Principes généraux de l'authentification 802.1x

Les acteurs

Trois acteurs interviennent dans la mise en oeuvre des protocoles 802.1x et Radius :

Le supplicant

C'est l'équipement de l'utilisateur, son PC, son téléphone IP, sa tablette ou son smartphone qui souhaite se connecter au réseau de l'organisation. C'est le **client final** de la demande de connexion. Pour cela :

- l'utilisateur s'identife
- auprès d'un poste de sécurité central,
- qui décide d'autoriser l'accès et des prérogatives à lui accorder aprsè son admission.

> Le **supplicant** est aussi appelé **client demandeur** ou **client final**.

L'équipement de réseau sur lequel le client final se connecte (commutateur ; borne Wifi compatible 802.1x) relaye, en tant que client RADIUS, cette demande de connexion à un serveur d'authentification RADIUS, qui va, par exemple, identifier la personne en rapprochant le nom de connexion et le mot de passe de ceux stockés dans un annuaire LDAP ou encore une base de données SQL.

Si l'identification réussit, l'accord est transmis au client RADIUS qui **ouvrira** alors le port de connexion.

Le serveur d'authentification

> Le **serveur d'authentification** est aussi appelé **serveur d'identification**.

Le client Radius

C'est un équipement réseau (commutateur, borne wifi, ...) qui est central dans la connexion 802.1x et qui doit gérer le protocole 802.1x et le protocole d'authentification EAP.

> Le **client RADIUS** est aussi appelé **Authenticator** ou **NAS** (Network Access Server) ou encore **contrôleur d'accès**.

Le protocole 802.1x

Le protocole 802.1x est une solution standard de sécurisation de réseaux mise au point par l'IEEE en 2001. 802.1x permet d'authentifier un utilisateur souhaitant accéder à un réseau (câblé ou Wifi) grâce à un serveur central d'authentification.

L'autre nom de 802.1x est **Port-based Network Access Control** ou **User Based Access Control**.

802.1x permet de **sécuriser** l'accès à la **couche 2** (liaison de donnée) du réseau. Ainsi, tout utilisateur, qu'il soit interne ou non à l'entreprise, est dans l'obligation de s’authentifier avant de pouvoir faire quoi que soit sur le réseau. Certains équipements de réseau compatibles 802.1x peuvent réserver un traitement particulier aux utilisateurs non authentifiés, comme le placement dans un VLAN **guest**, une sorte de quarantaine sans danger pour le reste du réseau.

802.1x a recours au **protocole EAP** (Extensible Authentification Protocol) qui constitue un support universel permettant le transport de différentes méthodes d'authentification qu'on retrouve dans les réseaux câblés ou sans-fil.

802.1x nécessite donc la présence d'un **serveur d'authentification** qui peut être un **serveur RADIUS** (serveur Microsoft NPS - Network Policy Server ; Cisco ; un produit libre comme FreeRADIUS) ou encore un serveur **TACACS** dans le monde fermé des équipements Cisco.

Un port d'un commutateur réglé en mode 802.1x peut se trouver dans deux états distincts :

- État **contrôlé** si l'authentification auprès du serveur RADIUS a **réussi**.
- État **non contrôlé** si l'authentification a échoué.

La réussite ou l'échec de l'authentification va donc ouvrir ou fermer le port à toute communication.

Un port ouvert va, par exemple, permettre au client final d'obtenir une adresse IP auprès d'un serveur DHCP.

Dans des implémentations plus cloisonnées, le serveur RADIUS indiquera par exemple au client RADIUS dans quel VLAN placer le client final.

RADIUS

RADIUS (acronyme de Remote Authentication Dial-In User Service) est un **protocole client-serveur** permettant de centraliser des demandes d'authentification relayées par des équipements de réseau, comme des commutateurs ou bornes Wifi, considérés alors comme ses clients.

Par extension, un serveur qui centralise des demandes d'authentification et les soumet à un service d'annuaire LDAP ou à un service de base de données SQL est appelé serveur RADIUS.

RADIUS interroge une base de données d'authentification et d'autorisation qui peut être un domaine Active Directory, une base LDAP ou une base de données SQL. Ces bases ou annuaires peuvent se trouver sur le serveur lui-même ou sur un serveur tiers. Certaines implémentations de RADIUS disposent d'une base de données en propre.

A l'origine, RADIUS était surtout utilisé pour l'identification des clients des FAI, ses capacités de comptabilisation des accès (accounting) permettant notamment la journalisation des accès et leur facturation. RADIUS a été utilisé par la suite en entreprise pour l'identification des clients finals WIFI et pour l'identification des clients finals câblés.

Rôles du serveur RADIUS

1. Authentification

Le serveur RADIUS

- doit authentifier les requêtes qui sont issues des clients finals,
- via les clients RADIUS.

Base de l'authentification selon le protocole d'authentification négocié avec le client final :

- soit un couple identifiant/mot de passe,
- soit un certificat. Cela dépendra du protocole d'authentification négocié avec le client final.

2. Autorisation

Le serveur RADIUS décide quoi faire du client authentifié en délivrant une autorisation.

Pour cela, le serveur RADIUS envoie des informations (**attributs**) aux clients RADIUS comme par exemple le numéro du VLAN dans lequel placer le client authentifié.

3. Comptabilisation

Le serveur RADIUS comptabilise/journalise plusieurs données liées à la connexion : date et l'heure ; adresse MAC de l'adaptateur réseau du client final ; le numéro de VLAN, etc.

C'est son rôle comptable ou **d'accounting**.

Le serveur RADIUS se range dans le modèle AAA (Authentication, Authorization, Accounting).

RADIUS peut aussi servir à centraliser les accès sécurisés aux pages ou aux terminaux de paramétrage de tous les équipements réseau : commutateurs, routeurs, bornes wifi, contrôleurs wifi, etc.

Retour Authentification 802.1x

- Authentification réseau avec le protocole 802.1x