Configurer Windows comme supplicant

Les systèmes d'exploitation Microsoft Windows disposent d'une couche **supplicante** logicielle 802.1x.

> Les distributions Linux disposent de paquetages comme **Xsupplicant**.

Dans Windows, il faut lancer le **service de configuration automatique de réseau câblé** pour activer cette couche logicielle.

Commentaire associé à ce service

Le service Wired AutoConfig (DOT3SVC) est responsable de l'exécution de l'authentification IEEE 802.1X sur les interfaces Ethernet. Si votre déploiement de réseau câblé actuel applique l'authentification 802.1X, le service DOT3SVC doit être configuré de façon à s'exécuter pour l'établissement de la connectivité de Couche 2 et/ou fournir l'accès aux ressources réseau. Les réseaux câblés qui n'appliquent pas l'authentification 802.1X ne sont pas concernés par le service DOT3SVC.

La mise en route du service provoque l'apparition de l'onglet [Authentification] dans les propriétés de la carte réseau.

Signification des coches

Revenir à un accès réseau non autorisé

On coche cette option si on veut que, dans le cas où le système du client final ne répondrait plus aux règles (de pare-feu, de mises à jour système, d'antivirus), sa connexion soit coupée. Ces règles d'acceptation font partie des exigences que l'on peut paramétrer dans le service RADIUS Microsoft NPS.

Mémoriser mes informations d'identification...

Mise en cache du couple identifiant/mot de passe. Cette mise en cache peut être intéressante pour une machine non intégrée dans un domaine, pour éviter de devoir se ré-authentifier.

Pour des **tests**, il est plus utile, pour observer ce qui se passe, de décocher cette option. Un poste intégré dans un domaine pourra utiliser les informations d'ouverture de session Windows pour l'authentification 802.1x. Ce ne sera pas demandé une seconde fois.

Le bouton [Paramètres] sur à côté du choix [Microsoft PEAP (Protected EAP], permet d'accéder à l'écran des propriétés EAP protégées :

Valider le certificat du serveur

Cette coche n'est pas utile pour les activités suivantes.

Dans la méthode d'authentification, nous utiliserons **EAP-MSCHAP version 2**.

> Le bouton [Configurer] permet d'indiquer si on veut utiliser ou non, le nom et le mot de passe d'ouverture de session Windows dans le dialogue 802.1x.

> Dans les phases de test, la relance du mécanisme d'authentification en désactivant/réactivant la carte réseau, mais tout le dialogue ne serait pas visible dans un analyseur de trames. Il vaut mieux décocher/cocher **Activer l'authentification 802.1X** pour observer tout ce qui se passe.

Retour Authentification 802.1x

- Authentification réseau avec le protocole 802.1x

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/reseau/802.1x/supplicantwindows?rev=1700423009

Last update: **2023/11/19 20:43**