



# DOSSIER D'INGÉNIERIE

CLIENT :	CLIENT	Assala KASSIMI	
NOM DU PROJET :	Mise en place d'un POC de contrôle d'accès ISE		
DATE :	30/04/2019	VERSION :	V1

FIGURE 1: INFRASTRUCTURE DU CLIENT .....	4
FIGURE 2 : BENCHMARKING DES SOLUTIONS .....	5
FIGURE 3 : INFRASTRUCTURE SECURISEE .....	6
FIGURE 4 : L'ARCHITECTURE ISE .....	7
FIGURE 5 : ARCHITECTURE ENTIERE DU CONTROLE D'ACCES .....	7
FIGURE 6 : FONCTIONNEMENT DU 802.1X .....	8
FIGURE 7 : LA COMMUNICATION DU SERVEUR RADIUS .....	9
FIGURE 8 : LA CONNEXION MAB .....	10
FIGURE 9 : LIEN MAB .....	11
FIGURE 10: FONCTIONNEMENT DU WEBAUTH .....	11
FIGURE 11 : LE LIEN VPN POUR LES ACCES DISTANT .....	12
FIGURE 12 : LES TYPES D'AUTORISATION .....	12
FIGURE 13 : FONCTIONNEMENT DU BYOD .....	13
FIGURE 14 : DETECTION DES EQUIPEMENTS .....	13
FIGURE 15 : PROFILING .....	14
FIGURE 16 : FONCTIONNEMENT DU GUEST .....	14
FIGURE 17 : LES TYPES DU GUEST .....	15

## SOMMAIRE

### Table des matières

Liste des figures .....	2
SOMMAIRE .....	3
L'étude de l'existant.....	4
1- Objectif du document .....	4
2- Architecture physique du client .....	4
3- Problématique .....	5
4- Benchmarking .....	5
4- La solution choisie .....	6
5- ISE: Cisco Identity Services Engine .....	6
5-1 L'architecture ISE.....	6
5-2 Les fonctionnalités du ISE.....	7

# L'étude de l'existant

## 1- Objectif du document

Le présent document est un livrable de la phase ingénierie et étude de l'existant. Il a pour objectif de décrire le périmètre des solutions et des fonctionnalités qui seront installées, de donner une étude détaillée d'ingénierie de la solution proposée par CBI à un client pour l'implémentation effective de l'infrastructure réseau et sécurité.

## 2- Architecture physique du client

Pour répondre aux besoins du client, l'infrastructure proposée est basée sur des équipements Cisco et constituée de trois couches : Accès, Distribution, et Cœur du réseau :

- Couche d'Accès : Elle se compose des utilisateurs Wired et Wireless
- Couche de distribution : Elle se compose de deux Switch Catalyst de série 4500, Serveur d'application, Serveurs RADIUS, TACACS, et ACS, Contrôleur WI-FI de série 4400.
- Couche de Cœur réseau : Elle se compose de la partie sécurité des Firewall Sophos XG, un lien VPN pour l'accès distant aux sites externes.

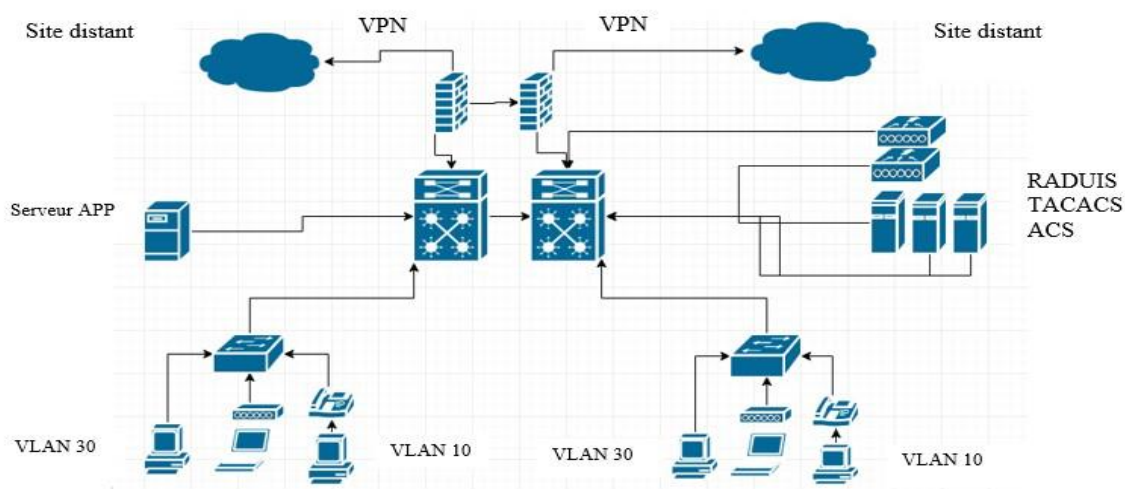


Figure 1: Infrastructure du client

### 3- Problématique

L'entreprise confronte des attaques internes et externes au sein de son réseau qui permet la propagation des intrusions, des virus, aussi, le vol des informations confidentiels. Un accès d'un utilisateur avec un matériel malveillant ou maladroit cause une intense non-conformité du réseau. Le client exprime son besoin d'avoir une plateforme qui permet de générer les systèmes, les matériels, et le réseau entier afin de réaliser une infrastructure de très haute performance de sécurité.

### 4- Benchmarking




  			
ACCÈS RÉSEAU	ISE	HPE ClearPass	ForceScout
Identification Passive	Y	N	N
EasyConnect	Y	Y	Y
802.1X	Y	Y	Limité
SAML	Y	Limité	N
TACACS +	Y	N	N
La visibilité			
La visibilité des APP	Y	N	Y
La visibilité des équipements	Y	Y	Y
L' amélioration de la visibilité des EndUsers	Y	Y	Y
IOT	Y	Y	Y
La visibilité du réseau	Y	Y	Y
La mobilité			
Guest Services	Y	Y	Limité
BYOD	Y	Y	Y
MDM	Y	Y	Y
Le service de la Location	Y	N	N
La sécurité pour les menaces			
La détection des anomalies	Y	Y	Y
Posture	Y	Y	Y
NAC	Y	N	Y
Architecture			
APIs	Y	Y	Y
SDS	Y	N	Limité
La passerelle	Y	N	N

Figure 2 : Benchmarking des solutions

## 4- La solution choisie

La nouvelle architecture du client avec la mise en place de la solution ISE pour le contrôle d'accès de l'entreprise.

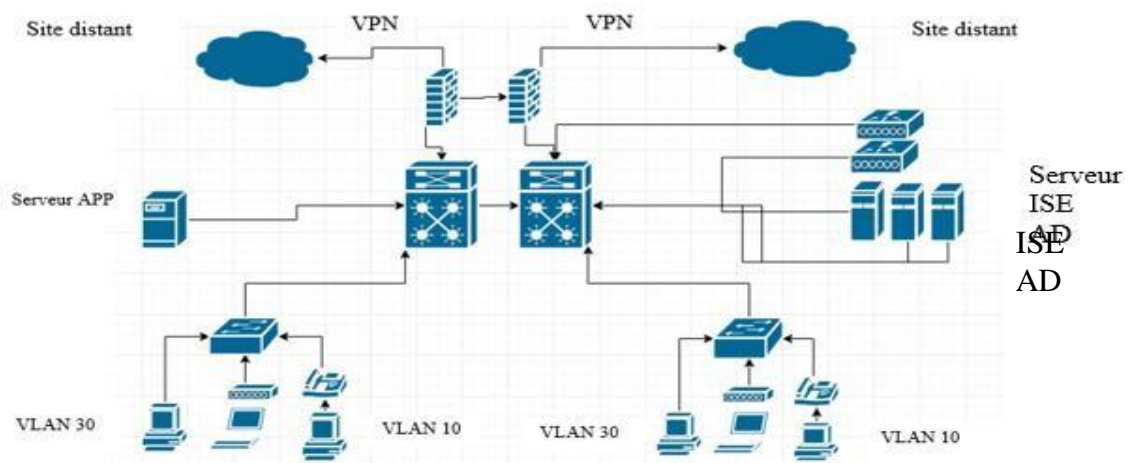


Figure 3 : Infrastructure sécurisée

## 5- ISE: Cisco Identity Services Engine



Cisco Identity Services Engine (ISE) est une plate-forme leader du réseau d'entreprise, dédiée au contrôle d'accès au réseau du client.

### 5-1 L'architecture ISE



Figure 4 : L'Architecture ISE

## 5-2 Les fonctionnalités du ISE

### Le contrôle d'accès

Cette option permet de contrôler l'accès interne ou externe au réseau du client

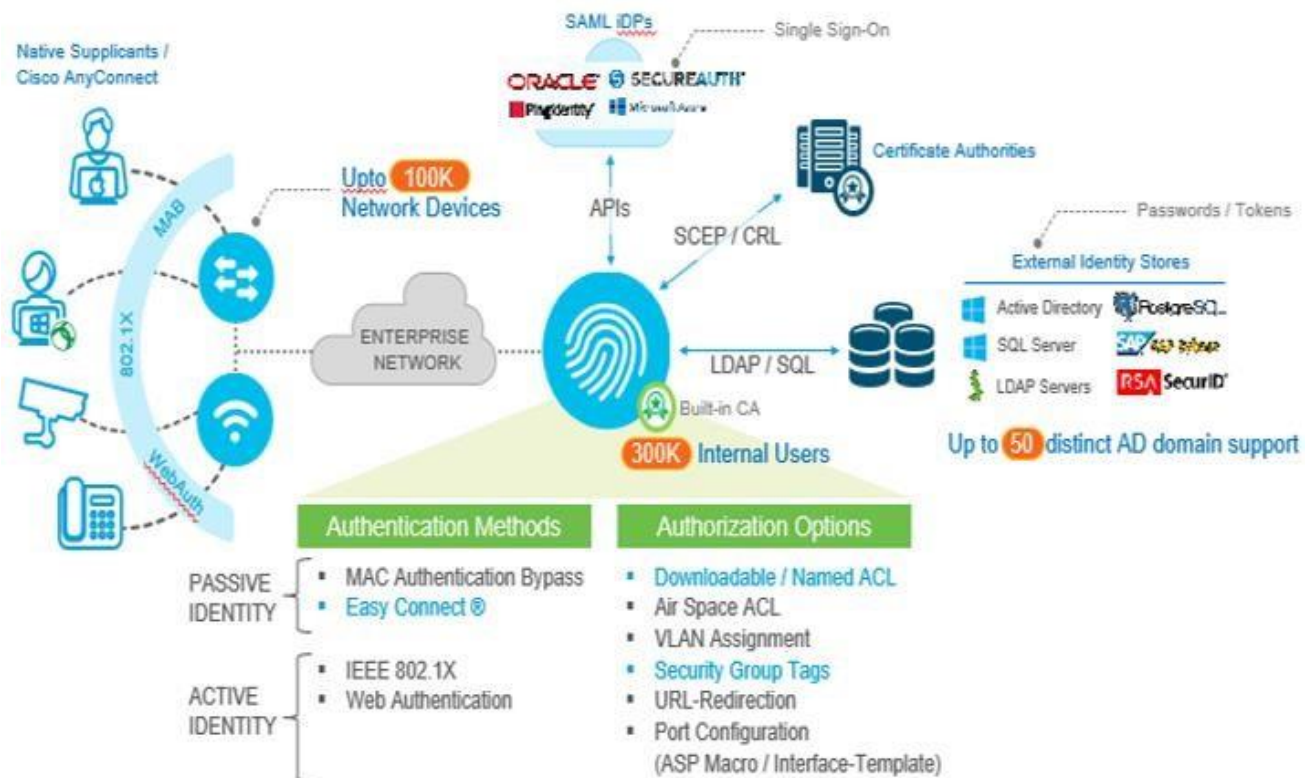


Figure 5 : Architecture entière du contrôle d'accès

### ❖ Authentification

L'authentification est une procédure, par laquelle un système informatique certifie l'identité d'une personne ou d'un ordinateur. Le but de cette procédure étant d'autoriser la personne à accéder à certaines ressources sécurisées. Il va comparer les informations des utilisateurs autorisés stockées dans une base de données à celles fournies. L'accès sera autorisé lorsque les informations sont identiques.

Les différentes authentifications sont :



La norme IEEE-802.1X permet de contrôler l'accès aux équipements d'infrastructures réseau







**CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur

Il existe une réponse appelée CHANGE PASSWORD où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe. Change-password est un attribut VSA (Vendor-Specific Attributes), c'est-à-dire qu'il est spécifique à un fournisseur, et dans ce cas, c'est un attribut de Microsoft et pour être plus précis, celui de MS-Chap v2. Il n'appartient pas aux attributs radius standard définis dans la RFC 2865. Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

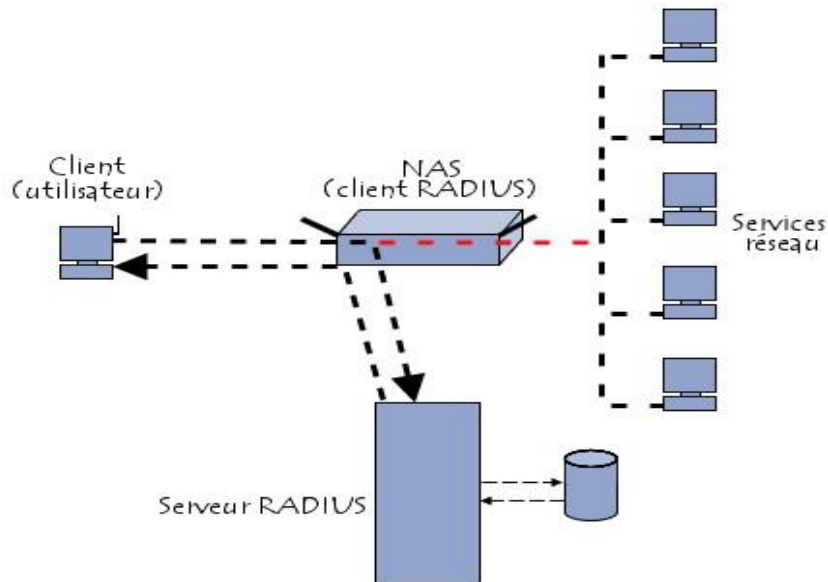


Figure 7 : La communication du serveur RADIUS

802.1X	MAB	WebAuth
--------	-----	---------

L'authentification MABypass active le contrôle d'accès basé sur le port en utilisant l'adresse MAC de l'équipement. Un port compatible MAB peut être activé ou désactivé de manière dynamique en fonction de l'adresse MAC du périphérique connecté au Switch.

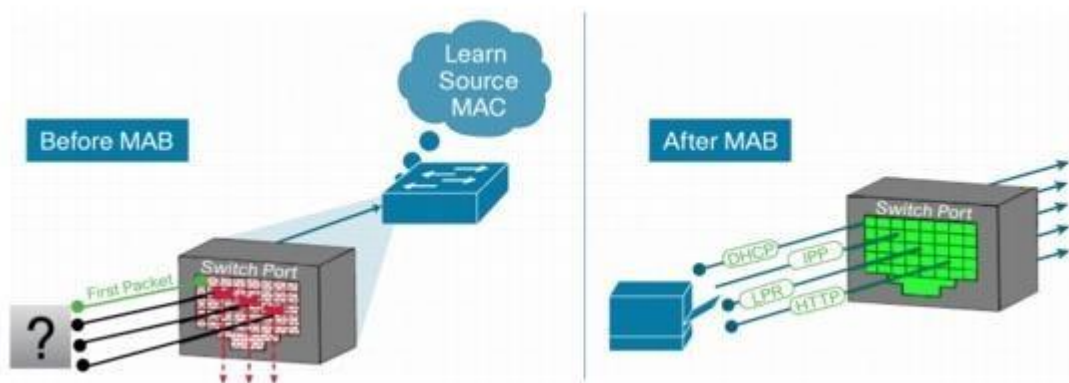


Figure 8 : La connexion MAB

Avant MAB, l'identité du système d'extrémité était inconnue et tout le trafic était bloqué. Le commutateur examine un seul paquet pour apprendre et authentifier l'adresse MAC source. Une fois que l'authentification MAB a réussi, l'identité du nœud final est connue et tout le trafic de ce nœud final est autorisé. Le commutateur effectue un filtrage de l'adresse MAC source afin de garantir que seul le point de terminaison authentifié par MAB est autorisé à envoyer du trafic.

L'authentification d'adresse MAC en elle-même n'est pas une idée nouvelle. L'un des premiers précurseurs de MAB est l'architecture VMPS (Cisco Policy Management Server) VLAN. Avec VMPS, vous créez un fichier texte contenant les adresses MAC et les VLAN auxquels elles appartiennent. Ce fichier est chargé dans le commutateur de serveur VMPS à l'aide du protocole TFTP (Trivial File Transfer Protocol). Tous les autres commutateurs vérifient ensuite avec le commutateur de serveur VMPS pour déterminer à quel VLAN appartiennent ces adresses MAC. MAB représente une évolution naturelle de VMPS. Au lieu de stocker les adresses MAC sur un commutateur de serveur VMPS, MAB valide les adresses MAB stockées dans un référentiel centralisé et pouvant être interrogées à l'aide du protocole RADIUS standard.

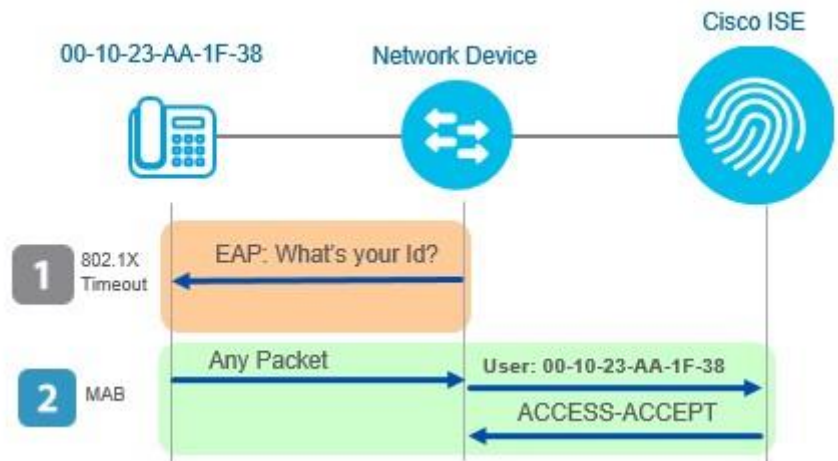


Figure 9 : Lien MAB

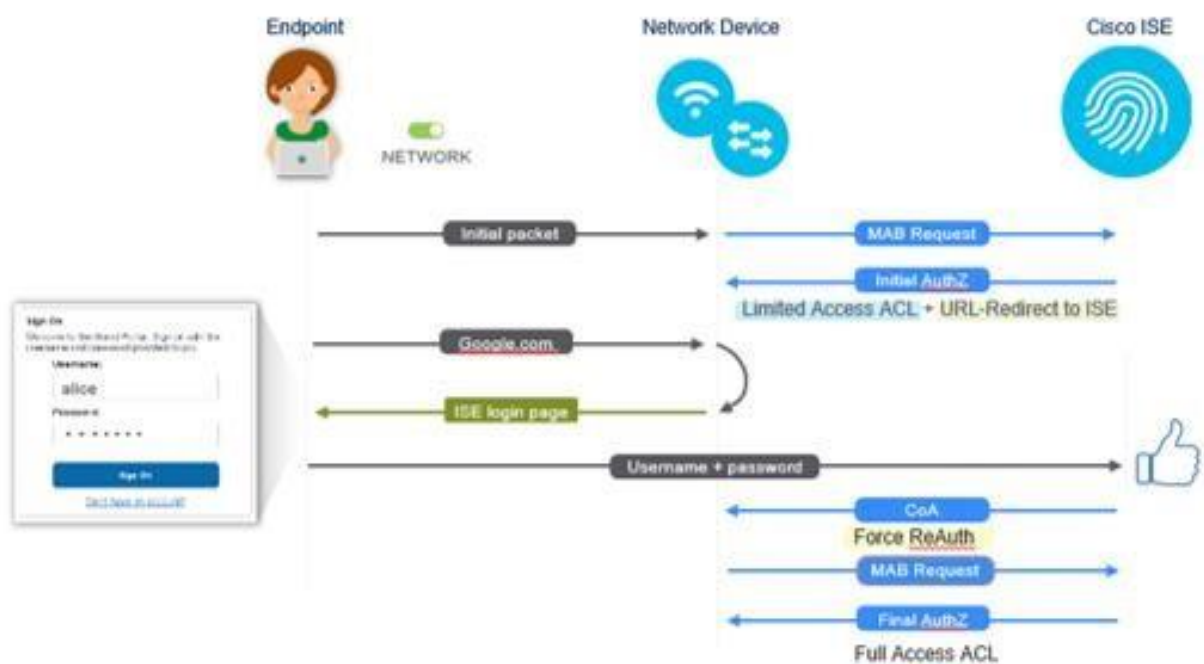


Figure 10: Fonctionnement du WebAuth



Figure 11 : Le lien VPN pour les accès distant

### ❖ Autorisation

L'autorisation peut être appliquée à des niveaux plus granulaires que les sites Web ou l'intranet d'une entreprise. Votre identité individuelle peut faire partie d'un groupe d'identités qui partagent une politique d'autorisation commune.

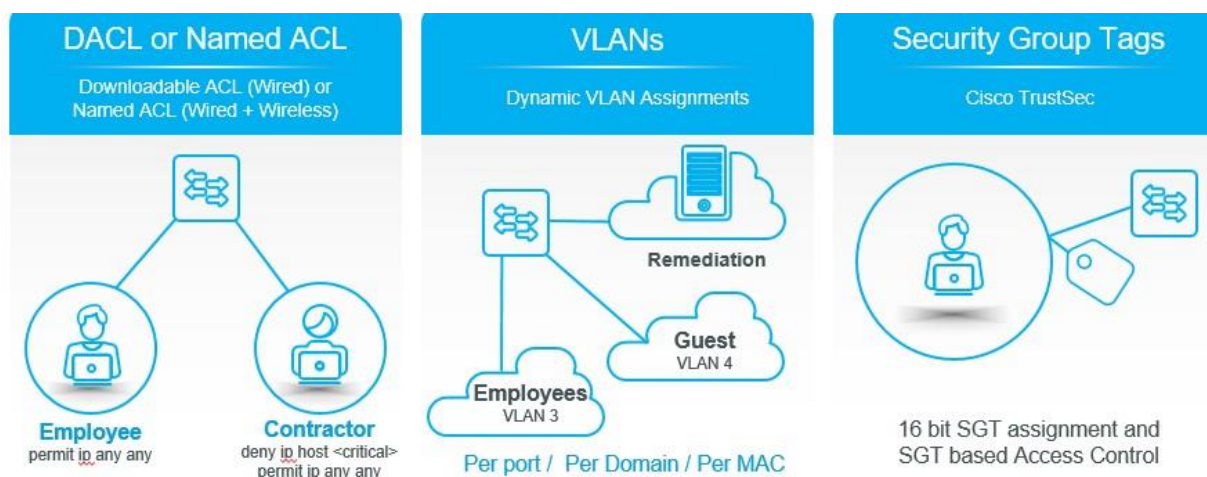


Figure 12 : Les types d'autorisation

## ✚ BYOD : Bring-Your-Own-Device

BYOD est un concept qui permet à un utilisateur d'utiliser son propre équipement dans l'entreprise.

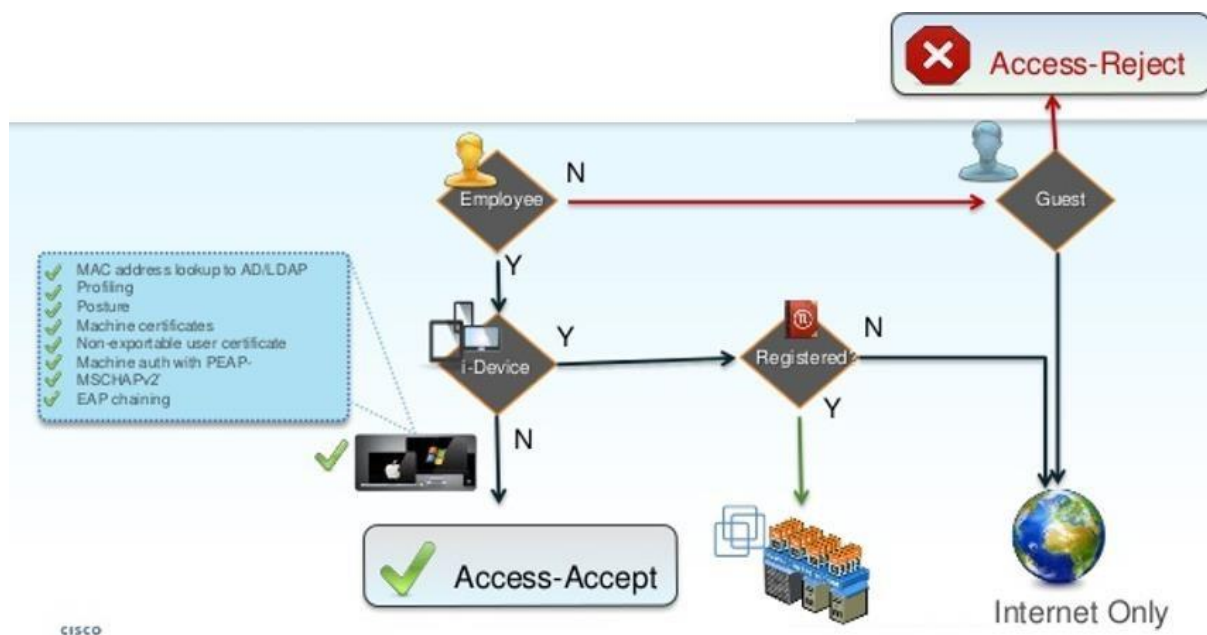


Figure 13 : Fonctionnement du BYOD

## ✚ Les profils et la visibilité

La détection des équipements accèdent au réseau



Figure 14 : Détection des équipements

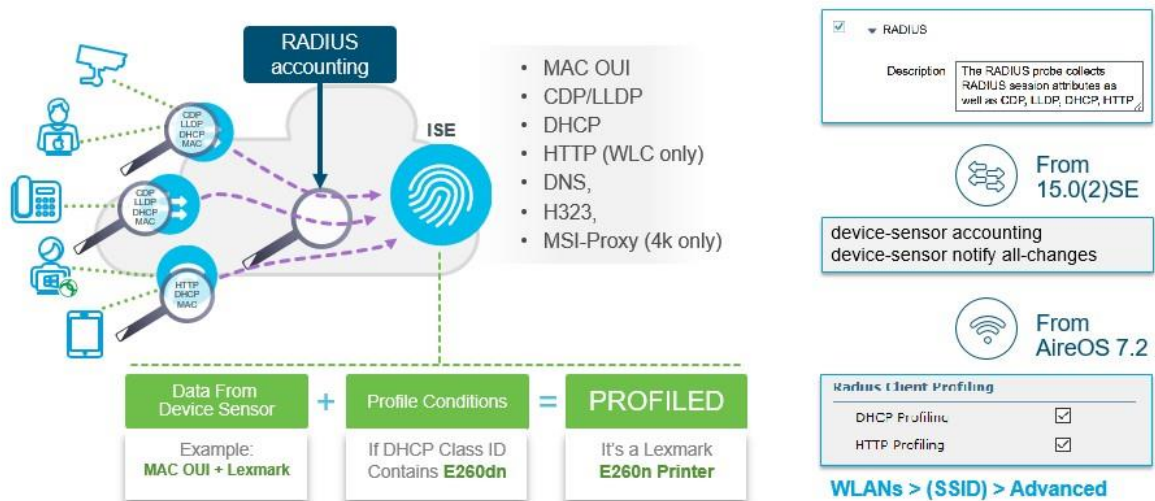


Figure 15 : Profiling

## + Guest Access

### Wireless

- Open SSID
- Central Web Authentication
- Controller in DMZ
- ISE separate interface for DMZ

### Wired

- Guest VLAN
- Flexible Authentication
  - 802.1X fails to MAB for CWA

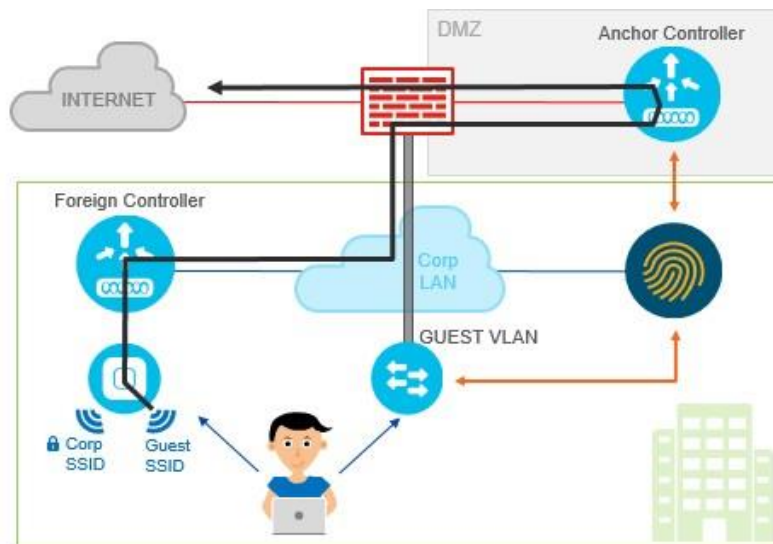


Figure 16 : Fonctionnement du Guest



Les types du Guest sont les suivants :



Figure 17 : Les types du Guest