Présentation de la solution DUO SECURITY

Duo Security est une solution de sécurité d'accès développée par Cisco.
Elle est spécialisée dans le 2FA (authentification à deux facteurs) pour protéger l'accès à des ressources critiques : VPN, WiFi, serveurs, applications cloud, etc...

Son rôle est d'ajouter une couche de sécurité supplémentaire à l'authentification à l'aide d'une validation secondaire, de ce fait, elle vérifie l'identité de l'utilisateur et l'était de son appareil (s'il est à jour).

Elle peut empêcher les connexions non autorisées, même si le mot de passe est compromis.

Duo Mobile (aussi appelé Duo Authenticator) :

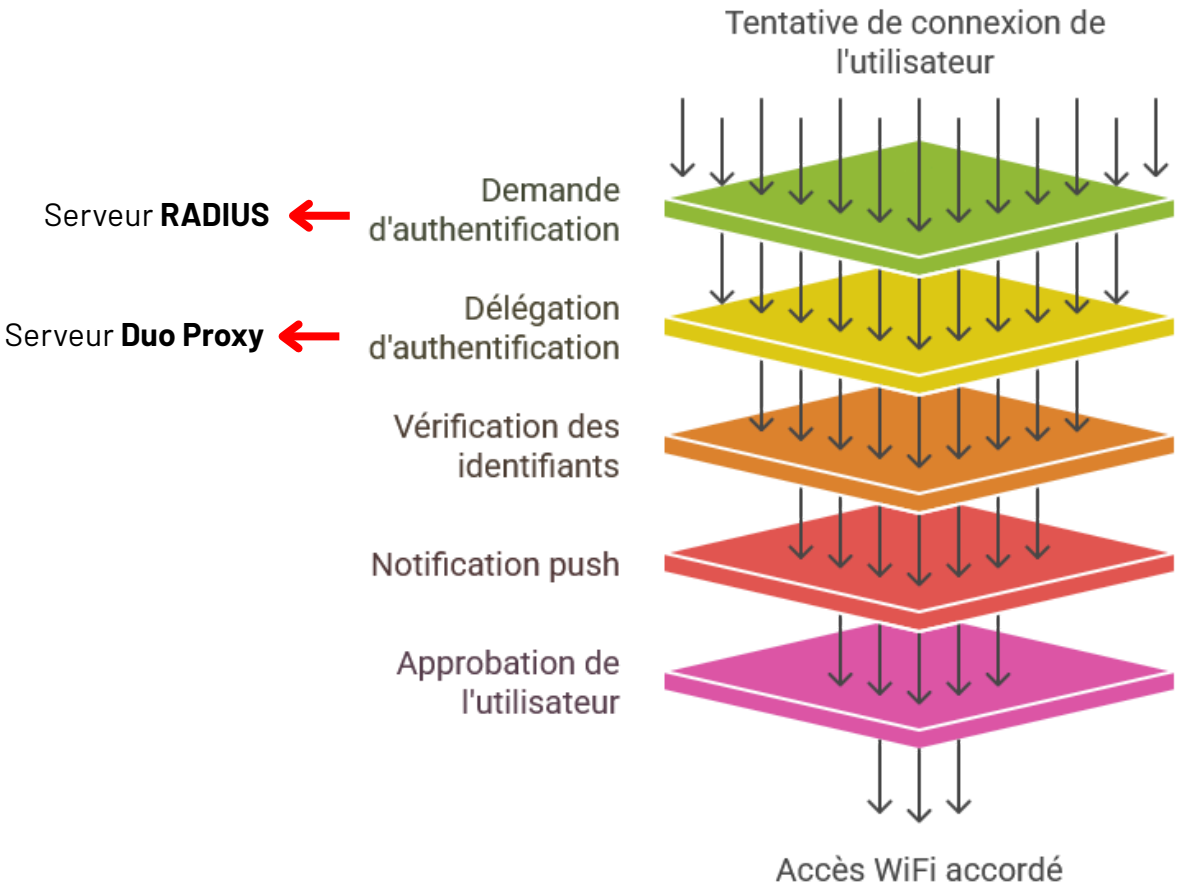
Il s'agit de l'application mobile que l'utilisateur installe sur son téléphone (Android ou iOS)
Elle permet de recevoir une notification **"push"** quand une connexion est en cours, pouvoir valider ou refuser une tentative de connexion en un seul clic et générer des codes de sécurité même hors ligne.

Fonctionnement de l'authentification

L'utilisateur tente de se connecter au WiFi d'entreprise :

1. Le contrôleur WiFi (ou switch) fait une demande d'authentification au serveur RADIUS.
2. Le serveur RADIUS délègue l'authentification à Duo Proxy, il envoie donc la requête au serveur Duo Proxy.
3. Le Duo Authentication Proxy vérifie les identifiants de l'utilisateur (via RADIUS).
4. Si les identifiants sont corrects, le Proxy envoie une requête à Duo Cloud (admin.duo.com).
5. Duo Cloud envoie alors une notification Push à l'utilisateur sur son téléphone.
6. L'utilisateur approuve la demande 2FA sur son téléphone.
7. Duo renvoie une réponse au Proxy qui valide l'authentification.
8. Le Proxy retourne "OK" au serveur RADIUS et l'accès WiFi est accordé.
9. L'utilisateur est connecté, et selon les règles, placé dans son VLAN.

Processus d'authentification WiFi



Configuration du Duo Authentication Proxy

Prérequis :

Serveur dédié → Dans cet exemple, le serveur est sur une VM Ubuntu en **192.168.200.102**

Compte Duo Security → Un compte Duo Security a été créé au préalable

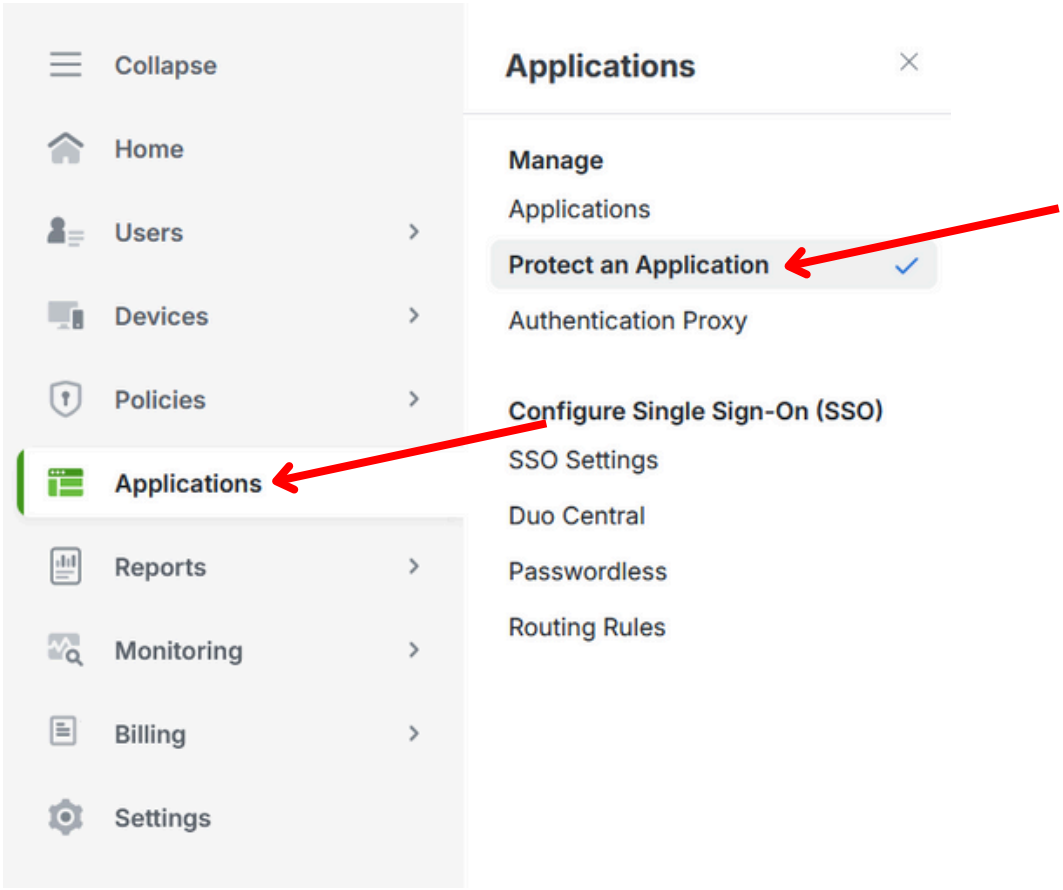
Accès à la console WiFi → La borne WiFi est en **172.16.0.10** et s'administre depuis son interface web

Serveur RADIUS actif → Le serveur RADIUS est une VM Windows server en **172.16.0.26**

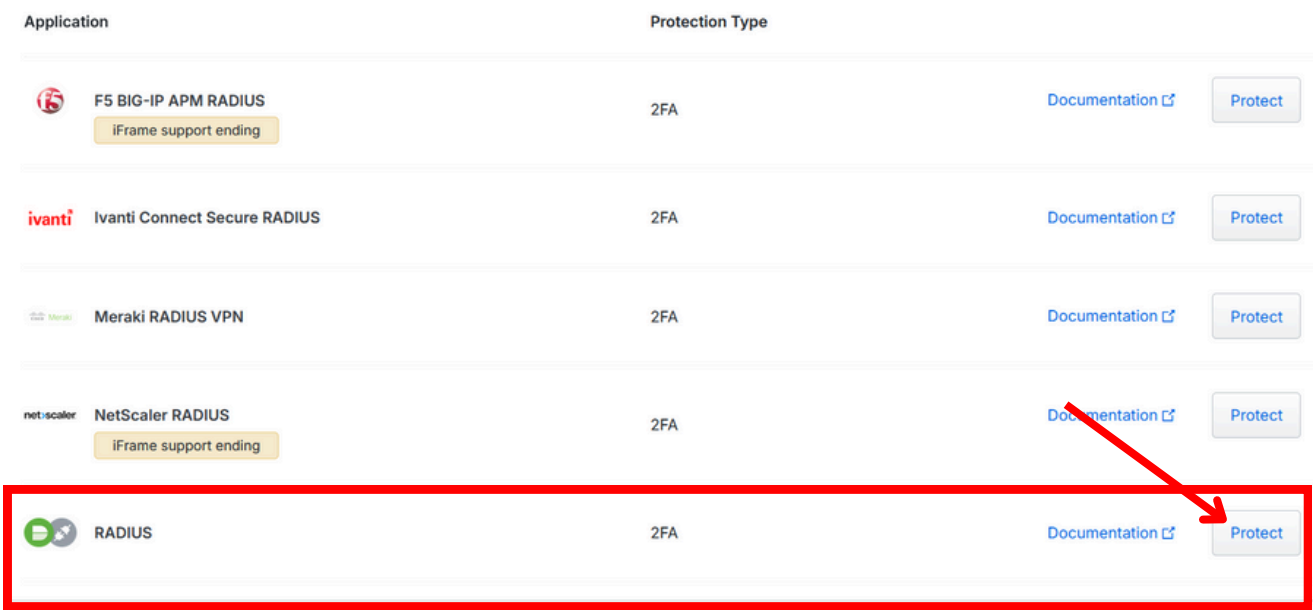
Accès Internet → Le serveur Duo Proxy a accès à internet pour pouvoir contacter Duo

Etape 1. Création de l’application RADIUS depuis l’Admin Panel de DUO

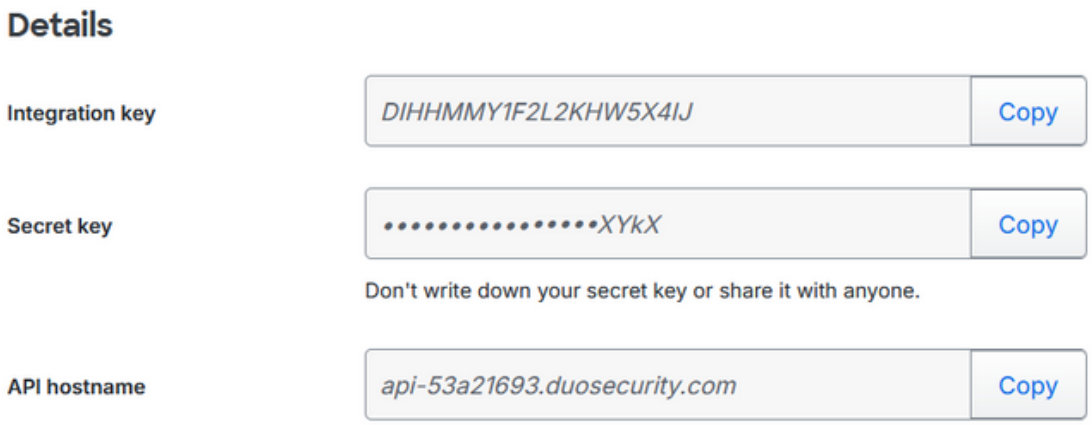
Aller sur le site de duo et se connecter avec ses identifiants admin, ensuite aller dans “Applications” puis cliquer sur “Protect an Application”.



Dans la barre de recherche, taper “Radius” et chercher RADIUS dans les propositions. Ensuite, lorsqu’il est trouvé, cliquer sur le bouton “Protect”.

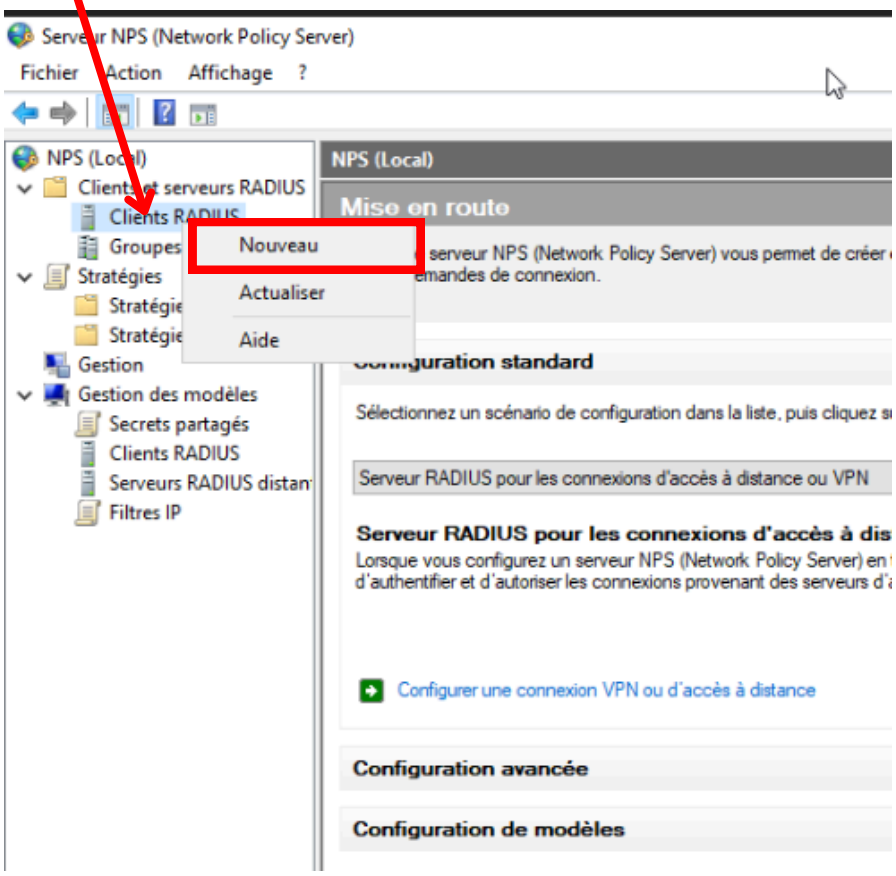


Une page va alors s’ouvrir, le champs “details” affiche plusieurs informations à retenir ; l’integration key, la secret key et l’API hostname.
Les copier et les mettre de côté dans un fichier texte.



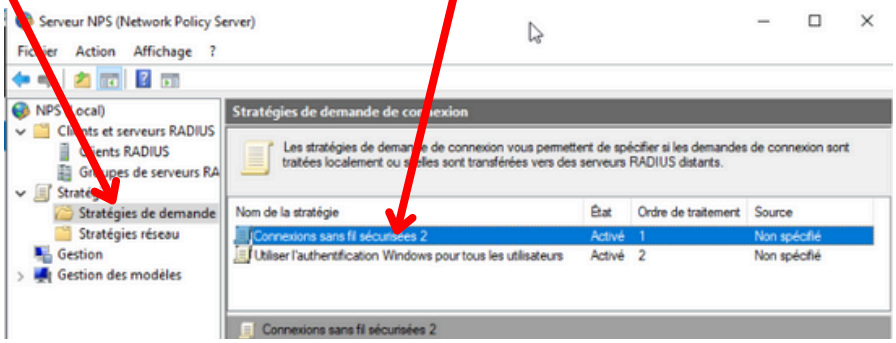
Etape 2. Ajout du serveur Proxy DUO comme client RADIUS

Se rendre sur le serveur RADIUS et ouvrir NPS, ensuite dans le menu, cliquer droit sur “Clients Radius” puis cliquer gauche sur “nouveau”:

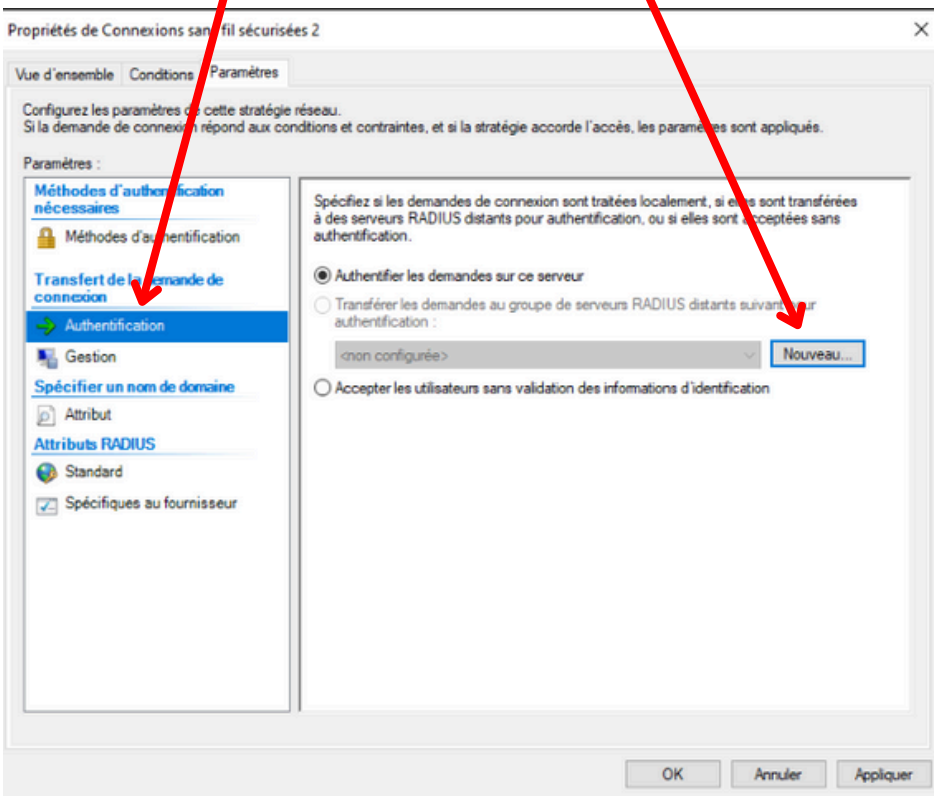


Etape 3. Modification des stratégies de connexions sur le serveur Radius

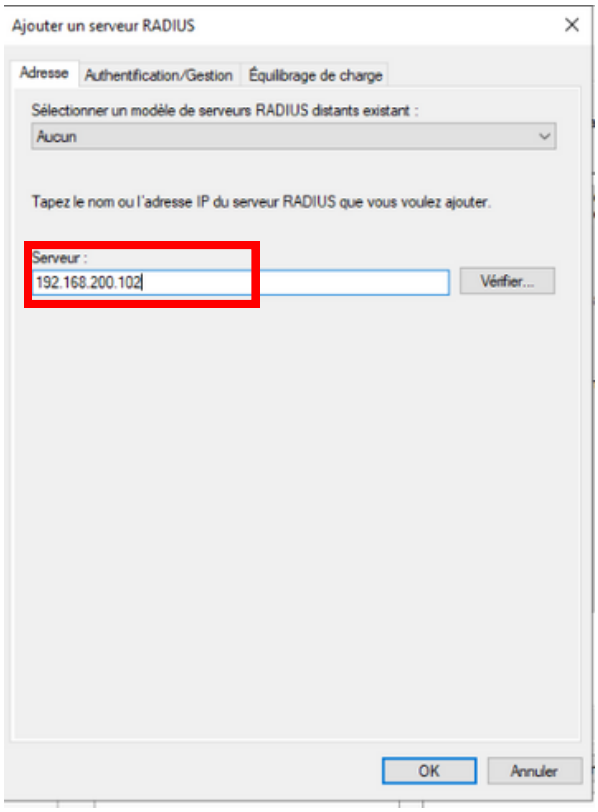
Pour faire en sorte que toute requête Wi-Fi soit transférée au Duo Proxy, il faut modifier les stratégies de connexion NPS.
Pour cela, aller sur le serveur Radius et lancer NPS, cliquer sur “Stratégies de demande de connexion”, puis cliquer sur la stratégie de connexion wifi.

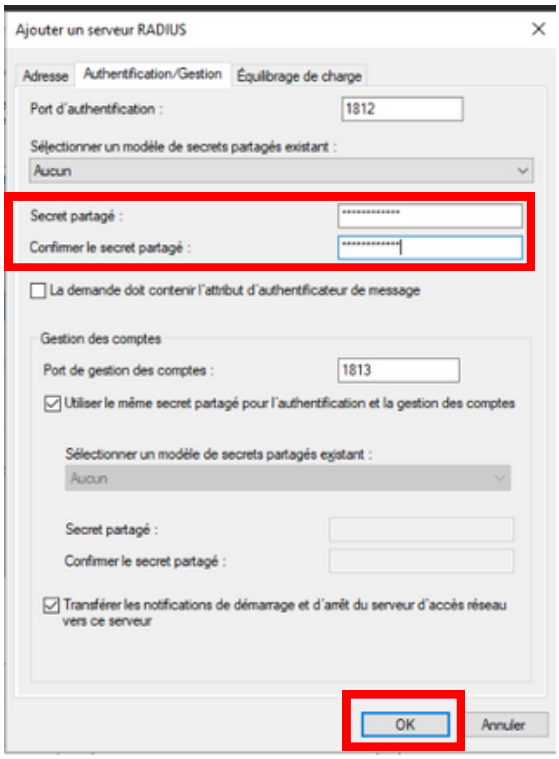


Cliquer ensuite sur “Authentification” puis sur “Nouveau”



Renseigner l'IP du serveur proxy et cliquer sur vérifier, ensuite aller dans Authentification/Gestion
Remplir dans le champs le secret partagé cliquer sur OK.





Le serveur Proxy a été configuré sur le Radius et peut maintenant être interrogé lors d'une tentative de connexion au Wifi, cliquer sur "Appliquer" puis sur "OK".