Sécurisation des accès Wifi par serveur RADIUS

Microsoft NPS

Ershad Ramezani

Table des matières

Introduction

La demande : un serveur RADIUS

Ce projet demande la mise en place d'un serveur RADIUS dans notre réseau. La description de l'architecture du réseau est les suivantes :

- 2 vlans *formation* et *administratif*.
- Un point d'accès Wifi supportant le système d'authentification basé sur RADIUS.
- Un serveur RADIUS
- Un serveur DHCP avec une étendue par VLAN

L'objectif est de :

- Configurer les accès Wifi avec authentification des utilisateurs par leurs comptes utilisateur sur le serveur RADIUS.
- Le SSID Personnel est masqué pour le réserver au seul personnel administratif
- Une fois connecté chaque utilisateur se voit attribué une adresse IP en fonction du SSID de connexion.

Tous d'abord on commence par regarder quelques définitions sur le RADIUS :

RADIUS : qu'est-ce que c'est ?

RADIUS est l'acronyme de *Remote Access Dial In User Service*. RADIUS fait partie d'une solution AAA. La prise en charge du protocole et des normes RADIUS est devenue l'exigence pour les fournisseurs de NAS. Point d'accès Wi-Fi avec WPA2 ou un switch avec IEEE 802.1x (EAP) sont référé comme un **Network Access Server** (NAS). Le protocole RADIUS est un protocole client/serveur qui utilise UDP pour communiquer.

RADIUS est utilisé par divers appareils qui contrôlent l'accès aux réseaux TCP/IP. Voici quelques exemples :

- Un pare-feu avec service VPN peut utiliser RADIUS.
- Les points d'accès Wi-Fi avec cryptage WPA-2-Enterprise peut utiliser RADIUS.

AAA (Authentication, Authorization, and Accounting):

Tous ces dispositifs ont besoin d'exercer quelques formes de contrôle afin d'assurer la sécurité. Cette exigence est appelée **Authentication, Authorization, and Accounting** (AAA). AAA est aussi parfois appelé le Triple A Framework.

Authentification

L'authentification est généralement la première étape pour accéder à un réseau. Il s'agit d'un processus permettant de confirmer si les informations d'identification fournies par un utilisateur sont valides. Le moyen le plus courant de fournir des informations d'identification consiste à utiliser un nom d'utilisateur et un mot de passe.

Autorisation

Autorisation est un moyen par qui le NAS contrôle l'usage de la Ressources. Après que l'utilisateur s'est authentifié, NAS peut imposer certains restrictions ou accorder certains privilèges.

Gestion (Accounting)

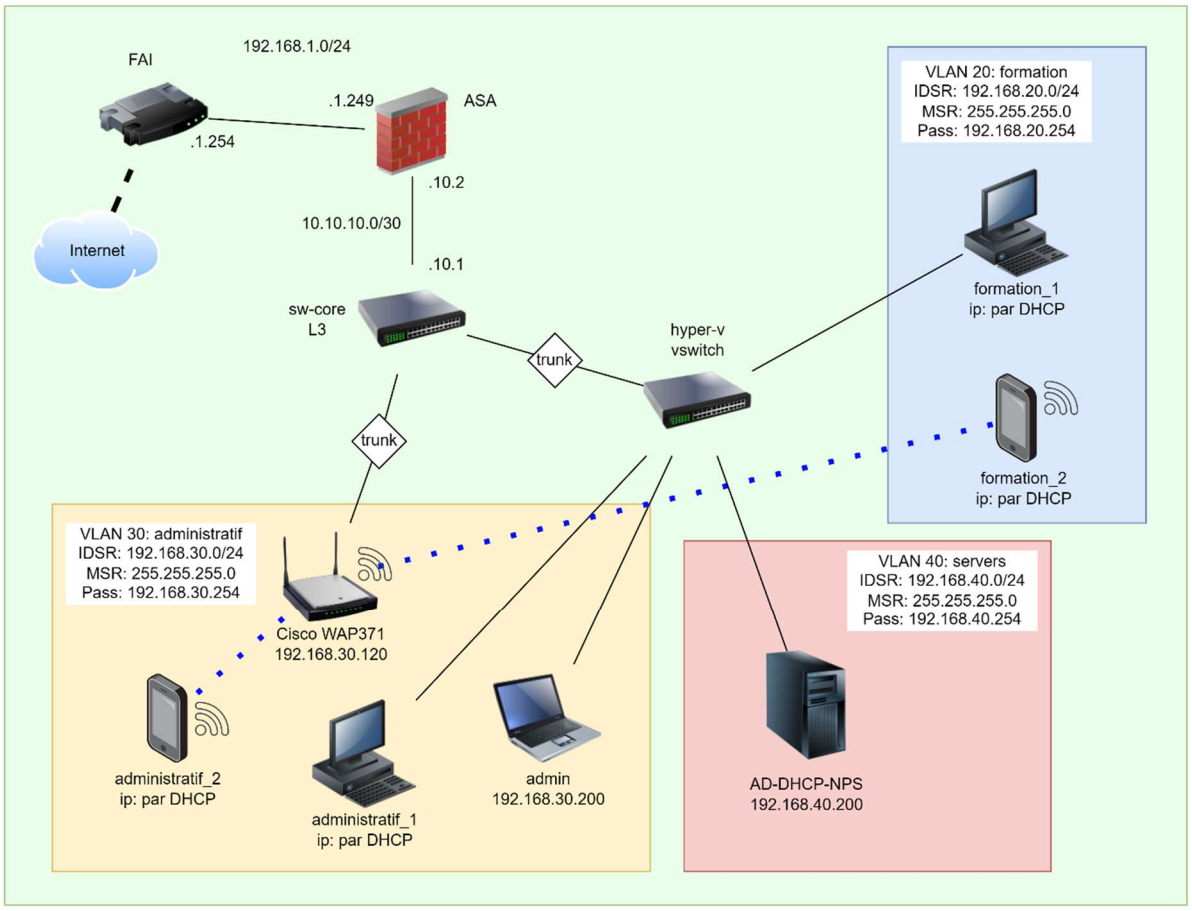
C'est un moyen de mesurer l'utilisation des ressources. Une fois que le réseau ou le NAS a établi qui est l'utilisateur et imposé un contrôle approprié sur la session établie, il peut également mesurer son utilisation.

La solution : Network Policy Server (NPS)

Network Policy Server (NPS) est l'implémentation Microsoft d'un serveur RADIUS. À l'aide de NPS, vous pouvez configurer et gérer de manière centralisée l'authentification d'accès au réseau, fournir une autorisation pour les demandes de connexion et comptabiliser les journaux d'informations.

Dans un premier temps, on va mettre en place l'architecture du réseau. Ensuite on mettra en place le serveur NPS.

Schéma



Explication sur le réseau mis en place

Avant commencer la mise en place du serveur RADIUS, je donne une explication sur la façon notre réseau est construit :

Sous-réseaux et VLANs

5 sous-réseaux sont créés. Trois sous-réseaux pour trois VLANs *formation*, *administratif* et *serveurs*. Un sous-réseau entre le *switch cœur* et le *routeur*. Le dernier sera pour le réseau entre le routeur et le routeur de FAI.

VLAN ID	VLAN name	Description	IDSR	MSR	Passerelle
20	formation	-	192.168.20.0/24	255.255.255.0	192.168.20.254
30	administratif	-	192.168.30.0/24	255.255.255.0	192.168.30.254
40	servers	-	192.168.40.0/24	255.255.255.0	192.168.40.254
50	firewall	-	10.10.10.0/30	255.255.255.252	-
-	-	-	192.168.1.0/24	255.255.255.0	-

Configuration de v-Switch sur Hyper-V

A part du switch L3 et le routeur, tous nos machines sont virtuelles et installées sur le Hyper-V. Le commutateur virtuel de Hyper-V nous permet de mettre nos machines dans des vlans différents. Voici comment il est configuré sur le Hyper-V :

La version complète est disponible aussi mais protéger par un mot de passe.

Merci de me contacter par email :

Ershad.ra@gmail.com