EXTRAIT DE RAPPORT DE STAGE · MALO LE FOLL

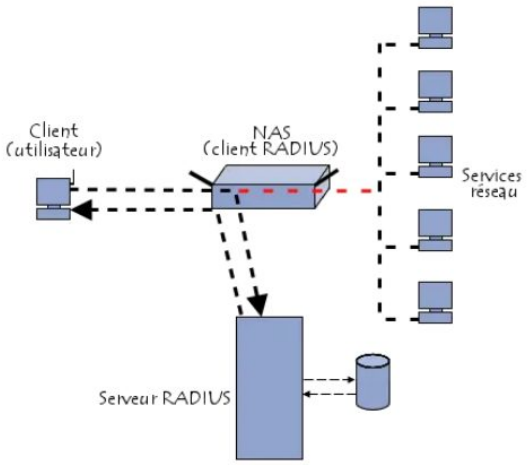
Authentification Wi-Fi 802.1X avec un serveur RADIUS

École des Beaux-Arts de Nantes Saint-Nazaire
Stage administrateur réseau · 6 janvier – 14 février 2025

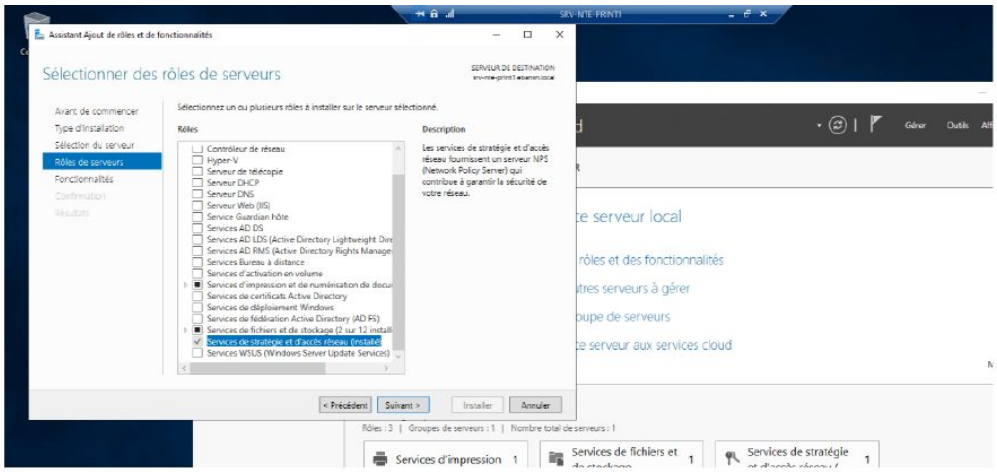
Objectif : remplacer la clé WPA du Wi-Fi étudiant par une connexion avec le compte Active Directory (WPA2-Enterprise), via le rôle NPS de Windows Server 2019, le contrôleur Wi-Fi Cisco et l'authentification 802.1X sur les switchs.

Extrait d'une activité du rapport. Les informations internes (adresses IP, clés, noms) sont masquées.

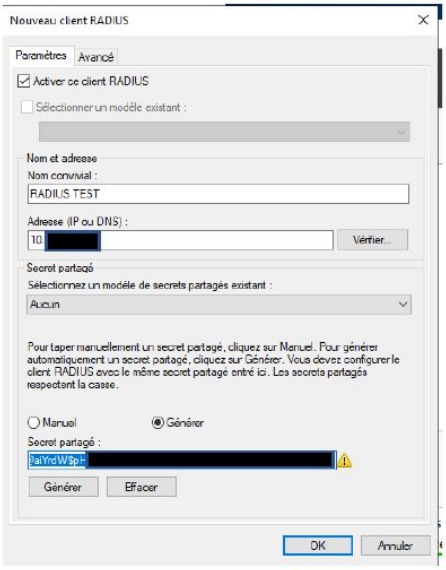
Pour cette activité, j'étais complètement en autonomie. Le but de cette activité était de mettre en place un serveur RADIUS lié au WIFI étudiant, pour supprimer les clés WPA et se connecter uniquement au WIFI grâce à un compte AD. La mise en place de ce système permettrait de renforcer la sécurité du réseau. Mon tuteur avait déjà commencé, avec un autre stagiaire, la mise en place de ce système, mais sans aboutir. J'ai donc recommencé sur un nouveau wifi créé pour le test. L'étape 1 pour commencer, était de lire beaucoup de documentation sur, par exemple, comment créer un serveur NPS (Network Policy and Access services) ou aussi comprendre et mettre en place un serveur Radius. RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification.
Le fonctionnement de RADIUS ressemble dans notre cas à celui-ci (schéma ci-dessous) :
Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
Le NAS achemine la demande au serveur RADIUS ;
Le serveur RADIUS consulte la base de données, dans notre cas, il consulte l'Active Directory et l'utilisateur est autorisé ou non à accéder au wifi.



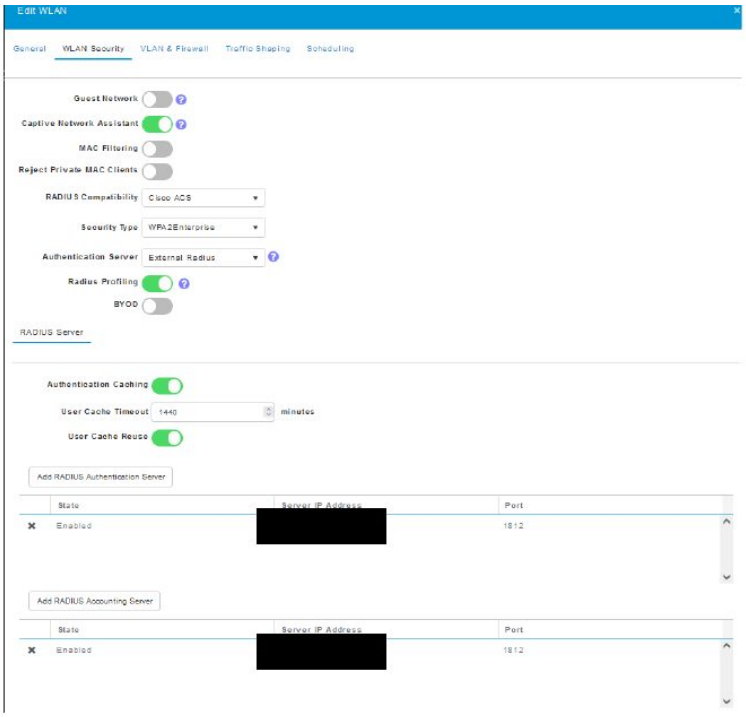
Après avoir lu et compris le fonctionnement du serveur, je suis passé à l'étape 2, qui est l'installation du serveur avec Windows serveur 2019. Pour commencer, il me fallait un serveur Windows, j'ai donc utilisé le serveur d'impression (Print1) qui m'a servi de test, car mon tuteur m'a dit que c'était le serveur le moins sensible pour un test. Pour commencer l'installation, je me suis connecté avec le bureau à distance sur le serveur PRINT1. Ensuite, depuis le gestionnaire de serveur, j'ai ajouté des rôles et des fonctionnalités. L'installation est simple, mais la fonctionnalité importante à ajouter est « Services de stratégie et d'accès au réseau ».



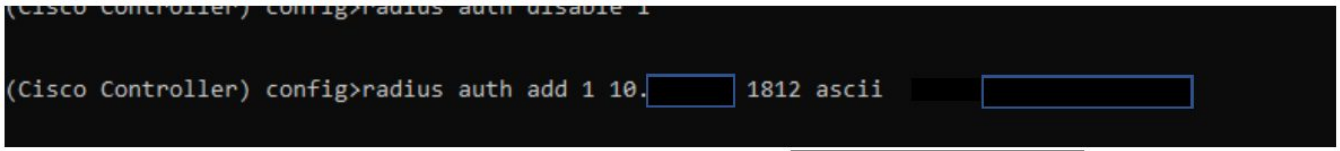
Après avoir ajouté la fonctionnalité, on a donc installé le serveur NPS qui permet de configurer les clients RADIUS. Il faut ouvrir le serveur NPS et grâce à cette fenêtre (voir annexe 2), on a accès au paramétrage du serveur RADIUS. Pour commencer, j'ai d'abord ajouté un client RADIUS qui correspond, dans notre cas, au contrôleur de WIFI Cisco.



J'ai renseigné un secret partagé, ce qui sera demandé par la suite pour connecter mon serveur aux autres appareils. J'ai ensuite fait la configuration de la connexion sans fil 802.1X. Donc, dans un premier temps, on coche "connexion sans fil sécurisée" puis on sélectionne un commutateur par lequel notre requête va passer et ensuite, on l'ajoute dans un groupe.
Donc, pour ajouter l'utilisateur dans un groupe, il faut aller sur l'AD et créer un groupe, dans lequel on va mettre seulement les utilisateurs autorisés à se connecter au réseau WIFI. Donc, une fois le groupe créé, j'ajoute mon compte à ce groupe, pour pouvoir effectuer des futurs tests. Après cela, la connexion sans fil est paramétrée. Je suis donc passé à la configuration du contrôleur WIFI Cisco.



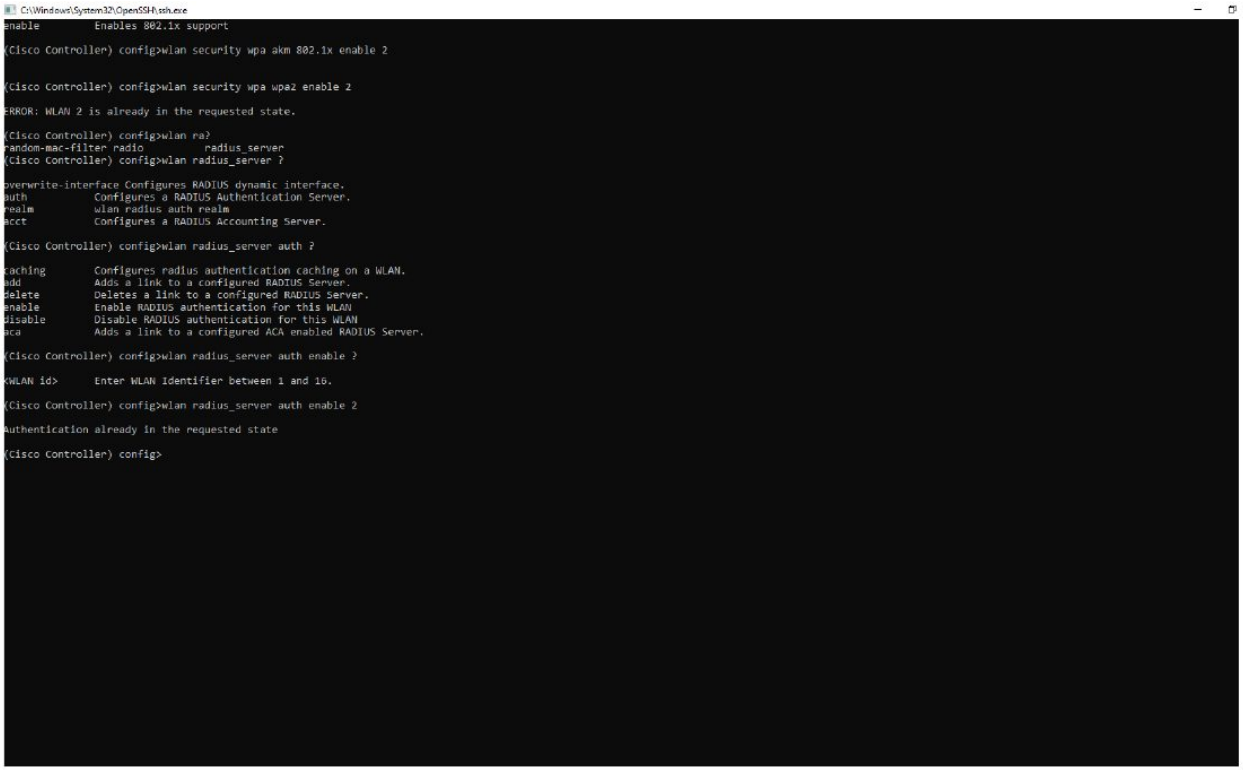
Cette partie a été plus simple, car il m'a suffi de sélectionner dans «security type» «WPA2Entreprise» et j'ai eu accès au paramètre du serveur RADIUS, où j'ai ajouté dans « Authentification server », mon serveur RADIUS. Sauf que je ne pouvais pas ajouter le « server Accounting », donc j'ai dû me connecter en ssh au contrôleur de WIFI, pour avoir plus d'accès sur la configuration globale.
D'abord, j'ai ajouté le serveur radius.



(Cisco Controller) config>radius auth add 1 10.X.X.X 1812 ascii [redacted]

radius auth add 1 : cette commande ajoute un nouveau serveur RADIUS. Le chiffre 1 indique que c'est le serveur numéro 1 (Donc, dans notre cas, le serveur 1 est srv-nte-print1).
10.X.X.X : c'est l'adresse IP du serveur RADIUS
1812 : c'est le numéro de port utilisé par le serveur RADIUS pour communiquer.
ascii : cela indique le type de communication utilisé (ici, du texte simple).
[redacted] c'est une clé secrète partagée entre le contrôleur et le serveur RADIUS. C'est comme un mot de passe que seuls les utilisateurs connaissent, pour s'assurer que personne d'autre ne peut se faire passer pour eux.

Ensuite, j'ai configuré le Wlan 2 qui correspond au WIFI test pour l'authentification RADIUS.



(Cisco Controller) config>wlan security wpa akm 802.1x enable 2

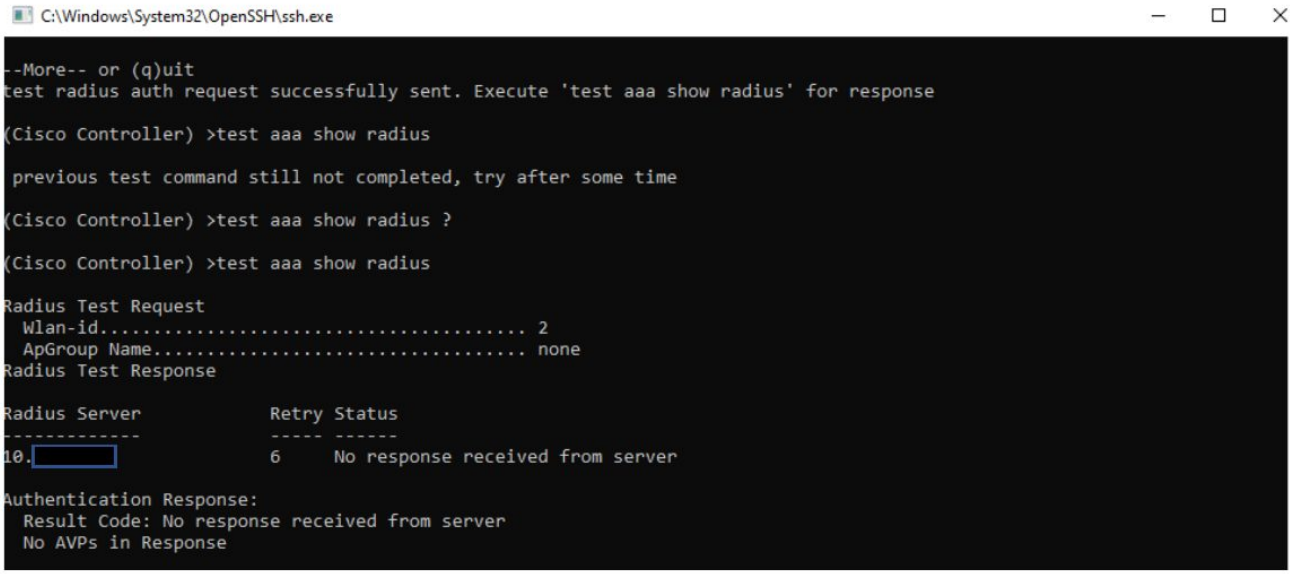
wlan security wpa akm 802.1x enable 2 : cette commande configure le WLAN (Wireless Local Area Network) numéro 2, pour utiliser le protocole de sécurité WPA (Wi-Fi Protected Access) avec la technique d'authentification AKM (Authentication and Key Management) 802.1x.
Plus précisément, le contrôleur est configuré pour activer le protocole d'authentification 802.1x sur le WLAN 2.
Ce protocole permet aux utilisateurs sans fil de s'authentifier auprès d'un serveur RADIUS, avant de pouvoir accéder au réseau.

(Cisco Controller) config>wlan radius_server auth enable 2

wlan radius_server auth enable 2 : cette commande active l'authentification RADIUS pour le WLAN numéro 2. Ici, le contrôleur est configuré pour utiliser un serveur RADIUS, pour authentifier les utilisateurs sans fil qui tentent de se connecter au WLAN 2.

Ces deux commandes configurent le WLAN 2 pour utiliser le protocole de sécurité WPA avec authentification 802.1x et RADIUS. La première commande active le protocole 802.1x pour le WLAN 2, et la deuxième commande active l'authentification RADIUS pour ce même WLAN.

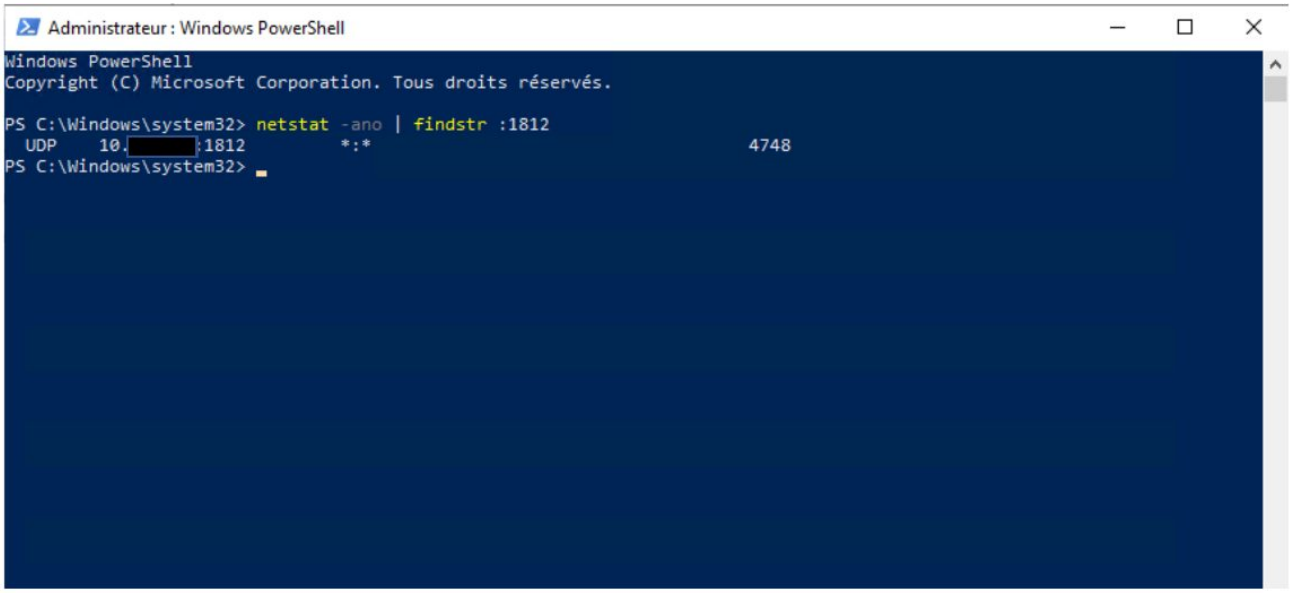
Une fois cela fait, il faut tester le serveur radius pour vérifier qu'il est fonctionnel. J'ai donc fait la commande « test aaa show radius »



Le test effectué, test aaa show radius, permet de vérifier la communication entre le contrôleur Cisco et un serveur RADIUS.

Dans notre cas, le test révèle que le contrôleur n'a pas reçu de réponse du serveur RADIUS à l'adresse 10.X.X.X. Le message "No response received from server" indique clairement un problème de communication.
Si le contrôleur ne peut pas communiquer avec le serveur RADIUS, les utilisateurs ne pourront pas s'authentifier pour accéder au réseau sans fil.

J'ai vérifié l'adresse IP et la connectivité du serveur RADIUS. Je me suis assuré que l'adresse IP 10.X.X.X était correcte et que le serveur RADIUS était en ligne et accessible depuis le contrôleur. J'ai utilisé la commande ping 10.X.X.X pour vérifier la connectivité de base.
Après, j'ai examiné les paramètres du serveur RADIUS. J'ai vérifié que le serveur RADIUS était correctement configuré, pour accepter les demandes d'authentification provenant du contrôleur Cisco. Je me suis également assuré que les adresses IP et les secrets partagés étaient correctement configurés des deux côtés.
Pour les Firewalls, j'ai vérifié si des firewalls bloquaient la communication entre le contrôleur et le serveur RADIUS. Ce n'était pas le cas. J'ai quand même cherché si les protocoles des ports 1812 et 1813 par défaut étaient bien pris en compte.



D'abord, j'ai ouvert l'invite de commandes Windows PowerShell. C'est un outil qui me permet de donner des instructions à l'ordinateur en tapant du texte.

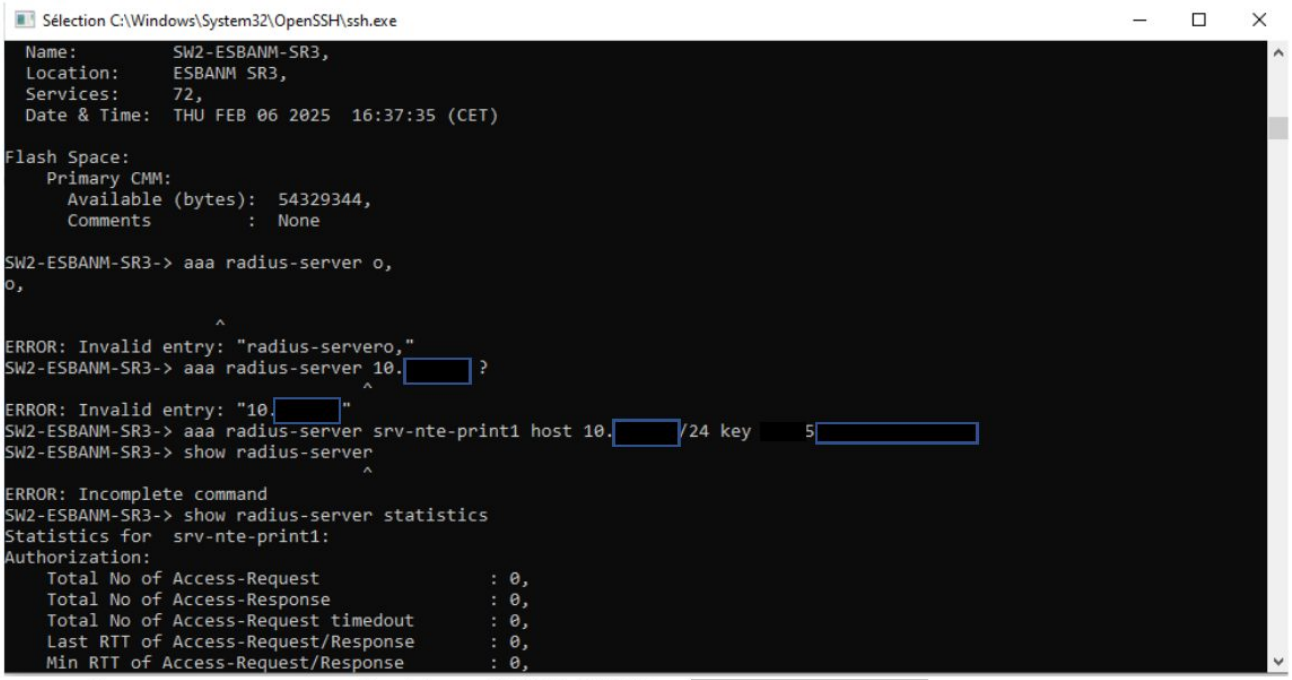
Ensuite, j'ai utilisé la commande netstat -ano | findstr :1812. Cette commande est composée de deux parties :
netstat -ano : cette partie me montre toutes les connexions au réseau actives sur mon ordinateur, avec des détails comme l'adresse IP et le numéro de port utilisés.
| findstr :1812 : le symbole | (appelé "pipe") envoie la sortie de la première commande à la deuxième commande. findstr :1812 filtre les résultats pour ne garder que les lignes qui contiennent le texte ":1812". Cela me permet de voir facilement si un programme utilise le port 1812.
Il utilise ce port pour communiquer avec le serveur, qui contient les informations d'identification.

L'image montre qu'il y a un programme (avec le numéro 4748) qui écoute sur le port 1812 et que l'adresse locale est 10.X.X.X. Cela signifie qu'un serveur RADIUS est probablement en train de fonctionner sur cet ordinateur.

Après avoir vérifié tout cela, j'ai renseigné le serveur RADIUS dans le serveur AD pour être sûr que le serveur RADIUS peut aller chercher les comptes pour l'authentification (voir annexe 3).

Problèmes réseau : je me suis assuré qu'il n'y a pas de problèmes de réseau, tels que des interruptions de service, des erreurs de routage ou des problèmes de DNS qui pourraient empêcher la communication entre le contrôleur et le serveur RADIUS.
J'ai donc paramétré les switchs qui étaient entre le serveur et le contrôleur de WIFI, il y en avait 2. Le premier switch, celui qui était le plus proche de ma machine, était dans le SR3. J'ai donc d'abord mis en place l'authentification 802.1x.
802.1X sont des standards liés à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE. Il permet de contrôler l'accès aux équipements d'infrastructures réseau.

Puis j'ai configuré le serveur RADIUS sur le switch avec cette commande.



aaa radius-server srv-nte-print1 host 10.X.X.X/24 key [redacted]

aaa radius-server srv-nte-print1 :
Définit un serveur RADIUS avec l'identifiant srv-nte-print1.
Cet alias est utilisé pour référencer le serveur dans d'autres configurations AAA.

host 10.X.X.X /24 :
Spécifie l'adresse IP du serveur RADIUS (10.X.X.X).
/24 est obligatoire seulement sur la version de ce switch, car la syntaxe habituelle n'inclut pas de masque de sous-réseau ici.
La bonne syntaxe devrait être : aaa radius-server srv-nte-print1 host [redacted] key [redacted]

key [redacted]
Définit la clé partagée, utilisée pour sécuriser les échanges entre l'équipement et le serveur RADIUS.
Cette clé doit être exactement la même que celle configurée sur le serveur NPS, sinon les requêtes seront rejetées.

Après avoir ajouté le serveur, la commande suivante est utilisée pour afficher les statistiques des transactions RADIUS :
show radius-server statistics
Les résultats montrent qu'aucune requête n'a été envoyée (Access-Request: 0), ce qui signifie :
Soit l'équipement utilisateur n'a pas encore tenté d'authentification, soit l'authentification AAA n'est pas correctement appliquée dans la configuration.
Mais dans notre cas, je n'avais pas encore fait de test, donc aucune « request » envoyée.
J'ai donc ensuite activé sur les 2 switchs le protocole 802.1x, que j'ai déjà activé précédemment sur le contrôleur de WIFI. Ce protocole permet donc de passer les requêtes d'authentification.



J'ai utilisé la commande suivante pour activer l'authentification 802.1x sur le commutateur :

SW2-ESBANM-SR3-> aaa authentication 802.1x srv-nte-print1

Cette commande indique au commutateur d'utiliser le serveur d'authentification "srv-nte-print1" pour authentifier les utilisateurs et les appareils.
Les authentifications 802.1x ont été activées avec succès sur le commutateur. Les utilisateurs et les appareils doivent maintenant s'authentifier, avant de pouvoir se connecter au réseau.
J'ai donc configuré l'authentification 802.1x sur l'autre commutateur du réseau.
Et ensuite retenté l'authentification 802.1x avec la commande :

SW2-ESBANM-SR3-> aaa test-radius-server srv-nte-print1 type authentification user … pasword …



aaa test-radius-server : cette commande permet de tester la connectivité et l'authentification avec un serveur RADIUS.

srv-nte-print1 : c'est le nom du serveur RADIUS configuré sur le switch.

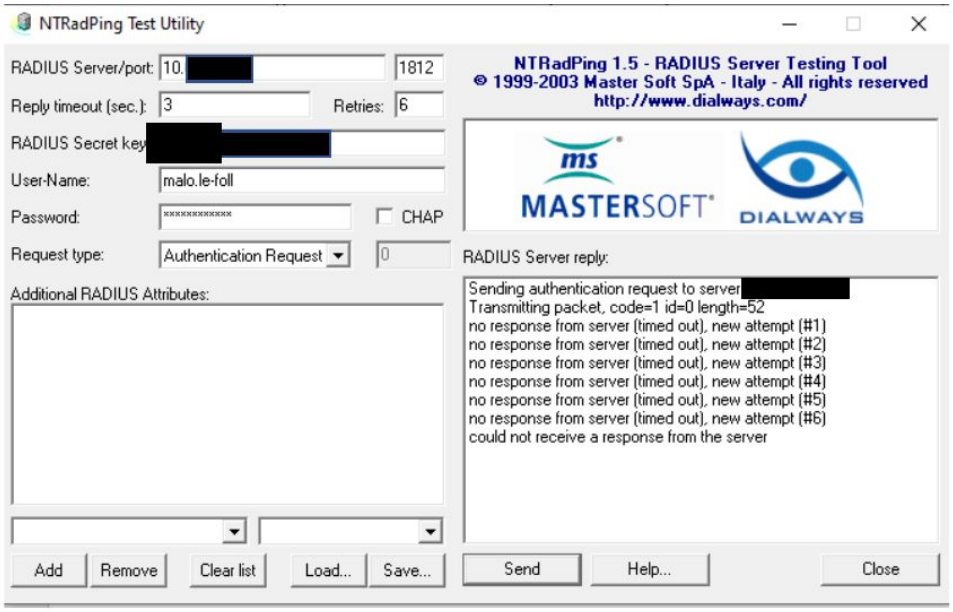
type authentication : cela spécifie que le test concerne l'authentification des utilisateurs.

user password : cela représente l'utilisateur et son mot de passe testés pour l'authentification sur le serveur RADIUS.

Le test affiche toujours une erreur, donc je pense que le problème vient directement du serveur NPS, qui a un problème dans sa configuration. Je suis donc retourné sur le serveur PRINT1 et j'ai « reset » la configuration des clients RADIUS. Après avoir paramétré les clients RADIUS, j'ai installé un logiciel pour tester les requêtes UDP.

Un test a été réalisé afin de vérifier la communication entre un utilisateur et le serveur d'authentification. Ce test est effectué à l'aide de l'outil NTRadPing 1.5, permettant d'envoyer des requêtes et d'obtenir une réponse du serveur distant.

Le serveur testé est accessible à l'adresse 10.X.X.X (l'ip du serveur RADIUS), et les requêtes sont envoyées sur le port 1812, qui est normalement utilisé pour ce type d'authentification. L'objectif de cette procédure est de s'assurer que le serveur est bien en mesure de recevoir et traiter les demandes envoyées par les utilisateurs authentifiés.



L'outil NTRadPing a été configuré avec les paramètres suivants : l'adresse IP du serveur, le port, la clé secrète de communication, ainsi que les identifiants de connexion pour l'utilisateur testé. Une série de six tentatives a été envoyée, chacune avec un délai d'attente de 3 secondes pour la réponse du serveur.

À chaque envoi, une requête d'authentification est transmise et un retour est attendu du serveur. L'outil doit alors afficher la réponse reçue ou un message d'échec en cas d'absence de retour.

Les résultats du test montrent que le serveur n'a répondu à aucune des six tentatives envoyées. L'outil a systématiquement affiché le message :

"No response from server (timed out), new attempt (#X)"

Après six essais, le message final indique :

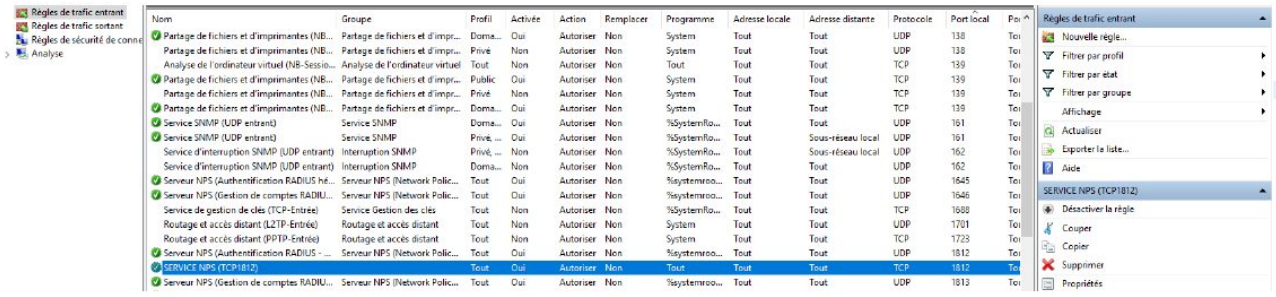
"Could not receive a response from the server"

Cela signifie que les requêtes envoyées par l'utilisateur n'ont pas pu atteindre le serveur ou que celui-ci n'a pas traité les demandes et renvoyé une réponse. Ce comportement peut être causé par plusieurs éléments empêchant la communication entre les deux équipements.

L'absence totale de réponse peut être attribuée à diverses possibilités, telles que, le serveur n'est pas opérationnel ou qu'il n'est pas correctement configuré, pour accepter les requêtes de l'utilisateur, malgré un reset total du serveur, pour sa reconfiguration. Une autre cause potentielle pourrait être la présence d'un pare-feu ou d'une règle de filtrage réseau, bloquant le trafic sur le port 1812.

Une erreur dans la configuration de la clé secrète partagée entre le serveur et l'utilisateur pourrait empêcher l'établissement d'une communication correcte. Également un problème d'adressage IP ou de routage sur le réseau peut expliquer cette absence de réponse. Mais, bien qu'ayant vérifié que la clé, le mot de passe ou même l'adresse IP étaient corrects, le serveur ne répond toujours pas.

L’étape suivante consistera à modifier les règles du firewall, qui est peut-être la cause possible de ce blocage, en effectuant des vérifications sur le serveur.



J'ai ajouté la règle TCP port 1812 pour permettre aux serveurs d'envoyer des requêtes d'authentification via ce port.
Cependant, après avoir ajouté la règle, j'ai constaté que le serveur ne recevait toujours pas les requêtes. Donc le problème ne venait pas du Firewall.

La mise en place d'un serveur RADIUS sous Windows est une solution stratégique pour renforcer la sécurité et la gestion des accès au réseau. Cette étude de cas a permis de configurer le rôle NPS (Network Policy Server), en définissant une nouvelle solution d'authentification pour les équipements réseau dans un cadre sécurisé.

Sur le plan technologique, le contrôleur Wi-Fi a été configuré pour passer de l'authentification des utilisateurs au serveur RADIUS via WPA2-Enterprise ou WPA3-Enterprise, garantissant ainsi une sécurité renforcée. Également, les deux switchs ont été paramétrés pour supporter l'authentification 802.1X, permettant un contrôle des connexions filaires.

Aspects sécuritaires, normatifs et réglementaires :

L'implémentation du serveur RADIUS est dans une logique de conformité aux normes et aux réglementations :

Sécurité des accès : l'utilisation de l'authentification robuste via EAP (Extensible Authentication Protocol) permet de réduire le risque d'usurpation d'identité et évite la mise au clair de la clé WPA pour les étudiants.

Normes et régulations : cette architecture répond aux réglementations telles que le RGPD, en assurant un contrôle des accès aux données.

Protection des échanges : le chiffrement des communications entre utilisateurs, contrôleurs et serveur RADIUS via TLS (Transport Layer Security) garantit la confidentialité des données d'authentification.

Dimensions économiques et juridiques :

D'un point de vue économique, l'investissement initial (licences Windows Server, maintenance) peut être compensé par une meilleure efficacité et une réduction des incidents de sécurité comparée à une simple authentification WPA.

Sur le plan juridique, la traçabilité des connexions via les logs RADIUS peut servir pour superviser et contrôler les connexions.

Toutefois, un problème persiste : les requêtes UDP sur le port 1812 aboutissent à un timeout, empêchant l'authentification des utilisateurs. Ce blocage aurait pu être dû au Firewall, mais après vérification, aucune règle interdit le port 1812. Malgré tout, une fois ce problème résolu, cette infrastructure permettra d'assurer un contrôle d'accès robuste, conforme et optimisé, garantissant ainsi la sécurité et l'efficacité des communications au sein du réseau.