République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida

Faculté des sciences

Département informatique

Mémoire de fin d'étude

Pour l'obtention du diplôme de master en informatique

Spécialité : Sécurité des systèmes informatique

Thème :

Elaboration et mise en place d'une stratégie de sécurité et de conformité pour contrôler l'accès au réseau

Mémoire présenté par :

REKIA Sidahmed

Promoteur : Mr NEHAL djilali **Encadreur:** Mr MECHAREK Mohamed

Année Universitaire: 2018/2019

Résumé :

Les entreprises sont au quotidien exposées aux attaques qui pourraient les conduire à des catastrophes diverses. Une stratégie de sécurité valide aiderait les entreprises à protéger leurs systèmes informatiques. Le domaine de la sécurité étant vaste, nous nous sommes tout particulièrement intéressés au contrôle des accès de leur réseau informatique et le contrôle de conformité de la machine qui accède au réseau avec la stratégie de posture. La solution est encore plus nécessaire quand on sait que, dans certains établissements, le nombre d'utilisateurs qui sollicitent fréquemment le réseau est très important.

Nous avons proposé une solution de Cisco ISE qui offre une approche réseau permettant un accès sécurisé et une protection intelligente et intégrée grâce à des solutions de conformité et de stratégie basées sur l'intention. La solution mise en place permet aux employés et les invités d'apporter leurs propres appareils, assure l'évaluation de posture des périphériques qui se connectent au réseau, la gestion d'une manière efficace l'accès au réseau, attribue les privilèges d'accès selon les taches prédéfinies et s'assurer que la stratégie de posture est appliquée pour garantie la conformité des machines.

Mots clés : stratégie de sécurité, contrôle d'accès, conformité, protection, Cisco ISE, stratégie de posture.

Abstract :

Companies are exposed to daily attacks that could lead to various disasters. A valid security strategy would help businesses protect their computer systems. The field of security is vast, we are particularly interested in controlling access to their computer network and compliance control of the machine that accesses this network with the posture strategy. The solution is even more necessary when we know that in some institutions, the number of users who frequently request the network is very important.

We have proposed a Cisco ISE solution that provides a network approach for secure access and intelligent and integrated protection through intent-based compliance and strategy solutions. The solution put in place allows employees and guests to bring their own devices, provides posture assessment of devices that connect to the network, effectively managing network access, assigns privileges to access according to predefined tasks and ensure that the posture strategy is applied to guarantee the conformity of the machines.

Keywords: security strategy , access control, conformity control , protection, Cisco ISE, posture strategy.

الملخص

تتعرض الشركات لهجمات يومية قد تؤدي إلى كوارث مختلفة. من شأن إستراتيجية أمنية صالحة أن تساعد الشركات على حماية أنظمة الكمبيوتر الخاصة بهم. نظرًا لأن مجال الأمان واسع ، فنحن مهتمون بشكل خاص بالتحكم في الوصول إلى شبكة الكمبيوتر الخاصة بهم والتحكم في المطابقة للجهاز الذي يصل إلى هذه الشبكة بإستراتيجية الموقف. الحل ضروري أكثر عندما نعلم أنه في بعض المؤسسات ، يكون عدد المستخدمين الذين يطلبون الشبكة بشكل متكرر مهم للغاية .

لقد اقترحنا حلاً يوفر cisco ISE منهجًا شبكيًا يتيح الوصول الآمن والحماية الذكية والمتكاملة من خلال حلول الامتثال والإستراتيجية القائمة على القصد ، والحل الذي تم وضعه يسمح للموظفين والضيوف بإحضار أجهزتهم الخاصة ، يوفر تقييماً للموقف للأجهزة التي تتصل بالشبكة ، وإدارة الوصول إلى الشبكة بفعالية ، وتعيين امتيازات الوصول وفقًا لمهام محددة مسبقًا والتأكد من تطبيق سياسات الأمن لضمان توافق الأجهزة.

الكلمات الدالة : إستراتيجية أمنية , بالتحكم في الوصول إلى شبكة , الامتثال ,الحماية , وضع أمان

Remerciements

Je voudrais remercier dieu pour toute l'énergie qu'il m'a donnée durant ces cinq années, nous croyons au destin, nous pouvons traverser les moments difficiles en regardant toujours le bon côté de la chose, hamdoulillah.

Mes pensées vont vers mes parents, qui ont toujours cru en moi. C'est grâce à leur soutient et prières que j'ai accomplie ce travail, ils savent déjà combien je leur dois.

Comme je remercie mon promoteur Mr Djilali Nehal pour m'avoir pris en charge et aidé tout au long du projet, Ainsi que mon encadreur Mr Mecharek Mohamed de m'avoir orienté avec ces précieux conseils et remarques.

Mes remerciements les plus sincères à toutes les personnes qui auront contribué de près ou de loin à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Enfin, je tiens aussi à remercier les membre jury pour avoir accepté d'examiner et de juger ce travail.

Sommaire

.

Liste des figures

Liste des tableaux

Introduction Générale

Introduction :

la sécurité des systèmes informatiques a toujours été un sujet sensible qui préoccupe toutes les entreprises. Elle constitue un domaine qui a toujours été d'actualité, encore plus de nos jours vu les avancées permanentes qui surviennent dans le monde des technologies de l'information.

Pour garantir les accès légitimes aux données et ressources d'un système, la sécurité informatique consiste à mettre en place des mécanismes d'authentification et de contrôle de conformité .

La solution de contrôle d'accès au réseau (NAC) est une technologie garantissant un accès sécurisé aux ressources réseau des entreprises en se basant sur l'authentification et l'identification des utilisateurs et des machines en plus la vérification de leurs compatibilités d'avec les stratégies de la sécurité.

Problématique :

Les entreprises devant désormais prendre en compte le problème de la croissance exponentielle des périphériques mobiles accédant à leurs réseaux et les risques de sécurité qu'ils apportent. Le problème est encore multiplié par la complexité des environnements de réseau modernes qui comprennent des types très variés d'utilisateurs finaux (employés, directeur, stagiaire) et d'accès (filaire, sans fil).

Dans ce cadre, le Laboratoire des Equipements de Télécommunications (LET) d'Algérie Télécom envisage de déployer une solution qui assure le contrôle des hôtes connectés à son réseau en détectant, identifiant et analysant les attaques de manière pertinente. Ce qui nous amène à proposer une stratégie de sécurité pour contrôler la conformité en exploitant CISCO ISE .

Objectif :

L'objectif de notre projet de fin d'étude est la mise en place d'une architecture de base qui permet aux employés et les invités d'apporter leurs propres appareils. Elle permet de gérer d'une manière efficace l'accès au réseau, refuser l'accès des utilisateurs au réseau sans authentification, donner les privilèges d'accès selon les taches prédéfinies et s'assurer que les stratégies de sécurité sont appliquées .

le mémoire est organisé en quatre chapitres :

- **Chapitre I :**Dans le premier chapitre nous parlerons des principes de sécurité informatique, les attaque et les mécanismes de défense.

- **Chapitre II :**Dans le deuxième chapitre, on présente un état de l'art sur les solutions de sécurité pour contrôle la conformité des machines ainsi que la solution choisie.

- **Chapitre III :**Ce chapitre est consacré à la conception et déploiement de notre solution de contrôle de conformité et mise en place la stratégie de sécurité .

- **Chapitre IV :**Le quatrième chapitre sera réservé aux tests des fonctionnalités de la solution réalisée au cours de ce projet de fin d'étude.

- **Conclusion et Perspectives :**Nous terminerons avec une conclusion générale et les perspectives .

Chapitre I : Généralités sur la sécurité des réseaux informatiques

I.1Introduction :

Les réseaux des entreprises sont un moyen important de communication qui permet l'échange d'informations au sein de l'entreprise. ces informations présentent l'actif qui permet de motiver et générer les activités donc ,toute sorte d'erreur (intentionnelle ou accidentelle) qui touche ces informations est inacceptable, cela conduit à l'augmentation de l'importance de la sécurité informatique .

Au cours de ce chapitre on va voir une présentation de l'Entreprise d'accueil après en va traiter la sécurité avec ses différents principes en citant par la suite les attaques et les mécanismes nécessaires pour protéger le réseau contre ces attaques.

I.2 Sécurité des systèmes informatiques :

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leurs ont été octroyés.

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs ; les consignes et règles deviennent de plus en plus compliqués au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance . [1]

I.3. Principes de la sécurité informatique :

La sécurité informatique vise généralement les principaux objectifs suivants :

- L'intégrité :Garantit la conformité de l'information c'est-à-dire garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé.
- La confidentialité : consistant à assurer qu'une information est accessible uniquement par les entités qui ont le droit d'accéder à celle-ci.
- L'authentification : consistant à assurer que seules les personnes autorisées aient accès aux ressources.
- La disponibilité: permettant de maintenir le bon fonctionnement du système d'information .
- La non répudiation : permettant de garantir qu'une transaction ne peut être niée ;

I.3.1 L'intégrité :

Garantit la conformité de l'information. Elle permet aux utilisateurs d'avoir l'assurance que l'information est exacte et qu'elle n'a pas été changée par une personne non autorisé. Il est ici question d'endiguer toute altération non admis des dispositifs et informations .

I.3.2 La confidentialité :

La confidentialité doit assurer la protection des données contre les accès non autorisées. Les données de la communication ne peuvent pas être connues par un tiers non autorisé.

I.3.3 L'authentification :

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

I.3.4 La disponibilité :

Assure que l'information parvienne à être utilisable et les acteurs de la communication accèdent aux données dans de bonnes conditions. Elle permet aux utilisateurs de pouvoir accéder aux applications qui traitent ces informations.

I.3.5 La non répudiation :

Elle assure le fait qu'une personne ou entité (émetteur ou récepteur) ne puisse nier avoir effectué une activité.

I.4 les Attaques :

I.4.1 définition de l'attaque :

Dans le domaine de la sécurité informatique une attaque se définit comme n'importe quelle action qui compromet la sécurité d'un système informatique .

I.4.2 Buts des attaques :

- Interruption: vise la disponibilité des informations .
- Interception: vise la confidentialité des informations .
- Modification: vise l'intégrité des informations .
- Fabrication: vise l'authenticité des informations .

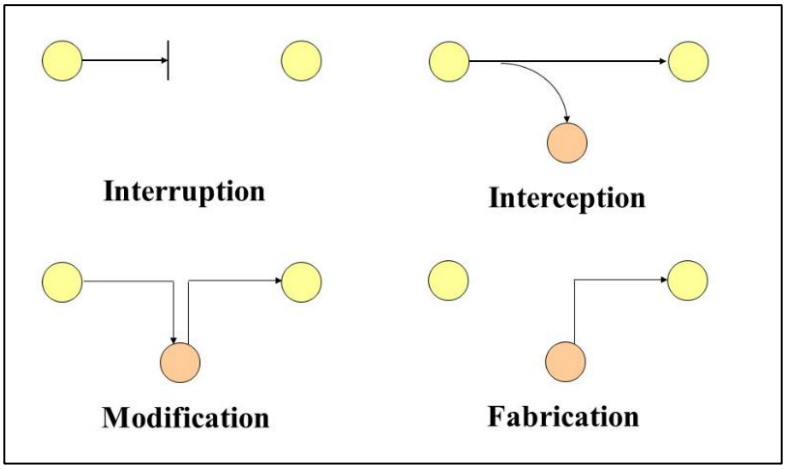

Figure. I. 1.Buts des attaques.

I.4.3 Les effets d'une attaque :

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.

I.4.3.a les attaques passives :

Écoutes indiscrètes ou surveillance de transmissions sont des attaques de nature passive. Le but de l'adversaire est d'obtenir une information qui a été transmise

I.4.3.b les attaques actives

Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux .

I.4.4 type d'attaque :

Il y a quatre catégories d'attaques :

- Programmes malveillants : Virus, vers et Cheval de Troie .
- Attaques de reconnaissance
- Attaques d'accès
- Attaques par déni de service (DoS)

I.4.4.a -Programmes malveillants

Un Programme malveillant est un Programme conçu pour infiltrer ou endommager un système informatique sans le consentement éclairé de son propriétaire. [3]

Les trois principaux types d'attaques de programmes malveillants sont les virus, les chevaux de Troie et les vers.

I.4.4.b-Attaques de reconnaissance

Reconnaissance, également appelée collecte d'informations, est la découverte et le mappage non autorisés de systèmes, de services ou de vulnérabilités.[4]

Dans la plupart des cas, procède une attaque par accès ou par déni de service.

Les attaques de reconnaissance peuvent comporter les éléments suivants:

- Requêtes d'information sur Internet
- Balayages Ping
- Balayage de ports
- Analyseurs de paquets

I.4.4.c Attaques d'accès

Les attaques d'accès exploitent des vulnérabilités connues dans les services d'authentification, les services FTP et les services Web pour accéder aux comptes Web, aux bases de données confidentielles et à d'autres informations sensibles.[4]

Les attaques d'accès peuvent être effectuées de différentes manières, notamment:

- Attaques de mot de passe
- Redirection de port
- Attaques de l'homme du milieu

I.4.4.d Attaques par déni de service (DoS)

Une attaque en déni de service consiste à bloquer une machine cible en lui envoyant des requêtes inutiles. Cela l'empêche de rendre le service pour lequel on l'a installée.[5]

Les attaques DoS peuvent prendre de nombreuses formes. Elles empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système. Voici quelques exemples des menaces DoS les plus courantes :

- Ping of death
- Smurf Attack
- TCP SYN flood attack

I.5 Mécanismes de défense:

À cause des menaces provenant des attaques, Il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer :

I.5.1 Antivirus:

Il s'agit d'un logiciel capable de détecter et de détruire les virus contenus sur une machine. Ce logiciel permet de surveiller la présence de virus et éventuellement de nettoyer, supprimer ou mettre en quarantaine le ou les fichiers infectés. Il surveille tous les espaces dans lesquels un virus peut se loger. [6]

I.5.2 Chiffrement:

Le chiffrement consiste à rendre un texte incompréhensible en le codant. Les algorithmes de chiffrement permettent de transformer un texte écrit en clair en un texte chiffré. Cette transformation se fonde sur une ou plusieurs clés. Le texte chiffré peut alors être envoyé à son destinataire.[7]

La cryptanalyse consiste à déchiffrer un texte chiffré en effectuant sur ce texte avec une clé. Il existe deux méthodes de chiffrement : chiffrement à clé symétrique et chiffrement à clé asymétrique (ou clé publique)

I.5.2.a clé symétrique :

La clé de chiffrement est identique à la clé de déchiffrement. Ainsi c'est la même clé qui va nous permettre à la fois de chiffrer le message et de permettre aux destinataires de le déchiffrer.

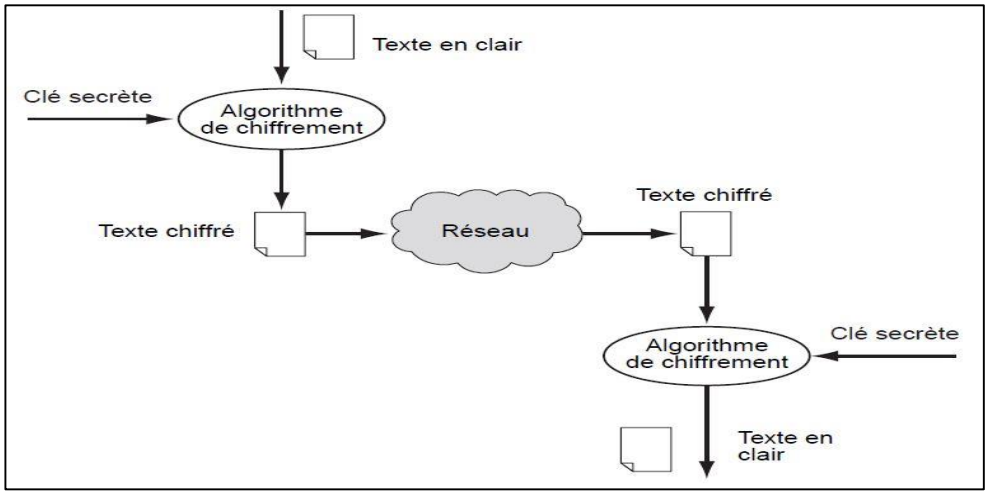

Figure. I. 2.Algorithme de chiffrement symétrique[7]

I.5.2.b clé asymétrique :

Dans ce cas, les clés de chiffrement et de déchiffrement sont distinctes, et généralement symétriques entres elles: la clé de chiffrement permet de déchiffrer ce qui a été chiffré avec la clé de déchiffrement, et vice versa. Le possesseur d'une telle paire de clés, en rend une (au choix) publique, c'est-à-dire qu'il la donne à tout le monde, dans une sorte d'annuaire. Tout correspondant qui veut envoyer un message, chiffre son message à l'aide de la clé publique du destinataire. Seul le possesseur de la clé secrète correspondant à cette clé publique pourra déchiffrer le message. [7]

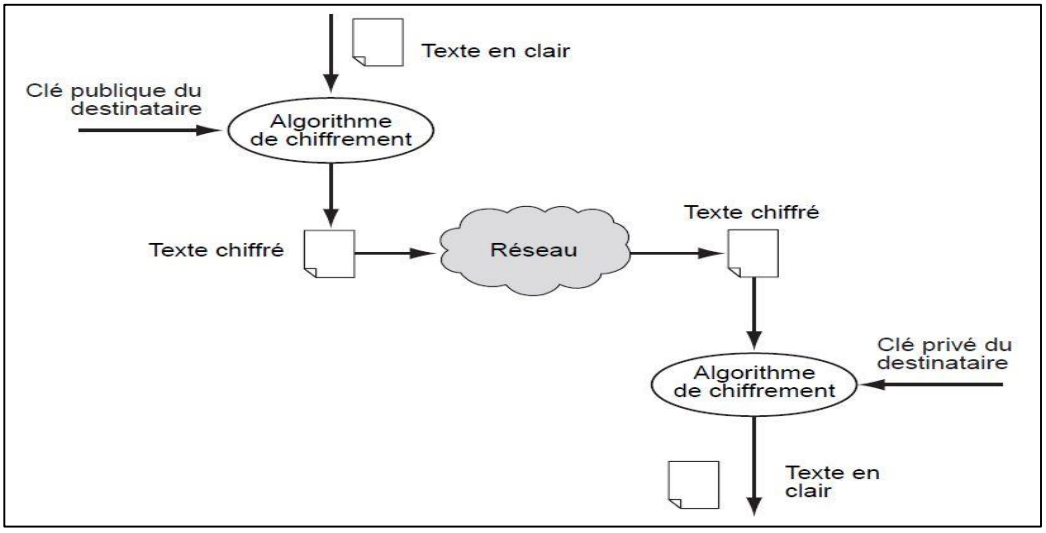

Figure. I. 3.Algorithme de chiffrement asymétrique.[7]

I.5.3 Pare feu :

C’est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité. Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées a communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante. Il permet d'une part de bloquer des attaques ou connexions suspectes d’accéder au réseau interne. D’un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d’informations vers l’extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau. [8]

I.5.3 proxy :

Un proxy est un serveur qui fait fonction d’intermédiaire entre les ordinateurs d’un réseau local et internet. Il peut également assurer un suivi des connexions (logs utilisateurs) et filtrer les connexions à internet en analysant les requêtes des clients et les réponses des serveurs pour les comparer à la liste blanche (liste de requête autorisées) ou à la liste noire (liste de requête interdites).[9]

I.5.4 Système de détection d’intrusion :

Un système de détection d'intrusions (IDS) est un élément matériel ou logiciel qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et malveillante. Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis.[10]

I.5.5 Système de prévention d’intrusion :

Le système de prévention d'intrusion, ou IPS (*Intrusion Prevention system*) a pour fonction non seulement de détecter les comportements suspects mais aussi de les stopper. Il est doté de filtres de détection d’un ensemble de règles qui vont lui indiquer la façon adéquate à réagir : bloquer le flux réseau, le laisser passer ou demander l’intervention humaine.[10]

conclusion :

En conclusion, la sécurité informatique est l’ensemble des moyens mis en œuvre pour réduire la vulnérabilité d’un système contre les menaces accidentelles ou intentionnelles, parmi ces moyens la mise en place d’une solution de contrôle de conformité qui est devenu aujourd’hui un élément important dans le réseau de chaque entreprise. Ce qui a conduit les constructeurs des infrastructures réseau à proposer des solutions de contrôle de conformité.

Chapitre II : Etat de l'art

II.1 Introduction :

La sécurité des réseaux informatiques est un sujet sensible. Si on parle de la sécurité des réseaux le concept qui nous vient toujours à l'esprit est la sécurité contre des attaques externes. Mais en réalité les dégâts qui peuvent venir de l'intérieur sont beaucoup plus dangereux. De ce fait il est nécessaire de développer, au sein des entreprises, des architectures permettant de vérifier la conformité des utilisateurs qui se connectent au réseau afin de garantir sa sécurité.

Dans ce chapitre nous allons présenter le contrôle d'accès au réseau avec ses protocole, Contrôle de conformité et citer de manière générale des différentes solutions qui assurent le contrôle de conformité.

II.2 L'importance de stratégies de sécurité réseau:

les organisations doivent élaborer des stratégies de sécurité réseau efficaces pour les raisons suivantes: [12]

- Les violations de la sécurité peuvent être très coûteuses en termes de perturbation de l'activité et des pertes financières qui peuvent en résulter.
- De plus en plus d'informations sensibles sont transférées sur Internet ou sur des intranets qui y sont connectés.
- Les réseaux utilisant des liens Internet sont de plus en plus populaires car ils sont moins chers que les lignes louées dédiées. Cela implique toutefois que différents utilisateurs partagent des liens Internet pour transporter leurs données.
- Les directeurs d'entreprise sont de plus en plus tenus de fournir une sécurité efficace de l'information.

Pour qu'une organisation atteigne le niveau de sécurité approprié et à un coût acceptable, elle doit procéder à une évaluation détaillée des risques afin de déterminer la nature et l'étendue des menaces existantes et potentielles. Les contre-mesures aux menaces perçues doivent trouver un équilibre entre le degré de sécurité à atteindre, leur acceptabilité pour les utilisateurs du système et la valeur des systèmes de données à protéger.

II.3 NAC (Network Access Control) :

II.3.1. Principe de fonctionnement :

Le contrôle d'accès au réseau (NAC) permet de s'assurer que seules les machines connue ont autorisé à se connecter à votre réseau et qu'ils répondent aux exigences de votre réseau avant d'obtenir l'accès.

Le NAC permet de définir une stratégie de sécurité complète pour un réseau, de la mettre en œuvre sur un serveur centralisé et de faire en sorte que le réseau applique automatiquement cette stratégie à tous les utilisateurs du réseau.

Les quatre principales fonctionnalités de NAC sont : [13]

- Authentification et autorisation .
- Évaluation de la posture (évaluation d'un endpoint entrant par rapport aux stratégies du réseau)
- Mise en quarantaine des systèmes non conformes (permet au client d'appliquer les dernières mises à jour de sécurité, de mettre à jour son logiciel antivirus, etc., sans avoir un accès global au réseau)
- Remédiation des systèmes non conformes .

II.3.2. protocole de contrôle d'accès :

Il faut un ensemble de protocoles pour définir et implémenter une stratégie qui décrive comment sécuriser l'accès aux nœuds de réseaux par des machines quand, initialement, ils tentent d'accéder au réseau.

II.3.2.1 le protocole 802.1X :

IEEE 802.1X est un standard de l'IEEE qui permet de contrôler l'accès au réseau en se basant sur les ports. Il assure l'authentification aux équipements connectés à un port Ethernet. Ce standard peut être utilisé pour quelques points d'accès WiFi, 802.1X est une fonctionnalité disponible sur certains commutateurs réseau.[14]

IEEE 802.1x utilise le protocole EAP pour mettre en communication le client et le serveur d'authentification via le contrôleur.

Les acteurs du 802.1x :

• **Demandeur** : C'est le système à authentifier (le client),

• **Port Access Entity (PAE)** : C'est le point d'accès au réseau,

• **Authenticator System :** C'est système authentificateur qui contrôle les ressources disponibles via le PAE.

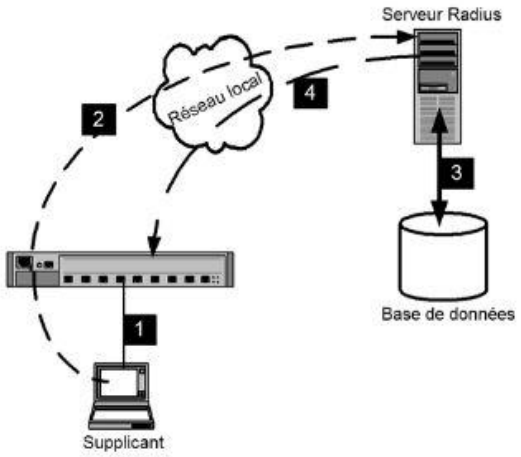

Figure. II. 2.Principes de l'authentification 802.1X [14]

Suivant le schéma de la figure II.2, le demandeur va envoyer les éléments d'authentification (certificat, identifiant, mot de passe...) vers le serveur Radius(1). Cependant, il ne communique pas directement avec le serveur et d'ailleurs. C'est le commutateur qui va servir d'intermédiaire (2), car il connaît l'adresse du serveur. Pour interroger sa base de données (3), le serveur Radius a besoin d'un identifiant qu'il utilise comme point d'entré. Le commutateur envoi les éléments d'authentification au serveur .après le serveur accepte ou refuse l'authentification et renvoie sa réponse au commutateur (4). Et celui-ci ouvre le port sur le VLAN commandé par le serveur.

II.3.2.2 EAP :

Le protocole d'authentification extensible (EAP, pour Extensible Authentication Protocol) est utilisé pour transmettre les informations d'authentification entre le demandeur (le poste de travail) et le serveur d'authentification (Radius ou autre).

Ce protocole est extensible, car on peut définir de nouvelles méthodes d'authentifications. Il est indépendant de la méthode utilisé.

Les méthodes d'authentification du protocole d'authentification extensible (EAP) :

Étant donné que la sécurité d'un réseau WLAN (Wi-Fi Local Area Network) est essentielle et que les types d'authentification EAP offrent un meilleur moyen de sécuriser la connexion d'un réseau WLAN, les fournisseurs développent et ajoutent rapidement des types d'authentification EAP à leurs points d'accès WLAN. On peut citer [15] :

- EAP-MD5 : Authentification avec un mot de passe.
- EAP-TLS : authentification mutuelle entre le client et le serveur d'authentification par le biais de certificats (côté client et côté serveur)
- EAP-TTLS : Authentification avec n'importe quelle méthode d'authentification, au sein d'un tunnel TLS , il ne nécessite que des certificats côté serveur .
- EAP-PEAP : authentification mutuelle du client et du serveur Radius par le biais d'un certificat côté serveur, le client peut utiliser un couple login/mot de passe

II.3.2.3 RADIUS :

Le protocole RADIUS (Remote Authentication Dial-In User Service) est un protocole de type AAA (Authentication Autorization Accounting) permettant de centraliser l'authentification et l'autorisation des accès distants. Il repose essentiellement sur un serveur (RADIUS), connecté à une base d'identification (LDAP par exemple) et un client RADIUS, nommé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Les échanges entre le client RADIUS et le serveur RADIUS est chiffré et authentifié avec l'appui d'un secret partagé. [16]

Pour l'authentification il y a quatre types de paquets :

- Access-Request : envoyé par le contrôleur d'accès, contenant les informations sur le client (login/mot de passe, ...).
- Access-Accept : envoyé par le serveur dans le cas où l'authentification est un succès.

- Access-Reject : envoyé par le serveur dans le cas où l'authentification est un échec, ou si il souhaite fermer la connexion.
- Access-Challenge : envoyé par le serveur pour demander des informations complémentaires, et donc la réémission d'un paquet Access-Request.

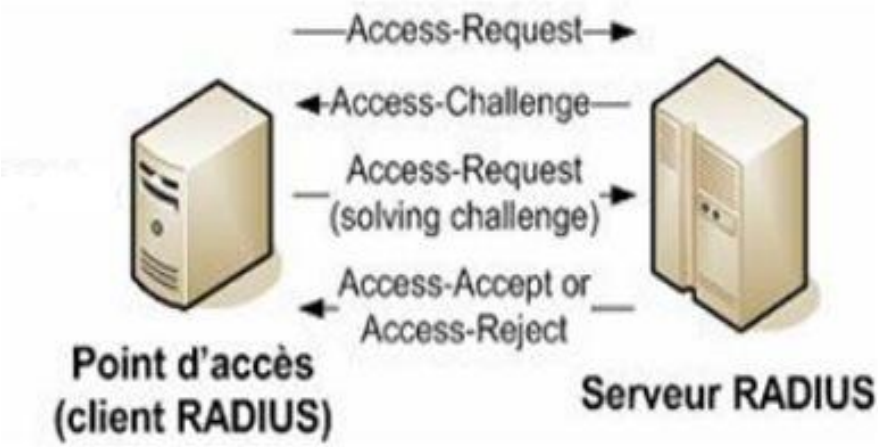

Figure. II.3.Etablissement d'une session au sens Radius [14]

la méthode d'authentification Radius :

1. le poste utilisateur transmet les informations nécessaires à l'authentification (login, mot de passe, adresse MAC) au client RADIUS ;

2. le client RADIUS envoi un paquet "Access-Request" au serveur RADIUS. Il contient l'ensemble des informations de l'utilisateur (ID du client, mot de passe, numéro du port). Si un mot de passe est présent, ce dernier sera haché en utilisant la fonction de hachage MD5

3. le serveur RADIUS reçoit la requête, vérifie l'authenticité du paquet en vérifiant le secret qu'il partage avec le client RADIUS, puis vérifie l'identité de l'utilisateur en extrayant et en comparant les informations contenues au sein d'une base de données ou d'un annuaire (AD ou LDAP). Le serveur RADIUS peut demander soit de ré-émettre un accès-request, soit demander des informations complémentaires.

4. le client RADIUS génère ensuite une requête Access-Request contenant les informations d'authentification demandées par le challenge ;

5. enfin, le serveur RADIUS valide ou refuse la requête en transmettant un paquet de type "Access-Accept" ou "Access-Reject". Ce paquet peut contenir une liste de services qui sont autorisés (par exemple le Vlan).

II.3.3 Composants de NAC :

Les composants qui constituent l'architecture de la solution NAC sont [17] :

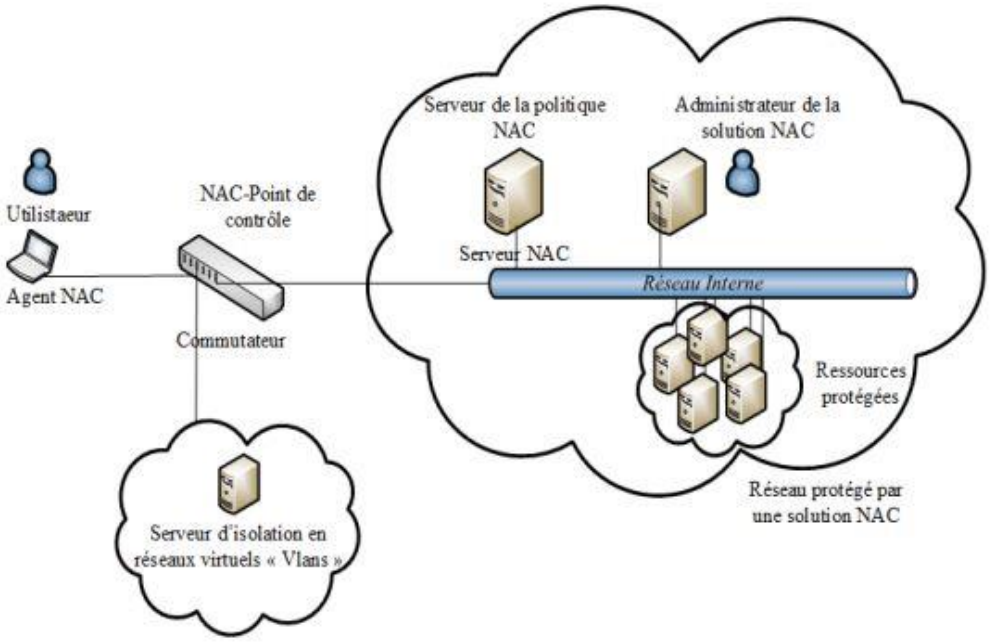

Figure. II. 4.Composants de NAC [11]

II.3.3.1 Agent :

L'agent de confiance est l'un des composants essentiel du NAC qui s'agit d'un logiciel client installée localement sur un endpoint, Sa responsabilité principale consiste à collecter des informations à l'état du poste tel que la présence ou non d'antivirus et des derniers correctifs de sécurité.

En outre, il communique également la "posture" (ou ce qu'il apprend) au serveur de politiques.

II.3.3.2 Network Access Device (NAD):

Il s'agit des équipements d'accès au réseau (Les routeurs, les commutateurs, les points d'accès sans fil) qui appliquent les actions envoyées par le serveur de stratégie de sécurité après analyse de l'état du poste. Le NAD autorise, interdit ou isole un poste qui tente de se connecter au réseau d'entreprise en fonction des stratégies de sécurité appliquées. Le Serveur de stratégie va télécharger des règles de filtrage réseau (Access List) sur les ports d'un routeur, forcer une redirection d'URL, affecter un port d'un commutateur à un VLAN particulier en fonction du résultat du contrôle.

II.3.3.3 Serveur de stratégie :

Ce serveur évalue les informations de sécurité de l'endpoint provenant des équipements d'accès au réseau et détermine la stratégie d'accès qu'il convient de lui appliquer.

le serveur Cisco Secure Access Control (ACS) est un serveur AAA(authentification, autorisation et administration) de type RADIUS, La fonction principale du serveur ACS est d'agir en tant que point de décision de la stratégie dans les déploiements NAC. En plus de cela, le serveur Cisco Secure Access Control évalue également les informations d'identification de l'utilisateur et calcule l'état de sécurité des endpoints du réseau.

II.3.3.4 Serveur de politique antivirus :

Une composante essentielle de NAC est la capacité de veiller à ce que les ordinateurs tentant d'accéder au réseau d'entreprise doivent répondre aux exigences de stratégie de sécurité approuvée pour Logiciel antivirus.

II.4 Contrôle de conformité :

Selon l'ISO (International Organization for Standardization), l'évaluation de la conformité est l'opération qui consiste à vérifier que des produits, matériaux, services, systèmes ou compétences de personnels sont conformes aux spécifications d'une norme pertinente. [18]

Dans le domaine de sécurité informatique le contrôle de la conformité consiste à vérifier que tous les équipements de réseau respectent la stratégie de sécurité appliquée .Donc les constructeurs ont décidé de développer des solutions permettant d'assurer la conformité des hôtes connectés au réseau.

II.4.1 l'importance de la conformité des appareils :

- Les vulnérabilités sont partout dans les logiciels obsolètes
- Des applications et des logiciels non autorisés peuvent provoquer des fuites de données.
- Les faibles paramètres de sécurité rendent les appareils faciles à exploiter
- Les endpoins dépourvus des dernières technologies de sécurité sont risqués

II.4.2 Les solutions de conformité :

Plusieurs solutions NAC sont disponibles. Elles peuvent être classifiées sous deux principales catégories : libres et commerciales.

II.4.2.1 Les solutions libres :

II.4.2.1.a PacketFence :

PacketFence est une solution de conformité réseau (NAC, Network Access Control) approuvée et gratuite comprenant un ensemble de fonctionnalités [19] :

- une gestion centralisée câblée et sans fil, L'enregistrement des périphériques réseau grâce à un puissant portail captif .
- Detecte les activité réseau anormales (worms , spyware …) grace a snort
- La gestion simple et efficace des invités se connectant sur le réseau .
- L'authentification des utilisateurs en se référant au standard 802.1X
- Detection DHCP qui permet de reconnaitre téléphones IP , smarttphone et tablette .
- Peut réaffecter un port ne respectant pas la stratégie de sécuritré a un vlan particulier (quarantaine).

II.4.2.1.b FreeNAC :

FreeNAC est une solution Open Source pour géré l'accès au réseau local et la gestion de VLAN. FreeNAC fournit une assignation de réseau local virtuel conviviale, un contrôle d'accès au réseau local (pour tous types de périphériques réseau tels que serveurs, stations de travail, imprimantes, téléphones IP, webcams, etc.), un inventaire des périphériques finaux du réseau en direct, la gestion de VLAN et permet documentation sur le câblage de correction.

Les périphériques finaux sont identifiés par leur adresse MAC (en "mode VMPS") ou par leur certificat et leur adresse MAC (en "mode 802.1x"). Sur la couche de communication, FreeRadius est inclus pour les modes 802.1x et OpenVMPS pour VMPS. Les routeurs et les commutateurs sont analysés via SNMP pour identifier tous les périphériques et lier les adresses MAC aux adresses IP aux ports physiques. Des fonctionnalités d'entreprise telles que la redondance et la surveillance sont également incluses . [20]

II.4.2.2 Les solutions commerciales :

Dans cette partie, on va étudier quelques solutions de contrôle d'accs au réseau (NAC) libre et commerciales qui existent dans le marché afin de pouvoir par la suite choisir une solution adéquate à notre projet.

II.4.2.2.a NAC CISCO (appliance) :

L'Appliance Cisco NAC est une solution intégrée centrée sur le réseau, administrée à partir de la console Web de Clean Access Manager et appliquée via le serveur Clean Access et (éventuellement) l'agent. L'Appliance Cisco NAC vérifie les systèmes client, applique la configuration réseau requise, distribue les correctifs et le logiciel antivirus, et met en quarantaine les clients vulnérables ou infectés afin qu'ils soient corrigés avant que les clients n'accèdent au réseau [21]

Composants de NAC Appliance :

NAC Appliance comprend les composantes obligatoires (CAS, CAM) et d'autres optionnelle (CA Agent) [22] :

1. **Clean Access Server (CAS):**

le serveur NAC applique les privilèges d'accès en fonction de la conformité des terminaux et de l'authentification de l'utilisateur. Un utilisateur ne peut pas accéder au réseau tant qu'il ne s'est pas authentifié et que le périphérique ne répond pas aux exigences de posture définies.

2. Clean Access Manager (CAM)

Le Clean Access Manager (CAM) est le serveur d'administration et la base de données qui centralise la configuration et la surveillance de tous les serveurs, des utilisateurs et des règles de Clean Access dans un déploiement de l'Appliance Cisco NAC. Vous pouvez l'utiliser pour gérer jusqu'à 20 serveurs Clean Access. La console d'administration Web de Clean Access Manager est une interface de gestion sécurisée basée sur un navigateur.

3. Clean Access Agent (en option)

client léger à lecture seule qui améliore les fonctions d'évaluation des vulnérabilités et accélère le processus de remédiation.

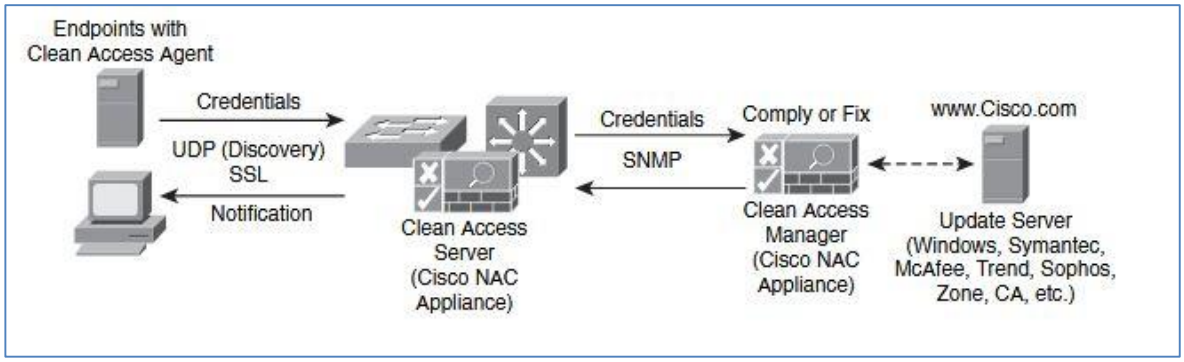

Figure. II. 4.*Composants de NAC Appliance* [22]

II.4.2.2.b NAP Microsoft(Microsoft, 2008)

Network Access Protection (NAP) est une plate-forme d'application de la stratégie intégrée dans Windows Server. Elle permet de s'assurer que des ordinateurs clients dans un réseau privé répondent aux exigences définies par l'administrateur en matière d'intégrité système.

Fonctionnement de NAP :

Lorsqu'un client NAP tente de se connecter au réseau, l'état d'intégrité du client est validé par rapport aux stratégies d'exigences d'intégrité définies dans le serveur NPS (Network Policy Server). Si un client n'est pas conforme aux stratégies d'intégrité définies, l'administrateur peut choisir de limiter l'accès du client à un réseau de quarantaine avec un d'accès limité. Ce réseau contient idéalement des ressources de mise à jour pour que le client obtienne la conformité. Seuls les clients qui se conforment aux stratégies d'intégrité requises disposent d'un accès illimité au réseau.

La protection d'accès réseau présente quatre aspects importants :

• **Validation de la stratégie**: détermine si les ordinateurs sont conformes à la stratégie de sécurité.

• **Limitation d'accès réseau**: restreint l'accès réseau aux ordinateurs en fonction de leur état.

• **Correction automatique:** fournit les mises à jour nécessaires pour permettre à l'ordinateur de «redevenir conforme». Une fois que celui-ci est conforme, les restrictions réseau sont supprimées.

• **Conformité permanente**: met à jour automatiquement les ordinateurs compatibles afin qu'ils adhèrent aux modifications en cours dans les exigences de stratégie d'intégrité.

Le déploiement de la technologie NAP exige :

- Des serveurs dotés de Windows Server.
- Les ordinateurs clients exécutant des systèmes d'exploitation Microsoft.

II.4.2.2.c UAC Juniper :

Juniper UAC une solution offrant de manière transparente un accès sécurisé aux utilisateurs invités, un contrôle d'accès au réseau et aux applications, ainsi qu'une visibilité et une surveillance réseau. Les stratégies d'accès sont appliquées au niveau 2 avec les points d'accès ou commutateurs sans fil compatibles du fournisseur 802 .1X, aux niveaux 2 à 4 avec les nouveaux commutateurs Ethernet de la série EX de Juniper Networks et aux couches 3 à 7 avec toute plate-forme de pare-feu Juniper. [24]

Les clients ont la possibilité de déployer la solution complète de contrôle de compte d'utilisateur ou de sélectionner des composants pour différents degrés de contrôle d'accès et de visibilité, en introduisant progressivement le contrôle d'accès à leur rythme. C'est entièrement au client et à ses besoins en matière de contrôle d'accès.

La solution Juniper UAC garantit que seuls les utilisateurs authentifiés et les périphériques conformes aux stratégies de réseau et de sécurité ont accès au réseau et aux ressources autorisées. Il permet aux entreprises de surveiller et de contrôler l'accès au réseau et aux applications en fonction de divers paramètres, notamment l'identité de l'utilisateur et / ou du périphérique, son emplacement et la conformité aux stratégies de sécurité et de réseau.

Les composants de la solution UAC :

La solution Juniper UAC se compose de trois composants de base [25] :

- un agent (l'agent UAC)
- un serveur de gestion des strategies (Infranet Controller)
- des points d'application .

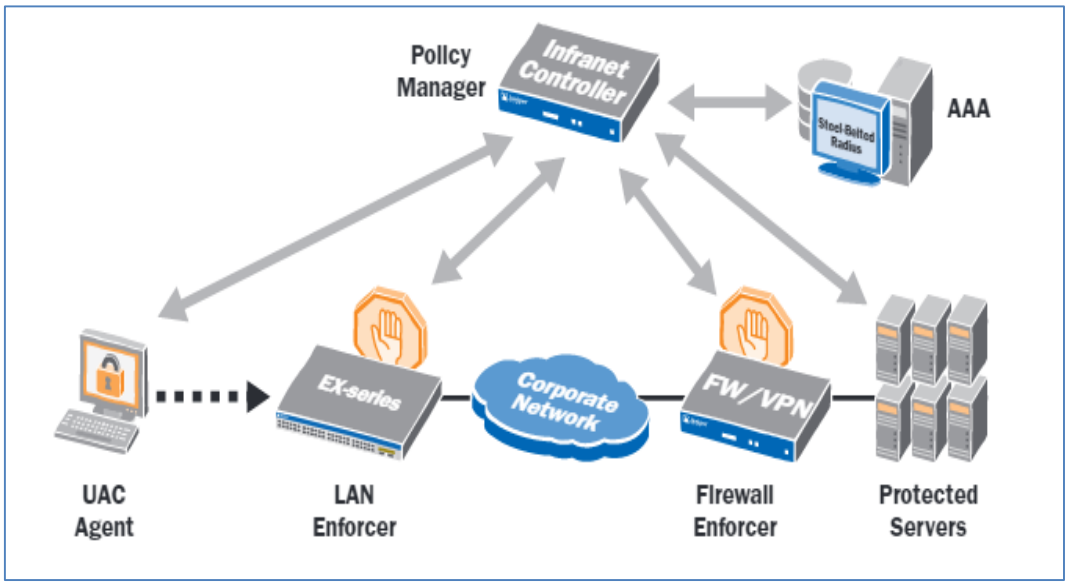

Figure. II.5. composants de UAC[25]

L'agent Juniper UAC:

Un logiciel client téléchargeable, sert de demandeur 802 .1X et permet de collecter des informations sur la posture de l'hôte.

Serveur de gestion des stratégies :

C'est un serveur centralisé de gestion des stratégies qui constitue le moteur de stratégie de sécurité et d'accès pour UAC, ainsi que l'interface avec les infrastructures AAA d'entreprise existantes.

Le serveur de gestion des stratégies combine les informations collectées par le agent avec la stratégie de conformité définies par l'entreprise, implémente la stratégie d'accès appropriée pour chaque utilisateur / session et transmet cette stratégie aux points d'application du réseau.

Points d'application :

Les points d'application contrôlent l'accès au réseau et à ses ressources en fonction de stratégies créées et fournies par le serveur de gestion des stratégies. Les commutateurs Ethernet de la série EX de Juniper Networks sont des points d'application pour toute plate-forme d'accès filaire ou sans fil compatible 802 .1X d'autres fournisseurs.

II.4.3 Comparaison entre les solution NAP , UAC et NAC :

	Microsoft NAP	Juniper UAC	Cisco NAC
Évaluation de la posture de l'appareil	Oui	Oui	Oui
Authentification utilisateur / appareil	Nécessite MS RADIUS	Nécessite quelques modifications à l'infrastructure d'authentification / répertoire	S'intègre avec l' infrastructure actuelle
Remediation	Très limité	Oui	Oui
système d'exploitation	Seulement MS	MS,MAC OSX	MS,MAC OSX
Portail d'accès invité	Non	Pas de connexions temporaires	Oui
La gestion des d'actifs	Non	Manuel	Automatisé

tableau II .1 Comparaison entre les solution NAP , UAC et NAC

Contrairement aux Juniper et Cisco, Microsoft a choisi d'implémenter sa solution uniquement dans la partie Soft . L'un des points faible de cette solution est sa compatibilité seulement avec les systèmes de Microsoft.

II.5 Cisco ISE (Identity Services Engine) :

Cisco ISE (Identity Services Engine) est la dernière technologie de contrôle d'accès de Cisco et son centre d'innovation, basé sur 802.1x pouvant être déployé sur des appliances ou des machines virtuelles. Cela signifie que de nombreuses fonctionnalités ne sont pas disponibles dans l'appliance NAC. Certains exemples sont :

- ISE capable d'exécuter le même matériel pour un CAM, un CAS, un profileur, un serveur invité et un ACS sur la même solution .
- Prise en charge multi-forêt AD.
- ISE peut être virtualisé alors que NAC est uniquement une appliance.
- Accès invité très puissant .
- ISE prend en charge les listes de contrôle d'accès dynamiques .

II.5.1. Définition :

Identity Services Engine (ISE) est la dernière génération des plates-formes de contrôle d'accès proposées par Cisco et qui permet aux entreprises d'imposer leurs stratégies de

sécurité lors de l'accès, de renforcer la sécurité de leurs infrastructures et de rationaliser leurs opérations de services.[26]

L'architecture unique de Cisco ISE permet aux entreprises de recueillir les informations concernant les utilisateurs et les périphériques, en temps réel à partir du réseau. L'administrateur peut ensuite utiliser ces informations pour prendre des décisions de gouvernance proactive en liant l'identité à divers éléments du réseau, y compris les commutateurs, les contrôleurs de réseau local sans fil (WLC) et les passerelles des réseaux privés virtuels (VPN).

Posture est un service de Cisco ISE (Identity Services Engine) qui vous permet de vérifier la conformité, également appelée posture, des points d'extrémité avant de leur permettre de se connecter à votre réseau. Un agent de posture, tel que l'agent NAC (Network Admission Control), s'exécute sur le endpoint . Client Provisioning garantit que les ordinateurs d'extrémité reçoivent l'agent de posture approprié. [27]

II.5.2 les fonctions et caractéristiques de cisco ISE :

Cisco ISE exécute les fonctions suivantes [28] :

- Combine l'authentification, l'autorisation, la comptabilité (AAA), la posture et le profileur dans une Appliance.
- Fournit une gestion complète de l'accès des invités pour les administrateurs Cisco ISE, les administrateurs de sponsors sanctionnés ou les deux.
- Applique la conformité des terminaux en fournissant des mesures complètes de provisionnement des clients et en évaluant la posture des périphériques pour tous les terminaux qui accèdent au réseau, y compris les environnements 802.1X
- Prise en charge de la découverte, du profilage, du placement basé sur des stratégies et de la surveillance des périphériques d'extrémité sur le réseau
- Centraliser la gestion des politiques d'accès réseau pour offrir un accès sécurisé aux utilisateurs quelle que soit leur connexion (sans fil, VPN ou filaire)
- Prend en charge l'évolutivité nécessaire pour soutenir un certain nombre de scénarios de déploiement, du petit bureau aux grands environnements d'entreprise .
- utilisation de balises de groupe de sécurité (SGT) et de listes de contrôle d'accès de groupe de sécurité (SGACL)

Caractéristiques	Avantages
Gestion centralisée	- Aide les administrateurs à configurer et gérer de manière centralisée les services de posture, d'invité, d'authentification et d'autorisation dans une console Web unique.
Contrôle d'accès	- Offre une gamme d'options de contrôle d'accès, y compris des listes de contrôle d'accès téléchargeables (dACL), des attributions de réseau local virtuel (VLAN), des redirections d'URL, des listes de contrôle d'accès nommées

	et des listes de contrôle d'accès du groupe de sécurité (SGACL) avec la technologie Cisco TrustSec
Service de posture d'extrémité (Endpoint)	- Effectue des évaluations de posture sur les Endpoint connectés au réseau. -Applique les stratégies de conformité appropriées pour les Endpoint via un agent client permanent
Surveillance et dépannage	Inclut une console Web intégrée pour la surveillance, la création de rapports et la résolution des problèmes afin d'aider les opérateurs du service d'assistance et les opérateurs réseau à identifier et à résoudre rapidement les problèmes .

tableau II .2Caractéristiques et avantages [29]

II.5.3 Composants de déploiement ISE :

Une solution typique de contrôle d'accès au réseau basée sur ISE comprend quatre composants: endpoints, périphériques réseau, Cisco ISE et services externes.

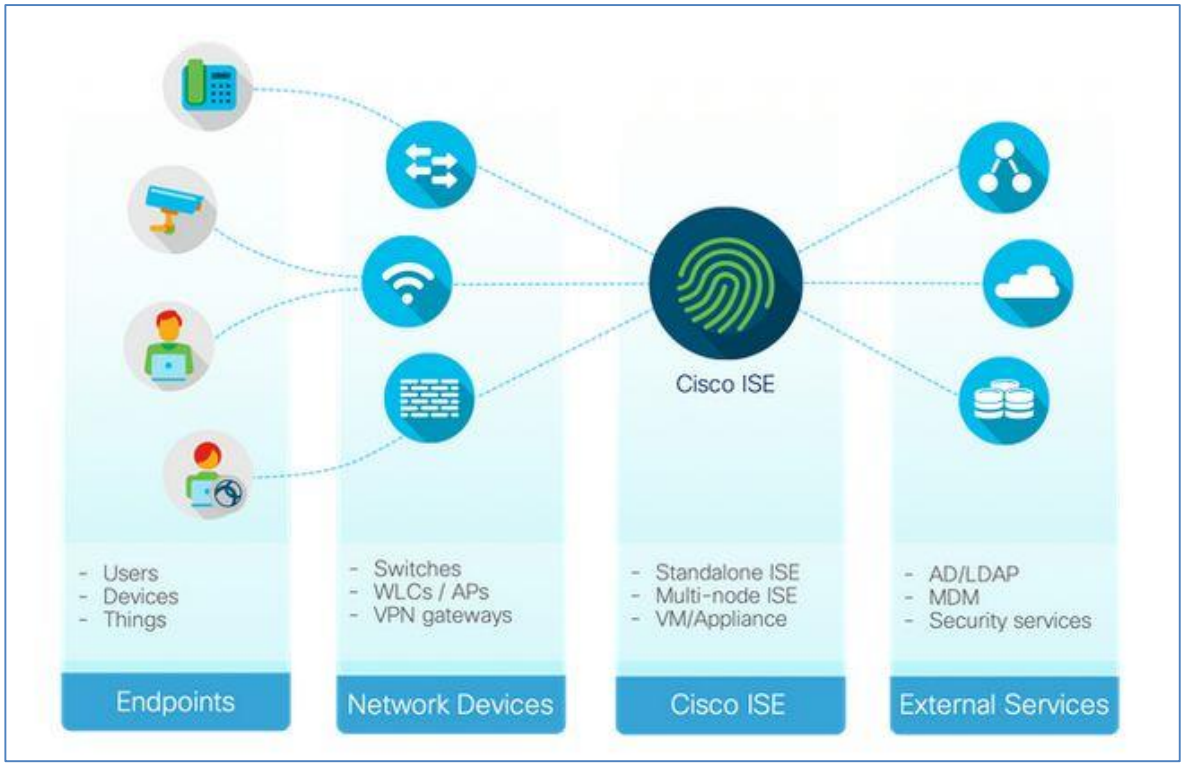

Figure. II. 7.Composants de la solution ISE[34]

Les endpoints ont besoin d'un accès au réseau et les périphériques du réseau fournissent un accès réseau aux ordinateurs d'extrémité, en fonction des instructions fournies par ISE. ISE peut éventuellement d'exploiter des services externes pour en savoir plus sur les endpoints correspondants pour les décisions de stratégie.

Lorsqu'il s'agit de déployer un réseau basé sur l'identité, étant donné que ces quatre parties du réseau sont impliquées, diverses équipes et personnes doivent être impliquées. Divers cas d'utilisation ISE, tels que l'accès en invité, le BYOD, la posture, etc., nécessitent que les points finaux communiquent avec ISE via des périphériques réseau.

II.5.4 Méthodologies d'authentification:

II.5.4.1 IEEE 802.1X :

La norme 802.1x définit un protocole d'authentification et de contrôle d'accès basé sur le client / serveur qui empêche les clients non autorisés de se connecter à un réseau local via des ports accessibles au public. Le serveur d'authentification authentifie chaque client connecté à un port de commutateur et attribue ce port à un VLAN avant de mettre à disposition les services offerts par le commutateur ou le réseau local. [30]

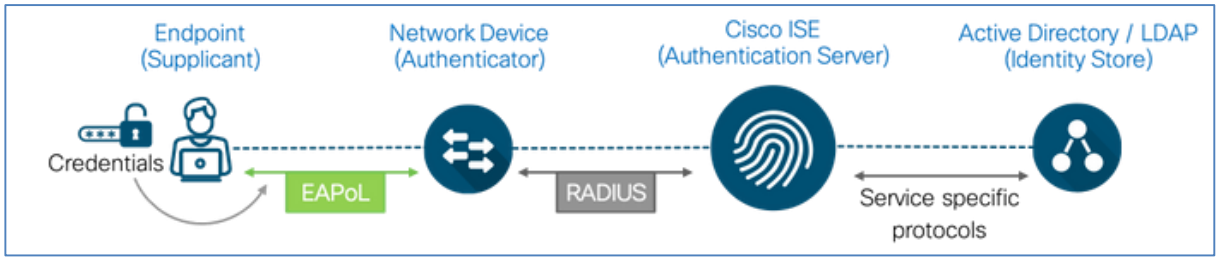

Figure. II. 8. 802.1x Authentification[34]

Jusqu'à ce que le client soit authentifié, le contrôle d'accès 802.1X autorise uniquement le trafic EAPOL (Extensible Authentication Protocol over LAN) via le port auquel le client est connecté. Une fois l'authentification réussie, le trafic normal peut transiter par le port.

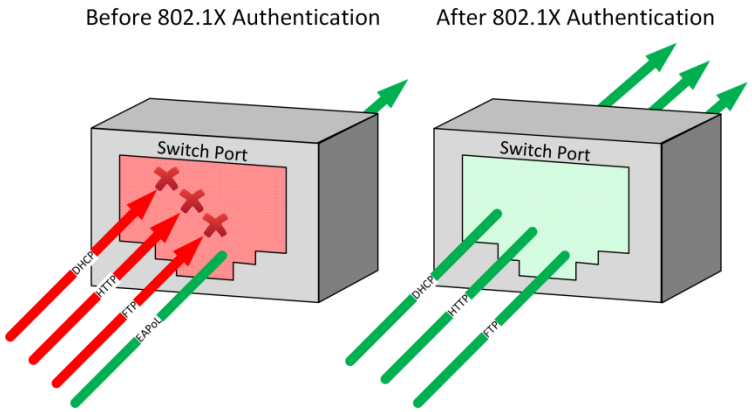

Figure. II. 9. Authentification 802.1x port de commutateur[34]

II.5.4.2 MAC Authentication Bypass (MAB) :

MAB active le contrôle d'accès basé sur le port en utilisant l'adresse MAC d'un endpoint. Un port compatible MAB sur le commutateur peut être activé ou désactivé de manière dynamique en fonction de l'adresse MAC du périphérique qui s'y connecte. Les adresses MAC des endpointdoivent sont ajoutées à la liste blanche dans une base de données présente dans ISE ou dans un emplacement externe afin de permettre l'accès réseau aux endpoint connus. MAB n'est pas vraiment une méthode d'authentification; il fonctionne davantage comme un contournement d'authentification lorsqu'un point de terminaison n'est pas en mesure d'effectuer l'authentification 802.1X. Bien que le MAB puisse protéger les réseaux contre les accès non autorisés, il ne constitue pas une alternative sécurisée à 802.1X car les adresses MAC peuvent être falsifiées facilement.

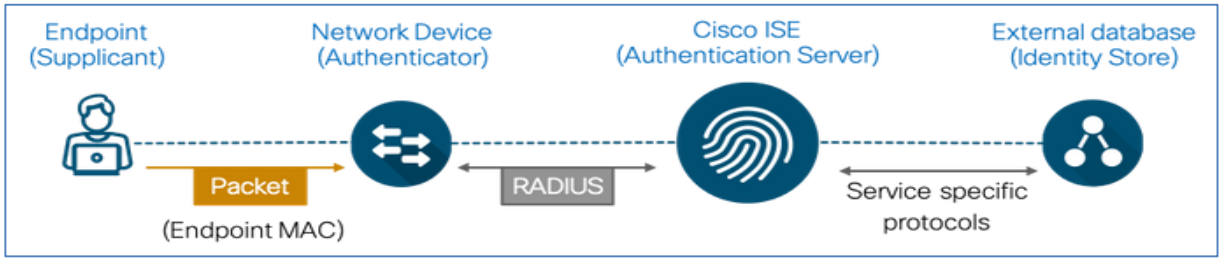

Figure. II. 10 .*MAB Authentification*[34]

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 MAB a réussi, l'identité du endpoint est connue et tout le trafic provenant de ce endpoint est autorisé. Le commutateur effectue le filtrage des adresses MAC source afin de garantir que seul le point de terminaison authentifié par MAB est autorisé à envoyer du trafic. [31]

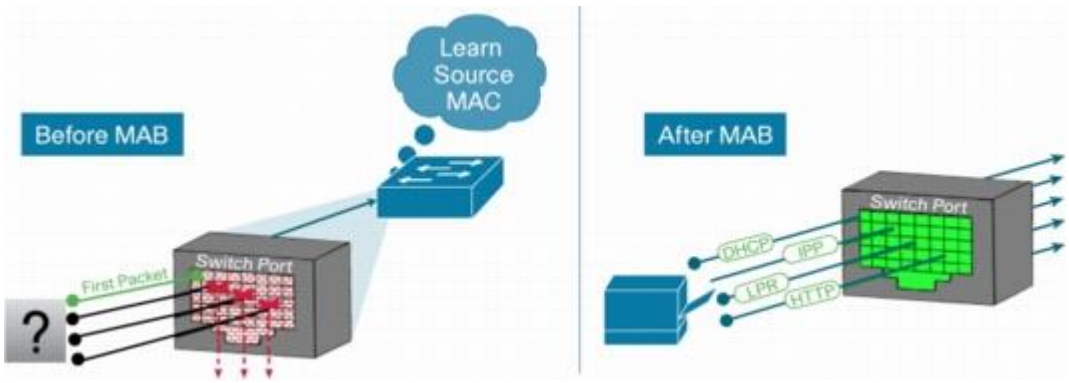

Figure. II. 11. Accès réseau par défaut avant et après IEEE MAB[31]

II.5.4.3 Web Authentification :

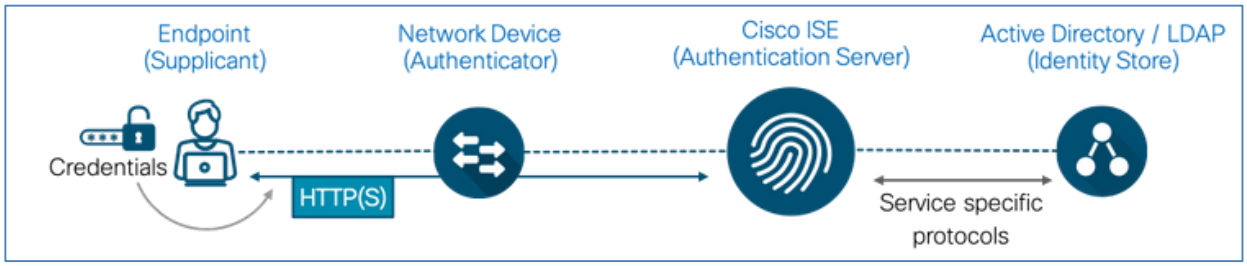

Figure. II. 12.Web Authentification[34]

Les authentifications Web sont généralement utilisées pour intégrer des utilisateurs invités à un accès Internet. Les plates-formes Cisco offrent plusieurs options, l'authentification Web locale (LWA) et l'authentification Web centrale (CWA).

Dans le premier cas, les pages Web sont hébergées dans des périphériques réseau tels qu'un commutateur ou un contrôleur de réseau local sans fil. Dans le second, tous les portails Web sont hébergés de manière centralisée sur ISE. CWA, qui est la méthode préférée, est généralement une session MAB avec une autorisation de redirection d'URL sur le port du commutateur. Jusqu'à ce que le endpointcorrespondant soit authentifié avec succès, le trafic Web du endpointest redirigé vers ISE via un portail de connexion permettant aux utilisateurs finaux de saisir leurs informations d'identification. Une fois l'authentification réussie, ISE initie un changement de l'autorisation (Change-of-Authorization CoA) afin de permettre un accès supplémentaire.

II.5.4.4 EasyConnect :

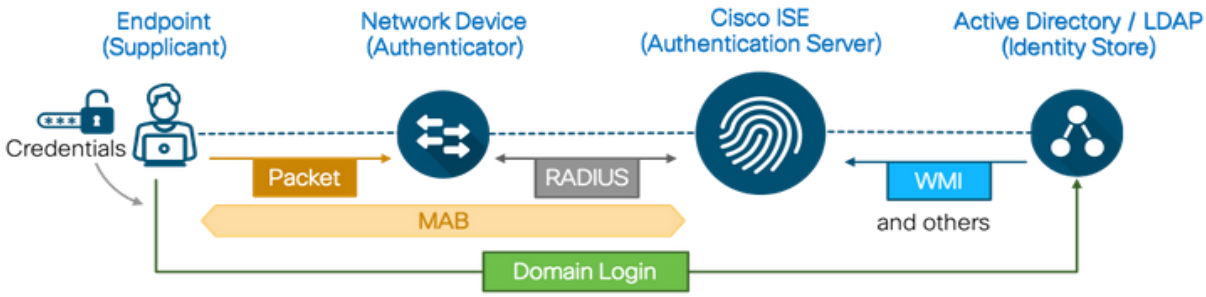

Figure. II. 13.EasyConnect Authentification[34]

La fonctionnalité Cisco ISE EasyConnect permet aux entreprises d'implémenter un accès réseau basé sur l'identité sans avoir besoin de 802.1X. Aucun suppliant ou configuration de suppliant n'est nécessaire sur les ordinateurs d'extrémité. Une session EasyConnect, similaire au flux CWA, commence par un contournement de l'authentification

MAC. ISE découvre l'emplacement, l'adresse MAC et les adresses IP d'un end point par le biais d'une session MAB initiale. Cette session MAB initiale est autorisée avec un accès limité depuis ISE pour permettre à un endpoint géré par Windows Active Directory d'effectuer une connexion de domaine Windows. Une fois la connexion au domaine réussie, le mappage ID utilisateur-adresse IP du contrôleur de domaine Active Directory (AD) est extrait vers ISE et fusionné avec la session MAB initiale. Une fois que l'ID utilisateur et son appartenance au groupe AD sont résolus, ISE modifie l'autorisation pour autoriser un accès supplémentaire.

Une comparaison des différentes méthodes d'authentification :

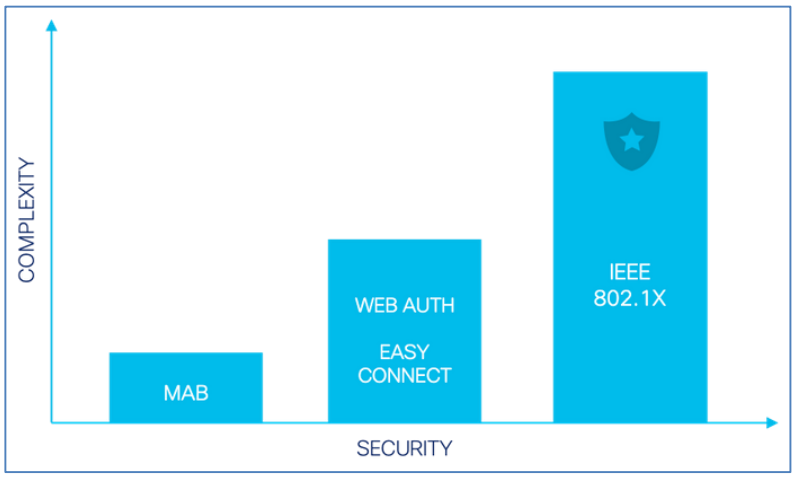

Figure. II. 14. Analyse de complexité des méthodes d'authentification[34]

IEEE 802.1X est la méthode d'authentification la plus sécurisée et la plus flexible. Plusieurs méthodes EAP permettent de gérer divers types d'informations d'identification, en fonction du endpoint et du type d'environnement. Bien que les options Authentification Web et EasyConnect fournissent le contexte d'ID utilisateur nécessaire pour la visibilité et le contrôle d'accès, elles sont limitées à des types de points de terminaison spécifiques. Par exemple, l'authentification Web requiert une interaction de l'utilisateur et un périphérique avec un navigateur Web compatible. EasyConnect ne fonctionne que pour Windows. Points de terminaison gérés par Active Directory. Enfin, MAB est une méthode d'authentification moins sécurisée et un mécanisme de secours pour IEEE 802.1X, mais constitue l'option la plus simple pour configurer le niveau de base d'accès contrôlé.[34]

II.5.5 Méthodologies d'autorisation:

Une stratégie d'autorisation ISE est composée de règles d'autorisation définies pour un utilisateur spécifique et un groupe d'utilisateurs afin d'autoriser, de refuser ou de fournir un accès limité aux ressources réseau. Les profils d'autorisation vous permettent de choisir les attributs à renvoyer lorsqu'une demande RADIUS est acceptée ou rejetée à l'aide de commandes de type d'accès RADIUS ACCESS-ACCEPT et ACCESS-REJECT. L'autorisation d'accès limité peut varier d'un environnement à l'autre.

II.5.5.1 Affectation dynamique de VLAN :

L'un des moyens traditionnels de limiter l'accès au réseau consiste à placer des endpoints différents VLAN en fonction de leur rôle. L'accès aux endpoints dans des VLAN spécifiques peut être contrôlé par des règles définies aux limites de la couche 3, telles que les routeurs ou les pare-feu. ISE peut autoriser des endpoints sur des VLAN spécifiques à l'aide d'un nom ou d'un numéro de VLAN. De plus, dans les plates-formes telles que les gammes Cisco Catalyst 2960X, 3650, 3850 et 9300, les VLAN peuvent être appliqués par adresse MAC.

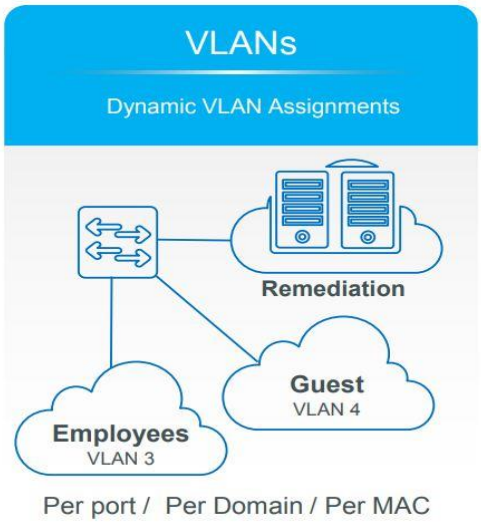

Figure. II.15Affectation dynamique de VLAN[34]

II.5.5 .2 Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès peuvent être utilisées pour contrôler l'accès au réseau au niveau du port. Ils peuvent soit être téléchargés sur le réseau depuis ISE, soit être configurés localement sur un commutateur et être référencés par ISE lors de l'autorisation. L'autorisation d'ACL nommée peut être effectuée avec un attribut standard RADIUS appelé ID de filtre, en utilisant le nom de l'ACL. Pour les téléchargements ACL, une liste ACL par utilisateur ou une liste ACL téléchargeable (dACL) peut être utilisée. Ces deux options de téléchargement de la liste de contrôle d'accès utilisent des paires de valeurs d'attribut RADIUS (AVP) personnalisées de Cisco. Alors que les ACL par utilisateur ont une limite de 4000 caractères, les dACL n'en ont pas. Toutefois, la recommandation pratique pour les dACL est 64 entrées de contrôle d'accès (ACE).

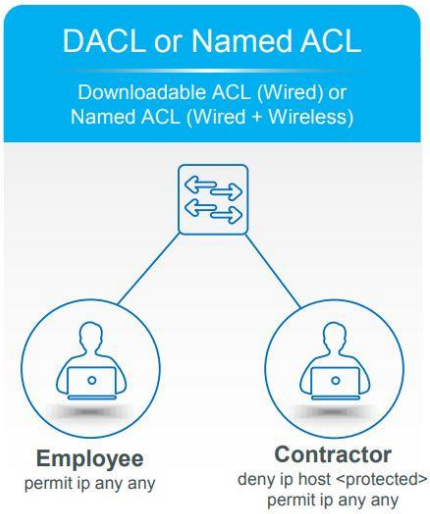

Figure. II. 16 Listes de contrôle d'accès [34]

II.5.5.3 Security Group Tags (SGTs):

Les SGT offrent une alternative efficace à la segmentation basée sur le VLAN. Tout comme l'autorisation VLAN, l'affectation d'un SGT seul à un endpointne contrôle pas l'accès. À la place, après les attributions SGT, les endpoints doivent être soumis à des règles d'application de sortie basées sur les SGT. Notez que bien que dans la plupart des cas, un accès basé sur l'identité soit nécessaire pour la segmentation basée sur SGT, ce document ne traite pas de la segmentation basée sur les balises de manière détaillée.

II.5.5.4 Redirection d'URL :

Cette ACL définit le trafic qui est redirigé vers ISE pendant les scénarios CWA, BYOD et Posture. Tout trafic autorisé par liste de contrôle d'accès est redirigé (192.168.1.10 dans l'exemple ci-dessous). Le refus implicite empêche la redirection des autres types de trafic. Nous vous recommandons de spécifier que seuls les protocoles HTTP et HTTPS doivent être autorisés, car ce trafic est poussé vers la CPU du commutateur. Si un contrôle d'accès supplémentaire est nécessaire avec l'ACL de redirection, nous vous recommandons d'utiliser dACL avec l'ACL de redirection.

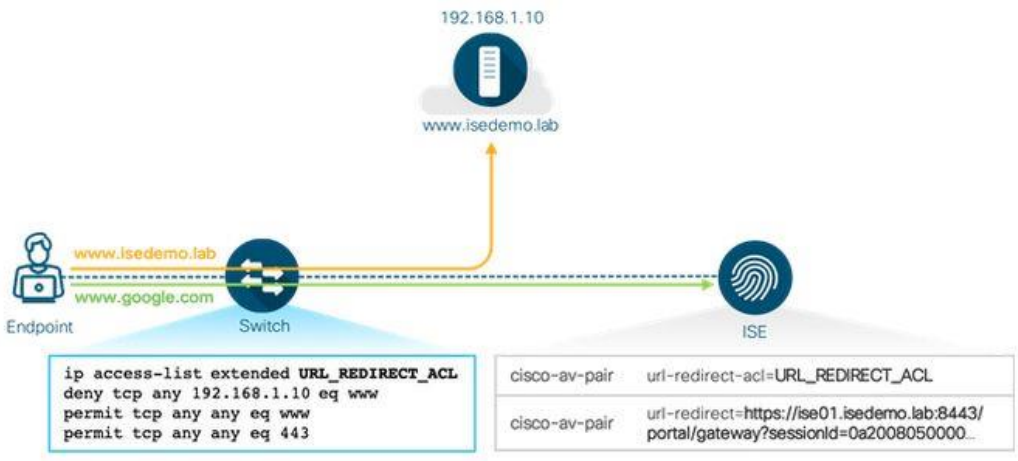

Figure. II. 17Redirection d'URL[34]

II.6.6 la conformité du périphérique avec la stratégie de sécurité :

Le moteur Cisco Identity Services (ISE) et le client Cisco AnyConnect Secure Mobility vérifient l'état de sécurité des périphériques qui se connectent au réseau. La conformité des périphériques n'est que l'un des nombreux cas d'utilisation qui font de ISE et de AnyConnect un élément essentiel de vos opérations réseau et de vos programmes de cybersécurité.

L'évaluation de la posture commence par l'authentification de l'utilisateur et, une fois validée, ISE n'accorde qu'un accès réseau très limité pour lui permettre d'évaluer le périphérique. Pendant l'évaluation, il vérifie la version du système d'exploitation du périphérique, les paramètres système, le logiciel de protection des points finaux et d'autres indicateurs. Si le périphérique manque de correctifs critiques, par exemple, ISE force les systèmes de mise à jour logicielle à les appliquer.

De cette manière, seuls les appareils compatibles obtiennent un accès sécurisé au réseau. [32]

II.5.7les cas d'utilisation de Cisco IdentityServices Engine :

dans cette partie on va voir les différents cas d'utilisation que le moteur ISE (Cisco Identity Services Engine) peut vous permettre de résoudre. [33]

II.5.7.1 invités et Accès sans fil sécurisé :

ISE crée des comptes locaux pour les invités. Ces comptes peuvent être créés par un employé hébergeant l'invité (le sponsor) à l'aide d'un portail intégré ou créés par l'invité lui-même en fournissant des informations de base. L'invité peut recevoir des informations d'identification par e-mail / SMS et l'utiliser pour s'authentifier auprès du réseau et obtenir ainsi un accès au réseau. L'administrateur peut définir le niveau d'accès à fournir à ces utilisateurs.

Après l'authentification réussie, basée sur les informations du groupe, ISE fournit le bon accès à une connexion sans fil, qu'il s'agisse d'une session d'identité passive (Easy Connect), MAB (Passage d'adresses MAC) ou 802.1x.

Ceci peut être réalisé en assignant l'utilisateur à un VLAN, DACL, ACL.

II.5.7.2 sécurisé l'accès filaire :

Sécuriser le réseau câblé est essentiel pour empêcher les utilisateurs non autorisés de connecter leurs périphériques au réseau. pour cela ISE authentifie les utilisateurs et les points de terminaison via 802.1X, l'authentification Web, le MAB et d'autres moyens. ISE peut interroger des sources d'identité externes pour des résolutions d'identité et appliquer les stratégies de réseau appropriées en donnant des instructions aux périphériques de réseau.

II.5.7.3 Bring Your Own Device (BYOD) " Apportez votre propre appareil " :

De nombreuses organisations ont mis en place une politique permettant aux employés de connecter leurs appareils personnels, tels que les smartphones, au réseau sans fil de l'entreprise et de les utiliser à des fins professionnelles.

ISE fournit également un portail My Devices, un portail utilisateur, qui permet à l'utilisateur final d'enregistrer leur point de terminaison BYOD et de le marquer comme perdu pour le mettre en liste noire du réseau.

II.5.7.4 Conformité (posture) :

La posture exploite les agents installés et temporaires en regardant à l'intérieur du terminal afin de garantir que les correctifs du système d'exploitation, les filtres anti-virus, tous les éléments, etc., sont installés, activés et mis à jour avant d'autoriser le périphérique à se connecter au réseau.

La solution choisie :

En prenant en considération les fonctionnalités fournies par CISCO ISE et les besoins de l'entreprise, on a opté pour cette solution dont les détails de déploiement de cette solution vont être expliqués dans le chapitre qui suit.

conclusion :

Dans ce présent chapitre, nous avons essayé de mettre en relief le principe de fonctionnement de toute solution NAC, ensuite nous nous sommes attardés sur une solution particulière proposée par Cisco Systems, à savoir la plate-forme ISE.

Dans le chapitre suivant, on va entamer la partie pratique qui a pour but de déployer Cisco ISE dans un réseau câblé afin d'assurer le contrôle de conformité et atteindre les résultats prévues.

Chapitre III : implémentation et mise en place de la solution

III.1 Introduction :

Après avoir achevé les notions théoriques, nous passons à la mise en place de notre solution, qui représente notre tâche principale , Dans ce chapitre nous allons présenter d'abord l'entreprise d'accueil et mettre le point sur la partie pratique. la réalisation d'une solution qui assure le contrôle de conformité des hôtes connectés au réseau d'Algérie Télécom (LET Alger).

III.2 présentation de l'Entreprise Algérie Telecom:

ALGERIE TELECOM est une société par actions à capitaux publics opérant sur le marché des réseaux et services de communications électroniques.

Sa naissance a été consacrée par la loi 2000/03 du 5 août 2000, relative à la restructuration du secteur des Postes et Télécommunications, qui sépare notamment les activités Postales de celles des Télécommunications

ALGERIE TELECOM est régie par cette loi qui lui confère le statut d'une entreprise publique économique sous la forme juridique d'une société par actions SPA.

Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs [36]:

- Rentabilité

- Efficacité

- Qualité de service

Les objectifs de l'établissement :

ALGERIE TELECOM est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications ;
- Développer un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.

Organisation d'Algérie Télécom :

ALGERIE TELECOM est organisée en Divisions, Directions Centrales, et Régionales, a cette structure s'ajoutent deux filiales:

- Mobile (Mobilis)

- Télécommunications Spatiales (RevSat)

Le laboratoire des équipements de télécommunications (LET ALGER)

Est un établissement à caractère national dépondant de la direction territoriale d'Alger (Algérie Telecom).

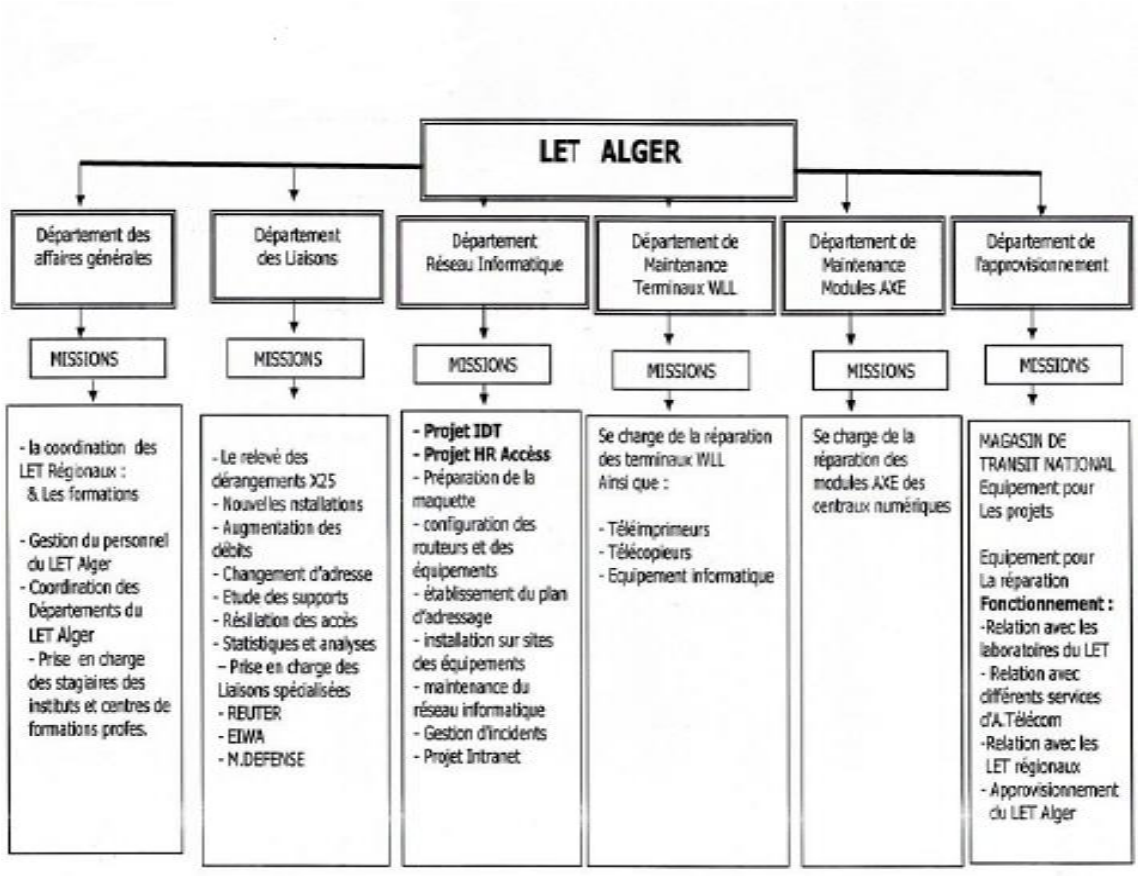

Figure. III. 1 Organisation d'Algérie Télécom

III.3 Architecture de base du réseau :

Afin d'implémenter notre solution, nous avons besoin d'un commutateur et deux machines virtuelles.

Les équipements requis sont :

- Un commutateur (Switch) de gamme Cisco Catalyst 3560

Les machines virtuelles requises serviront à installer :

- Cisco ISE Version 1.1.2
- Un contrôleur de domaine .

L'installation des machines virtuelles s'est déroulée sur le serveur de l'entreprise, Leur déploiement s'effectue au sein du réseau existant de l'entreprise. Par conséquent, le choix des adresses est relié au plan d'adressage disponible ; les adresses à utiliser doivent appartenir au réseau 10.16.250.0 et ayant comme masque 255.255.255.0 .

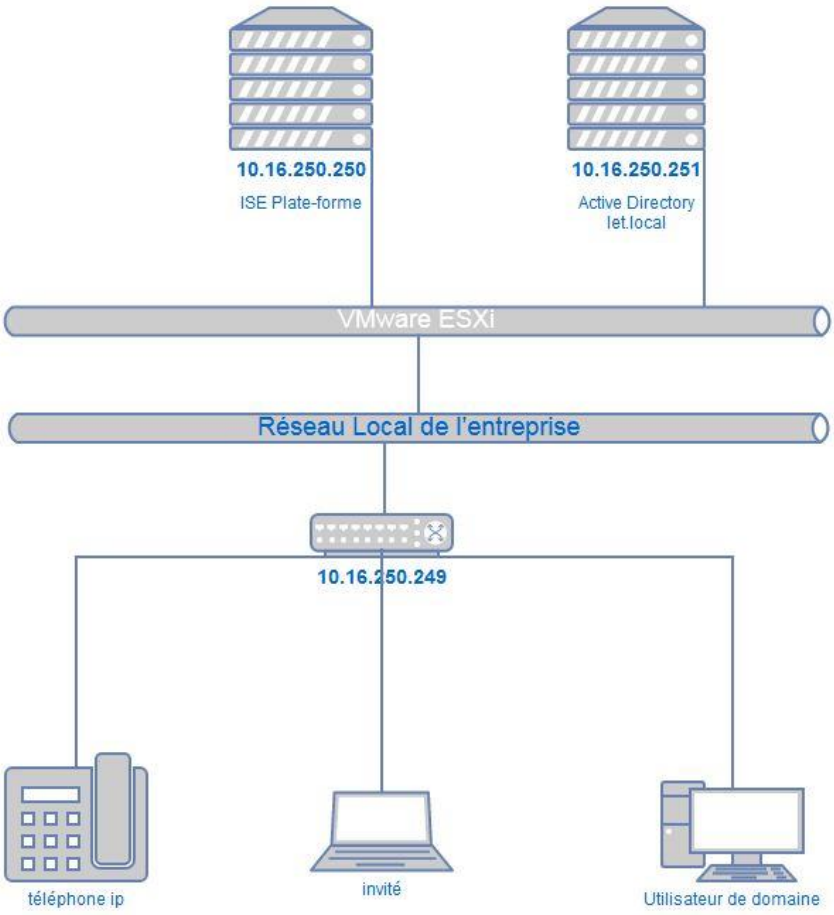

Figure. III. 2 Architecture du réseau

III.3. Installation et intégration de Cisco ISE et Active Directory

1.Installation du contrôleur de domaine (Active Directory)

Active Directory est un service Microsoft server permettant de stocker , gérer et sécurisé les comptes d'utilisateurs .

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau , d'ordinateurs utilisant le système Windows.

pour installé le AD nous avons installé d'abord Windows server 2012 dans une virtuel machine , après ajouter le rôle Active Directory – Directory Services (AD DS)

notre configuration de serveur AD est indiquée dans le tableau suivant :

Nom serveur	ADLET
Adresse ip	10.16.250.251
Masque sous reseau	255.255.255.0
Le nom de domaine	Let.local

tableau III .1configuration de serveur AD

La prochaine étape à suivre pour préparer l'utilisation d'AD pour s'authentifier auprès de Cisco ISE 2.1 consiste à créer un groupe « domaine users » dans Active Directory à utiliser pour authentifie les utilisateur employé .

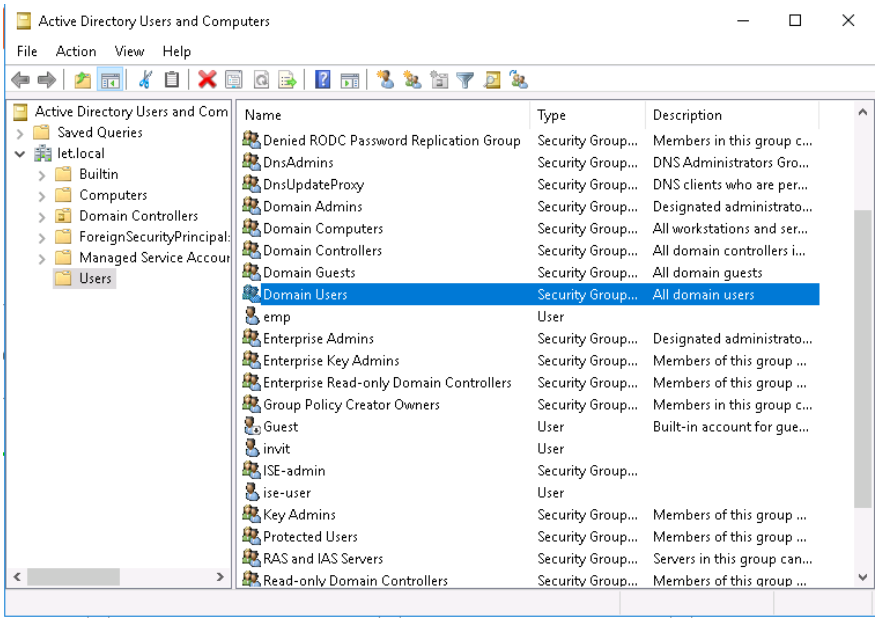

Figure. III. 3 création d'un groupe " domaine users "

Aprés la création de groupe nous avons ajouté des utilisateur a ce groupe :

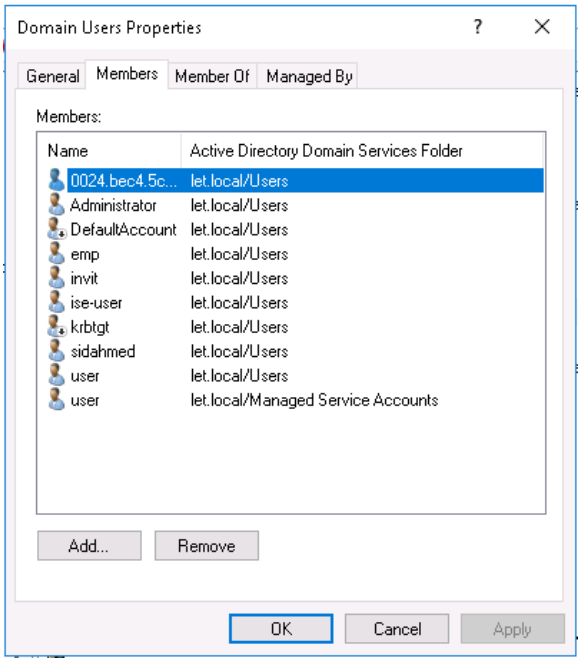

Figure. III. 4 ajout d'un employé au domaine

2.Installation ISE :

pour installé ISE nous avons utilisé un serveur de l'entreprise et instalé ISE dans une machine virtuelle .

ISE requiert une machine virtuelle ayant au minimum les caractéristiques suivantes :

- Mémoire vive de 4 GB
- 4 processeurs (CPUs)
- Mémoire disque de 200 GB
- Deux cartes réseaux (2 NIC)

après le démarrage de la machine, certaines données ont été saisies pour commencer l'installation, comme indiquée dans le tableau suivant :

nom de la machine	Cisco-ise
Adresse ip	10.16.250.250
Masque sous-réseau	255.255.255.0
Passerelle par défaut	16.16.250.249
nom de domaine	let.local

tableau III .2 configuration de ISE

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: cisco-ise
Enter IP address[]: 10.16.250.250
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.16.250.1
Enter default DNS domain[]: 8.8.8.8
Domain name can not be an IP address
Enter default DNS domain[]: at.dz
Enter primary nameserver[]: 8.8.8.8
Add secondary nameserver? Y/N [N]: n
Enter NTP server[time.nist.gov]:
Add another NTP server? Y/N [N]: n
Enter system timezone[UTC]:
Enable SSH service? Y/N [N]: y
Enter username[admin]: admin
Enter password:
Enter password again:
Error: password cannot contain user name
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up network interface...
```

Figure. III. 5 Paramètres de configuration réseau lors de l'installation

3. intégration de AD et ISE :

Avant de pouvoir utiliser Active Directory pour contrôler l'authentification à ISE pour les administrateurs, nous devons joindre ISE au domaine. pour ce cela il faut que :

- ajouter le nom de Domain de Active directory a ISE :

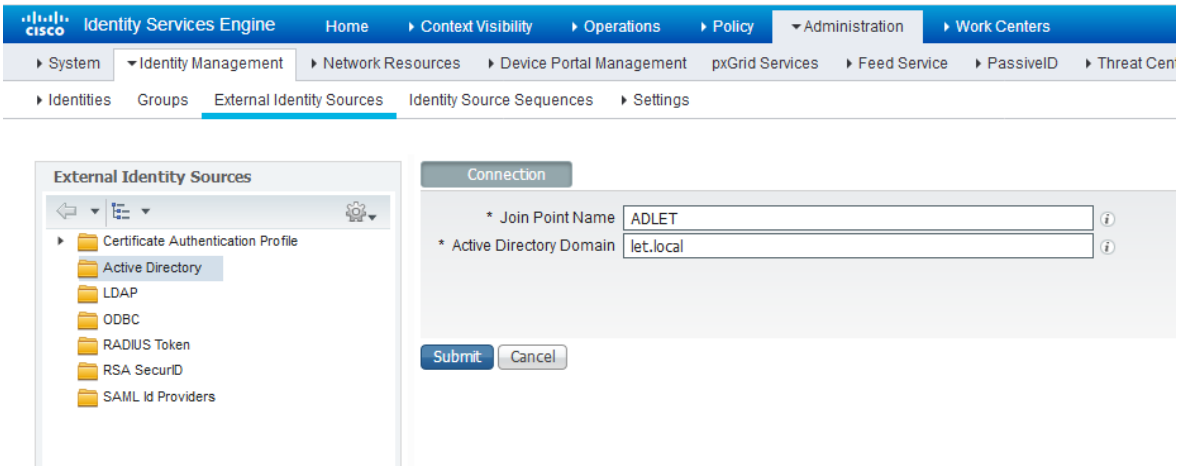

Figure. III. 6. Jointure de ISE à Active Directory

- ajouter compte de l'administrateur du domaine a ISE :

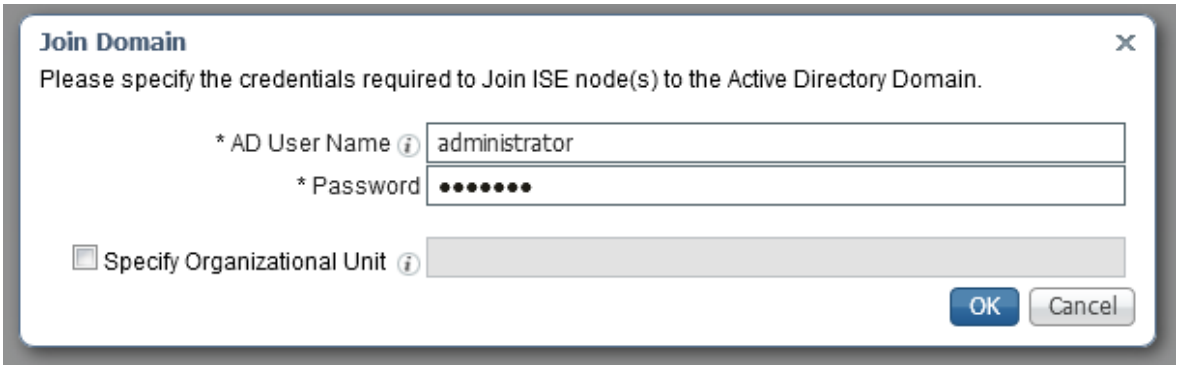

Figure. III. 7 Ajout administrateur de AD

Une fois que ISE a rejoint AD, on obtient :

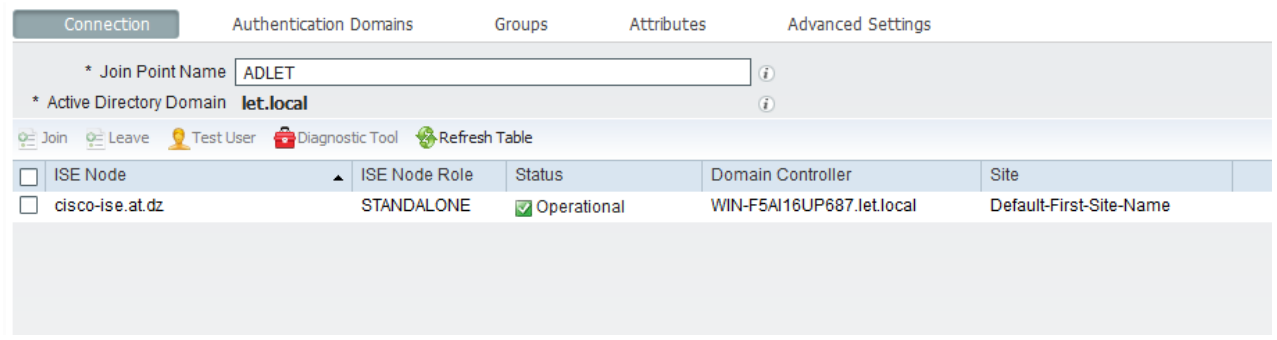

Figure. III.8 résultat de la Jointure de ISE à Active Directory

la dernière étape, ajouter le groupe créé dans AD « domaine users » à ISE; afin que nous puissions le sélectionner ultérieurement.

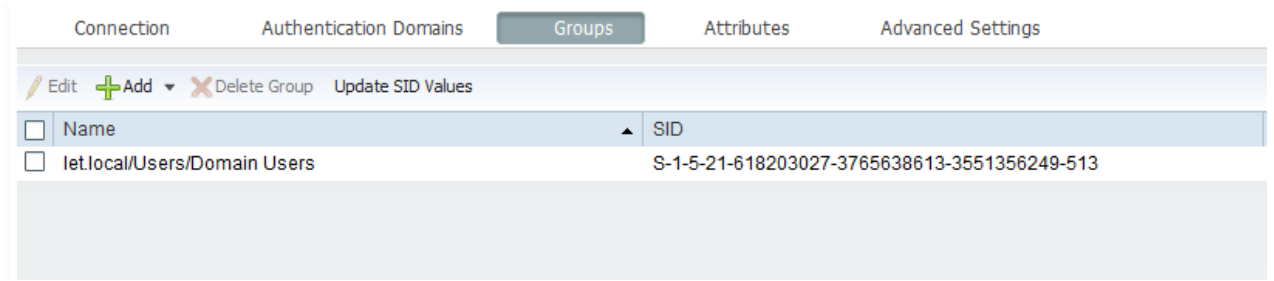

Figure. III.9 ajout de groupe de domaine a ISE

III.4.Configuration de l'ISE :

La configuration ISE comprend les étapes suivantes:

1. Configurez et déployez les services de provisionnement client.
2. Configurez les stratégies d'authentification
3. Configurez les stratégies d'autorisation.
4. Configurez les stratégies de posture.

III.4.1 Configurez et déployez la stratégie d'approvisionnement du client:

Afin d'effectuer une évaluation de la posture et déterminer l'état de conformité d'une machine , Cisco ISE utilise des stratégies de ressources d'approvisionnement client qui déterminent les fichiers d'agent et de configuration à télécharger sur les endpoints en fonction d'attributs tels que l'identité de l'utilisateur et le type de système d'exploitation client.

Avant de pouvoir configurer des stratégies de ressources de provisionnement client, il faut assurer que ces ressources sont disponibles dans Cisco ISE:

- ✓ Les agents de posture.
- ✓ Modules de conformité d'agent.

Les agents de posture :

Les agents de posture sont des applications qui résident sur des ordinateurs clients pour aider l'utilisateur à se connecter au réseau. Il effectue une évaluation de la posture sur l'ordinateur client pour s'assurer qu'il est conforme aux consignes de sécurité du réseau avant d'accéder au réseau.

L'agent NAC :

C'est un agent persistant qui fournit l'évaluation de la posture et la correction pour les ordinateurs clients.il est installé et chargé automatiquement chaque fois qu'un utilisateur se connecte.

L'agent Web :

Un agent temporaire qui fournit une évaluation de la posture temporelle pour les ordinateurs clients, il est retiré de la machine client après la fin de la session de connexion.

Modules de conformité d'agent :

Le module de conformité contient une liste de champs, tels que le nom du fournisseur, la version du produit, le nom du produit et les attributs fournis par OPSWAT qui prennent en charge les conditions de posture de Cisco ISE.

Pour ajouter des ressources d'approvisionnement, on a télécharger l'agent NAC , agent web et Modules de conformité a partir du site cisco.com et on les ajouté comme des ressources existantes à partir d'un ordinateur local .

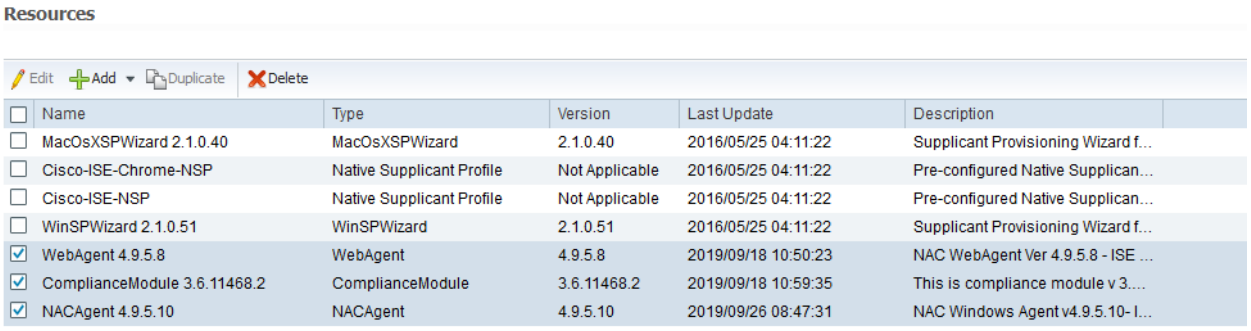

Figure. III.10 la liste des agents

Les stratégies d'approvisionnement du client obligent les utilisateurs du domaine à télécharger l'agent NAC et les utilisateurs invités à télécharger l'agent Web.

Après le téléchargement des agents a ressources d'approvisionnement de client, nous avons définis deux règle de "Client Provisioning» :

la première « Employée_windows » fournit l'agent NAC aux utilisateurs qui sont dans le domaine, et la deuxième « Guest_windows » fournit l'agent temporaire "Web Agent" aux autres utilisateurs "Guests".

Figure. III.11Règles du Client Provisioning

III.4.2 Configurez les stratégies d'authentification :

Les stratégies d'authentification des utilisateurs dans Cisco ISE nous permettent d'authentifier un certain nombre de types de sessions de connexion en utilisant divers protocoles d'authentification standard, notamment le protocole PAP (Password Authentication Protocol), le protocole CHAP (Challenge-Handshake Authentication

Protocol), PEAP (Extensible Authentication Protocol) et EAP (Extensible Authentication Protocol).

Cisco ISE spécifie le protocole autorisé disponible pour les périphériques réseau sur lesquels l'utilisateur tente de s'authentifier et spécifie les sources d'identité à partir desquelles l'authentification de l'utilisateur est validée.

Les stratégies d'authentification basées sur des règles consistent en des conditions basées sur des attributs qui déterminent les protocoles autorisés et la source d'identité ou la séquence source d'identité à utiliser pour le traitement des demandes.

La première règle de notre stratégie support la méthode d'authentification MAC Authentication Bypass (MAB), elle permet de vérifier si l'adresse Mac de périphérique existe dans la liste interne des endpoints .

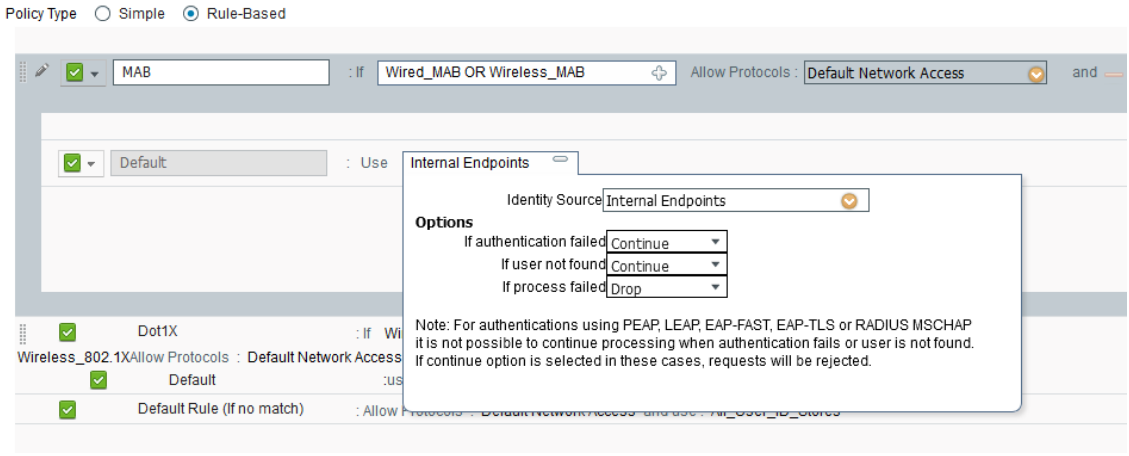

Figure. III.12 Règles d'authentification MAB

La deuxième règle basée sur la méthode 802.1X, cette règle authentifie les comptes utilisateurs à partir du Active directory.

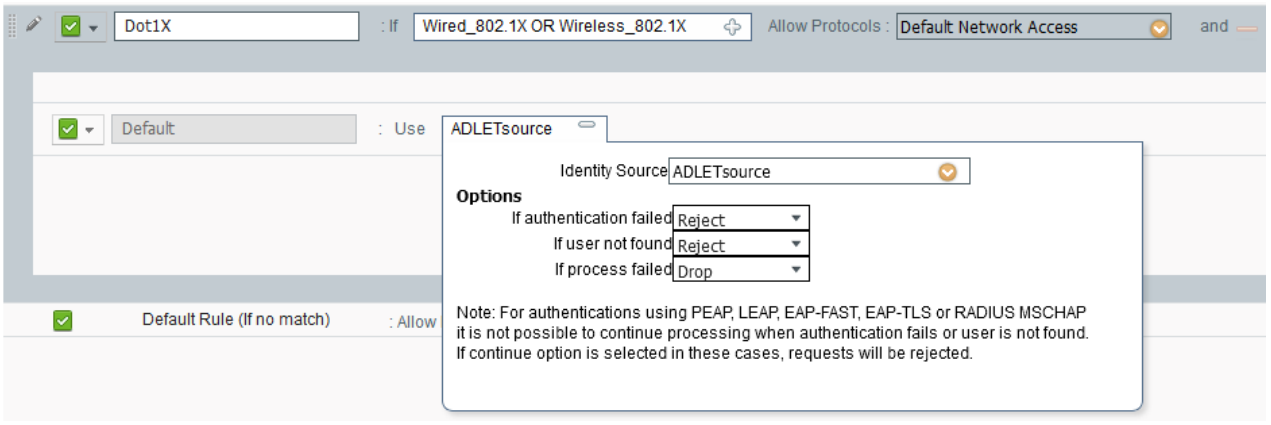

Figure. III.13Règles d'authentification 802.1x

III.4.3 Configurez les stratégies de posture :

Posture est un service qui permet de vérifier la conformité de tous les endpoints qui se connectent à un réseau et conforme aux stratégies de sécurité de l'entreprise.

3.1 Conditions de posture :

Une condition composée contient une ou plusieurs conditions simples, elle peut être associée à une exigence de posture.

Une condition de posture peut être l'une des conditions simples suivantes

- Conditions de fichier - Une condition qui vérifie l'existence d'un fichier, la date d'un fichier et les versions d'un fichier sur le client.
- Conditions du registre - Une condition qui vérifie l'existence d'une clé de registre ou la valeur de la clé de registre sur le client.
- Conditions d'application - Une condition qui vérifie si une application ou un processus est en cours d'exécution ou ne s'exécute pas sur le client.

Le service Posture utilise des contrôles internes basés sur les conditions de composition antivirus et antispyware (AV / AS)

Cisco ISE charge les conditions de composition antivirus et antispyware préconfigurées dans les pages de condition composite AV et AS. Ces conditions composées peuvent vérifier si les produits antivirus et antispyware spécifiés existent sur tous les clients. Lors de l'ajout d'une condition d'antivirus et après le choix du système d'exploitation, la liste des vendeurs s'affiche :

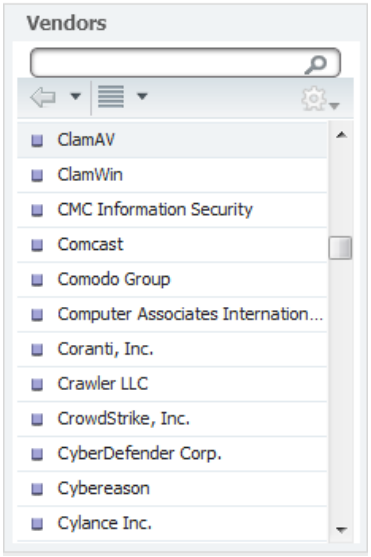

Figure. III.14 liste des vendeurs d'antivirus

A partir de cette liste de fournisseur antivirus, nous avons choisi ClamWin comme un antivirus installé sur tous les ordinateurs des employés de notre entreprise, ensuite nous avons créé deux conditions de posture :

3.1.1 ClamWin_AV_Installed :

une condition de posture AV qui valide l'installation de ClamWin AV sur un endpoint . Ce contrôle sera utilisé dans les exigences de posture appliquées aux employés.

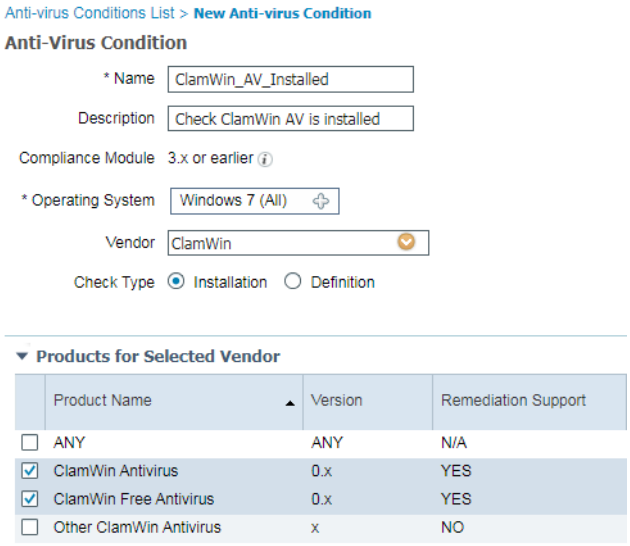

Figure. III.15 condition d'installation clamwin

3.1.2 Any_AV_Installed

Une condition de posture AV qui valide l'installation de tout AV pris en charge sur une machine. Ce contrôle sera utilisé pour les exigences de posture appliquées aux utilisateurs invités.

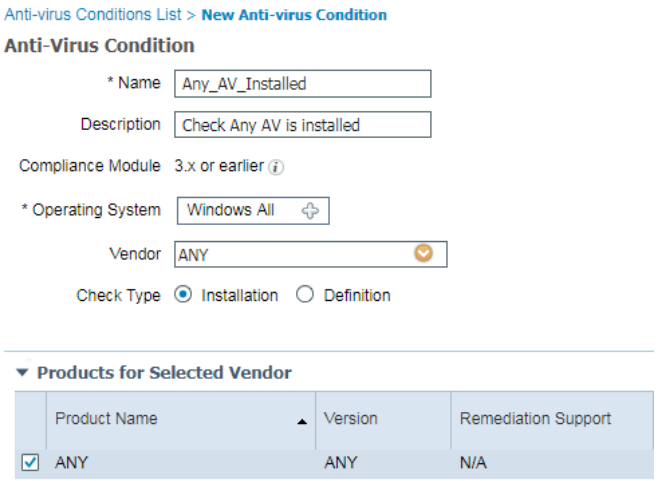

Figure. III.16 condition d'installation un AV

3.2 Posture remédiation :

Une correction de lien permet aux clients de cliquer sur une URL pour accéder à une page ou à une ressource de correction. L'agent client ouvre un navigateur avec le lien et permet aux clients de se corriger pour la conformité.

La page correction de lien affiche toutes les corrections, ainsi que leur nom et description, ainsi que leurs modes de correction.

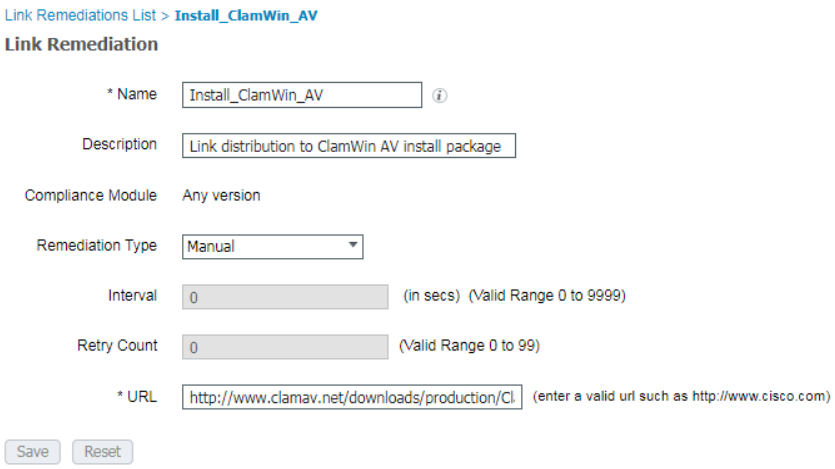

Figure. III.17 Ajout du fichier de remédiation

3.3 Les exigences de posture :

Une exigence de posture est un ensemble de conditions composées avec une action de correction associée pouvant être liée à un rôle et à un système d'exploitation. Tous les clients qui se connectent à votre réseau doivent satisfaire aux exigences obligatoires lors de l'évaluation de la posture pour devenir conformes sur le réseau.

Les exigences de posture qui seront appliquées aux employés et aux utilisateurs invités :

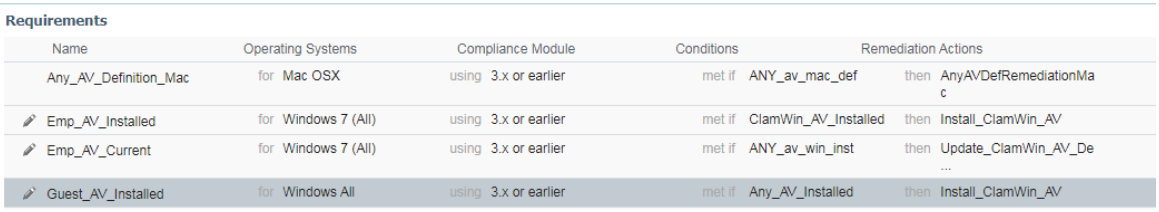

Figure. III. 18 définition de la règle d'exigence

A la fin notre stratégie de posture assure que ClamWin AV est installé et à jour sur les ordinateurs des employés de Windows 7 et que tout AV pris en charge est installé et à jour sur les ordinateurs des utilisateurs invités.

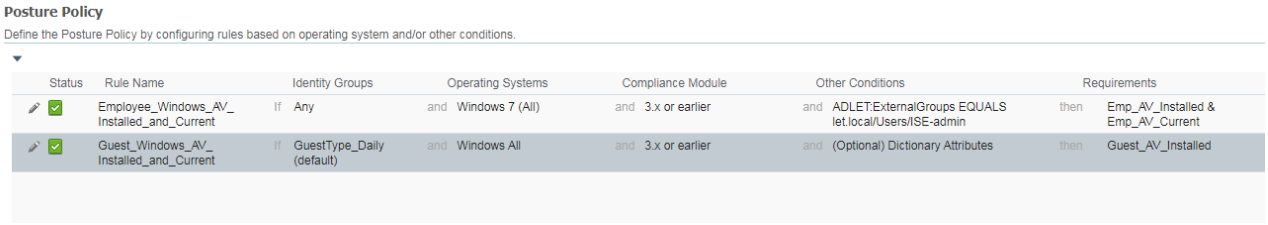

Figure. III. 19 les Règles de posture

3.4 Le statut de conformité :

Après la vérification la conformité de la machine par rapport à la règle de posture, le statut de conformité peut être:

Inconnu: Aucune donnée n'a été collectée pour déterminer la conformité de la posture.

Non conforme: une évaluation de la posture a été effectuée et une ou plusieurs exigences ont échoué.

Conforme: machine est conforme à toutes les exigences obligatoires.

III.4.4 Configurez les stratégies d'autorisation :

La stratégie d'autorisation place les types de l'accès et de services à accorder aux machines basés sur leurs attributs tels que l'identité, la méthode d'accès, et la conformité aux stratégies de posture. Les stratégies d'autorisation dans cet exemple s'assurent que des machines qui ne sont pas posture conforme sont mises en quarantaine. C'est-à-dire, les machines sont accordés l'accès limité suffisamment pour provision le logiciel agent et au remediate ont manqué des conditions requises. Seulement on accorde des machines conformes de posture l'accès au réseau privilégié.

Les stratégies d'autorisation associent des règles à des identités d'utilisateur et de groupe spécifiques pour créer les profils correspondants. Lorsque ces règles correspondent aux attributs configurés, le profil d'autorisation correspondant accordant l'autorisation est renvoyée par la stratégie et l'accès au réseau est autorisé en conséquence.

4.1 la création de dACL :

Entrée dACL	La description
permit udp any any eq domain	Autoriser le système de noms de domaine (DNS) pour la résolution de noms
permit udp any eq bootpc any eq boot ps	Autoriser DHCP
permit tcp any host 10.16.250.250 eq 8443	Autoriser le portail CWA / Cient Provisioning Portal (CPP) sur le nœud ISE Policy Service
permit tcp any host 10.16.250.250 eq 8905	Autoriser la découverte d'agents directement sur le nœud Service de politique
permit udp any host 10.16.250.250 eq 8905	Autoriser la découverte d'agents et les connexions persistantes
permit tcp any host 10.16.250.250 eq 8909	Autoriser l'installation de l'agent Cisco NAC, de l'agent Web Cisco NAC et de l'assistant de provisionnement des supplicants
permit udp any host 10.16.250.250 eq 8909	
permit IP any host 192.230.240.8	Autoriser le trafic vers le serveur de base de données de définitions ClamWin; cette entrée est spécifique à cet exemple
deny ip any any	Refuser tout autre trafic

Tableau III .3 listes des ACL

4.2 La création de profil d'autorisation :

Pour créer un profil d'autorisation nous avons le choix entre plusieurs options telles que l'affectation à un VLAN, la redirection vers un URL (portail d'authentification Web, portail de Client Provisioning, URL externe, etc.) à base d'une liste de contrôle d'accès, et même l'application d'un ACL sur le port du commutateur.

Dans notre stratégie on a créé deux profils d'autorisation :

le premier profil d'autorisation pour les utilisateurs de l'agent NAC authentifié / 802.1X nommé **Posture_Remediation** . Le profil exploite à la fois la nouvelle liste DACL pour le contrôle d'accès au port et la liste de contrôle d'accès URL pour la redirection du trafic.

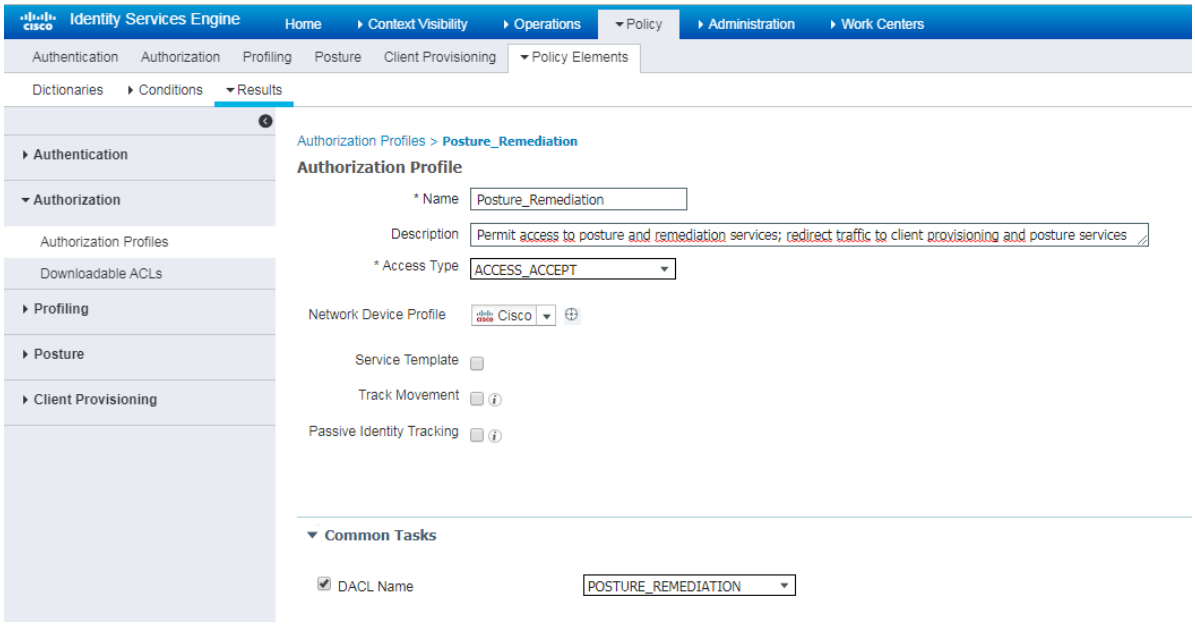

*Figure. III.20 profil d'autorisation " **Posture_Remediation** "*

Remarque : L'ACL ACL-POSTURE-REDIRECT ACL doit être configuré localement sur le commutateur. La liste de contrôle d'accès est référencée par son nom dans la stratégie d'autorisation ISE. Pour l'ACL de redirection de commutateur, les entrées d'autorisation déterminent quel trafic doit être redirigé vers ISE .

le deuxième profil d'autorisation pour les utilisateurs Web Agent authentifiés par le Web et nommés **CWA_Posture_Remediation** . Le profil permettant de rediriger les utilisateurs vers le portail invité en se référant à la liste d'accès définie au niveau de commutateur .

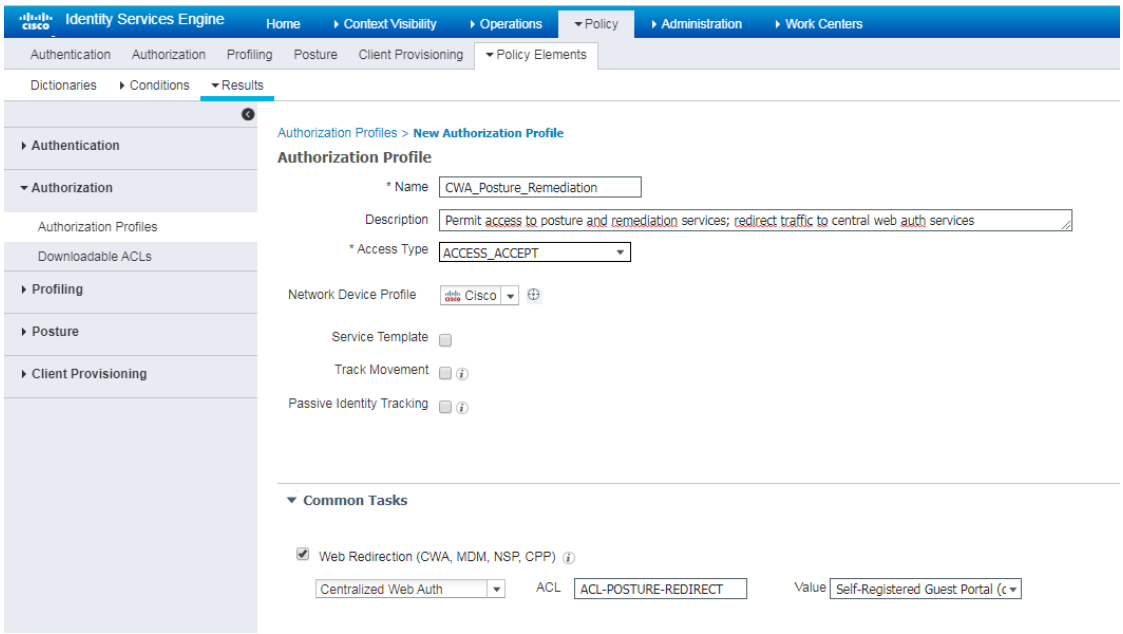

Figure. III. 21 profil d'autorisation CWA

La différence entre les deux profils réside dans l'attribut URL redirection cisco-av-pair. Les utilisateurs invité qui doivent être authentifiés sont redirigés vers le portail invité pour CWA. Une fois authentifiés, les utilisateurs employés sont automatiquement redirigés vers le CPP.

Après la création de profils d'autorisation, nous pouvons définir les règles d'autorisation. Qui comportent trois éléments: nom, attributs et autorisations. L'élément d'autorisation correspond à un profil d'autorisation.

Ces règles autorisent l'accès aux utilisateurs authentifiés au domaine (employé) ou via le portail web (invité) et ayant des machines conformes aux règles de posture.

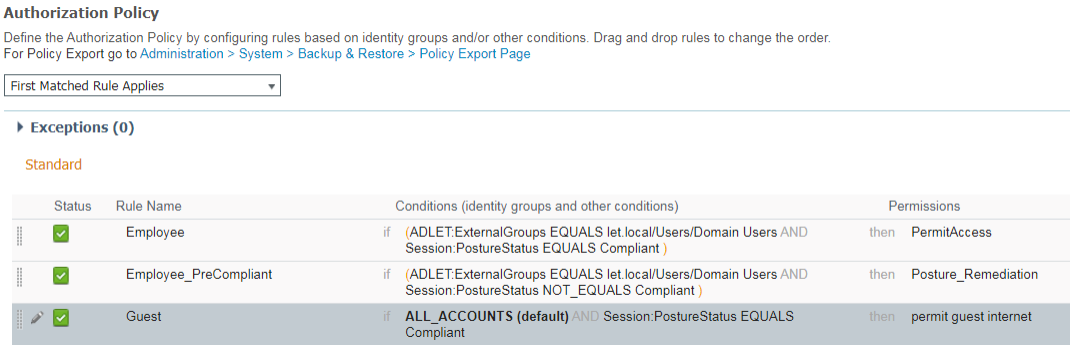

Figure. III. 22 Règles d'autorisation

Les stratégies d'autorisation décrites dans la figure. III 21 garantissent que les endpoints non conformes à la posture sont mis en quarantaine. c'est-à-dire que les endpoints se voient accorder un accès limité suffisant pour fournir le logiciel de l'agent et corriger les exigences en échec. Seuls les endpoints conformes à la posture bénéficient d'un accès réseau privilégié.

III.5. configuration de commutateur :

III.5.1 Activer les fonctions AAA et dot1x :

La commande aaa new-model permet d'activer les fonctions d'authentification, d'autorisation et de comptabilité du Switch .

Les commandes qui suivront définissent les services du serveur RADIUS qui aura la charge d'authentifier les utilisateurs, de leur affecter des profils d'autorisation et Active la comptabilité pour les authentifications 802.1X et MAB .

```
C3750(config)#radius-server attribute 8 include-in-acce cr
C3750(config)#aaa authentication dot1x default group radius
C3750(config)#aaa authorization network default group radius
C3750(config)#aaa accounting dot1x default start-stop group radius
C3750(config)#dot1x system-auth-control
```

Figure. III.23 activation de aaa au niveau du commutateur

III.5.2 Configuration de serveur RADIUS :

Pour que le commutateur peut communiquer avec Cisco ISE en tant que serveur source RADIUS , il faut lui attribué l'adresse de ISE avec une clé. Cette dernière est mentionnée lors de l'ajout du commutateur à la liste des périphériques réseaux au niveau de l'ISE.

La commande radius-server vsa send permet au serveur d'accès au réseau de reconnaître et d'utiliser les attributs de comptabilité et d'authentification propres au fournisseur.

L'utilisation de paramètre *accounting* avec la commande radius-server vsa send limite l'ensemble des attribut vsa au seule attribut de comtabilitie , L'utilisation de paramètre *authentification* avec la commande radius-server vsa send limite l'ensemble des attribut vsa au seule attribut de authentification.

```
C3750(config)#ip radius source-interface Vlan 25
C3750(config)#radius-server attribute 6 on-for-login-auth
C3750(config)#radius-server attribute 25 access-request include
C3750(config)#radius-server host 10.16.250.250 key let2015
C3750(config)#radius-server vsa send accounting
C3750(config)#radius-server vsa send authentication
```

Figure. III.24 activation de serveur radius au niveau du commutateur

après l'authentification et correction de son accès réseau (un utilisateur ayant un accès restreint pour raison de non-conformité) l'utilisateur peut avoir un accès plus étendu. Pour assurer que le commutateur est en mesure de gérer correctement le comportement de changement d'autorisation RADIUS en prenant charge les fonctions de posture de Cisco ISE, le CoA (Change of Authorization) doit être activé au niveau du commutateur.

```
C3750(config)#aaa server radius dynamic-author
C3750(config-locsvr-da-radius)#client 10.16.250.250  server-key let2015
C3750(config-locsvr-da-radius)#ex
```

Figure. III.25 Activation du CoA au niveau du commutateur

III.5.3 Activer la redirection d'URL et device-tracking :

nous avons activer les fonctions d'authentification Web standard pour Cisco ISE, y compris les dispositions relatives à la redirection des URL lors de l'authentification vers la page web via un portail captif .

La configuration de device-tracking (suivi des périphériques) est très critique pour connaître l'adresse IP d'un endpoint et la mapper à sa session d'accès au réseau.

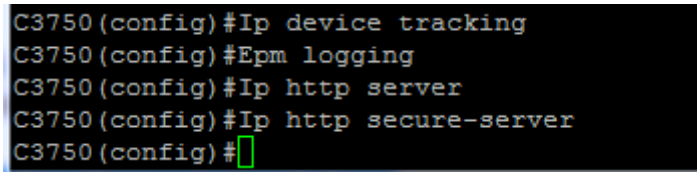

Figure. III.26Activation de HTTP et HTTPS

III.5.4 ACL :

nous avons utilisé deux listes d'accès déclarée au niveau du commutateur:

la premier liste pour la redirection du trafic : tout flux ayant comme réaction "permit" doit être redirigé . Il est à préciser que tout trafic à rediriger autre que HTTP et HTTPS sera rejeté. Le tableau suivant expose les différentes règles déclarées sous la liste d'accès :

Entrées de l'ACL	Description
deny udp any eq bootpc any eq bootps	Refuser tout trafic DHCP
deny udp any any eq domain	Refuser tout trafic DNS
deny udp any host 10.16.250.250 eq 8905	Refuser tout trafic sur le port 8905 deny et tcp a tout adresse 172.25.0.200 eq 8905
deny tcp any host 10.16.250.250 eq 8905	
deny tcp any host 10.16.250.250 eq 8909	Refuser tout trafic sur le port 8909 dédié aux portails CWA et CPP
deny udp any host 10.16.250.250 eq 8909	
deny tcp any host 10.16.250.250 eq 8443	Refuser tout trafic sur le port 8443 Denya tout adresse 172.25.0.200 eq 8909 "client provisioning"
deny ip any host 192.230.240.8	Refuser tout trafic ip serveur antivirus
permit ip any any	Permettre tout autre trafic

tableau III .4 listes des ACL de redirection appliqué au niveau de commutateur

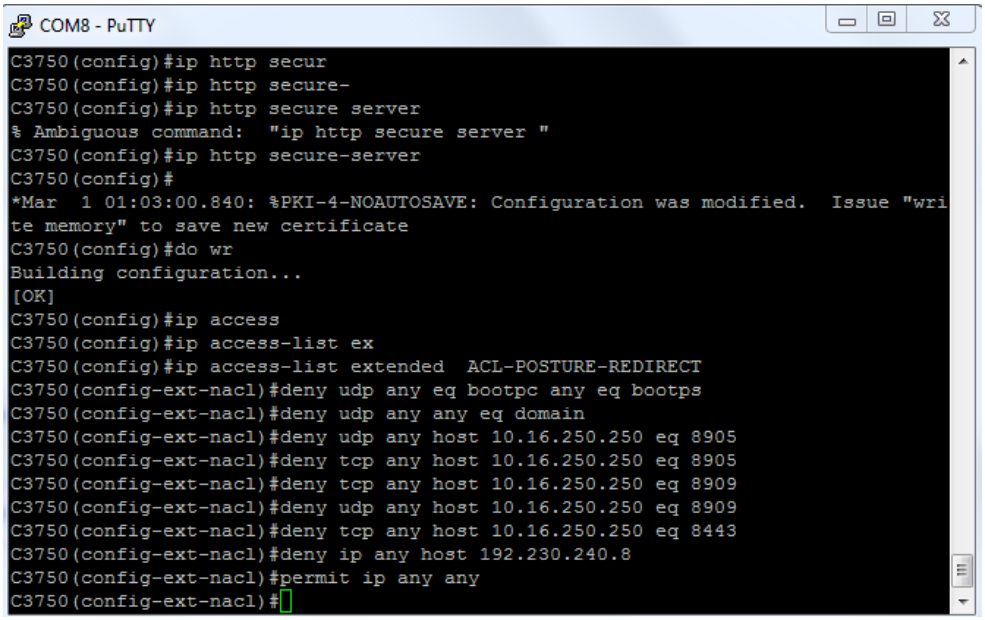

Figure. III.27 configuration ACL de redirection au niveau de commutateur

Une deuxième ACL est appliqué sur le port qui autorise tous les adresses ip :

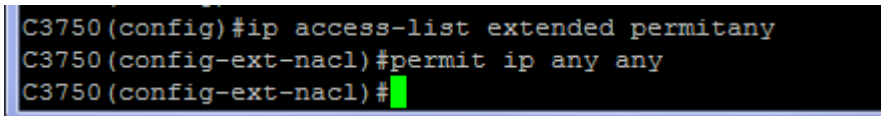

Figure. III.28 ACL d'autorisation adresse ip

III.5.5 Configuration les ports du commutateur:

Pour configuré le port du commutateur, nous avons d'abord Activez les ports du commutateur pour le mode d'accès , et configurer de manière statique le VLAN d'accès , ensuite Active l'authentification 802.1X et MAB sur l'interface faste Ethernet 1/0/3et donne la priorité et l'ordre à 802.1x puis MAB lors de l'authentification .

le demandeur de endpoint doit envoyer un message périodique de démarrage EAP sur LAN (EAPoL-Start) dans le switchport pour accélérer l'authentification. Si un périphérique ne peut pas s'authentifier on utilisant le protocole 802.x a cause de nature et apré attente de delais attribué au protocole 802.x, il peut tanter d'etre authentifie en utilisant le protocole MAB. Si son adresse MAC est dans la base de donnée interne de ISE, il est alors autorisé à accéder au réseau .

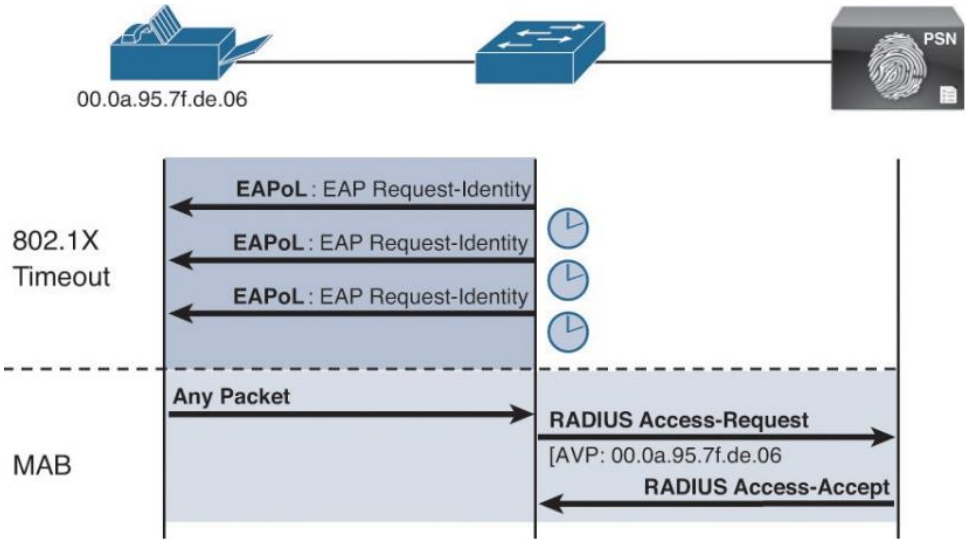

Figure. III.29 diagramme d'authentification

Activer le mode hôte Multi-domain, pour permet à un périphérique de données et à un périphérique vocal, tel qu'un téléphone IP, de s'authentifier sur le même port de commutateur. Le port est divisé en un domaine de données et un domaine vocal, il faut activer Multi-domain.

```
interface FastEthernet1/0/3
 switchport access vlan 10
 switchport mode access
 authentication event fail action next-method
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
```

Figure. III.30 Configuration de l'interface

Conclusion :

Dans ce chapitre nous avons réalisé une architecture réelle qui nous a permis de faire une configurations nécessaires pour déployer la solution de cisco ISE au sein de réseau câblé.

nous avons rencontré plusieurs difficultés en termes de nouveauté de l'équipement et aussi le manque d'expérience concernant l'utilisation de CISCO ISE au niveau de l'entreprise ce qui a rendu difficile de régler les problèmes confrontés.

une phase de test est indispensable afin de valider le comportement des différents composants vis-à-vis des machines tentant d'accéder au réseau.

Chapitre 4 : Test et validation

IV.1 Introduction :

Une fois la solution mise en place, nous procédons à la phase de test dans le but de nous assurer du bon fonctionnement des équipements et de la configuration. La vérification consiste à essayer de se connecter aux réseaux filaire, avec deux scénario :une fois en tant que employé et une fois invité.

IV.2 Test utilisateur de domaine :

Le premier test à effectuer nous permettra de nous garantir du bon déroulement de l'authentification au domaine et de la validation de posture pour un utilisateur du réseau câblé.

La première des chose nous avons activé l'authentification 802.1X sur les cartes réseau Ethernet car par défaut elle est désactiver sur un système Windows.

Nous avons démarrer le service « Configuration automatique de réseau câblé », responsable de l'exécution de l'authentification IEEE 802.1X sur les interfaces Ethernet.

Après avoir lancé "services.msc" et cliqué sur le service correspondant, la fenêtre suivante s'affiche pour démarrer le service :

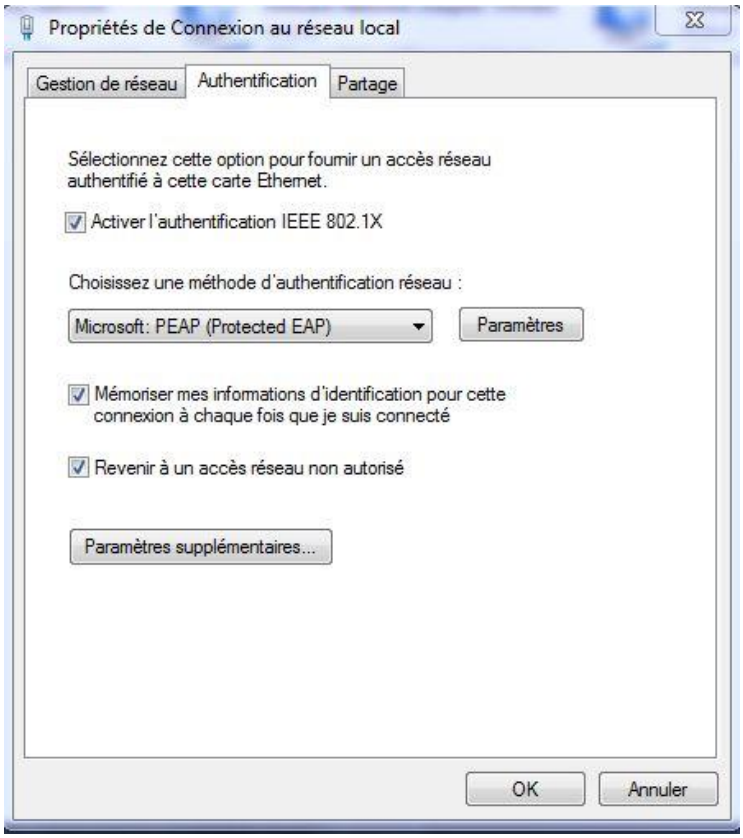

Figure. IV .1. Activation du DOT1X sur la carte Ethernet

après avoir activé l'authentification 802.1X , dans les paramètres de protocole EAP. le client Vérifié l'identité du serveur en validant le certificat et à partir des autorités de certification racines de confiance.

dans la liste, sélectionnez le certificat auto-signé d'ISE.

sélectionnez Configurer puis désactiver l'utilisation automatiquement de la connexion Windows, puis validé ces opération (click sur ok).

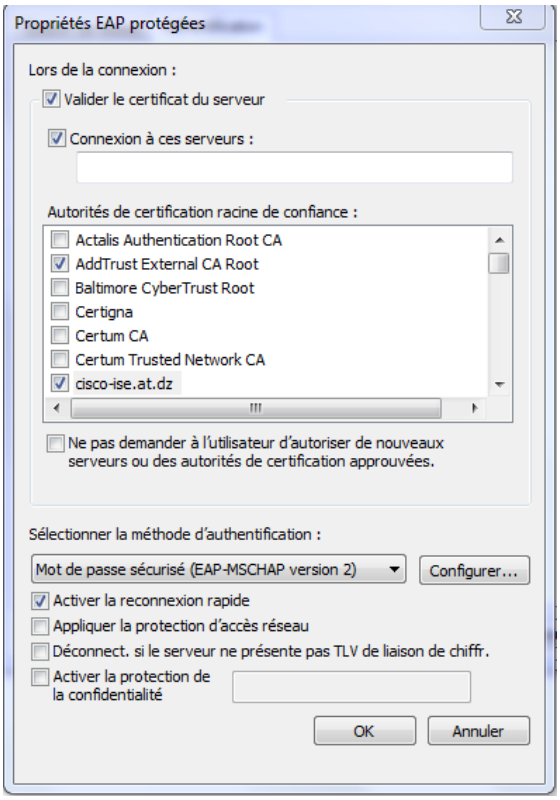

Figure. IV.2 autorisation de certificat ISE

Dès que le branchement du câble sur l'interface Ethernet de la machine , la fenêtre d'authentification s'affiche :

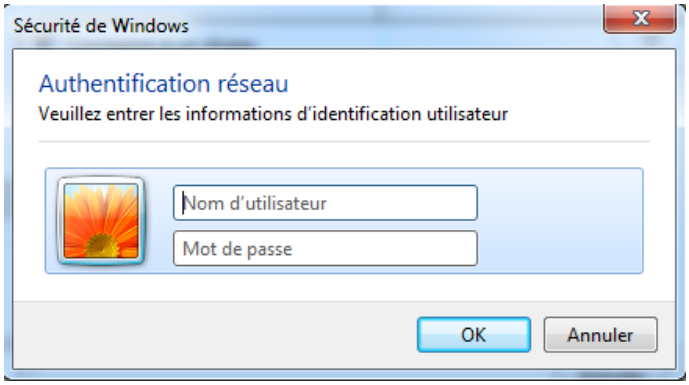

Figure. IV.3 Fenêtre d'authentification

Au niveau de commutateur, nous pouvons observer le déroulement de l'authentification :

```
*Mar 13 01:05:02.742: %AUTHMGR-5-START: Starting 'dot1x' for client (0024.bec4.5c6a) on Interface Fa1/0/3
*Mar 13 01:05:04.739: %LINK-3-UPDOWN: Interface FastEthernet1/0/3, changed state to up
*Mar 13 01:05:12.784: %DOT1X-5-SUCCESS: Authentication successful for client (0024.bec4.5c6a) on Interface Fa1/0/3
*Mar 13 01:05:12.792: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (0024.bec4.5c6a) on Interface Fa1/0/3
*Mar 13 01:05:12.842: %EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0024.bec4.5c6a|
        AUDITSESID=0A10FAF9000000EB3E07ACCD| AUTHTYPE=DOT1X|
        EVENT=APPLY
*Mar 13 01:05:12.842: %EPM-6-AAA: POLICY=xACSACLx-IP-POSTURE_REMEDIATION-5d82435f |
        EVENT=DOWNLOAD-REQUEST
```

Figure. IV.4 authentification coté commutateur

au niveau de ISE, la règle d'autorisation préCompilant est appliqué sur l'employé:

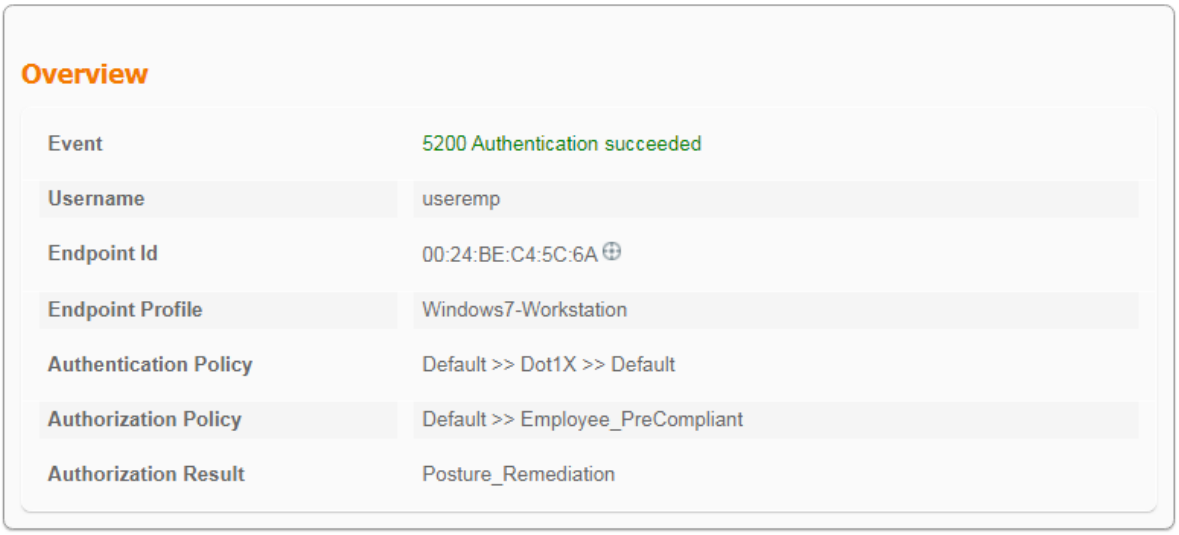

Figure. IV.5 authentification coté ISE

Une fois la session ouverte et en essayant d'accéder au navigateur mozila , nous nous sommes trouvés redirigés vers la page de client provisioning portal a cause de l'application de acl coté commutateur .

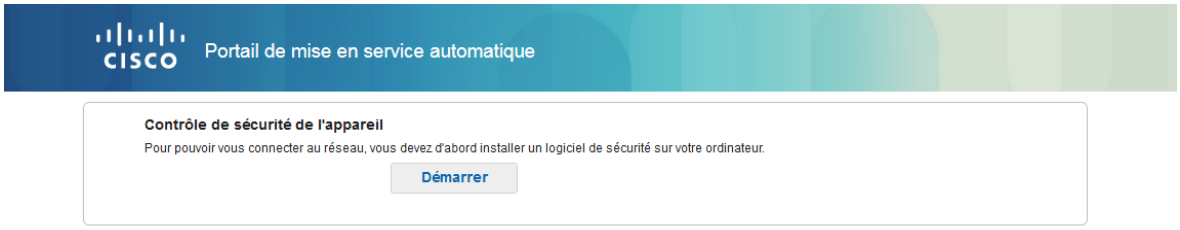

Figure. IV.6 Redirection vers la page de Client Provisioning

ISE oblige le nouveau client a télécharger l'agent NAC.

En cliquant sur le bouton "démarrer ", ISE nous oblige a installé l'agent NAC lors de la première visite et le téléchargement se lance :

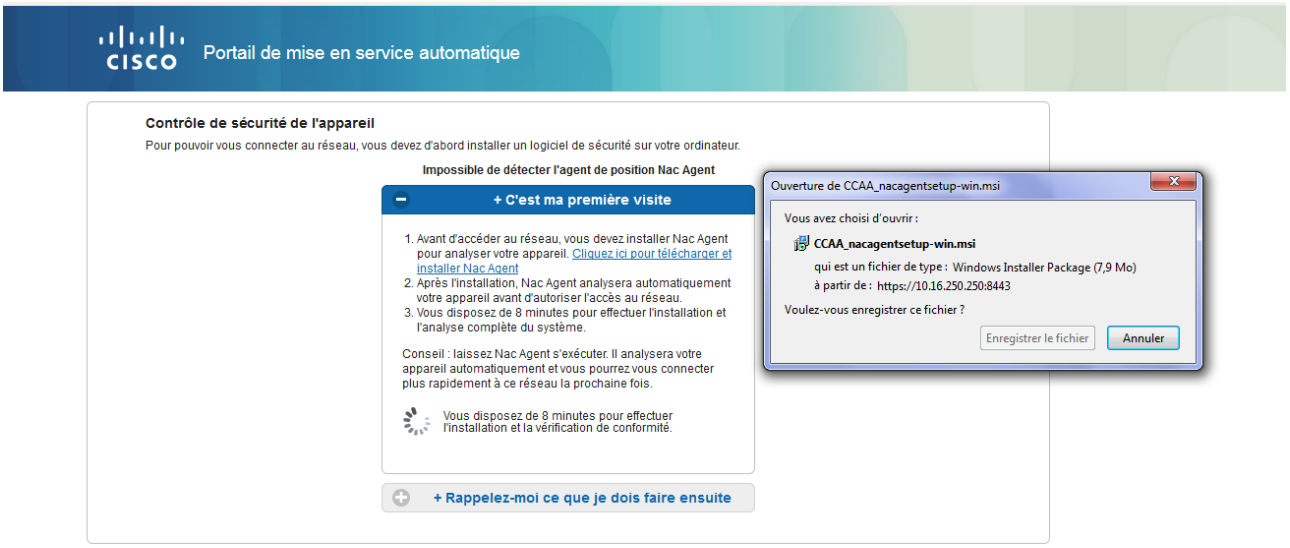

Figure. IV.7 lien de téléchargement agent NAC

après l'installation de NAC Agent qui scan la machine et affiche les informations suivants :

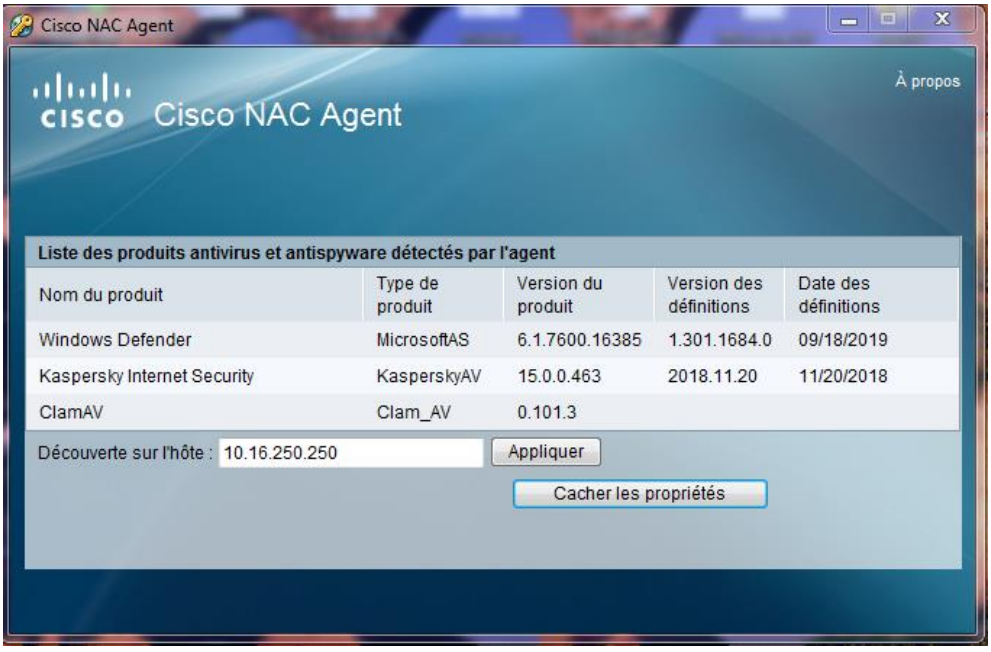

Figure. IV.8 installation de NAC AGENT

L'agent NAC nous indiquer que notre machine n'est pas conforme avec la stratégie de sécurité car notre machine n'a pas l'anti virus ClamWin comme indiqué dans l'image suivante :

Figure. IV.9 message de NAC Agent

pour que la machine soit conforme au stratégie de sécurité , nous avons installé l'anti virus ClamWin :

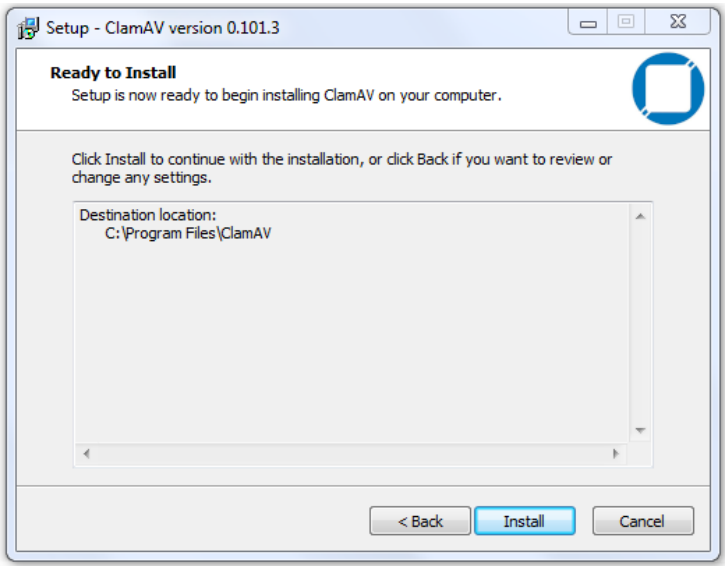

Figure. IV.10 installation de AV ClamAV

Après l'installation l'antivirus ClamWin L'agent NAC nous présente un accès plus étendu au réseau, comme mentionné sur la figure ci-dessous :

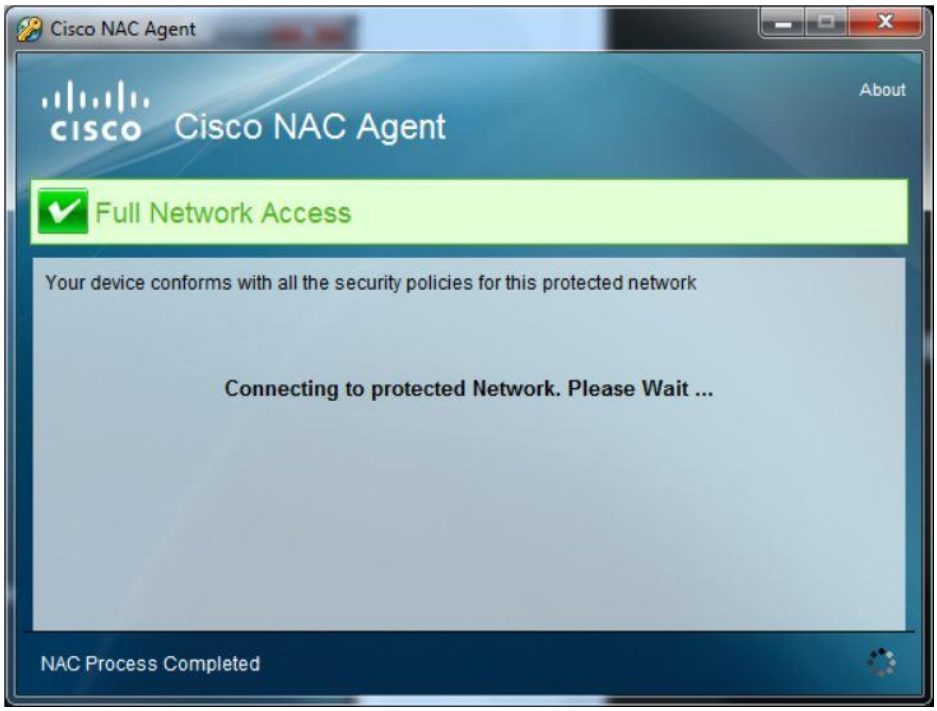

Figure. IV.11 accès autorisé au employée

IV. 3 test invité :

dès qu'un invité se connecte, il se trouve redirigé vers le portail captif sur son navigateur.

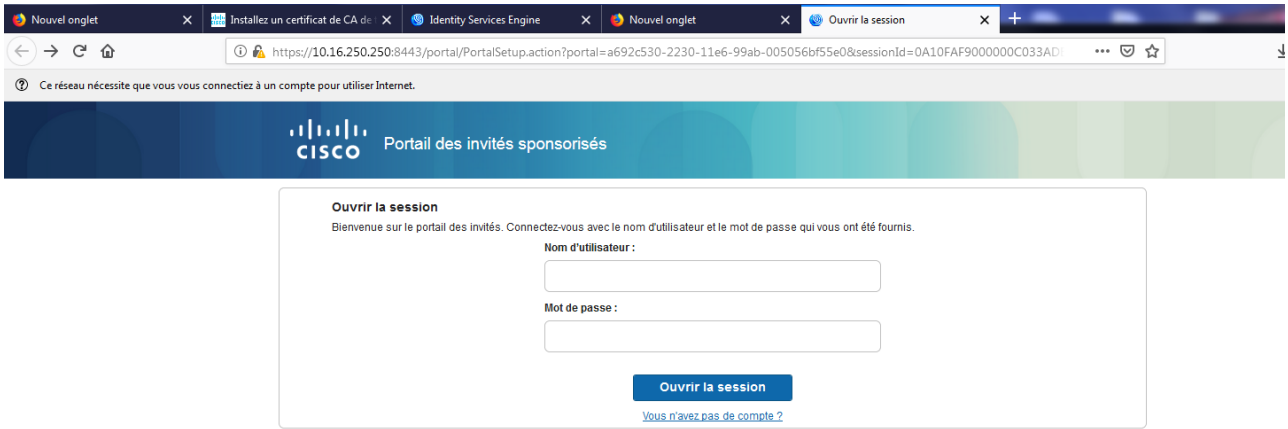

Figure. IV.12 page de Portail invité

Au niveau du commutateur, nous pouvons observer le déroulement de notre authentification en tant qu'invité :

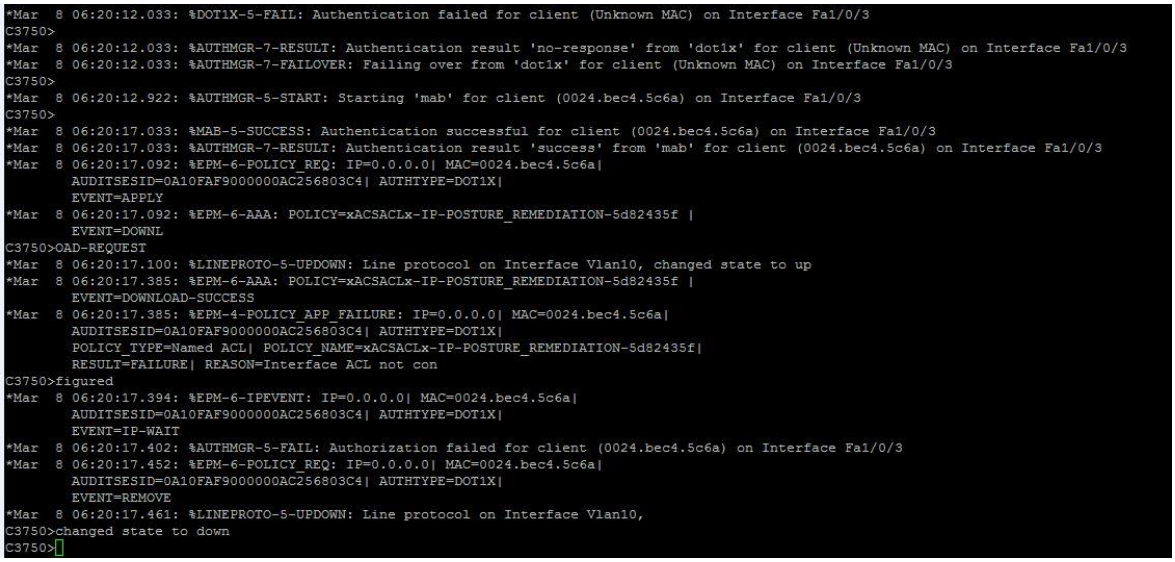

Figure. IV .13. Évènements d'authentification de l'invité observés au commutateur

Lors de la première connexion d’un invité, il va créer un nouveau compte:

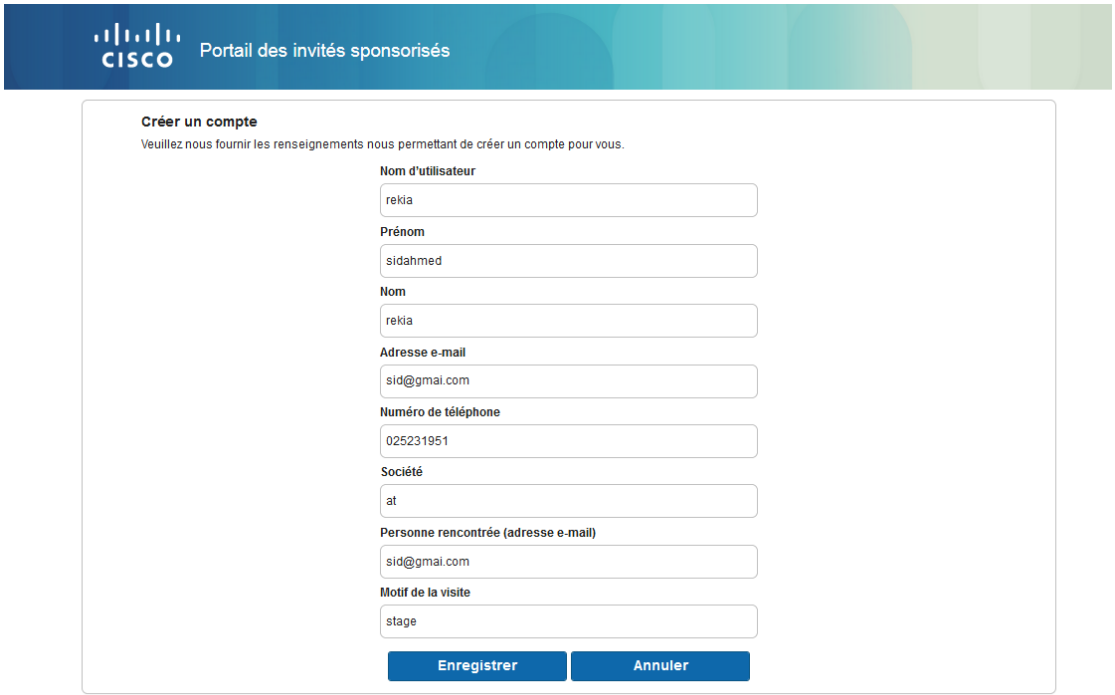

Figure. IV.14 création d'un compte invité

après l'enregistrement d'un nouveau compte , ISE Crée un compte invité avec un mot de passe généré comme indiqué dans la figure suivante :

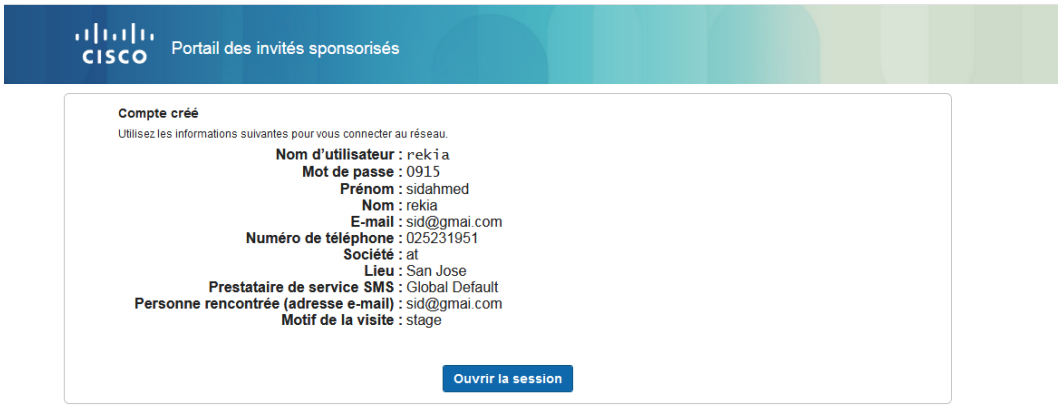

Figure. IV.15 les information de compte

Après la création de compte au niveau du portail invité , nous sommes redirigés vers la page de Client Provisioning pour installé l'agent web :

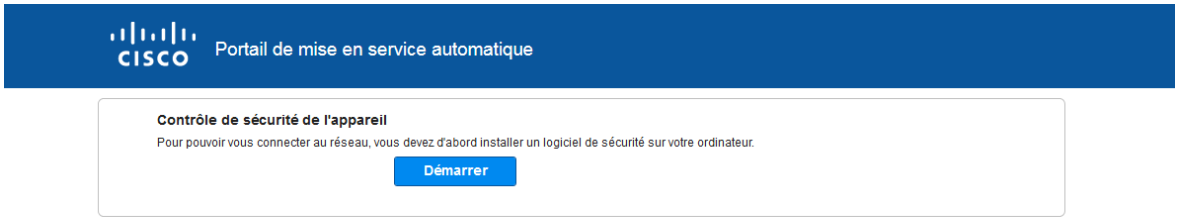

Figure. IV .16 Redirection vers portail de mise en service

Par la suite, l'agent temporaire se lance pour vérifier la posture de la machine :

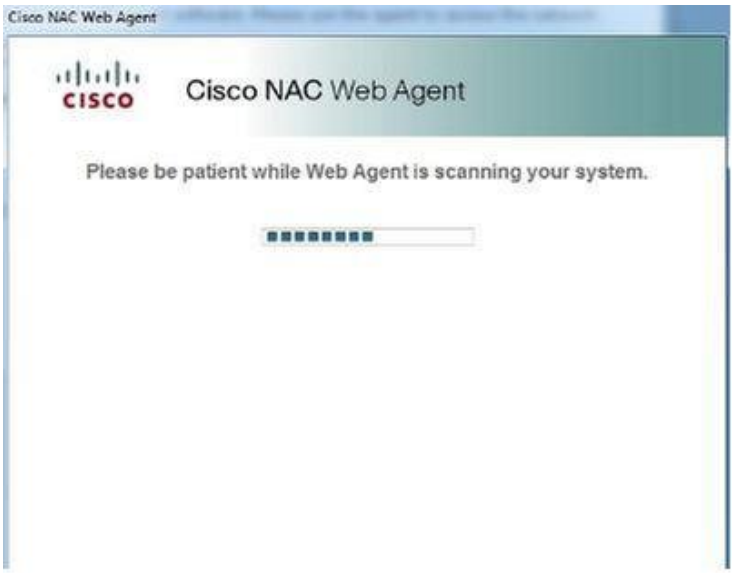

Figure. IV.17 vérification de posture avec un agent temporaire

Une fois le scan terminé, l'agent web de ISE nous a présenté un accès internet seulement car nous avons testé un invité qui a déjà un anti virus:

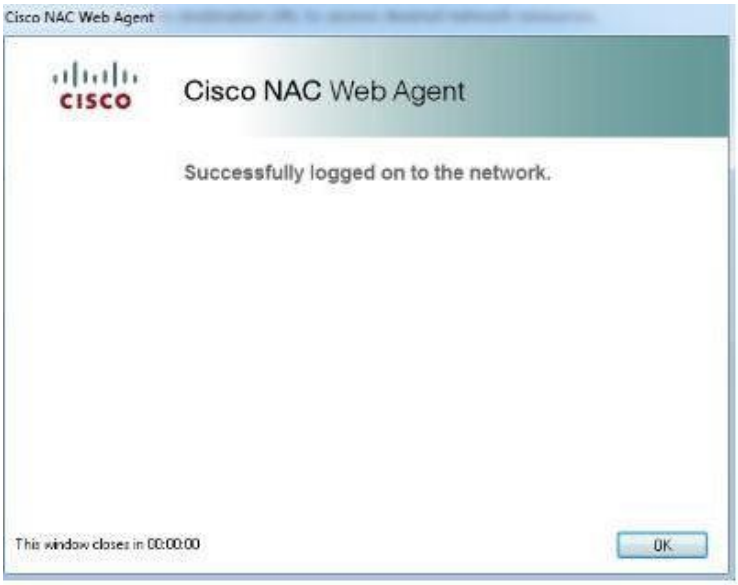

Figure. IV.18 . Accès complet au réseau

au niveau de Log Ise on peut voir les détails des information suivants :

Authentication Details

Source Timestamp	2019-10-21 08:02:07.03
Received Timestamp	2019-10-21 08:02:08.59
Policy Server	cisco-ise
Event	5231 Guest Authentication Passed
Username	sidahmed
User Type	GuestUser
Endpoint Id	00:24:BE:C4:5C:6A
Calling Station Id	00-24-BE-C4-5C-6A
IPv4 Address	192.168.130.108
Authentication Identity Store	Guest Users
Identity Group	GuestType_Guest
Audit Session Id	0A10FAF90000013F5C9165BA
Authentication Method	webauth
Authentication Protocol	PAP_ASCII
NAS IPv4 Address	10.16.250.249

Figure. IV.19 .détails de l'authentification coté ISE

Conclusion :

Cette partie du mémoire était consacrée à l'essai de la solution avec différents scénarios afin de prouver le bon fonctionnement et l’efficacité de notre solution, en essayant de connecter une machine au réseau, en essayant de connecter une machine aux services disponibles au sein des composants plate-forme Cisco ISE.

Conclusion et perspectives :

Dans le cadre de ce projet réalisé au sein de l'entreprise Algérie Telecom , et partant d'un souci de sécurité et d'un besoin de protection des ressources critiques et vitales d'une manière permanente, nous avons mis en place d'une solution de contrôlé d'accès aux réseaux filaire qui assure la conformité des machines avec la stratégie de sécurité .

La solution est encore plus nécessaire quand on sait que, dans certains établissements, le nombre d'utilisateurs qui sollicitent fréquemment le réseau est très important, après une analyse approfondie des besoins de l'entreprise, nous avons pu faire une étude comparative de différentes solutions possibles qui nous a conduits à adopté la solution cisco ise et la valider sur un environnement de test.

Nous avons déployée la solution de Cisco ISE qui permet de réagir, en temps réel, à toute tentative de connexion au réseau par référence aux stratégie de sécurité prédéfinies au niveau de la plateforme Cisco ISE. l'utilisateur est appelé à s'authentifier en présentant son compte utilisateur et le mot de passe associé au cas où il appartient au domaine, sinon et s'il s'agit d'un utilisateur invité, il sera rediriger vers un portail Web pour créé un compte temporairement , etobtient un accès internet , la vérification de la conformité de la machine client est celle de la validation de l'état des machines , l'utilisateur doit installé un agent pour collecte les information de la machine , chacune doit disposer de l'antivirus clamWin. Dans le cas contraire, l'utilisateur bénéficie d'une période de grâce, au cours de laquelle, un fichier de remédiation lui est offert afin de pouvoir accéder.

Malgré toutes les difficultés rencontrées nous avons pu atteindre notre objectif qui est la mise en place de la solution dans le réseau câblé. Comme perspectives on propose :

- d'implémenter la solution dans le réseau sans fils afin de mieux bénéficier de la solution .
- vérifier l'état de la mise a jour de SEet l'existence de certain application de sécurité (par exemple : ccleaner)
- intégration d'un serveur CA (certificat authentification) pour gérer l'installation des certificats Ise dans les machines des employée .

Bibliographies

[1]- W.Stallings , Network Security Essentials, 2nd edition, Prentice Hall, 2003.

[2]- M. choisnard : réseaux et sécurité informatiques, université de bourgogne , 2015 .

[3]- L.Bloch et C.Wolfhugel, Sécurité Informatique : Principes etméthode, Juin 2011.

[4]- CCNA Sécurité .

[5]- M.HOTTE, Q.E.LUTUN , T.ASCOET: Protection contre les attaques de déni de service dans les réseaux IP , université paris descartes , 2011 .

[6]- G.CHARPENTIER, O.MONTIGNY, M.ROUSSEAU, « Virus / antivirus », janvier 2004.

[7]- Guy Pujolle : Les Reseaux - Eyrolles (6ème Ed) 2008 .

[8]- B.Ulmann, « Cisco et la sécurité », Novembre 2004.

[9]- C.DUFRESNES : Parefeu - Proxy - DMZ
http://notionsinformatique.free.fr/reseaux/parefeu.pdf

[10]- J.Zhou, M.Heckman, B.Reynolds, A.Carlson, M.Bishop. Modeling network intrusion detection alerts for correlation. In Proceedings of ACM Transactions on Information and System Security (TISSEC). Volume 10 Issue 1. février 2007

[11]- C.Llorens , L.Levier , D.Valois : Tableaux de bord de la sécurité 2e édition réseau Groupe Eyrolles2006,

[12] - The Open University : Network security , 2014 .

[13]- c.paquet CCNA Security exam 640-553 : Implementing Cisco IOS Network Security (IINS)

[14]- S.BORDÈRES , M.Paru : Authentification réseau avec Radius 802.1x, EAP, FreeRadius , Editeur Eyrolles en novembre 2006

[15]- https://www.intel.fr/content/www/fr/fr/support/articles/000006999/network-and-i-o/wireless-networking.html

[16]- PODMILSAK, Audric :Extended Authentication Protocol. [En ligne] http://igm.univ-mlv.fr/~dr/XPOSE2008/802.1x/EAP.html

[17]- Livre Blanc Network Access Control (Contrôle d'accès au réseau) , Enterasys secure Networks , 2008 .

[18]-
http://www.iso.org/iso/fr/home/faqs/faqs_conformity_assessment_and_certification.html

[19]- https://packetfence.org/about.html#/overview

[20]- https://www.openhub.net/p/8572

[21]-
https://www.cisco.com/c/dam/global/fr_fr/assets/documents/pdfs/datasheet/vpn_security/Cisco_NAC_Fiche_technique.pdf

[22]-
https://www.cisco.com/c/en/us/td/docs/security/nac/appliance/configuration_guide/49/cam/49cam-book/m_intro.html

[23]- V. Hoffman , ImplementingNAP and NACSecurity Technologies , a Indianapolis Indiana, 2008.

[24]- UNIFIED ACCESS CONTROL ,
https://www.juniper.net/us/en/local/pdf/brochures/1500051-en.pdf

[25]- White Paper , Juniper Networks Unified Access Control (UAC) and EX-Series Switches mars 2008

[26]-https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html

[27]-https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116143-config-cise-posture-00.html

[28]-https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_00.html

[29]- https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html#Productoverview

[30]-Configuring IEEE 802.1X Port-Based Authentication ,
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.pdf

[31]- https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

[32]- https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html

[33]- Cisco Identity Services EngineOrdering GuideAugust 2019 ,
https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/guide_c07-656177.pdf

[34]- https://community.cisco.com/t5/security-documents/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515

[35]- https://fr.wikipedia.org/wiki/Politique_de_s%C3%A9curit%C3%A9_informatique

[36]- *https://www.algerietelecom.dz*