[SCOM] TEMA 2: Port-Based Network Access Control: PBNAC en IEEE 802 Local Area Networks

IEEE 802.1x

Los puertos están bloqueados por defecto, bloqueando el tráfico normal (EAP puede pasar), hasta que el usuario se autentique con unas credenciales válidas. Hay un intermediario (Autenticador) que se encarga de revisar las credenciales contra un servidor de autenticación (Radius, por ejemplo).

IEEE 802.1x y EAP

Es un protocolo que define un mecanismo de transporte de credenciales (Extensible Authentication Protocol) entre el usuario (suplicante) y el servidor de autenticación. Este protocolo es el único que puede atravessar puertos bloqueados. EAP se tiene que apoyar en otro tipo de portocolos ya que solo define la infraestructura para el transporte de credenciales, pero no las mueve. Los protocolos más usados para la transmisión de credenciales suelen ser:

- 802.1x (Wifi y Ethernet)
- Radius: Remote Access Dial-In User Service (Del autenticador al server de autenticación)
    - Su funcionamiento se basa en el secreto compartido, lo que lo hace no muy seguro.
    - También permiten la autorización y el accounting (Triple A, Autorización, Autenticación y Acounting)
- Tacans (Del autenticador al server de autenticación)
- Diameter (Del autenticador al server de autenticación)

Hay que distinguir el protocolo de transporte, el protocolo EAP y los credenciales, son cosas diferentes. Normalmente el intermediario solicita la identidar al usuario (suplicante), saca el paquete EAP del 802.1X y se lo pasa al server de autenticación