GUIDE D'INSTALLATION ET DE CONFIGURATION : ARCHITECTURE RADIUS SÉCURISÉE (802.1X / AD)

Objectif du Projet

L'objectif est de mettre en place un système d'authentification réseau sécurisé (802.1X) centralisé. La solution s'appuie sur :

- **FreeRADIUS** : Le serveur cœur qui gère les requêtes d'authentification.
- **daloRADIUS** : L'interface web pour l'administration simplifiée des utilisateurs et des NAS.
- **Active Directory (AD)** : La source de vérité pour les comptes utilisateurs, connectée via le module **LDAP**.
- **Protocole PEAP-MSCHAPv2 (NTLM)** : Méthode d'authentification par mot de passe via un tunnel sécurisé, utilisant **Samba/Winbind** pour la validation AD.
- **EAP-TLS** : Méthode d'authentification par certificats numériques pour une sécurité maximale.
- **Switch Netgear (M4300-52G)** : Contrôle l'accès physique au réseau filaire.
- **Bornes Wi-Fi (NAS)** : Contrôlent l'accès sans fil via une borne TEST et le SSID `MOBILESSID`.

Étape 1 : Prérequis et Accès Super-Utilisateur

Commande :

```
su
```

Explication :

- `su` permet de basculer vers l'utilisateur **root** (super-utilisateur).
- **Pourquoi ?** Certaines commandes nécessitent des droits administratifs (installation de logiciels, modification de fichiers système).
- **Exemple** : Sans `su` , vous ne pourriez pas installer Apache ou FreeRADIUS.

Étape 2 : Mise à jour du Système

Commande :

```
dnf update -y
```

Explication :

- dnf est le gestionnaire de paquets de RHEL/CentOS (comme apt pour Debian).
- update met à jour tous les paquets installés.
- -y répond automatiquement "oui" aux questions.
- **Pourquoi ?** Évite les conflits et les vulnérabilités avec des paquets obsolètes.
- **Exemple** : Si vous ne mettez pas à jour, une faille de sécurité dans Apache pourrait être exploitée.

Étape 3 : Installation d'Apache (httpd)

Commandes :

```
dnf install httpd -y
systemctl enable --now httpd
firewall-cmd --add-service=http --permanent
firewall-cmd --reload
```

Explication :

1. **Installation d'Apache** :
    - httpd est le nom du paquet Apache sur RHEL.
    - **Pourquoi ?** daloRADIUS est une application web, elle a besoin d'un serveur web (Apache) pour fonctionner.
2. **Activation et démarrage** :
    - systemctl enable --now httpd :
        - enable : Active Apache au démarrage du serveur.
        - --now : Démarre Apache immédiatement.
    - **Pourquoi ?** Sans cela, daloRADIUS ne serait pas accessible.
3. **Ouverture du pare-feu** :
    - firewall-cmd --add-service=http --permanent :
        - Ouvre le port 80 (HTTP) dans le pare-feu.
    - --permanent : Rend la règle persistante après un redémarrage.
    - firewall-cmd --reload : Recharge le pare-feu pour appliquer les changements.
    - **Pourquoi ?** Sans cela, vous ne pourriez pas accéder à l'interface web de daloRADIUS depuis un navigateur.

Vérification :

```
systemctl status httpd
```

- Doit afficher active (running) en vert.

Exemple de sortie :
● httpd.service - The Apache HTTP Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)

- Active: active (running) since Mon 2026-01-09 10:00:00 CET; 1h ago

---

Étape 4 : Installation de MariaDB

Commandes :

```
dnf install mariadb-server mariadb -y
systemctl enable --now mariadb
mysql_secure_installation
```

Explication :

1. **Installation de MariaDB** :
    - mariadb-server : Le serveur de base de données.
    - mariadb : Les outils clients pour interagir avec MariaDB.
    - **Pourquoi ?** FreeRADIUS et daloRADIUS stockent les utilisateurs, les NAS (switchs), et les logs dans une base de données.
2. **Activation et démarrage** :
    - systemctl enable --now mariadb :
        - Démarre MariaDB et l'active au démarrage.
    - **Pourquoi ?** Sans MariaDB, FreeRADIUS ne pourrait pas stocker les données.
3. **Sécurisation de MariaDB** :
    - mysql_secure_installation :
        - Définir un mot de passe pour l'utilisateur **root**.
        - Supprimer les utilisateurs anonymes.
        - Désactiver la connexion root à distance.
        - Supprimer la base de test.
    - **Pourquoi ?** Protège votre base de données contre les accès non autorisés.

Création de la base radius :

```
mysql -u root -p -e "CREATE DATABASE radius;"
mysql -u root -p -e "GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY 'radiuspassword';"
mysql -u root -p -e "FLUSH PRIVILEGES;"
```

- **Explication** :
    - CREATE DATABASE radius; : Crée une base de données nommée radius.

- GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY 'radiuspassword'; :
  - Crée un utilisateur radius avec tous les droits sur la base radius.
  - **Pourquoi ?** FreeRADIUS utilisera cet utilisateur pour se connecter à la base.
- FLUSH PRIVILEGES; : Recharge les permissions pour qu'elles soient prises en compte.

Étape 5 : Installation de PHP et dépendances

Commandes :

```
dnf install php php-mysqlnd php-gd php-mbstring php-xml php-pear -y
pear install DB
```

Explication :

1. **Installation de PHP** :
   - php : Le langage de script côté serveur.
   - php-mysqlnd : Permet à PHP de communiquer avec MariaDB.
   - php-gd : Pour la génération d'images (graphiques, CAPTCHA).
   - php-mbstring : Pour la gestion des chaînes de caractères multi-octets (UTF-8).
   - php-xml : Pour le traitement des fichiers XML.
   - php-pear : Pour installer des paquets PHP supplémentaires.
   - **Pourquoi ?** daloRADIUS est écrit en PHP et nécessite ces extensions.
2. **Installation de DB via PEAR** :
   - pear install DB :
     - Installe le paquet DB de PEAR, nécessaire pour daloRADIUS.
   - **Pourquoi ?** daloRADIUS utilise ce paquet pour interagir avec la base de données.

Vérification :

```
php -v
```

- Affiche la version de PHP installée.
- **Exemple de sortie** :
  PHP 8.1.12 (cli) (built: Oct 22 2022 08:58:21)

Étape 6 : Installation de FreeRADIUS

Commandes :

```
dnf install freeradius freeradius-utils freeradius-mysql -y
systemctl enable --now radiusd
```

Explication :

1. **Installation de FreeRADIUS** :
    - freeradius : Le serveur RADIUS principal.
    - freeradius-utils : Outils utiles pour tester et gérer FreeRADIUS.
    - freeradius-mysql : Module pour connecter FreeRADIUS à MariaDB.
    - **Pourquoi ?** FreeRADIUS est le cœur de l'authentification 802.1X.
2. **Activation et démarrage** :
    - systemctl enable --now radiusd :
        - radiusd est le nom du service FreeRADIUS.
        - **Pourquoi ?** Sans cela, FreeRADIUS ne démarrera pas automatiquement.

Vérification en mode debug :

```
pkill radiusd
radiusd -X
```

- **Explication** :
    - pkill radiusd : Arrête le service FreeRADIUS.
    - radiusd -X : Lance FreeRADIUS en mode debug (pour voir les erreurs en temps réel).
    - **Pourquoi ?** Permet de diagnostiquer les problèmes de configuration.
    - **Sortie attendue** :
      Ready to process requests.
    - **Quitter** : Ctrl+C.

Étape 7 : Configuration de FreeRADIUS avec MariaDB

Commandes :

```
mysql -u root -p radius < /etc/raddb/mods-config/sql/main/mysql/schema.sql
ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
```

Explication :

1. **Import du schéma SQL** :
    - /etc/raddb/mods-config/sql/main/mysql/schema.sql :

        - Contient la structure des tables nécessaires pour FreeRADIUS (utilisateurs, NAS, logs).
    - **Pourquoi ?** Sans ces tables, FreeRADIUS ne pourrait pas stocker les données.
2. **Activation du module SQL** :

    - ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ :
        - Crée un lien symbolique pour activer le module SQL.
    - **Pourquoi ?** FreeRADIUS utilise des modules modulaires. Il faut "activer" ceux dont on a besoin.

Configuration du fichier SQL (/etc/raddb/mods-available/sql) :

```
sql {
  driver = "rlm_sql_mysql"
  server = "localhost"
  port = 3306
  login = "radius"
  password = "radiuspassword"
  radius_db = "radius"
```

3. }

    - **Explication des paramètres** :
        - driver = "rlm_sql_mysql" : Utilise le pilote MySQL.
        - server = "localhost" : Adresse du serveur MariaDB.
        - login et password : Identifiants de l'utilisateur radius créé précédemment.
        - radius_db = "radius" : Nom de la base de données.
    - **Pourquoi ?** FreeRADIUS doit savoir comment se connecter à la base de données.
4. **Mise à jour des permissions** :

    ```
    chgrp -h radiusd /etc/raddb/mods-enabled/sql
    ```

    - **Explication** :
        - chgrp -h radiusd : Change le groupe du fichier pour que le service FreeRADIUS (radiusd) puisse y accéder.
    - **Pourquoi ?** Sans cela, FreeRADIUS n'aurait pas les droits pour lire la configuration SQL.

Étape 8 : Installation de daloRADIUS

Commandes :

```
dnf install wget unzip -y
```

```
wget https://github.com/lirantal/daloradius/archive/master.zip
unzip master.zip
mv daloradius-master /var/www/html/daloradius
```

Explication :

1. **Installation des dépendances** :
    - wget : Pour télécharger des fichiers.
    - unzip : Pour extraire les archives ZIP.
2. **Téléchargement et extraction** :
    - wget https://github.com/lirantal/daloradius/archive/master.zip :
        - Télécharge la dernière version de daloRADIUS.
    - unzip master.zip : Extrait l'archive.
    - mv daloradius-master /var/www/html/daloradius :
        - Déplace le dossier dans /var/www/html/ pour qu'il soit accessible via Apache.

Import des tables SQL :

```
mysql -u root -p radius < /var/www/html/daloradius/contrib/db/mysql-daloradius.sql
```

- **Explication** :
    - Importe les tables spécifiques à daloRADIUS (utilisateurs, NAS, profils).
    - **Pourquoi ?** Sans ces tables, daloRADIUS ne pourrait pas fonctionner.

Configuration de daloRADIUS (/var/www/html/daloradius/app/common/includes/daloradius.conf.php) :

```
$configValues['CONFIG_DB_ENGINE'] = 'mysqli';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = 'radiuspassword';
$configValues['CONFIG_DB_NAME'] = 'radius';
```

- **Explication des paramètres** :
    - CONFIG_DB_ENGINE : Type de base de données (mysqli pour MySQL/MariaDB).
    - CONFIG_DB_HOST : Adresse du serveur MariaDB.
    - CONFIG_DB_USER et CONFIG_DB_PASS : Identifiants de l'utilisateur radius.
    - CONFIG_DB_NAME : Nom de la base de données.
- **Pourquoi ?** daloRADIUS doit savoir comment se connecter à la base de données.

Étape 9 : Configuration de SELinux

Commandes :

setsebool -P httpd_can_network_connect_db 1
chcon -R -t httpd_sys_rw_content_t /var/www/html/daloradius/

Explication :

1. **Autoriser Apache à se connecter à MariaDB** :
    - setsebool -P httpd_can_network_connect_db 1 :
        - Active une règle SELinux qui permet à Apache (httpd) de se connecter à une base de données.
    - **Pourquoi ?** SELinux bloque par défaut les connexions réseau sortantes d'Apache.
2. **Modifier le contexte de sécurité** :
    - chcon -R -t httpd_sys_rw_content_t /var/www/html/daloradius/ :
        - Donne à Apache les permissions nécessaires pour lire/écrire dans le dossier de daloRADIUS.
    - **Pourquoi ?** Sans cela, Apache n'aurait pas les droits pour accéder aux fichiers de daloRADIUS.

Étape 10 : Redémarrage des Services

Commande :

systemctl restart radiusd mariadb httpd

Explication :

- Redémarre **FreeRADIUS**, **MariaDB** et **Apache** pour appliquer toutes les configurations.
- **Pourquoi ?** Les changements de configuration ne sont pris en compte qu'après un redémarrage des services.

Étape 11 : Accès à l'Interface daloRADIUS

URL :

http://<IP_DU_SERVEUR>/daloradius/app/operators/login.php

Identifiants par défaut :

- **Username** : administrator

- **Password** : radius

Exemple : Si l'IP de votre serveur est (ex: 192.10.50.50), l'URL sera :

http://192.10.50.50/daloradius/app/operators/login.php

Bonus : Simplifier l'URL avec un Alias Apache

Objectif : Rendre l'URL plus simple (ex: http://192.10.50.50/radius au lieu de .../daloradius/app/operators/login.php).

Étapes :

1. **Créer un fichier de configuration Apache** :
   nano /etc/httpd/conf.d/radius_simple.conf

Ajouter la configuration :

```
Alias /radius /var/www/html/daloradius/app/operators
<Directory /var/www/html/daloradius/app/operators>
    DirectoryIndex login.php
    Options FollowSymLinks
    AllowOverride All
    Require all granted
```

2. </Directory>

   - **Explication** :
     - Définit login.php comme page par défaut.
     - Require all granted :
       - Autorise l'accès à ce dossier.
         a. Alias /radius /var/www/html/daloradius/app/operators :
            i. Associe /radius au dossier des opérateurs de daloRADIUS.
         b. DirectoryIndex login.php :

3. **Redémarrer Apache** :
   systemctl restart httpd

4. **Tester la nouvelle URL** :
   http://192.10.50.50/radius

Cas Pratiques : Contrôle d'Accès avec Switch Netgear

1. Configurer le Switch Netgear (NAS)

Objectif : Dire au switch d'interroger FreeRADIUS avant d'autoriser l'accès.

Dans daloRADIUS :

- Allez dans **Management > NAS > New NAS**.
- **NAS IP/Host** : IP du switch (ex: 192.10.50.55).
- **NAS Secret** : Mot de passe partagé (ex: radiuspassword).
- **NAS Shortname** : Nom pour identifier le switch (ex: Switch_Etage1).

Sur le switch Netgear :

- **Security > RADIUS > Server Configuration** :
  - **Server IP** : IP du serveur RHEL (ex: 192.10.50.50).
  - **Secret Key** : radiuspassword.
  - **Port** : 1812 (port par défaut pour l'authentification RADIUS).
- **Security > 802.1X > Port Control** :
  - Passez le port en mode 802.1X Based.

Pourquoi ? :

- Le switch **ne laisse passer aucun trafic** tant que FreeRADIUS n'a pas autorisé la connexion.
- Le **NAS Secret** doit être identique des deux côtés (switch et FreeRADIUS).

---

2. Autoriser un PC et Bloquer un Collègue

Méthode 1 : Authentification par Mot de Passe (PEAP-MSCHAPv2)

Objectif : Utiliser un nom d'utilisateur et un mot de passe.

Dans daloRADIUS :

- Créez un utilisateur pour vous :
  - **Management > Users > New User**.
  - **Username** : nicolas.
  - **Password** : mon_mot_de_passe.

Sur le PC Windows :

- **Paramètres réseau > Ethernet > Authentification** :
  - Activez 802.1X.
  - Méthode d'authentification : Microsoft: EAP protégé (PEAP).
  - Entrez vos identifiants (nicolas / mon_mot_de_passe).

Résultat :

- Votre PC est autorisé.
- Votre collègue (sans compte) est bloqué.

Méthode 2 : Authentification par Certificat (EAP-TLS)

Objectif : Utiliser des certificats numériques (plus sécurisé).

Sur le serveur RHEL :

Générer les certificats :

```
cd /etc/raddb/certs/
```

1. ./bootstrap

    - **Explication** :
        - Crée un **CA** (Autorité de Certification), un certificat serveur, et un certificat client.
        - Les fichiers importants :
            - ca.pem : Certificat de l'autorité de certification.
            - server.pem : Certificat du serveur.
            - client.p12 : Certificat client (à installer sur le PC).

Configurer EAP-TLS (/etc/raddb/mods-enabled/eap) :

```
 default_eap_type = tls
tls-config {
   private_key_file = ${certdir}/server.key
   certificate_file = ${certdir}/server.pem
   ca_file = ${certdir}/ca.pem
```

2. }

    - **Pourquoi ?** :
        - default_eap_type = tls : Force l'utilisation de EAP-TLS.
        - Les chemins vers les certificats doivent être corrects.
3. **Redémarrer FreeRADIUS** :

    ```
    systemctl restart radiusd
    ```

Sur le PC Windows :

- Installez le certificat client.p12 :
    - Double-cliquez sur le fichier > **Certificat personnel**.
- **Paramètres réseau > Ethernet > Authentification** :
    - Méthode : Carte à puce ou autre certificat.

- Sélectionnez le certificat installé.

Résultat :

- Seul le PC avec le certificat valide peut se connecter.

Installation du serveur DHCP par VLAN (SI BESOIN)

Pour que les PC reçoivent une IP automatiquement dans le bon VLAN.

Commandes :

```
dnf install dhcp-server -y
nano /etc/dhcp/dhcpd.conf
```

Configuration à ajouter (exemple pour le VLAN 10) :

```
subnet 192.168.10.0 netmask 255.255.255.0 {
   range 192.168.10.50 192.168.10.150;
   option routers 192.168.10.1;
   option domain-name-servers 8.8.8.8;
}

systemctl enable --now dhcpd
```

Cas Pratique : Configuration de la Borne Wi-Fi (NAS)

L'objectif est de transformer ta borne Wi-Fi en "client RADIUS" (NAS) pour qu'elle interroge ton serveur RHEL.

1. Déclaration dans daloRADIUS

- **Action :** Allez dans **Management > NAS > New NAS**.
- **NAS IP/Host :** IP de la borne (ex: 192.10.50.100).
- **NAS Secret :** Mot de passe partagé (ex: radiuspassword).
- **NAS Type :** Sélectionnez Wireless-802.11.

Pourquoi ? Sans cette déclaration, FreeRADIUS rejettera les demandes provenant de l'IP de la borne pour des raisons de sécurité.

---

2. Configuration sur l'interface de la Borne

- **Type de sécurité :** Choisissez **WPA2-Enterprise** (ou WPA3-Enterprise).

- **Serveur RADIUS :** 192.10.50.50 (Ton serveur RHEL).
- **Secret Partagé :** radiuspassword (Doit être identique à daloRADIUS).
- **Port d'authentification :** 1812.

---

3. Interconnexion Active Directory (LDAPS)

Le module LDAP permet au RADIUS de lire les informations des utilisateurs et de vérifier leur appartenance aux groupes dans l'AD **NOM-ENTREPRISE.LOCAL**.

Fichier : `/etc/raddb/mods-enabled/ldap`

```
ldap {
    server = "dc-01.nom-entreprise.local"
    identity = "cn=admin-radius,ou=ServiceAccounts,dc=nom-entreprise,dc=local"
    password = "MotDePasseSecret"
    base_dn = "dc=nom-entreprise,dc=local"

    # Utilisation du port 636 pour le LDAPS
    tls {
        start_tls = no
        ca_file = ${certdir}/ca-ad.pem
        require_cert = "demand"
    }

    user {
        base_dn = "ou=Users,dc=nom-entreprise,dc=local"
        filter = "(sAMAccountName=%{%{Stripped-User-Name}:-%{User-Name}})"
    }
}
```

---

4. Configuration de l'authentification NTLM (MS-CHAPv2)

Pour valider le mot de passe sans qu'il circule en clair, on utilise Samba/Winbind. Cette étape inclut le correctif pour les caractères spéciaux.

A. Configuration Samba (`/etc/samba/smb.conf`)

```
[global]
   netbios name = RADIUS-SRV
   workgroup = NOM-ENTREPRISE
   realm = NOM-ENTREPRISE.LOCAL
   security = ADS
```

```
  # Correctif indispensable pour les caractères spéciaux et accents
  unix charset = UTF-8
  dos charset = cp1252

  ntlm auth = mschapv2-and-ntlmv2-only
  winbind use default domain = yes
```

B. Configuration du module MS-CHAP (/etc/raddb/mods-enabled/mschap)

```
mschap {
   use_mppe = yes
   with_ntdomain_hack = yes
   ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{mschap:User-Name}
--domain=%{mschap:NT-Domain}"
}
```

---

5. Configuration du Tunnel EAP et des Serveurs Virtuels

C'est ici que l'on définit comment le tunnel sécurisé (PEAP) est monté et comment les requêtes sont traitées à l'intérieur.

A. Configuration EAP (/etc/raddb/mods-enabled/eap)

```
eap {
   default_eap_type = peap
   timer_expire = 60

   tls-config tls-common {
      private_key_file = ${certdir}/server.key
      certificate_file = ${certdir}/server.pem
      ca_file = ${certdir}/ca.pem
   }

   peap {
      tls = tls-common
      default_eap_type = mschapv2
      virtual_server = "inner-tunnel" # Redirection vers le tunnel interne
   }
}
```

B. Serveur Virtuel par défaut (sites-enabled/default) Ce serveur écoute sur les ports 1812/1813 et initie le tunnel EAP.

```
server default {
   authorize {
```

```
        filter_username  # Nettoyage selon tes règles REGEX
        preprocess
        eap             # Démarre le tunnel PEAP
    }
    authenticate {
        eap
    }
    post-auth {
        update {
            &session-state: += &reply: # Nécessaire pour les clés MPPE du Wi-Fi
        }
    }
}
```

C. Serveur Virtuel Interne (sites-enabled/inner-tunnel) C'est ici que l'authentification finale AD se produit, une fois le tunnel sécurisé.

```
server inner-tunnel {
    authorize {
        filter_username
        preprocess
        mschap
        eap
    }
    authenticate {
        Auth-Type MS-CHAP {
            mschap  # Appel de ntlm_auth configuré plus haut
        }
        eap
    }
}
```

Résumé Technique de la Solution

- **Sécurité :** Le client vérifie le certificat du serveur (EAP-PEAP).
- **Fiabilité :** Le module filter_username rejette les identifiants mal formés (espaces, doubles @).
- **Compatibilité :** La configuration smb.conf (UTF-8) garantit que même les mots de passe avec caractères spéciaux sont validés par l'Active Directory via NTLM.
- **Architecture :** LDAP(S) assure la visibilité des comptes, tandis que MS-CHAPv2 assure la preuve de possession du mot de passe.

Cas Pratique : Authentification Centralisée RADIUS & LDAP

Équipement : Netgear M4300-52G

Objectif : Gestion des accès administrateurs (SSH et Web) via **FreeRADIUS** connecté à l'**Active Directory**.

---

1. Configuration du Switch (Côté Matériel)

Sur ce modèle, la syntaxe est très précise : il faut différencier le trafic d'authentification (auth) du trafic de comptabilité (acct).

A. Déclaration du serveur et du Secret (Clé)

Le "Secret" est le mot de passe que le switch et le serveur utilisent pour se faire confiance mutuellement.

```
# 1. Déclarer l'hôte pour l'authentification
(M4300-52G) (Config)# radius server host auth 192.10.50.50

# 2. Définir le Secret (Méthode sécurisée par prompt)
(M4300-52G) (Config)# radius server key auth 192.10.50.50
# Enter secret: ********** (Tapez votre clé, ex: radiuspassword)
# Re-enter secret: **********

# 3. Forcer le serveur en tant que Primaire
(M4300-52G) (Config)# radius server primary auth 192.10.50.50
```

B. Activation des accès (CLI & Web)

Il ne suffit pas de déclarer le serveur, il faut dire au switch de l'utiliser pour ses propres accès.

```
# Priorité RADIUS, puis Local si le serveur est injoignable (Fallback)
(M4300-52G) (Config)# aaa authentication login default radius local

# Activation spécifique pour l'interface Graphique Web (GUI)
(M4300-52G) (Config)# ip http authentication radius local

# Sauvegarde de la configuration (Essentiel !)
(M4300-52G) # write memory
```

---

2. Configuration du Serveur (Logic & OID)

A. Le filtrage par OID (Indispensable pour l'AD)

Dans le fichier /etc/raddb/mods-enabled/ldap, pour que FreeRADIUS comprenne la hiérarchie des groupes Windows, on utilise l'OID **1.2.840.113556.1.4.1941** (Matching Rule In Chain) :

# Permet de trouver l'utilisateur même s'il est dans un sous-groupe du groupe Admin
membership_filter = "(member:1.2.840.113556.1.4.1941:=%{control:Ldap-UserDn})"

B. Le bloc de contrôle (sites-enabled/default)

C'est ici qu'on lie l'IP du switch, le groupe LDAP et les privilèges :

```
authorize {
    ...
    if (NAS-IP-Address == 192.10.50.55) {
        update control {
            Auth-Type := ldap
        }
        ldap
        # Vérification stricte du groupe via l'OID configuré précédemment
        if (!(LDAP-Group == "DL-NET-SWITCH-ADMIN")) {
            reject
        }
        # Attribution des privilèges Admin
        update reply {
            Service-Type = "Administrative-User",
            Cisco-AVPair = "shell:priv-lvl=15",
            Netgear-Management-Privilege = 1
        }
        return
    }
    ...
}
```

Voici comment intégrer cette nouvelle règle de sécurité dans ta documentation. Elle suivra exactement la même structure (Commande, Explication, Pourquoi) pour conserver une cohérence professionnelle.

Cas Pratique : Filtrage des accès Wi-Fi par SSID et Groupe LDAP

Objectif : Restreindre l'accès au Wi-Fi "MOBILESSID" aux seuls utilisateurs appartenant au groupe Active Directory spécifique.

Configuration à modifier :

Fichier : /etc/raddb/sites-enabled/inner-tunnel

Bloc de code à insérer :

Dans la section authorize { ... }, après l'appel au module filter_username, ajoutez :

```
# Filtrage par SSID (Called-Station-Id)
if (outer.request:Called-Station-Id =~ /MOBILESSID/) {

   # Appel du module LDAP pour charger les attributs de l'utilisateur
   ldap

   # Vérification de l'appartenance au groupe AD
   if (!(LDAP-Group == "WIFI-MOBILE-ACCESS")) {
      update reply {
         Reply-Message = "Acces refuse : Groupe incorrect pour ce reseau"
      }
      reject
   }
}
```

Explication :

1. **if (outer.request:Called-Station-Id =~ /MOBILESSID/)** :
   - Le Called-Station-Id est un attribut envoyé par la borne Wi-Fi qui contient généralement l'adresse MAC de la borne suivie du SSID (ex: AA-BB-CC-DD-EE-FF:MOBILESSID).
   - L'opérateur =~ permet de faire une recherche par expression régulière pour vérifier si le nom du Wi-Fi est présent dans l'attribut.
2. **ldap** :
   - Appelle le module LDAP configuré précédemment pour interroger l'Active Directory et récupérer les groupes auxquels l'utilisateur appartient.
3. **if (!(LDAP-Group == "WIFI-MOBILE-ACCESS"))** :
   - Vérifie si l'utilisateur est membre du groupe autorisé. Le ! signifie "n'est pas membre de".
4. **reject** :
   - Arrête immédiatement le processus d'authentification et refuse la connexion si la condition n'est pas remplie.

Pourquoi ?

- **Sécurité accrue** : Cela empêche un utilisateur qui possède des identifiants valides (comme un compte générique ou un compte d'un autre service) de se connecter sur un Wi-Fi qui ne lui est pas destiné.
- **Isolation des accès** : Vous liez l'infrastructure physique (le SSID diffusé) à une politique de sécurité logique gérée centralement dans l'AD.

Attribution des Droits (Reply Attributes)

Attribut	Valeur	Rôle
Service-Type	Administrative-User	Autorise l'accès au système.
Cisco-AVPair	shell:priv-lvl=15	Mode **#** (Privilège 15) automatique en SSH.
Netgear-Management-Privilege	1	Droits d'écriture sur l'interface Web.

Maintenance et Diagnostic Rapide

En cas de problème de connexion, utilisez ces outils de vérification :

Commandes sur le Switch

- **show radius server** : Vérifie si le serveur est listé avec le type Primary et s'il est actif (marqué par un *).
- **show radius server 192.10.50.50** : Affiche les compteurs. Si Access-Accept n'augmente pas, la clé ou le compte est erroné.
- **show ip http** : Confirme que Authentication Method affiche bien Radius.
- **show users** : Permet de voir qui est actuellement loggé sur le switch.

Diagnostic sur le Serveur

- **radiusd -X** : Arrêtez le service (systemctl stop radiusd) et lancez-le manuellement avec -X. C'est le mode "Debug" : vous verrez passer chaque étape de l'authentification et l'erreur exacte en cas de rejet (mauvais mot de passe, utilisateur non présent dans le groupe AD, etc.).

Source :
https://debian-facile.org/doc:reseau:web:freeradius
https://wiki.freeradius.org/guide/NTLM-Auth-with-PAP-HOWTO
https://falz.net/wiki/Freeradius_AD_LDAP_Authentication

https://gemini.google.com/app
https://doc.sambaedu.org/utiliser-se4/guide-administration/freeradius