Configuration Radius NPS pour l'authentification 802.1x via EAP-TLS

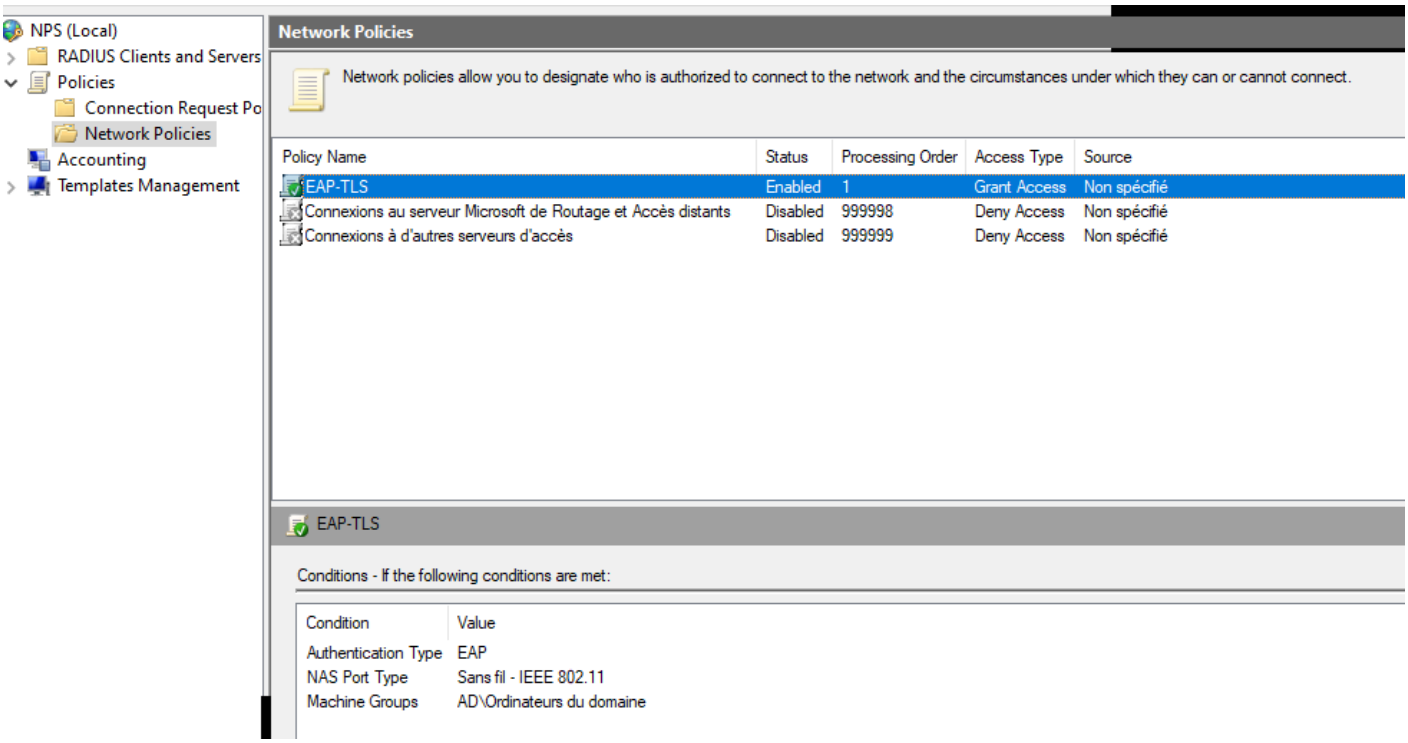
Cette documentation détaille la configuration du rôle NPS (Network Policy Server) sous Windows Server 2022 afin d'authentifier les utilisateurs ou ordinateurs au réseau Wifi. On peut également l'adapter pour la connexion filaire (non détaillée ici).

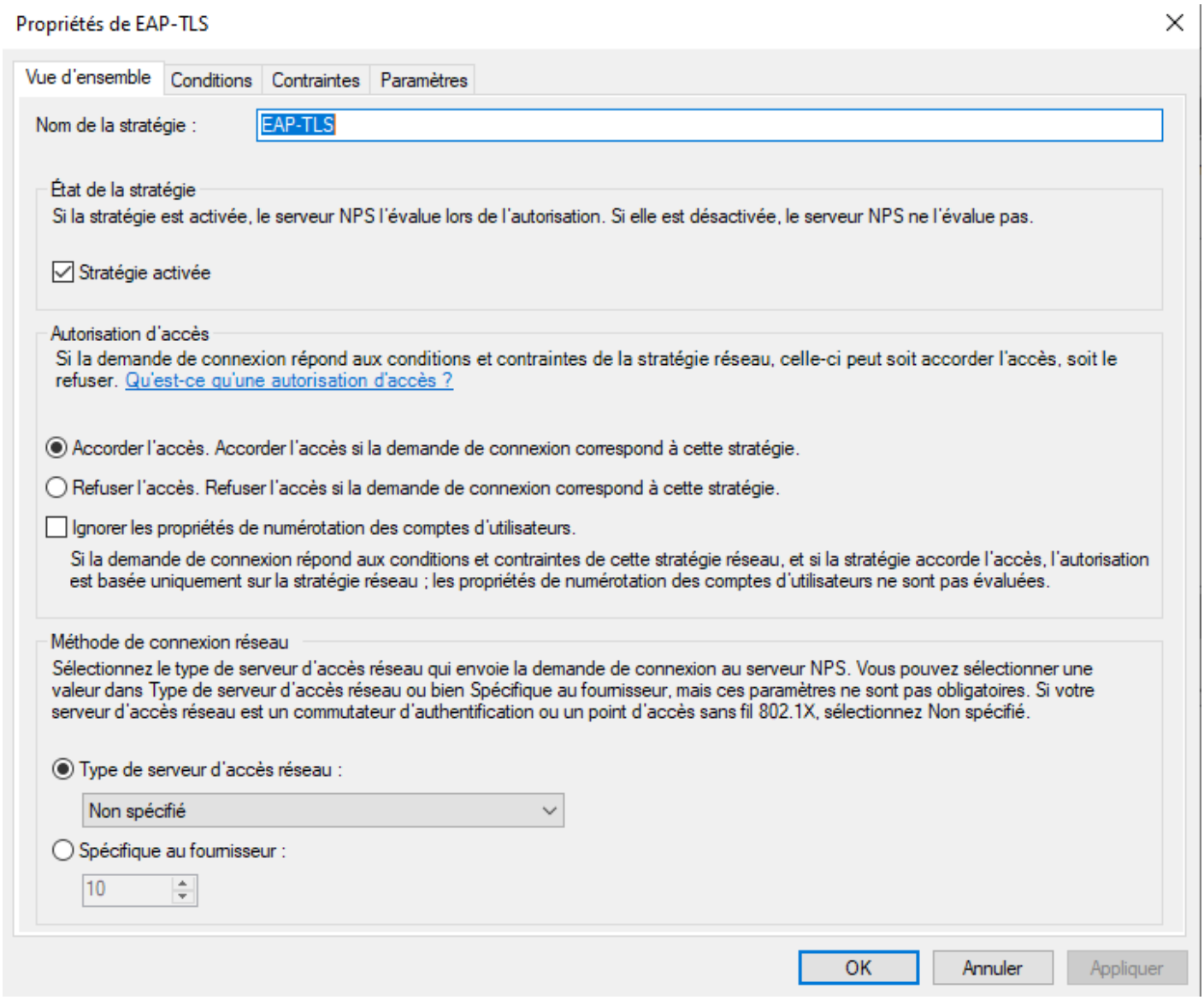
Parmi les méthodes d'authentification, le PEAP-TLS est la méthode la plus sécurisée, mais rarement supportée. De plus, elle chiffre la communication de la clé publique, qui n'a pas trop de sens.

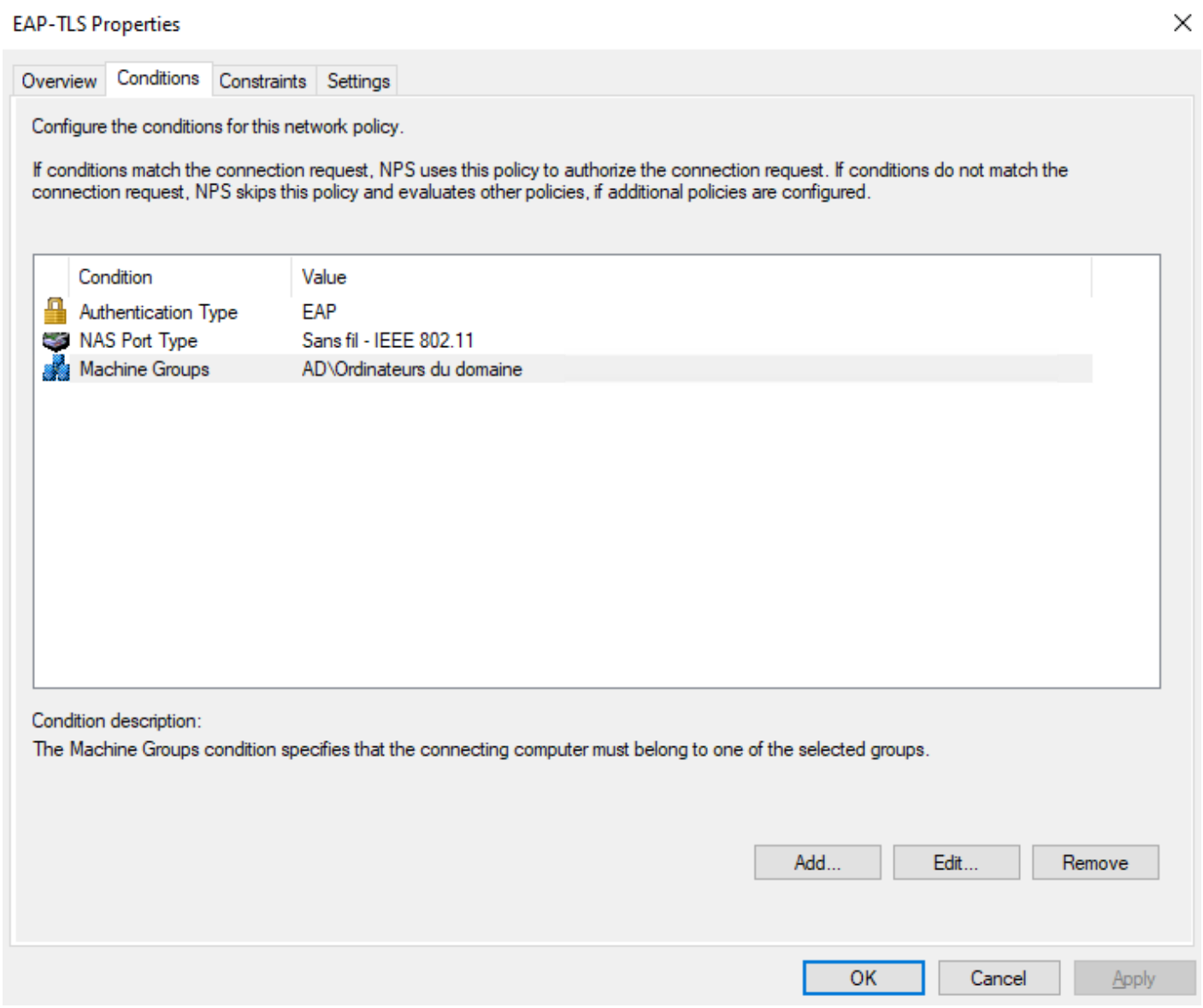
Authentication Methods	RADIUS NPS Server	Requirements for Client	Security Level
PAP	N/A	Username and Password	Least Safe
CHAP	N/A	Username and Password	Unsafe
MS-CHAP-v2	N/A	Username and Password	Unsafe
EAP-MS-CHAP-v2	N/A	Username and Password	Unsafe
PEAP-MSCHAP-v2	Computer Certificate	Username and Password	Safe
EAP-TLS	Computer Certificate	User Certificate	Safer
PEAP-TLS	Computer Certificate	User Certificate	The safest

Vous trouverez plus d'informations ici : Protocole EAP (Extensible Authentication Protocol) pour l’accès réseau dans Windows | Microsoft Learn

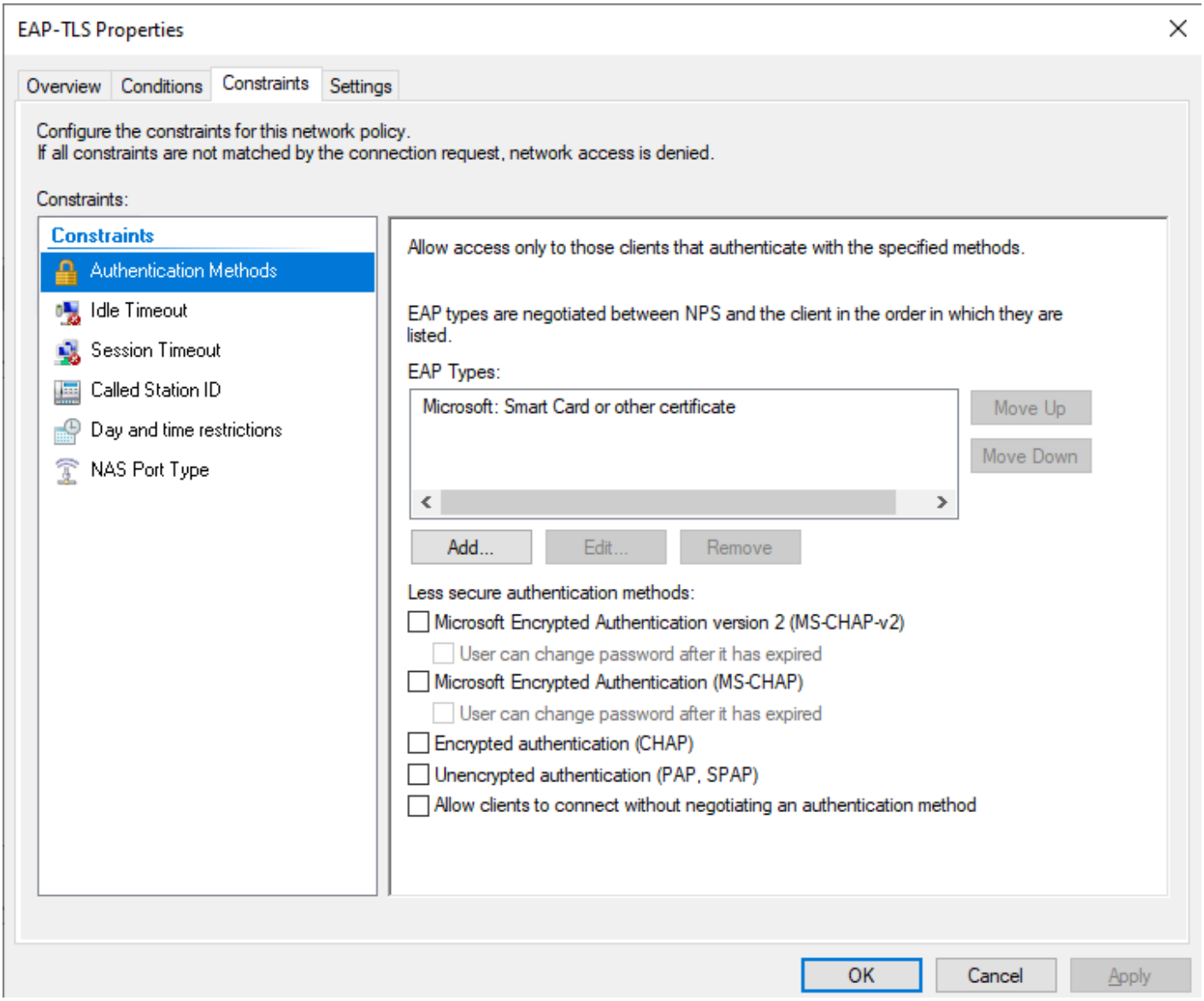
Après l'installation du rôle NPS, on définit la stratégie réseau comme ceci :


NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Source
EAP-TLS
Enabled
1
Grant Access
Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants
Disabled
999998
Deny Access
Non spécifié
Connexions à d'autres serveurs d'accès
Disabled
999999
Deny Access
Non spécifié
EAP-TLS
Conditions - If the following conditions are met:
Condition
Value
Authentication Type
EAP
NAS Port Type
Sans fil - IEEE 802.11
Machine Groups
AD\Ordinateurs du domaine

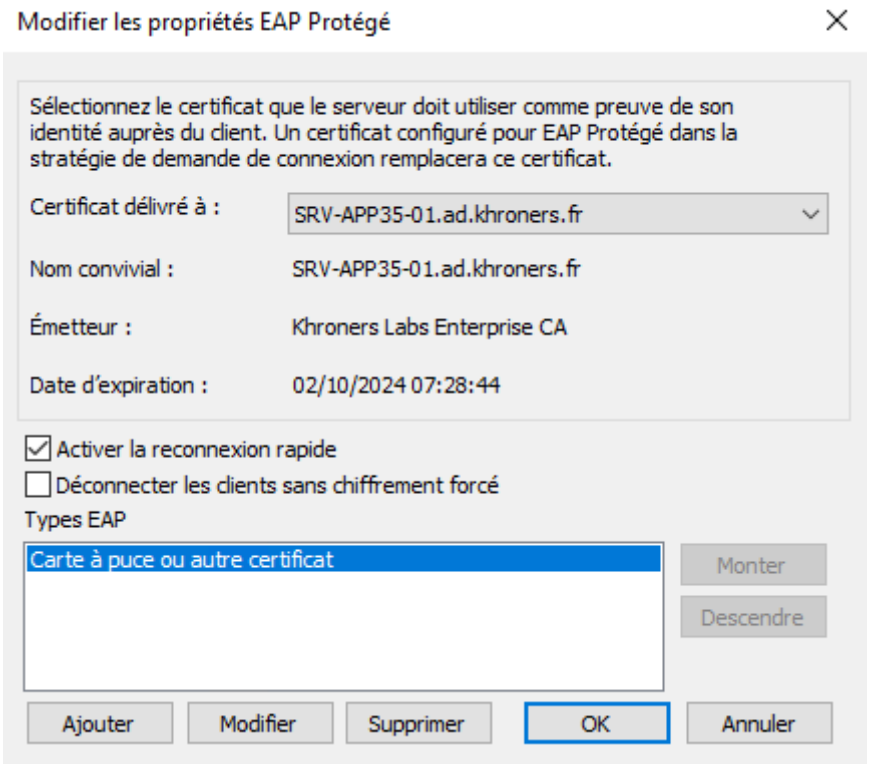

Propriétés de EAP-TLS
Vue d'ensemble
Conditions
Contraintes
Paramètres
Nom de la stratégie :
EAP-TLS
État de la stratégie
Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.
Stratégie activée
Autorisation d'accès
Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. Qu'est-ce qu'une autorisation d'accès ?
Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.
Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.
Ignorer les propriétés de numérotation des comptes d'utilisateurs.
Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.
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
OK
Annuler
Appliquer



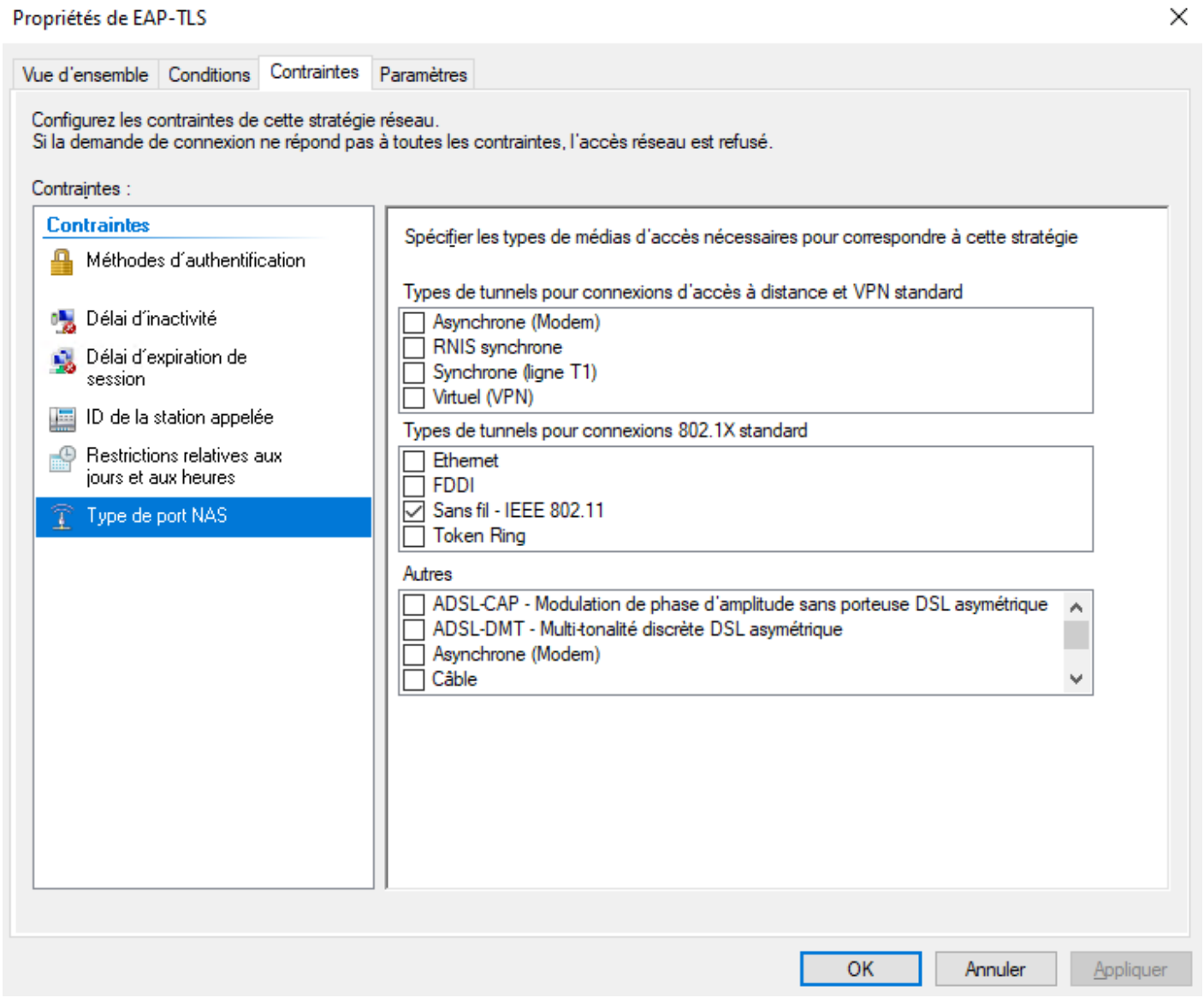
Le "TLS" de "EAP-TLS" correspond à "Microsoft: Smart Card or other certificate".



On clique sur "Microsoft: Smart Card or other certificate" et "Modifier..." :



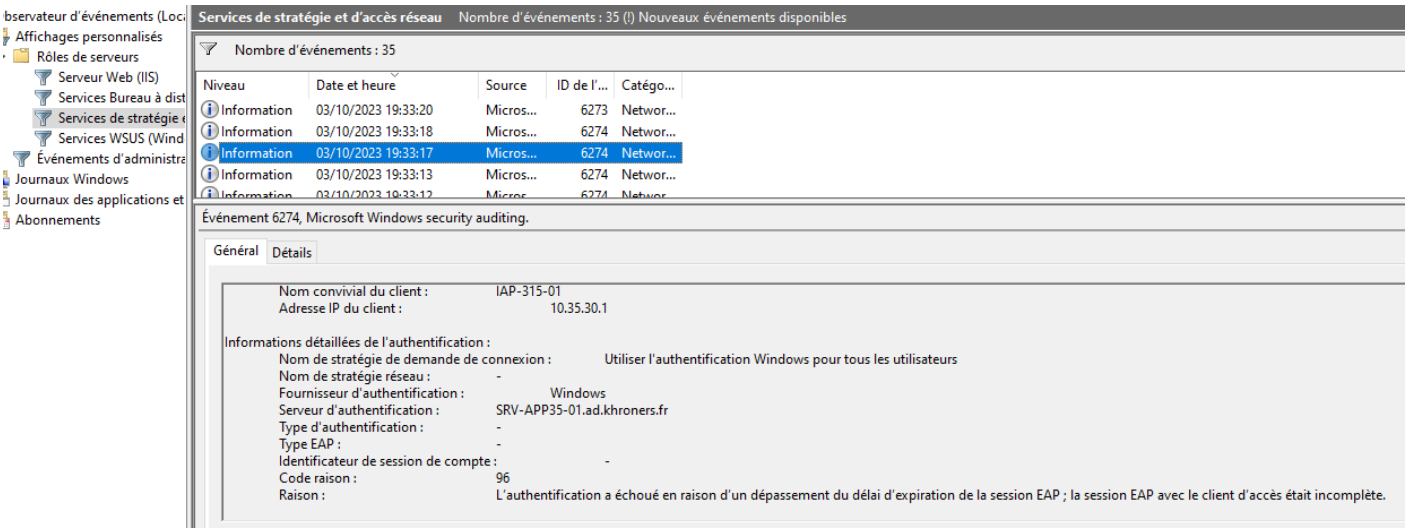
Cela correspond au PEAP-TLS (ou également dit PEAP-EAP-TLS).

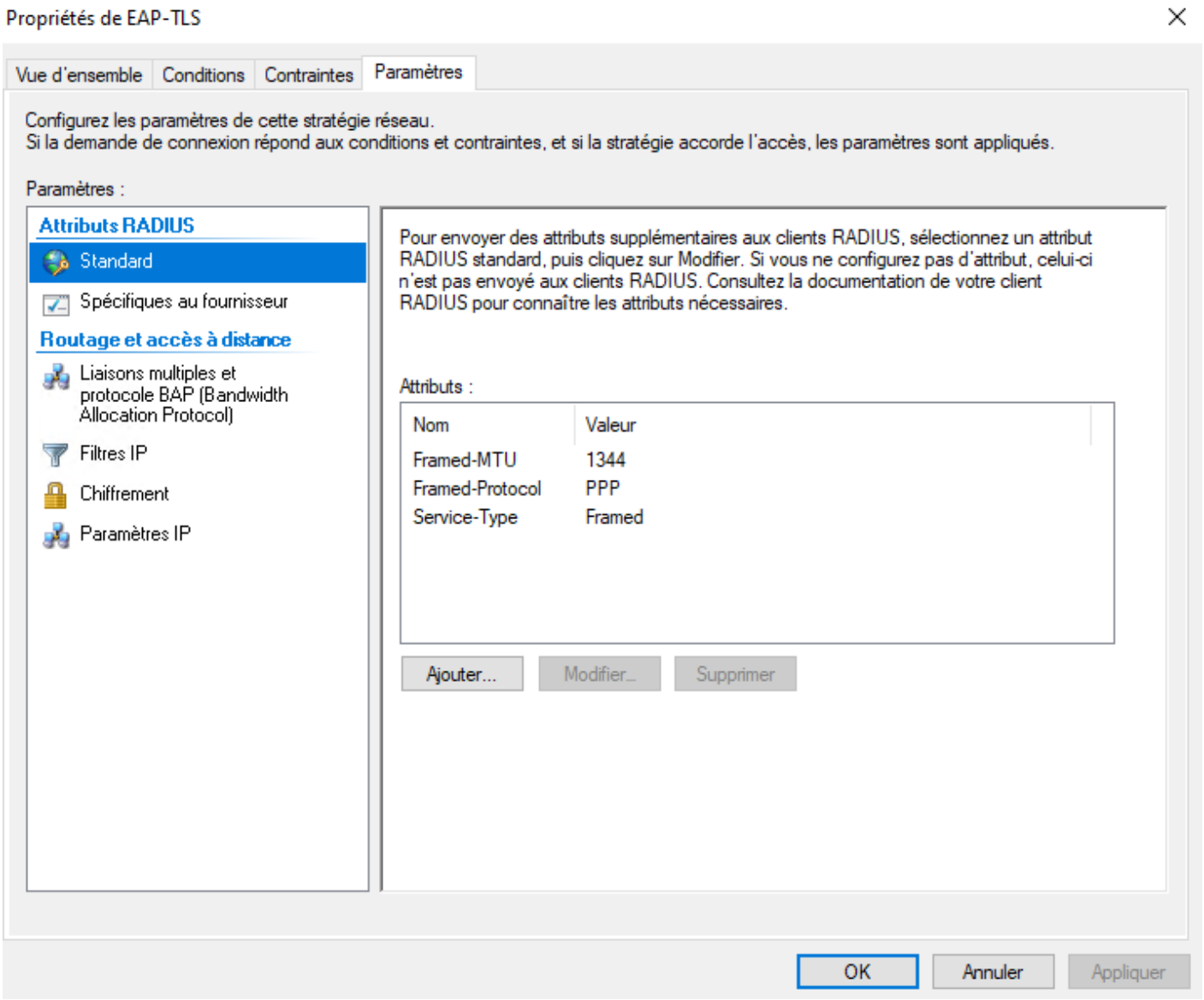


Dans mon cas, j'ai du ajouter l'attribut "Framed-MTU" avec une valeur de 1344, car j'ai l'erreur suivante :

> Authentication failed due to an EAP session timeout; the EAP session with the access client was incomplete.

Vous pouvez observer les logs dans l'observateur d'évènements, sous "Affichages Personnalisés" > "Rôles de serveurs" > Services de stratégie et d'accès réseau".





On ajoute également le(s) client(s) RADIUS en définissant un secret partagé.

Dans les bornes wifi, on choisit WPA2 Entreprise (ou WPA3 Entreprise si supporté), en renseignant l'adresse IP du serveur NPS et le secret partagé.

Revision #6
Created 5 October 2023 20:12:59 by Khroners
Updated 24 October 2023 20:31:17 by Khroners