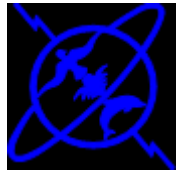


UNIVERSITÉ MOHAMMED V – AGDAL
FACULTÉ DES SCIENCES
Rabat

Le contrôle d'accès réseau et la prévention d'intrusion

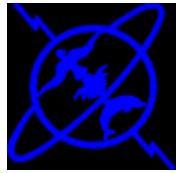
Présentée par

Abdelmajid Lakbabi

(Doctorant sous l'encadrement du Professeur Said Elhajji)

Discipline : Informatique
Spécialité : Sécurité des réseaux informatiques

Université Mohammed V
AGDAL - RABAT



Sommaire

I. Introduction & Motivation

- **Complexité des réseaux**
- ***sophistication des attaques***
- **complexité des solutions de sécurité**

II. Network Access Control (NAC)

1. *NAC - Etat d'art technologique*

- **Mécanisme et fonctionnalités de Base**
- **Topologie et architecture**
- **Limitations des solutions commerciales actuelles**

2. *Standardisation – Ouverture et interfaçage Multi-vendeurs*

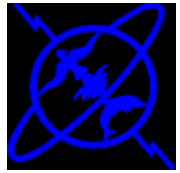
- **Trusted Network Connect (TNC)**
- **Architecture de base et flux**
- **Extensions et interfaçage**
- **Support TPM**

III. Conclusion & perspectives

Tendre vers une architecture :

- **Standardisée**
- **Ouverte**
- **Intégrable aux solutions de prévention d'intrusion actuelles**
- **Répondant aux récentes menaces, liées à l'évolution technologique, la complexité, et l'ouverture des réseaux modernes**

Université Mohammed V
AGDAL - RABAT



Résumé:

Introduction & Motivation

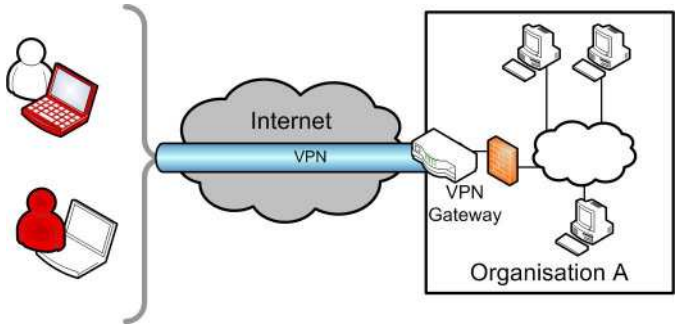
- Nature changeante des structures réseaux
  - Du statique et homogène vers dynamique et hétérogène
  - Les nœuds mobiles se connectent et communiquent avec les différentes parties du réseau (câbles, wifi et VPN)
    - Les invités, consultants, contractuels, ou stagiaires …
    - Utilisant leurs portables, PC, Mac ou Smartphones & tablet
- Les Hackers adaptent leurs stratégies
  - ciblent les parties vulnérables du réseau « «endpoints »
    - Vol de de mot de passe, de sessions, ou d'informations privées

- Usurpation d'identité et manipulation des privilèges de l'utilisateur
- Etablissement de réseau de type Botnet

- Les terminaux réseaux constituent une réelle menace pour les réseaux interconnectés

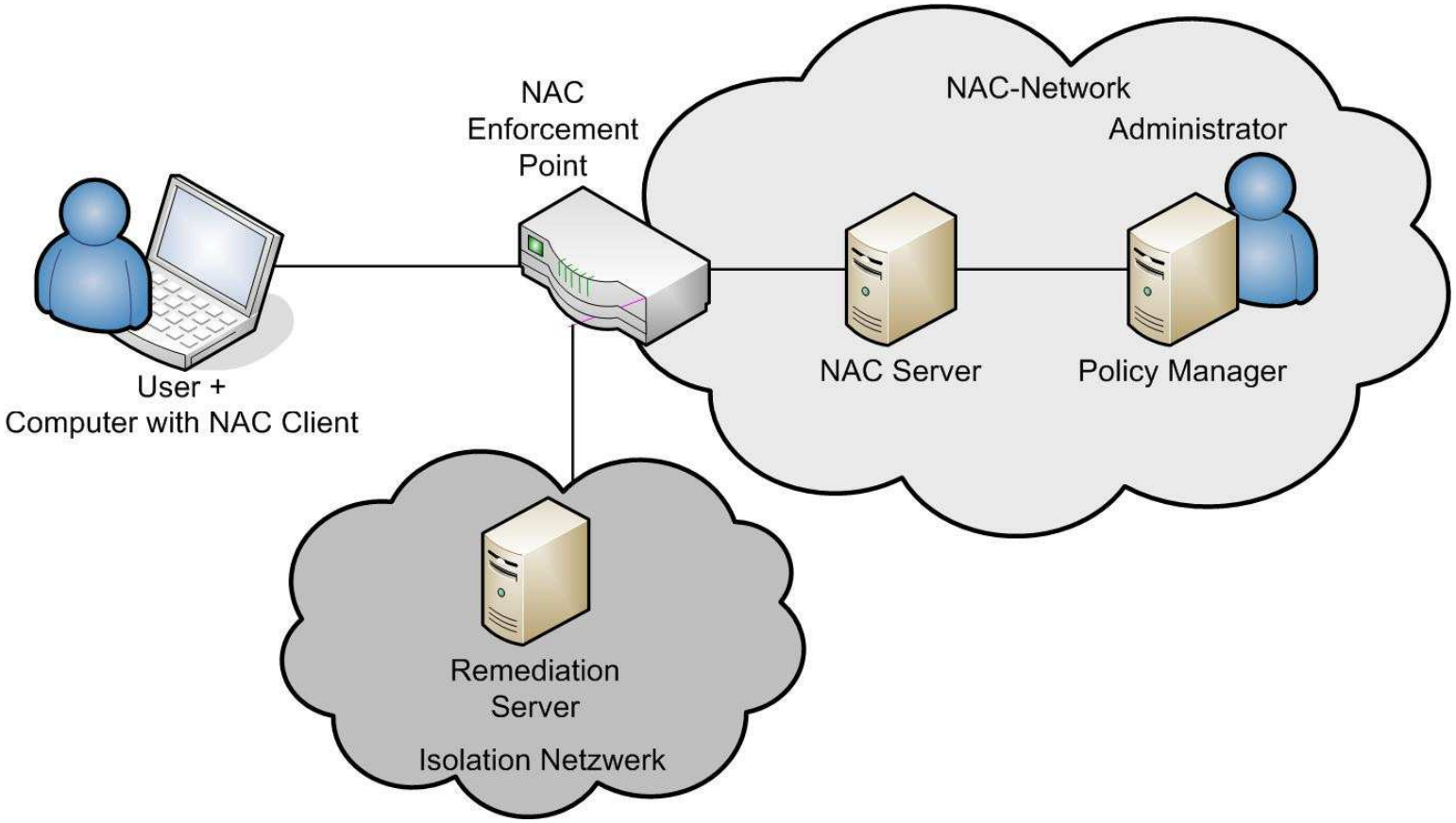
  Les mécanismes classiques tels que les

  Firewalls, IDS, VPNs, et l'authentification des utilisateurs ne permettent plus de neutraliser les nouvelles menaces



De quoi on a besoin alors ?

Plateforme de sécurité répartie



Phase d'admission

- Authentification de l'utilisateur
- Vérification de l'intégrité de l'équipement utilisé pour se connecter
- Comparer le statut d'intégrité résultant à la politique de sécurité globale
- Décider quel type d'accès sera accordé à l'utilisateur
- Où sera fait ce contrôle ?
-

Phase d'après Admission

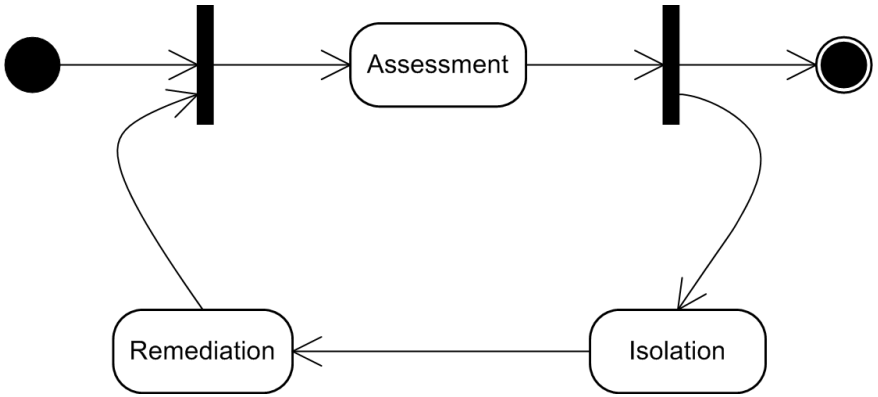
Phase critique, il s'agit de superviser et contenir tout comportement anormal des équipements & utilisateurs déjà connecté au réseau

- Supervision continu du réseau avec la capacité de réagir en cas de besoin
- Intégration des équipements de détection d'intrusion et de corrélation d'événements afin de réagir adéquatement au trafic illicite.

Standardisation

Trusted Network Connect (TNC)

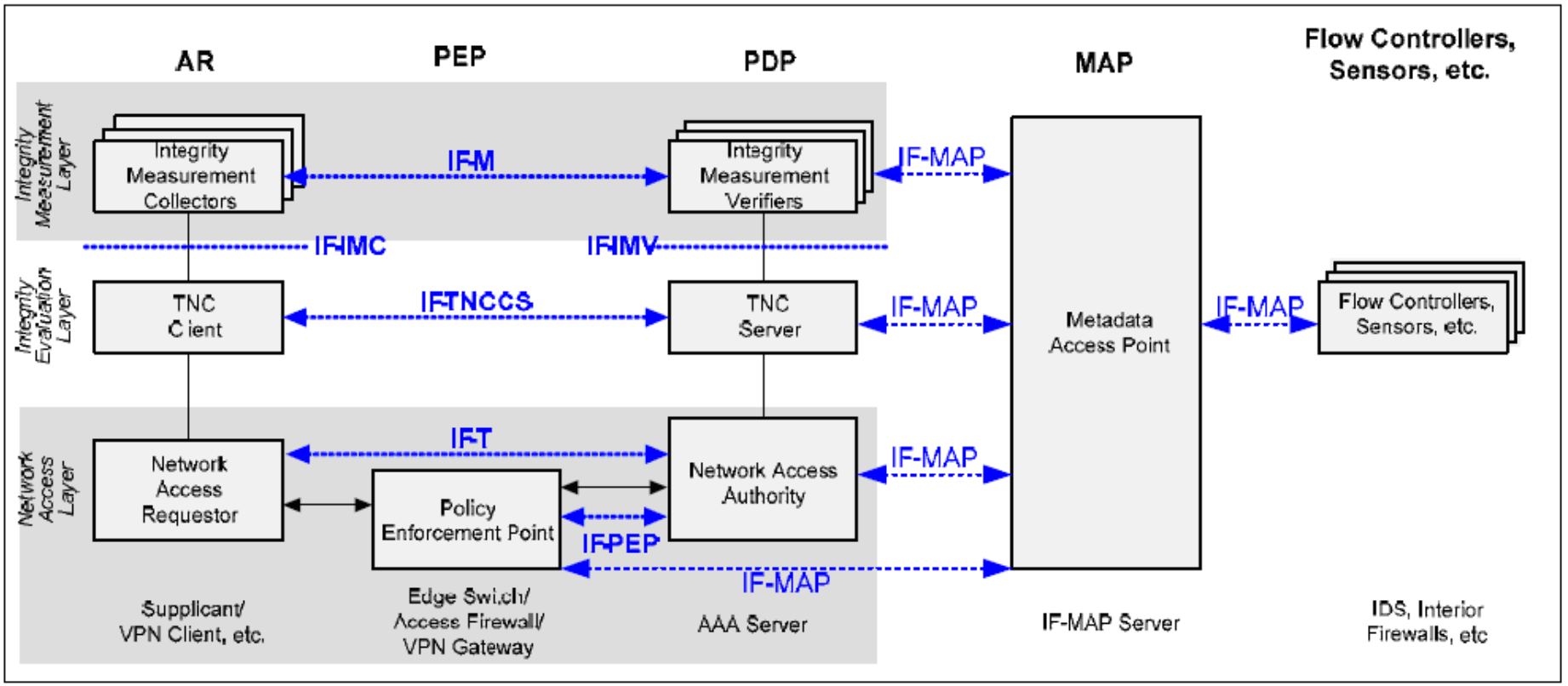
- Architecture ouverte pour le NAC
  - Spécifié par TNC sous-groupe de TCG
  - Spécifications disponible pour le grand Public
    - Garantir l'interopérabilité entre les différents constructeurs
  - Support de technologies existantes (802.1X, EAP)
    - Le cycle TNC consiste en 3 phases "Handshake":



- Assessment
  - TNC Authentification
    - Identité + intégrité de la plateforme
- Isolation
  - Quarantaine des nœuds non-conformes
- Remediation
  - Application des Patches et correctifs

Université Mohammed V
AGDAL - RABAT

Standards et Flux



Intégration IPS & TPM au NAC

- La perspective est d'intégrer, tous les composants de prevention d'intrusion et de corrélation d'évènements au système NAC, afin de prendre la décision adéquate envers nœuds à problème au sein du réseau.

- Le Trusted Platform Module (également nommé puce TPM), Ce chipset est présent sur presque tous les modèles d'ordinateurs portables, nous permettra d'enregistrer et valider l'état du système.

- Permet de vérifier l'intégrité du système
- Authentifie le résultat de contrôle du système par le mécanisme NAC

Conclusion & perspectives

- Les Méthodes classique, s'avèrent inefficace d'où, la nécessité de proposer une plateforme ouverte et adaptée en réponse aux nouvelles menaces réseaux

Bibliographie :

Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control by Daniel Hoffman (Apr 21, 2008)

Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design by Denise Helfrich, Lou Ronnau, Jason Frazier, and Paul Forbes (Dec 18, 2006)

Role-Based Access Control, Second Edition by David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli (Jan 31, 2007)