Fiche de Synthèse - Projet de Sécurisation des Accès Réseau (RADIUS)

Ce document présente la fiche de synthèse du projet de sécurisation des accès réseau, réalisé dans le cadre de mon stage de 2ème année de BTS SIO SISR. Il détaille le contexte, les défis techniques, les réalisations et les compétences acquises au sein de l'organisation d'accueil.

1

Identité du Stagiaire

Nicolas EBERHARD

2

Organisation d'Accueil

SCT Ceramics (Société Céramique Technique)

3

Secteur d'Activité

Industrie de haute technologie (Médical, Aéronautique)

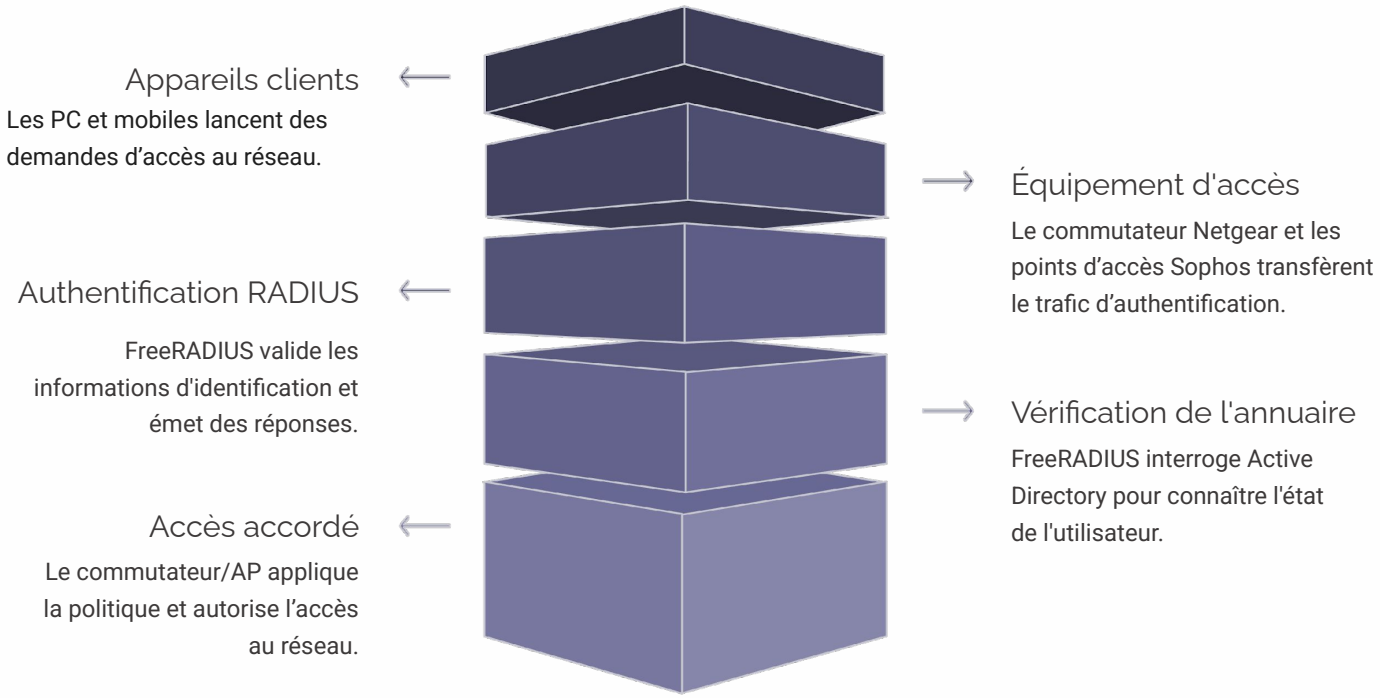
4

Problématique Clé

Centraliser et sécuriser les accès réseau (Wi-Fi et filaires) d'un site industriel sensible, tout en simplifiant la gestion des authentifications.

Architecture et Environnement Technique

Pour répondre à la problématique de sécurisation, une architecture robuste a été mise en place, s'appuyant sur des technologies éprouvées et adaptées aux exigences d'un environnement industriel de haute technologie. Cette section détaille la topologie logique du réseau et le socle technique utilisé.



Le schéma ci-dessus illustre la topologie logique de l'infrastructure d'authentification. Les clients (PC, mobiles) se connectent aux équipements d'accès (Switch Netgear, bornes Wi-Fi Sophos) qui délèguent l'authentification au serveur FreeRADIUS. Ce dernier vérifie les identifiants auprès de l'Active Directory via LDAP, garantissant une gestion centralisée des utilisateurs.

Le Socle Technique

Système d'Exploitation
Red Hat Enterprise Linux 9 (RHEL 9)

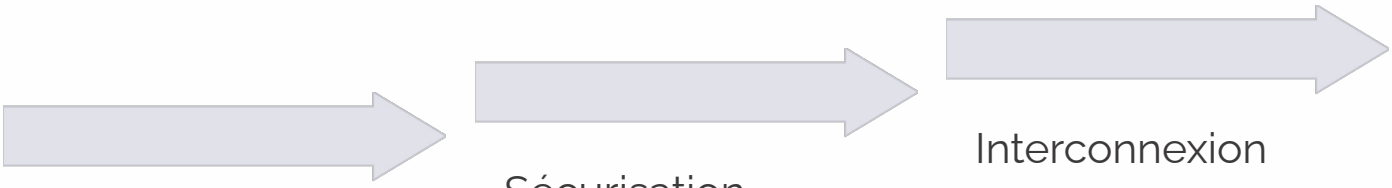
Serveur d'Authentification
FreeRADIUS 3.0

Interface de Gestion
daloRADIUS (Web et Logs)

Annuaire d'Utilisateurs
Active Directory (via LDAP)

Réalisations Techniques et Missions Clés

Ce projet a impliqué plusieurs missions techniques cruciales, chacune contribuant à l'établissement d'une solution d'authentification robuste et sécurisée. Mes interventions ont couvert l'installation, la configuration et l'intégration de différents composants pour assurer une protection optimale des accès réseau.



Déploiement du Serveur d'Authentification

- Installation complète de la pile LAMP (Linux, Apache, MariaDB, PHP).
- Configuration minutieuse du service FreeRADIUS.
- Mise en place de certificats SSL/TLS pour sécuriser tous les échanges.

Sécurisation Réseau Filaire et Sans-Fil

- Configuration du protocole 802.1X sur le Switch Netgear M4300 pour les accès filaires.
- Paramétrage de l'authentification WPA2-Entreprise sur les bornes Wi-Fi Sophos.

Interconnexion LDAP et Filtrage Granulaire

- Intégration transparente entre FreeRADIUS et l'Active Directory via LDAP.
- Développement de scripts (inner-tunnel) pour restreindre l'accès à certains SSID en fonction des groupes Active Directory des utilisateurs.

Chacune de ces étapes a été essentielle pour construire une solution d'authentification centralisée qui non seulement renforce la sécurité, mais offre également une flexibilité de gestion pour les administrateurs réseau de SCT Ceramics.

Analyse et Bilan du Projet

Le projet a été riche en apprentissages, avec des défis techniques surmontés et une consolidation significative de mes compétences. Cette section récapitule les principales difficultés rencontrées, les solutions apportées et les compétences acquises au regard du référentiel BTS SIO SISR.

Difficultés Rencontrées et Solutions

Bug MSCHAPv2 : Un problème d'encodage des caractères spéciaux a été identifié lors de l'utilisation de mots de passe complexes de l'Active Directory avec MSCHAPv2.

Solution : Ce bug a été résolu par l'ajustement des bibliothèques de traitement du module MSCHAP de FreeRADIUS, assurant ainsi la compatibilité avec tous les types de mots de passe.

Compétences Acquises (Référentiel SISR)

o

B1.3 : Installer et configurer des éléments d'infrastructure

Maîtrise du déploiement de serveurs d'authentification (FreeRADIUS) et de leur intégration dans un environnement réseau existant.

o

B1.4 : Assurer la continuité de service

Développement de compétences en diagnostic et dépannage via l'utilisation d'outils comme `radiusd -X` pour identifier et résoudre les problèmes.

o

Sécurité des Systèmes

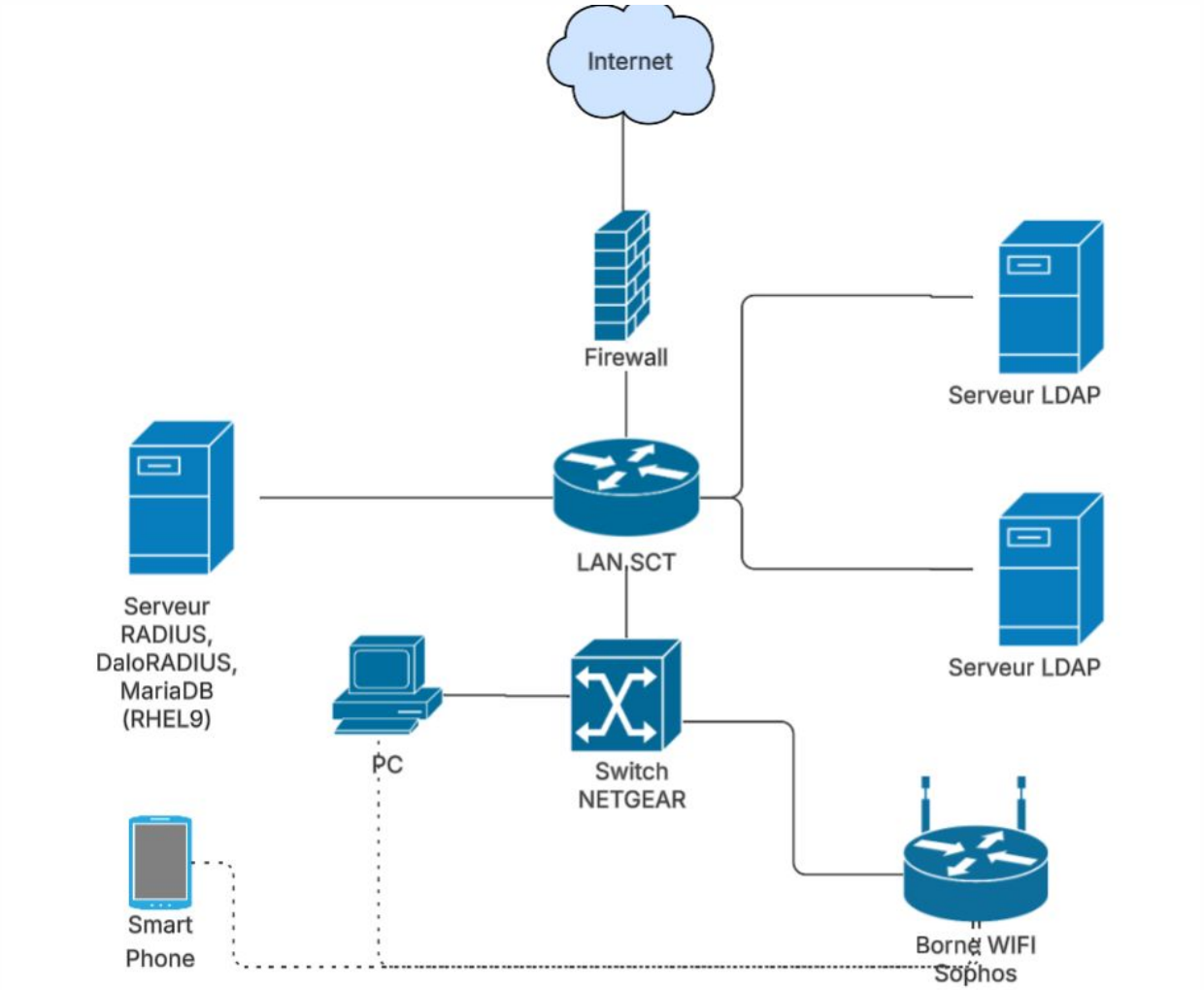
Compréhension approfondie des enjeux de sécurité liés à l'authentification centralisée et mise en œuvre de solutions robustes (802.1X, WPA2-Entreprise).

Conclusion du Projet

> La solution FreeRADIUS mise en place permet désormais à SCT Ceramics de garantir que seuls les équipements autorisés accèdent au réseau. Elle offre une traçabilité complète des connexions, renforçant ainsi la posture de sécurité globale de l'entreprise face aux menaces internes et externes. Ce projet a été une opportunité unique de concrétiser mes connaissances théoriques en compétences opérationnelles et de contribuer activement à la sécurité d'une infrastructure critique.

Annexes & Preuves de Mise en Œuvre

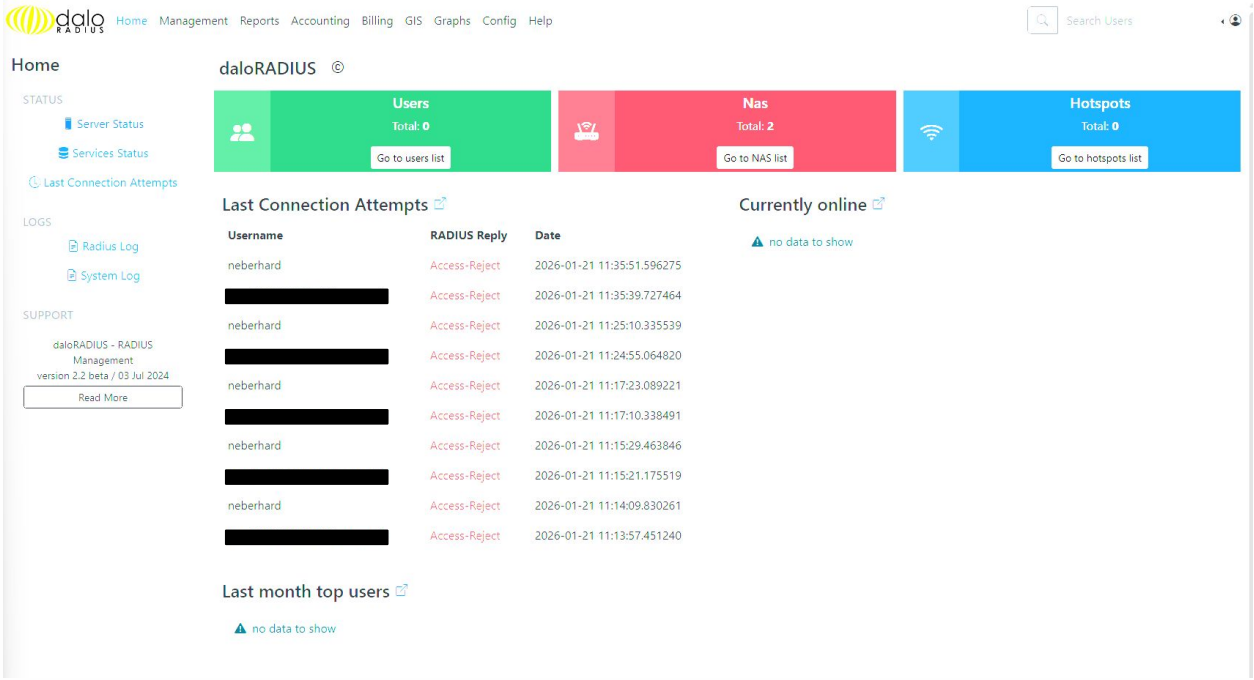
Architecture de test (Bac à sable) :



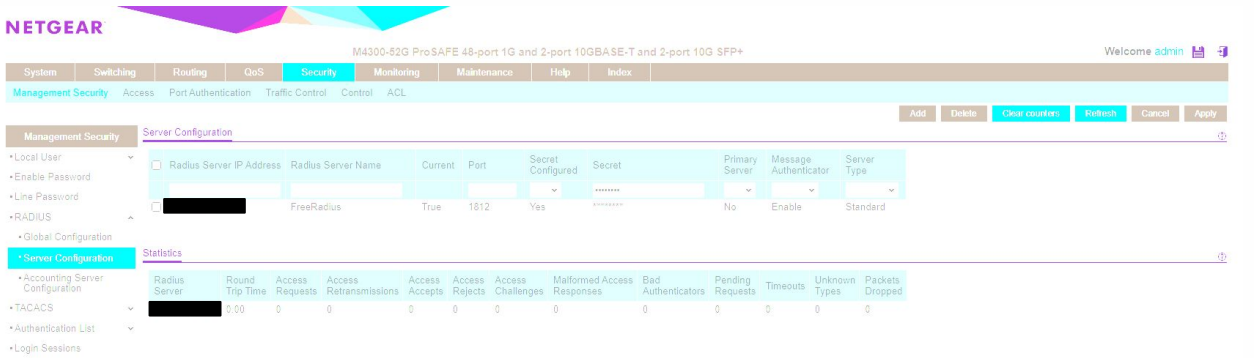
Logs de tests : Extrait de la commande `radiusd -X` validant une authentification par Login/Password et par Certificat.

```
(5) Login OK: [user@example.org] (from client Switch port 23 cli
(5) Sent Access-Accept Id 195 from                to                length 178
(5)   MS-MPPE-Recv-Key = 0x663c43dc348b424461d8552457de466d64ead7fdb147d4bd4e7e338db527d8f4
(5)   MS-MPPE-Send-Key = 0xc841abec8bbdcdde1a91f8c208fac1526ef7f523432764d7d4a20a53a7743ee4
(5)   EAP-Message = 0x03800004
(5)   Message-Authenticator = 0x00000000000000000000000000000000
(5)   User-Name = "user@example.org"
(5) Finished request
(8) Login OK: [anonymous] (from client Switch port 23 cli
(8) Sent Access-Accept Id 14 from                to                length 171
(8)   User-Name = "neberhard"
(8)   MS-MPPE-Recv-Key = 0xf2099a4375ae14c7f8dc40749cbc7db90d46024680081b0f8c859aca8c0a35ab
(8)   MS-MPPE-Send-Key = 0x41b725aa61f8e4f7cc682e43814e58ad68053322539ddedfb3550ce059cfd66d
(8)   EAP-Message = 0x03160004
(8)   Message-Authenticator = 0x00000000000000000000000000000000
(8) Finished request
```

Captures d'écran d'administration : Interface de gestion **daloRADIUS** montrant le tableau de bord opérationnel.



Configuration du **Switch Netgear** (déclaration du NAS et secret partagé).



Capture radiusd -X : Interface montrant les logs de connexion avec les noms d'utilisateurs provenant de l'AD.

Capture de configuration Sophos : Vue de l'interface "Wireless Security" montrant le pointage vers le serveur RADIUS et le mode WPA2-EAP.

Extrait de configuration inner-tunnel : Code source montrant la structure `if` et l'appel au `LDAP-Group`.

```
server inner-tunnel {
    authorize {
        if (User-Name =~ /^host\//) {
            update control {
                Auth-Type := Reject
            }
        }

        filter_username
        preprocess

        # On utilise Called-Station-Id (qui contient l'adresse MAC + le SSID)
        if (outer.request:Called-Station-Id =~                ) {

            # On appelle le module LDAP pour charger les groupes
            ldap

            # SI l'utilisateur n'est PAS dans le groupe, on REJETTE direct
            if (!(LDAP-Group ==                                )) {
                update reply {
                    Reply-Message = "Acces refuse : Groupe incorrect"
                }
                reject
            }
        }

        mschap
        -ldap
        eap
}

    authenticate {
        eap
        Auth-Type MS-CHAP {
            mschap
        }
    }

    post-auth {
        ldap
        if (session-state:User-Name) {
            update reply {
                User-Name = "%{session-state:User-Name}"
            }
        }
        sql
    }
}
```