Université Cadi Ayyad
Ecole Nationale des Sciences Appliquées de Safi
Département Informatique, Réseaux et
Télécommunications (IRT)

**RAPPORT D'AVANCEMENT**

# Etude, choix, et déploiement d'une solution de control d'accès au réseau pour une PME

Réalisé par :
**Anas SIDKI**
**Safaa SNINI**

Effectué a :
**SECUREDATA – Casablanca**

Encadré a l'ENSAS par :
**Dr Hakim EL-BOUSTANI**

Encadré a SECUREDATA par :
**Monsieur Jamal AZZA**

# Introduction générale

La sécurité des réseaux devient, de nos jours, un thème indispensable pour garantir la disponibilité et l'efficacité des ressources sur le réseau. La spécification de l'accès au réseau est devenue très importante pour la protection des ressources des tentatives d'intrusions internes ou externes, ainsi que des accès aux données et informations de haute importance ou très confidentielles, par des membres non qualifiés. C'est pour cela que chaque utilisateur ou machine, voulant accéder au réseau, doit être identifié et doit subir quelques tests de compatibilité avec le réseau (intégration au domaine, existence d'un antivirus bien défini sur la machine qui veut s'authentifier, etc.) ; il sera, par la suite, attribué selon son identité et les droits d'accès qui lui seront attribués vers les ressources et les sous réseaux auxquels il aura accès.

Ce mémoire présente le travail qu'on avait effectué au sein de l'entreprise SECUREDATA dans le cadre d'un stage de fin d'études en cycle d'ingénieur en génie Télécommunications et Réseaux. Il s'agit de l'étude, le choix et le déploiement d'une solution de control d'accès au réseau pour une PME.

Le contrôle d'accès au réseau (Network Access Control ou NAC) est une approche de la sécurité informatique qui tente d'unifier les technologies des périphériques de sécurité, l'identifiant ou le système d'authentification et l'application de la sécurité réseau. Les critères essentiels d'une solution NAC sont la performance, la sécurité, la facilité d'utilisation et la capacité à gérer de nouvelles pratiques des PME.

La solution NAC qu'on va déployer apporte une visibilité sur les appareils connectés sur l'infrastructure du Datacenter à l'extrémité, donne un contrôle d'accès à l'infrastructure WAN et LAN tout en gardant la dynamique de l'infrastructure réseaux ainsi que la prise en charge des utilisateurs externe de l'entreprise.

# Problématique

« La donnée est au cœur de ce monde sans couture », c'est ce qu'a soutenu Isabelle Falque Pierrotin, présidence de la Commission Nationale de l'Informatique et des Libertés (CNIL). Les données sont aujourd'hui à l'épicentre des enjeux de conformité rencontrés à travers le monde qui est profondément marqué par des cyberattaques de plus en plus fréquentes.

En 2015, 8 entreprises françaises sur 10 ont été attaquées. Ces attaques prennent des formes très diverses, du ransomware (61 %) au déni de service (38 %) en passant par la défiguration de site web (23 %) ou encore le vol de données personnelles (18 %). Philippe Trouchaud, expert en cybersécurité associé au sein du cabinet PwC, affirme que 35 % des incidents sont générés par des collaborateurs internes à l'entreprise qui s'est amplifié avec l'amplification du phénomène de BOYD.

Cependant, toutes les infractions ne sont pas intentionnelles. La grande majorité des incidents de cybersécurité sont, en fait, accidentels. C'est ce qui rend la menace interne si risquée. Des employés dignes de confiance peuvent se tromper ou se faire voler leurs identifiants sans que ce soit de leur faute. Les erreurs et la négligence des employés sont les principales causes des violations de données, et non l'intention malveillante.

D'où l'importance d'utiliser un système de sécurité pour garder les informations sensibles en lieu sûr et empêcher leur divulgation et de s'assurer que ces dernières sont entre les mains de personnes qui ont les droits d'en disposer.

Notre projet consiste donc à déployer une solution qui a pour but de protéger l'accès au réseau d'entreprise sous différentes formes tel que le contrôle d'accès de l'utilisateur que ça soit interne ou externe, l'authentification de la machine et la vérification du respect des postes clients aux règles de sécurité imposées par l'entreprise.

# Les objectifs

L'objectif général de ce projet est de présenter une compréhension approfondie du concept de contrôle d'accès au réseau et de son fonctionnement essentiel, ainsi que de déployer la solution NAC proposée par Extreme Networks qui est l'un des leaders du marché du réseaux.

Objectifs de la mise en place d'une solution NAC :

- Visibilité
  - Avec Quoi, Comment, Quand et Qui se connecte à l'infrastructure réseau.
- Contrôle d'accès à l'infrastructure
  - Supprimer le « libre accès sur le réseau ».
  - Identité de l'utilisateur.
  - IoT
- BYOD Mobilité (Bring Your Own Device)
  - Politique d'accès des équipements personnels (Wireless et Lan).
  - Rendre dynamique l'infrastructure réseau.
- Prise en charge des utilisateurs externe à L'entreprise
  - Invités
  - Intervenants (Consultants, etc.)
- Conformité à la politique de Sécurité
  - De l'accès
  - De l'utilisation

# Plan du rapport

**Chapitre I** : Présentation du contexte général du projet

**Chapitre II** : Etude contrôle d'accès au réseau et choix de solution

I. Introduction
II. Mécanisme de contrôle d'accès Réseaux
    1. Définition de contrôle d'accès Réseau
    2. Fonctionnement et mécanisme de contrôle d'accès Réseaux
    3. Comparaison des deux situations avec et sans NAC
    4. Les différentes solutions de NAC
III. La virtualisation
IV. Conclusion

**Chapitre III** : Déploiement d'une solution NAC d'Extreme Networks

I. Introduction
II. Déploiement de la solution NAC Extreme dans l'architecture réseau de l'entreprise
    1. Etude de cas
    2. Les composants utilisés dans le déploiement de la solution NAC Extreme
    3. Etapes de pré-configuration des composants NAC
    4. Etapes de configuration

**Chapitre IV** : Test et validation de la solution NAC Extreme Networks