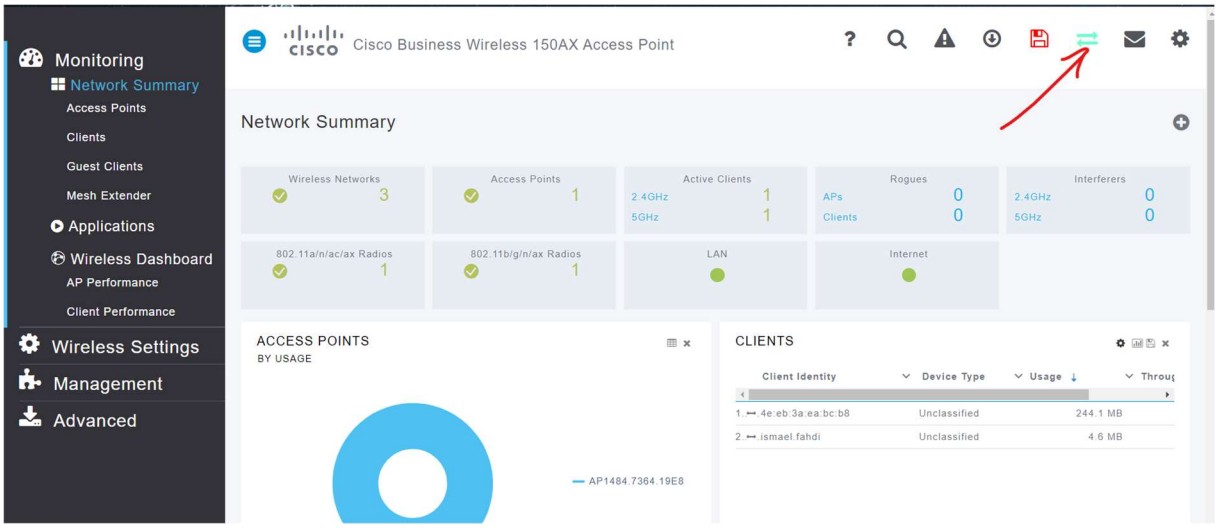
(config-if)#dot1x pae authenticator

(config-if)#authentication event no-response action authorize vlan 99

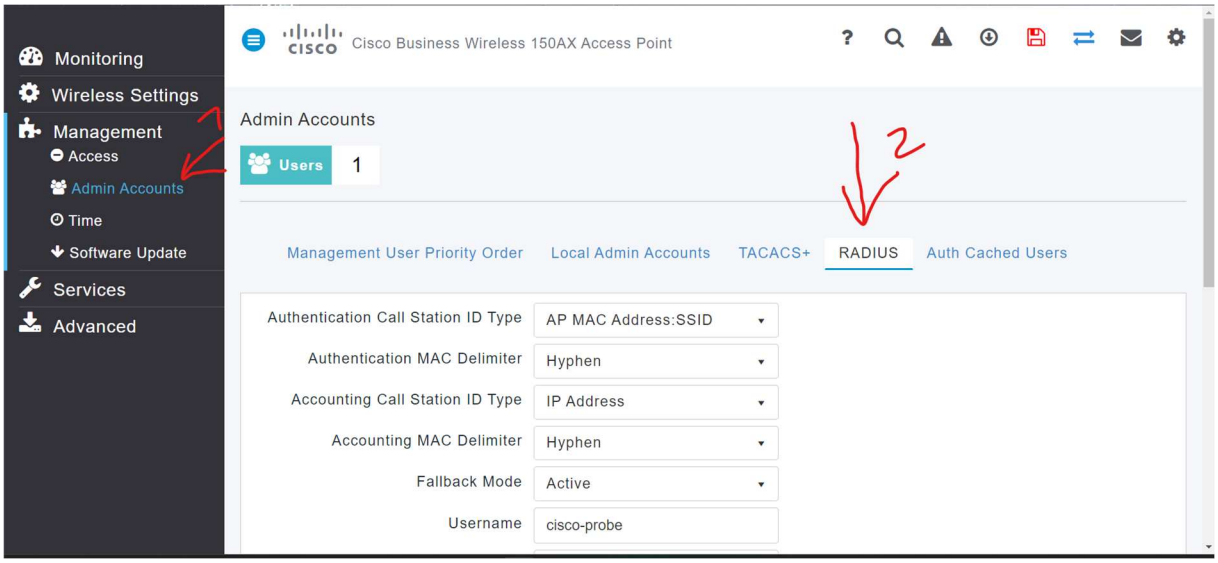
(config-if)#authentication event fail action authorize vlan 100

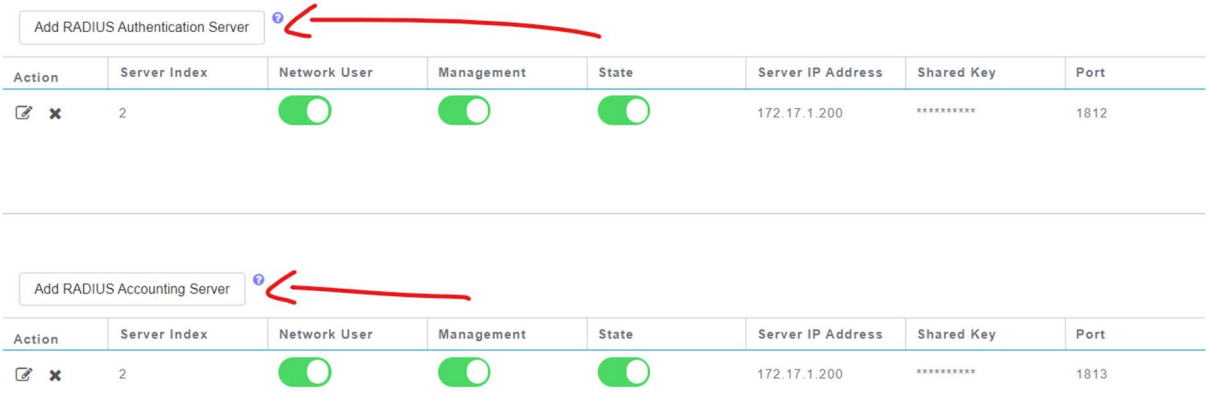
Configuration de la borne wifi

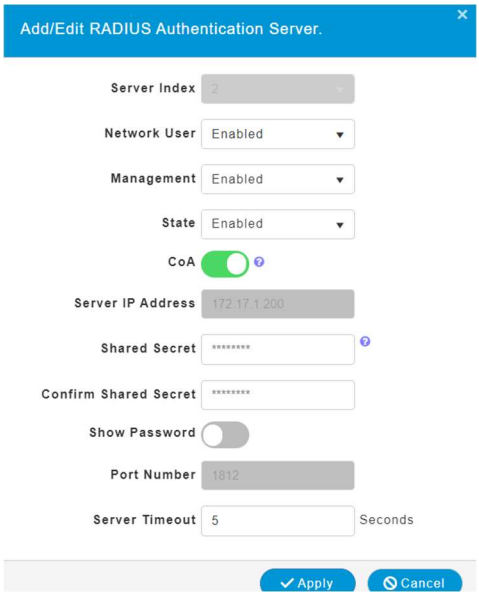
Il faut passer en mode expert



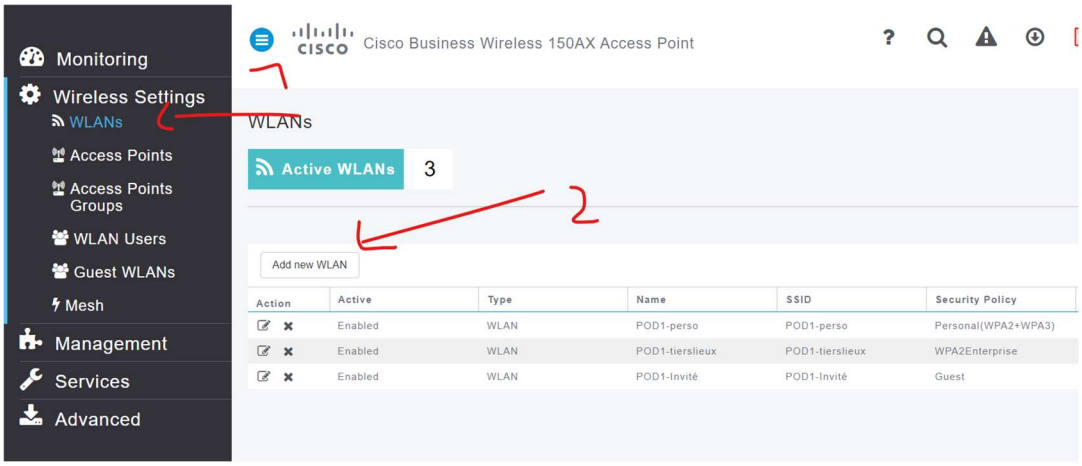
Ajouter l'ip du radius

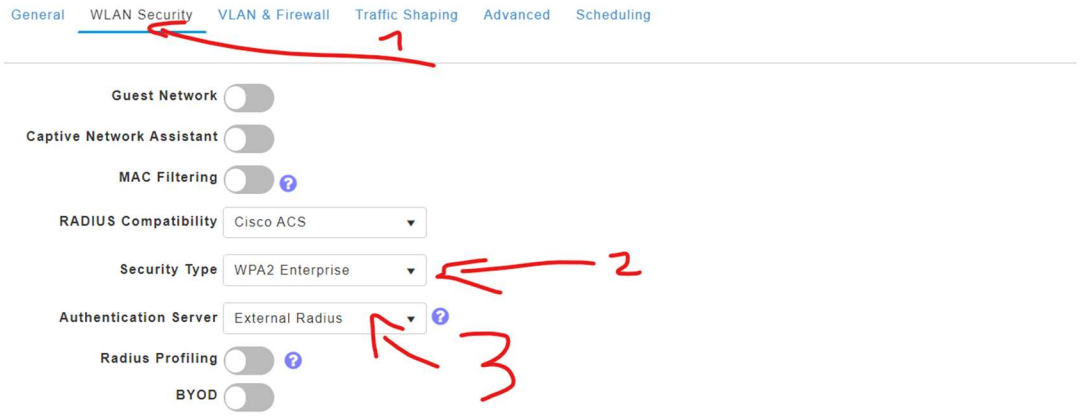






Relier le wifi avec le radius


Monitoring
Wireless Settings
WLANs
Access Points
Access Points Groups
WLAN Users
Guest WLANs
Mesh
Management
Services
Advanced
Cisco Business Wireless 150AX Access Point
WLANs
Active WLANs 3
Add new WLAN
Action
Active
Type
Name
SSID
Security Policy
Enabled
WLAN
POD1-perso
POD1-perso
Personal(WPA2+WPA3)
Enabled
WLAN
POD1-tierslieux
POD1-tierslieux
WPA2Enterprise
Enabled
WLAN
POD1-Invité
POD1-Invité
Guest
1
2


General
WLAN Security
VLAN & Firewall
Traffic Shaping
Advanced
Scheduling
Guest Network
Captive Network Assistant
MAC Filtering
RADIUS Compatibility
Cisco ACS
Security Type
WPA2 Enterprise
Authentication Server
External Radius
Radius Profiling
BYOD
1
2
3


RADIUS Server
Authentication Caching
Add RADIUS Authentication Server
Ac...
State
Server IP Address
Port
Enabled
172.17.1.200
1812
Add RADIUS Accounting Server
Ac...
State
Server IP Address
Port
Enabled
172.17.1.200
1813