REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

CHERIFI Youcef Idriss

Filière : Télécommunications

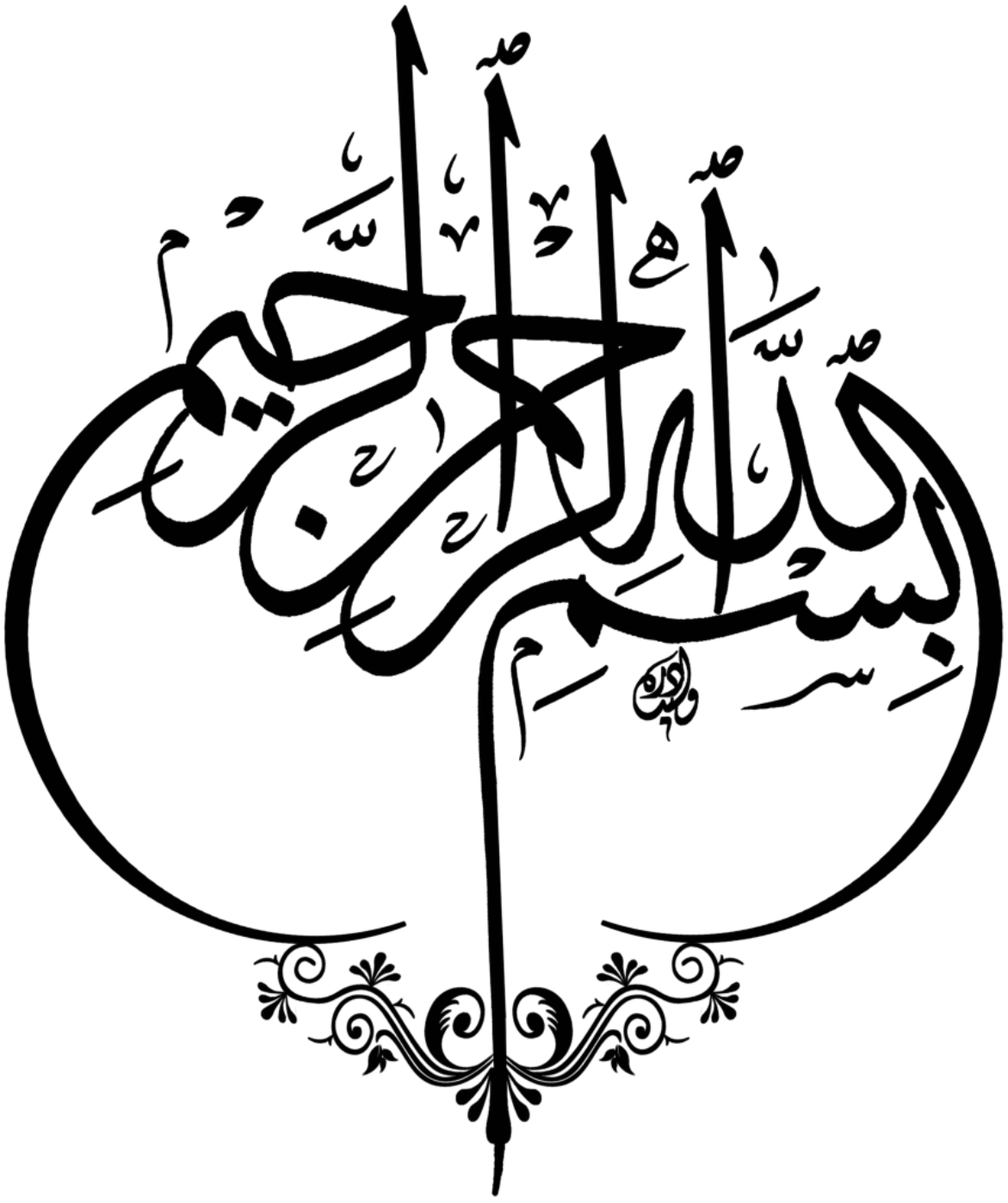
Spécialité **:** Réseaux et Télécommunications

Etude et mise en place d'une solution NAC basée sur Cisco ISE pour l'organisation OURHOUD-SONATRACH

Devant le jury :

Messaoudi	Noreddine	Prof	Université	Président
Meraihi	Yacine	Prof	Université	Examinateur
Mahdi	Ismahane	MCB	Université	Rapporteur

Année Universitaire : 2024/2025


بسم الله الرحمن الرحيم

Résumé :

Les entreprises sont quotidiennement confrontées à des menaces pouvant compromettre la disponibilité et la sécurité de leurs systèmes informatiques. Pour y faire face, il est indispensable de mettre en place une stratégie de protection efficace. Parmi les différents volets de la cybersécurité, nous nous sommes intéressés plus particulièrement au contrôle d'accès réseau et à la vérification de la conformité des terminaux souhaitant se connecter à l'infrastructure, en s'appuyant sur le principe de posture.

Dans ce travail, nous proposons l'utilisation de Cisco Identity Services Engine (ISE), une solution qui offre une approche centralisée et intelligente de la gestion des accès. Elle permet non seulement de sécuriser les connexions, mais aussi de garantir le respect des politiques de conformité et d'usage. Cette approche facilite l'intégration des appareils personnels (BYOD), évalue en continu l'état de sécurité des terminaux, attribue des droits d'accès adaptés aux profils des utilisateurs et applique de manière cohérente les stratégies définies.

Mots-clés : Sécurité des réseaux, Contrôle d'accès réseau (NAC), Cisco ISE, Posture de sécurité, BYOD

Abstract **:**

Companies are increasingly exposed to threats that may compromise the security and availability of their information systems. To address this issue, it is essential to implement effective protection strategies. Among the many aspects of cybersecurity, this work focuses on network access control and the compliance verification of endpoints attempting to connect to the infrastructure, based on posture assessment.

In this project, we propose the use of Cisco Identity Services Engine (ISE), a solution that provides a centralized and intelligent approach to access management. It not only secures connections but also ensures compliance with defined security policies. The solution enables the integration of personal devices (BYOD), continuously assesses endpoint security, assigns access rights according to user profiles, and enforces posture policies, thereby enhancing both security and network efficiency.

Keywords: Network Security, Network Access Control (NAC), Cisco ISE, Security Posture, BYOD

ملخص:

تواجه الشركات يومياً تهديدات قد تعرض توفر وأمن أنظمتها المعلوماتية للخطر. وللتصدي لهذه التهديدات، من الضروري وضع استراتيجية حماية فعالة. من بين مختلف جوانب الأمن السيبراني، اهتممنا بشكل خاص بالتحكم في الوصول إلى الشبكة والتحقق من مطابقة الأجهزة الطرفية التي ترغب في الاتصال بالبنية التحتية، بالاعتماد

.على مبدأ الموقف

، وهو حل يوفر نه ًجا (ISE) CISCO IDENTITY SERVICES ENGINE في هذا العمل، نقترح استخدام مركزيًا وذكيًا لإدارة الوصول. وهو لا يتيح فقط تأمين الاتصالات، بل يضمن أي ًضا الامتثال لسياسات الامتثال ، ويقيّم باستمرار حالة أمان الأجهزة الطرفية، (BYOD) والاستخدام. يسهل هذا النهج دمج الأجهزة الشخصية

ويمنح حقوق وصول ملائمة لملفات تعريف المستخدمين، ويطبق السياسات المحددة بشكل متسق

الكلمات المفتاحية: أمن الشبكات، التحكم في الوصول إلى الشبكة، الوضع الأمني، احضر جهازك الخاص

Remerciements

Avant tout, je rends grâce à Dieu pour la force et la persévérance dont Il m'a doté tout au long de ces années d'études. Ce parcours, parfois semé d'embûches, trouve aujourd'hui son aboutissement grâce à Sa bienveillance.

J'exprime toute ma reconnaissance à mes parents, dont le soutien moral, les sacrifices et les encouragements constants ont été le pilier de ma réussite. C'est en grande partie grâce à eux que j'ai pu atteindre ce stade de mon parcours académique.

Je souhaite également adresser mes vifs remerciements à ma promotrice Madame MAHDI Ismahane pour ses orientations précieuses et ses conseils avisés, ainsi qu'à mon encadreur BOUDJEMLINE Fateh pour sa disponibilité, son accompagnement rigoureux et sa patience tout au long de ce travail.

Ma gratitude s'étend aussi aux membres du jury, qui ont bien voulu consacrer de leur temps pour évaluer ce mémoire et contribuer, par leurs remarques, à son enrichissement.

Enfin, je remercie chaleureusement mes amis, qui m'ont soutenu dans les moments difficiles, encouragé dans les périodes de doute et partagé les joies de ce cheminement. Leur présence a rendu cette expérience à la fois humaine, enrichissante et inoubliable.

Sommaire

Introduction générale 1
Introduction 2
Chapitre I 4
Présentation de l'Organisme d'Accueil et du Thème 4
I. Présentation d'Organisme d'Accueil 5
I.1 La création de l'Organisation OURHOUD 5
I.2. Etapes majeurs de développement du champ OURHOUD 6
1.3 Situation géologique 7
1.4. Description du champ OURHOUD 8
1.5. Organigramme d'OURHOUD 9
I.5. Problématique 10
I.6 Objectif 10
Chapitre II 11
Généralités sur la sécurité des réseaux informatiques 11
II.1 Introduction 12
II.2 Sécurité des systèmes informatiques 12
II.3 Objectifs de la sécurité 13
II.3.1 L'intégrité 13
II.3.2 La confidentialité 14
II.3.3 La disponibilité 14
II.3.4 La non répudiation 14
II.3.5 L'authentification 14
II.4 Politique de sécurité 14
II.4 Les Menaces 15
II.4.1 Programme malveillants 15
II.4.2 Fraude et vol 16
II.4.3 Sabotages causés par les employés 16
II.4.4 Erreurs et omissions 16
II.4.5 Les Hackers 16
II.5 Les attaques 16
II.5.1 Buts des attaques 17
II.5.2 Classifications des attaques réseaux 17

II.5.3 Etapes d'une attaque 18
II.5.4 Les différents types d'attaque réseau 19
II.5.4.1 Les attaques de reconnaissance 19
II.5.4.2 Les attaques du mot de passe 20
II.5.4.3 Les attaques d'accès 20
II.5.4.4 Les attaques du réseau contre la disponibilité 21
II.5.4.5 Les attaques rapprochées 21
II.5.4.6 Les attaques de la relation d'approbation 21
II.6 Mécanismes de défense 22
II.6.1 Audit de sécurité 22
II.6.2 Journalisation 22
II.6.3 Antivirus 22
II.6.4 Systèmes de détection d'intrusion 23
II.6.5 Pare-feu 23
II.6.6 Contrôle d'accès 23
II.6.7 Authentification réseau 24
II.6.8 Bourrage de trafic 24
II.6.8 Chiffrement des données 24
II.6.9 Signature numérique 25
II.6.10 Protection physique 25
II.6.11 Bonnes pratiques 25
Conclusion 27
CHAPITRE III 28
Mécanismes et Solutions de Sécurité Réseau 28
III.1 Introduction 29
III.2 NAC (Network Access Control) 29
III.2.1 Types de contrôle d'accès au réseau 30
III.2.2 Concepts du contrôle d'accès au réseau. 31
III.3 Protocoles de contrôle d'accès au réseau 32
III.3.1 Le protocole 802.1x 32
III.3.2 RADIUS 34
III.3.2.1 La méthode d'authentification Radius [23] 34
III.3.3 Les méthodes d'authentification 35
III.3.3.1 Les types de paquets existants 35
III.4 Architecture générale du NAC 36

III.4.1 Composants de NAC 37
III.4.1.1 Agent 37
III.4.1.2 Network Access Device (NAD) 37
III.4.1.3 Serveur de stratégie 37
III.4.1.4 Serveur de politique antivirus 38
III.5 Présentation des solutions de contrôle d'accès réseau (NAC) 38
III.5.1 Les solutions libres 38
III.5.1.1 OpenNAC 38
III.5.1.2 PacketFence 38
III.5.1.3 FreeNAC 39
III.5.2 Les solutions commerciales 39
III.5.2.1 FortiNAC 39
III.5.2.2 Juniper Unified Access Control (UAC) 39
III.5.3 Analyse comparative des solutions NAC 40
III.5.4 La solution de contrôle d'accès choisie 41
III.6 Définition de CISCO ISE (Identity service engine) 42
III.6.1 Les avantages de l'ISE 43
III.6.2 Les fonctions et caractéristiques de Cisco ISE 44
III.6.3 Les différents types de personas sur Cisco ISE : [40] 45
III.6.4 Composants de déploiement ISE 46
III.6.5 Méthodologies d'authentification 47
III.6.5.1 IEEE 802.1X 47
III.6.5.2 MAC Authentication Bypass (MAB) 48
III.6.5.3 EasyConnect 48
III.6.5.4 Une comparaison des différentes méthodes d'authentification 49
III.6.6 Méthodologies d'autorisation 49
III.6.6.1 Affectation dynamique de VLAN 50
III.6.6.2 Listes de contrôle d'accès (ACLs) 50
III.6.6.3 Security Group Tags (SGTs) 51
III.6.6.4 Redirection d'URL 51
III.6.7 La conformité du périphérique avec la stratégie de sécurité 51
III.6.8 Les cas d'utilisation de Cisco Identity Services Engine 52
Conclusion 57
Chapitre IV 58
Mise en place de la solution de sécurité CISCO ISE 58

IV.1 Introduction 59
IV.2 Environnement de travail et topologie du laboratoire NAC basé sur Cisco ISE 59
IV.2.1. Environnement de travail 59
IV.2.1.1 Prérequis matériels 59
IV.2.1.2 Prérequis logiciels 59
IV.2.2 Topologie du laboratoire 60
IV.3 L'implémentation de la solution ; 61
IV.3.1 Configuration au niveau de switch 61
IV.3.1.1 Activer les fonctions AAA et 802.1X 61
IV.3.2 Configuration au serveur ISE 64
IV.3.2.1 Accéder à l'interface d'administration du serveur ISE 65
IV.3.2.1.1 La création d'un Device Type 66
IV.3.2.2 Ajout du Switch dans Cisco ISE comme Network Device 67
IV.3.2.3. Création d'un groupe d'utilisateurs dans Cisco ISE 68
IV.3.2.4 Création d'un utilisateur et association à un groupe 68
IV.3.2.5 La définition des politiques d'autorisation et définir un Policy Set pour l'authentification 802.1X filaire 70
IV.3.2.5.1 La définition des politiques d'autorisation 70
IV.3.2.5.1.1 Création d'une ACL téléchargeable (Downloadable ACL - DACL) 70
IV.3.2.5.1.2 Création d'un Profil d'Autorisation 71
IV.3.2.5.2 Création d'un Policy Set pour l'authentification 802.1X filaire 73
IV.3.2.6. Configuration des Authentication et Authorization Policy 74
IV.3.2.6.1 Authentication Policy 74
IV.3.2.6.2 Authorization Policy 75
IV.3.2.7. Sauvegarder la configuration du serveur ISE 77
IV.4 Procéder aux tests 78
IV.4.1 Vérification des résultats d'authentification et d'autorisation sur le switch 78
IV.4.2 Vérification de l'assignation du VLAN 79
IV.4.3 Vérification de l'application de I'ACL téléchargeable 80
IV.4.4 Vérification de la session d'authentification sur le port Fa0/2 81
IV.4.5.1 Vérification des authentifications dans l'interface ISE 82
IV.4.5.2 Détails de l'authentification dans I'ISE 82
Conclusion 85
Conclusion et perspectives 86
Conclusion et perspective 87

Bibliographies 88

Liste des figures

Figure (I-1) : diagramme circulaire montrant la part relative de chacune des compagnies ... 5
Figure (*I-2)* : situation géographique 7
Figure (*I-3)* : Situation Géologique 8
Figure (*I-4) :* Le Champ OURHOUD 9
Figure (*I-5)* : Organigramme d'OURHOUD 9
Figure (II-1) : Principaux objectifs de sécurité 14
Figure (II-2) : Buts des attaques [4] 17
Figure (II-3) : Classification des attaques réseaux [6] 18
Figure (III-1) : Solution NAC en ligne 31
Figure (III -2) : Solution NAC hors bande 31
Figure (III -3) : les composants du mécanisme de 802. 1x [21] 33
Figure (III -4) : L'architecture protocolaire du mécanisme 802. 1x [21] 33
Figure (III -5) : Le processus de l'authentification Radius [22] 34
Figure (III -6) : les caractéristiques des différents méthodes d'authentification [20] 35
Figure (III -7) : Etapes d'authentification 802.1X [20] 36
Figure (III -8) : Architecture générale de NAC 37
Figure (III -9) : Architecture fonctionnelle de Cisco Identity Services Engine (ISE) montrant ses principales composantes [35] 42
Figure (III -10) : Les différents types de personas sur Cisco ISE [40] 45
Figure (III -11) : Composants de la solution ISE [41] 46
Figure (III -12) : 802.1x Authentification [41] 47
Figure (III -13) : Authentification 802.1x port de commutateur [41] 47
Figure (III -14) : MAB Authentification [41] 48
Figure (III -15) : EasyConnect Authentification [41] 48
Figure (III -16) : Analyse de complexité des méthodes d'authentification [41] 49
Figure (III -17) : Affectation dynamique de VLAN [41] 50
Figure (III -18) : Listes de contrôle d'accès [41 50
Figure (III -19) : Redirection d'URL [41] 51
Figure (III -20) : Cas d'utilisation de Cisco ISE Guest [44] 52
Figure (III -21) : Cas d'utilisation du sans-fil sécurisé Cisco ISE [44] 53
Figure (III -22) : Cas d'utilisation de l'accès filaire sécurisé Cisco ISE 54

Figure (III -23) : Cas d'utilisation du BYOD avec Cisco ISE [44] 55
Figure (III -24) : Visibilité de la conformité Cisco ISE Cas d'utilisation. [44] 56
Figure (IV -1) : Topologie du lab 60
Figure (IV -2) : Activer AAA dans le switch 61
Figure (IV -3) : Configure l'authentification 802.1X 62
Figure (IV -4) : Active l'autorisation via le serveur RADIUS 62
Figure (IV -5) : Active l'accounting 62
Figure (IV -6) : Attribuer un nom au servuer et une adresse IP et une clé 62
Figure (IV -7) : Active globalement le protocole 802.1X sur le switch. 63
Figure (IV -8) : Assigne les utilisateurs authentifiés au VLAN 10 63
Figure (IV -9) : Activer le suivi des périphériques connectés 63
Figure (IV -10) : Activer le device tracking 64
Figure (IV -11) : Interface de l'ISE 65
Figure (IV -11) : La création d'un device type 66
Figure (IV -12) : Ajout du Switch dans Cisco ISE comme Network Device 67
Figure (IV -13) : Création d'un groupe d'utilisateurs 69
Figure (IV -14) : Création d'un utilisateur et association à un groupe 69
Figure (IV -15) : Création d'une ACL téléchargeable (Downloadable ACL - DACL) 71
Figure (IV -15) : Création d'un Profil d'Autorisation 72
Figure (IV -16) : Création d'un Policy Set pour l'authentification 802.1X filaire 73
Figure (IV -17) : Configuration des policy d'authentification 75
Figure (IV -18) : Configuration des policy d'authorization 76
Figure (IV -19) : Sauvegarder la configuration du serveur ISE 77
Figure (IV -20) : L'apparition de l'interface qui nous montre la réussite de l'authentification et de l'autorisation grâce à la commande debug dot1x all 78
Figure (IV -21) : Vérification de l'assignation du VLAN 79
Figure (IV -22) : Vérification de l'application de I'ACL téléchargeable 80
Figure (IV -23) : Vérification de la session d'authentification sur le port Fa0/2 81
Figure (IV -23) : Vérification des authentifications dans l'interface ISE. 82
Figure (IV -24) : Détails de l'authentification dans I'ISE 84

Liste des tableaux

Tableau 1Tableau comparatif des fonctionnalités NAC..... 40

Liste des abréviations

Abréviation	Signification
AAA	Authentication, Authorization and Accounting
AD	Active Directory
API	Application Programming Interface
AVP	Attribute Value Pair
BYOD	Bring Your Own Device
CPU	Central Processing Unit
CWA	Central Web Authentication
DACL	Downloadable Access Control List
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IoMT	Internet of Medical Things
IoT	Internet of Things
IPS	Intrusion Prevention System
IP	Internet Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
MDM/EMM	Mobile Device Management / Enterprise Mobility Management
MnT	Monitoring Node
MSCHAPv2 version 2	Microsoft Challenge Handshake Authentication Protocol
NAD	Network Access Device
NAS	Network Access Server
NVRAM	Non-Volatile Random Access Memory
OT/ICS	Operational Technology / Industrial Control Systems
PAN	Policy Administration Node
PEAP	Protected Extensible Authentication Protocol
PSN	Policy Service Node
QoS	Quality of Service

RAM	Random Access Memory
RADIUS	Remote Authentication Dial-In User Service
SGACL	Security Group Access Control List
SGT	Security Group Tag
SGTs	Security Group Tags
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
UAC	User Access Control
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VMPS	VLAN Membership Policy Server
VSA	Vendor Specific Attribute
WAN	Wide Area Network

Introduction générale

Introduction

La sécurité des systèmes et des réseaux informatiques constitue aujourd'hui un enjeu stratégique majeur pour les entreprises et les organisations. Avec la transformation numérique et l'évolution rapide des technologies de l'information et de la communication, les infrastructures informatiques sont devenues à la fois le support et le moteur des activités quotidiennes. Cette dépendance accrue aux systèmes d'information s'accompagne cependant d'une multiplication des menaces, qu'elles soient externes ou internes, mettant en péril la confidentialité, l'intégrité et la disponibilité des données et des services.

Traditionnellement, la sécurité des réseaux reposait essentiellement sur une architecture périmétrique, intégrant des mécanismes tels que les firewalls et les zones démilitarisées (DMZ), destinés à contrer les attaques venues de l'extérieur. Si ces mesures restent indispensables, elles se révèlent toutefois insuffisantes face à la montée des menaces internes, aux risques liés aux utilisateurs malveillants ou négligents, ainsi qu'à la complexité croissante des environnements numériques. En effet, un poste non sécurisé ou un périphérique non autorisé, une fois connecté au réseau interne, peut rapidement devenir une porte d'entrée pour des attaques sophistiquées.

Dans ce contexte, les organisations, à l'image de l'entreprise OURHOUD – Sonatrach, doivent répondre à plusieurs défis : contrôler l'accès aux ressources réseau, garantir la conformité des terminaux, assurer la traçabilité des connexions, et gérer la diversité des profils et périphériques (ordinateurs, smartphones, tablettes, objets connectés). Face à ces exigences, les solutions de sécurité traditionnelles atteignent leurs limites et la mise en place d'une technologie de contrôle d'accès réseau (Network Access Control – NAC) s'impose comme une nécessité.

Le Cisco Identity Services Engine (ISE) représente une réponse adaptée à ces besoins. En intégrant des mécanismes avancés d'authentification, d'autorisation, d'audit (AAA), ainsi que des fonctionnalités de posture et de gestion des terminaux, il permet aux entreprises de renforcer leur sécurité interne, de s'adapter dynamiquement aux profils utilisateurs, et de faire face efficacement aux nouvelles menaces.

Le mémoire est organisé en quatre chapitres :

- **Chapitre I : Présentation de l'organisme d'accueil et du thème**
  Ce premier chapitre présente le cadre de réalisation de ce projet, à savoir l'entreprise OURHOUD – Sonatrach, ainsi que le thème du mémoire et son importance dans le contexte professionnel étudié.

- **Chapitre II : Généralités sur la sécurité des réseaux informatiques**
  Dans ce chapitre, nous abordons les fondements de la sécurité des systèmes et des réseaux, en définissant les principaux objectifs de sécurité (confidentialité,

intégrité, disponibilité, authentification et non-répudiation) ainsi que les menaces et vulnérabilités courantes.

- **Chapitre III : Mécanismes et solutions de sécurité réseau**
  Ce chapitre est consacré à l'étude des mécanismes et solutions de sécurité, avec un accent particulier sur le NAC. Nous présentons ses fonctionnalités, ses modes de déploiement, ses protocoles associés, ainsi qu'une analyse comparative des solutions existantes, avant de justifier le choix de Cisco ISE comme solution retenue.

- **Chapitre IV : Mise en place de la solution de sécurité Cisco ISE**
  Ce dernier chapitre est dédié à la partie pratique, à travers l'implémentation d'une solution NAC basée sur Cisco ISE. Nous décrivons la configuration du serveur ISE et des équipements réseau afin d'illustrer l'efficacité de la solution pour le renforcement de la sécurité interne.

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

Chapitre I :

Présentation de l’Organisme d’Accueil et du Thème

I. Présentation d'Organisme d'Accueil

I.1 La création de l'Organisation OURHOUD

L'Organisation OURHOUD (crée en 1997, début de production ,2003) est l'opérateur délégué chargé du développement et de l'exploitation du champ OURHOUD .Les partenaires ont conçu l'Organisation OURHOUD comme un instrument doté de pouvoirs et procédures fiable approuvées par toutes les parties et I 'ont dotée de moyens matériels et ont affecté du personnel de haut niveau pour assurer son efficacité .L'organisation OURHOUD a su tirer profit de toute expérience acquise par Sonatrach et les partenaires (Anadarco, Cepsa, Agip, Maersk, Burlingtor, Ressource, Talisman) au bénéfice du projet et de la diversité culturelle.

Sonatrach est associée à six compagnies étrangères dans la mesure où le gisement chevauche trois blocs Sur le bloc 404, Sonatrach est associé à l'américaine Anadarko (qui a comme associés Agip et Maersk). Sur le bloc 406, la compagnie nationale est associée à l'espagnole CEPSA.Tandis que sur le bloc 405, elle est associée à Burlington Ressource (qui a comme associé Talisman).

Le gisement a fait l'objet d'une Unification qui permet de calculer la part de Pétrole qui revient à chaque compagnie. Actuellement, Cepsa a la plus grande part, Agip a remplacé Lasmo.

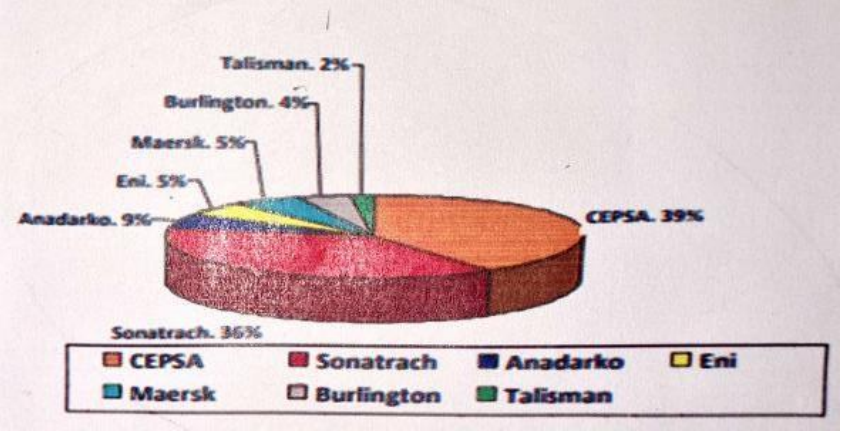


Figure (I-1) : diagramme circulaire montrant la part relative de chacune des compagnies

I.2. Etapes majeurs de développement du champ OURHOUD

- **09 Janvier 97 :** Signature de l'Accord Cadre d'Unitisation.Sonatrach désignée comme Opérateur.
- **01 Juillet 97 :** Création de I 'Organisation OURHOUD (Opérateur délégué par Sonatrach)
- **01 Août 98 :** Présentation du Dossier ELA (Exploitation Licence Association) au Ministère.
- **27 Octobre 98 :** Signature par les parties de la Procédure d'Opérations Unifiées (P.O.U)
- **21 Avril 99 :** Attribution du permis d'exploitation par le Ministère.
- **25 Mars 2000 :** Début des travaux de préparation du site des installations de production (plateformes, routes, puits d'eau, piste d'atterrissage) pour Le Projet EPC.
- **10 Août 2000 :** Signature du Contrat EPC avec JGC/INITEC Dates clés contractuelles : First-Oïl **: 04 Janvier 2003**
- Réception Provisoire **: 10 Mai 2003.**
- **14 Août 2000 :** signature de 2 Contrats avec GEPCO pour la réalisation de deux bases
- **2003 :** Début de production

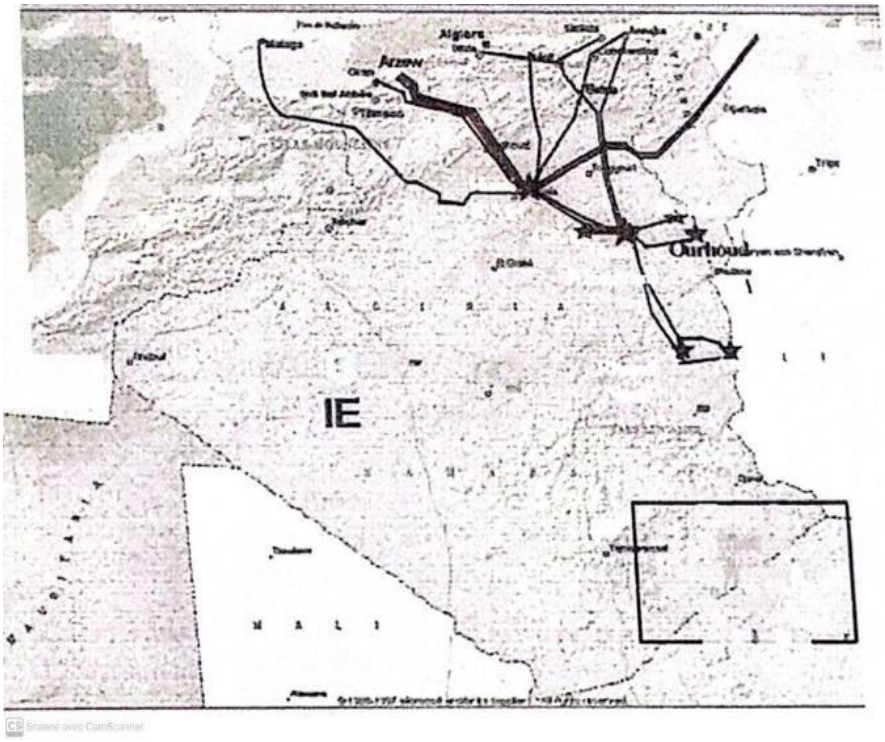


Figure (*I-2)* : situation géographique

1.3 Situation géologique :

Le gisement d'OURHOUD est situé dans le bassin de Ghadamès où se trouvent d'épaisses séries Paléozoïques et Mésozoïques. Ces deux séries sont séparées par la discordance Hercynienne.

Le gisement d'OURHOUD est localisé dans les blocs 404/406A/405 du bassin de Ghadamès et contient une huile légère sous saturée dans les grès du TAGI, piégée dans une structure anticlinale faillée. Le réservoir possède des caractéristiques pétro- physiques de grande qualité.

L'intervalle de production du réservoir TAGI est situé immédiatement au-dessus de la discordance Hercynienne, qui est généralement rencontré à une profondeur de 3100mètres dans la région de Qoubba, Le point le plus élevé de la structure se situe à -2772 m/NM, et le contact huile/eau est interprété à -3056 m/NM. La hauteur utile moyenne est d'environ 31,5m. Les valeurs moyennes de porosité et de perméabilité sont respectivement de 15% et 200 md, L'huile est fortement sous-saturée aux conditions initiales du réservoir, et à une densité de 0,8115 au stockage.

La pression initiale du réservoir est de 348,1 lbar à la profondeur de référence de -2978 m/NM
La température de gisement est de 102°C. [7)

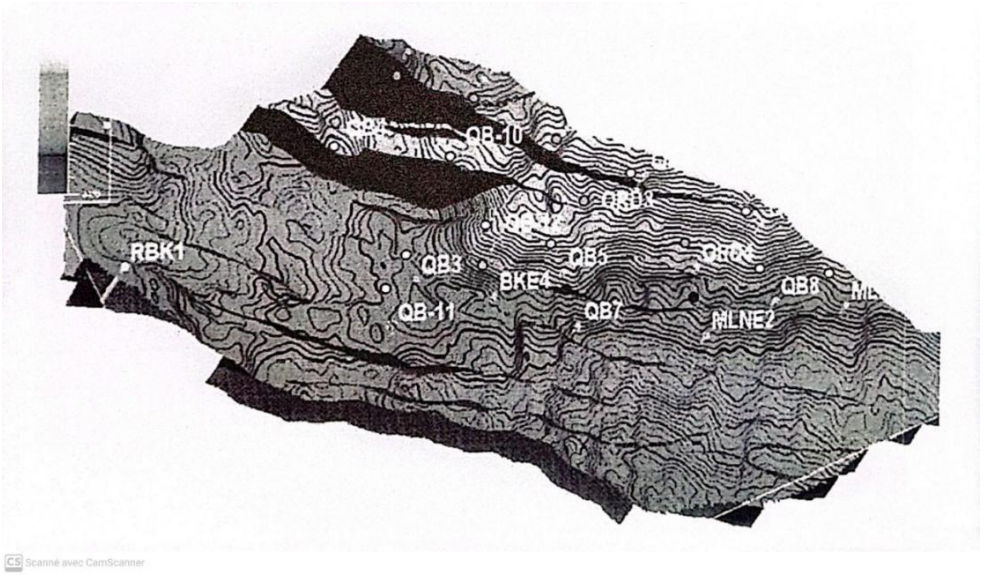


Figure (*I-3)* : Situation Géologique

1.4. Description du champ OURHOUD

Les installations regroupant la station de production (centrale production facilites /CPF) sont situées près du centre du champ.

Il y a sept stations satellites, quatre au sud du CPF et trois au nord, chacune d'elles collectant les fluides d'un groupe de cinq à neuf puits.
Le champ englobe :

- 57-Puits de production d'huile
- 05-puits injecteurs de gaz
- 36-puits injecteurs d'eau
- 10-Puits Producteurs d'eau de l'Albien
- 09-Puits producteurs d'eau du Mio-Pliocene
- 07-Stations satellites
- 01-Centre de traitement de brut (CPF ou Central ProcessingFacilities)
- 01-Réseau de collecte et dessertes

Figure (*I-4) :* Le Champ OURHOUD

1.5. Organigramme d'OURHOUD

L'organigramme d'OURGOUD illustré en figure

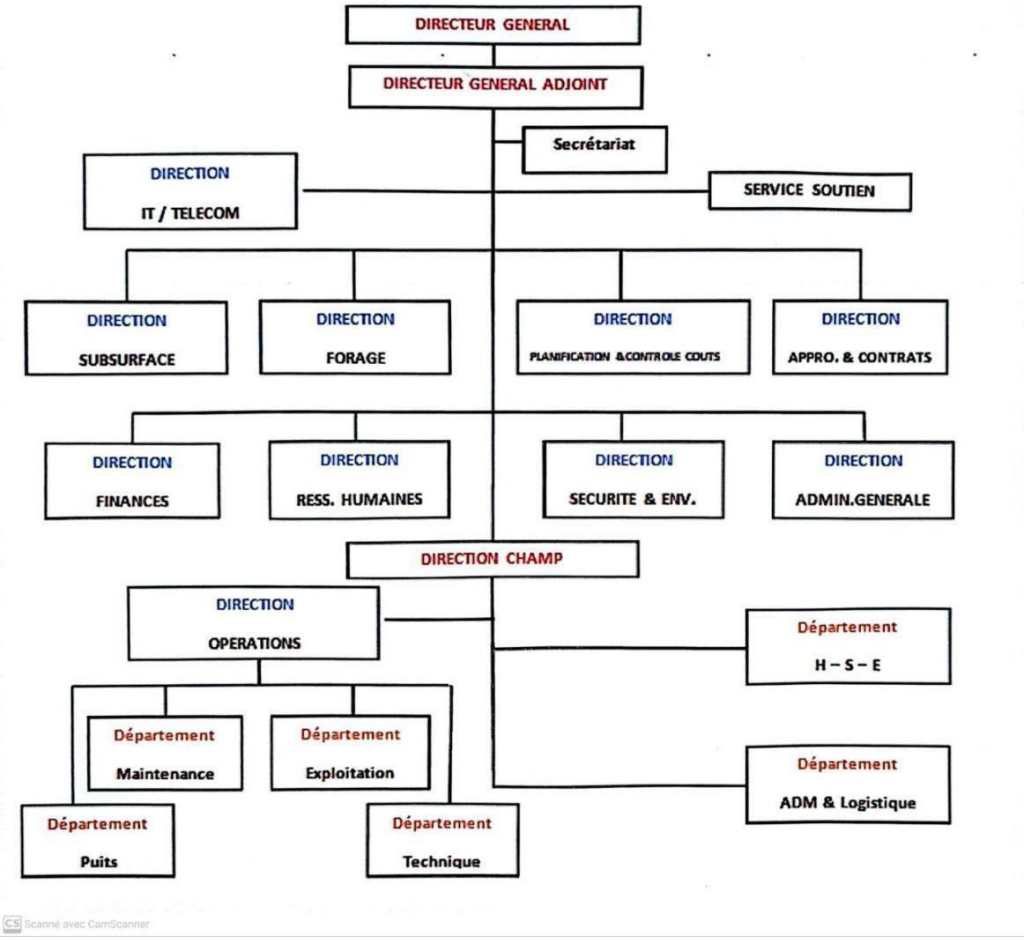


Figure (*I-5)* : Organigramme d'OURHOUD

I.5. Problématique

Dans un environnement critique comme celui d'OURHOUD – Sonatrach, la sécurité du réseau repose aujourd'hui sur une architecture comprenant des firewalls périmétriques et internes ainsi qu'une zone DMZ pour protéger les ressources exposées. Ces mécanismes constituent une base solide pour contrer les menaces externes, mais ils montrent leurs limites lorsqu'il s'agit de gérer les menaces internes. En effet, un utilisateur malveillant ou non autorisé, en connectant simplement un poste au réseau local, peut intercepter le trafic ou exploiter des failles de configuration.

À cette vulnérabilité s'ajoute le manque de contrôle sur la posture des terminaux : en l'absence de vérification systématique (mises à jour de sécurité, antivirus actif, conformité logicielle), un simple poste non sécurisé peut devenir une porte d'entrée pour des attaques ciblant l'ensemble du réseau.
Par ailleurs, les entreprises doivent désormais faire face à l'augmentation exponentielle des périphériques accédant au réseau (ordinateurs portables, smartphones, tablettes, objets connectés), combinée à la diversité des profils utilisateurs (employés, directeurs, prestataires, stagiaires) et aux multiples modes d'accès (filaire, sans fil, VPN). Cette complexité rend encore plus difficile la sécurisation globale de l'infrastructure.
Dans ce contexte, la simple sécurité périmétrique ne suffit plus. Il devient essentiel de mettre en place une solution de contrôle d'accès réseau (NAC) capable d'authentifier les utilisateurs, de vérifier la posture des terminaux et d'adapter dynamiquement les autorisations en fonction du profil et du type de périphérique. Cisco Identity Services Engine (ISE) se présente comme une réponse adaptée pour relever ces défis.
Ainsi, la problématique centrale de ce mémoire est :
Comment, au sein de l'organisation OURHOUD – Sonatrach, déployer une solution de contrôle d'accès réseau basée sur Cisco ISE afin de contrer les menaces internes, d'assurer l'évaluation de la posture des terminaux, et de répondre à l'augmentation et à la diversité des périphériques connectés aux réseaux modernes ?

I.6 Objectif

L'objectif principal de notre projet est de concevoir et de metre en place, au sein de l'organisation OURHOUD - Sonatrach, une solution de contrôle d'accès réseau (NAC) basée sur Cisco ISE, qui :

- Applique la norme IEEE 802.1X pour l'authentification et l'autorisation des utilisateurs et périphériques.
- Intègre des mécanismes de comptabilisation (accounting) afin de tracer et suivre les connexions réseau.
- Renforce la sécurité interne face aux menaces provenant de l'intérieur.

- Assure l'évaluation de la posture des terminaux (mises à jour, antivirus, conformité).

- Gère efficacement la croissance et la diversité des périphériques et profils utilisateurs (employés, invités, stagiaires, direction.

Chapitre II :

Généralités sur la sécurité des réseaux informatiques

II.1 Introduction

Dans l'ère numérique actuelle, les systèmes informatiques et les réseaux constituent l'épine dorsale des activités des entreprises. Ils assurent la circulation, le stockage et le traitement d'informations stratégiques qui représentent une véritable valeur pour l'organisation. Cependant, cette dépendance croissante aux technologies de l'information s'accompagne d'une exposition accrue aux menaces et aux vulnérabilités. La sécurité des systèmes informatiques devient ainsi un enjeu fondamental, non seulement pour garantir la continuité des services, mais également pour protéger les actifs informationnels de l'entreprise.

Les objectifs de la sécurité informatique reposent sur cinq principes essentiels : la confidentialité, qui vise à limiter l'accès aux seules personnes autorisées ; l'intégrité, qui garantit que les données ne sont ni altérées ni corrompues ; la disponibilité, qui assure l'accessibilité permanente des services ; l'authentification, qui valide l'identité des utilisateurs ; et enfin la non-répudiation, qui empêche tout déni d'action effectuée. Pour atteindre ces objectifs, une politique de sécurité doit être mise en place, comprenant l'identification des besoins, l'élaboration de procédures adaptées, la surveillance et la détection des vulnérabilités, ainsi que la définition d'actions correctives et préventives.

Toutefois, les menaces pesant sur les systèmes informatiques sont multiples : programmes malveillants, les hackers, erreurs et omissions, fraudes, vols d'information ou encore sabotages pouvant provenir aussi bien de l'extérieur que de l'intérieur de l'entreprise. Ces menaces se matérialisent par des attaques, dont les buts peuvent être variés : interrompre un service, intercepter des communications, modifier des données ou encore fabriquer de fausses informations. Ces attaques, classées en passives ou actives, suivent souvent un schéma précis, allant de la reconnaissance initiale à l'exploitation de vulnérabilités. Elles peuvent prendre différentes formes, telles que les attaques par mot de passe, les attaques d'accès non autorisé, les attaques visant la disponibilité des ressources, ou encore les attaques basées sur des relations d'approbation.

Face à cette réalité, les entreprises doivent recourir à des mécanismes de défense adaptés, combinant des solutions techniques, organisationnelles et humaines. Ces mesures incluent l'application de politiques de sécurité strictes, ainsi que la protection physique des infrastructures informatiques.

II.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 compliquées 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]

II.3 Objectifs de la sécurité

Le système d'information représente l'ensemble des données de l'entreprise ainsi que ses infrastructures matérielles et logicielles.
Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. [2]

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou organisation sont uniquement utilisées dans le cadre prévu. [2]

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité** qui garantit que les données sont bien celles que l'on croit être, qu'elles n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- **La confidentialité** qui consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- **La disponibilité** qui permet de garantir l'accès à un service ou à des ressources.
- **La non-répudiation** de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction.
- **L'authentification** qui consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qui| 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.

II.3.1 L'intégrité

Garantit que les données sont bien celles que l'on croit être, qu'elles n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle). [2]

II.3.2 La confidentialité

Qui consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction. [2]

II.3.3 La disponibilité

Permet de garantir l'accès à un service ou à des ressources. [2]

II.3.4 La non répudiation

La non-répudiation de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction. [2]

II.3.5 L'authentification

Consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qui| 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. [2]

Figure (II-1) : Principaux objectifs de sécurité

II.4 Politique de sécurité

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 leur ont été octroyés.
La sécurité informatique doit toutefois 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.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes : [2]

- ✓ **Identifier les besoins** en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- ✓ **Élaborer des règles et des procédures** à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- ✓ **Surveiller et détecter les vulnérabilités** du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- ✓ **Définir les actions** à entreprendre et les personnes à contacter en cas de détection d'une menace.

II.4 Les Menaces

Les systèmes d'information sont vulnérables par rapport à plusieurs menaces susceptibles de leur infliger différents types de dommages et des pertes significatives.
Les effets des différentes menaces varient considérablement suivant les conséquences affectant l'entreprise, certaines affectent la confidentialité ou l'intégrité des données, d'autres agissent sur la disponibilité des systèmes. [3]

Les menaces les plus communes sont représentées ci-dessous :

II.4.1 Programme malveillants

Ils font référence aux virus, chevaux de Troie, bombes logiques et autres logiciels indésirables. Souvent, leur point d'entrée se situe au niveau des ordinateurs personnels mal protégés lors de leur connexion sur Internet, Leurs effets peuvent s'étendre à tout le réseau de l'entreprise en contaminant d'autres matériels. Il est possible de se protéger de la plupart des risques liés à ces menaces. Aussi, dans les premières phases de mise en place de la sécurité du système d'information, un état des lieux, sous forme de diagnostic, va être nécessaire pour préparer une meilleure protection en détectant les vulnérabilités. [3]

II.4.2 Fraude et vol

Les fraudes ou vols peuvent être commis par l'intérieur ou l'extérieur de l'entreprise. Par expérience, il s'avère, la plupart du temps, que la menace vient de l'intérieur (des utilisateurs ayant des accès privilégiés aux systèmes). En effet, par défaut, ce sont les utilisateurs familiers de l'entreprise qui sont dans la meilleure position pour commettre des forfaits. [3]

II.4.3 Sabotages causés par les employés

Ce sont les personnels les plus familiarisés avec les systèmes et les applications. Ils peuvent donc perpétrer des dommages, sabotages ... Ce qui implique la nécessité de gérer et de contrôler de façon rigoureuse les comptes des utilisateurs, surtout de ceux qui ont des accès privilégiés aux systèmes. [3]

II.4.4 Erreurs et omissions

Ce sont des menaces importantes pour l'intégrité des données et des systèmes. Ces erreurs ont souvent une origine humaine. En effet, même les programmes les plus sophistiqués ne peuvent pas tout détecter.
N'importe quelle personne intervenant sur le système d'information (utilisateur, administrateur système, développeur ...) contribue directement ou indirectement à ces dangers mettant en péril la sécurité des systèmes. Souvent l'erreur concerne une menace (erreur d'entrée de données, erreur de programmation ...) ou encore crée elle-même la vulnérabilité. [3]

II.4.5 Les Hackers

Le terme hacker ou encore cracker fait référence à la personne qui s'introduit dans les systèmes d'information sans autorisation pour, dans le pire des cas, provoquer des dégradations dans les données ou les applications. Ses actions peuvent s'effectuer à partir de l'intérieur (dans le cas où il a pu obtenir un accès sur le réseau) ou de l'extérieur de l'entreprise.
Toutefois, il n'est pas toujours facile de détecter sa présence sur les systèmes ni de connaître ce qu'il a provoqué comme dégâts. [3]

II.5 Les attaques

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.
Sur Internet des attaques ont lieu en permanence, à raison de Plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, Vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de L'action de pirates informatiques.
Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer. [2]

II.5.1 Buts des attaques

Comme il est décrit dans la **Figure (II-2),** ils existent quatre objectifs potentiels d'une attaque [4] :

- **L'interruption :** vise la disponibilité des informations dans un réseau (Déni de service).
- **L'interception :** vise la confidentialité des données circulant dans un réseau (capture de contenu, analyse de trafic).
- **La modification :** vise l'intégrité des informations en provoquant des incohérences dans le système (modification, rejeu).
- **La fabrication :** vise l'authenticité des informations en usurpant l'identité d'un utilisateur ou d'un service (mascarade).

Figure (II-2) : Buts des attaques [4]

II.5.2 Classifications des attaques réseaux

Les attaques peuvent être classées en deux grandes catégories, selon la phase de leur opération :

Attaques passives : consistent à écouter et à surveiller les transmissions sur un canal, sans modifier les données dans un réseau. En effet, l'attaquant peut intercepter et capturer une donnée transmise, ou bien analyser le trafic d'un réseau dans le but de rechercher des informations sensibles pouvant être utilisées pour d'autres types d'attaques, tels que les mots de passe [5]. Les attaques passives sont généralement indétectables, mais une prévention est possible en cryptant la transmission entre les nœuds du réseau,

Attaques actives : consistent à modifier les messages transmis, à s'introduire dans des équipements d'un réseau, ou à perturber le bon fonctionnement de ce dernier. Contrairement aux attaques passives, les attaques actives sont détectables dû aux dommages conséquents qu'elles peuvent provoquer. Le but d'un attaquant est d'essayer de contourner ou d'entrer dans un système sécurisé pour voler, modifier, désactiver ou détruire des données sensibles.

Voici les attaques actives les plus connues [6] :

- **Par mascarade (ou usurpation d'identité) :** Cette attaque a lieu lorsqu'une entité prétend être une entité différente. Ce type d'attaque est l'origine de toutes les autres attaques actives,

- **Par rejeu :** Ce type d'attaques consiste à capturer un message transmis (attaque passive), ensuite à le retransmettre ultérieurement pour produire un effet non autorisé,

- **Par modification de message :** Cette attaque permet de modifier le contenu du message ou de réordonner les messages pour produire un effet non autorisé,

- **Par déni de service :** Le principe de cette attaque est de perturber ou d'interrompre le service d'un réseau. Son but est de saturer le service avec des messages inutiles afin de dégrader les performances du service ou de provoquer la perte des messages.

Il est difficiles de garantir une protection absolue contre les attaques actives à cause des vulnérabilités existantes au niveau matériel, logiciel et protocolaire, surtout si ces derniers n'ont pas été vérifiés et validés formellement.

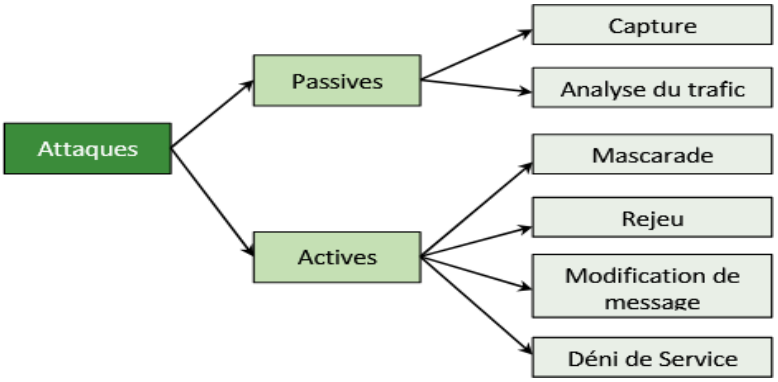


Figure (II-3) : Classification des attaques réseaux [6]

II.5.3 Etapes d'une attaque

Pour procéder à une attaque d'un réseau ou un service, l'assaillant suit généralement une méthode en sept étapes [7] :

1. **Analyse d'empreinte (reconnaissance) :** Un service d'une entreprise, comme par exemple sa page Web, peut fournir des données telles que les adresses IP des serveurs. Avec ces données, l'assaillant peut élaborer le profil ou l'empreinte de la sécurité de cette entreprise ;
2. **Enumération des informations** : l'assaillant étend sa connaissance du profil de sécurité en surveillant le trafic du réseau à l'aide d'un analyseur de paquets comme l'outil Wireshark par exemple. Par ailleurs, il peut chercher des informations telles que les

numéros de version des serveurs FTP ou des serveurs de messagerie. Ensuite, il peut croiser ces informations avec des bases de données de vulnérabilité ;

3. **Manipulation des utilisateurs pour obtenir un accès** : Les employés de l'entreprise utilisent parfois des mots de passe faciles à casser. Dans d'autres cas, ils peuvent être trompés par des assaillants astucieux et leur fournissent des données d'accès sensibles ;

4. **Escalade des privilèges** : Une fois un accès de base obtenu, l'assaillant utilise ses compétences pour augmenter ses privilèges d'accès au réseau, tout en essayant d'être indétectable par les techniques sécuritaires de l'entreprise ;

5. **Collecte d'autres mots de passe et secrets** : Avec davantage de privilèges d'accès, l'assaillant se sert de ses talents pour accéder à des informations sensibles bien protégées, tels que les rapports internes ou même les contrats numérisés de l'entreprise ;

6. **Installation de portes dérobées (Backdoors)** : Les portes dérobées sont des moyens permettant à l'assaillant d'entrer secrètement dans le système sans être détecté, servant de faille du système de l'entreprise. La porte dérobée la plus courante est le port TCP ou UDP ouverts en écoute ;

7. **Exploitation du système compromis** : Une fois qu'il a compromis le fonctionnement du système, l'assaillant utilise la porte dérobée pour lancer des attaques vers d'autres hôtes du réseau.

II.5.4 Les différents types d'attaque réseau

II.5.4.1 Les attaques de reconnaissance

Une attaque de reconnaissance ou « attaque passive » a pour objectif de regrouper des informations sur le réseau cible pour déceler toutes les vulnérabilités.
Cette attaque utilise, en général, les méthodes de base suivantes : [8]

1. **Un balayage de « ping » :** l'attaquant envoie des paquets « ping » à une plage d'adresses IP pour identifier les ordinateurs présents dans un réseau.

2. **Le balayage de port :** l'attaquant procède à une analyse de port (TCP et UDP) permettant de découvrir les services s'exécutant sur un ordinateur cible.

3. **Une capture de paquets (sniffing) :** la capture de paquets permet de capturer les données (généralement des trames Ethernet) qui circulent sur le réseau en vue d'identifier des adresse MAC, des adresses IP ou des numéros de ports utilisés dans le réseau cible. Cette attaque permet même de découvrir des noms d'utilisateur ou des mots de passe. Les logiciels de capture de paquets les plus couramment utilisés sont wireshark et tcpdump.

II.5.4.2 Les attaques du mot de passe

L'objectif de ces attaques est de découvrir les noms d'utilisateurs et les mots de passe pour accéder à diverses ressources. On distingue deux méthodes souvent utilisées dans ce type d'attaque : [8]

1. **L'attaque par dictionnaire :** cette méthode se base sur une liste de mots ou de phrases souvent utilisés comme mots de passe.

2. **L'attaque par force brute** : cette méthode essaie toutes les combinaisons possibles de lettres, de chiffres ou de symboles pour détecter le mot de passe d'un utilisateur.

II.5.4.3 Les attaques d'accès

Ces attaques ont pour objectif d'essayer de récupérer des informations sensibles sur les éléments du réseau. Les méthodes suivantes sont courantes pour effectuer une attaque d'accès : [8]

1. **Le phishing :** le phishing est une tentative de récupérer des informations sensibles (généralement des informations financières comme les détails de cartes de crédit, login, mot de passe, etc.), en envoyant des e-mails non sollicités avec des URL truqués.

2. **Le pharming :** c'est une autre attaque de réseau visant à rediriger le trafic d'un site web vers un autre site web.

3. **L'attaque de « Man-in-the-middle » :** un attaquant se place entre deux éléments réseaux pour essayer de tirer profit des données échangées. Cette attaque se base, entre autres, sur les méthodes suivantes :

    3.1. **L'usurpation d'identité (spoofing) :** c'est une pratique dans laquelle la communication est envoyée à partir d'une source inconnue déguisée en source fiable du récepteur. Elle permet de tromper un firewall, un service TCP, un serveur d'authentification, etc. L'usurpation d'identité peut avoir lieu à différents niveaux : une adresse MAC, une adresse IP, un port TCP/UDP, un nom de domaine DNS.

    3.1. **Le détournement de session (hijacking) :** l'attaquant pirate une session entre un hôte et un serveur pour obtenir un accès, non autorisé, à ce service. Cette attaque s'appuie sur le spoofing.

    3.1. **Les attaques mélangées :** les attaques mélangées combinent les caractéristiques des virus, des vers et d'autres logiciels pour collecter des informations sur les utilisateurs.

II.5.4.4 Les attaques du réseau contre la disponibilité

1. **Les attaques DoS (Denial of Service)**, ou attaques par déni de service, consistent à rendre indisponible un service de diverses manières. Ces attaques se divisent, principalement, en deux catégories : [8]

   1.2 Les dénis de service par saturation : ils consistent à submerger une machine de fausses requêtes afin qu'elle soit incapable de répondre aux requêtes réelles.

   1.3 Les dénis de service par exploitation de vulnérabilité : ils consistent à exploiter une faille du système distant afin de le rendre indisponible.

2. **Les attaques DDoS (Distributed Denial of Service)** relèvent d'un type d'attaque « DoS », provenant de nombreux ordinateurs connectés, contrôlés par les hackers, qui attaquent différentes régions géographiques. Le principe de ces attaques se base, entre autres, sur les méthodes suivantes : [8]

   2.1 L'attaque SYN flood : un attaquant envoie de nombreux paquets TCP- SYN pour lancer une connexion « TCP », sans envoyer un message « SYN-ACK ».

   2.2 L'attaque ICMP flood : un attaquant envoie de nombreux faux paquets ICMP vers l'ordinateur cible.

II.5.4.5 Les attaques rapprochées

Une attaque rapprochée est un type d'attaque où l'attaquant est physiquement proche du système cible. L'attaquant exploite l'avantage d'être physiquement proche des appareils cibles pour, par exemple, réinitialiser un routeur, démarrer un serveur avec un CD, etc. [8]

II.5.4.6 Les attaques de la relation d'approbation

Un attaquant, lors du contrôle d'une machine réseau, exploite la relation d'approbation entre cette machine et les différents périphériques d'un réseau pour avoir plus de contrôle. [8]

II.6 Mécanismes de défense

Un mécanisme de sécurité, est un ensemble de stratégies conçues pour détecter, prévenir et lutter contre une attaque de sécurité [9]. Avec l'évolution des systèmes et des réseaux, il existe une panoplie de mécanismes de sécurité servant à protéger les systèmes ainsi que les services qu'ils offrent. Nous abordons dans ce qui suit, les principaux mécanismes utilisés :

II.6.1 Audit de sécurité

L'audit de sécurité d'un réseau offre une image complète du réseau sous forme d'un rapport détaillé qui donne un aperçu instantané et en temps réel du statut du réseau. Une analyse peut être faite sur le résultat du balayage en utilisant des filtres dans les rapports, ce qui permet de sécuriser le réseau de manière proactive, par exemple, en fermant les ports ouverts, en supprimant les comptes utilisateurs qui ne sont plus utilisés ou en désactivant les points d'accès sans fil. En terme de sécurité, il permet d'identifier des points de vulnérabilité du réseau, cependant, il ne permet pas de détecter les attaques qu'a déjà subit le réseau ou que subira dans le futur. [10]

II.6.2 Journalisation

La journalisation consiste à enregistrer les activités et les connexions de chaque acteur utilisant un réseau. En effet, les journaux d'évènements (logs) constituent une brique technique indispensable à la gestion de la sécurité des réseaux et plus généralement des systèmes. En effet, les journaux sont une source d'information riche permettant de constater si des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.

Dans ce cas, les évènements constituant les journaux sont consultés et analysés en temps réel.
Les journaux peuvent également être employés a posteriori pour retrouver les traces d'un incident de sécurité ; l'analyse des journaux d'un ensemble de composants (postes de travail, équipements réseaux, serveurs, etc.) peut alors permettre de comprendre le cheminement d'une attaque et d'évaluer son impact. [10]

II.6.3 Antivirus

Un antivirus est un logiciel permettant de protéger une machine contre les programmes/logiciels néfastes ou les fichiers potentiellement exécutables. De nos jours, les antivirus sont aussi des anti-malwares c'est-à-dire il protègent aussi les machines contre tous les autres types de malwares à savoir les vers et les chevaux de Troie. Il consiste à chercher les codes malveillants dans les logiciels infectés.
Cependant, un antivirus ne protège pas le réseau contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime accédant à une ressource alors qu'il n'est pas autorisé à le faire. [10]

II.6.4 Systèmes de détection d'intrusion

Un système de détection d'intrusions (ou IDS 1) est un appareil ou une application qui alerte l'administrateur en cas de faille ou de violation de règles de sécurité dans un réseau, permettant ainsi de prévenir les risques d'intrusion. Ce système consiste à surveiller et analyser les activités d'un réseau en repérant celles qui sont anormales ou suspectes, cependant, il ne permet pas de détecter les accès incorrects mais autorisés par un utilisateur légitime.
Par ailleurs, certaines mauvaises détections peuvent arriver tels que les taux de faux positifs et les taux de faux négatifs. [10]

II.6.5 Pare-feu

Un pare-feu (ou Firewall en anglais) est un système logiciel ou matériel installé sur une machine ou un routeur, permettant de contrôler les communications qui traversent un réseau donné. Ce mécanisme permet de protéger un réseau privé de certaines intrusions provenant d'un réseau externe (par exemple internet), telles que les communications sortantes déclenchées par un malware installé. Par ailleurs, il a pour fonction de faire respecter la politique de sécurité du réseau, qui définit quelles sont les communications autorisées ou interdites. Concrètement, il s'agit d'une passerelle qui consiste à filtrer les paquets entrants et sortants en se basant sur une interface pour le réseau à protéger, et une autre pour le réseau externe (souvent c'est internet) [11]. Néanmoins, le pare-feu ne protège pas le réseau contre une attaque venant du réseau intérieur (c'est-à-dire celui qui ne le traverse pas), et il n'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système.

II.6.6 Contrôle d'accès

Le mécanisme du contrôle d'accès au réseau (NAC 2) permet de renforcer sa sécurité en limitant les ressources réseau accessibles aux terminaux selon une stratégie de sécurité définie. En effet, il permet de vérifie les droits d'accès aux données d'un utilisateur, toutefois, il n'empêche pas l'exploitation d'une vulnérabilité par un assaillant.
Le NAC convient particulièrement aux grands organismes et entreprises qui exercent un contrôle strict sur leur réseau. Les solutions existantes possibles pour gérer les accès autorisés sont l'utilisation des VPN ou des tunnels. [10]

II.6.7 Authentification réseau

L'authentification réseau permet d'authentifier une machine quand elle essaie de se connecter sur le réseau et savoir avec précision si elle est déjà connectée en lui donnant les autorisations nécessaires pour l'usage du réseau. L'authentification réseau est nécessaire au bon fonctionnement des autres mécanismes de défense, et elle est indépendante des autres méthodes d'authentifications vers les systèmes d'exploitation ou les applications.
Il existe deux catégories de protocoles qui peuvent être utilisés pour l'authentification réseau, il y a d'une part, (1) les protocoles propriétaires comme VMPS de Cisco Authentification qui est seulement valable sur une adresse MAC et réseau filaire ; et d'autre part, (2) il y a les protocoles ouverts comme RADIUS et 802.1x Authentification sur adresse MAC [12].

1. IDS : Intrusion Detection Systems
2. NAC : Network Access Control ou Network Admission Control

II.6.8 Bourrage de trafic

Le bourrage de trafic est destiné à protéger un réseau contre les attaques passives qui consistent à capturer et à analyser le trafic circulant dans le réseau. Ce mécanisme consiste à injecter des messages inutiles pour faire échouer les tentatives d'analyse du trafic. Cette pratique permet d'améliorer la confidentialité des données, notamment au niveau du volume du trafic. [10]

II.6.8 Chiffrement des données

Le chiffrement consiste à transformer un message en clair en un message incompréhensible, en utilisant généralement un algorithme basé sur des clés. Essentiellement, deux techniques de cryptographie sont utilisées : (1) Le chiffrement symétrique qui consiste à utiliser la même clé dite secrète pour chiffrer et déchiffrer un message, tandis que (2) le chiffrement asymétrique qui se base sur une paire de clés, c'est-à-dire une clé publique pour le chiffrement du message, et une clé privée pour le déchiffrer, sachant que seul le destinataire du message qui possède la clé privée lui permettant de déchiffrer le message. [10]

II.6.9 Signature numérique

La signature numérique est un mécanisme permettant de garantir l'intégrité et la non-répudiation d'un message ou d'un document électronique. Analogiquement à la signature manuscrite d'un document papier, la signature numérique permet d'authentifier un document ou un contrat électronique. [10]

II.6.10 Protection physique

La protection physique d'un réseau consiste à rendre inaccessible tous ses équipements, pour fournir une protection totale, mais qui peut être excessive, car le réseau n'aura aucun accès de l'extérieur. Par exemple, le fait d'isoler complètement le réseau d'un organisme sensible telle que une centrale nucléaire, toutefois, cette solution peut paraître trop radicale dans le cas des entreprises. [10]

II.6.11 Bonnes pratiques

La sécurité informatique peut être assurée à travers des bonnes pratiques permettant d'atténuer les risques de sécurité et rendre les attaques de plus en mental consistent à : [13]

- ✓ Concevoir une politique écrite de sécurité.
- ✓ Former les employés concernant les risques de social engineering et développer des stratégies pour valider les identités à travers le téléphone, le mail ou encore des personnes.
- ✓ Utiliser des mots de passe forts et les changer régulièrement.
- ✓ Contrôler d'accès physique aux systèmes.
- ✓ Utiliser des mots de passe forts et les changer régulièrement.
- ✓ Chiffrer les données sensibles et les protéger par mots de passe.
- ✓ Limiter la connexion en mode privilégié au niveau du système d'exploitation.
- ✓ Déployer le matériel et les logiciels la sécurité.
- ✓ Effectuer des sauvegardes et tester les fichiers sauvegardés régulièrement.

- ✓ Désactiver les services et les ports non utilisés.

- ✓ Garder les correctifs à jour en les installant chaque semaine ou tous les jours pour éviter les dépassements de mémoire tampon et les attaques par élévation de privilèges.

- ✓ Prévoir périodiquement des audits de sécurité pour tester le réseau et les systèmes et veiller à appliquer les recommandations qui en résultent.

Conclusion

En définitive, la sécurité des systèmes informatiques s'impose comme un élément incontournable pour assurer la pérennité et la performance des entreprises. Elle constitue une réponse stratégique aux risques croissants liés à la dépendance aux technologies de l'information. L'analyse des objectifs de sécurité, l'identification des menaces et des types d'attaques, ainsi que la mise en œuvre de politiques et de mécanismes de défense adaptés permettent de renforcer la résilience des systèmes face aux cybermenaces. Toutefois, il est important de souligner que la sécurité informatique n'est jamais absolue : elle nécessite une vigilance permanente, une adaptation continue et une combinaison équilibrée de mesures techniques, organisationnelles et physiques. C'est dans cette approche globale et proactive que réside la véritable efficacité d'une stratégie de sécurité informatique.

CHAPITRE III :

Mécanismes et Solutions de Sécurité Réseau

III.1 Introduction

La sécurité des réseaux constitue aujourd'hui un enjeu majeur pour les entreprises et les organisations, en raison de la multiplication des menaces, de la diversification des équipements connectés et de l'ouverture des systèmes d'information. Dans ce contexte, la mise en place d'une politique de sécurité réseau rigoureuse et de mécanismes de contrôle d'accès efficaces s'impose comme une nécessité afin de garantir la protection et la fiabilité des infrastructures.

Ce chapitre est consacré à l'étude approfondie des mécanismes et solutions de sécurité réseau, en mettant particulièrement l'accent sur le Network Access Control (NAC), qui joue un rôle central dans le contrôle d'accès et la gestion de la conformité des terminaux connectés au réseau. Dans un premier temps, nous présenterons la notion de NAC, ses principales fonctionnalités telles que l'authentification, l'autorisation, l'évaluation de la posture, la mise en quarantaine et la remédiation des systèmes non conformes. Nous aborderons également les différents types de déploiement du NAC (avec ou sans agent, basé sur le matériel ou dynamique) ainsi que les concepts liés au contrôle d'accès pré-admission et post-admission.

La suite du chapitre sera consacrée à l'étude des mécanismes fondamentaux d'authentification tels que le protocole IEEE 802.1X et RADIUS, ainsi que les différentes méthodes d'authentification EAP. Nous présenterons ensuite l'architecture générale d'une solution NAC et les composants essentiels impliqués dans son fonctionnement, avant d'examiner les principales solutions existantes sur le marché, qu'elles soient libres (OpenNAC, PacketFence, FreeNAC) ou commerciales (FortiNAC, Juniper UAC, Cisco ISE).

Une analyse comparative permettra de justifier le choix de la solution Cisco Identity Services Engine (ISE) comme la plus adaptée à notre projet. Nous décrirons ensuite en détail son architecture, ses fonctionnalités principales, ses modules (PAN, MNT, PSN), ainsi que ses différentes méthodologies d'authentification et d'autorisation. Enfin, nous aborderons les cas d'utilisation concrets de Cisco ISE, notamment l'accès invité, l'accès sans fil et filaire sécurisé, la gestion du BYOD (Bring Your Own Device) et la conformité des terminaux, afin d'illustrer son rôle central dans la mise en œuvre d'une politique de sécurité réseau complète et dynamique.

III.2 NAC (Network Access Control)

Le contrôle d'accès au réseau (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 : [14]

- Authentification et autorisation.
- Évaluation de la posture (évaluation d'un end-point 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.

III.2.1 Types de contrôle d'accès au réseau

- **NAC basé sur le matériel** : qu'il soit « en ligne » ou « hors bande », cette solution nécessite généralement un dispositif qui doit être déployé dans pratiquement tous les espaces où le NAC est requis. Certains de ces dispositifs fonctionnent entre la couche d'accès au réseau et les commutateurs réseau, tandis que d'autres ont remplacé les commutateurs d'accès [15].

- **NAC basé sur des agents logiciels :** l'étape suivante consiste à installer de petits programmes appelés « agents » sur tous les systèmes que le NAC doit contrôler. Ces agents résident sur les ordinateurs et autres appareils électroniques. Les résultats des analyses et de la surveillance des appareils sont souvent envoyés à un serveur centralisé via ces agents. Afin de se conformer aux réglementations de sécurité, les systèmes qui ne répondent pas aux normes ne se voient pas accorder l'autorisation d'accès au réseau et font souvent l'objet d'une mesure corrective [15].

- **NAC sans agents logiciels :** une autre variante est le NAC sans agent, qui utilise des composants logiciels à la demande. Dans cette configuration, un agent temporaire, généralement un contrôle ActiveX, analyse régulièrement le client à la recherche de failles de sécurité ou de violations de la politique de sécurité. Les résultats de l'analyse sont transmis au serveur de politique principal, où, si le système n'est pas conforme aux normes, une action est déclenchée si nécessaire. L'agent est téléchargé une fois la procédure terminée [15].

- **NAC dynamique :** également appelé « NAS Peer-to-Peer », car il s'agit d'une option qui ne nécessite aucune modification au niveau du réseau ni aucune installation de logiciel sur chaque ordinateur. Des agents sont installés dans des systèmes sécurisés et deviennent parfois nécessaires [15].

III.2.2 Concepts du contrôle d'accès au réseau.

- **Pré-admission et post-admission** : prise en charge basée sur des politiques avant l'accès au réseau de conception en vigueur dans le NAC. Un hôte doit d'abord passer une évaluation de pré-admission avant de se voir accorder un accès complet au réseau. Une fois l'accès autorisé, un hôte peut être examiné périodiquement afin de s'assurer qu'il ne devient pas une menace grâce à l'évaluation post- admission [16].

- **Avec agent ou sans agent** : les processus d'authentification et d'évaluation de la sécurité dans la technologie NAC peuvent être effectués directement par un agent logiciel installé sur le terminal ou indirectement en évaluant les réponses du terminal par un moteur d'analyse externe basé sur le réseau [17].

- **Hors bande ou en ligne** : l'emplacement des mécanismes de prise de décision et d'application au sein du réseau peut également avoir une incidence sur la configuration du NAC. Dans le cas des solutions hors bande Figure (III -2), on utilise souvent un serveur de politiques qui n'est pas directement impliqué dans le trafic réseau. Comme alternative, les systèmes NAC en ligne Figure (III-1) intègrent l'application et la prise de décision à un emplacement unique qui fait partie du flux de trafic normal [18].

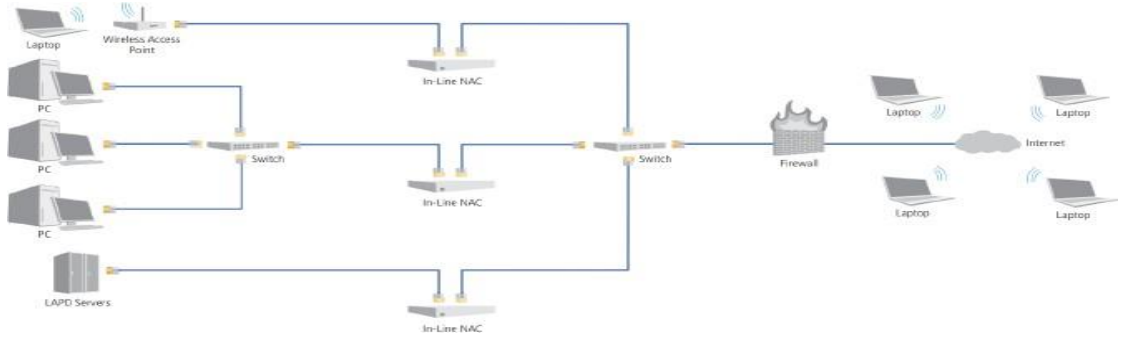


Figure (III-1) : Solution NAC en ligne

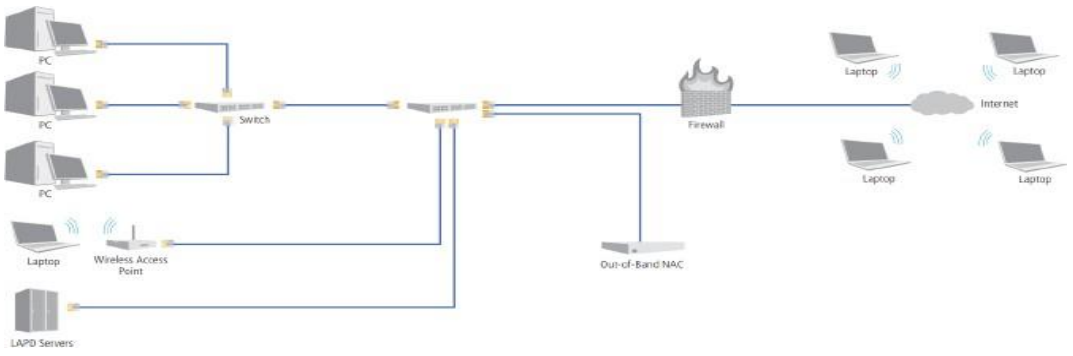


Figure (III -2) : Solution NAC hors bande

- **Remédiation, quarantaine et portails captifs :** L'idée derrière le déploiement de solutions NAC par les opérateurs réseau est que certains clients authentiques se verront refuser l'accès au réseau (si les utilisateurs n'avaient jamais de niveaux de correctifs obsolètes, le NAC serait inutile). Par conséquent, les solutions NAC nécessitent un moyen de résoudre les problèmes des utilisateurs finaux qui empêchent l'accès [19].

Il existe deux méthodes de remédiation courantes :

- **Quarantaine** : un réseau IP restreint, appelé réseau de quarantaine, permet aux utilisateurs d'accéder uniquement à des hôtes et des applications spécifiques. Lorsqu'un produit NAC détecte qu'un utilisateur final est obsolète, le port du commutateur est attribué à un VLAN qui n'est routé que vers les serveurs de correctifs et de mises à jour et non vers le reste du réseau [19].

- **Portails captifs** : un portail captif bloque le trafic HTTP vers les sites Web et redirige les visiteurs vers une application Web qui leur fournit des conseils et des outils pour mettre à jour leur PC. Aucune utilisation du réseau autre que la passerelle captive n'est autorisée tant que leur ordinateur n'a pas passé avec succès un examen automatique. L'accès sans fil payant fonctionne de manière similaire dans les points d'accès publics [19].

III.3 Protocoles de contrôle d'accès au réseau

III.3.1 Le protocole 802.1x

Le protocole 802.1X a été mis au point par l'IEEE en juin 2001. Il a pour but d'authentifier un client afin de lui autoriser l'accès à un réseau.
On utilise le protocole EAP (Extensible Authentication Protocol) et un serveur d'authentification qui est généralement un serveur RADIUS.
Le serveur RADIUS va authentifier chaque client qui se connecte au réseau sur un port. [20]

Le mécanisme de contrôle d'accès 802.1x est déployé dans le réseau LAN (Local Area Network) mettant en œuvre les technologies suivantes [21] :

- La technologie Ethernet dans le cas d'un accès à un switch ;

- La technologie Wi-Fi (Wireless-Fidelity) dans le cas d'une connexion à un point d'accès AP (Access Point).

L'authentification utilise le mécanisme de contrôle d'accès 802.1x qui définit trois composantes **Figure (III -3)** [21] :

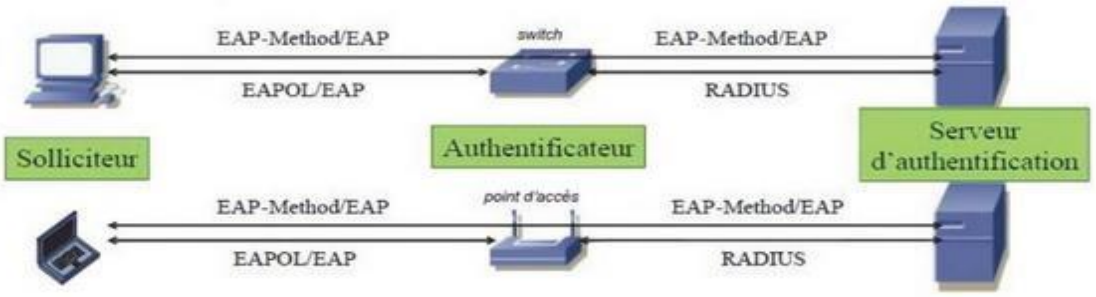


Figure (III -3) : les composants du mécanisme de 802. 1x [21]

- Le solliciteur est le dispositif (l'hôte du réseau) qui désire accéder au réseau Ethernet ou Wi-Fi ;
- L'authentificateur est le dispositif (le switch Ethernet ou le point d'accès Wi-Fi) qui contrôle l'accès du solliciteur au réseau LAN ;
- Le serveur d'authentification est le dispositif qui authentifie le solliciteur et autorise l'accès au réseau LAN.

Le mécanisme 802.1x s'appuie sur une suite de protocoles **Figure (III -4)** [21] :

- le protocole EAPOL (EAP (Extensible Authentication Protocol) Over LAN) échangé entre le solliciteur et l'authentificateur ;
- le protocole EAP échangé entre, d'une part, le solliciteur et, d'autre part, l'authentificateur ou le serveur d'authentification :
- le protocole EAP est porté par le protocole EAPOL sur l'interface entre le solliciteur et le serveur d'authentification.
- le protocole EAP porte des messages EAP-Method échangés entre le solliciteur et le serveur d'authentification ;
- le protocole RADIUS (Remote Authentication Dial-In User Service) échangé entre l'authentificateur et le serveur d'authentification. Le protocole RADIUS porte le protocole EAP et les messages EAP-Method sur l'interface entre l'authentificateur et le serveur d'authentification.

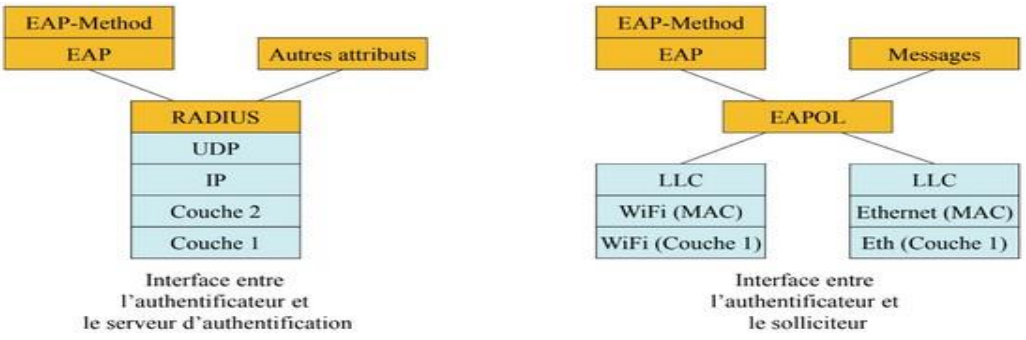


Figure (III -4) : L'architecture protocolaire du mécanisme 802. 1x [21]

III.3.2 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.
Pour l'authentification il y a quatre types de paquets [20] :

- **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)

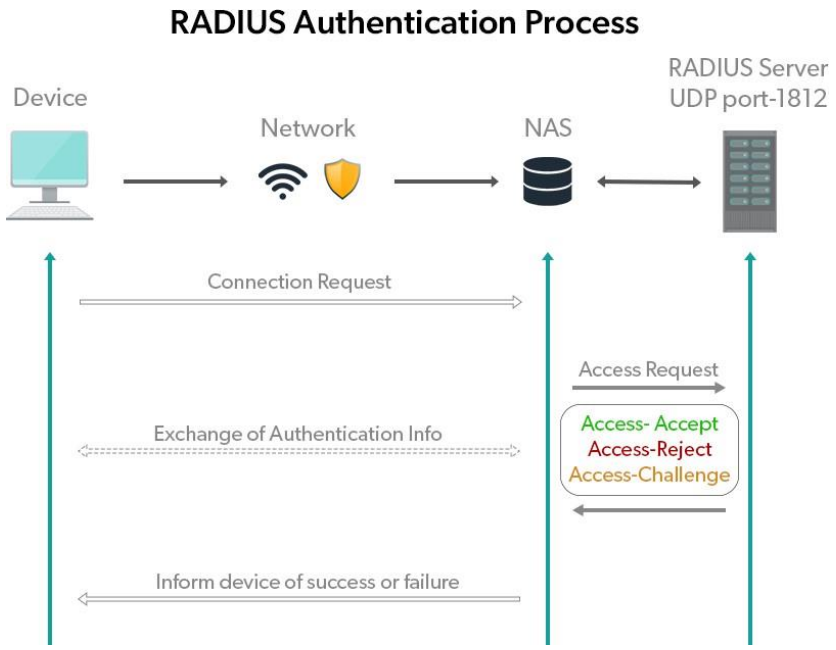


Figure (III -5) : Le processus de l'authentification Radius [22]

III.3.2.1 La méthode d'authentification Radius [23] :

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).

III.3.3 Les méthodes d'authentification

Il existe de nombreux choix pour la méthode d'authentification, pour citer certains des plus connus et utilisés :

Type d'EAP	Méthode d'authentification	Caractéristiques
EAP-MD5	Login/password	•Facile à implémenter •Supporté par la plupart des serveurs •Attaquable par dictionnaire hors-ligne •Pas d'authentification mutuelle
EAP-TLS	Certificat	•Utilisation de certificats par le client et le serveur, de ce fait création d'un tunnel sur. •Authentification mutuelle entre le client et serveur •Lourd à mettre en place à cause des certificats coté client.
EAP-PEAP EAP-TTLS	Login/password Et certificat	•Création d'un tunnel TLS •Moins lourd que EAP-TLS, car pas de certificat du coté client. •Moins sur que EAP-TLS, car pas de certificat du côté client.

Figure (III -6) : les caractéristiques des différents méthodes d'authentification [20]

III.3.3.1 Les types de paquets existants

Les types de paquets de base : [20]

- **EAP Request** : Envoyé par le contrôleur d'accès au client.
- **EAP Response** : Réponse du client au contrôleur d'accès.
- **EAP Success** : Paquet envoyé au client en fin d'authentification si elle est réussie.
- **EAP Failure** : Paquet envoyé au client en fin d'authentification si elle est ratée.

Les types de paquets ajoutés par la norme 802.1x : [20]

- **EAPoL-Start** : qui permet au client d'alerter le contrôleur d'accès qu'il souhaite se connecter.
- **EAPoL-Packet** : Paquet qui encapsule les paquets EAP.
- **EAPoL-Key** : Paquet qui permet l'échange de clé de cryptage.
- **EAPoL-Logoff** : permet d'amorcer la fermeture de session.

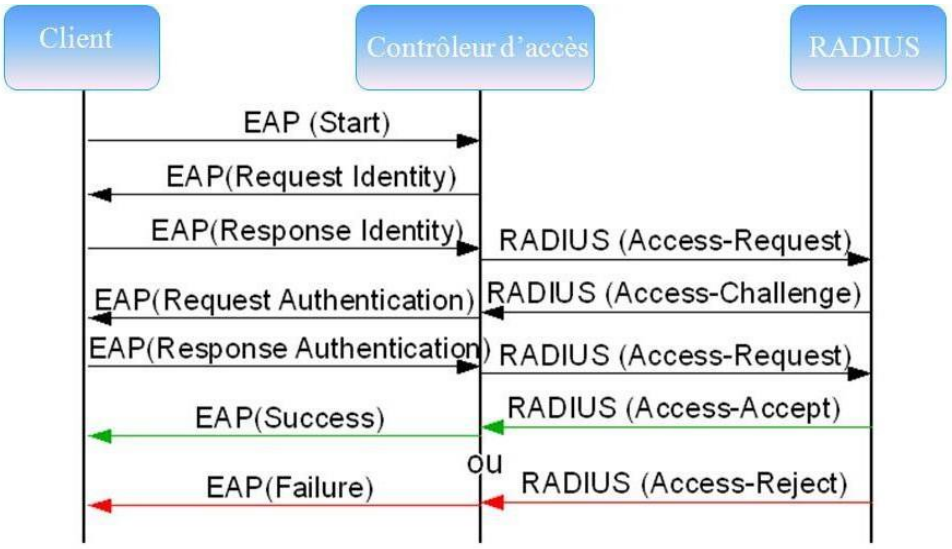


Figure (III -7) : Etapes d'authentification 802.1X [20]

III.4 Architecture générale du NAC

Tous les produits NAC comportent trois éléments fondamentaux : l'Access Requester (également appelé AR), le Policy Decision Point (PDP) et le Policy Enforcement Point (ou PEP) [25].

Une architecture NAC de haut niveau est illustrée dans la figure précédente (Figure I-5), dans laquelle les utilisateurs finaux peuvent accéder aux ressources de l'entreprise via un réseau WLAN, VPN et LAN [26]. Selon la mise en œuvre du fournisseur, les opérations PDP et PEP spécifiques peuvent être situées sur un seul serveur ou réparties sur plusieurs serveurs, mais en général, l'AR demande l'accès, le PDP attribue une politique et le PEP applique cette politique.

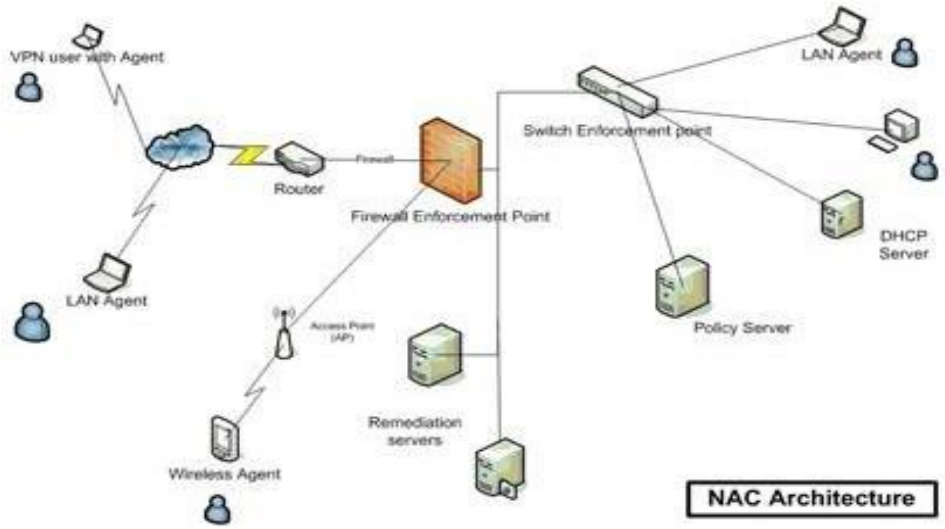


Figure (III -8) : Architecture générale de NAC

III.4.1 Composants de NAC :

III.4.1.1 Agent

L'agent de confiance est l'un des composants essentiels du NAC qui s'agit d'un logiciel client installée localement sur un end-point. Son principal rôle consiste à collecter des informations à l'état du poste tel que la présence ou non d'antivirus et des derniers correctifs de sécurité.

III.4.1.2 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.

III.4.1.3 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.

III.4.1.4 Serveur de politique antivirus

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

III.5 Présentation des solutions de contrôle d'accès réseau (NAC)

Dans cette partie, nous allons étudier certaines solutions gratuites et commerciales de contrôle d'accès réseau (NAC) existantes sur le marché afin de pouvoir choisir une solution adaptée à notre projet.

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

III.5.1 Les solutions libres

III.5.1.1 OpenNAC

OpenNAC est un outil open source de contrôle d'accès au réseau qui fournit un accès pour les réseaux LAN/WAN. Il fonctionne avec un large éventail de clients de systèmes d'exploitation (Windows, Linux, Mac, etc.) et de dispositifs réseau tels que Extreme Networks, Cisco, 3Com et Alcatel. Le logiciel est développé à partir de composants open source éprouvés tels que FreeRadius, iTop et lcinga.
OpenNAC est également idéal pour la configuration et la découverte du réseau, la sauvegarde de la configuration des dispositifs réseau et la surveillance du réseau, en plus du contrôle d'accès inhérent.
OpenNAC offre également d'autres fonctionnalités, telles que l'authentification, l'autorisation et l'accès au réseau basé sur des politiques d'audit. Il permet également la surveillance en temps réel des utilisateurs et des dispositifs sur le réseau [27].

III.5.1.2 PacketFence

PacketFence est également une solution NAC gratuite et open source. Elle comprend un portail captif pour l'enregistrement et la correction, et offre en outre une gestion unifiée des réseaux câblés et sans fil, la prise en charge de la norme 802.1X et l'isolation de couche 2 des dispositifs problématiques. PacketFence autorise en outre l'intégration d'autres applications. PacketFence peut être utilisé pour sécuriser efficacement des réseaux de petite taille comme des réseaux hétérogènes extrêmement vastes [29].Les autres fonctionnalités de PacketFence sont la comptabilisation de la bande passante, la détection des activités réseau anormales, les analyses proactives de vulnérabilité, et il fournit une expression verbale complète de l'état de santé du réseau [30, 31].

III.5.1.3 FreeNAC :

FreeNAC est une solution Open Source pour gérer 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. [32]

III.5.2 Les solutions commerciales :

III.5.2.1 FortiNAC :

FortiNAC est une solution d'accès Zero Trust qui supervise et protège tous les actifs numériques connectés au réseau de l'entreprise, couvrant les appareils informatiques, IoT, OT/ICS et IoMT. Avec un contrôle d'accès réseau qui améliore la Fortinet Security Fabric, FortiNAC offre visibilité, contrôle et réponse automatisée pour tout ce qui se connecte au réseau. FortiNAC fournit une protection contre les menaces IoT, étend le contrôle aux périphériques réseau tiers et orchestre la réponse automatique à un large éventail d'événements réseau. [33]

III.5.2.2 Juniper Unified Access Control (UAC) :

Juniper Unified Access Control (UAC) est une solution de contrôle d'accès réseau qui offre un contrôle d'accès granulaire et une application stricte pour les réseaux d'entreprise. UAC utilise une combinaison de politiques basées sur l'utilisateur, l'appareil et l'emplacement pour appliquer le contrôle d'accès et assurer une sécurité cohérente sur tous les points d'accès réseau, y compris les réseaux câblés et sans fil.

UAC offre une gestion dynamique des politiques et une intégration avec plusieurs méthodes d'authentification, telles que Active Directory, LDAP et RADIUS. Il comprend également des fonctionnalités avancées de détection et d'atténuation des menaces, telles que la mise en quarantaine basée sur des politiques et le contrôle d'accès au réseau pour les appareils IoT.

L'UAC peut être déployé en tant que solution sur site ou en tant que service cloud, offrant ainsi aux organisations flexibilité et évolutivité. Dans l'ensemble, Juniper UAC est un outil important pour les organisations qui cherchent à sécuriser leur infrastructure réseau et à se protéger contre les menaces avancées [34].

III.5.3 Analyse comparative des solutions NAC

Dans le cadre de l'étude comparative des solutions NAC (Network Access Control), nous avons analysé plusieurs solutions open source et commerciales afin d'évaluer leurs fonctionnalités et leur pertinence pour une adoption dans l'entreprise Ourhoud. Les solutions étudiées sont : OpenNAC, PacketFence, FreeNAC (solutions libres), ainsi que FortiNAC, Juniper UAC et Cisco ISE (solutions commerciales).

Tableau 1Tableau comparatif des fonctionnalités NAC

Solutions / Fonctionnalité	OpenNAC	PacketFence	FreeNAC	FortiNAC	Juniper UAC	Cisco ISE
1. Machine virtuelle	✓	✓		✓	✓	✓
2. Réseau câblé et sans fil	✓	✓	✓	✓	✓	✓
3. Assistance communautaire	✓	✓	✓			
4. Gestion de la bande passante				✓		
5. Assistance du fournisseur réseau		✓		✓	✓	✓
6. Agent NAC		✓		✓	✓	✓
7. Détection des périphériques	✓	✓	✓	✓	✓	✓
8. Intégration avec Active Directory	✓	✓		✓	✓	✓
9. Fonction de création de rapports	✓	✓		✓	✓	✓
10. Évaluation de la posture de l'appareil		✓		✓	✓	✓
11. Remédiation		✓		✓	✓	✓
12. Gestion des actifs	✓	✓		✓	✓	✓

III.5.4 La solution de contrôle d'accès choisie :

L'analyse du tableau comparatif montre que les solutions open source comme OpenNAC, PacketFence et FreeNAC offrent certaines fonctionnalités intéressantes, mais restent limitées en termes de support officiel, de remédiation avancée et d'intégration complète avec des environnements d'entreprise complexes.

Les solutions commerciales telles que FortiNAC et Juniper UAC présentent un panel plus large de fonctionnalités, mais elles ne couvrent pas de manière optimale tous les besoins liés à la visibilité, la posture de sécurité et la gestion des actifs de manière centralisée.

En revanche, Cisco ISE se démarque comme la solution la plus complète et robuste. Elle intègre l'ensemble des fonctionnalités essentielles : profilage précis des périphériques, intégration native avec Active Directory, gestion de la posture des terminaux, remédiation dynamique, production de rapports détaillés, et gestion centralisée des politiques de sécurité. De plus, Cisco ISE bénéficie du support technique du constructeur, ce qui garantit une stabilité et une pérennité à long terme.

Ainsi, dans le contexte de l'entreprise Ourhoud, où la sécurité réseau et la conformité sont primordiales, Cisco ISE représente la meilleure solution à déployer. Elle permettrait de garantir un contrôle d'accès rigoureux, une visibilité complète des actifs connectés et une gestion simplifiée grâce à une console centralisée. Ce choix s'inscrit dans une démarche de modernisation et de sécurisation optimale de l'infrastructure informatique de l'entreprise.

III.6 Définition de CISCO ISE (Identity service engine).

Cisco ISE est un système de contrôle d'accès réseau et d'application des politiques basé sur l'identité. Il s'agit d'un moteur de politiques commun permettant de contrôler l'accès aux terminaux et l'administration des périphériques réseau pour les entreprises. ISE permet à un administrateur de contrôler de manière centralisée les politiques d'accès pour les terminaux filaires, sans fil et VPN d'un réseau. [36]

ISE établit un contexte autour des terminaux, notamment les utilisateurs et les groupes (qui), le type de périphérique (quoi), l'heure d'accès (quand), le lieu d'accès (où), le type d'accès (Filaire/sans fil/VPN) (Comment), les menaces et les vulnérabilités. En partageant des données contextuelles essentielles avec des intégrations de partenaires technologiques et en mettant en œuvre la politique Cisco TrustSec pour la segmentation définie par logiciel, ISE transforme un réseau de simple canal de données en un dispositif de sécurité qui accélère le temps de détection et de résolution des menaces réseau.[36]

Cisco ISE est conçu pour être un produit stratégique de classe entreprise dans le réseau. À cette fin, Cisco ISE est conçu pour prendre en charge jusqu'à 250 000 terminaux actifs et simultanés, soit plus que tout autre produit sur le marché, afin de garantir une intégration, une itinérance et un contrôle d'accès au réseau transparents dans l'ensemble d'un réseau d'entreprise distribué. Cisco ISE représente l'avenir de la gestion des politiques d'accès contextuelles sur le nouveau réseau d'entreprise : le réseau mobile, distribué et sans frontières. Il n'est pas étonnant que Cisco ISE soit le produit de choix de plus de 4 000 clients, dont un certain nombre d'entreprises du Fortune 500, d'établissements d'enseignement et d'agences gouvernementales. [37]

Figure (III -9) : Architecture fonctionnelle de Cisco Identity Services Engine (ISE) montrant ses principales composantes [35]

III.6.1 Les avantages de l'ISE :

- **Visibilité intégrale** : L'ISE permet une visibilité inégalée sur le réseau grâce à des capacités de profilage étendues permettant d'identifier et d'évaluer avec précision tous les utilisateurs et appareils connectés au réseau. [37]

- **Contrôle d'accès réseau renforcé** : Contrôle exceptionnellement robuste pour accorder, limiter et mettre en quarantaine l'accès au réseau, conformément à la politique commerciale appropriée de l'entreprise ou aux exigences et directives de conformité en matière de sécurité. [37]

- **Efficacité opérationnelle** : L'automatisation de l'intégration et de la sécurité, le contrôle centralisé des politiques, la visibilité, le dépannage et l'intégration avec les solutions Cisco PrimeTM permettent de réduire considérablement le temps consacré par le service informatique et le service d'assistance aux corrections de sécurité des utilisateurs et du réseau. [38]

- **Accès fiable partout** : Cisco ISE fournit des politiques sur le dispositif d'accès au réseau en temps réel, afin que les utilisateurs mobiles ou distants puissent bénéficier d'un accès cohérent à leurs services à partir de connexions filaires et sans fil. [38]

- **Application intégrée** : Des capacités de détection des appareils sont intégrées à la plupart des commutateurs et contrôleurs sans fil Cisco afin d'étendre le profilage à l'ensemble du réseau au point d'entrée, sans les coûts et la gestion liés aux appareils superposés ou au remplacement de l'infrastructure. [38]

- **Réduction des coûts opérationnels** : Réduction des coûts opérationnels grâce à l'efficacité obtenue en tirant parti des capacités de détection et d'application intégrées au réseau existant, associées à un contrôle centralisé des politiques et à une visibilité du réseau afin de rationaliser les efforts visant à sécuriser l'accès. [37]

- **Sécurité unifiée et contrôle centralisé** : Application étendue et cohérente des politiques via des contrôles d'accès au réseau, la sécurité des appareils MDM et l'atténuation des menaces SIEM/TD afin d'identifier les menaces de sécurité et d'atténuer la propagation des attaques sur le réseau. [37]

III.6.2 Les fonctions et caractéristiques de Cisco ISE :

Cisco ISE exécute les fonctions suivantes [39] :

- 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)

III.6.3 Les différents types de personas sur Cisco ISE : [40]

1. **PAN (Policy Administration Node)** : c'est le centre de gestion. Les administrateurs définissent les règles ici, et elles sont envoyées aux autres nœuds.

2. **MnT (Monitoring Node)** : c'est le centre de surveillance. Il collecte les journaux et génère des rapports sur tout ce qui se passe dans le réseau.

3. **PSN (Policy Service Node)** : c'est le point d'entrée. Quand un appareil veut se connecter, il passe par le PSN qui applique la règle de sécurité (ex : accès autorisé, refusé, invité, etc.).

La **figure (III -10)** illustre les différents rôles (personas) de Cisco ISE :

- **Policy Services Node (PSN)** : point d'application des politiques de sécurité, il prend les décisions d'accès (RADIUS/TACACS+).
- **Policy Administration Node (PAN)** : console centrale pour l'administration et la gestion des politiques.
- **Monitoring and Troubleshooting Node (MnT)** : collecte les journaux et génère les rapports.
- **pxGrid Controller** : facilite le partage de contexte entre les composants de sécurité.

En fonction de la taille du déploiement, ces rôles peuvent être exécutés **tous ensemble sur un seul appareil (Standalone ISE)** ou être **répartis sur plusieurs appareils (Multi-Node ISE)** afin d'assurer la **redondance et la haute disponibilité**.

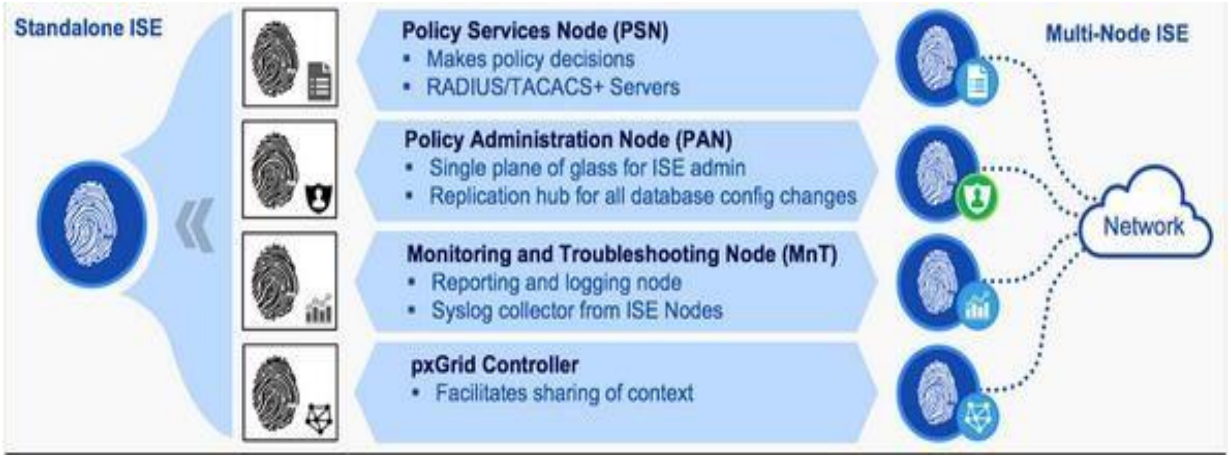


Figure (III -10) : Les différents types de personas sur Cisco ISE [40]

III.6.4 Composants de déploiement ISE :

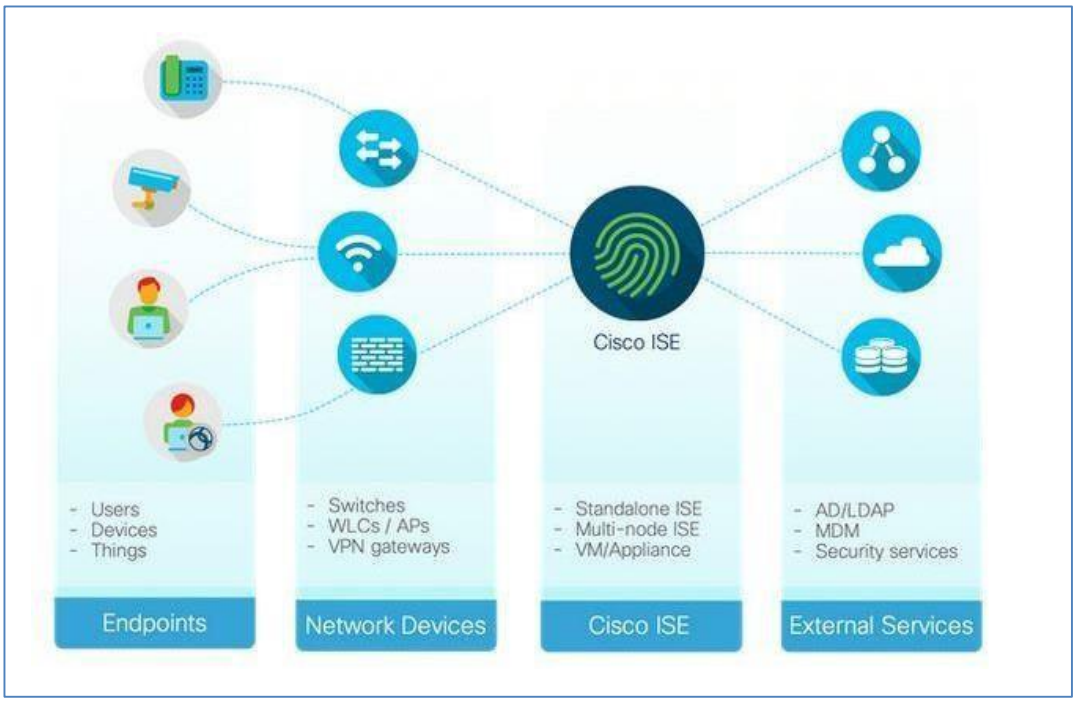


Figure (III -11) : Composants de la solution ISE [41]

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

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.

III.6.5 Méthodologies d'authentification :

III.6.5.1 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. [42]

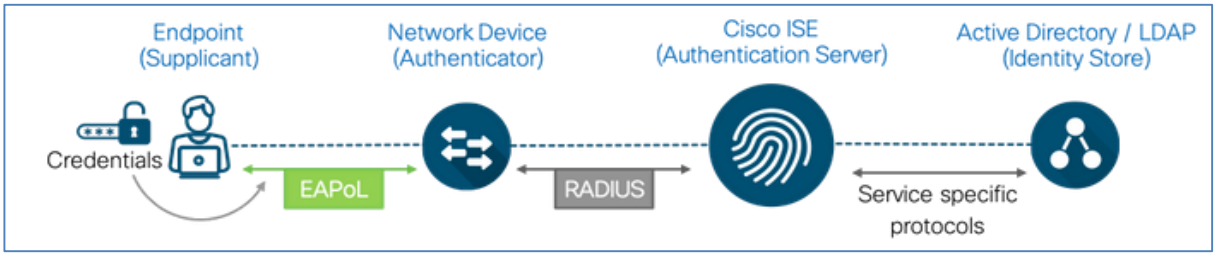


Figure (III -12) : 802.1x Authentification [41]

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.

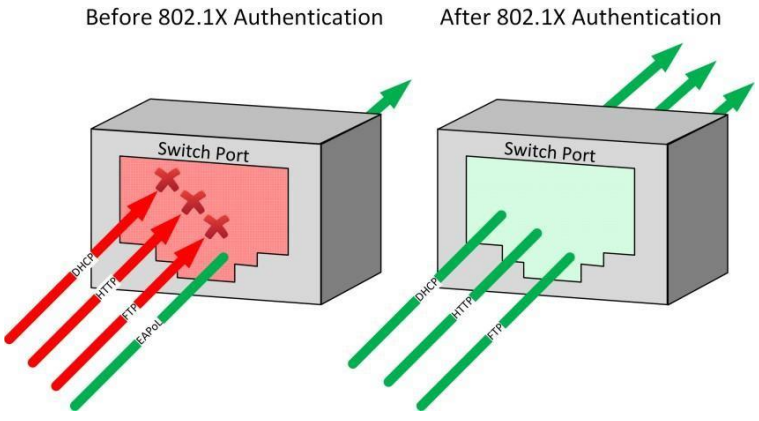


Figure (III -13) : Authentification 802.1x port de commutateur [41]

III.6.5.2 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.

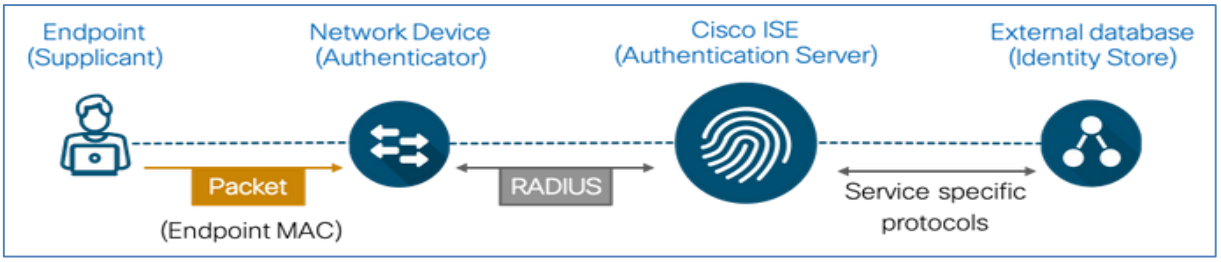


Figure (III -14) : MAB Authentification [41]

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. [42]

III.6.5.3 EasyConnect :

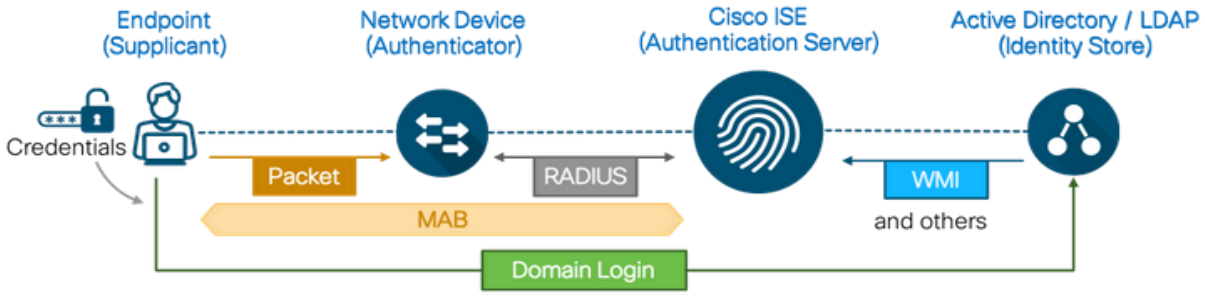


Figure (III -15) : EasyConnect Authentification [41]

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.

III.6.5.4 Une comparaison des différentes méthodes d'authentification :

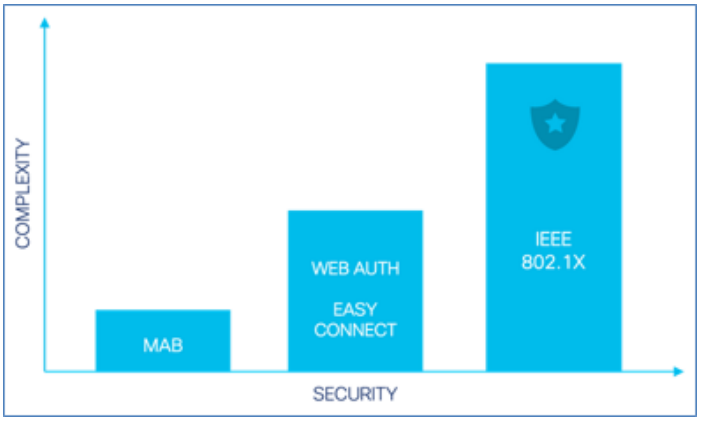


Figure (III -16) : Analyse de complexité des méthodes d'authentification [41]

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.[41]

III.6.6 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.

III.6.6.1 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.

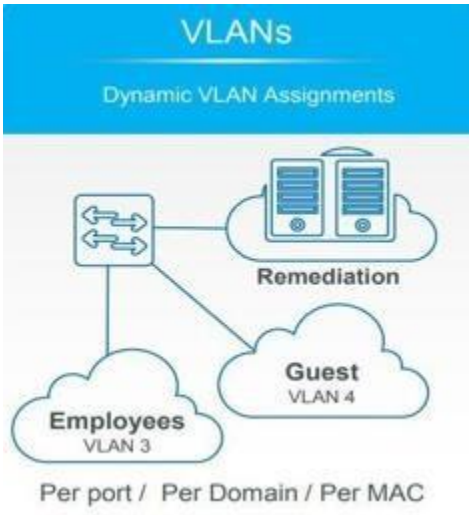


Figure (III -17) : Affectation dynamique de VLAN [41]

III.6.6.2 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).

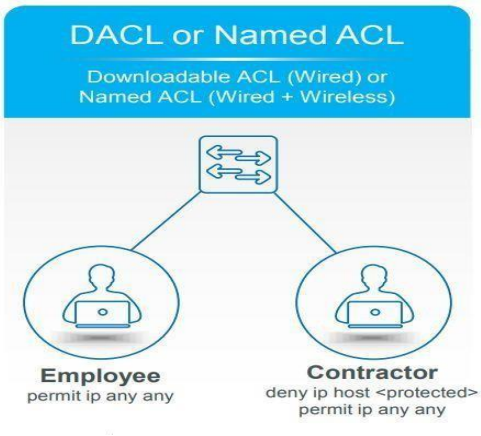


Figure (III -18) : Listes de contrôle d'accès [41.

III.6.6.3 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 ne 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.

III.6.6.4 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.

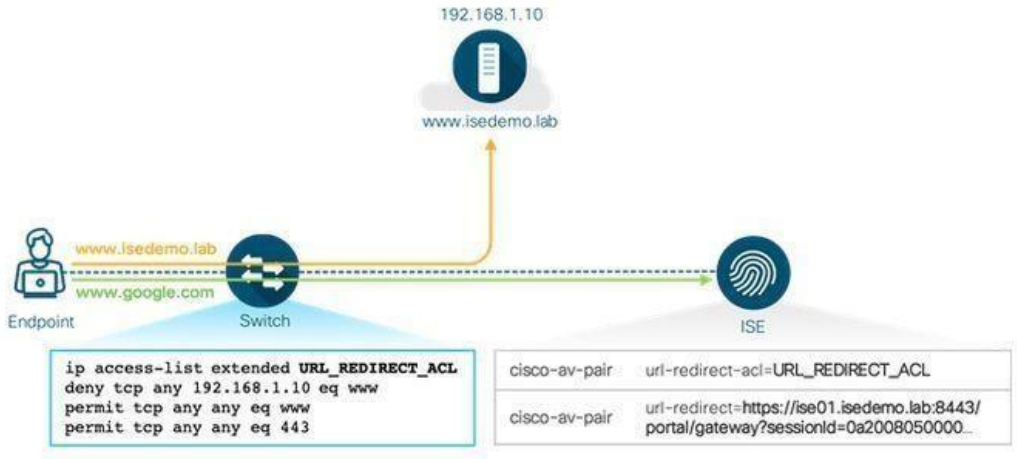


Figure (III -19) : Redirection d'URL [41]

III.6.7 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 d'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.[43]

III.6.8 Les cas d'utilisation de Cisco Identity Services Engine :

1. Access invité et accès sans fil sécurisé :

1.1.1 Le besoin d'un accès pour invité : [44]

De nombreuses organisations proposent un accès Internet gratuit à leurs visiteurs de courte durée (clients, fournisseurs, sous-traitants, etc.). Cisco ISE permet la création et l'authentification de comptes invités à des fins d'audit. Il propose trois types d'accès invité : hotspot (accès sans identifiants), auto-enregistrement, et accès sponsorisé. ISE offre aussi des API pour s'intégrer à d'autres systèmes (ex. : gestion des fournisseurs) afin de gérer les comptes invités. Les portails utilisateurs sont entièrement personnalisables pour refléter l'identité visuelle de l'organisation.

1.1.2 Le fonctionnement de l'accès invité :

ISE crée des comptes locaux pour les invités. Ces comptes peuvent être créés par un employé qui héberge l'invité (le parrain) à l'aide d'un portail intégré ou par l'invité lui-même en fournissant certaines informations de base. L'invité peut recevoir des identifiants par e-mail/SMS et les utiliser pour s'authentifier sur le réseau et ainsi obtenir un accès au réseau.
L'administrateur peut définir le niveau d'accès à accorder à ces utilisateurs. [44]

Figure (III -20) : Cas d'utilisation de Cisco ISE Guest [44]

1.2.1 Le besoin de sécurisé l'accès sans fil :

La sécurisation de l'accès sans fil constitue une priorité pour les organisations, car elle représente l'un des besoins fondamentaux en matière de sécurité réseau. Avec Cisco ISE, seuls les utilisateurs et équipements autorisés (BYOD ou appartenant à l'entreprise) peuvent accéder au réseau, conformément aux politiques établies. Chaque connexion débute par une phase d'authentification, active ou passive. L'authentification active repose sur le protocole 802.1x, tandis que l'authentification passive (Easy Connect) s'appuie sur des informations fournies par des sources d'identité comme Microsoft Active Directory. [44]

1.2.2 Le fonctionnement de l'accès sans fil sécurisé :

Une fois l'authentification réussie, ISE fournit, en fonction des informations du groupe, l'accès approprié à la connexion sans fil, qu'il s'agisse d'une session d'identité passive (Easy Connect), MAB (MAC Address Bypass) ou 802.1x. Pour ce faire, il suffit d'affecter l'utilisateur à un VLAN, DACL, ACL ou d'attribuer un SGT ou SGACL.

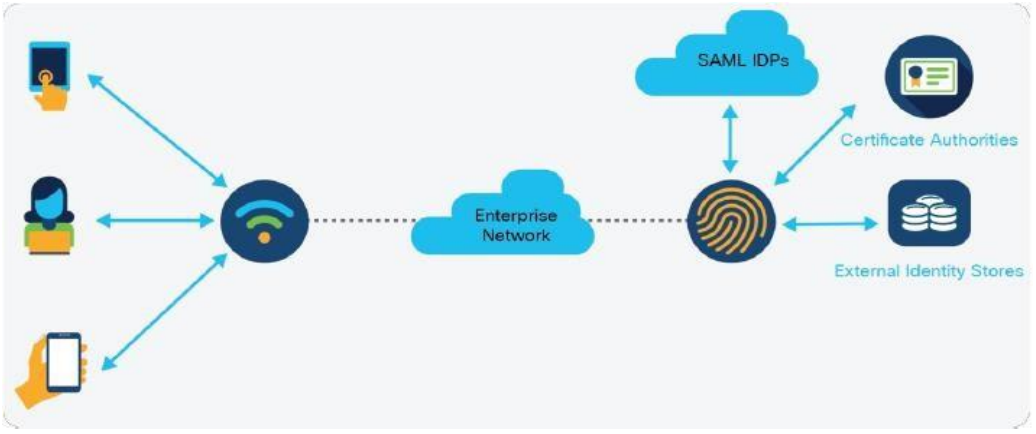


Figure (III -21) : Cas d'utilisation du sans-fil sécurisé Cisco ISE [44]

2. Accès filaire sécurisé

2.1 Le besoin d'un accès filaire sécurisé :

La sécurisation du réseau câblé est indispensable pour empêcher tout accès non autorisé. Avec Cisco ISE, l'authentification et l'autorisation des utilisateurs et des terminaux garantissent un accès contrôlé. L'authentification peut être active, via 802.1x et une source d'identité, ou passive, en s'appuyant sur Active Directory ou d'autres mécanismes. Après validation, l'autorisation s'applique par l'attribution de VLAN dynamiques, d'ACL téléchargeables ou d'autres méthodes de segmentation.[44]

2.2 Le fonctionnement d'un accès filaire sécurisé :

ISE authentifie les utilisateurs et les terminaux via 802.1X, l'authentification Web, MAB et d'autres moyens. ISE peut interroger des sources d'identité externes pour résoudre les identités et appliquer les politiques réseaux appropriés en donnant des instructions aux périphériques réseau. [44]

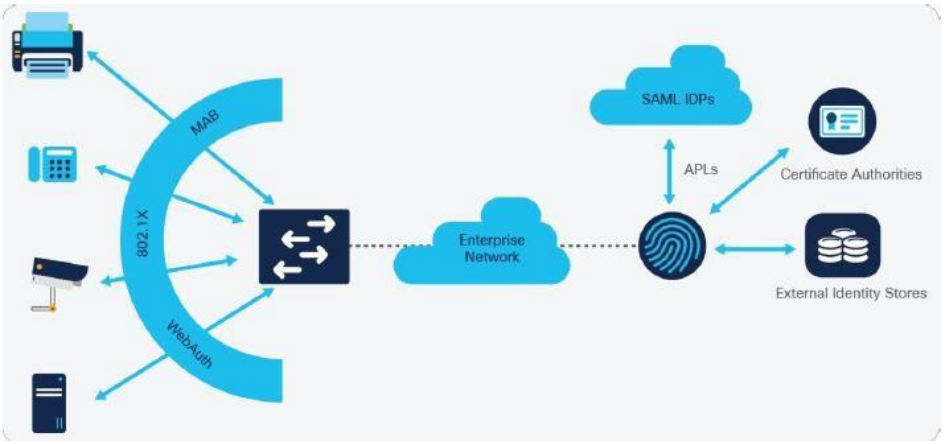


Figure (III -22) : Cas d'utilisation de l'accès filaire sécurisé Cisco ISE

3. Apportez votre propre appareil (BYOD)

3.1 Le besoin de BYOD :

De nombreuses organisations ont mis en place une politique qui permet 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. Cette politique est appelée « Bring Your Own Device » (BYOD, apportez votre propre appareil). Cependant, comme ces appareils appartiennent à des particuliers, ceux-ci n'apprécient pas d'installer des logiciels de gestion qui permettent aux organisations de « gérer » les terminaux. Dans de telles situations, ISE offre une méthode très simplifiée pour automatiser l'ensemble du processus d'intégration BYOD, de l'enregistrement des appareils à l'installation des certificats en passant par l'approvisionnement des suppliants.

Cela peut être fait sur des appareils fonctionnant sous différents systèmes d'exploitation tels qu'iOS, Android, Windows, macOS et ChromeOS. Le portail ISE My Devices, entièrement personnalisable, permet aux utilisateurs finaux d'intégrer et de gérer divers appareils. [44]

3.2 Le fonctionnement de BYOD :

Cisco ISE automatise l'intégration des terminaux BYOD grâce à plusieurs mécanismes, dont une autorité de certification intégrée qui génère et gère les certificats tout au long de leur cycle de vie. Un portail « Mes appareils » permet aux utilisateurs d'enregistrer leurs terminaux, de les déclarer perdus et de les placer en quarantaine. L'intégration peut se faire via un SSID unique, utilisé à la fois pour l'enrôlement et la connexion, ou via une approche à double SSID, distinguant un SSID ouvert pour l'intégration et un SSID sécurisé pour l'accès au réseau. Enfin, pour une gestion plus avancée, le processus BYOD peut être couplé à une solution MDM afin d'appliquer des politiques plus complètes. [44]

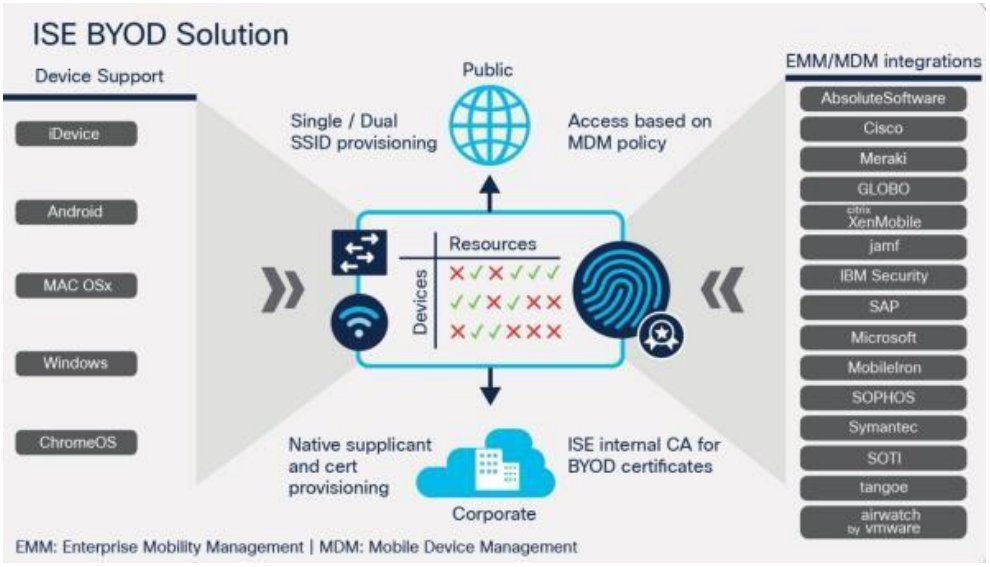


Figure (III -23) : Cas d'utilisation du BYOD avec Cisco ISE [44]

4. Conformité (posture)

4.1 Le besoin de la conformité (posture)

Les saboteurs se concentrent sur la corruption intentionnelle des données (ransomware) et l'exfiltration de données, ce qui compromet les terminaux d'un réseau. Les compromissions les plus efficaces et les plus médiatisées exploitent des problèmes connus qui pourraient être facilement résolus, mais qui ont été négligés. La visibilité de la conformité permetAux organisations de voir dans quelle mesure les terminaux des utilisateurs sont conformes à la politique de l'entreprise grâce à l'utilisation de Posture et/ou à l'intégration via des systèmes de gestion des appareils mobiles (MDM) et de gestion de la mobilité d'entreprise (EMM) (les systèmes MDM/EMM pris en charge sont disponibles ici). À l'aide du moteur Posture d'ISE ou d'un MDM, une organisation peut évaluer le nombre de terminaux conformes et s'assurer qu'aucun logiciel non conforme n'est installé et/ou exécuté. [44]

4.2 Le fonctionnement de la conformité

La fonctionnalité d**e** conformité (Posture) dans Cisco ISE permet de vérifier l'état des terminaux avant leur accès au réseau. Grâce à des agents temporaires ou installés, elle contrôle la présence et la mise à jour des correctifs systèmes, antivirus, pare-feu, etc. L'accès peut ensuite être différencié selon le niveau de conformité : les terminaux sûrs obtiennent un accès complet, tandis que ceux jugés non conformes sont restreints à des services limités ou de remédiation. Cette politique, basée sur le moteur Posture d'ISE ou intégrée à une solution MDM/EMM, réduit les risques en empêchant les appareils vulnérables ou obsolètes d'accéder aux ressources critiques.[44]

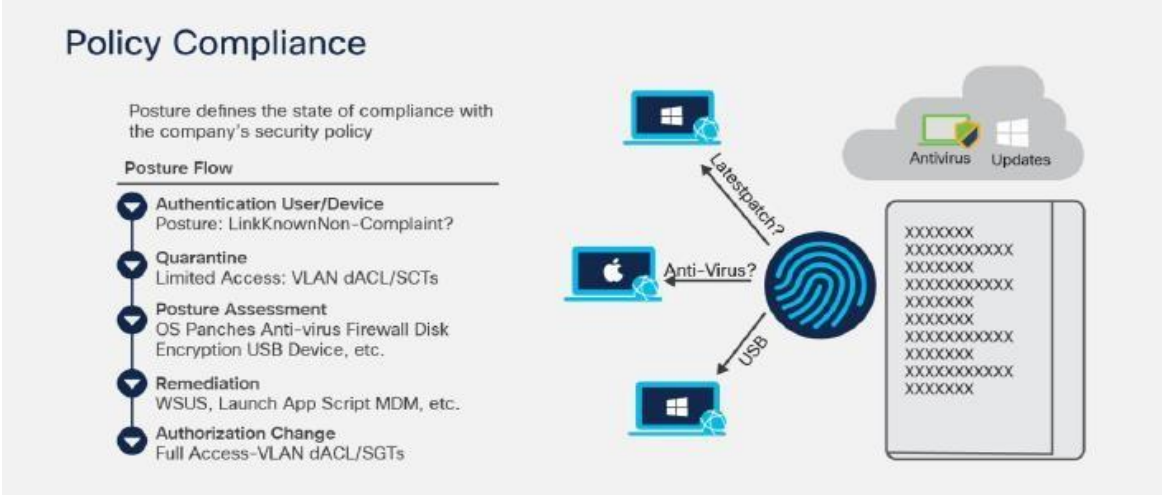


Figure (III -24) : Visibilité de la conformité Cisco ISE Cas d'utilisation. [44]

Conclusion

Dans ce chapitre, nous avons mis en évidence le principe de fonctionnement général d'une solution de Network Access Control (NAC)**,** en soulignant son rôle essentiel dans la sécurisation des infrastructures informatiques modernes. Nous avons ensuite porté une attention particulière à une solution spécifique largement adoptée dans le domaine, à savoir la plate-forme Cisco Identity Services Engine (ISE)**,** en exposant ses caractéristiques, ses mécanismes principaux ainsi que les avantages qu'elle offre en matière de visibilité, de contrôle et de conformité des terminaux. Cette étude théorique constitue une base solide pour comprendre la valeur ajoutée d'une telle technologie dans un contexte réseau d'entreprise.
Dans le chapitre suivant, nous passerons à l'aspect pratique de ce travail, qui consistera à déployer Cisco ISE au sein d'un réseau câblé. Cette étape nous permettra de vérifier expérimentalement les concepts abordés précédemment, d'évaluer les performances de la solution dans un environnement réel et d'atteindre les objectifs fixés en matière de contrôle d'accès et de conformité des équipements connectés.

Chapitre IV :

Mise en place de la solution de sécurité CISCO ISE

IV.1 Introduction :

Dans le cadre de ce laboratoire, nous avons mis en œuvre une solution d'authentification réseau basée sur le protocole IEEE 802.1X en utilisant le serveur Cisco Identity Services Engine (ISE). L'objectif est de renforcer la sécurité d'accès au réseau en permettant uniquement aux utilisateurs et périphériques autorisés de s'y connecter. Pour ce faire, nous avons configuré à la fois le switch d'accès et le serveur ISE afin d'assurer la gestion centralisée des identités, des droits d'accès et des politiques de sécurité.
Ce lab illustre ainsi le rôle essentiel du contrôle d'accès réseau (NAC) dans la protection des infrastructures d'entreprise.

IV.2 Environnement de travail et topologie du laboratoire NAC basé sur Cisco ISE :

IV.2.1. Environnement de travail :

Dans le cadre de ce laboratoire, nous avons mis en place un environnement de test permettant la mise en œuvre d'une solution de Network Access Control (NAC) basée sur le protocole 802.1X et le serveur Cisco Identity Services Engine (ISE). Cet environnement regroupe l'ensemble des équipements matériels et logiciels nécessaires à la réalisation des scénarios de configuration et de validation.

IV.2.1.1 Prérequis matériels :

- Serveur ISE (installé en machine virtuelle) : 4 cœurs CPU, 8 Go RAM, 200 Go disque, 1 interface réseau.
- Switch Cisco Catalyst 3560 : compatible AAA et 802.1X.
- Postes clients (Sales-PC et Admin-PC) : Windows 10, carte Ethernet compatible 802.1X, 8 Go RAM
- Routeur/Passerelle : assure le routage et la connectivité Internet

IV.2.1.2 Prérequis logiciels :

- Cisco Identity Services Engine (ISE) : version 2.7.
- Cisco IOS : image logicielle supportant AAA, RADIUS et 802.1X.
- Supplicant 802.1X intégré à Windows 10.
- Navigateur Web (Chrome/Firefox/Edge) pour l'accès à l'interface ISE.
- Outil d'administration SecureCRT pour la configuration du switch.

IV.2.2 Topologie du laboratoire :

La topologie mise en place pour ce laboratoire se compose des éléments suivants :

- Un serveur Cisco ISE (10.1.5.19) jouant le rôle de serveur RADIUS central.
- Un switch Cisco Catalyst 3560 (10.1.5.11) configuré comme authentificateur 802.1X.
- Un poste client « Sales-PC » connecté sur le port FastEthernet0/2 du switch et s'authentifiant via 802.1X.
- Un poste « Admin-PC » pour l'administration et la supervision du serveur ISE.
- Un VLAN 10 configuré dynamiquement et attribué par l'ISE aux utilisateurs authentifiés.

Cette architecture permet de simuler un scénario typique d'entreprise où l'accès au réseau est contrôlé par des politiques centralisées de sécurité.

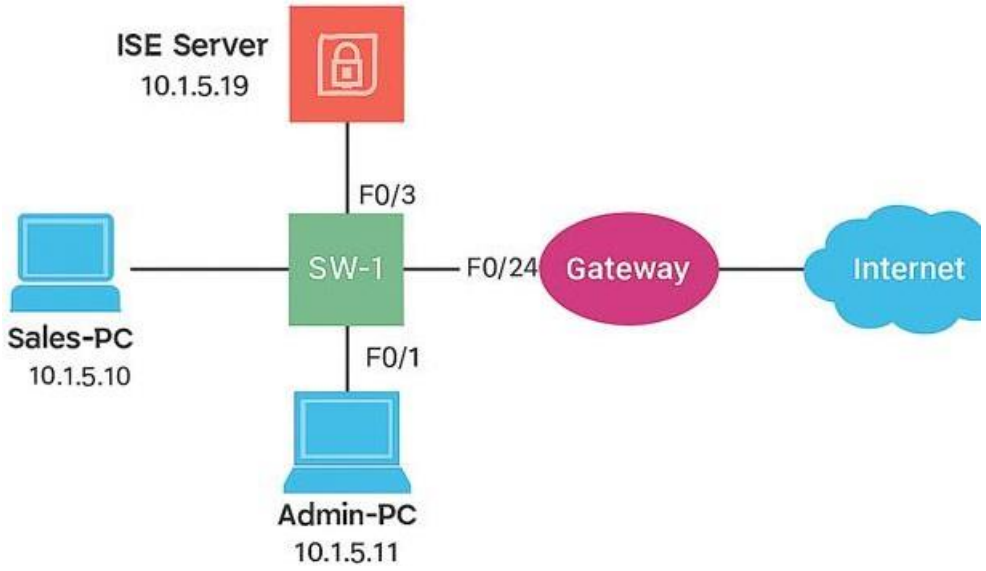


Figure (IV -1) : Topologie du lab

IV.3 L'implémentation de la solution ;

Configuration du 8021x au niveau du switch et du serveur ISE.

IV.3.1 Configuration au niveau de switch :

Dans cette section, nous présentons la configuration du protocole 802.1X sur le switch d'accès, élément essentiel de l'architecture NAC mise en place. L'objectif de cette configuration est de permettre au switch de jouer le rôle d'authenticator, en interagissant avec le serveur Cisco ISE (Authentication Server) via le protocole RADIUS, afin de contrôler l'accès des utilisateurs au réseau.

Les étapes de configuration consistent principalement à :

1. Activer le modèle AAA sur le switch,
2. Définir l'authentification, l'autorisation et l'accounting via RADIUS,
3. Établir la communication sécurisée avec le serveur ISE,
4. Activer 802.1X sur le switch et sur les interfaces concernées,
5. Associer les utilisateurs authentifiés à un VLAN spécifique,
6. Et enfin sauvegarder la configuration pour garantir sa persistance.

IV.3.1.1 Activer les fonctions AAA et 802.1X :

1. Active le modèle AAA (Authentication, Authorization, Accounting) sur le switch afin de permettre une gestion centralisée des accès.

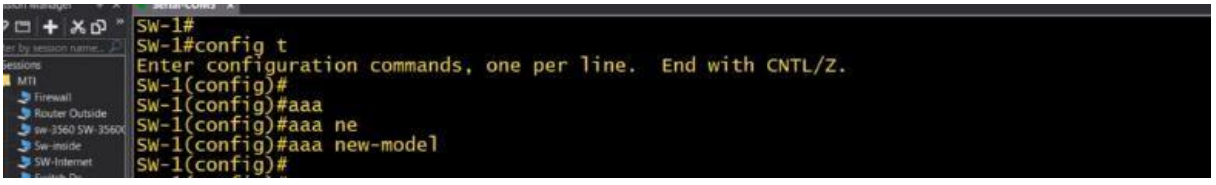


Figure (IV -2) : Activer AAA dans le switch

2. Configure l'authentification 802.1X en utilisant le serveur RADIUS (Cisco ISE).

Figure (IV -3) : Configure l'authentification 802.1X

3. Active l'autorisation via le serveur RADIUS, qui définit les droits d'accès après authentification.

Figure (IV -4) : Active l'autorisation via le serveur RADIUS

4. Active l'accounting afin de journaliser les connexions (début et fin de session) sur le serveur ISE.

Figure (IV -5) : Active l'accounting

5. Déclare le serveur RADIUS sous le nom ISE-RAD et Spécifie l'adresse IP du serveur Cisco ISE (10.1.5.19).
Ensuite définie la clé partagée entre le switch et le serveur RADIUS pour sécuriser les échanges.

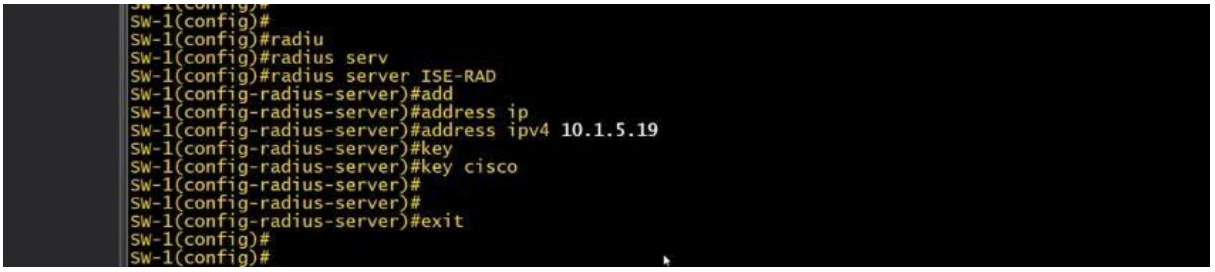


Figure (IV -6) : Attribuer un nom au servuer et une adresse IP et une clé

6. Active globalement le protocole 802.1X sur le switch.
Accède à l'interface FastEthernet 0/2 pour appliquer la configuration 802.1X.
Configure le port pour exiger une authentification avant d'autoriser le trafic.
Définit le switch comme authenticator dans le processus 802.1X.

Figure (IV -7) : Active globalement le protocole 802.1X sur le switch.

7. Assigne les utilisateurs authentifiés au VLAN 10

Figure (IV -8) : Assigne les utilisateurs authentifiés au VLAN 10

8. Active le suivi des périphériques connectés afin d'améliorer la visibilité et la sécurité.
Et on quitte le mode configuration et on revient en mode d'exécution.

Figure (IV -9) : Activer le suivi des périphériques connectés

9. On active le device tracking qui permet l'envoi d'attributs spécifiques (VSA) vers le serveur ISE pour appliquer des politiques avancées.
Et en fin on sauvegarde la configuration dans la mémoire NVRAM pour la rendre persistante après un redémarrage.

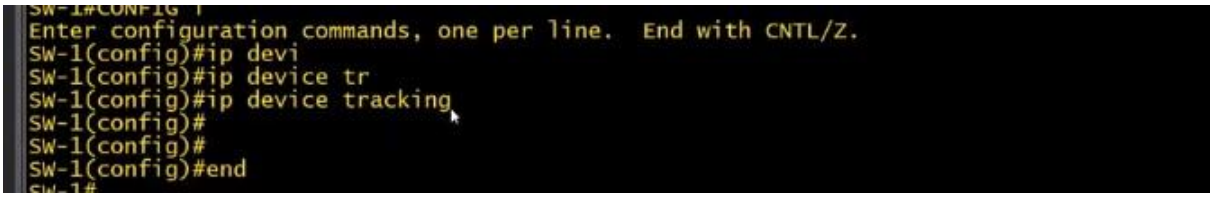


Figure (IV -10) : Activer le device tracking

IV.3.2 Configuration au serveur ISE :

Étapes de configuration du serveur ISE :

1. **Accéder à l'interface d'administration du serveur ISE la création d'un Device Type**

2. Ajouter le switch comme périphérique réseau (Network Device).

3. Créer les groupes d'utilisateurs

4. Créer un utilisateur et l'associer à un groupe

5. La définition des politiques d'autorisation et définir un Policy Set pour l'authentification 802.1X filaire

6. Configurer la règle d'autorisation associée

7. Sauvegarder la configuration du serveur ISE

IV.3.2.1 Accéder à l'interface d'administration du serveur ISE :

Pour administrer Cisco ISE, on utilise une interface graphique Web accessible via un navigateur. Dans notre cas, le serveur ISE est configuré avec l'adresse IP 10.5.10.19, l'accès se fait en HTTPS, ce qui garantit la confidentialité des échanges entre l'administrateur et le serveur.

URL utilisée : https://10.5.10.19

Après avoir saisi cette adresse dans le navigateur, une fenêtre d'authentification s'affiche. L'administrateur entre alors son nom d'utilisateur et son mot de passe afin d'accéder à la console d'administration ISE.

L'accès sécurisé à l'interface graphique de Cisco ISE via HTTPS est une étape fondamentale, car il permet à l'administrateur de configurer et de superviser les politiques de contrôle d'accès réseau de manière centralisée.
L'authentification garantit que seuls les administrateurs autorisés peuvent effectuer des modifications, renforçant ainsi la sécurité et la traçabilité de la solution NAC,

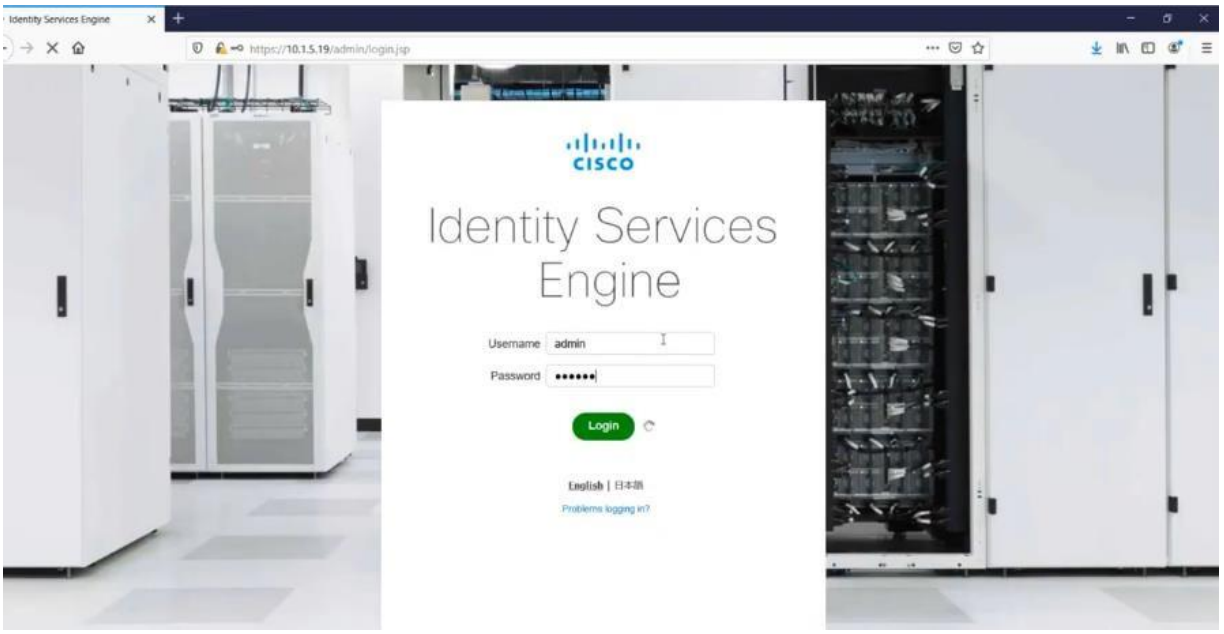


Figure (IV -11) : Interface de l'ISE

IV.3.2.1.1 La création d'un Device Type :

Après connexion à l'interface graphique de Cisco ISE, il est nécessaire de définir les Device Types afin de classer les équipements réseau par catégories Pour cela, l'administrateur suit le chemin suivant dans la console ISE Administration > Network Resources > Network Device Groups > Device Type

Une fois dans la section dédiée, un nouveau sous-groupe a été créé sous la catégorie par défaut All Device Types. Nous avons ajouté le type Wired, qui correspond aux équipements filaires (par exemple les switches). Enfin, la configuration a été sauvegardée à l'aide du bouton Save.
La création d'un Device Type est une étape de préparation organisationnelle. Elle n'est pas obligatoire pour le fonctionnement de 802.1X, mais elle représente une bonne pratique d'administration. Elle permet de regrouper les équipements selon leur nature (filaire, sans fil, VPN, etc.), de faciliter la gestion et la maintenance de la solution NAC et de rendre la configuration plus claire et scalable dans le cas de déploiements de grande envergure.

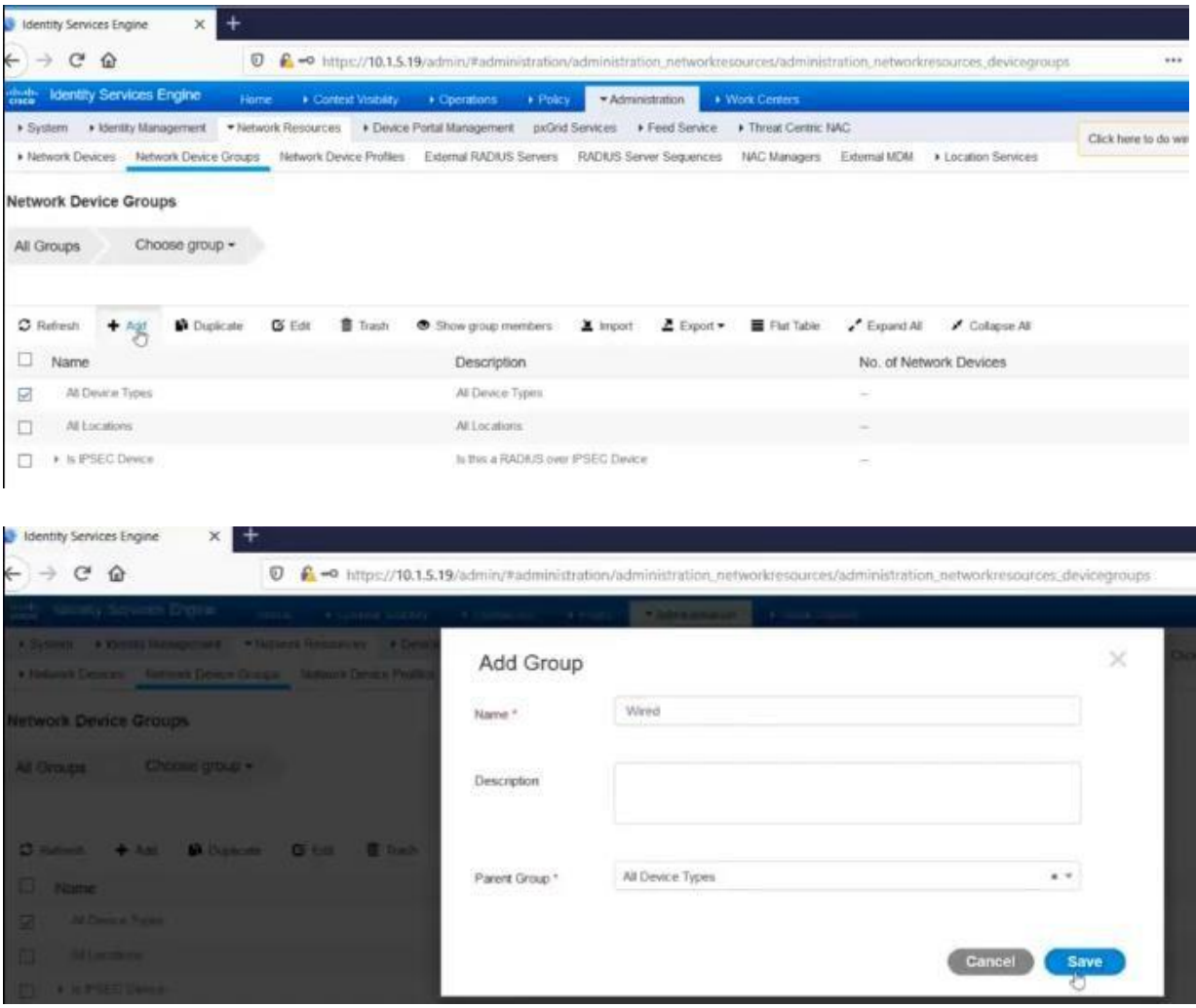


Figure (IV -11) : La création d'un device type

IV.3.2.2 Ajout du Switch dans Cisco ISE comme Network Device :

Après avoir créé le Device Type Wired, l'étape suivante consiste à ajouter le switch comme Network Device afin qu'il soit reconnu par le serveur ISE et puisse échanger des requêtes d'authentification via le protocole RADIUS.
Pour cela, l'administrateur suit le chemin suivant dans la console ISE :

☞ Administration → Network Resources → Network Devices

Dans le formulaire d'ajout, les informations suivantes ont été saisies :

- Name : SW-1 (nom logique attribué au switch)
- IP Address : 10.1.5.11 (adresse de gestion du switch)
- RADIUS Authentication Settings : activé, avec la clé partagée (Shared secret) 'cisco' identique à celle configurée préalablement sur le switch.
- Device Type : Wired (catégorie créée précédemment).

La configuration est validée en cliquant sur Save.

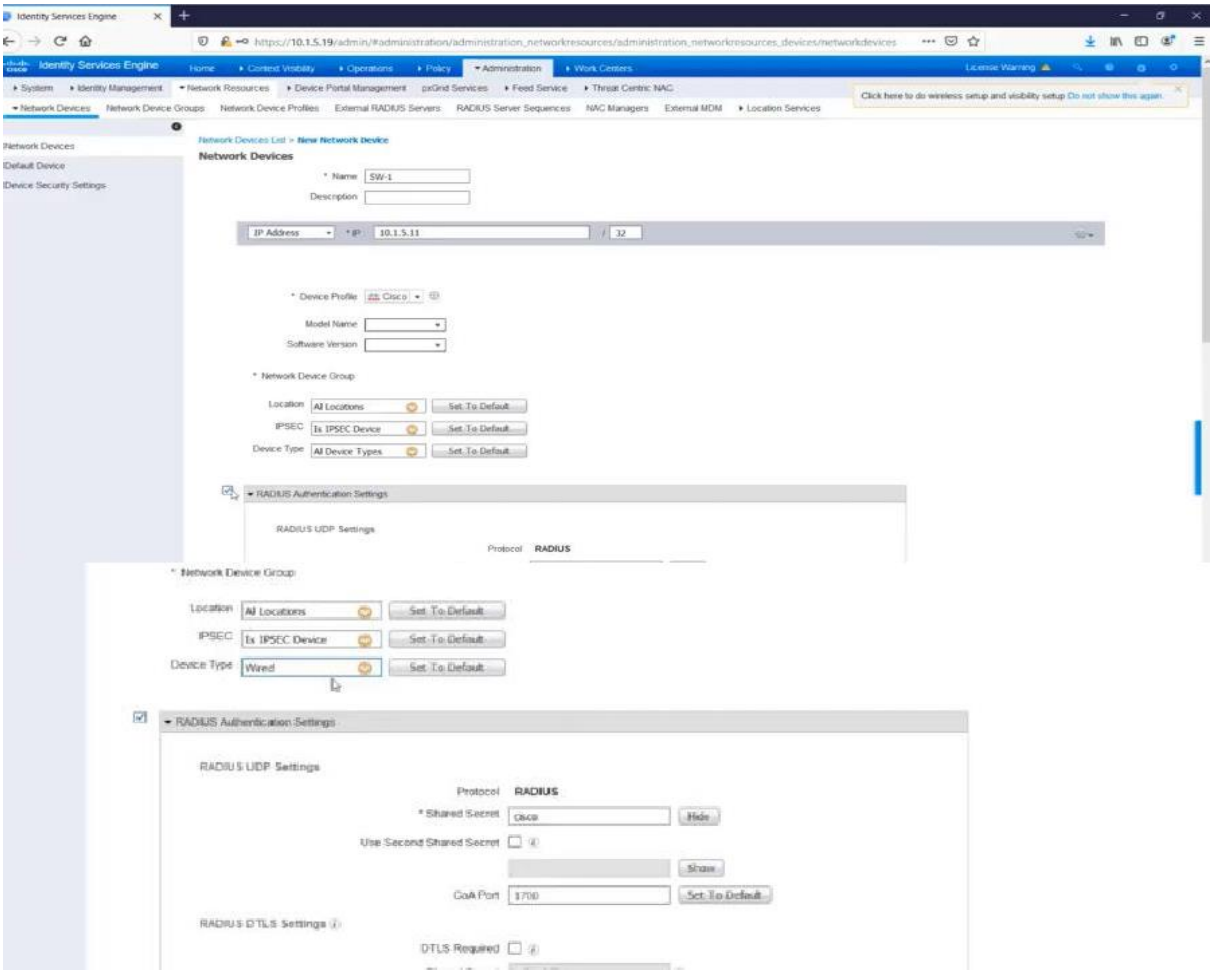


Figure (IV -12) : Ajout du Switch dans Cisco ISE comme Network Device

L'ajout du switch en tant que Network Device permet à Cisco ISE de l'identifier comme client RADIUS autorisé à soumettre des requêtes d'authentification.
L'utilisation d'une clé partagée (Shared secret) garantit la sécurité des échanges entre le switch et l'ISE, évitant qu'un équipement non autorisé puisse se faire passer pour un authenticator.

De plus, l'association du switch au Device Type Wired assure une organisation claire des ressources réseau et facilite l'application des politiques d'accès.

IV.3.2.3. Création d'un groupe d'utilisateurs dans Cisco ISE :

Dans un premier temps, il est nécessaire de définir des groupes d'utilisateurs afin de regrouper les identités selon des critères organisationnels (par exemple, département, rôle, fonction).

Pour ce faire, l'administrateur suit le chemin :

☞ Administration > Groups > User ldentity > Groups > Add

Un groupe nommé Sales a été créé puis enregistré (Submit). Ce groupe représentera l'ensemble des utilisateurs du service commercial.

IV.3.2.4 Création d'un utilisateur et association à un groupe :

Ensuite, un utilisateur a été créé dans la base interne d'ISE :

☞ Administration > Identities > Users > Add > Network Access User

Les paramètres saisis sont :

- Nom d'utilisateur (Username) : jdoe
- Mot de passe : cisco123
- User Groups : Sales

L'utilisateur a ensuite été validé via le bouton Submit.

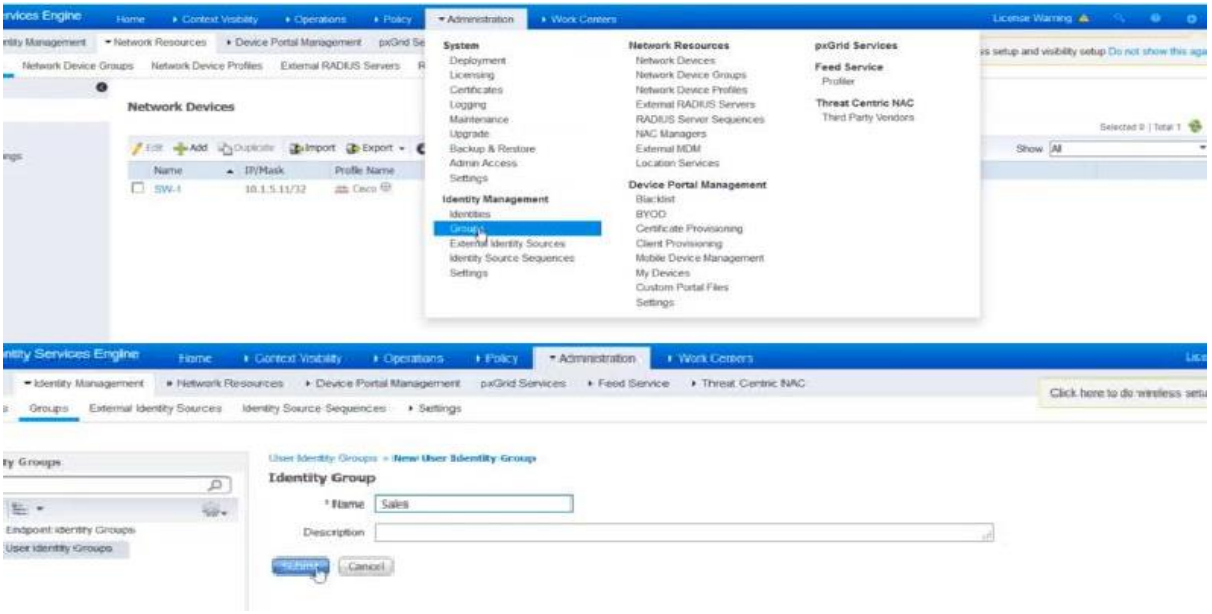


Figure (IV -13) : Création d'un groupe d'utilisateurs

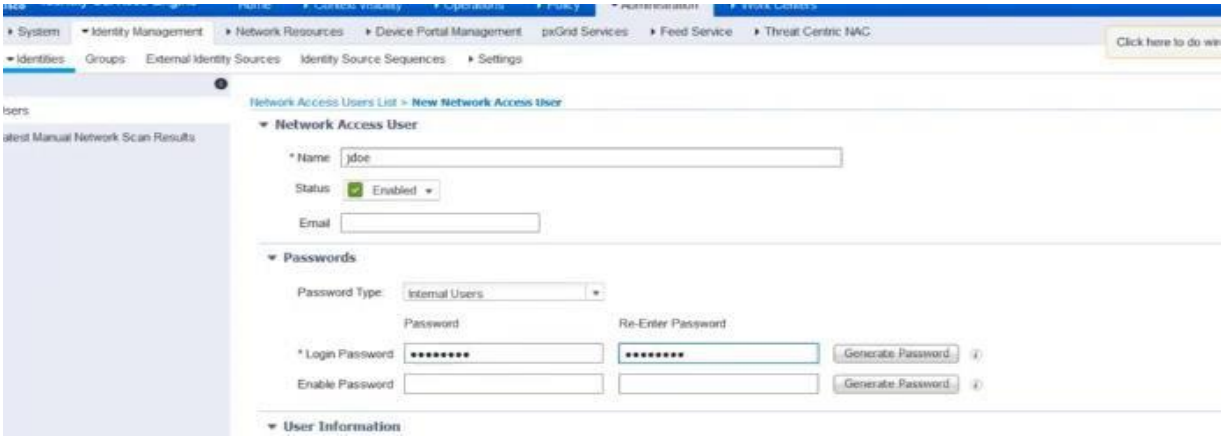


Figure (IV -14) : Création d'un utilisateur et association à un groupe

La gestion des identités dans Cisco ISE constitue le socle de la solution NAC.
La création de groupes d'utilisateurs permet d'appliquer des politiques d'accès différenciées selon les départements ou profils (ex : ventes, IT, invités).

L'ajout d'utilisateurs dans la base interne d'ISE facilite les tests en laboratoire, même si en environnement de production, l'intégration avec un Active Directory ou une base LDAP est généralement privilégiée.

Ainsi, l'utilisateur jdoe, membre du groupe Sales, pourra être authentifié par le serveur ISE lors de sa connexion au réseau, et les politiques associées à son groupe lui seront appliquées automatiquement.

IV.3.2.5 La définition des politiques d'autorisation et définir un Policy Set pour l'authentification 802.1X filaire :

IV.3.2.5.1 La définition des politiques d'autorisation :

La définition des politiques d'autorisation dans Cisco ISE se fait en deux parties :

1. Créer une ACL téléchargeable (DACL) pour définir les ressources auxquelles un utilisateur ou groupe peut accéder.

2. Créer un profil d'autorisation qui combine Différents attributs (ex. VLAN + ACL) et qui sera appliqué aux utilisateurs authentifiés.

IV.3.2.5.1.1 Création d'une ACL téléchargeable (Downloadable ACL - DACL) :

Avant de configurer les politiques d'autorisation, il est nécessaire de définir une Downloadable ACL (DACL), qui précise les ressources accessibles par un utilisateur ou un groupe d'utilisateurs.

Pour cela, l'administrateur suit le chemin :

☞ Policy > Results > Authorization > Downloadable ACLS > Add

Les paramètres configurés sont :

- Name : sales-ACL
- Type : IPv4
- DACL Content : permit tcp any any eq 80
  Permit tcp any any eq 443
  Deny ip any any

Cette ACL permet aux utilisateurs du groupe Sales d'accéder uniquement aux services Web (HTTP et HTTPS), tout autre trafic étant refusé.
Enfin, la configuration est sauvegardée via Save.

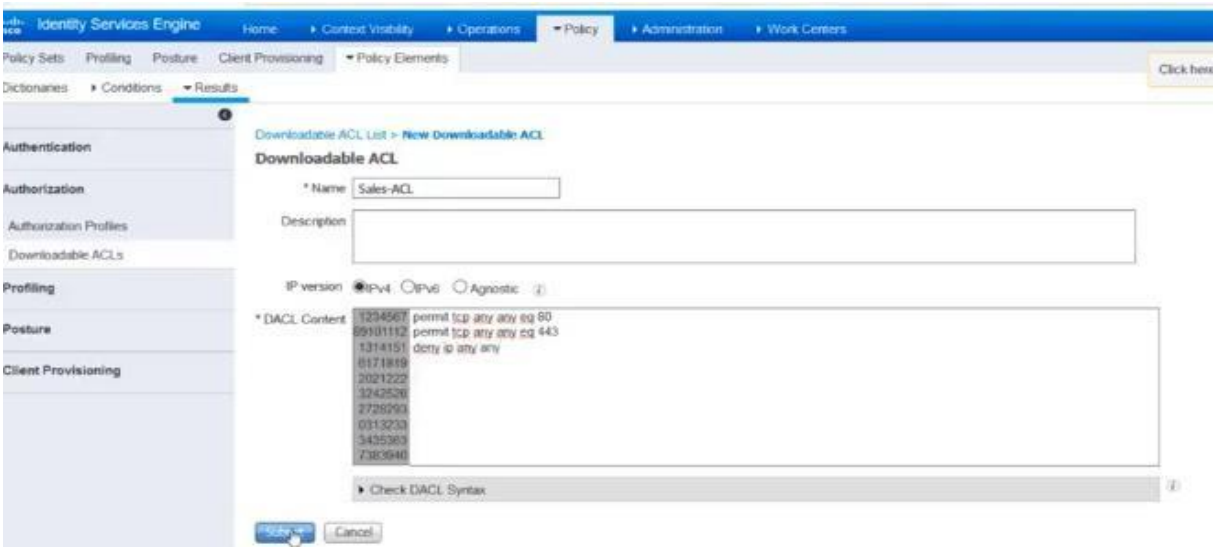


Figure (IV -15) : Création d'une ACL téléchargeable (Downloadable ACL - DACL)

IV.3.2.5.1.2 Création d'un Profil d'Autorisation :

Une fois la DACL définie, il est possible de créer un profil d'autorisation qui regroupe plusieurs attributs d"accès. Ce profil sera ensuite appliqué lors de l'authentification réussie d'un utilisateur.

Chemin de configuration :

☞ Policy > Results > Authorization > Authorization Profiles > Add

Les paramètres configurés sont :

- Name : sales-profile
- Access Type : ACCESS_ACCEPT
- Common Tasks : DACL Name : sales-ACL
  VLAN ID/Name : 10

Enfin, le profil est enregistré via Submit.

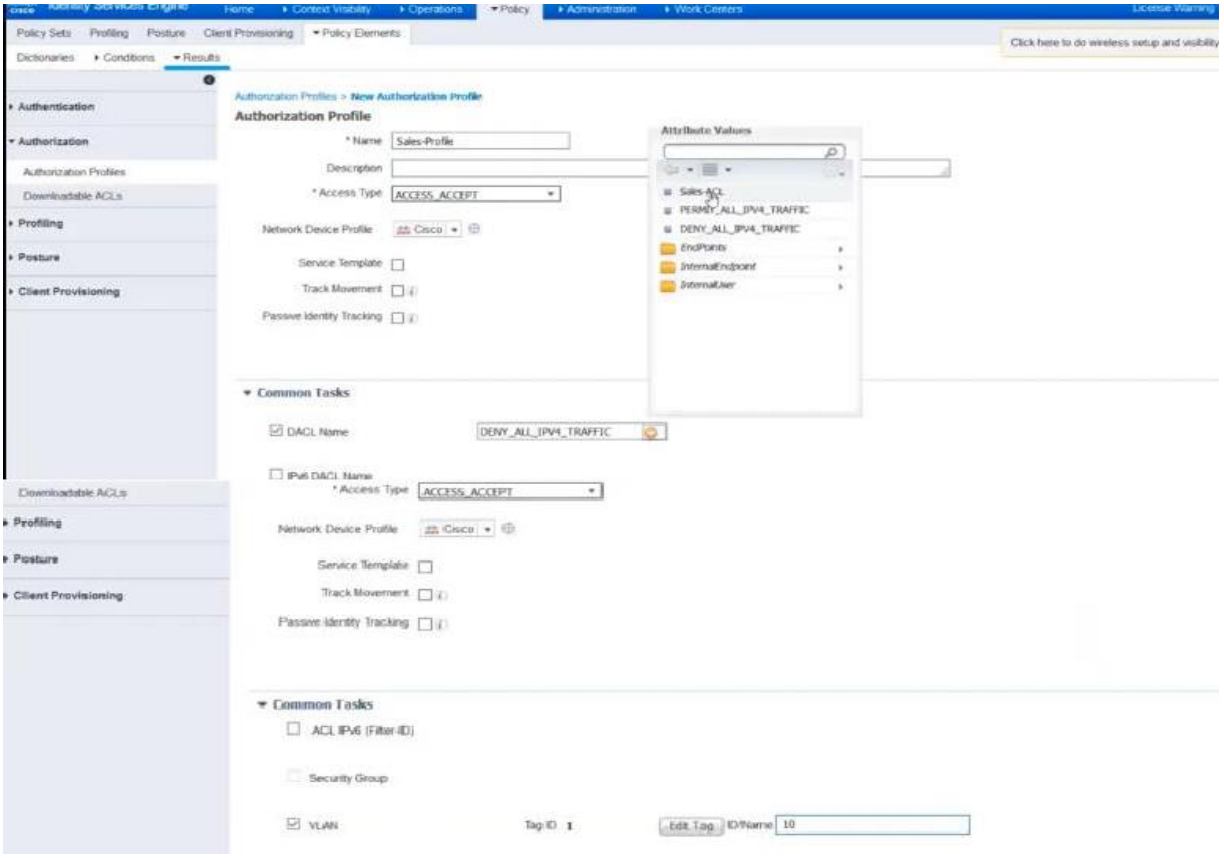


Figure (IV -15) : Création d'un Profil d'Autorisation

La définition d'une ACL téléchargeable (DACL) et d'un profil d'autorisation constitue une étape essentielle dans la mise en œuvre d'une solution NAC basée sur ISE.

La DACL permet d'appliquer des règles de contrôle d'accès spécifiques et dynamiques, adaptées aux utilisateurs ou groupes. Contrairement à une ACL classique configurée sur le switch, la DACL est centralisée et téléchargée automatiquement par l'ISE lors de l'authentification.
Le profil d'autorisation associe différents attributs réseau (VLAN, ACL, QoS, etc.) pour offrir une granularité fine dans la gestion des accès.

Dans notre cas, le groupe Sales est automatiquement placé dans le VLAN 10 et bénéficie uniquement d'un accès restreint aux services Web (HTTP/HTTPS). Cette approche illustre la capacité d'ISE à appliquer des politiques basées sur l'identité et le rôle de l'utilisateur, garantissant un haut niveau de sécurité et de flexibilité.

IV.3.2.5.2 Création d'un Policy Set pour l'authentification 802.1X filaire :

Dans Cisco ISE, un Policy Set regroupe les règles d'authentification et d'autorisation correspondant à un scénario précis (802.1X, MAB, VPN, etc.).
Pour notre laboratoire, nous avons créé un Policy Set dédié au réseau filaire (802.1X Wired).
Étapes de configuration :

1. Accéder au menu : Policy → Policy Sets

2. Cliquer sur Add pour ajouter un nouveau Policy Set.

3. Renommer l'entrée par défaut New Policy Set 1 en :

Wired-policy-set

4. Définir la condition d'application du Policy Set :

- Ouvrir Condition Studio → Editor
- Choisir : Network Device → Device Type → All Device Types#Wired
- Cliquer sur Use pour appliquer la condition.

5. Laisser le Default Network Access comme règle d'accès par défaut.

6. Sauvegarder la configuration via Save.

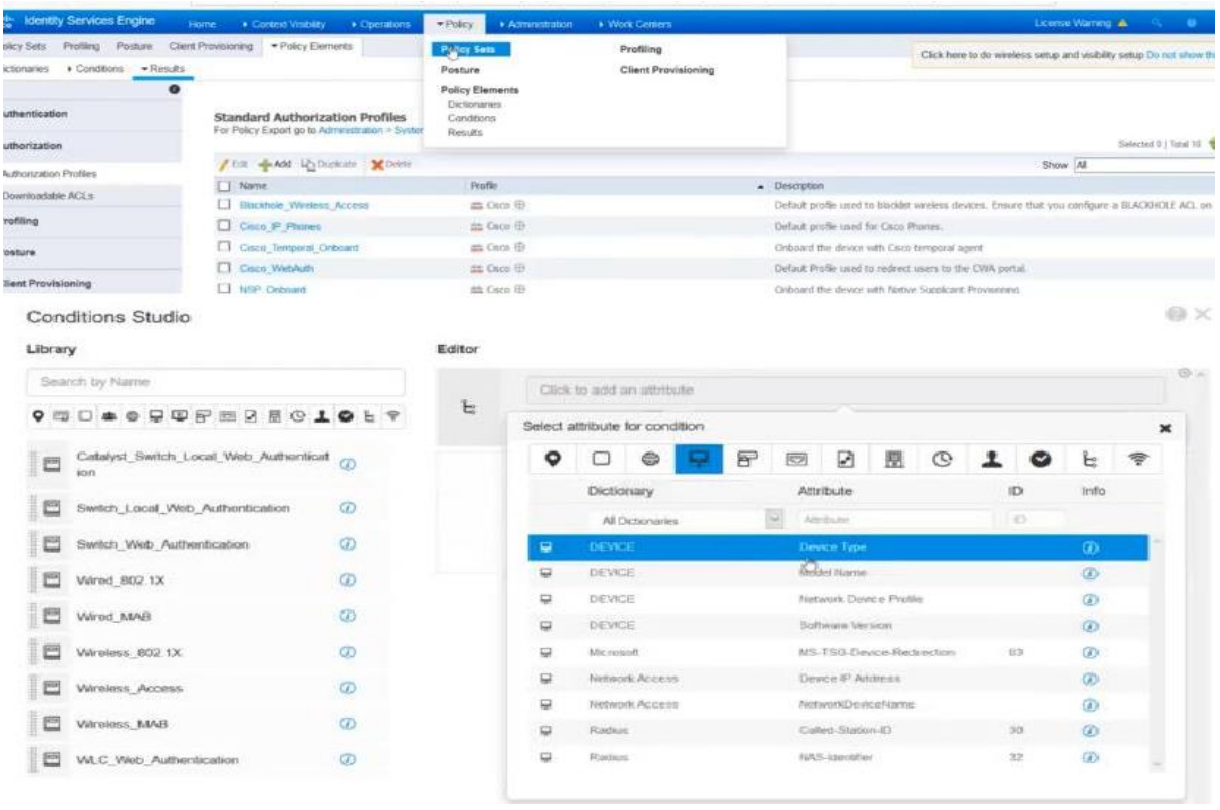


Figure (IV -16) : Création d'un Policy Set pour l'authentification 802.1X filaire

La création d'un Policy Set dédié au réseau filaire 802.1X (Wired-policy-set) permet de regrouper toutes les règles d'authentification et d'autorisation qui concernent les utilisateurs connectés via un switch configuré en authenticator.
L'utilisation de la condition Device Type = Wired garantit que ce Policy Set s'applique uniquement aux équipements classés dans cette catégorie, ce qui offre une meilleure segmentation des règles et une gestion plus souple dans des environnements complexes (par exemple, distinction entre réseau filaire, Wi-Fi, ou VPN).

Le Policy Set agit comme un conteneur logique : il définit d'abord les méthodes d'authentification acceptées, puis applique les politiques d'autorisation en fonction de l'identité ou du groupe de l'utilisateur.

IV.3.2.6. Configuration des Authentication et Authorization Policy :

Une fois le Policy Set Wired-policy-set créé, il est nécessaire de définir les politiques d'authentification et d'autorisation qui vont s'appliquer aux requêtes RADIUS envoyées par le switch.

IV.3.2.6.1 Authentication Policy :

Par défaut, un Policy Set contient une règle d'authentification et une règle d'autorisation dites catch all (génériques). Ces règles sont utilisées si aucune autre condition n'est remplie.

Dans notre cas, nous avons créé une nouvelle Authentication Policy appelée dot1x.

• Condition :

 Dans Condition Studio → Library, l'administrateur sélectionne l'option Wired_802.1X, qui contient deux attributs :

- La requête RADIUS doit provenir d'un équipement Wired.
- Le protocole d'authentification est 802.1X (et non MAB).

• Base d'authentification :

☞ L'ISE est configuré pour authentifier l'utilisateur via sa base locale (Internal Users).

Ainsi, chaque fois qu'une requête RADIUS 802.1X est reçue, l'ISE consulte sa base interne d'utilisateurs pour valider les identifiants.

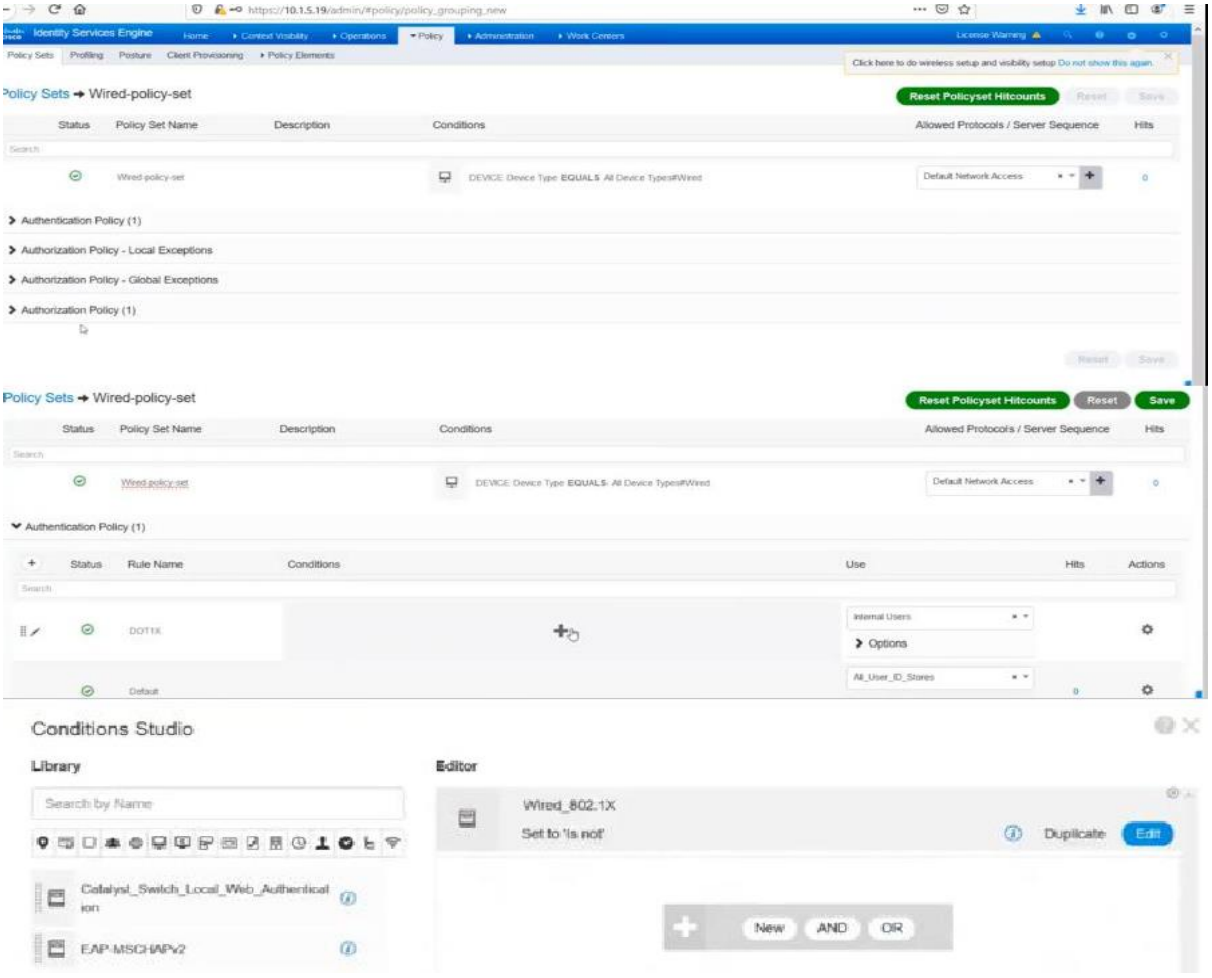


Figure (IV -17) : Configuration des policy d'authentification

IV.3.2.6.2 Authorization Policy :

Après l'authentification, une Authorization Policy est appliquée afin de définir le niveau d'accès attribué à l'utilisateur.

Nous avons créé une nouvelle règle appelée sales.

• Condition :

☞ Dans Condition Studio → Editor, nous avons choisi :

Identity Group → User Identity Groups : sales

Cela signifie que seuls les utilisateurs appartenant au groupe Sales sont concernés.

• Profil d'autorisation appliqué :

☞ Le profil sales-profile (précédemment créé) est associé à cette règle.
Ce profil contient :

- La DACL sales-ACL (permet accès HTTP/HTTPS uniquement).
- L'attribution au VLAN 10.

Enfin, la règle est sauvegardée via Save.

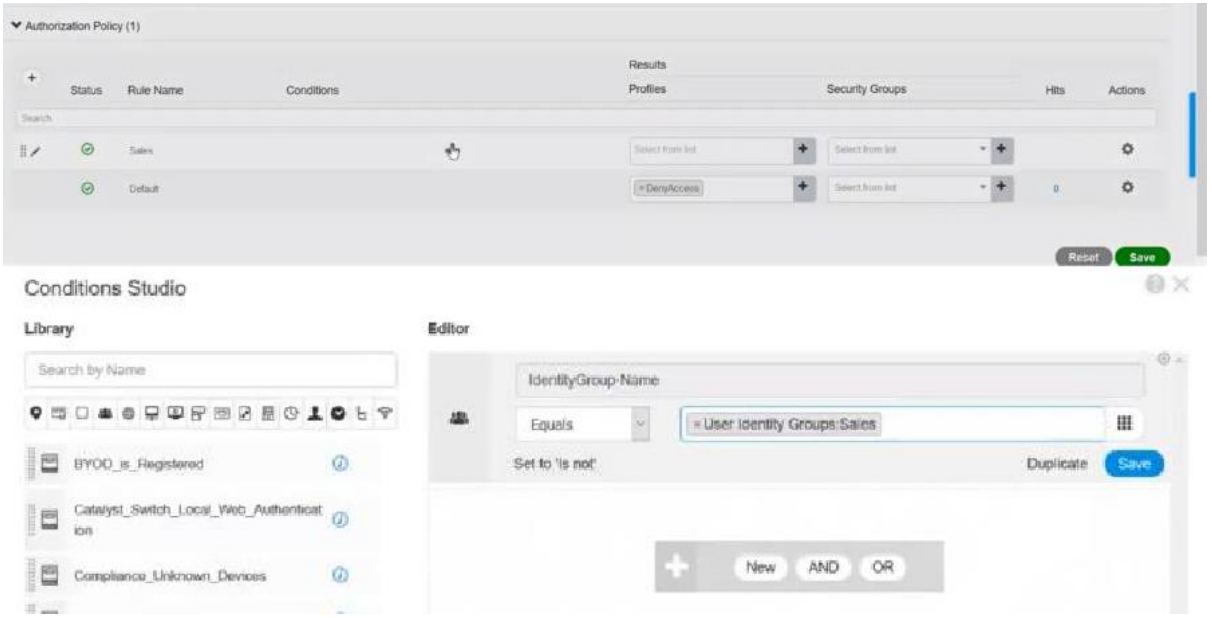


Figure (IV -18) : Configuration des policy d'authorization

La combinaison des Authentication Policies et Authorization Policies dans un Policy Set illustre le rôle central de Cisco ISE dans une solution NAC :
L'Authentication Policy vérifie l'identité de l'utilisateur (ici via la base interne).

L'Authorization Policy détermine les privilèges d'accès en fonction de l'appartenance à un groupe et applique dynamiquement un profil d'autorisation (VLAN, ACL, QoS, etc.).
Dans notre configuration, un utilisateur du groupe Sales (ex. jdoe) qui s'authentifie avec succès via 802.1X sera automatiquement placé dans le VLAN 10 et verra ses accès restreints aux services Web grâce à la DACL sales-ACL.

Cette approche montre la puissance d'ISE pour mettre en œuvre un contrôle d'accès granulaire, basé sur l'identité et le rôle, garantissant ainsi sécurité et flexibilité au sein du réseau d'entreprise.

IV.3.2.7. Sauvegarder la configuration du serveur ISE :

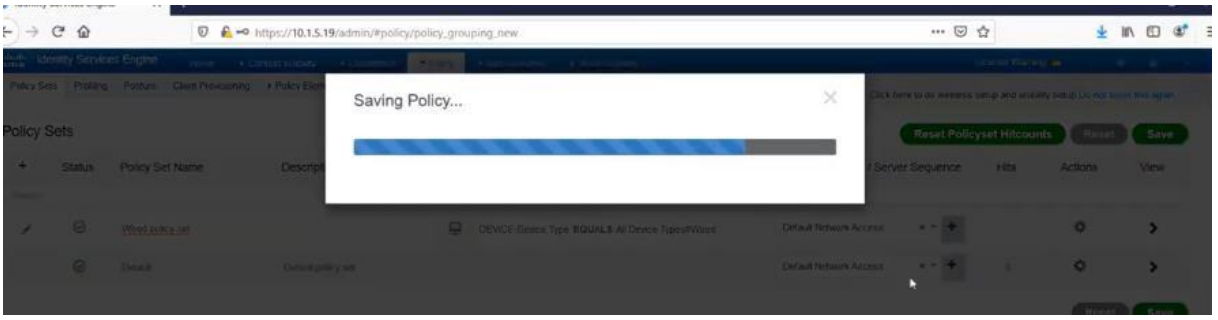


Figure (IV -19) : Sauvegarder la configuration du serveur ISE

IV.4 Procéder aux tests :

IV.4.1 Vérification des résultats d'authentification et d'autorisation sur le switch :

Pour observer en temps réel le processus d'authentification et d'autorisation 802.1X entre le switch et le serveur ISE, nous avons activé le mécanisme de debug sur le switch.

La commande utilisée est :

debug dot1x all

Cette commande permet d'afficher en console l'ensemble des événements relatifs à 802.1X notamment :

- la réception de la requête d'authentification envoyée par le client,
- la validation des informations par le serveur RADIUS (ISE),
- le résultat de l'authentification (succès ou échec),
- et l'assignation dynamique des autorisations comme le VLAN et l'application d'une ACL.

Dans notre cas, cette commande a produit les messages suivants confirmant la réussite de l'authentification et de l'autorisation, ainsi que l'assignation du VLAN 10 au port Fa0/2.

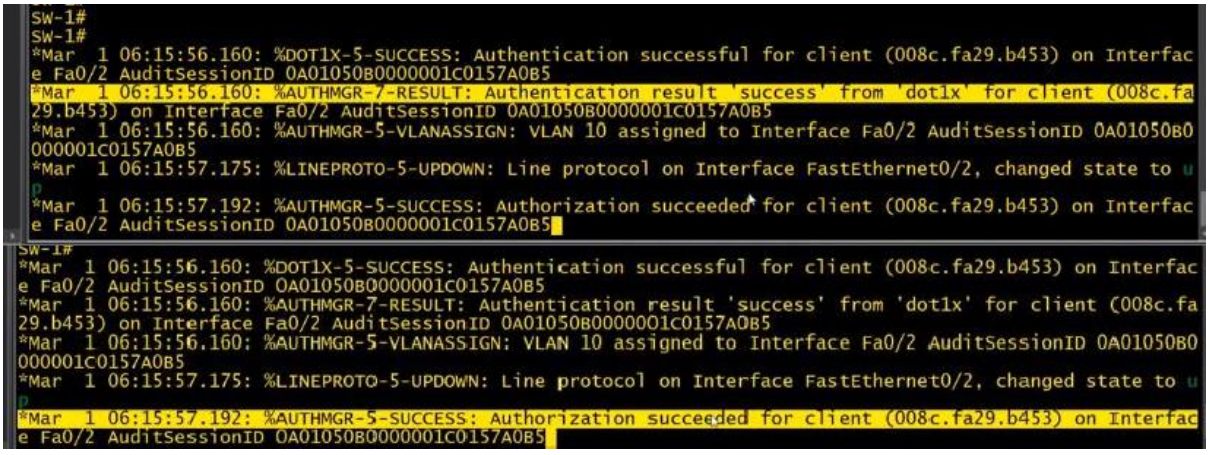


Figure (IV -20) : L'apparition de l'interface qui nous montre la réussite de l'authentification et de l'autorisation grâce à la commande debug dot1x all

IV.4.2 Vérification de l'assignation du VLAN :

Après l'authentification réussie de l'utilisateur jdoe au niveau du port Fa0/2, il est nécessaire de vérifier que le profil d'autorisation défini dans Cisco ISE a bien été appliqué par le switch. Pour ce faire,
Nous avons exécuté la commande suivante :

SW-1# show vlan brief

Cette commande permet d'afficher la table VLAN du switch ainsi que l'état des ports associés. Les résultats montrent clairement que le VLAN 10 (VLANO010) a été dynamiquement attribué au port Fa0/2, conformément au profil d'autorisation configuré dans ISE.

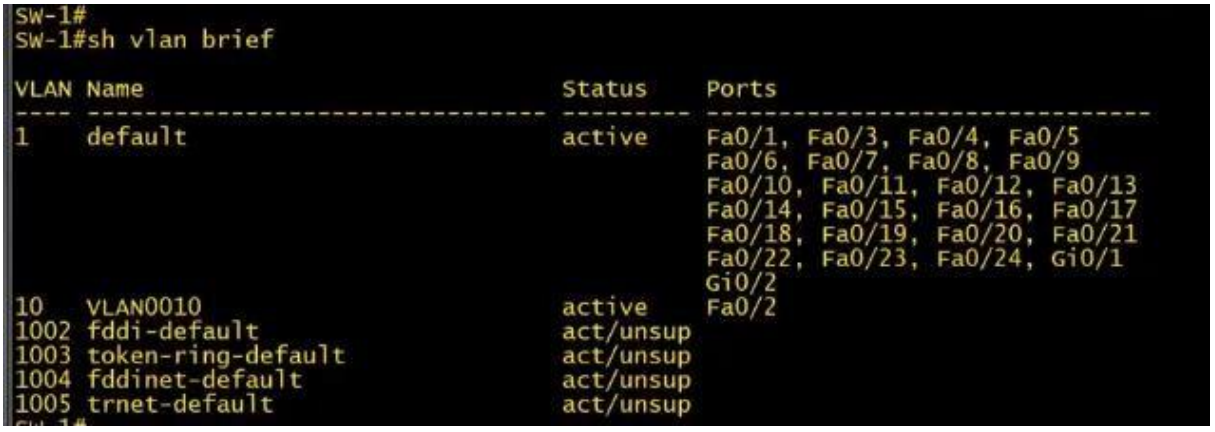


Figure (IV -21) : Vérification de l'assignation du VLAN

Le port Fa0/2, auquel est connecté le poste client de l'utilisateur sales, a bien été déplacé dans le VLAN 10 après authentification.
Cette assignation valide le bon fonctionnement de la communication entre le switch (NAS) et Cisco ISE via RADIUS.

Elle illustre également le principe de contrôle d'accès dynamique, qui permet d'affecter automatiquement des ressources réseau (VLAN, ACL) selon l'identité et le rôle de l'utilisateur.

IV.4.3 Vérification de l'application de I'ACL téléchargeable :

Afin de confirmer que I'ACL définie dans Cisco
ISE est effectivement appliquée au niveau du switch, nous avons exécuté la commande suivante :

SW-1# show ip access-lists

Le résultat montre la présence de deux listes de contrôle d'accès (ACL) :

1. Auth-Default-ACL : ACL par défaut installée par le switch pour permettre le trafic nécessaire au processus d'authentification (par exemple DHCP, EAPoL, etc.)

2. xACSACLX-IP-Sales-ACL-5ea45477 (per-user) : ACL dynamique téléchargée depuis Cisco ISE. Cette ACL correspond à la DACL "sales-ACL" que nous avons créée dans ISE et qui a été associée au profil d'autorisation "sales-profile".

Le contenu de cette ACL confirme que :

- Le trafic HTTP (tcp eq 80) et HTTPS (tcp eq 443) est autorisé.
- Tout autre trafic est bloqué (deny ip any any).

```
SW-1#
SW-1#sh ip access
SW-1#sh ip access-lists
Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348 (38 matches)
    20 permit udp any any range bootps 65347 (2 matches)
    30 deny ip any any (90 matches)
Extended IP access list xACSACLx-IP-Sales-ACL-5ea45477 (per-user)
    10 permit tcp any any eq www
    20 permit tcp any any eq 443
    30 deny ip any any
SW-1#
```

Figure (IV -22) : Vérification de l'application de I'ACL téléchargeable

- L'apparition de la DACL KACSACLX-IP-Sales-ACL-xxxxx prouve que le switch a bien téléchargé les règles d'accès depuis ISE via le protocole RADIUS,
- L'application de cette ACL au port Fa0/20 garantit que l'utilisateur du groupe sales n'a accès qu'aux ressources prévues dans la politique de sécurité.
- Cette étape illustre le rôle essentiel du NAC basé sur ISE : contrôler dynamiquement l'accès réseau en fonction de l'identité et du rôle de l'utilisateur

IV.4.4 Vérification de la session d'authentification sur le port Fa0/2 :

Afin de confirmer l'aboutissement du processus d'authentification et d'autorisation nous avons utilisé la commande :

SW-1# show authentication sessions interface fa0/2

Cette commande fournit des informations détaillées sur l'état de la session 802.1X de l'utilisateur connecté au port Fa0/2.
Les résultats obtenus indiquent que :

- L'utilisateur jdoe (saisi côté client) s'est authentifié avec succès (Authc Success)
- Le processus d'autorisation est validé (Authz Success).
- Le VLAN 10 a été dynamiquement attribué au port conformément au profil d'autorisation.
- La DACL XACSACLX-IP-Sales-ACL a été téléchargée depuis Cisco ISE et appliquée à l'utilisateur.
- L'authentification a été réalisée via le serveur RADIUS (ISE), mentionné comme Authentication Server.

```
SW-1#sh authentication sessions interface F0/2
*Mar  1 06:17:22.412: %SYS-5-CONFIG_I: Configured from console by console
            Interface:  FastEthernet0/2
          MAC Address:  008c.fa29.b453
           IP Address:  10.1.5.3
            User-Name:  jdoe
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-Sales-ACL-5ea45477
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01050B0000001C0157A0B5
     Acct Session ID:  0x0000001D
              Handle:  0x4C00001D

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

Figure (IV -23) : Vérification de la session d'authentification sur le port Fa0/2 :

Ce résultat confirme que le workflow complet du NAC est opérationnel **:**

1. Identification et authentification de l'utilisateur par 802.1X.

2. Autorisation dynamique appliquée par Cisco ISE (VLAN + ACL).

3. Contrôle d'accès granulaire respectant la politique de sécurité définie dans ISE.

Ainsi, cette commande valide la cohérence entre la configuration du switch, les politiques sur ISE et le comportement attendu au niveau du client,

IV.4.5.1 Vérification des authentifications dans l'interface ISE :

Dans la première capture, on observe l'interface graphique du serveur Cisco ISE qui présente l'état d'une authentification dans l'onglet Overview.

Les éléments affichés sont :

- **Event : 5200 Authentication succeeded** → l'utilisateur a été authentifié avec succès.
- **Username : jdoe** → l'identité utilisée par le client.
- **Endpoint ID : 00:8C:FA:29:B4:53** → l'adresse MAC du poste client.
- **Authentication Policy : Wired policy-set >> DOT1X** → l'authentification a été traitée par la politique dédiée au 802.1X.
- **Authorization Result : Sales-Profile** → le profil d'autorisation (incluant VLAN et ACL) a été appliqué au client.

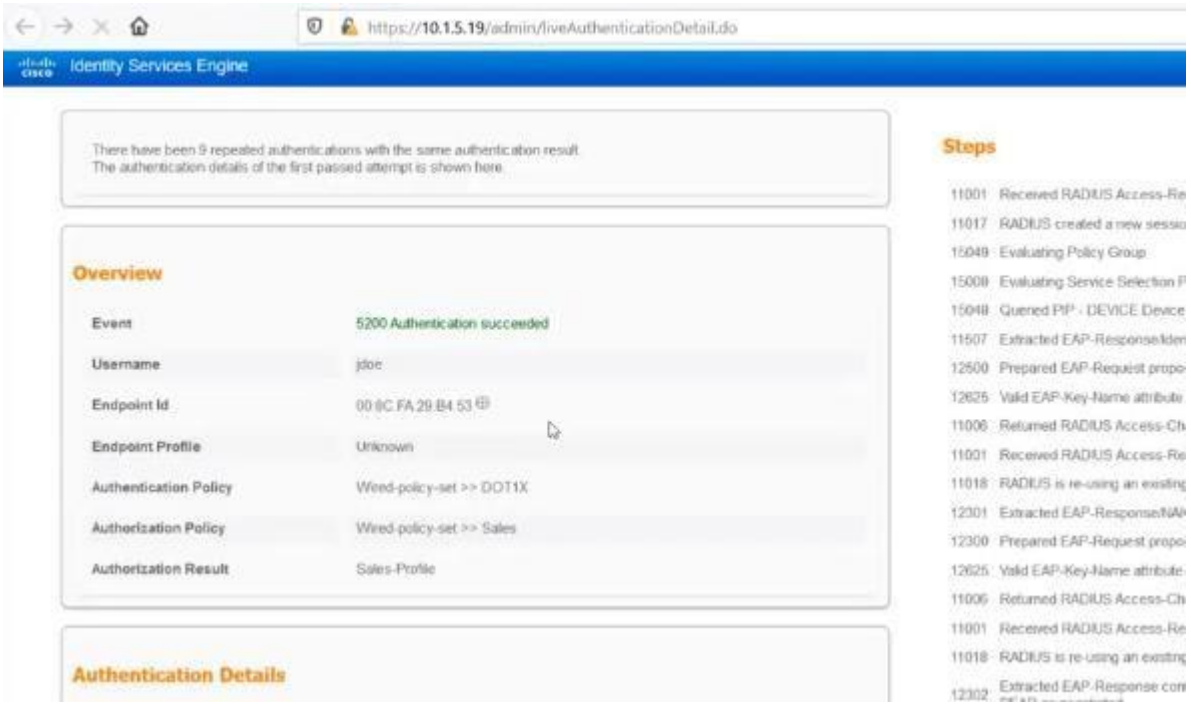


Figure (IV -23) : Vérification des authentifications dans l'interface ISE.

Cette vue d'ensemble permet de vérifier que le processus complet d'authentification et d'autorisation a été correctement exécuté par l'ISE.
L'utilisateur jdoe, membre du groupe Sales, a été identifié puis autorisé avec application d'un profil d'accès spécifique (Sales-Profile).
Cela démontre la capacité du serveur ISE à associer chaque utilisateur à une politique de sécurité adaptée, garantissant un contrôle d'accès basé sur l'identité.

IV.4.5.2 Détails de l'authentification dans I'ISE :

La seconde capture fournit une vue plus détaillée des informations liées à l'authentification réussie :

- **Date et heure (Source Timestamp /Received Timestamp)** : 2025-08-25 16:31:46 → permet de tracer précisément l'événement.
- **Policy Server : ISE-1** → indique quel nœud du cluster ISE a traité la requête.
- **Event : 5200 Authentication succeeded** → confirme le succès du processus.
- **Username : jdoe et User Type : User** → identifiant et type d'utilisateur.
- **Authentication Identity Store : Internal Users** → l'authentification s'est appuyée sur la base locale d'ISE.
- **Identity Group : User Identity Groups Sales** → confirme l'appartenance de l'utilisateur au groupe Sales.
- **Authentication Method: dot1x et Protocol PEAP (EAP-MSCHAPv2)** → détaille le protocole utilisé.
- **Network Device: SW-1 et Device Type Wired** → identifie l'équipement ayant initié la requête.
- **NAS IPv4 Address : 10.1.5.11** → adresse du switch qui relaie l'authentification.

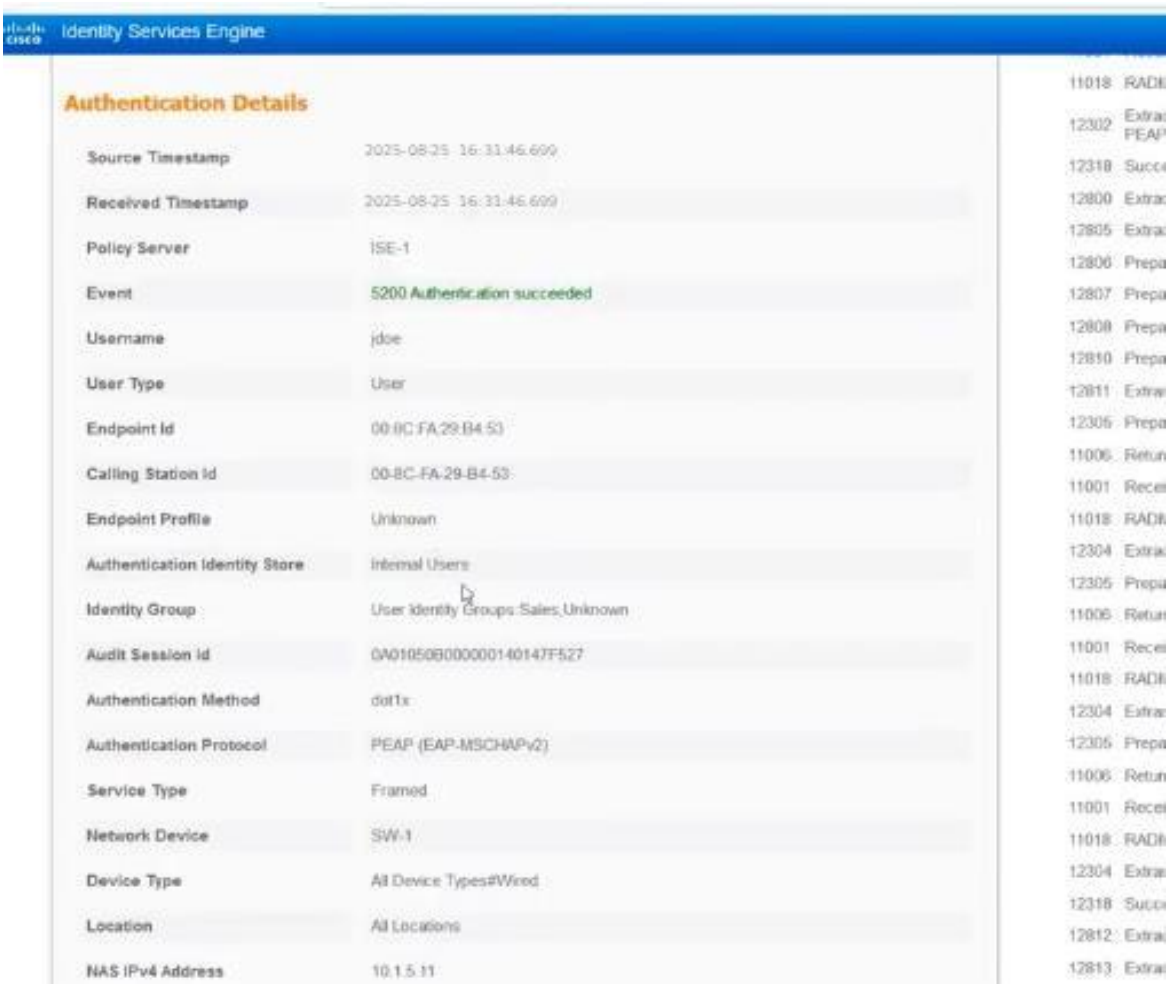


Figure (IV -24) : Détails de l'authentification dans I'ISE

Les détails présentés dans cette capture permettent d'assurer une traçabilité complète du processus d'authentification. On constate que l'utilisateur jdoe, appartenant au groupe Sales, a été authentifié via le protocole 802.1X (PEAP/EAP-MSCHAPv2) et autorisé par le serveur ISE à travers le profil associé

L'association explicite entre l'utilisateur, son groupe d'identité, le périphérique réseau (SW-1) et les politiques appliquées confirme la cohérence et l'efficacité de la mise en place d'une solution NAC basée sur Cisco ISE.

Conclusion :

À l'issue de ce laboratoire, nous avons pu vérifier le bon fonctionnement du mécanisme d'authentification 802.1X avec Cisco ISE.

Après la configuration conjointe du switch et du serveur ISE, l'utilisateur appartenant au groupe Sales a été authentifié avec succès et autorisé à accéder au réseau. Le serveur ISE a non seulement validé son identité mais a également appliqué automatiquement les politiques de sécurité associées, telles que l'assignation dynamique de VLAN et le téléchargement d'ACL.

Ce travail met en évidence l'efficacité d'une solution NAC dans la sécurisation des accès et la segmentation dynamique du réseau, contribuant ainsi à une meilleure résilience et à une gestion plus fine de la sécurité informatique

Conclusion et perspectives :

Conclusion et perspective

Dans le cadre de ce mémoire réalisé au sein de l'entreprise **OURHOUD – Sonatrach**, nous nous sommes intéressés à l'étude et à la mise en œuvre d'une solution de **contrôle d'accès réseau (NAC)** reposant sur la plateforme **Cisco Identity Services Engine (ISE)**. L'objectif était de renforcer la sécurité du réseau interne en garantissant que seuls les utilisateurs et terminaux autorisés et conformes puissent accéder aux ressources critiques de l'organisation.

Après avoir présenté le contexte général et les enjeux liés à la sécurité des systèmes d'information, nous avons étudié les différents mécanismes et solutions de protection disponibles. Une analyse comparative des solutions existantes nous a permis de justifier le choix de Cisco ISE, qui s'est révélé le plus adapté aux besoins de l'entreprise en matière de gestion centralisée des identités, de contrôle d'accès dynamique et d'évaluation de la conformité des postes.

La mise en place de cette solution sur un environnement de test a démontré sa capacité à :

- appliquer le protocole **IEEE 802.1X** pour l'authentification et l'autorisation des utilisateurs et des périphériques,
- rediriger les invités vers un portail d'accès sécurisé,
- vérifier en temps réel la **posture des terminaux** (mises à jour, antivirus, conformité logicielle),
- et offrir des mécanismes de remédiation afin de corriger les postes non conformes.

Ainsi, la solution déployée permet de réagir efficacement aux tentatives d'accès non autorisées et contribue à réduire la surface d'attaque interne, un point crucial pour une organisation critique comme Sonatrach.

Ce travail, bien qu'il ait permis d'atteindre les objectifs fixés, ouvre également la voie à plusieurs perspectives d'amélioration, notamment :

- l'intégration avec des solutions **MDM (Mobile Device Management)** pour une gestion plus fine des périphériques mobiles,
- l'automatisation avancée des politiques de sécurité à l'aide d'outils d'orchestration,
- et l'extension du déploiement à l'ensemble de l'infrastructure réseau de l'entreprise.

En conclusion, ce projet a mis en évidence l'importance d'une stratégie de sécurité proactive et adaptée aux menaces actuelles, tout en démontrant l'efficacité de Cisco ISE comme socle central pour le contrôle d'accès réseau et la gestion de la conformité des terminaux.

Bibliographies :

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

[2] Jean-François PILLOU, Jean-Philippe BAY, *Tout sur la sécurité informatique*, 4e édition, Dunod, Paris, 2016. ISBN 978-2-10-074608-8.

[3] Jean-François CARPENTIER, *La sécurité informatique dans la petite entreprise : état de l'art et bonnes pratiques*, Éditions ENI, Saint-Herblain, 2009.

[4] A. Guermouche. Sécurité des réseaux - cours 2 : les attaques, 2019.

[5] SécuritéInfo.com. Introduction et initiation à la sécurité informatique, 2019

[6] Yousri Daldoul. Techniques avancées de sécurité et de cryptographie, 2016.

[7] Samir Diabi. Sécurité du réseau, 2019.

[8] Ali SEDIQI, *Sécurité des réseaux informatique*, ISTE Edition Limited, août 2019, 278 p., ISBN : 978-1-78405-621-6.

[9] Mickael Choisnard. Réseaux et sécurité informatique, 2015. Université de Bourgogne.

[10] Radja BOUKHARROU, *Sécurité des réseaux*, support de cours, Faculté des Nouvelles Technologies de l'Information et de la Communication, Département de l'Informatique Fondamentale et ses Applications, Université Abdelhamid Mehri Constantine II, Année universitaire 2019-2020.

[11] Yousri Daldoul. Techniques avancées de sécurité et de cryptographie, 2016

[12] Authentification.eu. Qu'est ce que l'authentification réseau ?, 2019.

[13] Ameur Salem ZAIDOUN, *Sécurité informatique, concepts et outils*, ISTE Edition Limited, mars 2023, 198 p., ISBN : 978-1-78405-907-1.

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

[15] DRosolen, “How to choose the best Network Access Control solution (NAC),” Silicon, Apr. 13, 2009. https://www.silicon.es/como-elegir-la-mejor-solucion-de-control-de-acceso-a-la-red-nac-751.*

[16]“Tutorial:Network Access Control (NAC): Page 4 of 11.”https://www.networkcomputing.com/careers-and-certifications/tutorial-network-access-control-nac/page/0/3.(traduction libre) (consulte´le21/08/2025).

[17]E. Chan, “Network Access Control (traduction libre)

[18]“What Is Network Access Control? Explaining NAC Solutions.” https://www.varonis.com/blog/network-access-control-nac.*

[19] “Network Access Control,” Wikipedia. Aug. 20, 2025. Available: https://en.wikipedia.org/w/index.php?title=Network_Access_Control&oldid=1137953892

[20]J.Gauthier,∗RADIUS—802.1X:authentificationetcontro^led’acce`s∗,Expose´IGM,Universite´deMarne−la−Valle´e,XPOSE2007.[Enligne].Disponiblesur:http://www−igm.univ−mlv.fr/ dr/XPOSE2007/jgauth02RADIUS/8021x.html (consulte´le21/08/2025).

[21] A. Pérez, *L’intégration de Wi-Fi dans le réseau de mobiles 4G*, Londres : ISTE Editions Limited, 2018, 270 p., ISBN 978-1-78405-426-7.

[22] B. Lee, *What Is the RADIUS Protocol?*, JumpCloud Blog. [En ligne]. Disponible sur : https://jumpcloud.com/blog/what-is-the-radius-protocol (consulte´le22/08/2025).

[23] “How RADIUS Server Authentication Works.” https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/authentication/radius_how_works_c.html (consulte´le23/08/2025).

[24] Microsoft, *Extensible Authentication Protocol (EAP) for network access*, Microsoft Learn, mis à jour le 9 juillet 2025. [En ligne]. Disponible sur : https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim

[25] “Tutorial: Network Access Control (NAC): Page 2 of 11.”

https://www.networkcomputing.com/careers-and-certifications/tutorial-network-access-control-nac/page/0/1 (consulte´le23/08/2025).

[26] H. N. Security, “Network Access Control (NAC),” Help Net Security, Nov. 26, 2007.

https://www.helpnetsecurity.com/2007/11/26/network-access-control-nac/ (consulte´le23/08/2025).

[27] OpenNac, http://sourceforge.net/projects/opennac, (consulte´le24/08/2025).

[28] Serrao, Gloria J., "Network access control (NAC): An open source analysis of architectures and requirements," IEEE International Carnahan Conference on Security Technology (ICCST), 2010

[29] Annuar, H., Shanmugam, B., Ahmad, A., Idris, N.B., AlBakri, S.H.and Samy, G.N., "Enhancement of network access control architecture with virtualization," International Conference on Informatics and Creative Multimedia (ICICM), 2013

[30] "PacketFence: Overview" http://www.packetfence.org/about/overview.html, (consulte´le22/08/2025).

[31] "PacketFence: Advanced Features" http://www.packetfence.org/about/advanced_features.html, (consulte´le24/08/2025).

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

[33] Fortinet, *Solutions de contrôle d'accès au réseau (NAC)*, Fortinet, [en ligne]. Disponible sur : https://www.fortinet.com/fr/products/network-access-control

[34]"UNIFIED ACCESS CONTROL." (consulte´le21/08/2025).. [Online]. Available: https://www.juniper.net/assets/us/en/local/pdf/brochures/1500051-en.pdf

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

[36] J. Kunst, *Deploying Cisco ISE for Guest Network Access*, Cisco Systems, septembre 2018. [En ligne]. Disponible en PDF, Cisco Public Information.

[37] 26 Cisco Systems, *Cisco Identity Services Engine (ISE) – At-A-Glance*, Cisco Public Information, septembre 2013. [En ligne]. Disponible sur : www.cisco.com/go/trademarks

[38] Cisco Systems, *Cisco Identity Services Engine (ISE) – Data Sheet*, Cisco Public Information, 2014. [En ligne]. Disponible sur : https://www.cisco.com

[39] -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

[40] Ctelecoms, *An In Depth Exploration of Cisco Identity Services Engine (ISE)*, Ctelecoms Blog, (consulte´le25/08/2025). [En ligne]. Disponible sur : https://www.ctelecoms.com.sa/en/Blog614/An-In-Depth-Exploration-of-Cisco-Identity-Services-Engine-ISE

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

[42]-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

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

[44] Cisco Systems, *Cisco Identity Services Engine – Ordering Guide*, Cisco Public Information, septembre 2020. [En ligne]. Disponible sur : https://www.cisco.com