

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد - تلمسان -

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme de MASTER**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : BOUIDAINE Albaraa et BOUCIF Meriem

Thème

**Gestion des accès par le modèle AAA et le protocole
802.1X**

Soutenu le 12/09/2020 devant le jury composé de :

| | | | |
|------------------------------------|-----|---------------|-------------------------|
| Mr. MOUSSAOUI Djillali | MCB | Univ. Tlemcen | Président |
| Mr. ZERROUKI Hadj | MCB | Univ. Tlemcen | Examineur |
| Mr. HADJILA Mourad | MCA | Univ. Tlemcen | Directeur de mémoire |
| Mr. BACHIR BOUIADJRA Abderrazak | MCB | Univ. SBA | Co-Directeur de mémoire |

À Nos Parents

& Nos Familles

RESUME

La gestion des accès au réseau est devenue très importante, d'une part pour la protection contre les tentatives d'intrusions, et d'autre part pour assurer la dynamique et la mobilité demandées sur les réseaux de nouvelle génération, dont : l'appartenance au VLAN, l'adressage IP, les mesures de sécurité, le filtrage et l'attribution des droits d'accès, voire même l'affectation de la qualité de service adéquate à chaque utilisateur ou ensemble d'utilisateurs. Ce projet représente une mise en place d'une solution de sécurité ayant comme objectif principal la gestion de l'ensemble des accès possibles au réseau : accès aux ressources réseau en filaire ou en Wifi, accès en configuration CLI/GUI, etc. Le présent travail consiste à déployer l'ensemble des mécanismes du modèle AAA (Authentication, Authorization, Accounting), ainsi de le compléter par la mise en œuvre du protocole 802.1X pour assurer la dynamique et la mobilité des accès au réseau.

Mots clés :

Sécurité, AAA, authentification, autorisation, traçabilité, TACACS+, RADIUS, EAP, 802.1X, MAB.

ABSTRACT

Network access management has become very important, on the one hand for protection against intrusion attempts, and on the other hand to ensure the dynamicity and mobility required on new generation networks, including: membership to VLAN, IP addressing, security measures, filtering and allocation of access rights, and even the allocation of the appropriate quality of service to each user or group of users. This project represents the implementation of a security solution whose main objective is the management of all possible access to the network: access to network resources by wired or WiFi, access in CLI / GUI configuration, etc. The present work consists in deploying all the mechanisms of the AAA model (Authentication, Authorization, Accounting), thus complementing it by the implementation of the 802.1X protocol to ensure the dynamicity and mobility of network access.

Keywords:

Security, AAA, authentication, authorization, accounting, TACACS +, RADIUS, EAP, 802.1X, MAB.

REMERCIEMENTS

Ce travail est l'aboutissement d'un dur labeur et de beaucoup de sacrifices ; nos remerciements vont d'abord au Créateur de l'univers le tout puissant et miséricordieux, qui nous a donné la santé, la volonté, la force, le courage et la patience, qui nous ont accompagnés tout au long de la préparation et l'élaboration de ce modeste travail et qui nous ont permis de l'achever dans de bonnes conditions.

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui nous voudrions, à travers ces quelques lignes, témoigner toute notre gratitude.

Nous tenons dans un premier temps adresser nos sincères et chaleureux remerciements à nos encadrants du projet de fin d'étude, Mr. HADJILLA Mourad ; professeur à l'Université Aboubakr Belkaid de Tlemcen et Mr. BACHIR BOUIADJRA Abderrazak ; professeur à l'Université Djilali Liabès de Sidi Bel Abbès, qui ont réussi à former un duo solide aux compétences complémentaires. Merci à vous deux pour votre patience, encouragement, disponibilité et surtout votre extrême amabilité malgré vos grandes charges de travail. Nous vous remercions de nous avoir encadrés, orientés, aidés et conseillés. Nous avons eu beaucoup de plaisir de travailler à vos côtés.

Nous adressons aussi nos vifs remerciements aux Membres du jury ; Mr. MOUSSAOUI Djilali d'avoir accepté présider le jury de soutenance et Mr. ZERROUKI Hadj d'avoir examiné notre travail.

Nous tenons à remercier également l'équipe de l'établissement ICT TOWERS de Sidi Bel Abbès et d'Alger, en particulier Mr. BACHIR BOUIADJRA Abderrazak, Mr. ZELLAT Salah Eddine, Mr. SADI Abdelbari, Mr. HASSAINE Hamid et Mr. AZZA Yassine, Pour l'excellent accueil qui nous a été réservé, le temps consacré lors de notre stage au sein de votre établissement, la qualité de l'accompagnement dont nous avons bénéficiée, la confiance et les connaissances que vous avez partagées avec nous. Merci également à tous les membres du personnel qui ont mis tout en œuvre pour que notre stage se déroule dans les meilleures conditions possibles.

Nous souhaitons adresser nos profonds remerciements et nos profondes reconnaissances à tous les professeurs du département de télécommunication de l'Université de Tlemcen pour la richesse et la qualité de leur enseignement en nous fournissant les outils nécessaires à la réussite de nos études.

Nous tenons à remercier finalement toute personne qui a, de près ou de loin, contribué d'une manière ou d'une autre au succès de ce travail et spécialement ceux que nous n'avons pas pu citer, mais qui sont présents dans nos esprits et dans nos cœurs.

DEDICACES

Toutes les lettres ne sauraient trouver les mots qu'il faut... Tous les mots ne sauraient exprimer la gratitude, L'amour, le respect, la reconnaissance... Aussi, c'est tout simplement que ... Nous dédions ce mémoire...

À NOS CHERS PARENTS, Aucune dédicace ne saurait exprimer notre respect, notre amour éternel et notre considération pour les sacrifices que vous avez consenti pour notre instruction et notre bien-être. Nous vous remercions pour tout le soutien inconditionnel, à la fois moral et économique et l'amour que vous portez depuis notre enfance et nous espérons que votre bénédiction nous accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que nous ne vous en acquittions jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais nous ne vous décevions.

À NOS CHERS SOEURS, pour leurs encouragements permanents, et leur soutien moral.

À NOS CHERS FRERES, pour leur appui et leur encouragement.

À NOS GRANDS PERES ET GRANDES MERES Qui nous ont accompagnées par leurs prières, leur douceur, puisse Dieu leur prêter longue vie et beaucoup de santé et de bonheur dans les deux vies.

À NOS CHERS oncles, tantes, leurs époux et épouses, à nos chers cousins et cousines ; Veuillez trouver dans ce travail l'expression de notre respect le plus profond et notre affection la plus sincère.

À TOUTES NOS TENDRES FAMILLES pour leurs soutiens tout au long de notre parcours universitaire, que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infailible. Merci d'être toujours là pour nous.

À NOS AMIS qui nous ont apporté leur soutien inestimable tout au long de notre démarche, et qui par leurs encouragements, on a pu surmonter tous les obstacles.

À NOS CAMARADES de la promotion 2018-2020 que nous avons servis avec humilité et avec lesquelles nous avons passé une scolarité exceptionnelle, riche d'enseignements, et d'expériences de rencontres, nous voulons ici dire notre sincère amitié.

TABLE DES MATIERES

| | |
|---|-----|
| RESUME | i |
| ABSTRACT..... | ii |
| REMERCIEMENTS..... | iii |
| DEDICACES | iv |
| TABLE DES MATIERES | v |
| LISTE DES TABLEAUX | ix |
| LISTE DES FIGURES | x |
| ABREVIATIONS | xiv |
| INTRODUCTION GENERALE | 1 |
| CHAPITRE 1 FONDAMENTAUX DE LA SECURITE | 3 |
| 1.1. Introduction..... | 4 |
| 1.2. Importance de la sécurité | 4 |
| 1.3. Cybersécurité vs. Sécurité de l'information..... | 5 |
| 1.4. Objectifs de la sécurité..... | 5 |
| 1.4.1. Confidentialité | 6 |
| 1.4.2. Intégrité..... | 7 |
| 1.4.3. Disponibilité | 8 |
| 1.5. Terminologie de la sécurité..... | 8 |
| 1.5.1. Terminologie générale..... | 8 |
| 1.5.2. Codes malveillants..... | 9 |
| 1.5.3. Types de hackers | 10 |
| 1.6. Equipes de sécurité | 11 |
| 1.7. Axes de sécurité | 13 |
| 1.7.1. Sécurité physique et environnementale | 14 |

| | | |
|------------|---|----|
| 1.7.2. | Sécurité administrative | 14 |
| 1.7.3. | Sécurité technique..... | 15 |
| 1.8. | Conclusion | 16 |
| CHAPITRE 2 | MODELE AAA..... | 18 |
| 2.1. | Introduction..... | 19 |
| 2.2. | Authentification | 19 |
| 2.2.1. | Définition..... | 19 |
| 2.2.2. | Modes d'authentification | 20 |
| 2.2.3. | Méthodes d'authentification | 22 |
| 2.2.4. | Facteurs d'authentification | 24 |
| 2.2.5. | Règles des mots de passe..... | 26 |
| 2.2.6. | Protocoles d'authentification | 29 |
| 2.3. | Autorisation..... | 32 |
| 2.3.1. | Définition..... | 32 |
| 2.3.2. | Méthodes d'autorisation AAA..... | 34 |
| 2.3.3. | Niveaux de privilège « <i>Privilege Levels</i> »..... | 35 |
| 2.3.4. | Accès CLI basé sur les rôles « <i>Role based CLI Access</i> » | 35 |
| 2.4. | Traçabilité « <i>Accounting</i> » | 36 |
| 2.4.1. | Définition..... | 36 |
| 2.4.2. | Méthodes de traçabilité AAA | 38 |
| 2.5. | Protocoles AAA | 39 |
| 2.5.1. | TACACS+ | 40 |
| 2.5.2. | RADIUS | 46 |
| 2.5.3. | Comparaison entre RADIUS et TACACS + | 50 |
| 2.6. | Conclusion | 51 |
| CHAPITRE 3 | PROTOCOLE 802.1X | 53 |
| 3.1. | Introduction..... | 54 |

| | | |
|---------------------------------|---|----|
| 3.2. | Composants de 802.1X | 54 |
| 3.2.1. | Client « <i>supplicant</i> » | 54 |
| 3.2.2. | Authentificateur « <i>authenticator</i> » | 55 |
| 3.2.3. | Serveur d'authentification « <i>Authentication Server</i> » | 55 |
| 3.3. | EAP « <i>Extensible authentication protocol</i> » | 56 |
| 3.4. | EAPOL « <i>EAP Over LAN</i> » | 58 |
| 3.5. | Echange de messages dans 802.1X | 59 |
| 3.6. | Méthodes d'EAP | 61 |
| 3.6.1. | Méthodes EAP basées sur un secret pré-partagé | 61 |
| 3.6.2. | Méthodes EAP basées sur une clé publique | 62 |
| 3.6.3. | Méthodes EAP basées sur les tunnels | 63 |
| 3.6.4. | Comparaison entre les méthodes d'EAP | 67 |
| 3.7. | 802.1X Host Modes | 68 |
| 3.8. | Fonctionnalités de l'authentification 802.1X | 70 |
| 3.8.1. | MAC Authentication Bypass « <i>MAB</i> » | 70 |
| 3.8.2. | VLAN Assignment | 71 |
| 3.8.3. | Guest VLAN | 72 |
| 3.8.4. | Restricted / Failed VLAN | 72 |
| 3.8.5. | Downloadable ACLs « <i>DAACLs</i> » | 73 |
| 3.9. | 802.1X Timers | 73 |
| 3.10. | Conclusion | 75 |
| CHAPITRE 4 IMPLEMENTATION | | 77 |
| 4.1. | Introduction | 78 |
| 4.2. | Configuration initiale | 80 |
| 4.2.1. | Configuration du switch d'accès « <i>authentificateur</i> » | 80 |
| 4.2.2. | Configuration du switch multi-layer | 82 |
| 4.2.3. | Les tests de connectivité | 85 |

| | | |
|--------|---|-----|
| 4.3. | Implémentation de la méthode 802.1X..... | 87 |
| 4.3.1. | Configuration initiale du modèle AAA | 87 |
| 4.3.2. | Ajout du serveur Radius au niveau du switch d'accès | 87 |
| 4.3.3. | Configuration du « <i>Port-Based Authentication</i> » | 88 |
| 4.4. | Configuration des variables 802.1X | 128 |
| 4.4.1. | Affectation des VLANs « <i>VLAN Assignment</i> »..... | 128 |
| 4.4.2. | Liste de contrôle d'accès téléchargeable « <i>DACLs</i> » | 134 |
| 4.4.3. | Restricted / Failed VLAN & Guest VLAN | 139 |
| 4.4.4. | Les Timers | 144 |
| 4.5. | Conclusion | 145 |
| | CONCLUSION GENERALE..... | 147 |
| | Bibliographie | 149 |

LISTE DES TABLEAUX

| | |
|--|----|
| Tableau 1.1 : Les protections contre les risques en implémentant la triade CID. | 8 |
| Tableau 2.1 : Comparaison entre mot de passe et phrase secrète. | 26 |
| Tableau 2.2 : Types de services RADIUS courants..... | 47 |
| Tableau 2.3 : Comparaison entre TACACS+ et RADIUS. | 50 |
| Tableau 3.1 : Comparaison entre les méthodes EAP..... | 68 |
| Tableau 4.1 : Matériels et outils utilisés. | 79 |

LISTE DES FIGURES

| | |
|---|----|
| Figure 1.1 : Triade CID..... | 6 |
| Figure 1.2 : Concepts généraux de la confidentialité..... | 7 |
| Figure 1.3 : Roue chromatique des équipes de sécurité..... | 11 |
| Figure 1.4 : Charte de création de couleurs secondaires..... | 13 |
| Figure 1.5 : Fondamentaux de la sécurité. | 13 |
| Figure 2.1 : Authentification locale. | 21 |
| Figure 2.2 : Authentification centralisée..... | 21 |
| Figure 2.3 : Exemple d'autorisation. | 34 |
| Figure 2.4 : Exemple de traçabilité..... | 37 |
| Figure 2.5 : Communication entre client et serveur TACACS+..... | 41 |
| Figure 2.6 : Flux de communication d'authentification TACACS+..... | 43 |
| Figure 2.7 : Flux de communication d'autorisation et de Traçabilité TACACS+..... | 45 |
| Figure 2.8 : Transport de communication EAP via RADIUS. | 46 |
| Figure 2.9 : Flux d'authentification et d'autorisation RADIUS. | 48 |
| Figure 2.10 : Flux de traçabilité RADIUS..... | 49 |
| Figure 3.1 : Rôles des équipements 802.1X. | 55 |
| Figure 3.2 : Architecture de 802.1X. | 55 |
| Figure 3.3 : Format de message EAP. | 57 |
| Figure 3.4 : Message de EAP Request / Response. | 57 |
| Figure 3.5 : Format de trame EAPOL..... | 59 |
| Figure 3.6 : Echange de messages EAPOL / 802.1X. | 60 |
| Figure 3.7 : MAC Authentication Bypass (MAB)..... | 71 |
| Figure 4.1 : Topologie de 802.1X..... | 78 |
| Figure 4.2 : Récapitulation de la partie pratique..... | 79 |
| Figure 4.3 : Configuration automatique de l'adresse IPv4 du client. | 85 |
| Figure 4.4 : Test de connectivité entre le client (192.168.1.1) et le MLS (192.168.1.20). | 85 |
| Figure 4.5 : Test de connectivité entre le serveur ISE (192.168.1.100) et le MLS (192.168.1.20)..... | 86 |
| Figure 4.6 : Test de connectivité entre le client (192.168.1.1) et le serveur ISE (192.168.1.100)..... | 86 |

| | |
|--|-----|
| Figure 4.7 : Ecran de gestion du serveur ISE. | 88 |
| Figure 4.8 : Ecran d'accueil du serveur ISE..... | 89 |
| Figure 4.9 : Etape 1 de l'ajout de l'équipement réseau. | 89 |
| Figure 4.10 : Etape 2 de l'ajout de l'équipement réseau. | 90 |
| Figure 4.11 : Etape 3 de l'ajout de l'équipement réseau. | 90 |
| Figure 4.12 : Etape 4 de l'ajout de l'équipement réseau. | 91 |
| Figure 4.13 : Etape 5 de l'ajout de l'équipement réseau. | 91 |
| Figure 4.14 : Etape 6.a de l'ajout de l'équipement réseau. | 92 |
| Figure 4.15 : Etape 6.b de l'ajout de l'équipement réseau. | 92 |
| Figure 4.16 : Etape 1 de l'ajout de groupes d'identité d'utilisateurs..... | 93 |
| Figure 4.17 : Etape 2 de l'ajout de groupes d'identité d'utilisateurs..... | 93 |
| Figure 4.18 : Etape 3 de l'ajout de groupes d'identité d'utilisateurs..... | 94 |
| Figure 4.19 : Etape 4 de l'ajout de groupes d'identité d'utilisateurs..... | 94 |
| Figure 4.20 : Etape 5 de l'ajout de groupes d'identité d'utilisateurs..... | 95 |
| Figure 4.21 : Etape 6 de l'ajout de groupes d'identité d'utilisateurs..... | 95 |
| Figure 4.22 : Etape 1 de l'ajout d'utilisateurs. | 96 |
| Figure 4.23 : Etape 2 de l'ajout d'utilisateurs. | 96 |
| Figure 4.24 : Etape 3 de l'ajout d'utilisateurs. | 97 |
| Figure 4.25 : Etape 4.a de l'ajout d'utilisateurs..... | 97 |
| Figure 4.26 : Etape 4.b de l'ajout d'utilisateurs. | 98 |
| Figure 4.27 : Etape 5 de l'ajout d'utilisateurs. | 98 |
| Figure 4.28 : Etape 6 de l'ajout d'utilisateurs. | 99 |
| Figure 4.29 : Etape 7 de l'ajout d'utilisateurs. | 99 |
| Figure 4.30 : Etape 8 de l'ajout d'utilisateurs. | 100 |
| Figure 4.31 : Etape 9.a de l'ajout d'utilisateurs..... | 100 |
| Figure 4.32 : Etape 9.b de l'ajout d'utilisateurs. | 101 |
| Figure 4.33 : Etape 1 de l'ajout de protocoles d'authentification. | 101 |
| Figure 4.34 : Etape 2 de l'ajout de protocoles d'authentification. | 102 |
| Figure 4.35 : Etape 3 de l'ajout de protocoles d'authentification. | 102 |
| Figure 4.36 : Etape 4 de l'ajout de protocoles d'authentification. | 103 |
| Figure 4.37 : Etape 5 de l'ajout de protocoles d'authentification. | 103 |
| Figure 4.38 : Etape 6 de l'ajout de protocoles d'authentification. | 104 |
| Figure 4.39 : Etape 7 de l'ajout de protocoles d'authentification. | 104 |
| Figure 4.40 : Etape 1 de la présentation de conditions d'authentification..... | 105 |

| | |
|--|-----|
| Figure 4.41 : Etape 2 de la présentation de conditions d'authentification..... | 105 |
| Figure 4.42 : Etape 3 de la présentation de conditions d'authentification..... | 106 |
| Figure 4.43 : Etape 1 de l'ajout de politiques d'authentification. | 106 |
| Figure 4.44 : Etape 2 de l'ajout de politiques d'authentification. | 107 |
| Figure 4.45 : Etape 5 de l'ajout de politiques d'authentification. | 107 |
| Figure 4.46 : Etape 6 de l'ajout de politiques d'authentification. | 108 |
| Figure 4.47 : Etape 7 de l'ajout de politiques d'authentification. | 108 |
| Figure 4.48 : Etape 8 de l'ajout de politiques d'authentification. | 109 |
| Figure 4.49 : Etape 9 de l'ajout de politiques d'authentification. | 109 |
| Figure 4.50 : Etape 1.1 de l'ajout de politiques d'autorisation 802.1X. | 110 |
| Figure 4.51 : Etape 1.2 de l'ajout de politiques d'autorisation 802.1X. | 111 |
| Figure 4.52 : Etape 1.3 de l'ajout de politiques d'autorisation 802.1X. | 111 |
| Figure 4.53 : Etape 1.4 de l'ajout de politiques d'autorisation 802.1X. | 112 |
| Figure 4.54 : Etape 1.5 de l'ajout de politiques d'autorisation 802.1X. | 112 |
| Figure 4.55 : Etape 1.6 de l'ajout de politiques d'autorisation 802.1X. | 113 |
| Figure 4.56 : Etape 2 de l'ajout de politiques d'autorisation 802.1X..... | 113 |
| Figure 4.57 : Etape 3 de l'ajout de politiques d'autorisation 802.1X..... | 114 |
| Figure 4.58 : Etape 7 de l'ajout de politiques d'autorisation 802.1X..... | 115 |
| Figure 4.59 : Etape 13 de l'ajout de politiques d'autorisation 802.1X..... | 116 |
| Figure 4.60 : Etape 1.1 de politique d'autorisation MAB. | 117 |
| Figure 4.61 : Etape 1.2 de politique d'autorisation MAB. | 117 |
| Figure 4.62 : Etape 1.3 de politique d'autorisation MAB. | 118 |
| Figure 4.63 : Etape 1.4 de politique d'autorisation MAB. | 118 |
| Figure 4.64 : Etape 2.1 de politique d'autorisation MAB. | 119 |
| Figure 4.65 : Etape 2.2 de politique d'autorisation MAB. | 119 |
| Figure 4.66 : Etape 2.4 de politique d'autorisation MAB. | 120 |
| Figure 4.67 : Etape 2.5 de politique d'autorisation MAB. | 120 |
| Figure 4.68 : Etape 8 de politique d'autorisation MAB. | 121 |
| Figure 4.69 : Etape 1 de test de l'authentification 802.1X. | 122 |
| Figure 4.70 : Etape 2.a de test de l'authentification 802.1X (Utilisateur1)..... | 123 |
| Figure 4.71 : Etape 2.b de test de l'authentification 802.1X (Utilisateur2)..... | 123 |
| Figure 4.72 : Etape 3 de test de l'authentification 802.1X. | 124 |
| Figure 4.73 : Etape 4 de test de l'authentification 802.1X. | 124 |
| Figure 4.74 : Etape 5.a de test de l'authentification 802.1X. | 125 |

| | |
|---|-----|
| Figure 4.75 : Etape 5.b de test de l'authentification 802.1X. | 125 |
| Figure 4.76 : Etape 6 de test de l'authentification 802.1X. | 126 |
| Figure 4.77 : Etape 1 de test de l'authentification MAB. | 126 |
| Figure 4.78 : Etape 2 de test de l'authentification MAB. | 127 |
| Figure 4.79 : Etape 3 de test de l'authentification MAB. | 127 |
| Figure 4.80 : Etape 4 de test de l'authentification MAB. | 128 |
| Figure 4.81 : Etape 1 de configuration de l'affectation des VLANs. | 129 |
| Figure 4.82 : Etape 2 de configuration de l'affectation des VLANs. | 129 |
| Figure 4.83 : Etape 3 de configuration de l'affectation des VLANs. | 130 |
| Figure 4.84 : Etape 5 de configuration de l'affectation des VLANs. | 130 |
| Figure 4.85 : Etape 1 de test de configuration de l'affectation des VLANs. | 131 |
| Figure 4.86 : Etape 3 de test de configuration de l'affectation des VLANs. | 131 |
| Figure 4.87 : Etape 4 de test de configuration de l'affectation des VLANs. | 132 |
| Figure 4.88 : Etape 6 de test de configuration de l'affectation des VLANs. | 132 |
| Figure 4.89 : Etape 7 de test de configuration de l'affectation des VLANs. | 133 |
| Figure 4.90 : Etape 8 de test de configuration de l'affectation des VLANs. | 133 |
| Figure 4.91 : Etape 1 de configuration des DACLs. | 134 |
| Figure 4.92 : Etape 2 de configuration des DACLs. | 134 |
| Figure 4.93 : Etape 3 de configuration des DACLs. | 135 |
| Figure 4.94 : Etape 4.a de configuration des DACLs. | 135 |
| Figure 4.95 : Etape 4.b de configuration des DACLs. | 136 |
| Figure 4.96 : Etape 7 de configuration des DACLs. | 136 |
| Figure 4.97 : Etape 10 de configuration des DACLs. | 137 |
| Figure 4.98 : Etape 1 de test de configuration de DACLs. | 138 |
| Figure 4.99 : Etape 2 de test de configuration de DACLs. | 138 |
| Figure 4.100 : Etape 3 de test de configuration de DACLs. | 139 |
| Figure 4.101 : Etape 1 de test de configuration de VLAN Restricted. | 140 |
| Figure 4.102 : Etape 2 de test de configuration de VLAN Restricted. | 141 |
| Figure 4.103 : Etape 3 de test de configuration de VLAN Restricted. | 141 |
| Figure 4.104 : Etape 1 de test de configuration de VLAN Guest. | 142 |
| Figure 4.105 : Etape 2 de test de configuration de VLAN Guest. | 142 |
| Figure 4.106 : Etape 3 de test de configuration de VLAN Guest. | 143 |
| Figure 4.107 : Etape 4 de test de configuration de VLAN Guest. | 143 |
| Figure 4.108 : Etape 5 de test de configuration de VLAN Guest. | 144 |
| Figure 4.109 : Test de timers. | 145 |

ABBREVIATIONS

| | |
|---------|--|
| AAA | Authentication, Authorization and Accounting |
| ACL | Access Control List |
| ACS | Access Control Server |
| AD | Active Directory |
| ARA | AppleTalk Remote Access |
| ARAP | Apple Remote Access Protocol |
| AS | Authentication Server |
| ASF | Alerting Standards Forum |
| ATM | Automated Teller Machine |
| AUX | Auxiliary |
| AV | Attribute Value |
| CDP | Cisco Discovery Protocol |
| CHAP | Challenge Handshake Authentication Protocol |
| CID | Confidentialité, Intégrité et Disponibilité |
| CLI | Command Line Interface |
| CS-MARS | Cisco Secure-Monitoring Analysis and Response System |
| CSV | Comma Separated Values |
| DAACL | Downloadable Access Control List |
| DES | Data Encryption Standard |
| DHCP | Dynamic Host Configuration Protocol |
| EAP | Extensible Authentication Protocol |
| EAPoL | Extensible Authentication Protocol over LAN |
| FAI | Fournisseur d'Accès à Internet |

| | |
|---------|---|
| FAST | Flexible Authentication via Secure Tunnel |
| FDDI | Fiber Distributed Data Interface |
| FTP | File Transfer Protocol |
| GUI | Graphical User Interface |
| HTTP | HyperText Transfer Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IOS | Internetwork Operating System |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| ISE | Identity Services Engine |
| ISP | Internet Service Providers |
| KDC | Key Distribution Center |
| LAN | Local Area Network |
| LAT | Local Area Transport |
| LEAP | lightweight extensible authentication protocol |
| MAB | MAC authentication Bypass |
| MAC | Media Access Control |
| MD5 | Message Digest 5 |
| MDA | MultiDomain Authentication mode |
| MIT | Massachusetts Institute of Technology |
| MITM | Man In The Middle |
| MS-CHAP | Microsoft Challenge Handshake Authentication Protocol |
| NAD | Network Access Device |
| NAS | Network Access Server |

| | |
|----------|---|
| NASI | NetWare Asynchronous Services Interface |
| NetBIOS | NETwork Basic Input Output System |
| ODBC | Open DataBase Connectivity |
| OTP | One-Time Password |
| PAC | Protected Access Credential |
| PAD | Packet Assembler / Disassembler |
| PAE | Port Access Entity |
| PAP | Password Authentication Protocol |
| PC | Personal Computer |
| PEAP | Protected Extensible Authentication Protocol |
| PKI | Public Key Infrastructure |
| PPP | Point to Point Protocol |
| RADIUS | Remote Authentication Dial-In User Service |
| RFC | Requests For Comments |
| RTC | Réseau Téléphonique Commuté |
| RTT | Round Trip Time |
| SGT | Security Group Tag |
| SLIP | Serial Line Internet Protocol |
| SMS | Short Message Service |
| SSH | Secure Shell |
| SVI | Switch Virtual Interface |
| TACACS + | Terminal Access Controller Access-Control System Plus |
| TCP | Transmission Control Protocol |
| TGS | Ticket Granting System |
| TLS | Transport Layer Security |

| | |
|------|---------------------------------|
| TTLS | Tunnel Transport Layer Security |
| UDP | User Datagram Protocol |
| VLAN | Virtual LAN |
| VPN | Virtual Private Network |
| VTY | Virtual Teletype |
| WEB | World Wide Web |
| WEP | Wired Equivalent Privacy |
| WiFi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |

INTRODUCTION GENERALE

Lors du déploiement d'un réseau filaire ou sans fil, des mesures de sécurité appropriées doivent être mises en place. L'utilisation des mots de passe pour accéder à des applications spécifiques n'est généralement pas suffisante pour empêcher les pirates d'accéder aux ressources de manière non autorisée et parfois paralysante. Afin de protéger adéquatement le réseau contre les intrus, il faut disposer de mécanismes utilisant des méthodes d'authentification éprouvées pour contrôler l'accès au réseau.

Dans les anciennes technologies de sécurité, les utilisateurs pouvaient accéder au réseau sans être authentifiés et juste en branchant leurs câbles à l'équipement d'accès au réseau. Donc quelle est la solution adéquate pour limiter et restreindre cet accès et remédier à ce problème ?

La gestion des accès par le modèle AAA et le protocole 802.1X a été proposée comme solution de sécurité pour assurer aux entreprises que seuls les utilisateurs autorisés ont accès à leurs données, et cela permet notamment de diminuer les risques d'intrusions et d'attaques ainsi que de protéger la confidentialité et l'intégrité de leurs données.

Ce mémoire est organisé comme suit :

Dans le premier chapitre, nous discuterons, en général, les concepts de base de la sécurité, ses objectifs ainsi les trois axes principaux de l'implémentation d'une bonne sécurité.

Puis nous verrons dans le deuxième chapitre, le modèle AAA qui permet d'offrir une authentification et une autorisation de l'utilisateur demandant l'accès au réseau ainsi de fournir le cadre pour l'accès aux réseaux et aux équipements à l'aide des protocoles RADIUS et TACACS+.

Ensuite, nous présenterons dans le troisième chapitre, le protocole 802.1X permettant une authentification centralisée des utilisateurs et une assurance de la dynamique et de la mobilité des accès au réseau.

Dans le quatrième et dernier chapitre intitulé « implémentation », nous passerons à la partie pratique de ce projet en implémentant les mécanismes présentés théoriquement dans les chapitres précédents.

CHAPITRE 1
FONDAMENTAUX DE LA
SECURITE

1.1. Introduction

Nous vivons dans un monde interconnecté où les actions individuelles et collectives ont le potentiel d'entraîner une bonté inspirante ou un préjudice tragique. L'objectif de la sécurité est de protéger chacun d'entre nous, notre économie, nos infrastructures essentielles et notre pays contre les dommages pouvant résulter d'une mauvaise utilisation, d'une compromission ou d'une destruction accidentelle ou intentionnelle des données ou des systèmes d'information.

Un équipement non protégé connecté à un réseau peut être infecté en quelques minutes. Et comme des informations confidentielles circulent dans les réseaux, la sécurité est devenue une préoccupation importante des utilisateurs et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques.

Ce chapitre présente les principes de base de la sécurité. Il commence par justifier son importance puis expliquer sa différence avec la cybersécurité. Ensuite, il cite ses objectifs principaux et ses équipes sans oublier sa terminologie nécessaire. Enfin, il explique les trois axes de l'implémentation d'une bonne sécurité.

1.2. Importance de la sécurité

À l'heure du "tout disponible partout tout de suite", le transport des données en dehors du domicile d'un particulier ou d'une entreprise est une réalité qui mérite que l'on s'interroge sur la sécurité des transmissions pour ne pas compromettre un système d'information. Que ce soit à l'échelle d'une entreprise, d'une multinationale ou à une plus petite échelle, la sécurité d'un système d'information prend plus ou moins d'importance selon la valeur que l'on confère à ces données [1].

De nos jours, les gens sont de plus en plus conscients de la sécurisation de leurs équipements connectés à Internet en raison d'événements de fuite de données, d'altération et d'utilisation abusive au cours des dernières années. La vulnérabilité du réseau et les nouvelles méthodes d'attaque augmentent de jour en jour, d'où l'évolution des techniques de sécurisation du réseau.

La sécurité des équipements et des réseaux est importante pour éviter [2] :

- La perte de données commerciales dans toute organisation ;
- L'interruption et l'utilisation abusive de la vie privée des personnes ;
- La menace et le compromis de l'intégrité des données de l'organisation ;
- La perte de réputation de l'organisation.

1.3. Cybersécurité vs. Sécurité de l'information

De nombreuses personnes confondent la sécurité de l'information traditionnelle avec la cybersécurité. Dans le passé, les programmes et les politiques de sécurité de l'information étaient conçus pour protéger la confidentialité, l'intégrité et la disponibilité des données dans les limites d'une organisation. Malheureusement, cela ne suffit plus. Les organisations sont rarement autonomes et le prix de l'interconnectivité est exposé aux attaques. Chaque organisation, quelle que soit sa taille ou sa situation géographique, est une cible potentielle.

La cybersécurité est le processus de protection des informations en empêchant, détectant et répondant aux attaques. Les programmes de cybersécurité reconnaissent que les organisations doivent être vigilantes, résilientes et prêtes à protéger et à défendre chaque connexion d'entrée et de sortie ainsi que les données organisationnelles où qu'elles soient stockées, transmises ou traitées.

Les programmes et les politiques de cybersécurité se développent et s'appuient sur les programmes traditionnels de sécurité de l'information, mais incluent également les éléments suivants [3] :

- Gestion et surveillance des cyber-risques ;
- Intelligence des menaces et partage d'informations ;
- Organisation tierce, gestion des dépendances logicielles et matérielles ;
- Réponse aux incidents et résilience.

1.4. Objectifs de la sécurité

Lors de la sécurisation d'un réseau, plusieurs principes de sécurité importants doivent être mis en place. Chaque mesure de sécurité mise en œuvre doit contribuer à la réalisation de l'un

des trois principes fondamentaux de la sécurité qui sont la confidentialité, l'intégrité et la disponibilité. On les appelle les qualités CID.

La plupart des problèmes de sécurité entraînent une violation d'au moins une facette de la triade CID. La compréhension de ces trois principes de sécurité contribuera à garantir que les contrôles et les mécanismes de sécurité mis en œuvre protègent au moins l'un de ces principes.

Chaque contrôle de sécurité mis en place par une organisation répond au moins à l'un des principes de sécurité de la triade CID. Comprendre comment contourner ces principes de sécurité est aussi important que comprendre comment les fournir [4].



Figure 1.1 : Triade CID.

1.4.1. Confidentialité

La confidentialité est l'exigence de ne pas mettre à disposition ou divulguer des informations privées ou confidentielles à des personnes, des entités ou des processus non autorisés. Elle repose sur trois concepts généraux, comme le montre la figure 1.2.

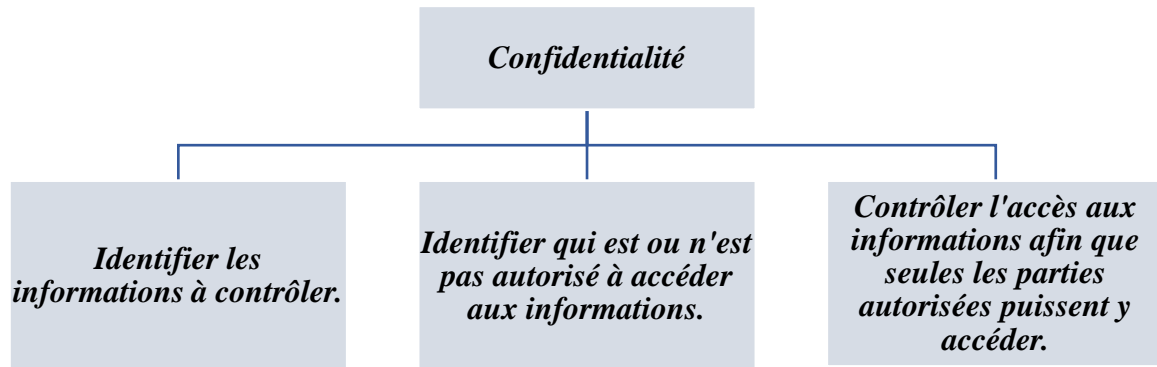


Figure 1.2 : Concepts généraux de la confidentialité.

Voici des exemples de mécanismes de sécurité conçus pour préserver la confidentialité[3]:

- Contrôles d'accès logiques et physiques ;
- Cryptage ;
- Vues de la base de données ;
- Routage du trafic contrôlé.

Dans le cadre de la confidentialité, le niveau de sensibilité des données doit être déterminé avant la mise en place des contrôles d'accès. Les données avec un niveau de sensibilité plus élevé auront plus de contrôles d'accès que les données à un niveau de sensibilité inférieur [4].

1.4.2. Intégrité

L'intégrité est la capacité d'assurer qu'un système et ses données n'ont pas été modifiés ou compromis. Elle garantit que les données sont une représentation exacte des données sécurisées d'origine (les informations reçues du destinataire sont exactement les informations envoyées à l'origine par l'expéditeur).

L'intégrité et la confidentialité sont interdépendantes. Si un mot de passe d'utilisateur est divulgué à la mauvaise personne, cette dernière pourrait à son tour manipuler, supprimer ou détruire des données après avoir accédé au système avec le mot de passe qu'il a obtenu [3].

Il s'agit d'un processus de validation du message ou de la communication entre deux utilisateurs finaux. Si quelqu'un modifie le message en reniflant les paquets, la valeur de vérification d'intégrité notifiant que la communication a été modifiée. Les codes d'authentification de hachage et de message sont utilisés pour valider l'intégrité d'un message. La comparaison de la valeur de hachage reçue et calculée détermine si la communication a été

modifiée ou non [2]. Un autre exemple de contrôle est la liste de contrôle d'accès (ACL) qui contribue à assurer l'intégrité [4].

1.4.3. Disponibilité

Le dernier composant de la triade CID est la disponibilité, qui stipule que les systèmes, les applications et les données doivent être disponibles pour les utilisateurs autorisés en cas de besoin et sur demande. La productivité des utilisateurs peut être considérablement affectée et les entreprises peuvent perdre beaucoup d'argent si les données ne sont pas disponibles [3]. Cela devient une grave préoccupation pour la réputation de l'organisation, ce qui entraîne une perte financière et l'enregistrement de certaines données importantes.

| CID | Risque | Contrôle |
|------------------------|---|---|
| Confidentialité | Perte d'intimité. Accès non autorisé à l'information. Vol d'identité. | Chiffrement. Authentification. Contrôle d'accès. |
| Intégrité | Les informations ne sont plus fiables ou précises. Fraude. | Maker / Checker. Qualité d'assurance. Journaux d'audit. |
| Disponibilité | Perturbation des activités. Perte de confiance du client. Perte de revenus. | Continuité de l'activité. Plans et tests. Stockage de sauvegarde. Capacité suffisante. |

Tableau 1.1 : Les protections contre les risques en implémentant la triade CID [2].

1.5. Terminologie de la sécurité

1.5.1. Terminologie générale

Avant de lancer une discussion significative sur la sécurité du réseau, il est d'abord nécessaire de définir quelques termes fondamentaux relatifs à la sécurité du réseau. Ces termes sont le fondement de toute discussion sur la sécurité du réseau et les éléments utilisés pour mesurer la sécurité d'un réseau [5].

- **Une ressource :** Tout objet qui a une valeur pour une organisation et qui doit être protégé.

- **Une vulnérabilité** : C'est une faiblesse d'un système qui pourrait être exploité par une menace.
- **Une menace** : Un danger potentiel pour une ressource ou pour le fonctionnement du réseau.
- **Une attaque** : C'est une action prise pour nuire à une ressource.
- **Un risque** : C'est la possibilité de perte, altération, destruction ou d'autres conséquences négatives de la ressource d'une organisation. Le risque peut naître d'une seule ou plusieurs menaces ou de l'exploitation d'une vulnérabilité.

Un risque = Une ressource + Une menace + Une vulnérabilité.

- **Contre-mesure** : Une protection qui atténue une menace potentielle ou un risque [6].
- **Attaquant** : La personne ou le processus qui lance une attaque. Cela peut être synonyme de menace.
- **Exploit** : L'instanciation d'une vulnérabilité ; quelque chose qui peut être utilisée pour une attaque. Une seule vulnérabilité peut conduire à plusieurs exploits, mais toutes les vulnérabilités ne peuvent pas avoir un exploit (par exemple, des vulnérabilités théoriques).
- **Cible** : La personne, l'entreprise ou le système qui est directement vulnérable et touché par l'exploit. Certains exploits ont des impacts multiples, avec à la fois des cibles primaires (principales) et des cibles secondaires (accessoires).
- **Défenseur** : Personne ou processus qui atténue ou empêche une attaque.
- **Compromis** : Exploitation réussie d'une cible par un attaquant [7].

1.5.2. Codes malveillants

Les types courants de codes malveillants qui peuvent être utilisés par les pirates sont les suivants :

- **Virus** : C'est un programme qui s'attache à un logiciel pour exécuter une fonction spécifique non souhaitée sur ordinateur. La plupart des virus nécessitent une activation par l'utilisateur. Cependant, ils peuvent également être programmés pour éviter la détection ;
- **Worms** : Ce sont des programmes autonomes qui exploitent des vulnérabilités connues dans le but de ralentir un réseau. Ils ne nécessitent pas l'activation de l'utilisateur, ils se dupliquent et tentent d'infecter d'autres équipements dans le réseau ;

- **Spyware** : Ce sont des logiciels espions qui sont généralement utilisés dans le but d'influencer l'utilisateur pour acheter certains produits ou services. Les spywares, en général, ne se propagent pas automatiquement, mais ils s'installent sans autorisation. Ils sont programmés pour :
 - Recueillir des informations personnelles sur les utilisateurs ;
 - Surveiller l'activité de navigation sur le Web pour détecter les caprices de l'utilisateur ;
 - La redirection des requêtes HTTP vers des sites de publicité préétablis.
- **Adware** : Réfère à tout logiciel qui affiche des publicités, sans l'autorisation de l'utilisateur, parfois sous la forme de fenêtres pop-up ;
- **Scaryware** : Réfère à une classe de logiciels utilisés pour convaincre les utilisateurs ayant leurs systèmes infectés par des virus, et leur proposer une solution dans le but de vendre des logiciels ;
- **Trojan horse** : C'est un programme ayant un comportement apparemment utile à l'utilisateur et un comportement caché malveillant conduisant généralement à un accès à la machine sur laquelle il est exécuté ;
- **Ransomwares** : C'est un programme conçu pour bloquer l'accès à un système informatique, par le chiffrement de contenu, jusqu'à ce qu'une somme d'argent soit payée.

1.5.3. Types de hackers

On distingue différents types de hackers existant dans le domaine informatique :

- **Les hackers aux chapeaux blancs « *white hat hackers* »** : Ce sont des personnes qui réalisent des audits de sécurité afin d'assurer la protection des systèmes d'information d'une organisation ;
- **Les hackers aux chapeaux noirs « *black hat hackers* »** : Ce sont des personnes expérimentées qui agissent à des fins illégales en pratiquant le vol de données, le piratage des comptes, l'infiltration dans les systèmes, etc. ;
- **Les hackers aux chapeaux gris « *grey hat hackers* »** : C'est un mélange de « white hat » et de « black hat » ;
- **Les hackers aux chapeaux bleus « *blue hat hackers* »** : Ce sont des testeurs de bogues pour assurer le bon fonctionnement des applications [6].

1.6. Equipes de sécurité

On distingue différentes équipes de sécurité existant dans le domaine informatique :

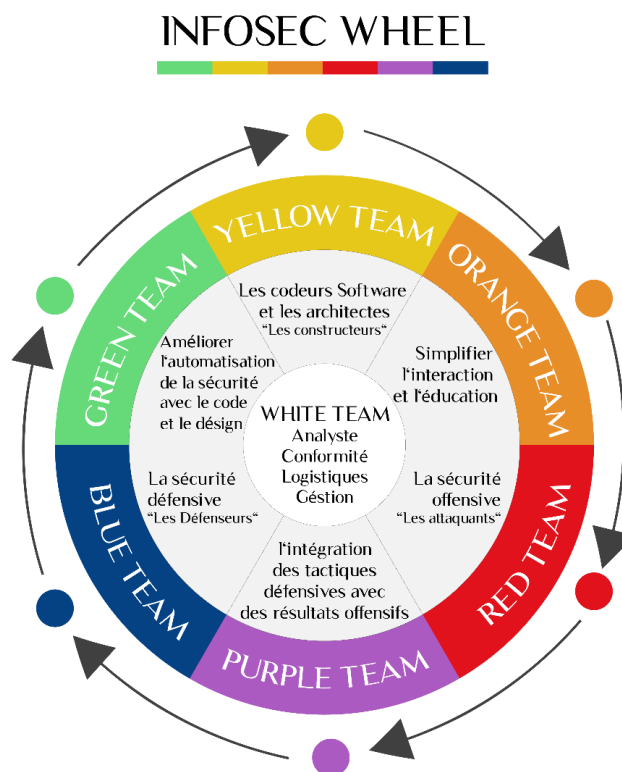


Figure 1.3 : Roue chromatique des équipes de sécurité.

1.6.1. Equipe jaune

Elle constitue l'équipe des constructeurs. Il s'agit de l'équipe chargée de développer le système de sécurité d'une organisation. Il peut s'agir d'un service informatique interne ou d'un fournisseur de solutions de sécurité tiers. Il peut également s'agir de développeurs d'applications ou de logiciels, censés d'assurer que leurs applications sont correctement sécurisées.

1.6.2. Equipe bleue

Il s'agit de l'équipe des défenseurs. C'est le groupe chargé de la protection du système créé par l'équipe jaune. Ils sont responsables de la mise en œuvre de la sécurité défensive, du contrôle des dommages et de la réponse aux incidents. Ils peuvent également jouer le rôle de chasseurs de menaces, de gardes de sécurité opérationnels et d'experts en criminalistique des

données. Les équipes bleue et jaune peuvent ne pas être les mêmes, car cela ira à l'encontre de l'objectif d'avoir différentes entités dédiées à des fonctions spécifiques. En outre, ils ne peuvent pas avoir de point de fusion (dans la roue chromatique) s'ils sont identiques.

1.6.3. Equipe rouge

Elle constitue l'équipe des attaquants. Il s'agit de l'équipe chargée de réaliser un « piratage éthique » sur une organisation. Ils sont autorisés à faire tout ce qui est nécessaire pour violer les défenses de sécurité. Ils effectuent plus que de simples tests de pénétration. Ils peuvent également effectuer des tests de conformité, des tests de boîte noire, l'analyse des applications Web, l'ingénierie sociale et une foule d'autres attaques. Tout comme les équipes jaune et bleue, l'équipe rouge ne peut pas être la même que les deux autres équipes.

1.6.4. Equipe violette

Le violet, étant la couleur entre le rouge et le bleu, représente un changement de mentalité, passant d'un pur défenseur à une équipe qui prend également le point de vue de l'attaquant. Des activités conjointes entre les équipes bleue et rouge peuvent être entreprises pour réfléchir sur les stratégies et les approches utilisées pour améliorer la sécurité d'une organisation. Les deux équipes se collaborent pour améliorer les résultats des campagnes de l'équipe rouge et également pour renforcer les capacités de l'équipe bleue.

1.6.5. Equipe orange

L'orange, évidemment la tarte entre le rouge et le jaune, c'est d'avoir des interactions entre les équipes rouge et jaune. Tout comme la façon dont l'équipe jaune assume la perspective de l'équipe bleue dans l'intersection verte, le changement de mentalité orange consiste à anticiper les attaques qui seront lancées par l'équipe rouge. Dans le même temps, l'équipe rouge étudie et prédit comment l'équipe jaune va construire le système et les points critiques qui seront probablement manqués pour faire place aux vulnérabilités. Dans le cadre de la collaboration orange, l'équipe rouge devrait partager et revoir ses conclusions avec l'équipe jaune.

1.6.6. Equipe verte

Le vert, étant la couleur entre le jaune et le bleu, symbolise un changement de mentalité de la part de l'équipe de constructeurs. Cela signifie que les créateurs du système de sécurité

soient mis à la place de l'équipe de défenseurs. Ils doivent apprendre comment l'équipe bleue développe les défenses qu'ils ajoutent au système, afin qu'ils puissent les ajouter au fur et à mesure de leur construction [8].

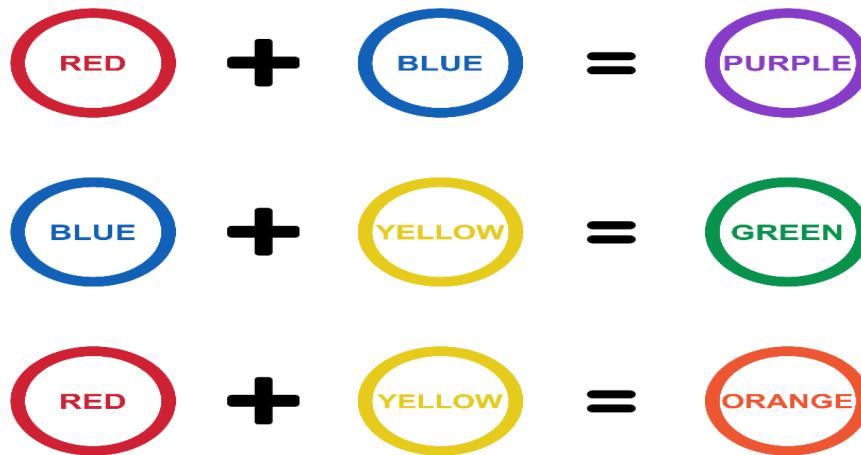


Figure 1.4 : Charte de création de couleurs secondaires.

1.7. Axes de sécurité

La sécurité informatique est souvent divisée en trois grandes catégories bien distinctes :

- Sécurité physique et environnementale ;
- Sécurité administrative ;
- Sécurité technique.

Ces trois grandes catégories définissent les objectifs principaux de l'implémentation d'une bonne sécurité. Ces contrôles regroupent des sous-catégories examinant plus précisément les différents contrôles et la manière de les mettre en œuvre.

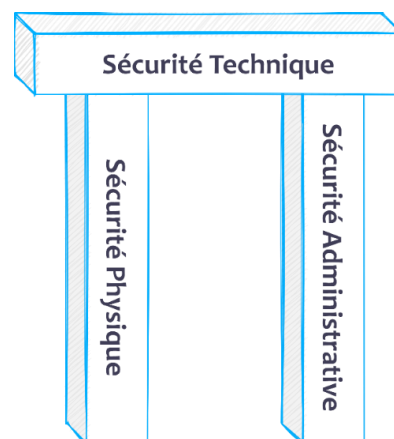


Figure 1.5 : Fondamentaux de la sécurité.

1.7.1. Sécurité physique et environnementale

La sécurité physique correspond à l'implémentation de mesures de sécurité dans une structure définie utilisées pour dissuader ou empêcher l'accès non-autorisé à des données confidentielles. Parmi les exemples de contrôles physiques et environnementaux figurent :

- Les caméras de surveillance ;
- Les systèmes d'alarme basés sur les changements au niveau des mouvements ;
- Les agents de sécurité ;
- Les photos d'identité ;
- Les portes en acier verrouillées à l'aide d'une clé ou d'un bouton ;
- La biométrie (y compris les empreintes digitales, la voix, le visage, l'iris, l'écriture et d'autres méthodes automatisées utilisées pour reconnaître des individus) [9] ;
- Les systèmes de protection climatique, pour maintenir une température et une humidité adéquates, en plus d'alerter le personnel en cas d'incendie [10].

1.7.2. Sécurité administrative

La sécurité administrative est principalement axée sur les politiques, elle définit les facteurs humains de la sécurité. Elle fait appel à tous les niveaux de personnel présents au sein d'une société et définit quels utilisateurs ont accès à quelles ressources / informations et cela en fonction des éléments suivants :

- Formation et sensibilisation ;
- Préparation en cas de catastrophe et plans de récupération ;
- Recrutement de personnel et stratégies de séparation ;
- Inscription et traçabilité du personnel [9] ;
- Journalisation des modifications de configuration ;
- Filtrage correct des employés (par exemple, effectuer des vérifications des antécédents criminels) ;
- Gestion des changements par un système qui informe les parties appropriées des changements appliqués [10].

1.7.3. Sécurité technique

La sécurité technique utilise la technologie comme élément de base dans le contrôle de l'accès et de l'utilisation de données confidentielles contenues dans une structure physique ou sur un réseau. Les contrôles techniques ont un vaste champ d'action et englobent parmi leurs technologies :

- Le cryptage ;
- Les cartes à mémoire ;
- L'authentification de réseau ;
- Les listes de contrôle d'accès (ACLs) ;
- Les logiciels de vérification de l'intégrité des fichiers [9] ;
- Les techniques de sécurité (par exemple, pare-feu, IPS et VPN) ;
- Les applications d'autorisation (par exemple, serveurs RADIUS ou TACACS +, Mots de passe à usage unique (OTP) et scanners de sécurité biométriques).

Les contrôles administratifs, physiques et techniques individuels peuvent être classés comme l'un des types de contrôle suivants :

- Préventif : Un contrôle préventif tente d'empêcher l'accès aux données ou à un système.
- Dissuasif : Un contrôle dissuasif tente d'empêcher un incident de sécurité en influençant l'attaquant potentiel à ne pas lancer d'attaque.
- DéTECTIF : Un contrôle détectif peut détecter quand l'accès aux données ou à un système se produit.

Chaque catégorie de contrôle (administratif, physique et technique) contient des composants pour ces types de contrôles (préventif, dissuasif et détectif). Par exemple, un contrôle de détection spécifique pourrait être l'un des suivants :

- Un contrôle administratif, tel qu'une entrée de journal de bord requise par une politique de sécurité ;
- Un contrôle physique, comme une alarme qui retentit lorsqu'une porte particulière est ouverte ;
- Un contrôle technique, tel qu'un équipement IPS générant une alerte [10].

« Nous ne pouvons jamais parler de la sécurité technique sans avoir une sécurité physique et administrative »

1.8. Conclusion

La vulnérabilité du réseau et les nouvelles méthodes d'attaque augmentent de jour en jour, d'où l'évolution des techniques de sécurisation du réseau. Puisque le risque nul d'être piraté n'existe pas, la sécurité doit être itérative de manière à rester efficace et pour l'atteindre quels que soit les obstacles prévus ou imprévus.

Ces techniques sont conçues pour protéger la confidentialité, l'intégrité et la disponibilité des données et ceci par la mise en place des contres mesures administratifs, physiques et techniques et par la gestion des accès qui permet de garantir que les utilisateurs ne puissent accéder aux ressources et aux informations auxquelles ils ne sont pas autorisés à accéder en se basant sur l'authentification, l'autorisation et la traçabilité.

Au cours du prochain chapitre, nous présenterons le modèle AAA qui permet de renforcer la sécurité du réseau en expliquant chacune de ses parties et ses protocoles les plus utilisés.

CHAPITRE 2
MODELE AAA

2.1. Introduction

L'authentification, l'autorisation et la traçabilité (AAA) est un ensemble de concepts primaires de sécurité informatique courants qui aide à contrôler l'accès aux réseaux. Ce modèle est utilisé quotidiennement pour protéger les données et les systèmes contre les dommages intentionnels ou même non intentionnels. C'est un moyen qui permet de contrôler qui sont autorisés à accéder au réseau (authentification), ce qu'ils peuvent faire pendant qu'ils y sont (autorisation) et de vérifier les actions qu'ils ont effectuées lors de l'accès au réseau (traçabilité).

Ce chapitre présente le modèle AAA et ses protocoles les plus utilisés. Il commence par expliquer l'authentification, ses modes, ses méthodes, ses facteurs et ses protocoles. Il décrit ensuite l'autorisation et ses méthodes, les niveaux de privilège et l'accès CLI basé sur les rôles. Ensuite, le chapitre définit la traçabilité et ses méthodes. Enfin, il explore les protocoles AAA avec une comparaison entre eux.

2.2. Authentification

2.2.1. Définition

L'authentification est un processus qui consiste à prouver une identité au système en utilisant une méthode d'authentification comme un nom d'utilisateur et un mot de passe. Cela a également pour but de déterminer si l'utilisateur est la même personne qu'il prétend être ou non.

Elle est utilisée dans tous les systèmes, pas seulement dans les réseaux informatiques. Dans le système bancaire, il faut prouver l'identité en entrant le mot de passe avant d'effectuer la transaction. De même, si un administrateur réseau a besoin d'accéder à un équipement réseau et souhaite apporter des modifications, une sorte d'authentification doit être définie sur l'équipement.

La première solution pratique et la moins utilisable, serait de définir localement la base de données des mots de passe et des noms d'utilisateur à l'intérieur de l'équipement. La deuxième option serait d'utiliser un serveur centralisé comme Cisco ACS ou ISE. Dans les équipements Cisco, on peut utiliser la combinaison des deux options en définissant une liste de méthodes, qui indique la liste des méthodes préférées pour l'authentification. Si une option n'est pas disponible, la deuxième option sera utilisée et ainsi de suite [2].

2.2.2. Modes d'authentification

Il existe deux modes d'authentification sur les équipements réseaux, le mode d'authentification locale et le mode d'authentification basée sur un serveur « centralisée ».

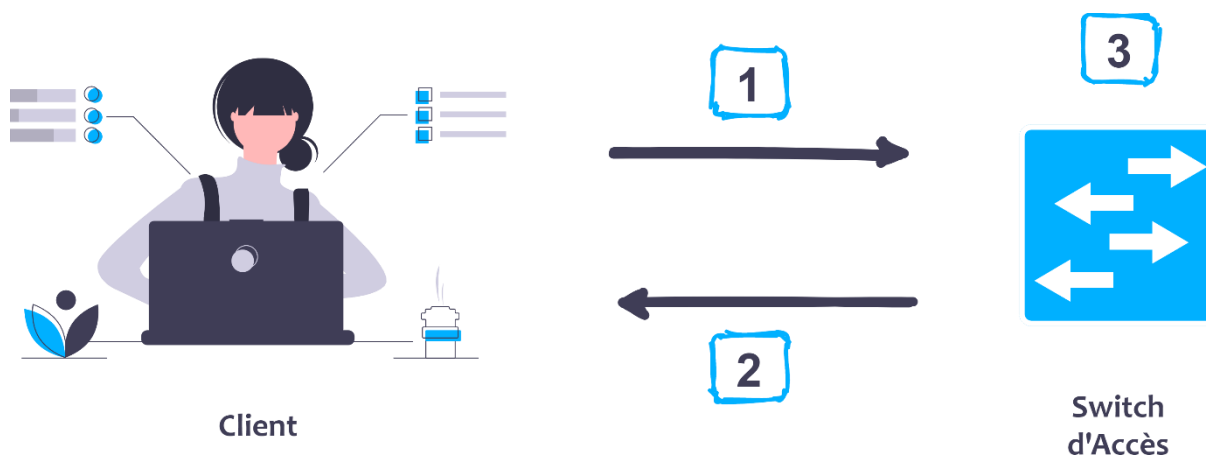
Pour le premier mode, les données d'authentification (nom d'utilisateurs, mot de passe, etc.) sont directement implémentées à l'intérieur de l'équipement réseau, il n'y a alors une interaction qu'entre le client et l'équipement qui stocke lui-même ces informations.

Pour le deuxième, il utilise un serveur extérieur pour stocker les données d'authentification et lorsqu'un utilisateur essaie de s'authentifier, l'équipement réseau consulte la base de données du serveur pour permettre l'accès à l'utilisateur [11].

2.2.2.1. Authentification locale

L'accès administratif aux lignes console, vty et AUX peut être authentifié localement à l'aide des éléments suivants :

- **Mots de passe de ligne « *line passwords* »** : facile à mettre en œuvre à l'aide des commandes de mot de passe « *password* » et de connexion « *login* », mais c'est la méthode la moins sécurisée et très vulnérable aux attaques par brute-force. Il y a également une perte de responsabilité car le mot de passe peut être partagé.
- **Authentification locale « *local authentication* »** : mise en œuvre pour améliorer la sécurité, car l'utilisateur doit fournir un nom d'utilisateur et un mot de passe, qui sont comparés aux entrées de la base de données locale de l'équipement.
- **AAA local « *local AAA* »** : également appelée AAA autonome « *self-contained AAA* », cette méthode est similaire à l'authentification locale mais elle peut fournir des méthodes d'authentification de secours [12].

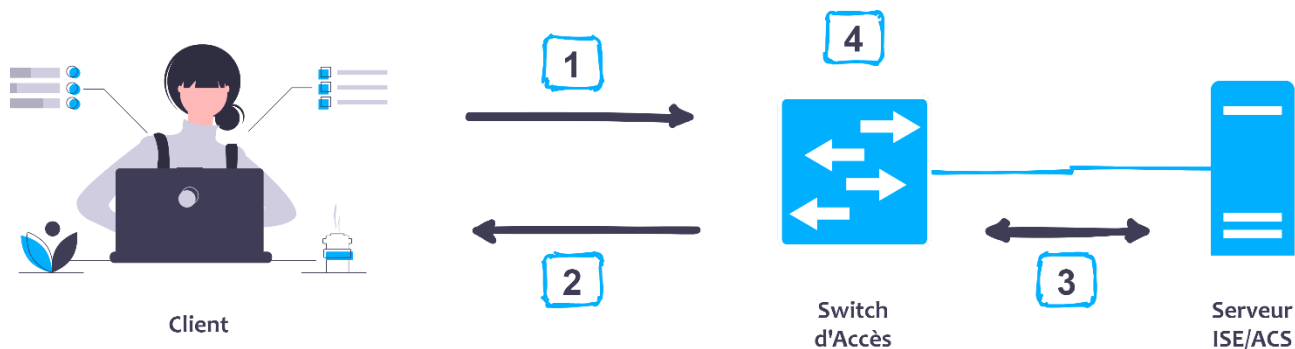
Exemple d'authentification locale :*Figure 2.1 : Authentification locale.*

1. Le client établit une connexion avec le switch d'accès ;
2. Le switch d'accès demande au client un nom d'utilisateur et un mot de passe ;
3. Le switch d'accès authentifie le nom d'utilisateur et le mot de passe à l'aide de la base de données locale et l'utilisateur est autorisé à accéder au réseau en fonction des informations contenues dans la base de données locale [13].

2.2.2.2. Authentification basée sur un serveur « centralisée »

C'est une méthode plus évolutive consistant à utiliser une solution basée sur un serveur tel que :

- Cisco Secure Access Control Server (ACS).
- Cisco Identity Services Engine (ISE) [12].

Exemple d'authentification centralisée :*Figure 2.2 : Authentification centralisée.*

1. Le client établit une connexion avec le switch d'accès ;
2. Le switch d'accès demande au client un nom d'utilisateur et un mot de passe ;
3. Le switch d'accès authentifie le nom d'utilisateur et le mot de passe à l'aide d'un serveur distant ;
4. L'utilisateur est autorisé à accéder au réseau en fonction des informations contenues dans le serveur [13].

2.2.3. Méthodes d'authentification

Il existe trois méthodes d'authentification : authentification par connaissance (quelque chose que l'utilisateur sait), authentification par possession (quelque chose qu'un utilisateur possède) et authentification par l'héritage des caractéristiques (ce que l'utilisateur est).

2.2.3.1. Authentification par connaissance

L'authentification par connaissance est une méthode consistant à fournir un secret par un utilisateur et qui n'est connu que par lui. Un exemple de cette méthode serait un utilisateur fournissant un mot de passe, un code de numéro d'identification personnel (PIN) ou répondant à des questions de sécurité.

L'inconvénient de l'utilisation de cette méthode est qu'une fois les informations sont perdues ou volées (par exemple, si le mot de passe d'un utilisateur est volé), un attaquant peut s'authentifier avec succès. Actuellement, il ne passe pas un jour sans avoir entendu parler d'une nouvelle faille chez les fournisseurs de services, les services cloud et les entreprises de réseaux sociaux.

L'authentification par mot de passe est la méthode d'authentification la plus couramment utilisée. Sa force est en fonction de sa longueur, de sa complexité et de son imprévisibilité. S'il est facile à deviner ou à déconstruire, il est vulnérable aux attaques. Une fois connu, il n'est plus utile comme outil de vérification. Le défi consiste à amener les utilisateurs à créer, garder secrets et mémoriser des mots de passe sécurisés. Les mots de passe faibles peuvent être découverts en quelques minutes, voire quelques secondes.

2.2.3.2. Authentification par propriété ou possession

Avec ce type d'authentification, l'utilisateur est invité à fournir la preuve qu'il possède. Par exemple, un système peut exiger qu'un employé utilise un badge pour accéder à une

installation. D'autres exemples d'authentification par propriété est l'utilisation d'un jeton, d'une carte à puce, d'une carte mémoire ou d'un mot de passe à usage unique (OTP). Similaire à la méthode précédente, si un attaquant est capable de voler l'objet utilisé pour l'authentification, il pourra accéder avec succès au système.

Un mot de passe à usage unique est un ensemble de caractéristiques qui peuvent être utilisées pour prouver une seule fois l'identité d'un sujet. Étant donné que l'OTP n'est valide que pour un seul accès, s'il est capturé, un accès supplémentaire serait automatiquement refusé. Les OTP sont généralement fournis via un périphérique de jeton matériel ou logiciel. Le jeton affiche le code, qui doit ensuite être saisi sur l'écran d'authentification. En variante, l'OTP peut être délivré par un courrier électronique, un message texte ou un appel téléphonique à une adresse ou un numéro de téléphone prédéterminés.

Une carte mémoire est un mécanisme d'authentification qui contient des informations d'utilisateur dans une bande magnétique et repose sur un lecteur pour traiter ces informations. L'utilisateur insère la carte dans le lecteur et entre un numéro d'identification personnel. Généralement, le code PIN est haché et stocké sur la bande magnétique. Le lecteur hache le code PIN saisi et le compare à la valeur sur la carte elle-même. Un exemple familier de ceci est une carte bancaire ATM.

Une carte à puce fonctionne de la même manière qu'une carte mémoire sauf qu'au lieu d'une bande magnétique, il dispose d'un microprocesseur et de circuits intégrés. L'utilisateur insère la carte dans un lecteur, qui possède des contacts électriques qui s'interfacent avec la carte et alimentent le processeur. L'utilisateur entre un code PIN qui déverrouille les informations. La carte peut contenir la clé privée de l'utilisateur, générer un OTP ou répondre à un défi.

2.2.3.3. Authentification par caractéristique

Un système qui utilise l'authentification par caractéristique authentifie l'utilisateur à base d'une caractéristique physique ou comportementale, parfois appelée attribut biométrique. Les caractéristiques physiques, physiologiques ou comportementales les plus utilisées sont les suivantes :

- Empreintes digitales ;
- Reconnaissance faciale ;

- Reconnaissance vocale ;
- Rétine et iris ;
- Informations sanguines et vasculaires ;
- Signature dynamique (comportementale).

Un système basé sur une signature dynamique authentifierait un utilisateur en lui demandant d'écrire sa signature et en comparant ensuite le modèle de signature à un enregistrement dans le système. Étant donné que la façon dont une personne signe son nom diffère légèrement à chaque fois, le système doit être conçu de manière à ce que l'utilisateur puisse toujours s'authentifier, même si la signature et le modèle ne sont pas exactement ce qui est dans le système [3].

2.2.4. Facteurs d'authentification

2.2.4.1. Authentification à deux facteurs

La forme traditionnelle d'authentification est l'authentification à un seul facteur qui consiste à entrer un mot de passe correspondant au nom d'utilisateur pour accéder aux ressources autorisées. De nos jours, cette méthode est considérée comme peu sécurisée pour de nombreuses raisons. L'une de ces principales raisons est qu'il est facile d'être compromis si le mot de passe est utilisé plusieurs fois par jour.

La sécurité monocouche n'est alimentée par aucune couche supplémentaire, ce qui signifie que si le mot de passe est compromis, le contrôle de ressources sera perdu et des cybercriminels non autorisés peuvent facilement pénétrer dans ses ressources. La solution à ce problème est l'authentification à deux facteurs et l'authentification multi facteurs.

L'authentification à deux facteurs est également appelée authentification à dual facteurs ou en deux étapes. Dans ce processus, une couche de sécurité supplémentaire est obtenue pour accéder aux ressources. Lorsque l'utilisateur entre son nom et son mot de passe, il est invité à entrer un code d'accès secret. Ce code est couramment envoyé par un SMS ou un appel automatique sur son téléphone mobile.

Le code d'accès est un code unique généré automatiquement par le serveur désigné. Ce n'est qu'un code à usage unique. Ce code est également sensible au temps, ce qui signifie que le code expire après un certain temps. De cette façon, le code ne peut être compromis par aucun utilisateur malveillant.

Dans la dernière technologie de génération de code d'accès, les codes peuvent être générés et envoyés par e-mail, texte, appel automatique, liens Web et par d'autres moyens. Dans l'expression faciale d'authentification à deux facteurs, une entrée biométrique ou d'autres gestes corporels peuvent également être utilisés. Ainsi, l'accès aux ressources devient hautement sécurisé et sans compromis en adoptant une authentification à deux facteurs.

L'authentification à deux facteurs dépend de différentes méthodes d'authentification utilisées comme deuxième couche du facteur de sécurité. Quelques-unes de ces méthodes sont expliquées dans la section précédente (authentification par connaissance, authentification par possession et authentification par caractéristique).

2.2.4.2. Authentification multi facteurs

L'authentification à deux facteurs améliore la sécurité de l'accès aux ressources, mais le niveau de sécurité dont une donnée critique a besoin n'est pas encore suffisant. Certains problèmes importants ont été trouvés associés à la sécurité de l'authentification à deux facteurs. Par exemple, en 2011, la société de sécurité RAS a annoncé qu'un grand nombre de comptes importants à deux facteurs ont été compromis. Dans cette attaque, les jetons d'authentification sécurisés ont été piratés par des cybercriminels.

Ainsi, le processus de récupération des comptes peut également être menacé car il utilise des réinitialisations de paramètres de compte. Donc, il y a certains problèmes avec l'authentification à deux facteurs. Pour améliorer encore la sécurité de l'authentification d'accès, un système d'authentification multi facteurs est utilisé. Ce système se compose de facteurs d'authentification en plusieurs étapes.

L'authentification multi facteurs est basée sur trois facteurs ou plus. Les trois principaux facteurs utilisés sont connus comme :

- Ce que vous savez (connaissance) (What you know) ;
- Ce que vous êtes (caractéristique) (What you are) ;
- Ce que vous avez (possession) (What you have) [14].

2.2.5. Règles des mots de passe

2.2.5.1. Mot de passe vs. Phrase secrète

➤ Mot de passe

Un mot de passe est une combinaison secrète de lettres, de chiffres et / ou de caractères que seul l'utilisateur doit connaître pour accéder à un système dont l'accès est limité et protégé (pas forcément constituée que de chiffres et de lettres, avec ou sans signification).

Le mot de passe est le type d'authentification le plus couramment utilisé aujourd'hui. Il est basé sur quelque chose que vous savez que personne d'autre ne sait. Malgré leur utilisation répandue, les mots de passe n'offrent qu'une faible protection [15].

➤ Phrase secrète

Une phrase secrète est une combinaison de mot de passe et de phrase et se compose de plusieurs mots et / ou caractères spéciaux utilisés pour contrôler l'accès à un système, un programme ou des données. Parce qu'elle est plus complexe qu'un simple mot de passe, elle est plus difficile à deviner ou à craquer, et elle ajoute un niveau de sécurité supplémentaire aux clés de cryptage les plus importantes.

La séquence de caractères choisie, pour créer une phrase secrète pour accéder à un système de sécurité, est l'une des premières décisions prises par l'utilisateur du système. C'est aussi le maillon le plus faible de presque tous les systèmes informatiques. Les êtres humains prennent de mauvaises décisions en ce qui concerne les phrases secrètes, et quelle que soit la sécurité du système informatique, une mauvaise phrase secrète peut causer d'énormes problèmes [16].

| Mot de passe | Phrase secrète |
|---|--|
| Il comporte moins de caractères | Elle comporte plus de caractères |
| Il peut être significatif ou non | Elle doit être significative |
| Difficile à retenir | Facile à retenir |
| Facile à craquer | Difficile à craquer |
| Il peut contenir le nom d'utilisateur, date de naissance, ... | Elle ne doit pas contenir le nom d'utilisateur, date de naissance, ... |

Tableau 2.1 : Comparaison entre mot de passe et phrase secrète.

2.2.5.2. Types d'attaque par mot de passe

Une attaque par mot de passe est une attaque qui tente de découvrir les mots de passe des utilisateurs. Les deux menaces de mot de passe les plus populaires sont les attaques par brute-force et les attaques par dictionnaire.

2.2.5.2.1. Attaque par brute-force

Une attaque par brute-force consiste à tester toutes les combinaisons possibles de lettres, de chiffres et de caractères pour casser un mot de passe. Elle effectue des recherches de mot de passe jusqu'à ce qu'un mot de passe correct soit trouvé [4].

Ces combinaisons sont utilisées pour créer des résumés de candidats qui sont ensuite comparés à ceux du fichier de résumé volé. C'est la méthode la plus lente et la plus difficile à réaliser mais la plus approfondie [15].

Une attaque par brute-force est plus efficace si les mots de passe sont courts et ne sont que des lettres ou des chiffres, et non une combinaison des deux. Plus le mot de passe est long, plus il faut d'efforts pour essayer toutes les combinaisons possibles. Faire d'un mot de passe un mélange de lettres, de chiffres et de caractères spéciaux augmente la difficulté de manière exponentielle [5].

Il existe deux grandes catégories d'attaques par brute-force :

- Attaques par brute-force en ligne : Dans ce type d'attaque, l'attaquant essaie de se connecter directement à une application ou à un système en utilisant de nombreuses combinaisons différentes d'informations d'identification. Ces attaques sont faciles à détecter car un grand nombre de tentatives par un attaquant peut être inspecté facilement;
- Attaques par brute-force hors ligne : Dans ce type d'attaque, l'attaquant peut accéder à des données chiffrées ou à des mots de passe hachés. Ces attaques sont plus difficiles à prévenir et à détecter que les attaques en ligne. Cependant, les attaques hors ligne nécessitent beaucoup plus d'efforts de calcul et de ressources de la part de l'attaquant[3].

2.2.5.2.2. Attaque par dictionnaire

Une attaque par dictionnaire se produit lorsque des attaquants utilisent un dictionnaire de mots courants pour découvrir des mots de passe. Un programme automatisé utilise le hachage

du mot du dictionnaire et compare cette valeur de hachage aux entrées du fichier de mots de passe système (attaque pré-image). Bien que le programme soit livré avec un dictionnaire, les attaquants utilisent également des dictionnaires supplémentaires qui se trouvent sur Internet. Il faut mettre en œuvre une règle de sécurité qui stipule qu'un mot de passe ne doit pas être un mot trouvé dans le dictionnaire pour se protéger contre ces attaques [4].

Les attaques basées sur des dictionnaires sont beaucoup plus efficaces que l'approche par brute-force. De toute évidence, la méthode basée sur le dictionnaire est plus efficace contre les mots de passe qui sont des mots, des noms ou des termes courants ou connus [5].

2.2.5.3. Recommandations

R1 : Utilisez un mot de passe long de 10 à 15 caractères.

R2 : Utilisez une combinaison de caractères minuscules et majuscules.

R3 : Utilisez au moins un ou plusieurs symboles / caractères spéciaux à un endroit aléatoire.

R4 : Utilisez au moins un ou plusieurs numéros à différents endroits.

R5 : Ne partagez jamais votre mot de passe avec d'autres [14].

R6 : N'utilisez pas de mots de passe composés de mots du dictionnaire ou de mots phonétiques.

R7 : Ne répétez pas les caractères (xxx) et n'utilisez pas de séquences (abc, 123, etc.) [15].

R8 : Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 30 jours est un bon compromis pour les systèmes contenant des données sensibles.

R9 : Choisissez un mot de passe qui n'est pas lié à votre identité et vos informations personnelles (mot de passe composé d'un nom de société, d'une date de naissance, etc.).

R10 : Ne demandez jamais à une personne de vous créer un mot de passe.

R11 : Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.

R12 : Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.

R13 : Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.

R14 : Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (par exemple : en ligne sur internet), encore moins sur un papier facilement accessible.

R15 : Configurez les logiciels, y compris votre navigateur Web, pour qu'ils ne se souviennent pas des mots de passe choisis [17].

« Votre mot de passe doit être traité de la même manière qu'une brosse à dents : vous ne le partagez pas et vous le changez régulièrement ! »

2.2.6. Protocoles d'authentification

2.2.6.1. Protocole PAP

Le protocole PAP « *Password Authentication Protocol* », comme son nom l'indique, est un protocole d'authentification par mot de passe. Il a été originalement utilisé dans le cadre du protocole PPP.

Son principe consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé. Ainsi, il n'est utilisé en pratique qu'à travers un réseau sécurisé.

2.2.6.2. Protocole CHAP

Le protocole CHAP « *Challenge Handshake Authentication Protocol* », défini par la RFC 1994, est un protocole d'authentification basé sur la résolution d'un défi, c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée.

Les étapes du défi sont les suivantes :

- Un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi ;
- La machine distante hache ce nombre et le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau ;
- Le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur ;
- Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.

Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

2.2.6.3. Protocole MS-CHAP

Microsoft a mis au point une version spécifique de CHAP, baptisée MS-CHAP « *Microsoft Challenge Handshake Authentication Protocol version 1*, noté parfois MS-CHAP-v1 », améliorant globalement la sécurité.

En effet, le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle. Ainsi MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur.

Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire. Le protocole MS-CHAP-v1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire.

2.2.6.4. Protocole MS-CHAPv2

La version 2 du protocole MS-CHAP a été définie en janvier 2000 dans la RFC 2759. Cette nouvelle version du protocole définit une méthode dite " authentification mutuelle ", permettant au serveur d'authentification et à la machine distante de vérifier leurs identités respectives.

Le processus d'authentification mutuelle de MS-CHAP-v2 fonctionne de la manière suivante :

- Le serveur d'authentification envoie à l'utilisateur distant une demande de vérification composée d'un identifiant de session ainsi que d'une chaîne aléatoire.
- Le client distant répond avec :
 - ✓ Son nom d'utilisateur ;
 - ✓ Un haché contenant la chaîne arbitraire fournie par le serveur d'authentification, l'identifiant de session ainsi que son mot de passe ;
 - ✓ Une chaîne aléatoire.
- Le serveur d'authentification vérifie la réponse de l'utilisateur distant et renvoie à son tour les éléments suivants :
 - ✓ La notification de succès ou d'échec de l'authentification ;
 - ✓ Une réponse chiffrée sur la base de la chaîne aléatoire fournie par le client distant, la réponse chiffrée fournie et le mot de passe de l'utilisateur distant.
- Enfin le client distant vérifie à son tour la réponse et, en cas de réussite, établit la connexion.

Le protocole MS-CHAP-v2 a été cassé et des outils de déchiffrement du mot de passe à partir d'écoute du réseau ont été rendus publics en 2012.

2.2.6.5. Protocole EAP

Le protocole EAP est une extension du protocole PPP, il est utilisé pour les connexions à Internet à distance (généralement via un modem RTC classique) et permettant notamment l'identification des utilisateurs sur le réseau. Contrairement à PPP, le protocole EAP permet d'utiliser différentes méthodes d'identification et son principe de fonctionnement rend très souple l'utilisation de différents systèmes d'authentification. EAP possède plusieurs méthodes d'authentification, dont les plus connues sont : LEAP ; PEAP ; EAP-FAST ; EAP-TLS et EAP-TTLS.

2.2.6.6. Protocole Kerberos

Le protocole Kerberos est issu du projet « Athena » du MIT, mené par Miller et Neuman. La version 5 du protocole Kerberos a été normalisée par l'IETF dans les RFC 1510 (septembre 1993) et 1964 (juin 1996).

L'objet de Kerberos est la mise en place de serveurs d'authentification (AS), permettant d'identifier des utilisateurs distants, et des serveurs de délivrement de tickets de service (TGS), permettant de les autoriser à accéder à des services réseau. Les clients peuvent aussi bien être des utilisateurs que des machines. La plupart du temps, les deux types de services sont regroupés sur un même serveur, appelé centre de distribution des clés (KDC).

Le protocole Kerberos repose sur un système de cryptographie à base de clés secrètes (clés symétriques ou clés privées), avec l'algorithme DES. Kerberos partage avec chaque client du réseau une clé secrète faisant office de preuve d'identité. Le principe de fonctionnement de Kerberos repose sur la notion de tickets :

- Afin d'obtenir l'autorisation d'accès à un service, un utilisateur distant doit envoyer son identifiant au serveur d'authentification.
- Le serveur d'authentification vérifie que l'identifiant existe et envoie un ticket initial au client distant, chiffré avec la clé associée au client. Le ticket initial contient :
 - ✓ Une clé de session, faisant office de mot de passe temporaire pour chiffrer les communications suivantes ;
 - ✓ Un ticket d'accès au service délivrant le ticket.
- Le client distant déchiffre le ticket initial avec sa clé et obtient ainsi un ticket et une clé de session.

Grâce à son ticket et sa clé de session, le client distant peut envoyer une requête chiffrée au service délivrant le ticket, afin de demander l'accès à un service. Par ailleurs, Kerberos propose un système d'authentification mutuelle permettant au client et au serveur de s'identifier réciproquement. L'authentification proposée par le serveur Kerberos a une durée limitée dans le temps, ce qui permet d'éviter à un pirate de continuer d'avoir accès aux ressources : on parle ainsi d'*anti-rejeu* [18].

2.3. Autorisation

2.3.1. Définition

Imaginez que vous êtes sur le point de prendre des vacances. Vous allez à une compagnie aérienne commerciale et demandez de réserver un billet d'avion. L'avion a quelques rangées à l'avant qui sont très belles, en cuir, larges et confortables. Vous préféreriez vous asseoir ici au

lieu des sièges qui sont plus éloignés car ceux-ci sont raides, inconfortables et n'offrent pas beaucoup d'espace.

Malheureusement, si vous avez acheté un billet de classe économique, vous ne pouvez pas vous asseoir sur le siège de première classe à l'avant de l'avion. La fonction d'autorisation de l'AAA est similaire à ce processus. Si vous possédez un billet autorisé de classe économique, vous ne pouvez pas accéder aux ressources de première classe. Ces informations sont toutes conservées dans la base de données de la compagnie aérienne et peuvent facilement être vérifiées en recherchant votre identité et en référençant l'attribution du siège. C'est le processus d'autorisation de base [19].

L'autorisation détermine l'accès aux ressources et les opérations effectuées par les utilisateurs en fonction de leur rôle de travail. Une fois l'authentification de l'utilisateur réussie, l'étape suivante consiste à gérer le niveau d'autorisation dont un utilisateur a besoin pour effectuer ses actions en justice.

Un exemple bancaire serait parfait à cet égard. Après avoir entré le mot de passe correct, nous obtenons l'autorisation de retirer le maximum d'argent en fonction du solde disponible sur le compte bancaire. De même, il existe des scénarios similaires dans les réseaux informatiques où nous devons restreindre l'accès à l'utilisateur. Par exemple, un utilisateur peut avoir besoin de ressources réseau huit heures par jour. De même, un administrateur réseau peut avoir besoin de ressources plus qu'un utilisateur. Des listes de méthodes personnalisées et par défaut sont utilisées pour définir l'autorisation dans les périphériques Cisco [2].

Exemple d'autorisation :

Dans cet exemple d'autorisation, un serveur AAA est ajouté pour donner une idée du processus lorsqu'un serveur externe est utilisé. Ce serveur peut être utilisé pour les autorisations, comme le montre la figure 2.3, mais il peut également être utilisé pour authentifier les utilisateurs.

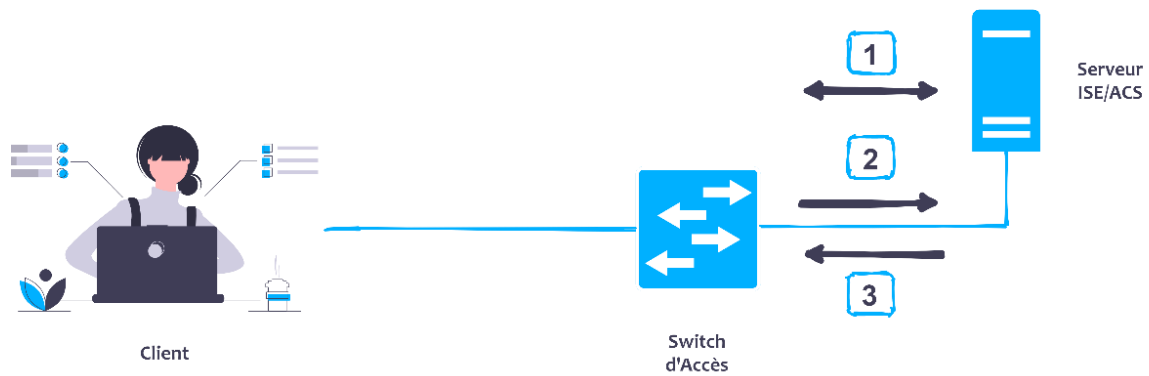


Figure 2.3 : Exemple d'autorisation.

Etape 1. Une fois l'authentification terminée, une session est établie avec un serveur AAA.

Etape 2. L'équipement réseau demande l'autorisation pour le service demandé au serveur AAA.

Etape 3. Le serveur AAA renvoie une réponse *PASS / FAIL* pour l'autorisation [19].

2.3.2. Méthodes d'autorisation AAA

AAA prend en charge cinq méthodes d'autorisation différentes :

- **If-Authenticated :** L'utilisateur est autorisé à accéder à la fonction demandée s'il a été authentifié avec succès.
- **None :** Le serveur d'accès au réseau ne demande pas les informations d'autorisation ; l'autorisation n'est pas effectuée.
- **Local :** L'équipement réseau ou le serveur d'accès consulte sa base de données locale, pour autoriser des droits spécifiques pour les utilisateurs.
- **TACACS+ :** Le serveur d'accès au réseau échange les informations d'autorisation avec le démon de sécurité TACACS+. L'autorisation TACACS+ définit des droits spécifiques pour les utilisateurs en associant des paires « *attribute-value* », qui sont stockées dans une base de données sur le serveur de sécurité TACACS +, avec l'utilisateur approprié.
- **RADIUS :** Le serveur d'accès au réseau demande des informations d'autorisation auprès du serveur de sécurité RADIUS. L'autorisation RADIUS définit des droits spécifiques pour les utilisateurs en associant des attributs, qui sont stockés dans la base de données du serveur RADIUS, avec l'utilisateur approprié [20].

2.3.3. Niveaux de privilège « *Privilege Levels* »

Il est généralement souhaitable que les utilisateurs disposent de différents niveaux d'accès en fonction de leur rôle professionnel, de leur expérience, etc. Une telle autorisation peut également être configurée sur l'équipement sans serveur AAA.

Pour cela, IOS fournit 16 niveaux d'accès, appelés niveaux de privilège. Le nombre de commandes disponibles pour un utilisateur dépend de son niveau de privilège. Des niveaux de privilèges plus élevés fournissent plus de commandes.

Par défaut, les trois niveaux suivants sont définis sur l'équipement :

- **Niveau de privilège 0** : Inclut les commandes *disable*, *enable*, *exit*, *help*, et *logout*. Vous ne pouvez pas vraiment accéder à ce niveau car après la connexion, le premier niveau accessible est le niveau 1. Ainsi, les commandes définies dans ce niveau sont disponibles pour tous les utilisateurs et n'affectent pas la configuration de l'équipement.
- **Niveau de privilège 1** : Inclut toutes les commandes *user-level* à l'invite '>' de l'équipement réseau. Ce niveau est également appelé *User-EXEC mode*. Les commandes à ce niveau n'affectent pas la configuration de l'équipement.
- **Niveau de privilège 15** : Inclut toutes les commandes *enable-level* à l'invite '#' de l'équipement. À ce niveau, toutes les commandes sont disponibles et toute configuration peut être visualisée ou modifiée. Ce niveau est également appelé *Privileged-EXEC mode* [19].

Remarque : Les commandes disponibles à des niveaux de privilège inférieurs sont automatiquement exécutables à des niveaux supérieurs, car un niveau de privilège inclut les privilèges de tous les niveaux inférieurs.

2.3.4. Accès CLI basé sur les rôles « *Role based CLI Access* »

Pour offrir plus de flexibilité que les niveaux de privilèges, Cisco propose une fonction d'accès CLI basée sur les rôles pour les administrateurs réseau afin de restreindre l'accès des utilisateurs. Les fonctionnalités d'accès CLI basées sur les rôles permettent à l'administrateur de définir des vues « *views* ». Ces vues sont l'ensemble des commandes opérationnelles et des configurations. La configuration d'une vue permet un accès sélectif ou partiel aux commandes du *mode EXEC* et du *mode Configuration*.

Les vues peuvent être des types suivants :

- **Root View** : Un système dans une vue racine a les mêmes privilèges qu'un utilisateur avec le niveau de privilège 15. Pour créer toute autre vue comme la *vue CLI* ou *Super vue*, l'administrateur doit être en vue racine.
- **CLI View** : Dans une vue CLI, il n'y a pas de vue supérieure ou inférieure en spécifique, elle consiste en un ensemble de commandes spécifiques.
- **Super view** : Une super vue comprend une ou plusieurs vues CLI, qui permettent aux utilisateurs de définir quelles commandes sont acceptées à partir d'un certain niveau et quelles informations de configuration sont disponibles pour les utilisateurs. Les utilisateurs qui se trouvent dans une super vue peuvent accéder à toutes les commandes configurées pour l'une des vues CLI qui font partie de la super vue.
- **Lawful Intercept View** : Un système dans une vue d'interception légale a accès aux commandes et aux informations de configuration spécifiées. Plus précisément, une vue d'interception légale permet à un utilisateur de sécuriser l'accès aux commandes d'interception légales ; ces commandes ne sont disponibles pour aucune autre vue ou niveau de privilège.
- **Parser View** : Les vues d'analyseur font la même chose que les niveaux de privilèges personnalisés, mais elles ont moins de commandes et donnent une vue de configuration claire. Du point de vue de l'implémentation, nous définissons d'abord une vue, puis nous lui affectons des commandes utilisateur ou de groupe. La fonction d'affichage de l'analyseur fournit un contrôle d'accès granulaire en limitant les utilisateurs autorisés à un certain niveau de privilège où des commandes d'ensemble spécifiques sont autorisées uniquement [2].

2.4. Traçabilité « *Accounting* »

2.4.1. Définition

La dernière partie de l'AAA est la traçabilité. Elle peut être expliquée à l'aide d'un exemple de l'industrie du transport aérien, Lorsque vous entrez ou montez à bord de l'avion, vous remettez une carte d'embarquement à l'agent et elle est numérisée à travers une machine. Cela explique votre embarquement dans l'avion. En ce qui concerne la compagnie aérienne, vous étiez là et vous étiez dans l'avion. La traçabilité AAA est similaire, lorsque vous essayez

d'accéder au réseau, et si vous êtes authentifié, AAA peut commencer à suivre toutes les actions que vous entreprenez.

La traçabilité dans un environnement Cisco permet de suivre et de sauvegarder toutes les actions effectuées par les utilisateurs. Par exemple, les administrateurs système peuvent avoir besoin de facturer aux services ou aux clients le temps de connexion ou les ressources utilisées sur le réseau (par exemple, le temps total de connexion). La traçabilité AAA permet de suivre cette activité, ainsi que les tentatives de connexion suspectes au réseau.

Lors de l'utilisation de la traçabilité AAA, l'équipement réseau peut envoyer des messages au serveur AAA. Il est ensuite possible d'importer les enregistrements de traçabilité dans une feuille de calcul ou un programme de traçabilité pour les visualiser. Le serveur de contrôle d'accès (ACS) peut être utilisé pour stocker ces messages de traçabilité téléchargeables au format .CSV ou utiliser la journalisation *Open Database Connectivity* (ODBC), qui est prise en charge dans ACS. De même, il est possible d'installer l'agent de journal et transmettre les informations de journal à *Cisco Secure-Monitoring Analysis and Response System* (CS-MARS) pour la surveillance de la mitigation et de la corrélation.

Les enregistrements de traçabilité envoyés par un équipement Cisco au serveur de traçabilité sont envoyés sous la forme d'une paire attribut-valeur (AV). Certaines de ces paires contiennent des informations telles que le nom d'utilisateur, l'adresse, le service demandé ou l'équipement Cisco traversé par cette demande.

Exemple de traçabilité :

Vous pouvez désormais utiliser la traçabilité AAA pour effectuer l'un des types de traçabilité. Dans cet exemple, vous récupérez une fois l'authentification et l'autorisation effectuées. Ici, la traçabilité des ressources effectue la traçabilité *START / STOP* pour FTP sur le réseau. Voir la figure 2.4.

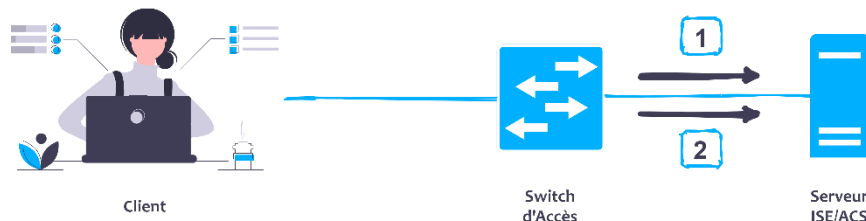


Figure 2.4 : Exemple de traçabilité.

Dans cet exemple, les étapes suivantes sont exécutées :

Étape 1. Une fois qu'un utilisateur a été authentifié, le processus de traçabilité AAA sur le client AAA génère un message de démarrage pour indiquer le début de la session.

Étape 2. Lorsque l'utilisateur termine sa session et se déconnecte, un message d'arrêt est envoyé par le client AAA pour indiquer la fin de la session.

Là encore, une liste de méthodes « *method list* » détermine le type de traçabilité à effectuer.

2.4.2. Méthodes de traçabilité AAA

AAA prend en charge plusieurs types de traçabilité, notamment :

- **Network accounting** : La traçabilité réseau fournit des informations pour toutes les sessions PPP, SLIP ou ARAP, y compris le nombre de paquets et d'octets.
- **Connection accounting** : La traçabilité des connexions fournit des informations sur toutes les connexions sortantes effectuées à partir du client AAA, telles que Telnet, LAT, TN3270, PAD, et rlogin.
- **EXEC accounting** : La traçabilité *EXEC* fournit des informations sur *user EXEC terminal sessions* « *user shells* » sur le serveur d'accès au réseau, y compris le nom d'utilisateur, la date, les heures de début et de fin, l'adresse IP du serveur d'accès et le numéro de téléphone d'où provient l'appel pour les utilisateurs entrants.
- **System accounting** : La traçabilité système fournit des informations sur tous les événements au niveau du système (par exemple, lorsque le système redémarre ou lorsque la traçabilité est activée ou désactivée).
- **Command accounting** : La traçabilité des commandes fournit des informations sur les commandes *EXEC shell* pour un niveau de privilège spécifié qui sont exécutées sur un serveur d'accès réseau. Chaque enregistrement de traçabilité de commande comprend une liste des commandes exécutées pour ce niveau de privilège, ainsi que la date et l'heure auxquelles chaque commande a été exécutée et l'utilisateur qui l'a exécutée.
- **Resource accounting** : L'implémentation Cisco de la traçabilité AAA fournit une prise en charge des enregistrements de démarrage et d'arrêt pour les appels qui ont réussi l'authentification de l'utilisateur. La fonctionnalité supplémentaire de génération d'enregistrements d'arrêt pour les appels dont l'authentification échoue dans le cadre de l'authentification de l'utilisateur est également prise en charge. Ces enregistrements sont

nécessaires pour les utilisateurs qui utilisent des enregistrements de traçabilité pour gérer et surveiller leurs réseaux [19].

2.5. Protocoles AAA

Les concepts de l'AAA peuvent être appliqués à de nombreux aspects du cycle de vie d'une technologie. Les deux principaux aspects de l'AAA liés aux réseaux sont les suivants :

A. L'administration des équipements « *Device administration* » :

L'administration des équipements est une méthode AAA pour contrôler l'accès à une console d'équipement réseau, une session Telnet, une session SSH ou toute autre méthode d'accès au système d'exploitation de l'équipement lui-même à des fins de configuration.

Par exemple, imaginez que votre entreprise dispose d'un groupe *Active Directory* nommé administrateurs réseau, qui devrait avoir un accès complet (niveau de privilège 15) aux commutateurs Cisco dans le réseau d'une entreprise. Ils devraient donc être en mesure d'apporter des modifications aux réseaux locaux virtuels (VLAN), voir la configuration en cours d'exécution de l'équipement, et plus encore.

Il pourrait y avoir un autre groupe nommé opérateurs de réseaux qui devrait être autorisé à afficher uniquement l'affichage des commandes *Show* et à ne rien configurer dans l'équipement.

L'administration des équipements AAA vous permet d'être plus granulaire. Le serveur ACS a la capacité de fournir des jeux de commandes, qui sont des listes de commandes dont l'exécution est autorisée ou refusée par un utilisateur authentifié.

L'administration des équipements peut être de nature très interactive, avec la nécessité de s'authentifier une fois mais d'autoriser plusieurs fois au cours d'une même session administrative dans la ligne de commande d'un équipement. En tant que tel, il se prête bien à l'utilisation du protocole client/serveur *Terminal Access Controller Access Control System* (TACACS), plus encore que *Remote Authentication Dial-in User Service* (RADIUS).

Comme son nom l'indique, TACACS a été conçu pour l'administration des appareils AAA afin d'authentifier et d'autoriser les utilisateurs pour les mainframes, les terminaux Unix et autres consoles.

TACACS sépare la partie autorisation d'AAA, permettant une seule authentification et plusieurs autorisations au sein de la même session. C'est pourquoi il se prête davantage à l'administration de périphériques qu'à RADIUS.

B. L'accès au réseau « *Network Access* » :

L'accès sécurisé au réseau consiste essentiellement à apprendre l'identité de l'utilisateur ou l'entité avant de permettre à cette entité de communiquer au sein du réseau. L'accès au réseau a vraiment pris une forte emprise à l'époque des modems et des réseaux commutés.

À cette époque, les entreprises fournissaient un accès au réseau pour les travailleurs en dehors des limites physiques des bâtiments de l'entreprise grâce à des modems. Les gens ont également accédé à Internet en utilisant l'accès à distance aux fournisseurs de services Internet (FAI) « *Internet service providers (ISPs)* » via leurs modems. Fondamentalement, il suffisait d'un modem et d'une ligne téléphonique.

Permettre à quiconque de se connecter à votre réseau simplement en composant le numéro de téléphone de votre modem n'est pas une idée sûre. L'utilisateur doit être authentifié avant d'autoriser la connexion. C'est là que RADIUS est entré en jeu à l'origine, comme en témoigne le nom du protocole « *Remote Access Dial In User Service* ».

RADIUS a été utilisé entre le périphérique d'accès réseau (NAD) et le serveur d'authentification. L'authentification était (PAP), (CHAP) ou (MS-CHAP).

Comme la technologie a continué d'évoluer, la connexion directe à une entreprise a été remplacée par des réseaux privés virtuels (VPNs) d'accès à distance. L'IEEE a normalisé une méthode pour utiliser le protocole EAP sur les réseaux locaux (IEEE 802.1X) et RADIUS a été utilisé comme protocole de choix pour acheminer le trafic d'authentification. En fait, IEEE 802.1X ne peut pas utiliser TACACS ; il doit utiliser RADIUS.

2.5.1. TACACS+

2.5.1.1. Définition

TACACS est créé et destiné à contrôler l'accès aux terminaux Unix. Cisco a créé un nouveau protocole appelé TACACS+, qui a été publié en tant que norme ouverte au début des années 1990. TACACS+ peut être dérivé de TACACS, mais il s'agit d'un protocole complètement séparé et non rétrocompatible conçu pour AAA. Bien que TACACS+ soit

principalement utilisé pour l'administration des équipements AAA, il peut être utilisé pour certains types d'accès réseau AAA.

Il est important de comprendre que TACACS+ n'est pas actuellement un protocole pris en charge avec Cisco ISE 1.2. Le serveur ACS est le serveur d'authentification principal produit par Cisco pour les entreprises qui ont besoin d'utiliser TACACS+ pour l'administration des équipements AAA.

TACACS+ utilise le port TCP (Transmission Control Protocol) 49 pour communiquer entre le client TACACS+ et le serveur TACACS+. Un exemple est un commutateur Cisco authentifiant et autorisant l'accès administratif à IOS CLI du commutateur. Le commutateur est le client TACACS+ et Cisco Secure ACS est le serveur, comme illustré sur la figure 2.5.

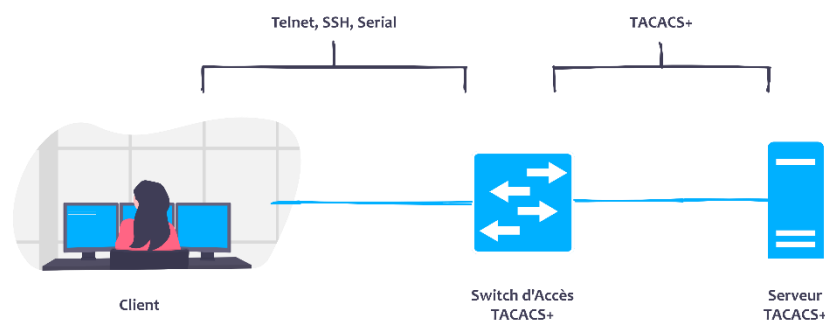


Figure 2.5 : Communication entre client et serveur TACACS+.

L'un des principaux différenciateurs de TACACS+ est sa capacité à séparer l'authentification, l'autorisation et la traçabilité en tant que fonctions distinctes et indépendantes. C'est pourquoi TACACS+ est si couramment utilisé pour l'administration d'équipements, même si RADIUS est toujours certainement capable de fournir une administration d'équipements AAA.

L'administration des équipements peut être de nature interactive, avec la nécessité de s'authentifier une fois mais d'autoriser plusieurs fois au cours d'une même session administrative dans la ligne de commande d'un appareil. Un équipement réseau peut avoir besoin d'autoriser l'activité d'un utilisateur par commande. TACACS+ est conçu pour accueillir ce type d'autorisation.

La communication TACACS+ entre le client et le serveur utilise différents types de messages selon la fonction. En d'autres termes, des messages différents peuvent être utilisés

pour l'authentification que ceux utilisés pour l'autorisation et la traçabilité. Un autre point intéressant à savoir est que la communication TACACS + cryptera toute la charge utile.

2.5.1.2. Messages d'authentification TACACS +

Lors de l'utilisation de TACACS + pour l'authentification, seuls trois types de paquets sont échangés entre le client et le serveur :

- **START** : Ce paquet est utilisé pour commencer la demande d'authentification entre le client AAA et le serveur AAA.
- **REPLY** : Messages envoyés du serveur AAA au client AAA.
- **CONTINUE** : Messages du client AAA utilisés pour répondre aux demandes de nom d'utilisateur et de mot de passe du serveur AAA.

Lorsqu'une demande d'authentification est envoyée du client au serveur, elle commence par un message START du client vers le serveur. Le message START indique au serveur qu'une demande d'authentification est en cours. Tous les messages du serveur vers le client lors de l'authentification seront une requête REPLY. Le serveur envoie un message REPLY demandant au client de récupérer le nom d'utilisateur qui est envoyé au serveur dans un message CONTINUE.

Une fois que le serveur a reçu le nom d'utilisateur, il envoie un message REPLY au client demandant le mot de passe, qui est renvoyé au serveur dans un autre message CONTINUE. Le serveur envoie ensuite un dernier message REPLY avec l'état de réussite ou d'échec de la demande d'authentification.

Les valeurs possibles renvoyées par le serveur AAA au client AAA dans le message REPLY final sont :

- **ACCEPT** : L'authentification de l'utilisateur a réussi et le processus d'autorisation peut commencer, si le client AAA est configuré pour l'autorisation.
- **REJECT** : L'authentification de l'utilisateur a échoué. La connexion sera refusée ou l'utilisateur sera invité à réessayer, selon la configuration du client AAA.
- **ERROR** : Une erreur s'est produite à un moment donné lors de l'authentification. Les clients AAA tentent généralement d'authentifier à nouveau l'utilisateur ou tentent une autre méthode d'authentification de l'utilisateur.

- **CONTINUE** : L'utilisateur est invité à fournir des informations supplémentaires. Cela ne doit pas être confondu avec le message CONTINUE envoyé du client AAA au serveur AAA. Cette valeur est envoyée par le serveur AAA dans un message REPLY, indiquant que plus d'informations sont nécessaires.

La figure 2.6 illustre les messages d'authentification entre le client et le serveur.

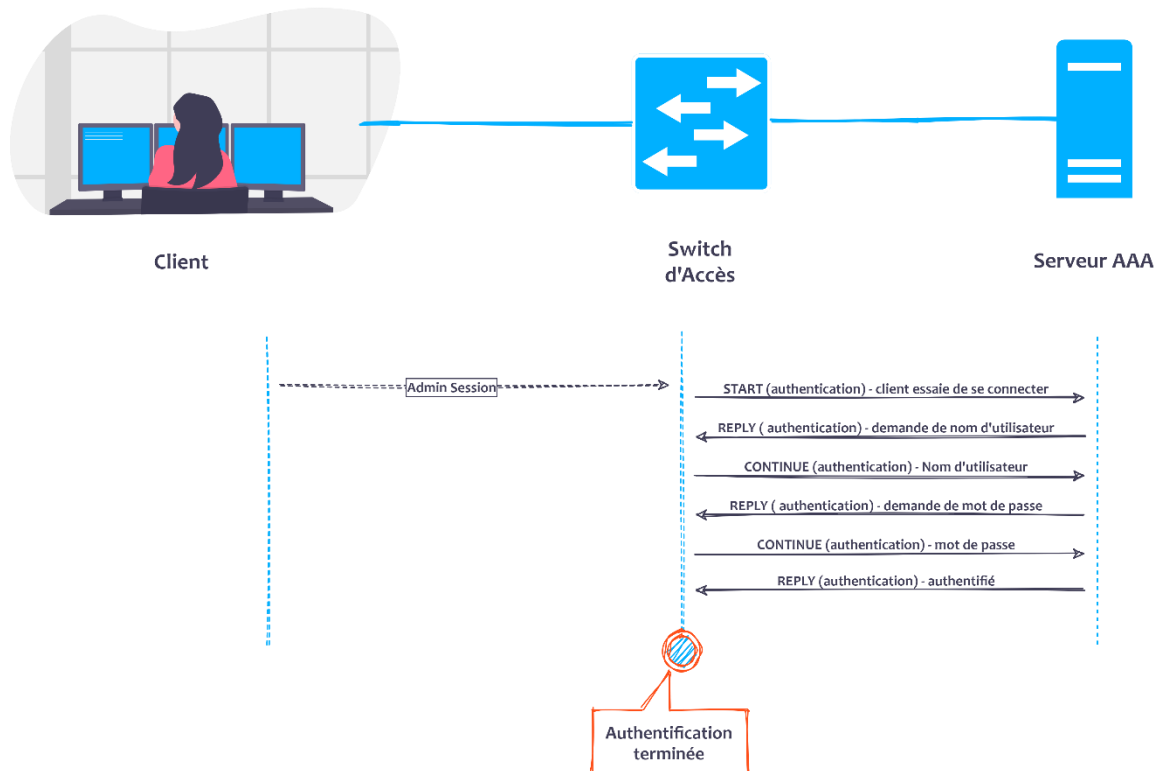


Figure 2.6 : Flux de communication d'authentification TACACS+.

2.5.1.3. Messages d'autorisation et de traçabilité TACACS +

Lors de l'utilisation de TACACS + pour l'autorisation, seuls deux messages sont utilisés entre le client AAA et le serveur AAA :

- **REQUEST** : Ce message est envoyé du client AAA au serveur AAA pour demander une autorisation qui peut être liée à l'accès à un *CLI shell* ou éventuellement à l'autorisation d'une commande spécifique. La communication protocolaire ne fait pas de discrimination. La fonction demandée est connue sous le nom de *service*. Par exemple, le service serait «shell» pour l'accès CLI à un équipement exécutant Cisco IOS. Chaque service peut être communiqué avec des paires valeur-attribut.

- **RESPONSE** : Ce message est renvoyé du serveur AAA au client AAA avec le résultat de la demande d'autorisation comprenant des détails spécifiques, tels que le niveau de privilège attribué à l'utilisateur final. Les messages de RESPONSE peuvent contenir l'une des cinq réponses :
- ✓ **FAIL** : Cette réponse indique que l'utilisateur doit se voir refuser l'accès au service demandé.
 - ✓ **PASS_ADD** : Cette réponse indique une autorisation réussie et les informations contenues dans le message RESPONSE doivent être utilisées en plus des informations demandées. Si aucun argument supplémentaire n'est renvoyé par le serveur AAA dans le message RESPONSE, la demande est simplement autorisée telle qu'elle est.
 - ✓ **PASS_REPL** : Indique une autorisation réussie, mais le serveur a choisi d'ignorer la requête REQUEST et la remplace par les informations renvoyées dans la RESPONSE.
 - ✓ **FOLLOW** : Cette réponse indique que le serveur AAA souhaite que le client AAA envoie la demande d'autorisation à un autre serveur. Les nouvelles informations sur le serveur seront répertoriées dans le paquet RESPONSE. Le client AAA peut utiliser ce nouveau serveur ou traiter la réponse comme un FAIL.
 - ✓ **ERROR** : Une réponse d'ERREUR indique un problème survenant sur le serveur AAA et un dépannage supplémentaire doit se produire.

Une fonction clé de l'AAA qui ne peut être négligée est la traçabilité. Il est crucial pour la sécurité d'avoir un enregistrement de ce qui s'est passé. En plus de la demande d'autorisation envoyée au serveur AAA, il devrait y avoir des enregistrements de traçabilité des activités de l'utilisateur.

Tout comme les messages d'autorisation, seuls deux types de messages sont utilisés dans la traçabilité :

- **REQUEST** : Ce message est envoyé du client AAA au serveur AAA pour indiquer une notification d'activité. Trois valeurs peuvent être incluses avec la requête REQUEST :
- ✓ **START** : L'enregistrement de type START indique qu'un service a commencé.

- ✓ **STOP** : L'enregistrement de type STOP indique que le service est terminé.
- ✓ **CONTINUE** : L'enregistrement de type CONTINUE est également parfois appelé enregistrement *Watchdog* ou *UPDATE*. Il est envoyé lorsqu'un service a déjà démarré et est en cours, mais il existe des informations mises à jour à fournir en relation avec le service.
- **RESPONSE** : Ce message est renvoyé du serveur AAA au client AAA avec le résultat de la demande de traçabilité et peut contenir l'une des trois réponses :
 - ✓ **SUCCESS** : Indique que le serveur a reçu l'enregistrement du client.
 - ✓ **ERROR** : Indique une erreur sur le serveur et que l'enregistrement n'a pas été stocké.
 - ✓ **FOLLOW** : Indique que le serveur souhaite que le client envoie l'enregistrement à un autre serveur AAA et inclut les informations de ce serveur dans la requête RESPONSE.

La figure 2.7 illustre un utilisateur autorisé à accéder à IOS EXEC CLI. C'est une continuation directe de la figure 2.6 où l'authentification a eu lieu. Dans cette illustration, l'utilisateur est autorisé à entrer dans IOS EXEC CLI et est autorisé à exécuter la commande *show run*. La commande que l'utilisateur demande à utiliser est contenue dans le message d'autorisation REQUEST.

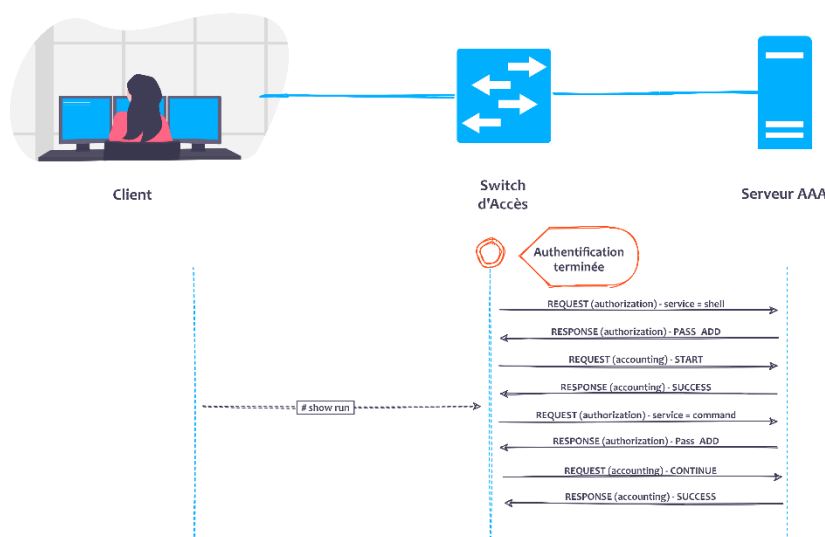


Figure 2.7 : Flux de communication d'autorisation et de Traçabilité TACACS+.

2.5.2. RADIUS

2.5.2.1. Définition

RADIUS est une norme IETF pour AAA. Comme avec TACACS +, RADIUS suit un modèle client / serveur dans lequel le client initie les requêtes au serveur. RADIUS est le protocole de choix pour l'accès au réseau AAA, et il est temps de se familiariser avec RADIUS. Lors d'une connexion régulière à un réseau sans fil sécurisé, RADIUS est très probablement utilisé entre l'équipement sans fil et le serveur AAA. Parce qu'il est le protocole de transport pour EAP, ainsi que de nombreux autres protocoles d'authentification.

A l'origine, RADIUS était utilisé pour étendre les authentifications à partir du protocole point à point (PPP) de la couche 2 utilisée entre l'utilisateur et le serveur d'accès au réseau (NAS) et transporter ce trafic d'authentification du NAS vers le serveur AAA effectuant l'authentification. Cela a permis d'étendre un protocole d'authentification de la couche 2 au-delà des limites de la couche 3 à un serveur d'authentification centralisé.

RADIUS a évolué bien au-delà des cas d'utilisation de l'accès réseau à distance pour lesquels il a été créé à l'origine. Aujourd'hui, il est toujours utilisé de la même manière, transportant le trafic d'authentification de l'équipement réseau vers le serveur d'authentification. Avec IEEE 802.1X, RADIUS est utilisé pour étendre l'EAP de la couche 2 de l'utilisateur au serveur d'authentification, comme le montre figure 2.8.

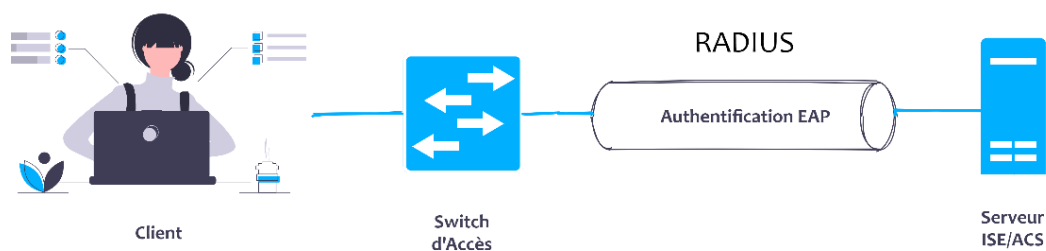


Figure 2.8 : Transport de communication EAP via RADIUS.

Il existe de nombreuses différences entre RADIUS et TACACS +. L'une de ces différences est que l'authentification et l'autorisation ne sont pas séparées dans une transaction RADIUS. Lorsque la demande d'authentification est envoyée à un serveur AAA, le client AAA s'attend à ce que le résultat de l'autorisation soit renvoyé en réponse.

2.5.2.2. Messages d'authentification et d'autorisation RADIUS

Il n'y a que quelques types de messages avec l'authentification et l'autorisation RADIUS:

- **Access-Request** : Ce message est envoyé du client AAA au serveur AAA pour demander une authentification et une autorisation. La demande peut être pour l'accès au réseau ou pour l'accès au *shell* de l'équipement. RADIUS ne fait pas de discrimination. La fonction demandée est connue sous le nom de *service type*. Par exemple, le type de service peut être « *framed* » pour une authentification IEEE 802.1X. Certains types de services RADIUS courants sont indiqués dans le tableau 2.2.

| Valeur | Nom de type de service | Couramment utilisé pour |
|--------|------------------------|---|
| 1 | Login | Login request : souvent utilisé avec les authentifications Web pour les équipements de réseau non-Cisco |
| 2 | Framed | IEEE 802.1X |
| 5 | Outbound | Utilisé pour local web authentication |
| 10 | Call-check | Utilisé pour MAC authentication Bypass (MAB) |

Tableau 2.2 : Types de services RADIUS courants.

- **Access-Accept** : Ce message est envoyé du serveur AAA au client AAA signalant une authentification réussie. Le résultat de l'autorisation sera inclus sous forme de paires AV qui peuvent inclure des éléments tels que le VLAN attribué « *assigned VLAN* », une liste de contrôle d'accès téléchargeable (DACL), une étiquette de groupe de sécurité (SGT), et bien plus encore.
- **Access-Reject** : Ce message est envoyé du serveur AAA au client AAA signalant l'échec de l'authentification. L'authentification échouée signifie également qu'aucune autorisation n'a été accordée.
- **Access-Challenge** : Ce message facultatif peut être envoyé du serveur AAA au client AAA lorsque des informations supplémentaires sont nécessaires, comme un deuxième mot de passe pour les authentifications à deux facteurs.

La figure 2.9 illustre un exemple de flux RADIUS.

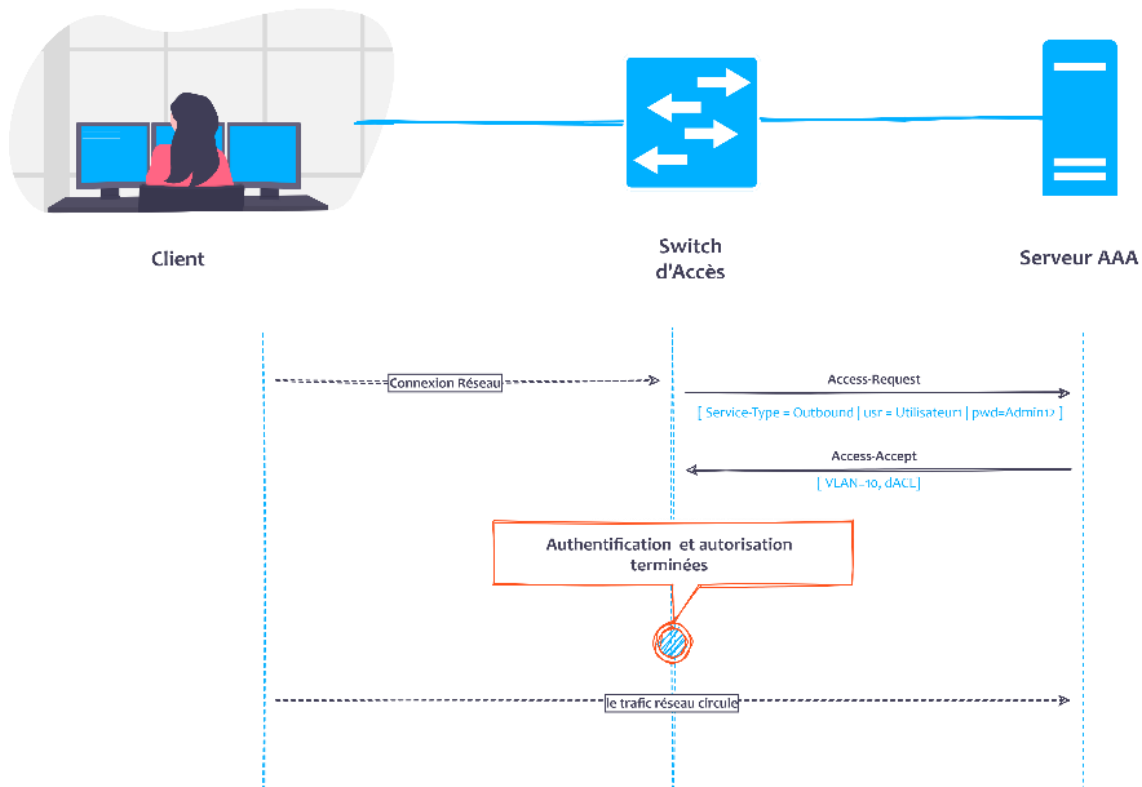


Figure 2.9 : Flux d'authentification et d'autorisation RADIUS.

Lorsque vous regardez la figure 2.9, gardez à l'esprit que l'authentification et l'autorisation sont combinées avec RADIUS. Le message Access-Accept inclut les paires AV définissant ce que l'utilisateur est autorisé à faire.

2.5.2.3. Messages de traçabilité RADIUS

Une fonction clé de l'AAA qui ne peut être négligée est la traçabilité. Il est crucial pour la sécurité d'avoir un enregistrement de ce qui s'est passé. En plus de la demande d'autorisation envoyée au serveur AAA, il devrait y avoir des enregistrements de traçabilité des activités de l'utilisateur. Seuls deux types de messages sont utilisés dans la traçabilité :

- **Accounting-Request** : Ce message est envoyé par le client AAA au serveur AAA. Cela peut inclure l'heure, les paquets, les informations DHCP, les informations CDP, etc. Le message peut être un message START indiquant que le service a commencé ou un message STOP indiquant que le service est terminé.

- **Accounting-Response** : Ce message agit comme un accusé de réception, de sorte que le client AAA sait que le message de traçabilité a été reçu par le serveur AAA.

La figure 2.10 illustre un exemple de flux de traçabilité RADIUS. C'est une continuation directe de la figure 2.9 où l'authentification et l'autorisation ont eu lieu.

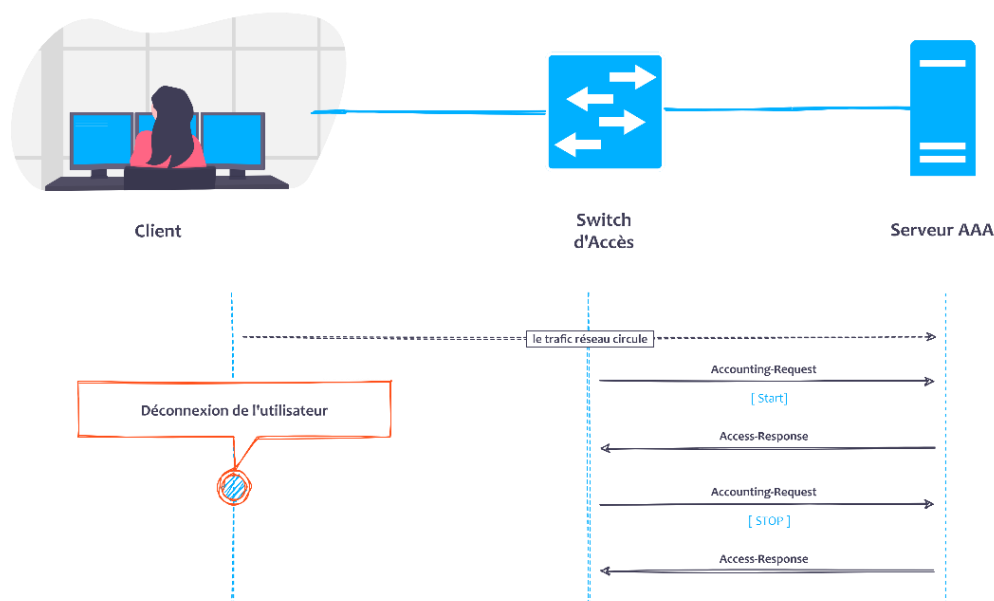


Figure 2.10 : Flux de traçabilité RADIUS.

Contrairement à TACACS +, RADIUS utilise UDP comme protocole de transmission. Les ports standard utilisés par RADIUS sont UDP / 1812 pour l'authentification et UDP / 1813 pour la traçabilité. Cependant, Cisco a pris en charge RADIUS avant la ratification de la norme et les ports utilisés étaient UDP / 1645 (authentification) et UDP / 1646 (traçabilité). La plupart des équipements Cisco prendront en charge l'utilisation de l'un ou l'autre ensemble de ports pour garantir une rétrocompatibilité.

Paires-AV « AV-Pairs » : Il y a des références à quelque chose appelé une paire attribue valeur tout au long des sections TACACS + et RADIUS. Lors de la communication avec un protocole AAA, de nombreux attributs peuvent être référencés pour dicter clairement les réponses ou les résultats. Le serveur RADIUS peut attribuer un attribut à la session d'authentification, tel qu'un VLAN. L'espace réservé VLAN est l'attribut, et le numéro VLAN réellement attribué est la valeur de cet espace réservé. L'espace réservé et sa valeur sont appariés et appelés paires-AV [21].

2.5.3. Comparaison entre RADIUS et TACACS +

| Caractéristiques | TACACS+ | RADIUS |
|--|--|---|
| Crée par | Cisco (Standard ouvert) | L'IETF (Standard ouvert) |
| Protocole de transport | TCP | UDP |
| Numéro du port d'authentification | TCP port 49 | UDP port 1812, 1645 (Authentication), 1813, 1646 (Accounting) |
| Utilisé pour | L'administration des équipements | L'accès au réseau |
| Cryptage de mot de passe | Oui | Oui |
| Cryptage de tout le paquet | Oui | Non |
| Prise en charge multi-protocole | Oui | Non |
| Mode de privilège | Prend en charge un seul mode de privilège | Prend en charge 15 modes de privilège |
| Ressources | A besoin de plus de ressources | A besoin de moins de ressources |
| Authentification, autorisation et traçabilité | Séparées | Authentification, autorisation sont combinées et traçabilité séparées |
| Traçabilité | Traçabilité approfondie | Traçabilité limitée |
| Journalisation des commandes | Il y a une journalisation complète des commandes | Il n'y a pas une journalisation des commandes |
| Challenge/Réponse | Bidirectionnel CHAP | Unidirectionnel CHAP |

Tableau 2.3 : Comparaison entre TACACS+ et RADIUS [22].

2.6. Conclusion

L'authentification, l'autorisation et la traçabilité (AAA) est un concept de sécurité informatique courant qui définit la protection des ressources du réseau. Il est utilisé pour prendre en charge les objectifs principaux de la sécurité (CID), en plus de fournir un cadre pour l'accès aux réseaux et aux équipements à l'aide des protocoles RADIUS et TACACS+.

Au cours du prochain chapitre, nous aborderons le protocole 802.1X permettant une authentification centralisée et une assurance de la dynamique et de la mobilité des accès au réseau.

CHAPITRE 3
PROTOCOLE 802.1X

3.1. Introduction

Les réseaux locaux, qu'ils soient filaires ou sans fil, sont souvent déployés dans des environnements qui permettent à des équipements non autorisés d'y être rattachés ou à des utilisateurs non autorisés d'accéder au réseau en utilisant un équipement rattaché. Par exemple, dans certaines zones d'un bâtiment accessible au public, un réseau d'entreprise peut fournir une connectivité au réseau local. Dans de tels environnements, il est souhaitable de restreindre l'accès aux services offerts par le réseau local aux seuls utilisateurs et équipements autorisés.

Initialement conçu pour la gestion sécurisée des accès des réseaux câblés à partir de commutateurs de paquets, le protocole d'authentification IEEE 802.1X « *Port-Based Authentication* » est devenu le standard le plus important en matière d'authentification permettant de bloquer le flux de données d'un utilisateur non authentifié et a été repris pour les réseaux sans fil.

Ce chapitre présente le protocole 802.1X. Il commence par la mise en clair de ses composants ainsi le protocole EAP utilisé pour l'échange de messages entre ces composants. Il décrit ensuite les méthodes d'EAP en plus d'une comparaison entre elles. Enfin, il explique quelques fonctionnalités du protocole 802.1X permettant de limiter les droits d'accès des utilisateurs.

3.2. Composants de 802.1X

La norme 802.1X définit trois entités principales qui participent à la méthode de contrôle d'accès définie dans cette norme :

3.2.1. Client « *supplicant* »

C'est l'équipement qui a besoin d'accéder ou demande l'accès à l'infrastructure LAN / WLAN ou aux services d'équipement de la couche 2. Cet équipement doit exécuter un logiciel client compatible 802.1X « *802.1X-compliant client software* » pour pouvoir répondre aux demandes d'un équipement de la couche 2.

3.2.2. Authentificateur « *authenticator* »

C'est l'équipement chargé de transmettre les informations entre le serveur d'authentification et le client. L'authentificateur est un équipement de la couche 2 qui sert d'intermédiaire ou de proxy entre le client et le serveur d'authentification, en demandant des informations d'identité au client, en vérifiant ces informations auprès du serveur d'authentification et en relisant la réponse renvoyée par le serveur d'authentification au client.

3.2.3. Serveur d'authentification « *Authentication Server* »

C'est l'équipement chargé d'effectuer l'authentification et l'autorisation réelles à travers l'authentificateur. Le serveur d'authentification valide l'identité du client et notifie l'équipement de la couche 2 faisant office d'authentificateur, qui relaie les informations au client.

La figure 3.1 donne un aperçu sur les différents composants de 802.1X.

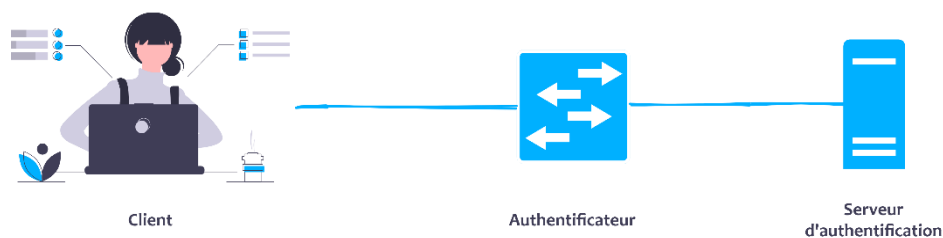


Figure 3.1 : Rôles des équipements 802.1X.

La figure 3.2 donne une idée sur l'architecture générale de 802.1X :

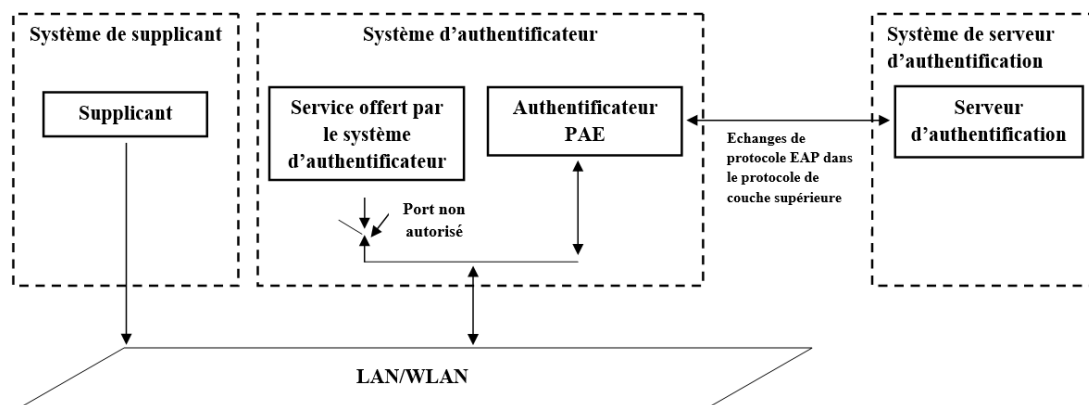


Figure 3.2 : Architecture de 802.1X.

L'entité d'accès au port (PAE) spécifiée dans la figure 3.2 fait référence à l'entité sur un équipement donné qui exécute l'algorithme 802.1X et le fonctionnement du protocole.

Le protocole d'authentification extensible (EAP) est le protocole clé utilisé pour transmettre les informations d'authentification entre le supplicant et le serveur d'authentification.

IEEE 802.1X définit l'encapsulation d'EAP sur IEEE 802 et est connu sous le nom d'EAP sur LAN (EAPOL). EAPOL a été initialement conçu pour Ethernet, mais a été étendu pour convenir à d'autres technologies telles que le sans-fil et l'interface de données distribuées sur fibre (FDDI).

EAP fournit des fonctions communes et une négociation de méthodes d'authentification appelées *méthodes EAP*. Les méthodes EAP prennent en charge différentes méthodes d'authentification, tels que les cartes à jeton « *token cards* », les mots de passe uniques, les certificats « *certificates* » et l'authentification par clé publique « *public key authentication* ».

3.3. EAP « *Extensible authentication protocol* »

Le protocole d'authentification extensible EAP est un framework d'authentification qui prend en charge plusieurs méthodes d'authentification. Fondamentalement, EAP permet à deux entités d'échanger des informations spécifiques à la méthode d'authentification que ces entités souhaitent utiliser. Le contenu de ces méthodes spécifiques d'authentification n'est pas défini dans EAP.

La flexibilité est l'un des avantages offerts par l'architecture EAP. Il n'est pas nécessaire de mettre à jour l'authentificateur pour prendre en charge les différentes ou nouvelles méthodes d'authentification. Seuls le client et le serveur d'authentification peuvent implémenter certaines ou toutes les méthodes d'authentification.

Aujourd'hui, il existe de nombreuses méthodes d'authentification, dont certaines sont définies dans les *RFC IETF* et certaines sont des méthodes spécifiques aux fournisseurs.

EAP spécifie que quatre types de messages peuvent être envoyés :

- **Request (0x01)** : Utilisé pour envoyer des messages de l'authentificateur au client ;
- **Response (0x02)** : Utilisé pour envoyer des messages du client à l'authentificateur ;

- **Success (0x03)** : Envoyé par l'authentificateur pour indiquer que l'accès est accordé ;
- **Failure (0x04)** : Envoyé par l'authentificateur pour indiquer que l'accès est refusé.

La figure 3.3 illustre le format de message EAP et la liste qui suit décrit chacun des champs.

| Code | Identifiant | Length | Data |
|------|-------------|--------|------|
|------|-------------|--------|------|

Figure 3.3 : Format de message EAP.

- **Code** : le champ code à un octet indique le type de message (*Request*, *Response*, *Success* ou *Failure*) ;
- **Identifiant** : le champ identifiant d'un octet contient un entier non signé utilisé pour faire correspondre les demandes avec les réponses. Chaque nouvelle demande utilise un nouveau numéro d'identification ;
- **Length** : le champ longueur sur deux octets indique le nombre total d'octets dans le paquet entier ;
- **Data** : la valeur du champ de données de longueur variable (y compris zéro octet) définit la façon dont le champ de données doit être interprété.

Le format de message EAP illustré sur la figure 3.3 est utilisé pour envoyer : *EAP-Request*, *EAP-Response*, *EAP-Success* ou *EAP-Failure*.

Pour *EAP-Request* et *EAP-Response*, un champ supplémentaire est introduit : le champ **Type**, comme illustré sur la figure 3.4. Le champ **Type** à un octet définit le type de demande ou de réponse. Un seul type est utilisé dans chaque paquet et le type de réponse correspond à la demande.

| Code | Identifiant | Length | Type | Req/Rsp DATA |
|------|-------------|--------|------|-----------------|
|------|-------------|--------|------|-----------------|

Figure 3.4 : Message de EAP Request / Response.

Pour *EAP-Success* et *EAP-Failure*, le champ **Data** à une longueur de zéro octet. Le reste de la structure reste le même que celui montré précédemment sur la figure 3.3.

Comme indiqué précédemment, les messages de *EAP-Request* et de *EAP-Response* sont subdivisés à l'aide du champ **Type**.

Certains types de EAP courants sont les suivants :

- LEAP (17)
- Identity (1)
- Notification (2)
- NAK (3)
- MD5-Challenge (4)
- One-Time Password (OTP) (5)
- Generic Token Card (6)
- EAP-TLS (13)
- EAP-TTLS (21)
- PEAP (25)
- EAP-FAST (43)

Le type prédéfini le plus important est **Identity** (type = 1) car il est utilisé dans le cadre de la phase d'introduction d'EAP :

- *EAP-Request / Identity* (Code = 1, Type = 1) : envoyé par l'authentificateur à un nouveau client.
- *EAP-Response / Identity* (Code = 2, Type = 1) : en réponse à *EAP-Request / Identity*, le client répond avec ce message contenant son nom d'utilisateur ou un autre identifiant qui sera compris par le serveur d'authentification.

Remarque : Pour plus de détails sur les autres types d'EAP, veuillez-vous référer à la RFC EAP (RFC 2284). Pour les autres types ou méthodes EAP, vous devez vous référer aux RFC ou aux (drafts).

3.4. EAPOL « *EAP Over LAN* »

La RFC EAP ne précise pas comment les messages doivent être communiqués. Ainsi, pour communiquer des messages EAP, il faut trouver un moyen de les encapsuler. Pour résoudre ce problème, IEEE 802.1X a défini un protocole appelé EAP sur LAN (EAPOL) pour que les messages EAP soient communiqués entre le supplicatant et l'authentificateur. EAPOL a été initialement conçu pour Ethernet mais a été étendu pour s'adapter à d'autres technologies. La figure 3.5 illustre le format de trame EAPOL.

| Ethernet MAC Header | Protocol Version | Packet Type | Packet Body Lenght | Packet Body |
|------------------------|---------------------|-------------|-----------------------|-------------|
|------------------------|---------------------|-------------|-----------------------|-------------|

Figure 3.5 : Format de trame EAPOL.

Les cinq types de messages EAPOL sont les suivants :

- **EAPOL-Packet (0)** : contient une trame EAP encapsulée. C'est le cas de la majorité des trames EAPOL.
- **EAPOL-Start (1)** : un client peut envoyer une trame *EAPOL-Start* au lieu d'attendre un défi de l'authentificateur (paquet EAPOL [*EAP-Identity / Request*]).
- **EAPOL-Logoff (2)** : utilisé pour renvoyer l'état du port à *non autorisé* lorsque le client a fini d'utiliser le réseau.
- **EAPOL-Key (3)** : utilisée pour échanger des informations de chiffrement cryptographique.
- **EAPOL-Encapsulated-ASF-Alert (4)** : fourni comme méthode permettant de transmettre des alertes *ASF* via un port qui est dans l'état non autorisé.

3.5. Echange de messages dans 802.1X

Comme indiqué précédemment, il existe trois entités dans 802.1X: le client, l'authentificateur et le serveur d'authentification.

Des messages sont échangés entre ces trois entités. 802.1X utilise EAP, ou plus spécifiquement EAPOL, pour transmettre ces messages entre le client et l'authentificateur et entre l'authentificateur et le serveur d'authentification utilisant RADIUS dans lequel EAP a été encapsulé, parfois appelé EAP sur RADIUS « *EAP over RADIUS* ».

La figure 3.6 illustre un échange EAPOL / 802.1X typique.

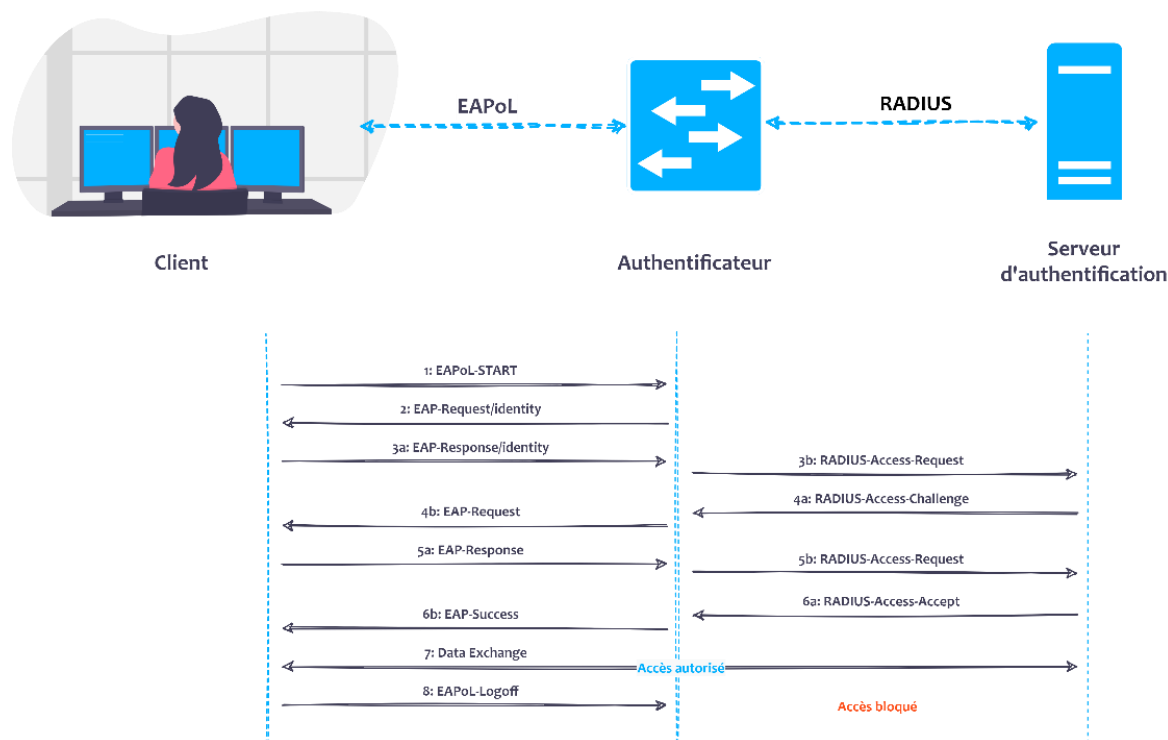


Figure 3.6 : Echange de messages EAPOL / 802.1X.

Le processus de fonctionnement dans 802.1X est le suivant :

Etape 1. Généralement, l'authentificateur envoie le premier message *EAP-Request* du type *Identity* au client pour lui demander son identité. Le client peut également démarrer ce processus s'il le souhaite en envoyant *EAPOL-Start*.

Etape 2. Si le client envoie *EAPOL-Start*, l'authentificateur demande l'identité du client en envoyant *EAP-Request / Identity*.

Etape 3. En réponse, le client envoie ses informations dans la trame *EAP-Response / Identity*. L'authentificateur décapsule les informations de la trame EAPOL et transmet les informations EAP qu'elle contient au serveur d'authentification en utilisant le protocole RADIUS en tant que *RADIUS-Access-Request*.

Etape 4. Le serveur RADIUS négocie avec le client en envoyant *RADIUS-Access-Challenge* à l'authentificateur, qui encapsule les informations EAP dans une trame EAPOL et les transmet au client en tant que *EAP-Request*.

Etape 5. En réponse à *EAP-Request*, le client renvoie *EAP-Response* à l'authentificateur, qui décapsule à nouveau les informations EAP et les envoie au serveur d'authentification à l'aide de *RADIUS-Access-Request*.

Etape 6. Il y a plusieurs échanges de *EAP-Response* / *RADIUS-Access-Request* et *RADIUS-Access-Challenge* / *EAP-Request* avant que le serveur RADIUS envoie *RADIUS-Access-Accept*, ce qui signifie que l'utilisateur a été authentifié.

Lorsque cette réponse est reçue par l'authentificateur, ce dernier décapsule les informations EAP et les envoie au client comme *EAP-Success*. Donc, le port est autorisé puis le client est autorisé à communiquer.

Etape 7. A ce stade, le client peut procéder à l'échange de données.

Etape 8. Une fois l'échange de données terminé et le client quitte le port d'accès, il envoie *EAPOL-Logoff* à l'authentificateur pour lui faire savoir qu'il a quitté le port et il peut maintenant être ramené à l'état bloqué ou non autorisé.

3.6. Méthodes d'EAP

La section précédente a expliqué que la trame d'identité *EAP-Request* / *Response* a un champ appelé **Type**. Ce champ a différentes valeurs qui aident également à décider d'utiliser quelle méthode d'authentification EAP après avoir été négociée entre le client et le serveur d'authentification [19].

Chacune de ces méthodes a ses propres avantages et inconvénients. Elles définissent le mécanisme d'authentification à utiliser, qui est généralement évident dans ses noms.

Les méthodes d'EAP peuvent être divisées en plusieurs catégories [21] :

3.6.1. Méthodes EAP basées sur un secret pré-partagé

3.6.1.1. LEAP (lightweight extensible authentication protocol)

Le protocole d'authentification extensible léger est une méthode EAP de type « 17 », il a été développé par *Cisco Systems* et il est également connu sous le nom de *Cisco-EAP*.

Il fournit un mot de passe entre le client et le serveur d'authentification. Il est considéré comme le protocole de *défi-réponse* basé sur un secret pré-partagé ou un mot de passe entre le client et le serveur d'authentification [23].

LEAP offre une authentification mutuelle au lieu d'une authentification unidirectionnelle entre le client et le serveur d'authentification.

L'authentification LEAP commence par une clé secrète pré-partagée. Le client envoie un défi aléatoire au serveur qui décrypte le défi et lui répond en le chiffrant avec la clé de session. Le client déchiffre le défi avec la clé de session et si la valeur du défi est la même que celle qu'il stocke chez le client, le serveur est valide.

De même, le serveur vérifie également le client par une méthode similaire, de sorte que cette authentification mutuelle est obtenue. Cette fonctionnalité élimine les attaques MITM par des points d'accès non autorisés [24].

LEAP crypte les transmissions de données à l'aide de clés WEP générées dynamiquement [19]. LEAP ne prend pas en charge la confidentialité des identités et il est vulnérable aux attaques par dictionnaires [23].

La pratique recommandée impose que si vous devez utiliser LEAP, cela ne doit être fait qu'avec des mots de passe suffisamment complexes [19].

3.6.2. Méthodes EAP basées sur une clé publique

3.6.2.1. EAP-TLS (Transport Layer Security)

EAP-TLS est une méthode de type « 13 » développée par Microsoft. Il est d'abord publié dans la RFC 2716 en octobre 1999, qui a été remplacé par la RFC 5216 en mars 2008. Il repose sur la sécurité de la couche de transport.

EAP-TLS utilise une phase de prise de contact TLS « *TLS Handshake phase* » pour authentifier le client et le serveur d'authentification [23].

Il utilise un certificat numérique d'infrastructure à clé publique (PKI) pour le client et le serveur d'authentification afin de fournir une authentification mutuelle entre eux. Le certificat PKI contiendra des informations sur le nom du serveur ou des informations sur le client. Cela

donne un moyen d'authentification mutuelle basée sur des certificats X.509 entre le client et l'authentificateur et entre l'authentificateur et le client.

Il génère et distribue de manière dynamique des clés de chiffrement basées sur le client et sur la session pour sécuriser les connexions. Les principales fonctionnalités fournies par EAP-TLS sont l'échange et l'établissement de clés, l'authentification mutuelle, la prise en charge de la fragmentation et du réassemblage et la reconnexion rapide [24].

Comme EAP-TLS utilise des certificats, il hérite de tous les problèmes liés avec eux tels qu'un problème de certificats non chiffrés ou un problème de vérification différée du certificat.

Le premier problème provient du fait que les certificats sont envoyés non chiffrés. Il en résulte une identité révélatrice qui est perdue dans la conversation.

Le deuxième problème vient du fait que le client est incapable de vérifier la signature ou la chaîne de certificats. De plus, le client ne peut pas vérifier si le certificat du serveur d'authentification a été révoqué entre-temps. Par conséquent, il n'y a aucun autre moyen pour éviter le problème à l'exception du report de la vérification.

EAP-TLS peut être considéré comme une méthode EAP sécurisée, de sorte qu'il est largement déployé dans de nombreuses applications. Il résiste à la plupart des attaques, telles que les attaques MITM [23].

Un inconvénient majeur d'EAP-TLS est qu'il est difficile de gérer les certificats dans un réseau de grande entreprise. Par exemple, le personnel informatique doit installer un nouveau certificat après l'achat d'un nouvel ordinateur portable ou de tout autre équipement qui utilisera l'authentification EAP-TLS.

3.6.3. Méthodes EAP basées sur les tunnels

3.6.3.1. EAP-TTLS (Tunnel Transport Layer Security)

EAP-TTLS est une méthode EAP de type « 21 » développée par *Funk Software* et *Certicom* [25].

EAP-TTLS est décrit dans la RFC 5281. Il s'agit d'une extension d'EAP-TLS qui élimine le certificat numérique PKI côté client et réduit la complexité de la mise en œuvre de TLS [24].

C'est une méthode basée sur le protocole TLS. L'authentification dans EAP-TTLS est généralement mutuelle, c'est-à-dire que le serveur d'authentification et le client s'authentifient mutuellement. Il utilise le certificat pour authentifier le serveur d'authentification et une méthode d'authentification plus simple pour authentifier le client.

Il se compose de deux phases : la phase de prise de contact TLS et la phase de tunnel TLS. Dans la première phase, le serveur d'authentification est authentifié auprès du client à l'aide du certificat X.509 du serveur. Une fois la première phase terminée, le tunnel sécurisé est établi.

Dans la deuxième phase, toutes les communications sont protégées par ce canal sécurisé. Le client est authentifié auprès du serveur d'authentification à l'aide des méthodes d'authentification héritées, telles que le mot de passe en texte clair ou le mot de passe de défi-réponse, ou un mécanisme d'authentification plus avancé, tel que l'authentification par jeton.

EAP-TTLS prend en charge la protection d'identité car un attaquant ne peut pas voir l'identité de l'utilisateur, car l'identité peut être envoyée dans la deuxième phase. Cependant, EAP-TTLS est connu pour être vulnérable à l'attaque MITM. Les protocoles tunnelés nécessitent la clé de session dérivée de la première phase, qui est utilisée pour fournir un tunnel sécurisé.

Dans un certain environnement, un client est autorisé à sauter la première phase et à passer directement à la deuxième phase. Dans ce cas, l'attaque MITM peut avoir lieu si l'attaquant peut détourner une session d'authentification valide. Cependant, un schéma de liaison cryptographique a été proposé pour protéger la méthode EAP basée sur un tunnel de l'attaque MITM. Par conséquent, EAP-TTLS peut être considéré comme sécurisé si une liaison cryptographique est appliquée [23].

3.6.3.2. EAP-FAST (Flexible Authentication via Secure Tunnel)

EAP-FAST est une méthode de type « 43 » créée par *Cisco Systems* comme une alternative à PEAP qui permet des réauthentifications plus rapides et prend en charge une itinérance sans fil plus rapide.

Tout comme PEAP, FAST forme un tunnel externe TLS, puis transmet les informations d'identification du client dans ce tunnel TLS. Là où FAST diffère du PEAP, c'est la possibilité d'utiliser des informations d'identification d'accès protégées (PAC) [21].

En général, EAP-FAST utilise le protocole *TLS handshake protocol* pour établir un tunnel mutuellement authentifié entre le client et le serveur d'authentification.

Le tunnel sécurisé peut être établi en utilisant soit la clé publique similaire à EAP-TLS, soit une clé symétrique pré-partagée connue sous le nom de PAC.

Le PAC peut être considéré comme un jeton de sécurité fourni au client par le serveur pour établir un tunnel sécurisé pour une future authentification réseau optimisée.

EAP-FAST se compose de deux phases. Dans la première phase, le client utilise le PAC pour établir le tunnel TLS sécurisé. Si le client n'a pas le PAC correspondant, le serveur demande au client d'initier le TLS Handshake complet (la poignée de main).

A la suite de cette prise de contact TLS complète, le client demande au serveur d'émettre le PAC qui peut être utilisé pour établir le tunnel TLS ultérieurement.

Dans la deuxième phase, l'authentification EAP-TLS ou les authentifications EAP-TLS héritées peuvent être utilisées pour authentifier le client dans le tunnel sécurisé.

Le PAC se compose de trois composants : un secret partagé, un élément opaque et d'autres informations facultatives. Le secret partagé est utilisé pour établir le tunnel sécurisé. L'élément opaque est fourni au client et présenté au serveur lorsque le client souhaite obtenir l'accès à la ressource réseau. L'élément opaque peut inclure le PAC et l'identité du client. Le serveur utilise un algorithme cryptographique fort pour protéger l'élément opaque afin de récupérer les informations nécessaires au serveur pour identifier et authentifier le client. Les autres informations peuvent contenir pour assurer l'intégrité de l'émetteur du PAC.

Il existe trois types de méthodes d'authentification :

Une authentification basée sur un certificat qui est utilisée dans EAP-TLS, une authentification combinée qui est utilisée dans EAP-TTLS, ou une authentification basée sur un PAC. Dans une authentification basée sur des certificats, le client et le serveur d'authentification utilisent les certificats pour s'authentifier mutuellement. Dans une authentification basée sur un PAC, le client utilise le PAC pour établir un tunnel TLS. Par conséquent, EAP-FAST est considéré comme une méthode EAP efficace qui combine les caractéristiques d'EAP-TLS et EAP-TTLS et adopte l'idée d'utiliser EAP-TLS avec une clé pré-partagée. En résumé, EAP-FAST est une méthode EAP très flexible qui est destinée à

l'équipement mobile restreint car elle prend en charge l'authentification mutuelle en utilisant une clé pré-partagée [23].

L'avantage d'EAP-FAST est qu'une entreprise n'a pas besoin de déployer de certificats numériques [25].

3.6.3.3. PEAP (Protected Extensible Authentication Protocol)

PEAP est une méthode de type « 25 » propriétaire développée par *Microsoft*, *Cisco* et *RSA Security*. PEAP fournit un tunnel chiffré et authentifié utilisant le protocole TLS Handshake, qui encapsule d'autres mécanismes d'authentification pour le client.

Il utilise TLS pour se protéger contre les clients non autorisés, se protéger contre diverses attaques contre la confidentialité et l'intégrité de l'échange de méthodes EAP interne et pour assurer la confidentialité de l'identité des clients EAP. Il fournit également un support pour le chaînage de plusieurs mécanismes EAP, la liaison cryptographique entre les authentifications effectuées par les mécanismes EAP internes et le tunnel, l'échange de paramètres arbitraires, la fragmentation et le réassemblage.

PEAP utilise la cryptographie à clé publique pour l'authentification et la négociation de la clé qui peut être utilisée pour crypter les données. PEAP utilise également TLS pour l'authentification et le cryptage du serveur, mais évite le besoin de certificats utilisateur en utilisant un deuxième protocole d'authentification entre le client et le serveur d'authentification, qui est protégé par le cryptage TLS. Le principe de base d'EAP-TTLS et PEAP est presque identique. La principale différence entre eux réside dans le fait que PEAP ne peut utiliser que des méthodes d'authentification héritées telles que l'authentification par *ID / mot de passe* dans la deuxième phase, alors qu'EAP-TTLS peut utiliser d'autres méthodes EAP ou des méthodes d'authentification héritées. Cependant, il est toujours dans le projet Internet de l'IETF en décembre 2008 [23].

3.6.4. Comparaison entre les méthodes d'EAP

| Types EAP / Caractéristiques | LEAP | PEAP | FAST | TLS | TTLS |
|---|---|---------------------------------------|--------------------------|---|---------------------------------------|
| Authentification coté client | Mot de passe(haché) | Certificat, compte/mot de passe | Mot de passe (PAC) | Certificat | Certificat, compte/mot de passe |
| Authentification coté serveur | Mot de passe(haché) | Certificat | Mot de passe (PAC) | Certificat | Certificat |
| Gestion des clés WEP | Oui | Oui | Oui | Oui | Oui |
| Détection des points d'accès non autorisés | Oui | Non | Oui | Non | Non |
| Fournisseur | Cisco | MS | Cisco | MS | Funk |
| Attributs d'authentification | Mutuelle | Mutuelle | Mutuelle | Mutuelle | Mutuelle |
| Difficulté de déploiement | Modéré | Modéré | Modéré | Difficile (en raison du déploiement du certificat client) | Modéré |
| Sécurité Wi-Fi | Élevée lorsque des mots de passe forts sont utilisés. | Élevée | Élevée | Très élevée | Élevée |
| Niveau de sécurité | + | ++++ | +++ | +++++ | ++++ |

| | | | | | |
|--|---|--------------|--------------------------|--------------------------------|--------------|
| Risques de sécurité | Attaque par dictionnaire et obtention du login client | Attaque MITM | Attaque par dictionnaire | Obtention de l'identité client | Attaque MITM |
| Distribution dynamique des clés | Oui | Oui | Oui | Oui | Oui |
| Protection d'identité | Non | Oui | Oui | Non | Oui |
| Longueur de clé | 2048 bits | / | 128 bits, 2048 bits | 2048 bits | 2048 bits |
| Protection d'intégrité | Non | Oui | Oui | Oui | Oui |
| Confidentialité | Non | Oui | Oui | Oui | Oui |

Tableau 3.1 : Comparaison entre les méthodes EAP [19-23-26-27-28].

3.7. 802.1X Host Modes

Un Host Mode sur un port 802.1X activé « *802.1X-enabled port* » décide d'autoriser un seul client à s'authentifier ou d'autoriser plusieurs clients ou une autre condition spéciale.

Quatre Host Modes sont disponibles et un mode est appliqué avec les quatre autres modes. Les quatre Host Modes sont les suivants :

- **Single-host mode ;**
- **Multiple-host mode ;**
- **Multidomain authentication mode ;**
- **Multiauthentication mode.**

Pre-authentication open access est le mode appliqué avec les quatre autres modes. Les sections qui suivent décrivent ces modes plus en détail et comment les configurer.

3.7.1. Single-Host Mode

Dans ce mode, un seul client peut être connecté à un port 802.1X activé. La commande utilisée pour configurer ce mode est la suivante :

```
SW(config-if)#authentication host-mode single-host
```

3.7.2. Multiple-Host Mode

Dans ce mode, plusieurs clients sont connectés à un port 802.1X activé. La caractéristique de ce mode est qu'un seul client doit être autorisé pour tous les clients pour avoir l'accès au réseau. La commande utilisée pour configurer ce mode est la suivante :

```
SW(config-if)#authentication host-mode multi-host
```

3.7.3. Multidomain Authentication Mode

Dans ce mode, également appelé MDA, un téléphone IP et un seul PC derrière le téléphone IP sont authentifiés indépendamment, même si le téléphone IP et le PC sont connectés à un seul port de switch.

Le Multidomain dans ce mode fait référence à deux domaines : **Data domain** et **Voice domain**.

Seules deux adresses MAC sont autorisées sur un port où MDA est activé. Le switch peut placer le PC dans un Data VLAN et le téléphone IP dans un Voice VLAN, même s'ils apparaissent sur le même port de switch. La commande utilisée pour configurer ce mode est la suivante :

```
SW(config-if)#authentication host-mode multi-domain
```

3.7.4. Multiauthentication Mode

Également connu sous le nom de multiauth mode, ce mode permet d'avoir un client 802.1X sur un voice VLAN et plusieurs clients 802.1X authentifiés sur un data VLAN. Dans ce mode, chaque client connecté doit être authentifié individuellement ; c'est la principale différence

entre le multiple-host mode et multiauth mode. La commande utilisée pour configurer ce mode est la suivante :

```
SW(config-if)#authentication host-mode multi-auth
```

3.7.5. Pre-Authentication Open Access Mode

Ce mode, qui peut être utilisé avec les quatre host modes, permet à un appareil d'accéder au réseau avant l'authentification. Ceci est utile pour tester la fonctionnalité 802.1X; c'est comme une fonctionnalité pilote qui est désactivée une fois que l'administrateur est à l'aise avec le déploiement 802.1X. Chaque fois que cela est appliqué sur un port de switch, il est toujours recommandé d'utiliser des ACLs statiques pour limiter le trafic de la couche 3.

Pre-authentication open access peut être configuré en plus avec l'un des quatre host modes. La commande utilisée pour configurer ce mode est la suivante :

```
SW(config-if)#authentication open
```

3.8. Fonctionnalités de l'authentification 802.1X

3.8.1. MAC Authentication Bypass « MAB »

La fonction de *MAC Authentication Bypass* (MAB) est utilisée pour autoriser les clients en fonction de leurs adresses MAC. Cela peut être utile dans les scénarios où l'authentification 802.1X expire en attendant une requête *EAPOL-response* du client connecté au port, auquel cas le switch essaiera d'autoriser le client à l'aide de MAB. Les équipements tels que les imprimantes, les télécopieurs, etc. entrent dans cette catégorie.

Lorsque cette fonctionnalité est activée, le switch utilise l'adresse MAC comme identité du client. Pour que cela réussisse, le serveur d'authentification doit disposer d'une base de données d'adresses MAC client autorisées.

Une fois qu'un client est détecté sur le port, le switch attend une trame Ethernet du client. Le switch envoie ensuite un *RADIUS-access/request* au serveur d'authentification comme illustré sur la figure 3.7.

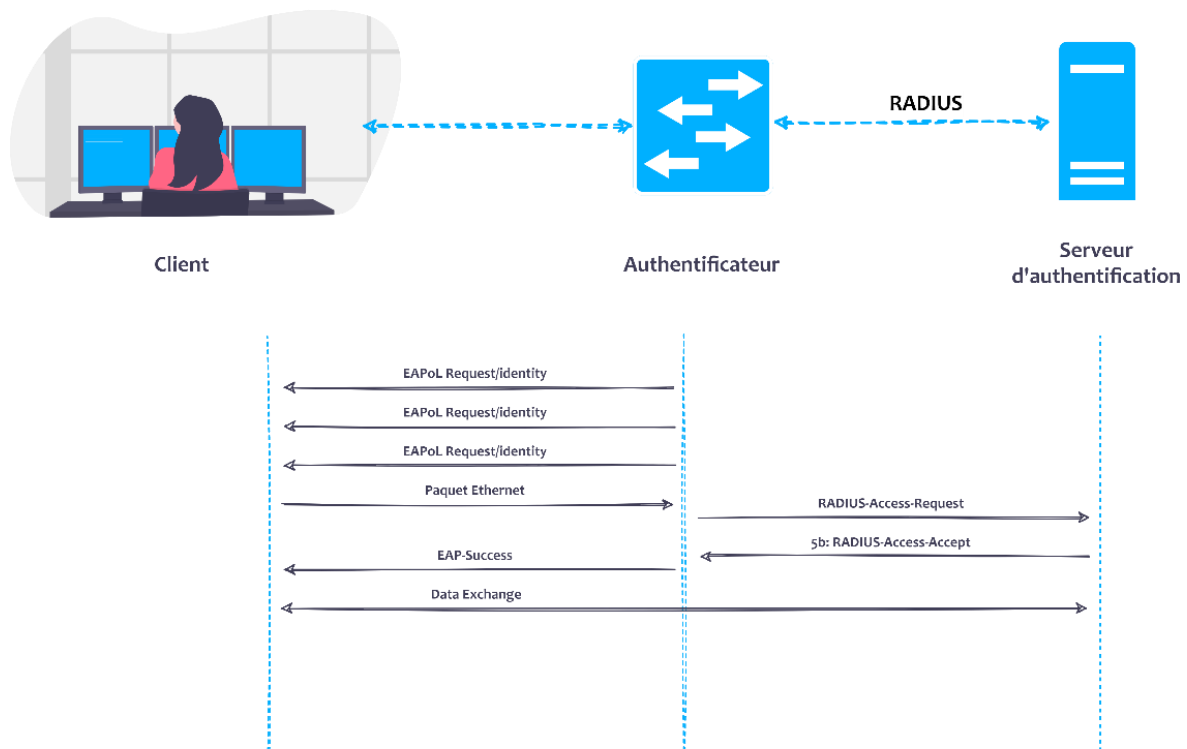


Figure 3.7 : MAC Authentication Bypass (MAB).

La commande utilisée pour configurer la fonctionnalité MAB est la suivante :

```
SW(config-if)#mab
```

3.8.2. VLAN Assignment

Cette fonction est utilisée pour spécifier un VLAN auquel un utilisateur doit être affecté après une authentification 802.1X réussie. Pendant l'authentification, le serveur d'authentification peut envoyer des informations de *VLAN assignment* au switch afin qu'un utilisateur puisse être affecté à un VLAN.

Cette fonction est automatiquement activée lors de la configuration de l'authentification 802.1X sur un port d'accès. Pour qu'elle fonctionne, il faut assurer que l'autorisation est configurée sur le switch pour permettre la configuration de l'interface à partir du serveur d'authentification.

3.8.3. Guest VLAN

Cette fonction est utilisée pour fournir des services limités aux clients *non-802.1X-compliant*. Lors de l'activation de cette fonction sur un port 802.1X, le switch affecte des clients à un *guest VLAN* lorsqu'il ne reçoit pas de réponse à sa trame *EAP request/identity* ou lorsque les paquets EAPOL ne sont pas envoyés par le client et qu'aucune méthode d'authentification de secours n'est activée.

Par défaut, le switch conserve l'historique des paquets EAPOL. Si un paquet EAPOL est détecté sur l'interface pendant la durée de vie de la liaison, le switch détermine que l'équipement connecté à cette interface est un client *802.1X-capable*, et l'interface ne passera pas à l'état *guest VLAN*. L'historique des paquets EAPOL est effacé si l'état de la liaison d'interface baisse.

Pour passer un client *non-802.1X-capable* à l'état *guest VLAN*, quel que soit l'historique des paquets EAPOL, la commande de configuration globale utilisée est la suivante :

```
SW(config)#dot1x guest-vlan supplicant
```

Pour configurer un *guest VLAN*, la commande utilisée est la suivante :

```
SW(config-if)#authentication event no-response action  
authorize vlan vlan-id
```

3.8.4. Restricted / Failed VLAN

Pour fournir un service limité aux clients qui échouent à l'authentification, un *restricted VLAN* ou un *failed VLAN* peuvent être configurés. Une chose qui doit être notée est que ces clients sont des 802.1X-compliant, donc ils ne peuvent pas être assignés au *guest VLAN*.

Un port peut être configuré pour qu'il se trouve dans un *restricted VLAN* après un nombre spécifié de tentatives d'authentification ayant échoué. Le switch compte les tentatives d'authentification ayant échoué, le nombre de tentatives ayant échoué s'incrémentant lorsque le serveur RADIUS répond par *Access-Reject EAP failure* ou une réponse vide sans paquet EAP. Lorsque ce nombre dépasse le nombre maximal configuré de tentatives d'authentification, le port est attribué au *restricted VLAN*.

Une fois qu'un port a été déplacé vers le *restricted VLAN*, le compteur de tentatives ayant échoué pour le port est réinitialisé et les messages *EAPOL-Start* du client sont ignorés. La valeur par défaut de *retries* est 2 et est configurable de 1 à 5.

Pour configurer un *restricted VLAN*, la commande utilisée est la suivante [20] :

```
SW(config-if)#authentication event fail [retry  
retries] action authorize vlan vlan-id
```

3.8.5. Downloadable ACLs « DACLs »

Une *Downloadable ACL* (DACL), également appelée « *per-user ACL* », est une ACL qui peut être appliquée dynamiquement à un port. Le terme « *downloadable* » provient du fait que ces ACL sont poussées du serveur d'authentification (par exemple, à partir d'un Cisco ISE) pendant la phase d'autorisation.

Lorsqu'un client s'authentifie sur le port, le serveur d'authentification peut envoyer une DACL qui sera appliquée au port et qui limitera les ressources auxquelles le client peut accéder sur le réseau [3].

3.9. 802.1X Timers

La configuration de 802.1X sur un switch peut ne pas être suffisante pour le faire fonctionner. Les timers peuvent être modifiés pour le faire fonctionner de manière acceptable. Il existe différents timers disponibles qui peuvent être modifiés pour obtenir le résultat souhaité. Les sections qui suivent présentent quelques-uns de ces timers, notamment les suivants :

- Quiet period ;
- Switch-to-client retransmission time (tx-period) ;
- Switch-to-client retransmission time for EAP-Request frames (supp-timeout) ;
- Switch-to-authentication-server retransmission time for Layer 4 packets (server-timeout) ;
- Switch-to-client frame retransmission number (max-reauth-req).

3.9.1.1. Quiet period

Lorsque le switch ne peut pas authentifier le client pour une raison quelconque (par exemple, l'authentification a échoué), le switch reste inactif pendant une période définie, puis réessaye. Le temps d'inactivité est déterminé par la valeur de *quiet-period*.

La valeur par défaut est 60 secondes. Ce timer peut être modifié pour fournir une réponse plus rapide. Pour configurer ce timer, la commande suivante est utilisée :

```
SW(config-if)#dot1x timeout quiet-period seconds
```

La plage de valeurs pour le paramètre *seconds* est comprise entre 0 et 65 535 secondes.

3.9.1.2. Tx-period

Le client répond à la trame *EAP-request/identity* à partir du switch avec une trame de *EAP-response/identity*. Si le switch ne reçoit pas cette réponse, il attend une période de temps définie, connue sous le nom de *retransmission time*, puis retransmet la trame. La durée pendant laquelle le switch attend la notification peut être modifiée de 1 à 65 535 secondes. La valeur par défaut est de 30 secondes. Pour configurer ce timer, la commande suivante est utilisée :

```
SW(config)#dot1x timeout tx-period seconds
```

3.9.1.3. Supp-timeout

Le client informe le switch qu'il a reçu la trame *EAP-request*. Si le switch ne reçoit pas cette notification, le switch attend une période de temps définie, puis retransmet la trame. Ce timer peut être modifié pour définir la durée pendant laquelle le switch attend la notification de 1 à 65 535 secondes. La valeur par défaut est de 30 secondes. Pour configurer ce timer, la commande suivante est utilisée :

```
SW(config-if)#dot1x timeout supp-timeout seconds
```

3.9.1.4. Server-timeout

Le serveur d'authentification notifie le switch chaque fois qu'il reçoit un paquet de couche transport (couche 4). Lorsque le switch ne reçoit pas de notification après l'envoi d'un paquet, il attend une période de temps définie, puis retransmet le paquet. Cela peut être modifié pour

définir la durée pendant laquelle le switch attend la notification de 1 à 65 535 secondes. La valeur par défaut est de 30 secondes. Pour configurer ce timer, la commande suivante est utilisée :

```
SW(config-if)#dot1x timeout server-timeout seconds
```

3.9.1.5. Max-reauth-req

Le client informe le switch qu'il a reçu la trame *EAP-request*. Si le switch ne reçoit pas cette notification, il attend une période de temps définie, puis retransmet la trame. Outre le réglage de *supp-timeout*, le nombre de fois que le switch envoie une trame *EAP-request/identity* peut être modifié au client avant de redémarrer le processus d'authentification de 1 à 10. La valeur par défaut est 2. Pour configurer ce timer, la commande suivante est utilisée [19] :

```
SW(config-if)#dot1x max-reauth-req count
```

3.10. Conclusion

Le protocole 802.1X permet de contrôler l'accès aux équipements et infrastructures réseau et assurer la dynamique et la mobilité du réseau en introduisant quelques-unes de ses fonctionnalités. Il fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil. Cette sécurité se traduit par une authentification préalable à l'accès au réseau.

Au cours du prochain chapitre, nous entamerons la partie pratique de ce projet en implémentant les mécanismes de sécurité du modèle AAA et du protocole 802.1X étudiés théoriquement dans les chapitres précédents.

CHAPITRE 4

IMPLEMENTATION

4.1. Introduction

Après avoir décrit les principes de la sécurité des réseaux et détaillé les mécanismes du modèle AAA ainsi le protocole 802.1X, son importance et la nécessité de son déploiement dans les réseaux actuels, à présent nous voudrions démontrer ces aspects pratiquement en utilisant des équipements réseaux et des solutions du constructeur Cisco.

En premier lieu, nous avons mis en place une topologie sur laquelle nous avons implémenté notre solution. Dans un second lieu, nous avons configuré la sécurité 802.1X en détaillant les étapes suivies et en capturant les résultats obtenus.

La figure 4.1 illustre la topologie sur laquelle nous avons travaillé et le tableau 4.1 résume les matériels et les outils utilisés.

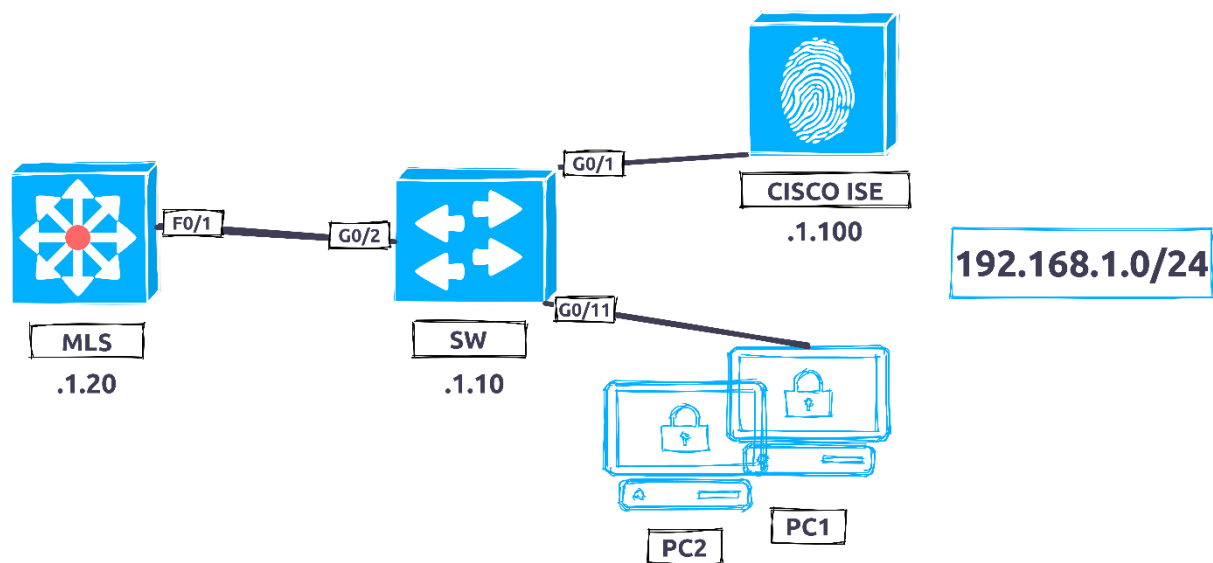


Figure 4.1 : Topologie de 802.1X.

| | |
|------------------|---|
| Matériels | <ul style="list-style-type: none"> - 3 PC Desktops avec un système Linux Centos 7. - PC Laptop Windows 10 doté d'un logiciel Putty pour accès et configuration des équipements. - Switch d'accès 2960G. - Switch Multi-Layer 3560. - Cisco ISE Virtual Appliance Version 2.0 |
| Outils | Vmware Workstation Version 15 |

Tableau 4.1 : Matériels et outils utilisés.

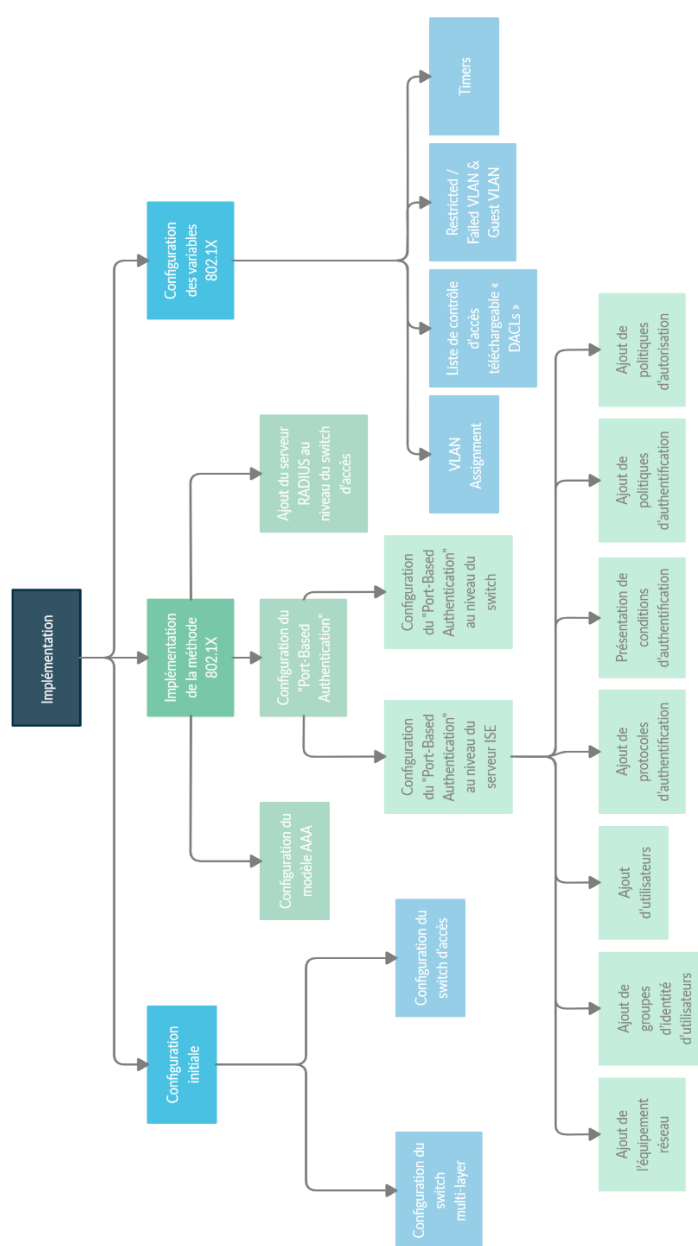


Figure 4.2 : Récapitulation de la partie pratique.

4.2. Configuration initiale

4.2.1. Configuration du switch d'accès « *authentificateur* »

4.2.1.1. Ajout d'un utilisateur d'administration

```
!  
username Utilisateur1 secret Admin12  
enable secret Admin123@  
!
```

4.2.1.2. Création des VLANs

```
!  
vlan 1  
    name Vlan1  
vlan 2  
    name ResVlan  
vlan 3  
    name GuVlan  
vlan 10  
    name Vlan10  
vlan 20  
    name Vlan20  
!
```

4.2.1.3. Configuration de line vty

```
!  
line vty 0 4  
    transport input all  
!
```

4.2.1.4. Configuration de l'interface VLAN 1

```
!  
interface vlan 1  
    IP address 192.168.1.10 255.255.255.0  
!
```

4.2.1.5. Configuration de l'interface connectée à l'ordinateur

```
!  
interface gigabitEthernet 0/11  
    switchport mode access  
    switchport access vlan 1  
!
```

4.2.1.6. Configuration de l'interface connectée au serveur ISE

```
!  
interface gigabitEthernet 0/1  
    switchport mode access  
    switchport access vlan 1  
!
```

4.2.1.7. Configuration de l'interface connectée au switch multi-layer en mode trunk

```
!  
interface gigabitEthernet 0/2  
    switchport mode trunk  
!
```

4.2.2. Configuration du switch multi-layer

4.2.2.1. Configuration du routage inter-vlan

4.2.2.1.1. Création des VLANs

```
!  
vlan 1  
    name Vlan1  
vlan 2  
    name ResVlan  
vlan 3  
    name GuVlan  
vlan 10  
    name Vlan10  
vlan 20  
    name Vlan20  
!
```

4.2.2.1.2. Configuration de l'interface VLAN 1

```
!  
interface vlan 1  
    IP address 192.168.1.20 255.255.255.0  
!
```

4.2.2.1.3. Configuration de l'interface connectée au switch d'accès en mode trunk

```
!  
interface fastEthernet 0/1  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!
```

4.2.2.1.4. Activation de routage

```
!  
ip routing  
!
```

4.2.2.1.5. Configuration des SVI (Switch Virtual Interfaces)

```
!  
interface vlan 1  
    IP address 192.168.1.20 255.255.255.0  
    no shutdown  
interface vlan 2  
    ip address 192.168.2.1 255.255.255.0  
    no shutdown  
interface vlan 3  
    ip address 192.168.3.1 255.255.255.0  
    no shutdown  
interface vlan 10  
    ip address 192.168.10.1 255.255.255.0  
    no shutdown  
interface vlan 20  
    ip address 192.168.20.1 255.255.255.0  
    no shutdown  
!
```

4.2.2.2. Création des pools DHCP

```
!  
ip dhcp pool one  
    network 192.168.1.0 255.255.255.0  
    default-router 192.168.1.20  
ip dhcp pool two  
    network 192.168.2.0 255.255.255.0  
    default-router 192.168.2.1  
ip dhcp pool three  
    network 192.168.3.0 255.255.255.0  
    default-router 192.168.3.1  
ip dhcp pool four  
    network 192.168.10.0 255.255.255.0  
    default-router 192.168.10.1  
ip dhcp pool five  
    network 192.168.20.0 255.255.255.0  
    default-router 192.168.20.1  
!
```


4.2.3. Les tests de connectivité

4.2.3.1. Configuration automatique de l'adresse IPv4 du client

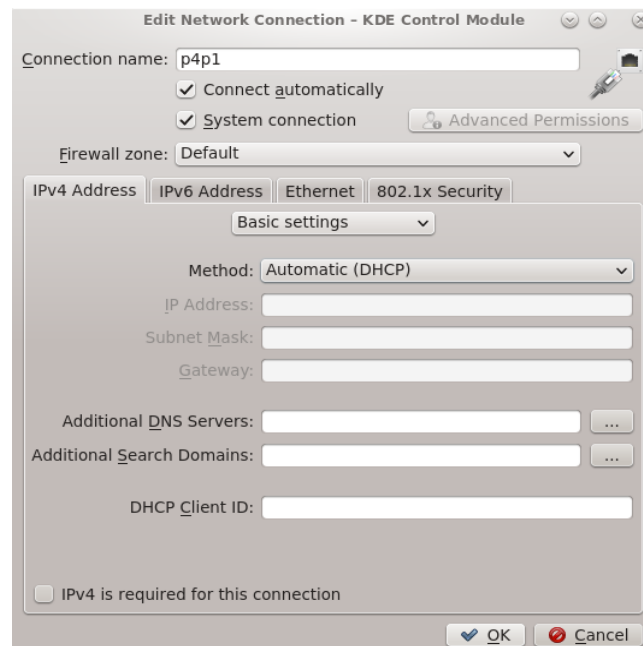


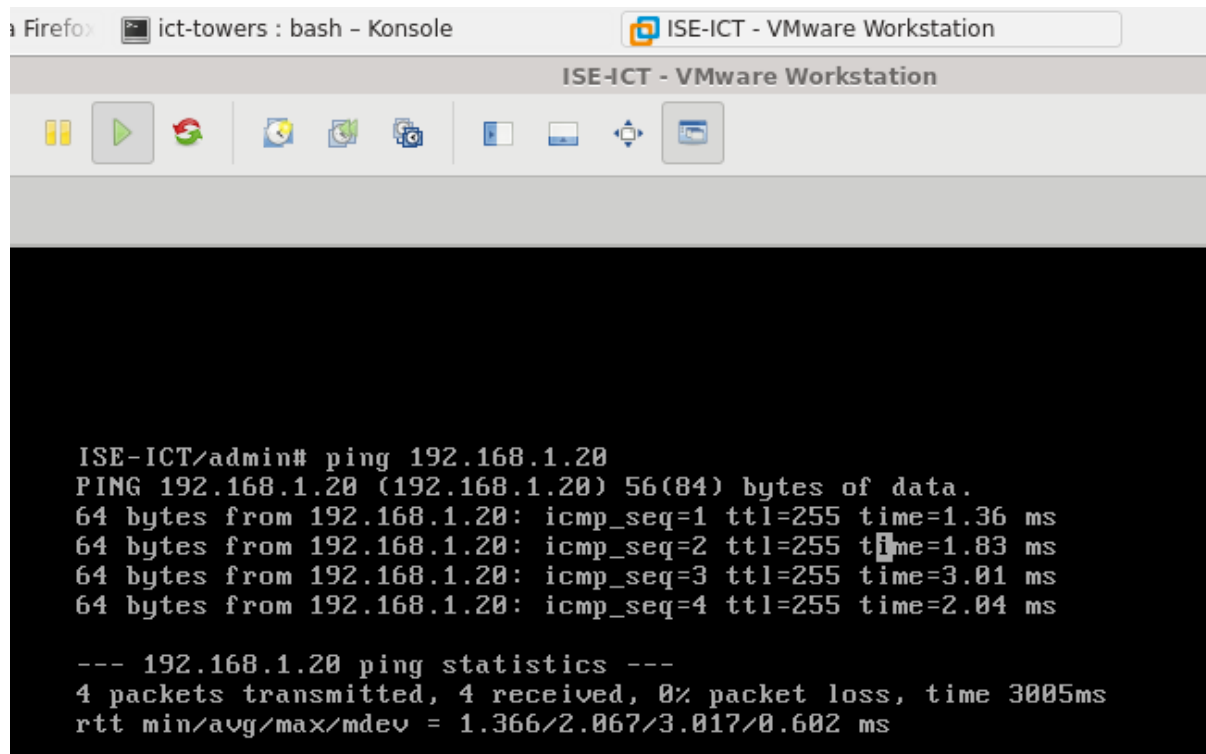
Figure 4.3 : Configuration automatique de l'adresse IPv4 du client.

4.2.3.2. Test de connectivité entre le client (192.168.1.1) et le MLS (192.168.1.20)

```
ict-towers : bash - Konsole
File Edit View Bookmarks Settings Help
[ict-towers@localhost ~]$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data:
64 bytes from 192.168.1.20: icmp_seq=1 ttl=255 time=0.654 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=255 time=0.629 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=255 time=0.664 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=255 time=0.658 ms
^C
--- 192.168.1.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.629/0.651/0.664/0.022 ms
[ict-towers@localhost ~]$
```

Figure 4.4 : Test de connectivité entre le client (192.168.1.1) et le MLS (192.168.1.20).

4.2.3.3. Test de connectivité entre le serveur ISE (192.168.1.100) et le MLS (192.168.1.20)



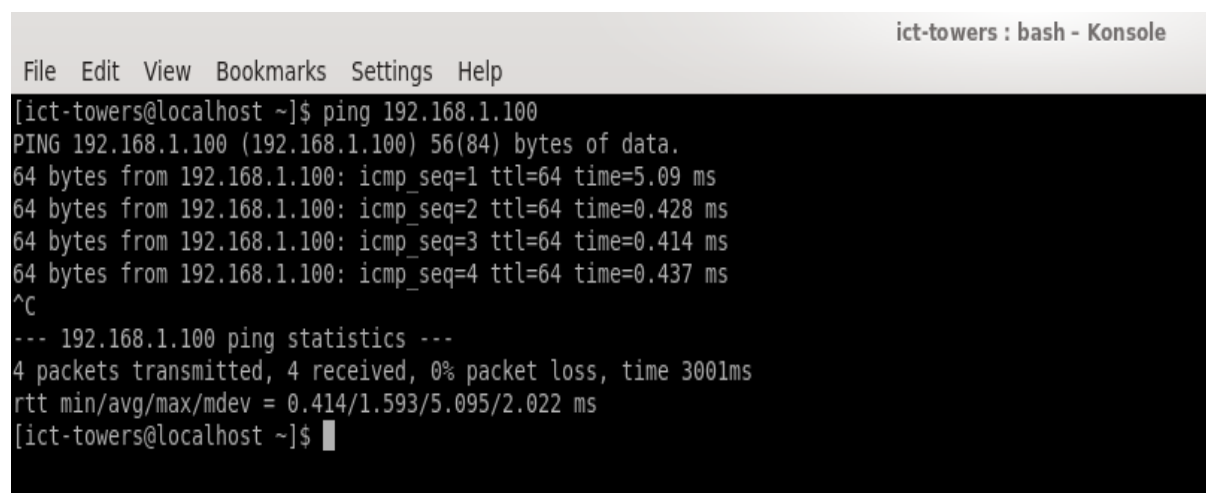
The screenshot shows a terminal window titled 'ict-towers : bash - Konsole' within an 'ISE-ICT - VMware Workstation' environment. The terminal output displays a successful ping test from the ISE-ICT server to the MLS server.

```
ISE-ICT/admin# ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data:
64 bytes from 192.168.1.20: icmp_seq=1 ttl=255 time=1.36 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=255 time=1.83 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=255 time=3.01 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=255 time=2.04 ms

--- 192.168.1.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.366/2.067/3.017/0.602 ms
```

Figure 4.5 : Test de connectivité entre le serveur ISE (192.168.1.100) et le MLS (192.168.1.20).

4.2.3.4. Test de connectivité entre le client (192.168.1.1) et le serveur ISE (192.168.1.100)



The screenshot shows a terminal window titled 'ict-towers : bash - Konsole'. The terminal output displays a successful ping test from the client to the ISE server.

```
[ict-towers@localhost ~]$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=5.09 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.428 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.414 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.437 ms
^C
--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.414/1.593/5.095/2.022 ms
[ict-towers@localhost ~]$
```

Figure 4.6 : Test de connectivité entre le client (192.168.1.1) et le serveur ISE (192.168.1.100).

4.3. Implémentation de la méthode 802.1X

4.3.1. Configuration initiale du modèle AAA

```
!  
aaa new-model  
aaa authentication login default group radius local  
aaa authentication dot1x default group radius  
aaa authorization network default group radius  
aaa accounting dot1x default start-stop group radius  
!
```

4.3.2. Ajout du serveur Radius au niveau du switch d'accès

```
!  
Radius server Ser-Radius  
    address ipv4 192.168.1.100 auth-port 1812 acct-port 1813  
    key cisco123  
ip radius source-interface Vlan1  
aaa server radius dynamic-author  
    client 192.168.1.100 server-key cisco123  
radius-server vsa send authentication  
radius-server vsa send accounting  
radius-server attribute 6 on-for-login-auth  
radius-server attribute 8 include-in-access-req  
!
```

4.3.3. Configuration du « *Port-Based Authentication* »

4.3.3.1. Configuration du « *Port-Based Authentication* » au niveau de switch :

```
!  
dot1x system-auth-control  
interface gigabitEthernet 0/11  
    switchport mode access  
    spanning-tree portfast  
    spanning-tree bpduguard enable  
    authentication port-control auto  
    authentication host-mode multi-auth  
    authentication open  
    dot1x pae authenticator  
    exit  
!
```

4.3.3.2. Configuration du « *Port-Based Authentication* » au niveau du serveur ISE

En accédant à l'adresse IP de gestion d'ISE, qui est 192.168.1.100, l'écran suivant apparaîtra.

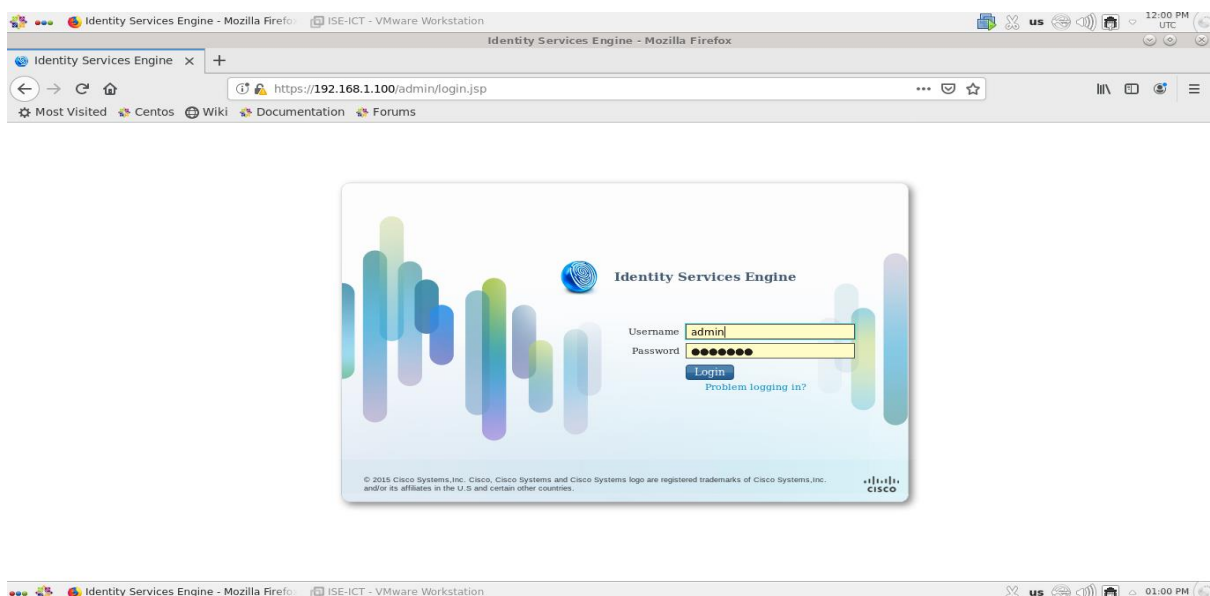


Figure 4.7 : Ecran de gestion du serveur ISE.

En utilisant le nom d'utilisateur et le mot de passe appropriés, le tableau de bord suivant apparaîtra, après une connexion réussie.

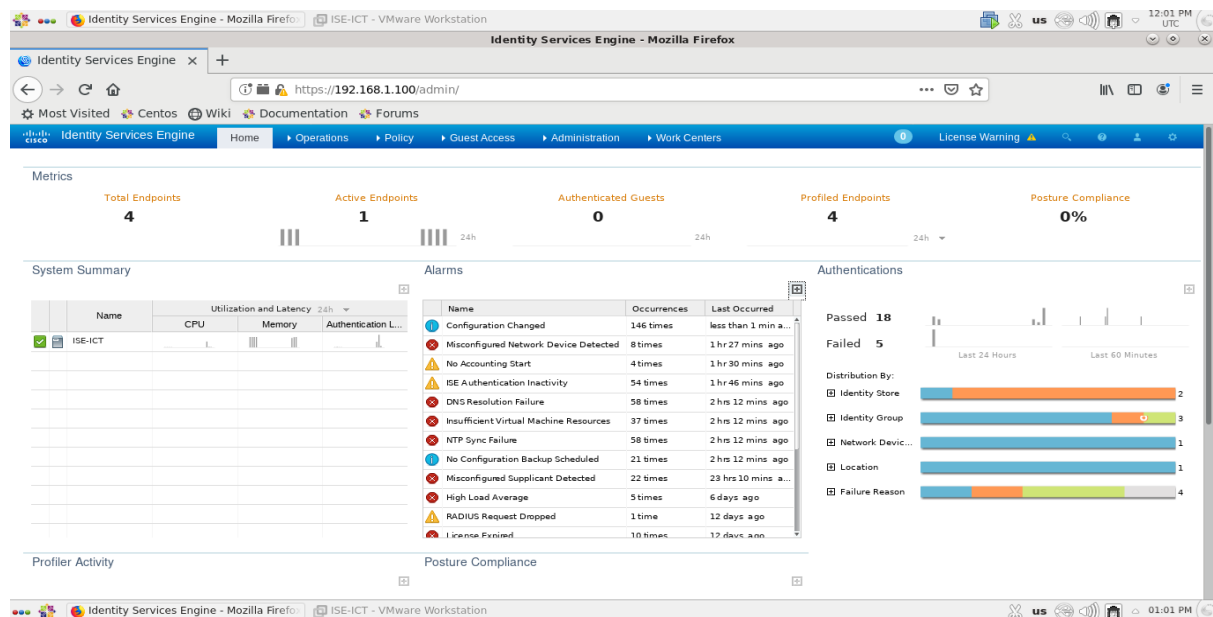


Figure 4.8 : Ecran d'accueil du serveur ISE.

4.3.3.2.1. Ajout de l'équipement réseau (Switch d'Accès)

Afin d'ajouter un équipement réseau, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Administration”** > **“Network Resources”** > **“Network Devices”** > **“Network Devices”**, l'écran suivant apparaîtra.

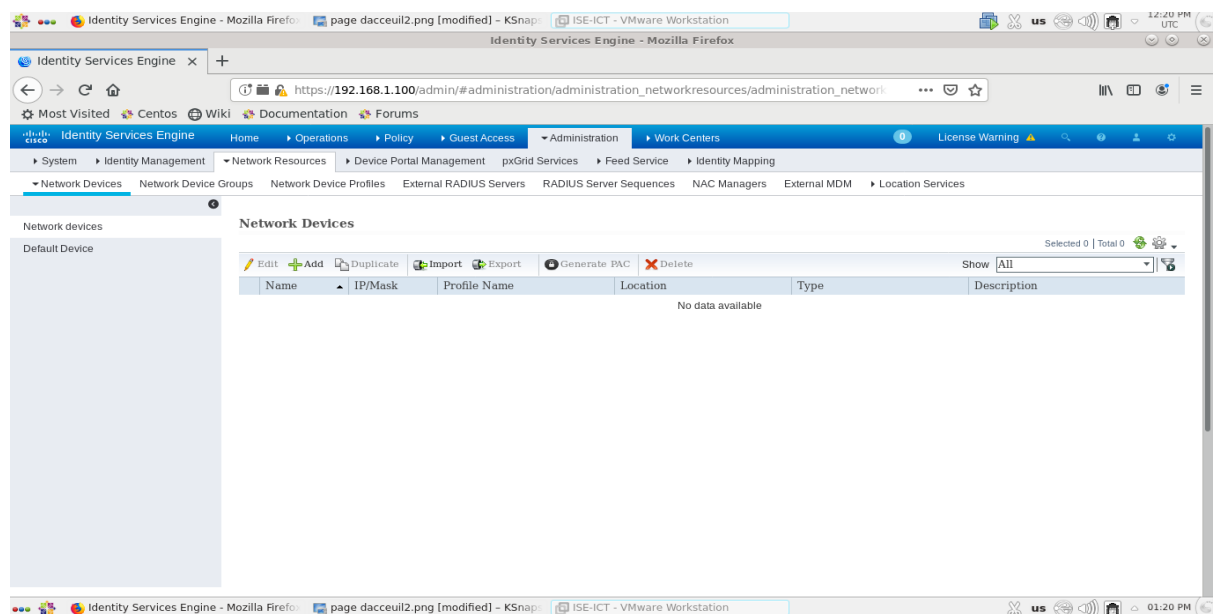


Figure 4.9 : Etape 1 de l'ajout de l'équipement réseau.

Etape 2. Nous avons cliqué sur “ADD”.

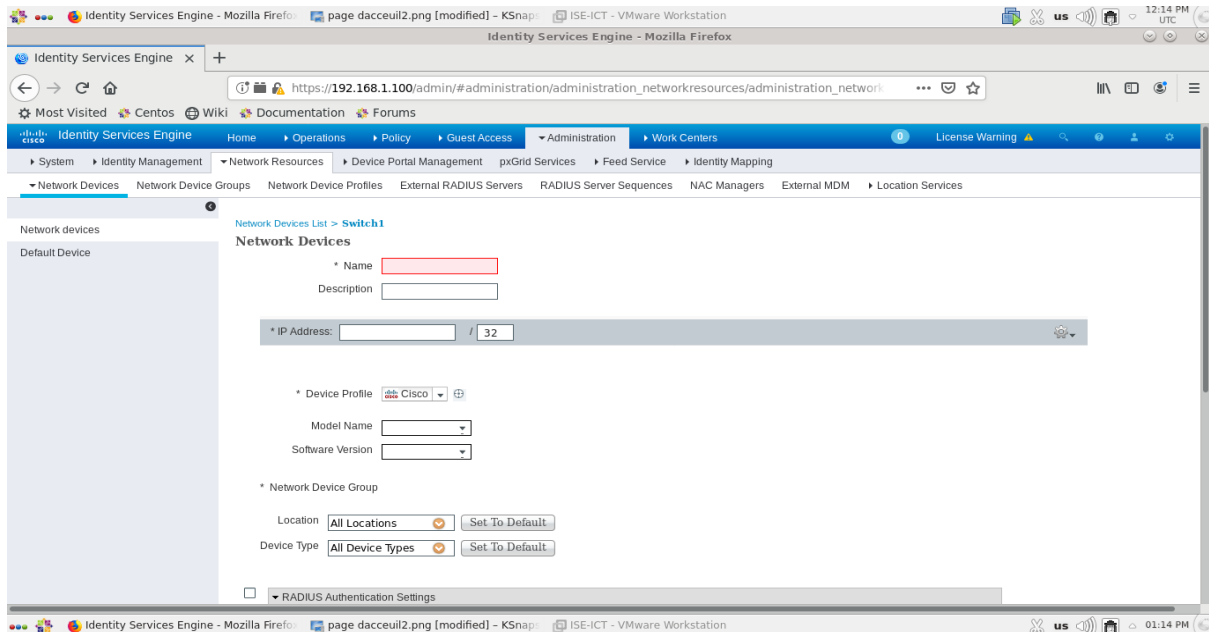


Figure 4.10 : Etape 2 de l'ajout de l'équipement réseau.

Etape 3. Nous avons rempli les champs par les informations suivantes :

Name : Authentificateur

IP Address : 192.168.1.10 / 24

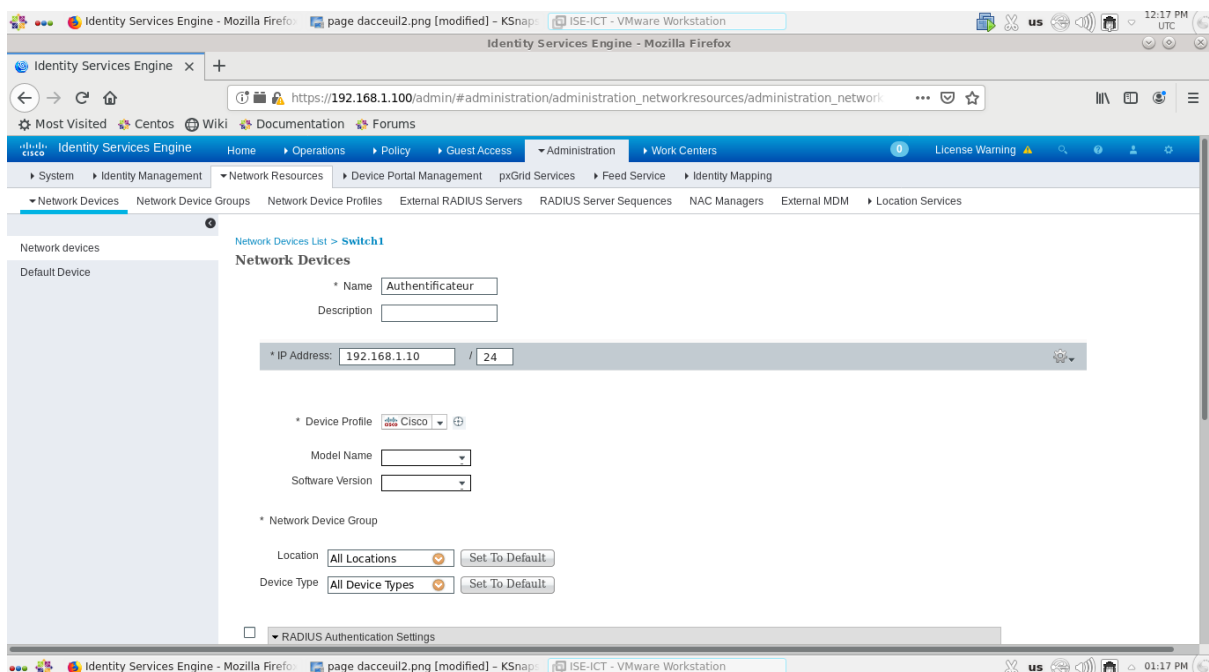


Figure 4.11 : Etape 3 de l'ajout de l'équipement réseau.

Etape 4. Nous avons coché l’option **“RADIUS Authentication Settings”** et nous avons rempli le champ du **“Shared Secret”** par la clé secrète partagée, qui est **“cisco123”**, entre le serveur ISE et le switch d’accès (Authentificateur).

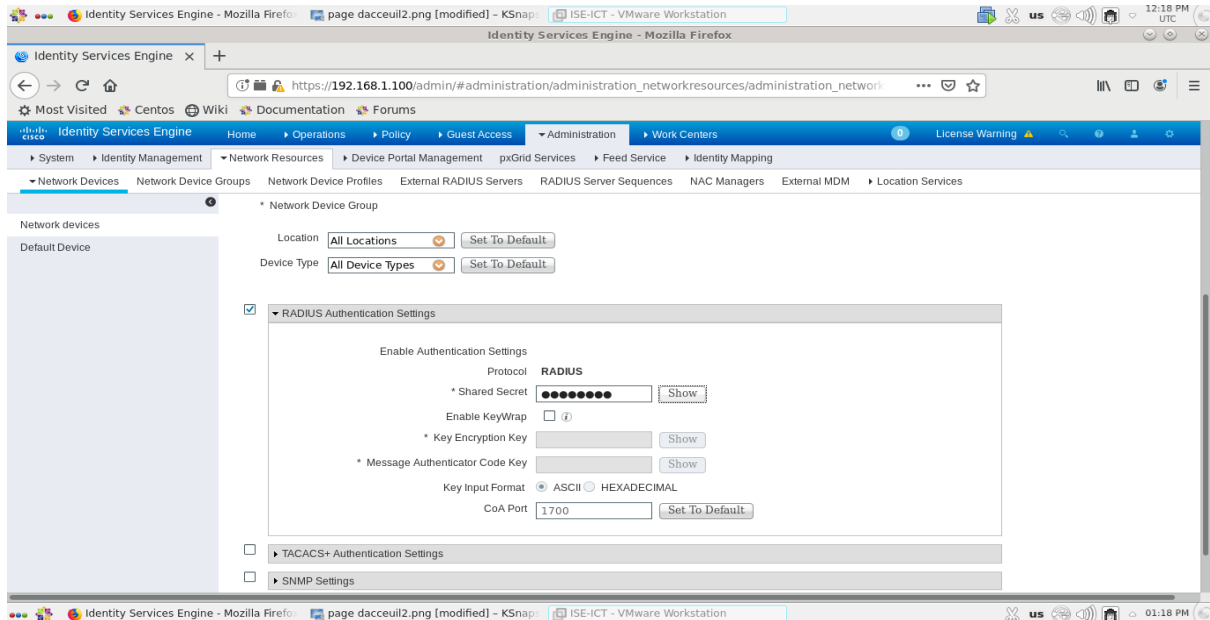


Figure 4.12 : Etape 4 de l’ajout de l’équipement réseau.

Etape 5. Nous avons cliqué sur **“Show”** pour confirmer que la clé secrète est correcte.

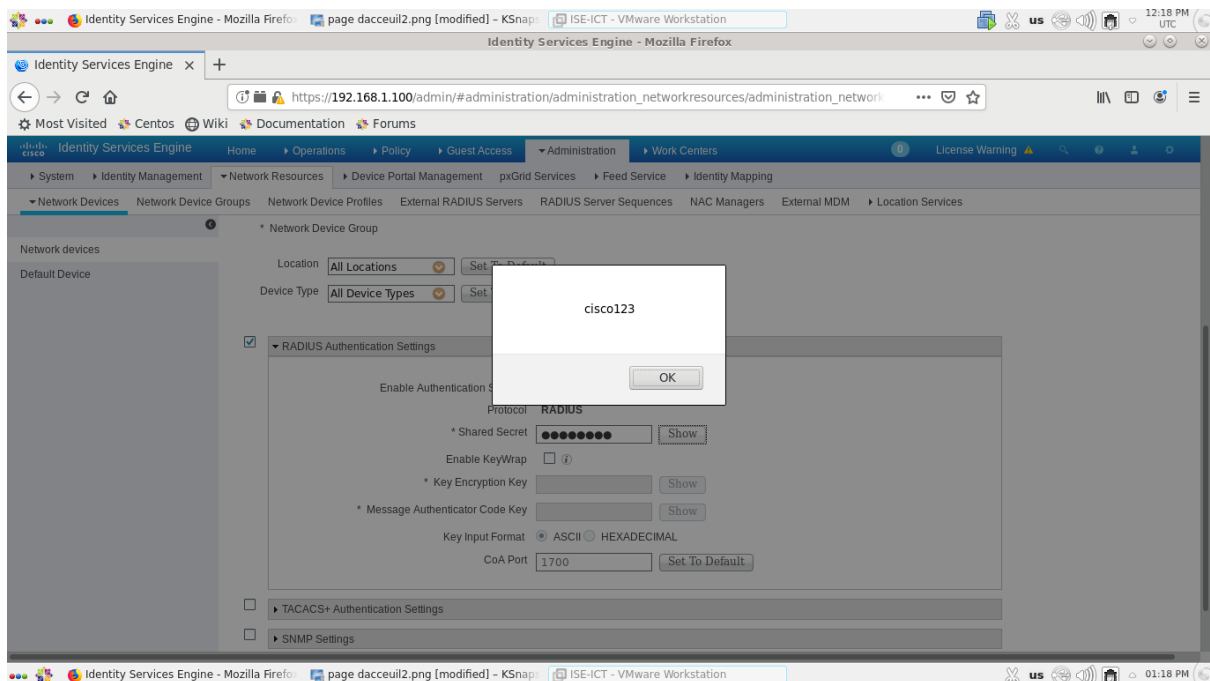


Figure 4.13 : Etape 5 de l’ajout de l’équipement réseau.

Etape 6. Nous avons cliqué sur **“Submit”** pour appliquer les changements.

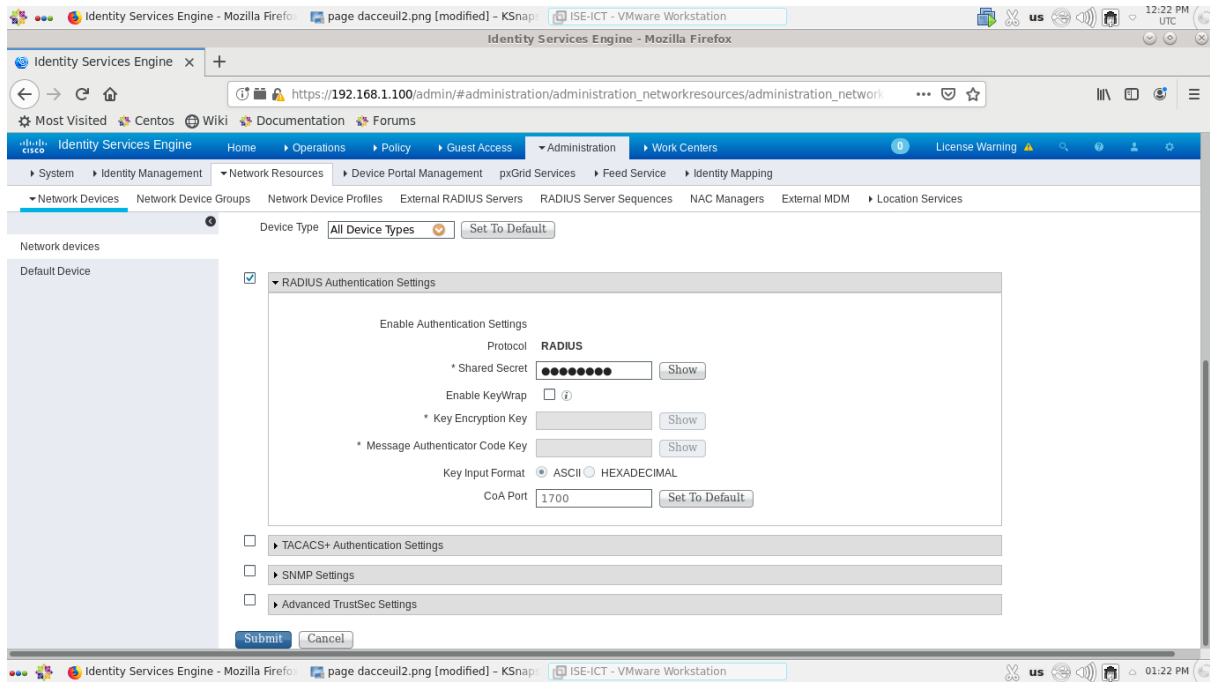


Figure 4.14 : Etape 6.a de l'ajout de l'équipement réseau.

Enfin, l'écran suivant apparaîtra.

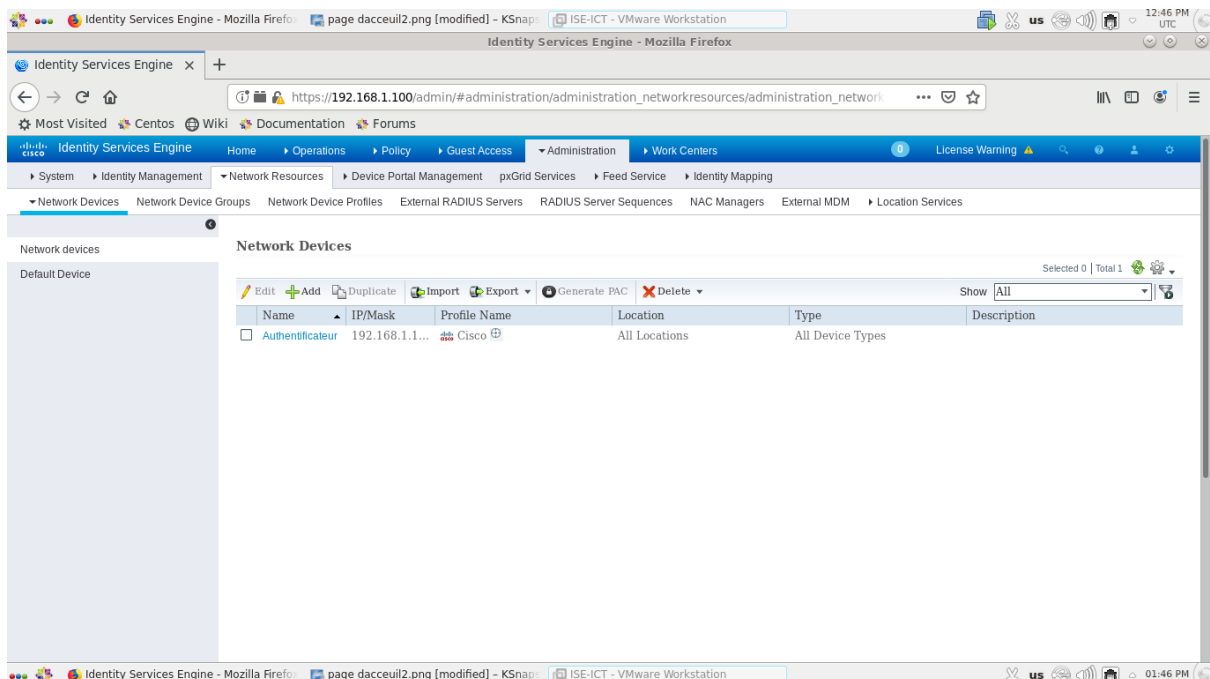


Figure 4.15 : Etape 6.b de l'ajout de l'équipement réseau.

4.3.3.2.2. Ajout de groupes d'identité d'utilisateurs (User Identity Groups)

Afin d'ajouter des groupes d'identité d'utilisateurs, Nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Administration”** > **“Identity Management”** > **“Groups”** > **“User Identity Groups”**, l'écran suivant apparaîtra.

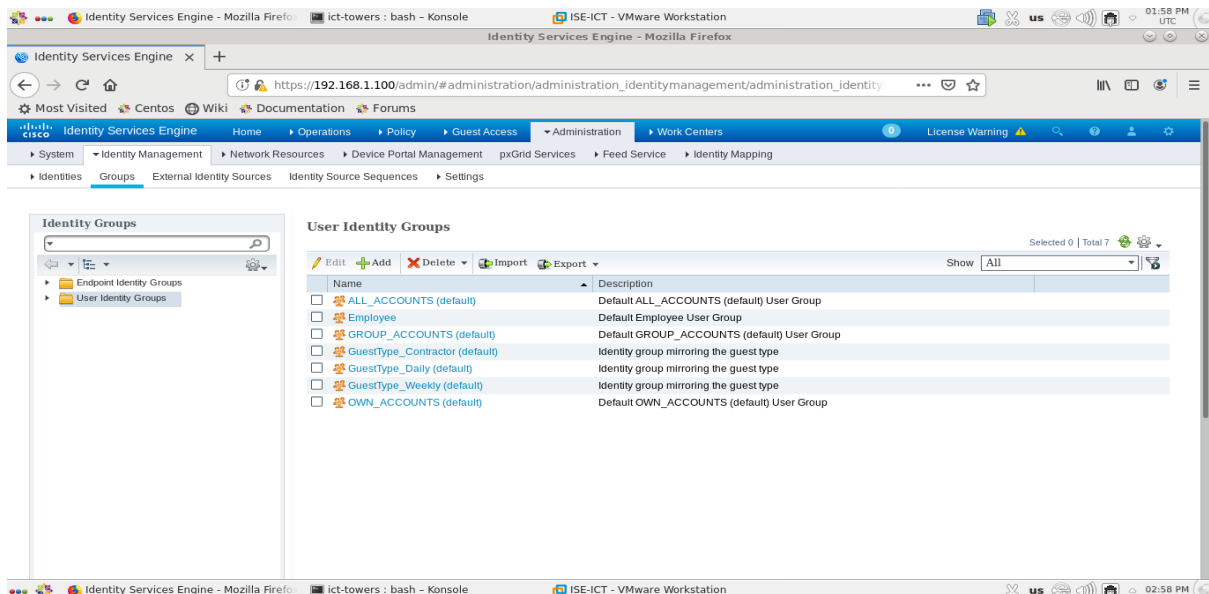


Figure 4.16 : Etape 1 de l'ajout de groupes d'identité d'utilisateurs.

Etape 2. Nous avons cliqué sur **“ADD”**.

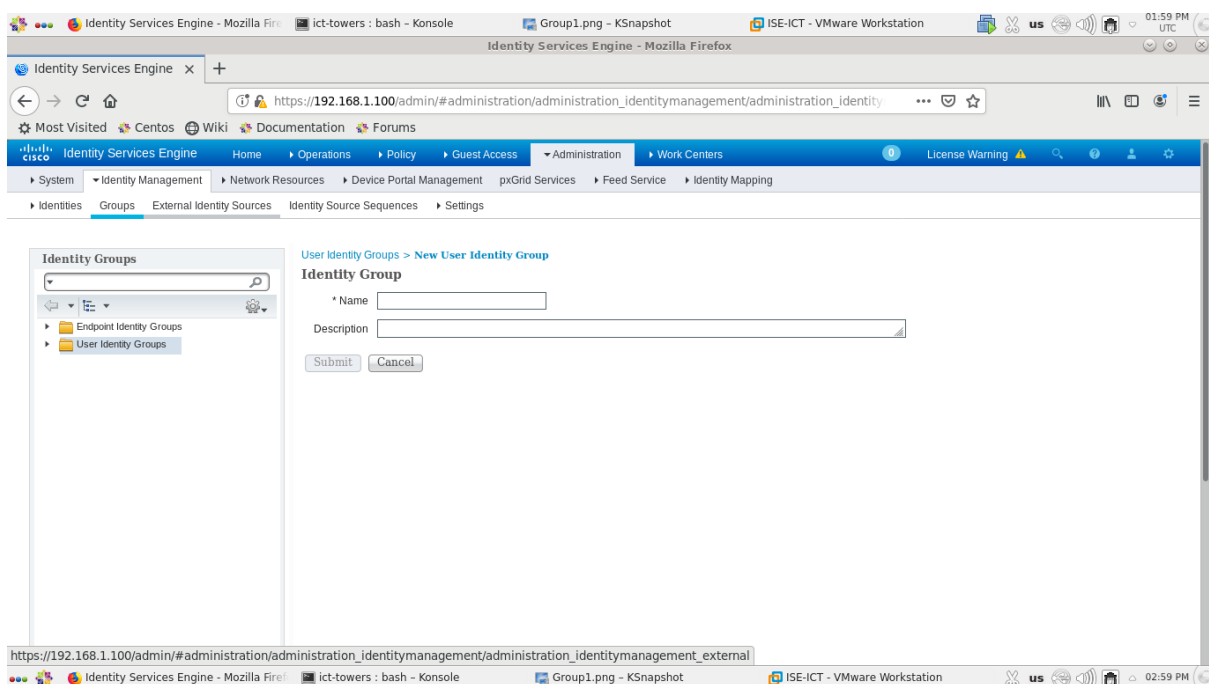


Figure 4.17 : Etape 2 de l'ajout de groupes d'identité d'utilisateurs.

Etape 3. Nous avons ajouté un premier groupe en remplissant le champ **“Name”** par **“Administrateur”**.

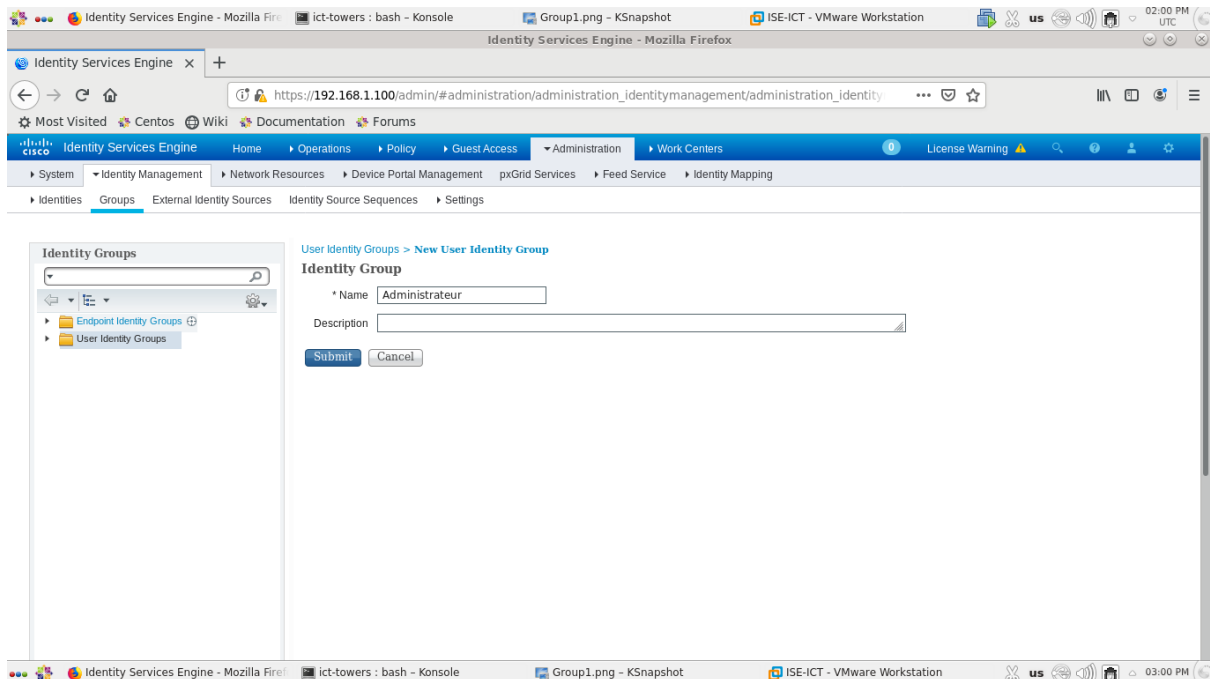


Figure 4.18 : Etape 3 de l'ajout de groupes d'identité d'utilisateurs.

Etape 4. Nous avons cliqué sur **“Submit”** pour appliquer les changements.

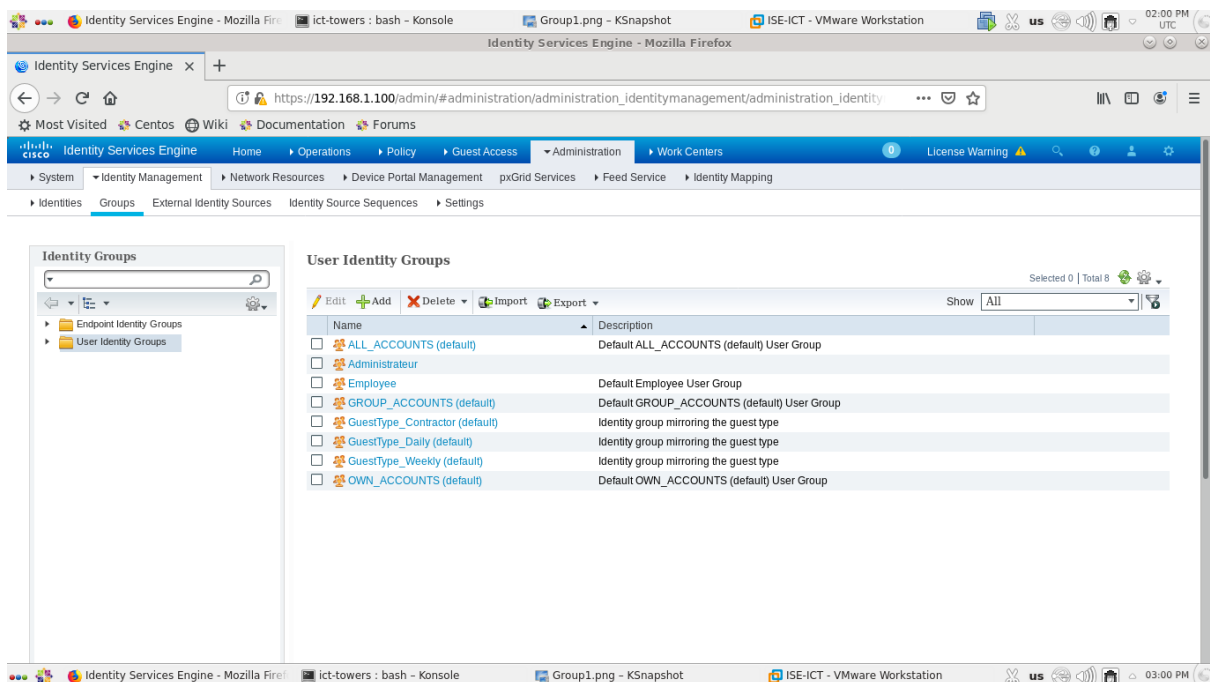


Figure 4.19 : Etape 4 de l'ajout de groupes d'identité d'utilisateurs.

Etape 5. Nous avons cliqué sur “ADD” et nous avons ajouté un deuxième groupe en remplissant le champ “Name” par “Client”.

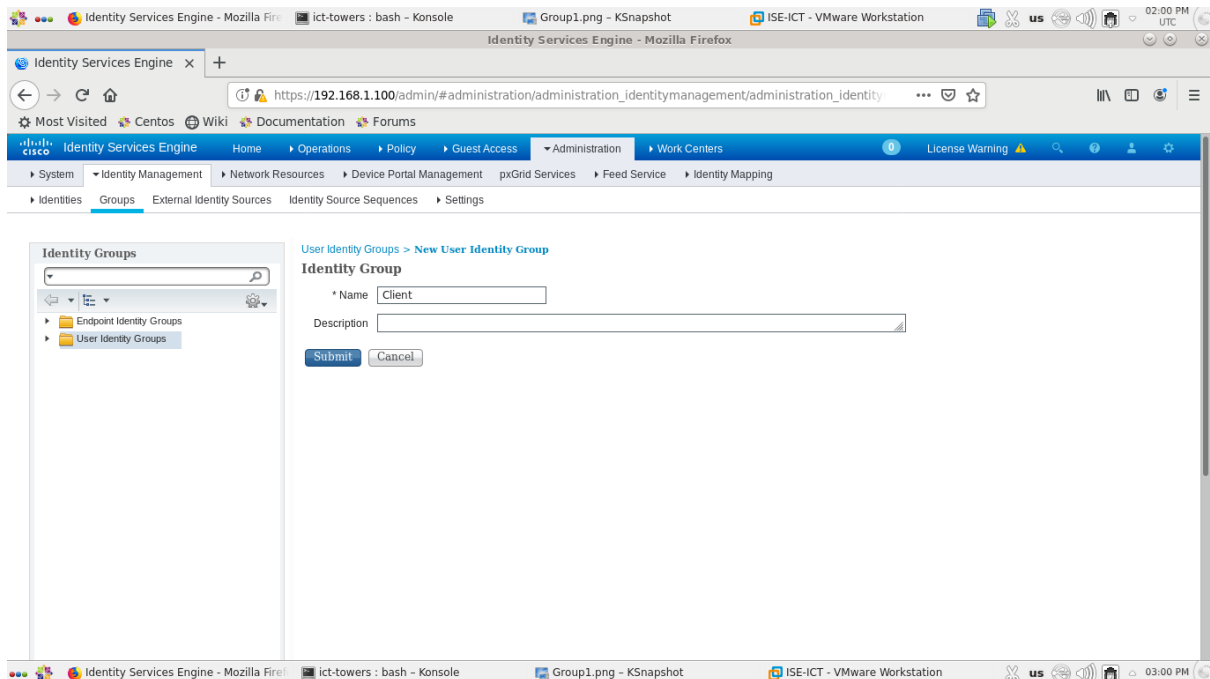


Figure 4.20 : Etape 5 de l'ajout de groupes d'identité d'utilisateurs.

Etape 6. Nous avons cliqué sur “Submit” pour appliquer les changements.

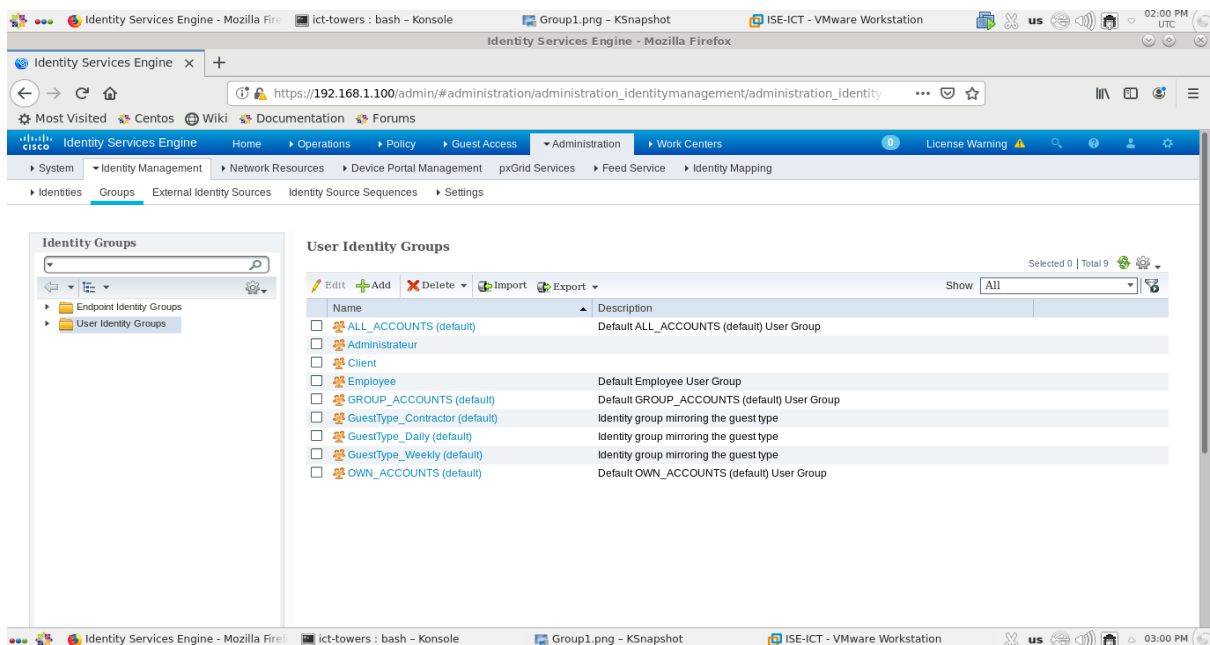


Figure 4.21 : Etape 6 de l'ajout de groupes d'identité d'utilisateurs.

4.3.3.2.3. Ajout d'utilisateurs (Users)

Afin d'ajouter des utilisateurs, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Administration”** > **“Identity Management”** > **“Identities”** > **“Users”**, l'écran suivant apparaîtra.

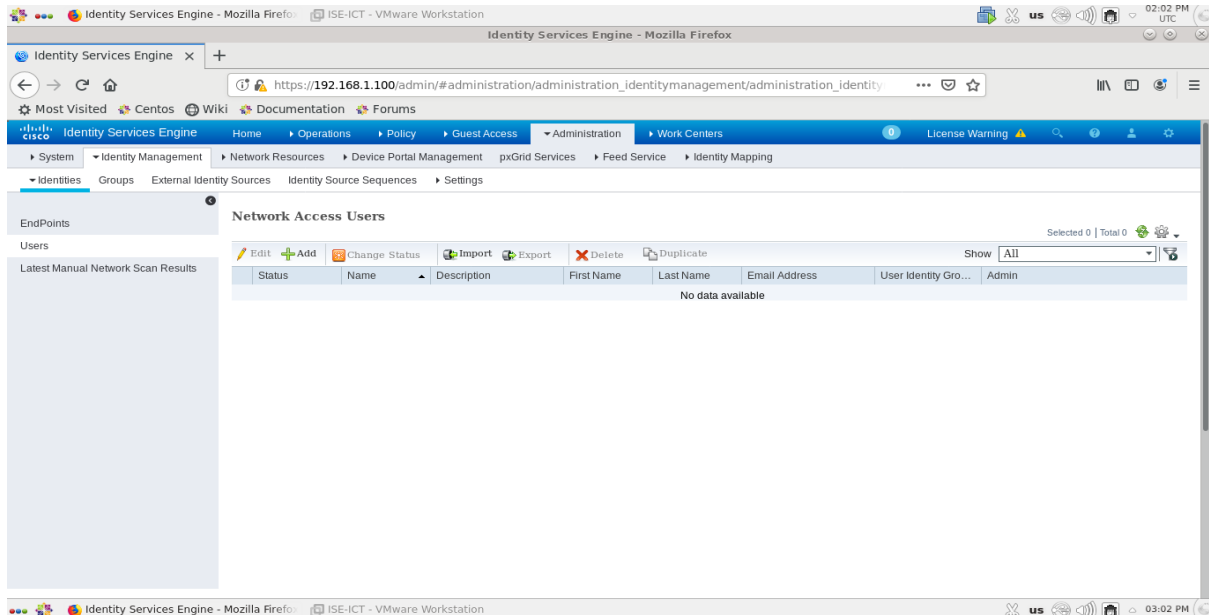


Figure 4.22 : Etape 1 de l'ajout d'utilisateurs.

Etape 2. Nous avons cliqué sur **“ADD”**.

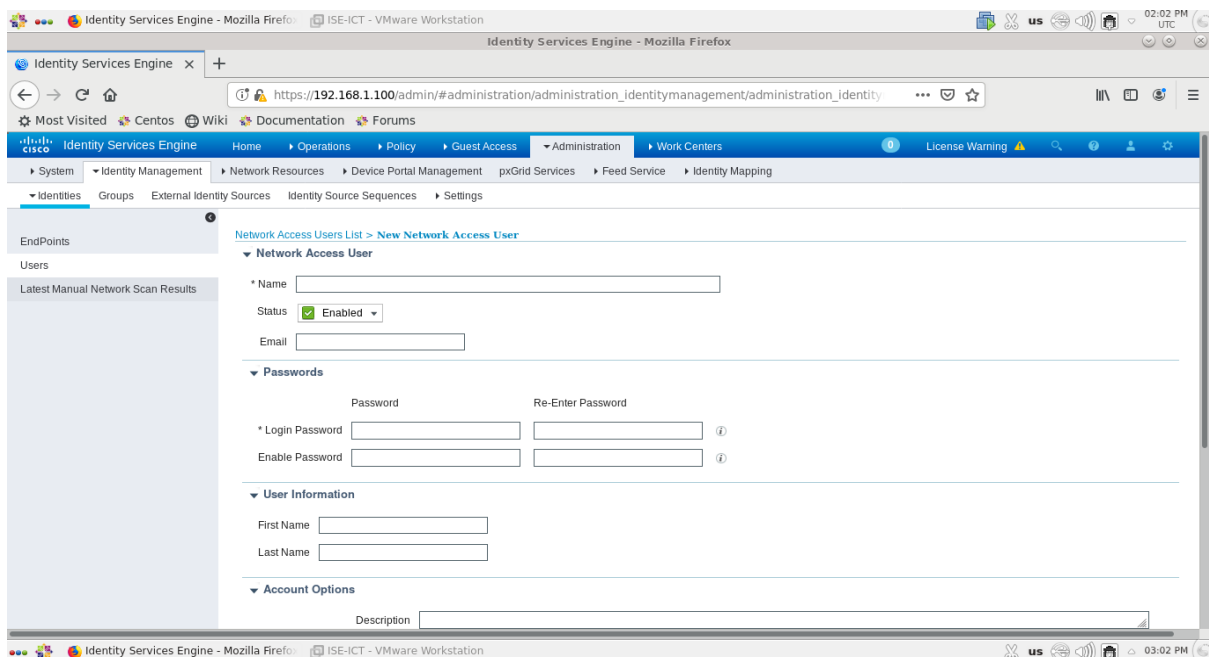


Figure 4.23 : Etape 2 de l'ajout d'utilisateurs.

Dans la section “**User Groups**”, nous avons cliqué sur “**Select an item**”. Ensuite, nous avons choisi l’option “**User Identity Group**” et enfin nous avons choisi le groupe “**Administrateur**”.

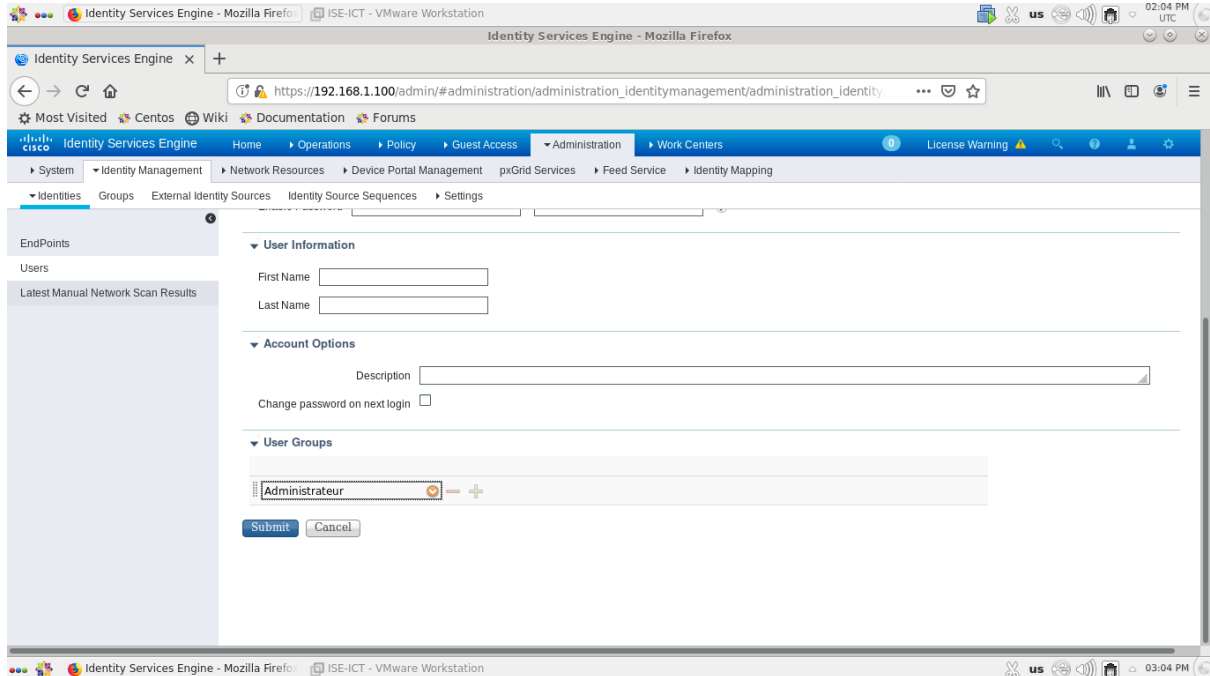


Figure 4.26 : Etape 4.b de l'ajout d'utilisateurs.

Etape 5. Nous avons cliqué sur “**Submit**” pour appliquer les changements.

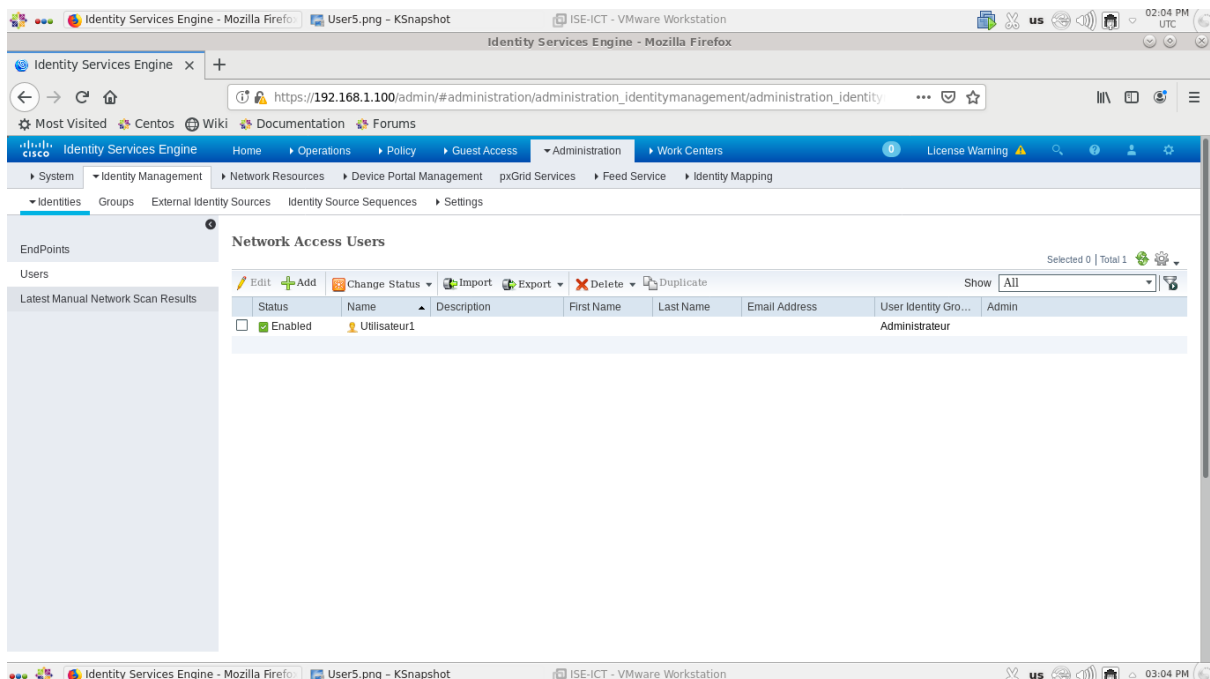


Figure 4.27 : Etape 5 de l'ajout d'utilisateurs.

Etape 6. Nous avons ajouté un deuxième utilisateur en remplissant les champs “*Name*” et “*Login Password*” par les informations suivantes :

- **Name :** *Utilisateur2*
- **Login Password :** (**Password :** *Client2*) (**Re-enter Password :** *Client2*)

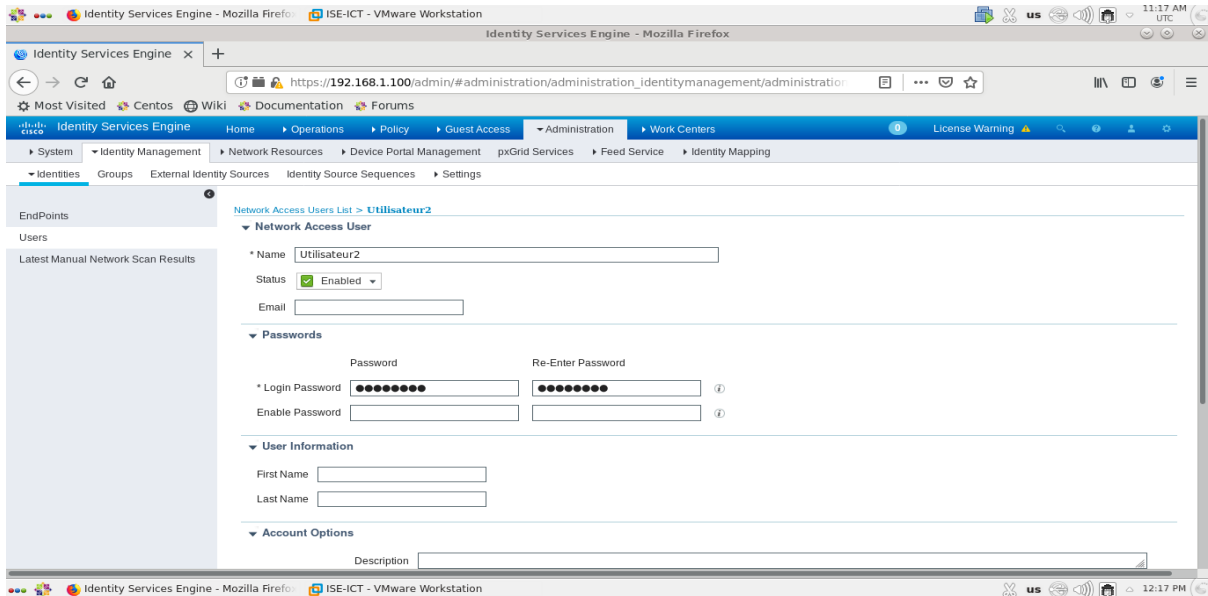


Figure 4.28 : Etape 6 de l'ajout d'utilisateurs.

Etape 7. Nous avons ajouté le deuxième utilisateur au groupe de clients.

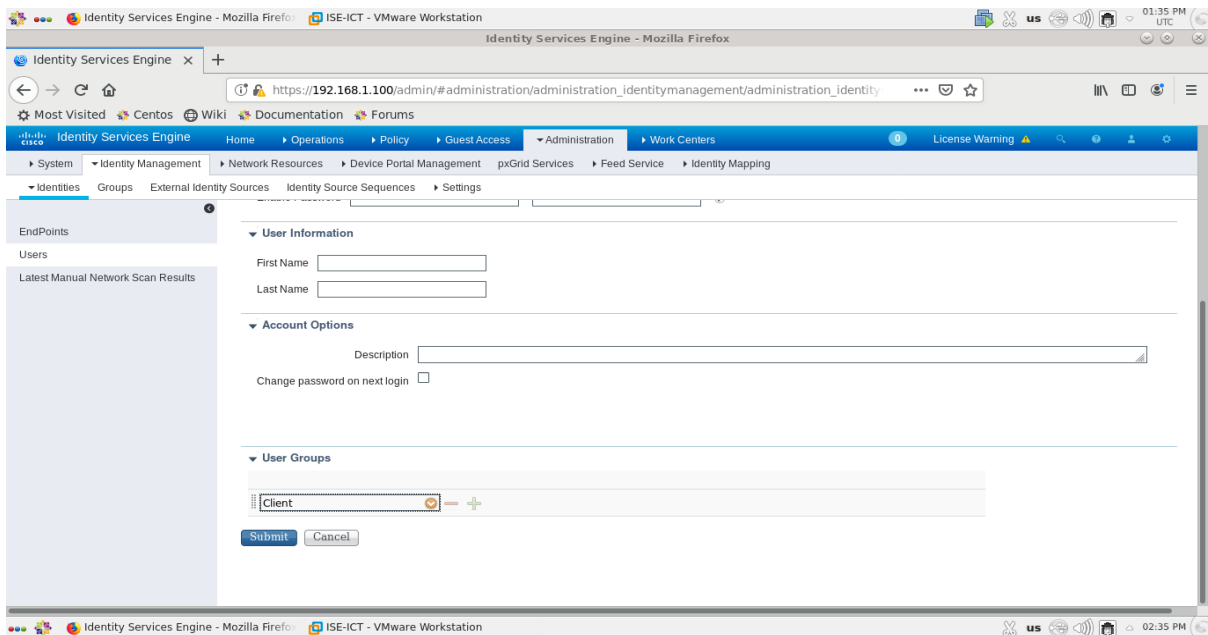


Figure 4.29 : Etape 7 de l'ajout d'utilisateurs.

Etape 8. Nous avons cliqué sur **“Submit”** pour appliquer les changements.

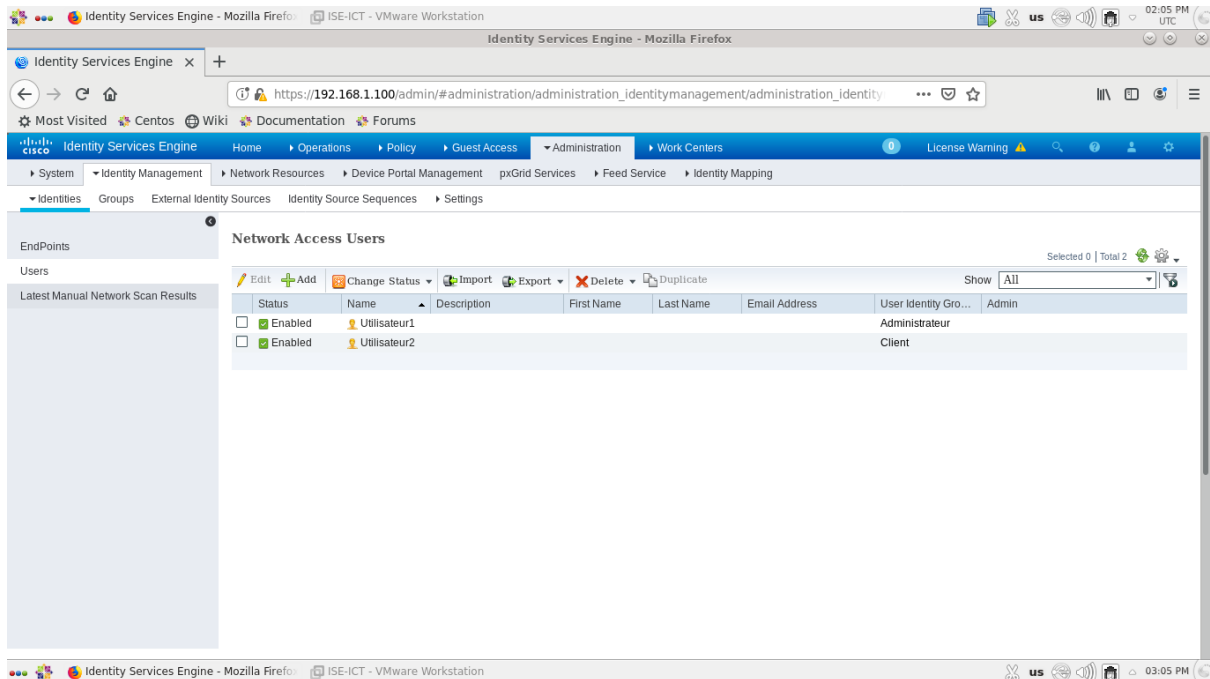


Figure 4.30 : Etape 8 de l'ajout d'utilisateurs.

Etape 9. Nous avons vérifié au niveau de groupes l'ajout des utilisateurs.

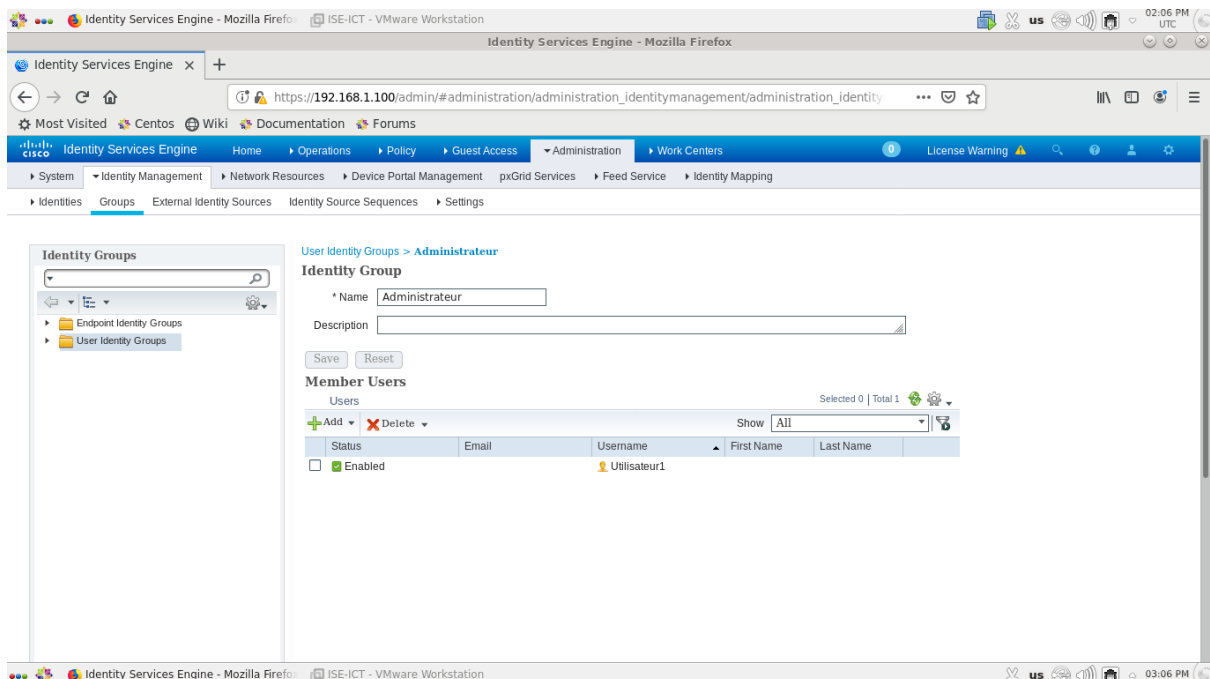


Figure 4.31 : Etape 9.a de l'ajout d'utilisateurs.

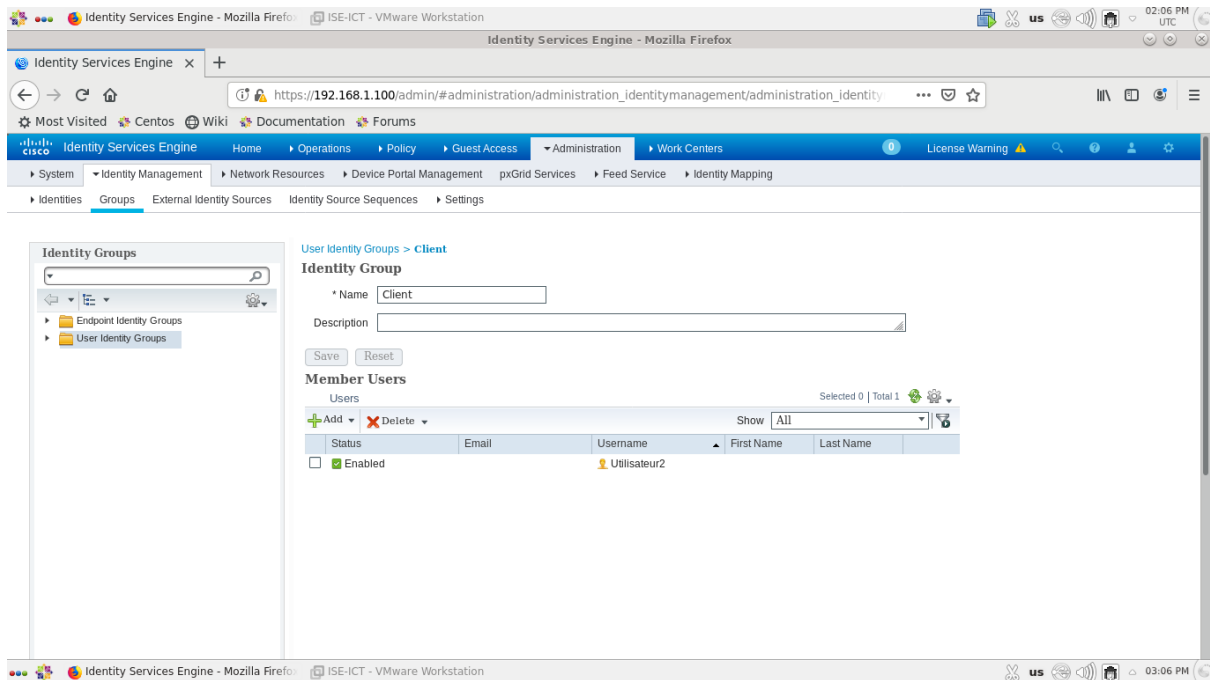


Figure 4.32 : Etape 9.b de l'ajout d'utilisateurs.

4.3.3.2.4. Ajout de protocoles d'authentification (Allowed Protocols)

Afin d'ajouter des protocoles spécifiques d'authentification, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Policy” > “Policy Elements” > “Results” > “Authentication” > “Allowed Protocols”**, l'écran suivant apparaîtra.

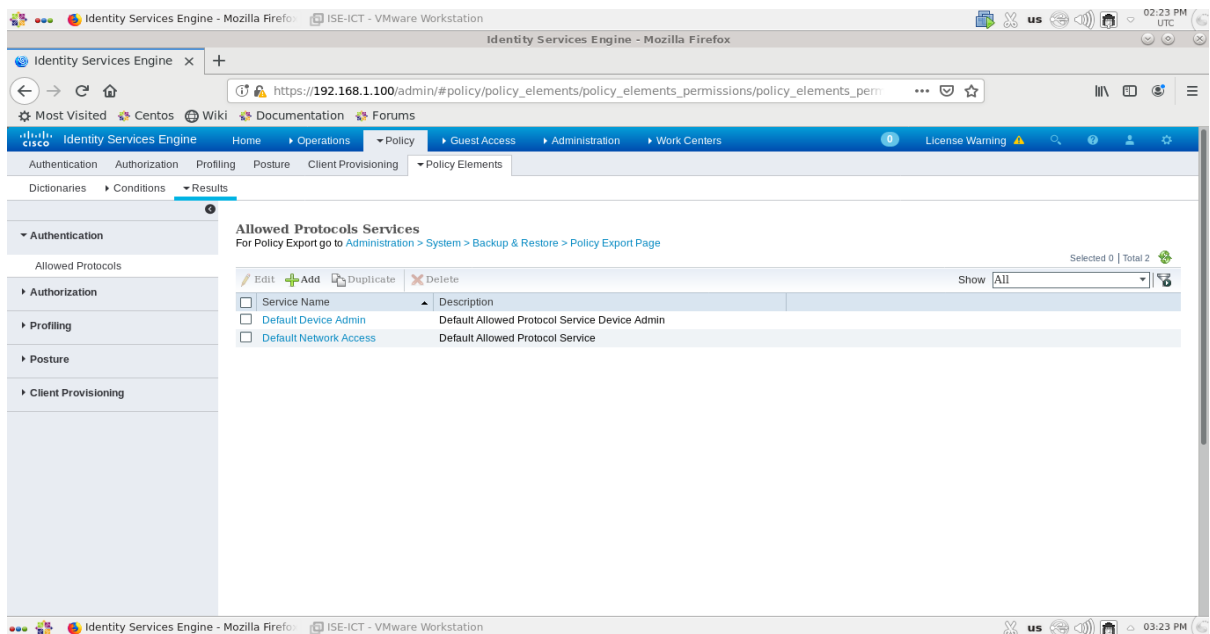


Figure 4.33 : Etape 1 de l'ajout de protocoles d'authentification.

Etape 2. Nous avons cliqué sur **“ADD”**.

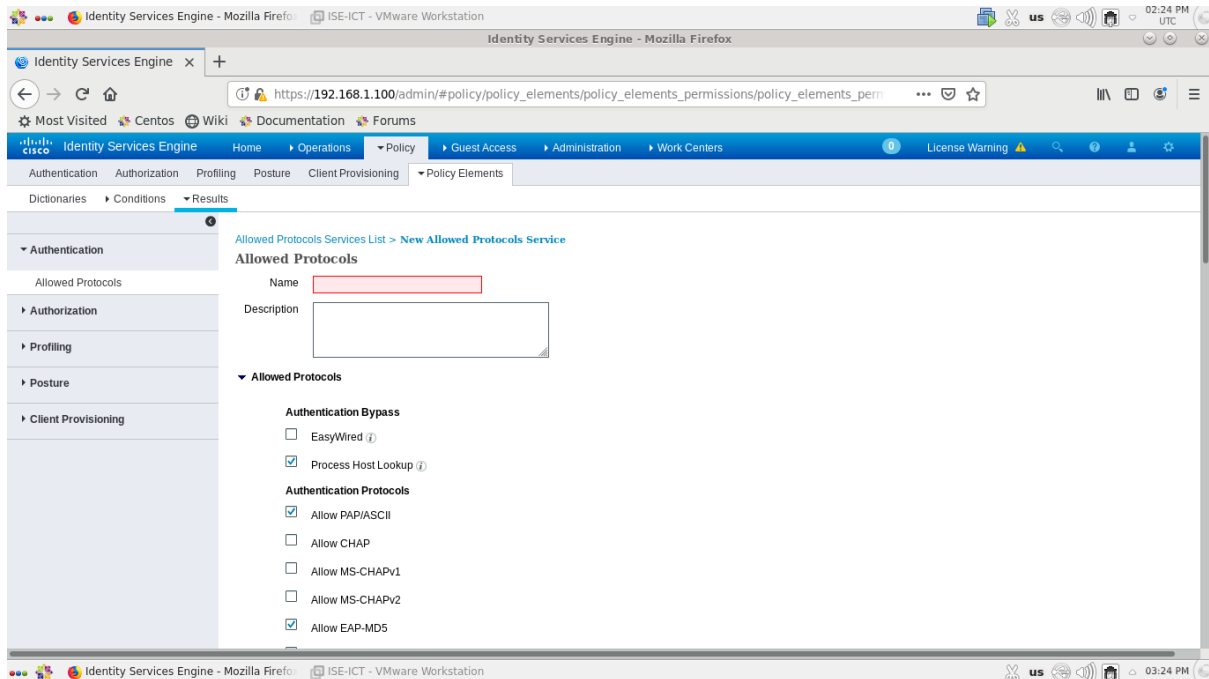


Figure 4.34 : Etape 2 de l'ajout de protocoles d'authentification.

Etape 3. Nous avons ajouté un premier protocole d'authentification 802.1X en remplissant le champ **“Name”** par **“DOT1X”**.

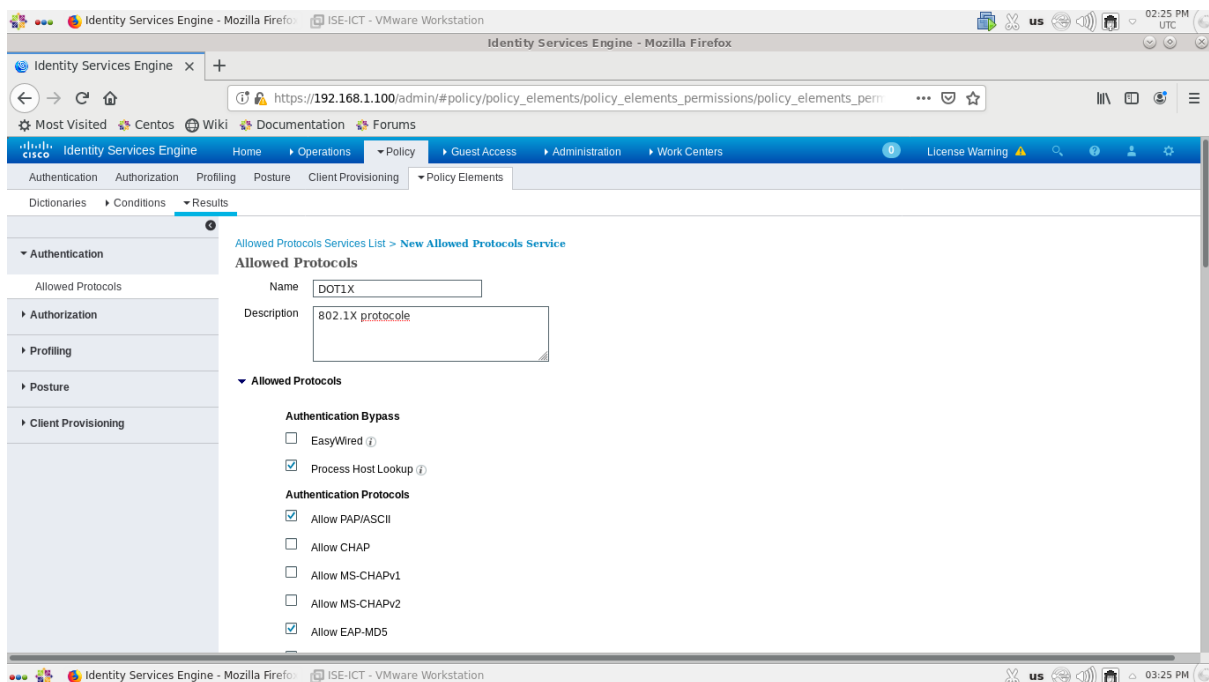


Figure 4.35 : Etape 3 de l'ajout de protocoles d'authentification.

Etape 4. Nous avons coché la méthode d’authentification à utiliser ainsi que ses variantes internes souhaitées.

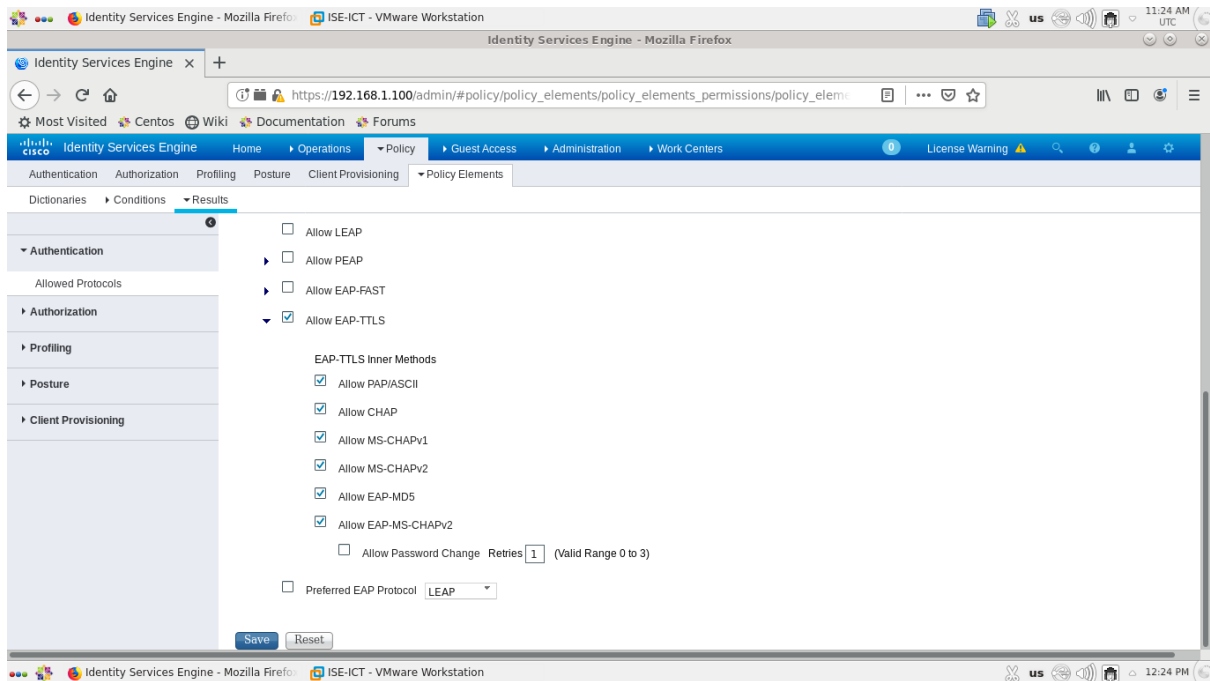


Figure 4.36 : Etape 4 de l’ajout de protocoles d’authentification.

Etape 5. Nous avons cliqué sur “Submit” pour appliquer les changements.

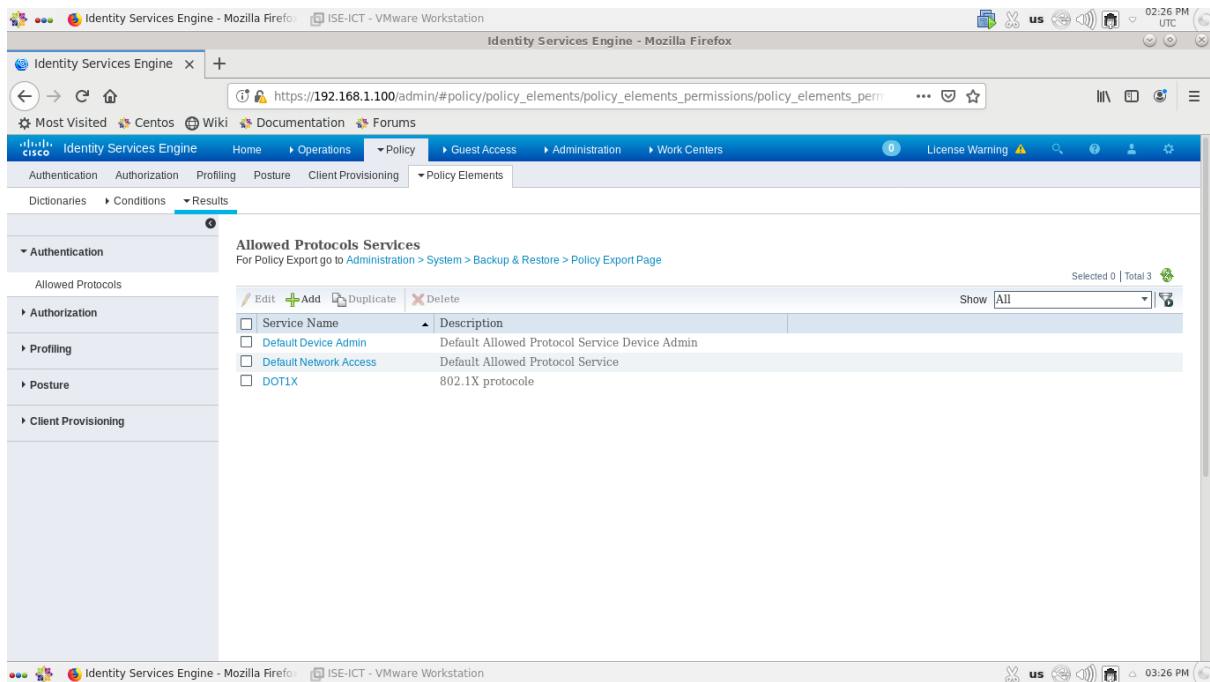


Figure 4.37 : Etape 5 de l’ajout de protocoles d’authentification.

Etape 6. Nous avons cliqué sur **“ADD”** et nous avons ajouté un deuxième protocole d’authentification MAB en remplissant le champ **“Name”** par **“MAB”**. Ensuite, nous avons coché la méthode d’authentification **Bypass** souhaitée.

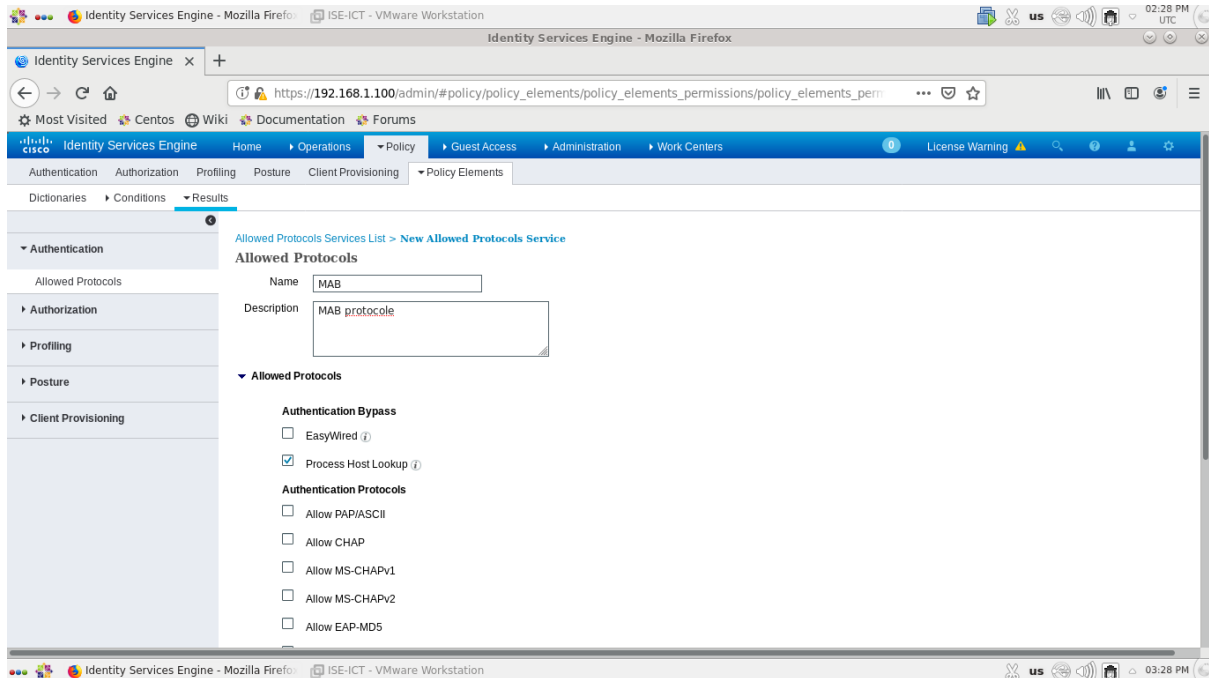


Figure 4.38 : Etape 6 de l’ajout de protocoles d’authentification.

Etape 7. Nous avons cliqué sur **“Submit”** pour appliquer les changements.

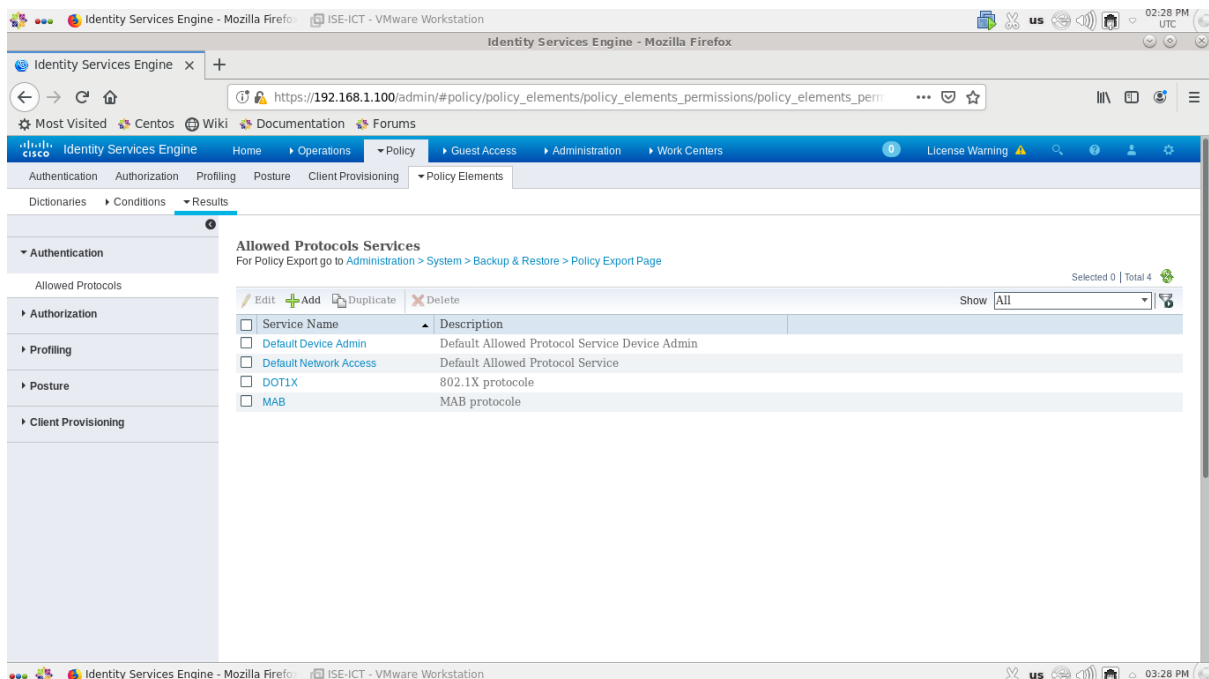


Figure 4.39 : Etape 7 de l’ajout de protocoles d’authentification.

4.3.3.2.5. Présentation de conditions d'authentification

Afin de comprendre la signification des conditions d'authentification prédéfinies sur ISE, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Policy” > “Policy Elements” > “Conditions” > “Authentication” > “Compound Conditions”**, l'écran suivant apparaîtra.

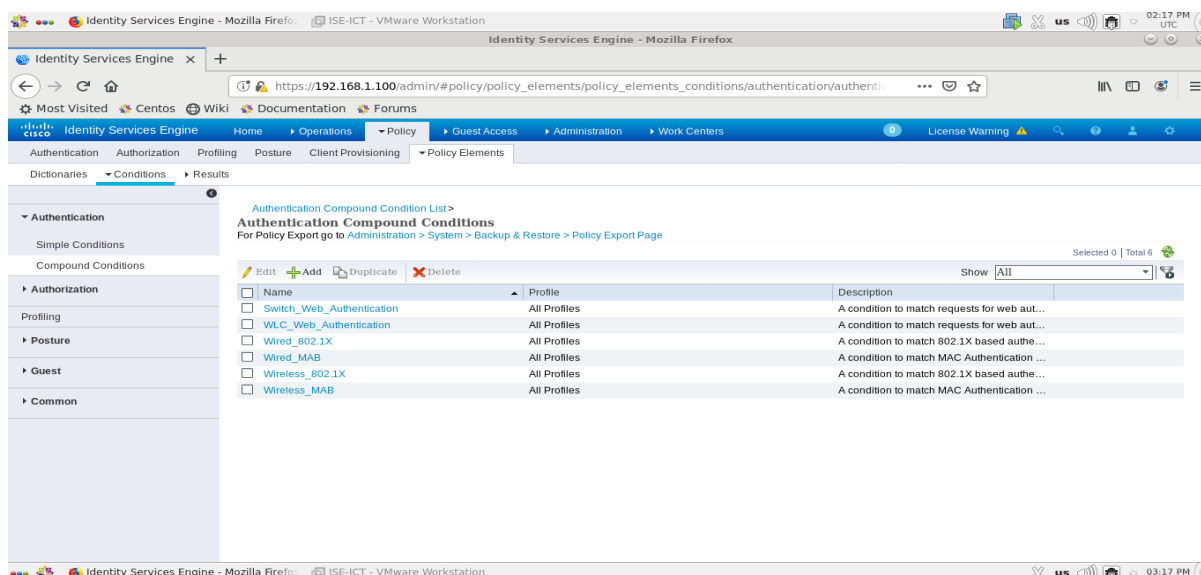


Figure 4.40 : Etape 1 de la présentation de conditions d'authentification.

Etape 2. Nous avons cliqué sur la condition **“Wired_802.1X”** pour comprendre sa signification.

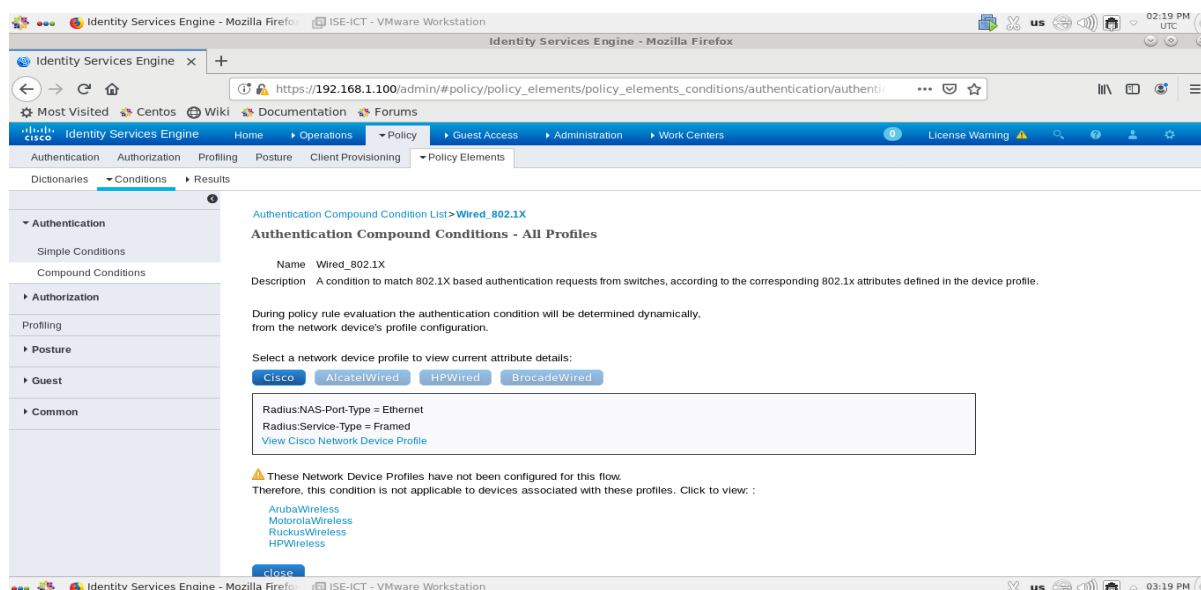


Figure 4.41 : Etape 2 de la présentation de conditions d'authentification.

Etape 3. Nous avons cliqué sur **“Close”** et nous avons cliqué sur la condition **“Wired_MAB”** pour comprendre sa signification.

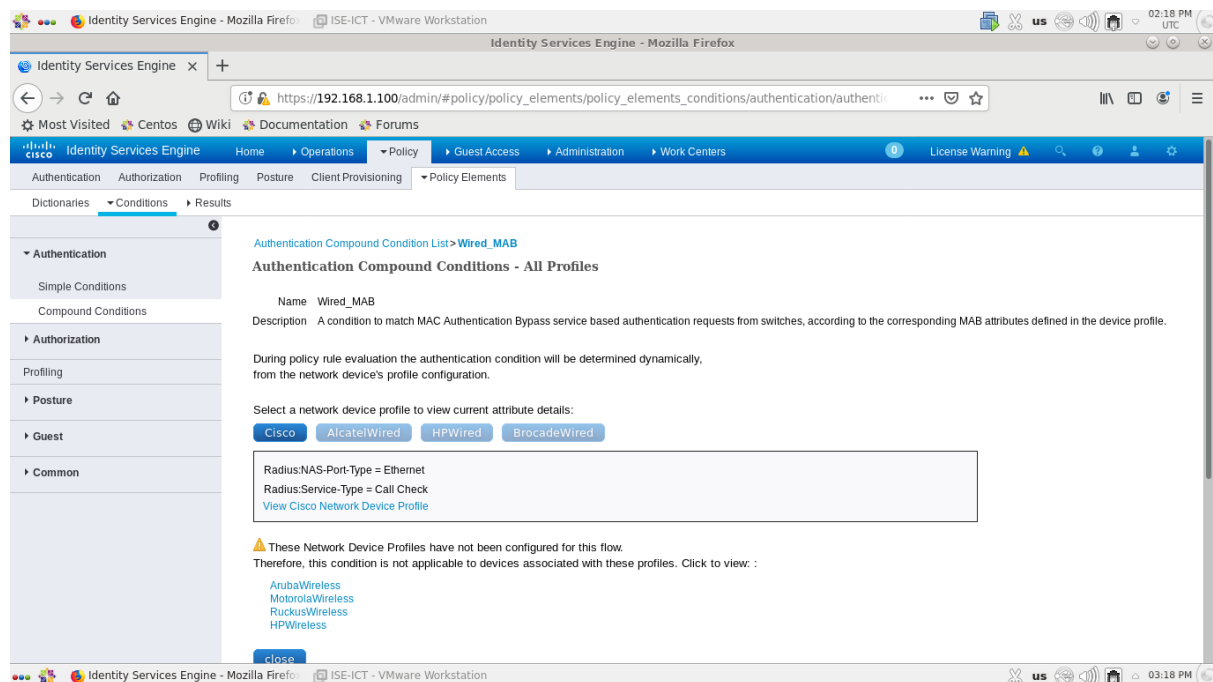


Figure 4.42 : Etape 3 de la présentation de conditions d'authentification.

4.3.3.2.6. Ajout de politiques d'authentification (Authentication Policy)

Afin d'ajouter des politiques d'authentification, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Policy”** > **“Authentication”**, l'écran suivant apparaîtra.

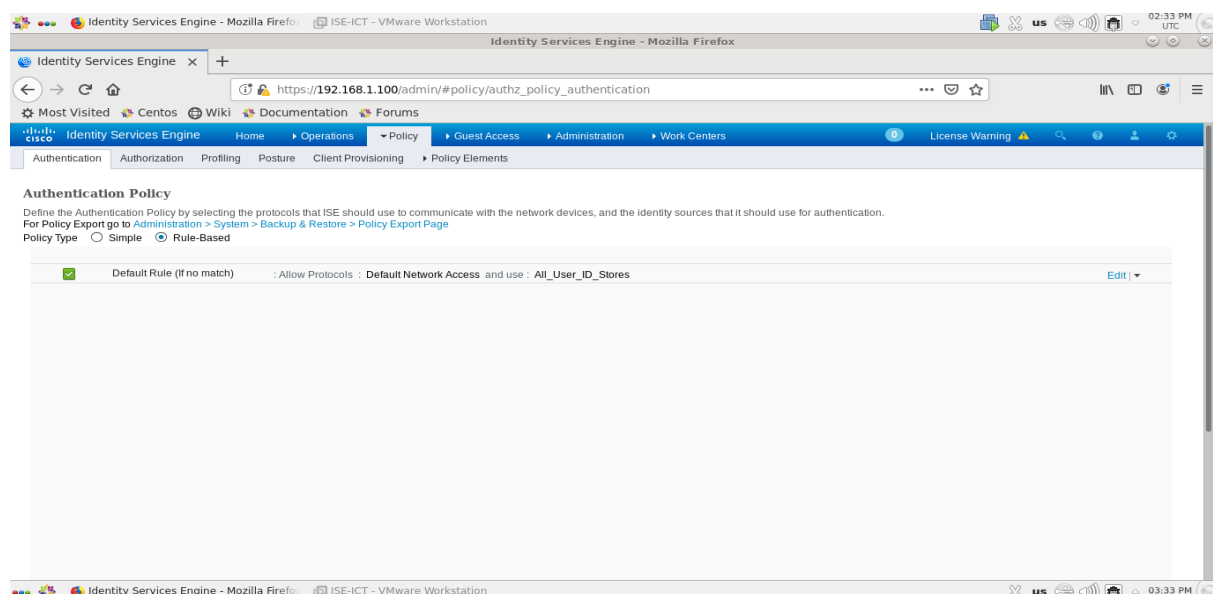


Figure 4.43 : Etape 1 de l'ajout de politiques d'authentification.

Etape 2. Nous avons cliqué sur la flèche qui se trouve à côté de l’option **“Edit”** et nous avons choisi l’option **“Insert new row below”**.

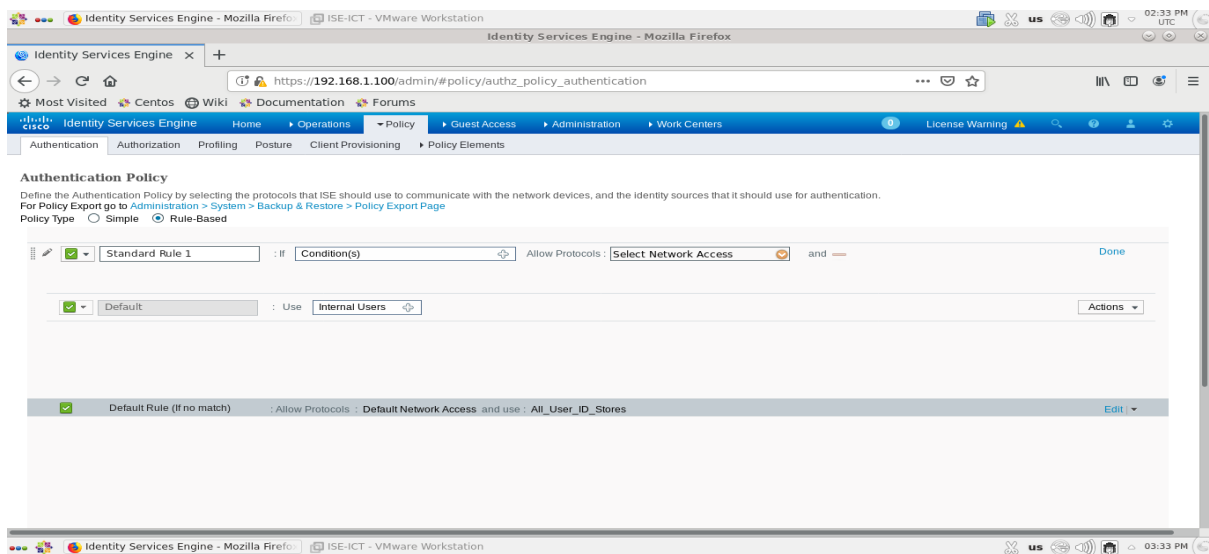


Figure 4.44 : Etape 2 de l’ajout de politiques d’authentification.

Etape 3. Nous avons changé le nom de la règle par **“802.1X”**.

Etape 4. Nous avons choisi la condition associée à l’authentification 802.1X en cliquant sur **“Condition(s)”** > **“Select Existing Condition from Library”** > **“Select Condition”** > **“Compound Condition”** > **“Wired_802.1X”**.

Etape 5. Nous avons choisi le protocole d’authentification en cliquant sur **“Select Network Access”** > **“Allowed Protocols”** > **“DOT1X”**.

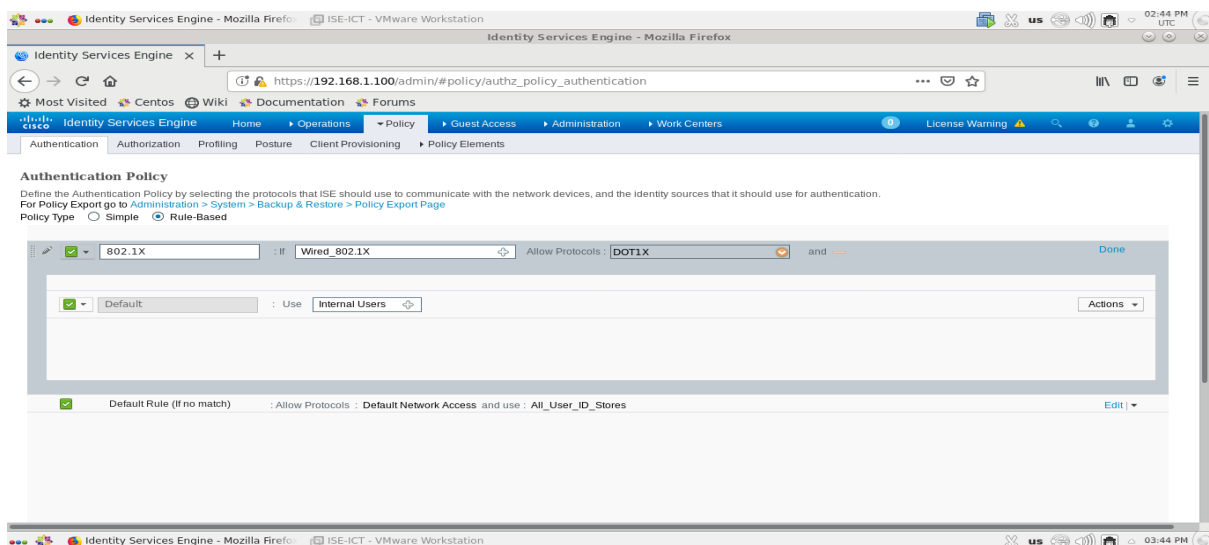


Figure 4.45 : Etape 5 de l’ajout de politiques d’authentification.

Etape 6. Nous avons cliqué sur **“Done”**.

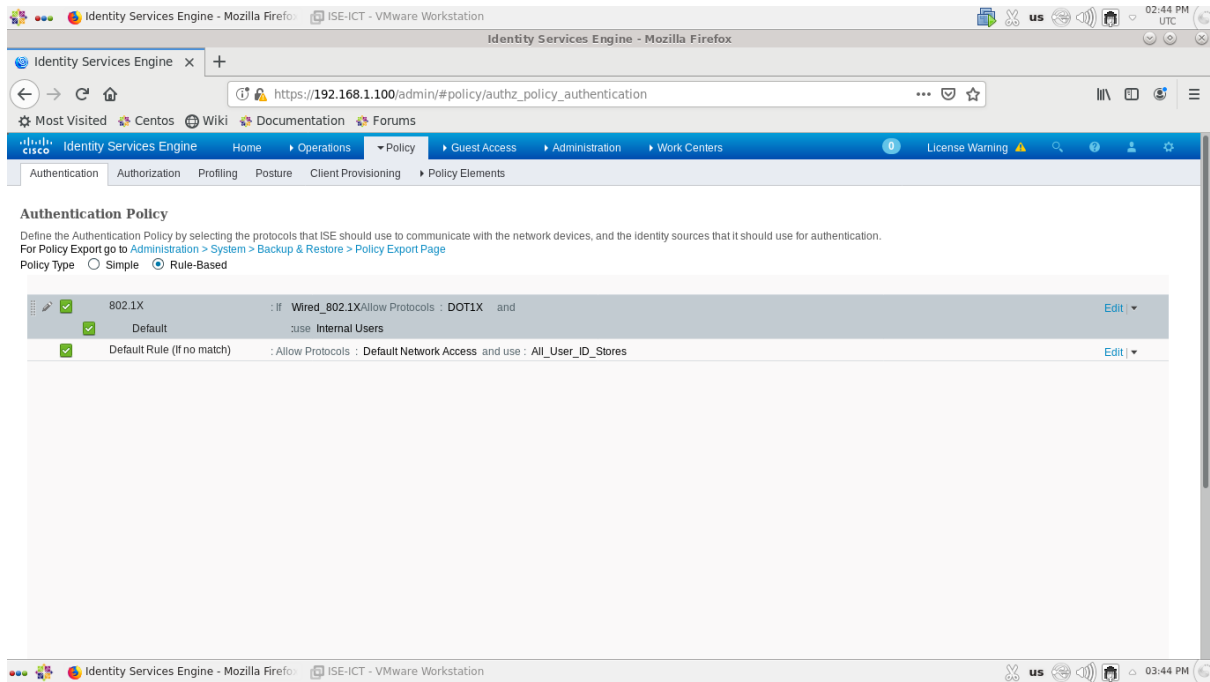


Figure 4.46 : Etape 6 de l'ajout de politiques d'authentification.

Etape 7. Nous avons ajouté une deuxième Policy pour l'authentification de secours **“MAB”** mais cette fois-ci nous avons utilisé l'option **“Internal Endpoints”**.

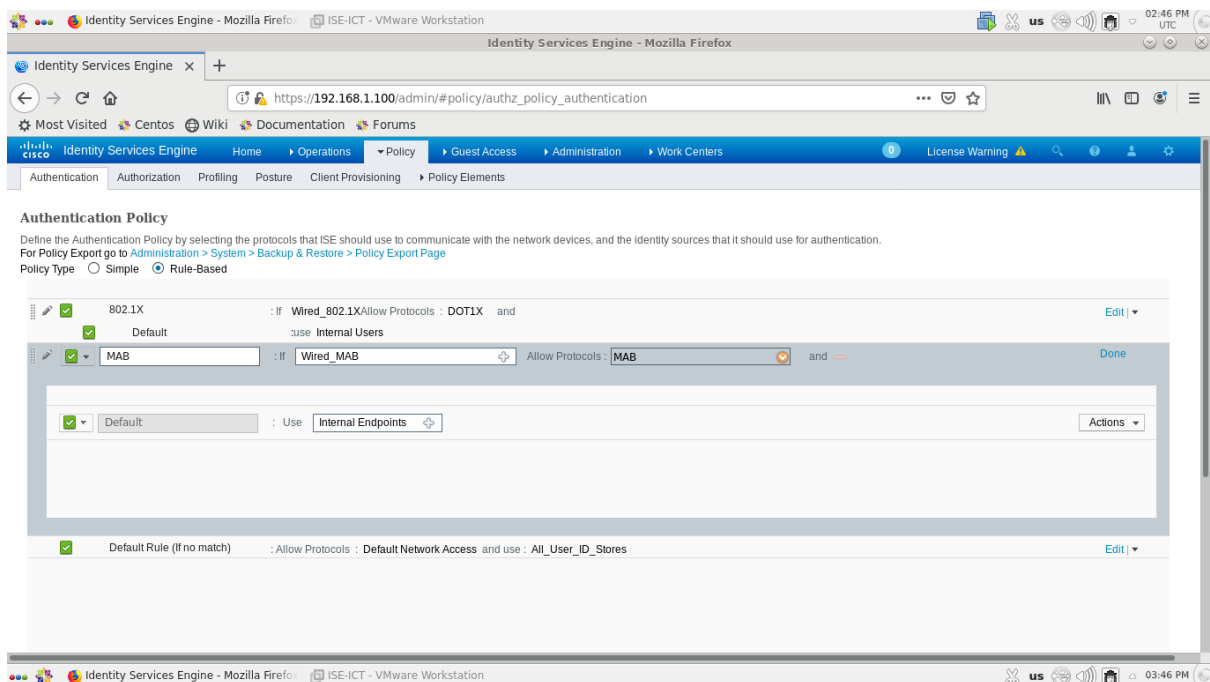


Figure 4.47 : Etape 7 de l'ajout de politiques d'authentification.

Etape 8. Nous avons cliqué sur **“Done”**.

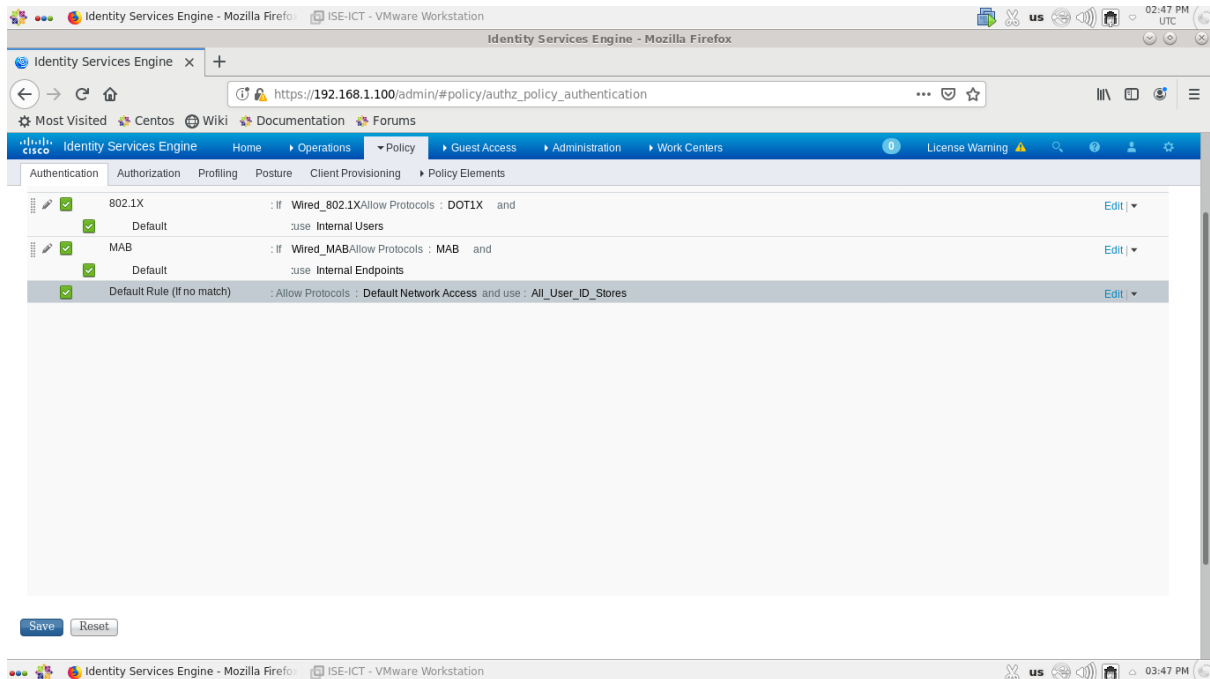


Figure 4.48 : Etape 8 de l'ajout de politiques d'authentification.

Etape 9. Nous avons cliqué sur **“Save”**.

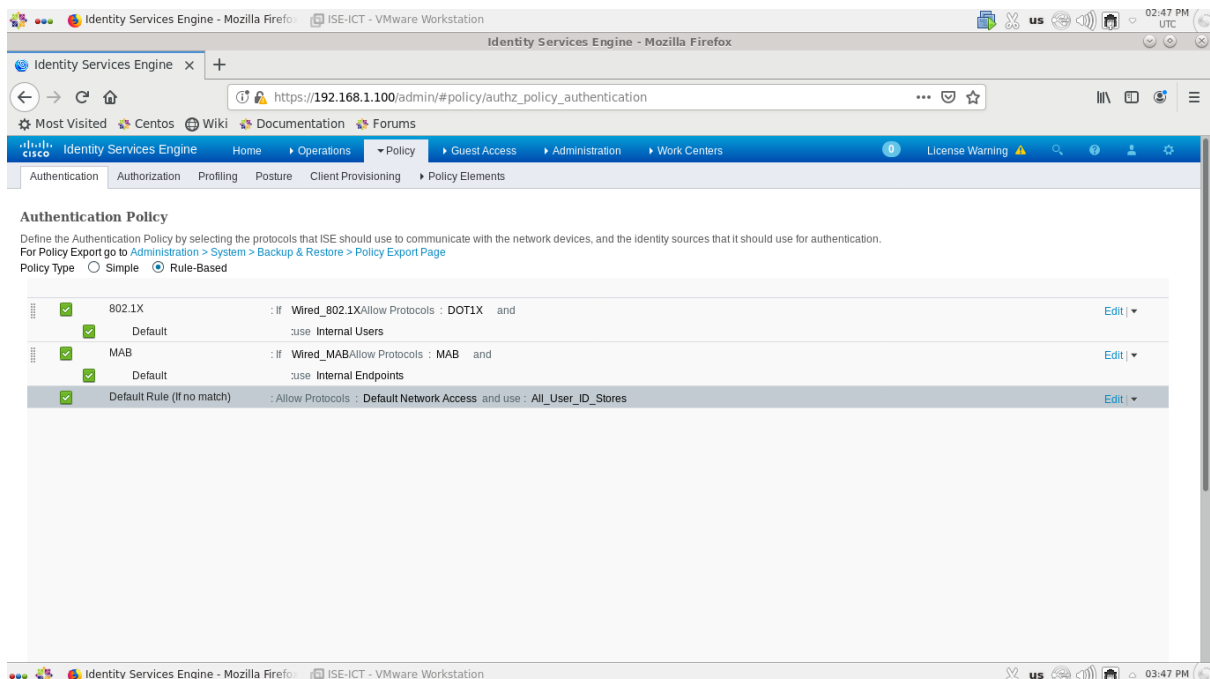


Figure 4.49 : Etape 9 de l'ajout de politiques d'authentification.

4.3.3.2.7. Ajout de politiques d'autorisation (Authorization Policy)

4.3.3.2.7.1. Politique d'autorisation 802.1X

Afin d'ajouter des politiques d'autorisation 802.1X, nous avons suivi les étapes suivantes :

Etape 1. Tout d'abord, nous avons ajouté des profils d'autorisation. Pour cela nous avons suivi les sous-étapes suivantes :

Etape 1.1. Nous avons cliqué sur : **“Policy”** > **“Policy Elements”** > **“Results”** > **“Authorization”** > **“Authorization Profiles”**, l'écran suivant apparaîtra.

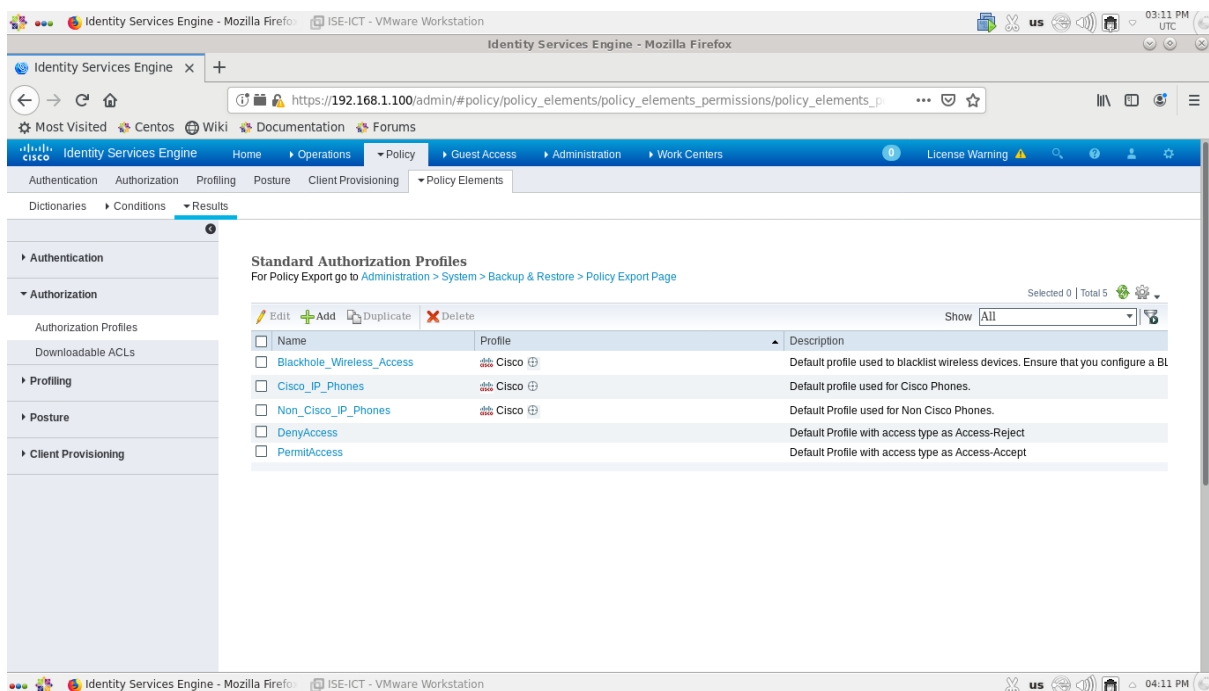


Figure 4.50 : Etape 1.1 de l'ajout de politiques d'autorisation 802.1X.

Etape 1.2. Nous avons cliqué sur “ADD”.

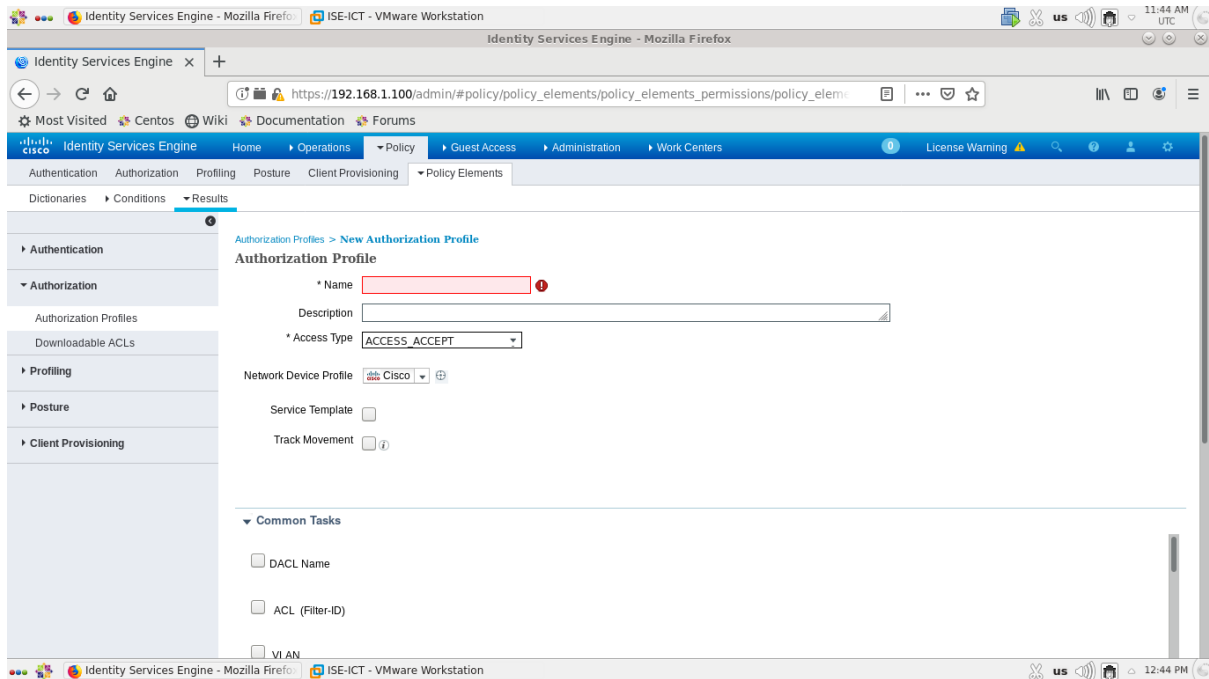


Figure 4.51 : Etape 1.2 de l'ajout de politiques d'autorisation 802.1X.

Etape 1.3. Nous avons ajouté un premier profil d'autorisation 802.1X en remplissant le champ “Name” par “Wired_Admin_auth”.

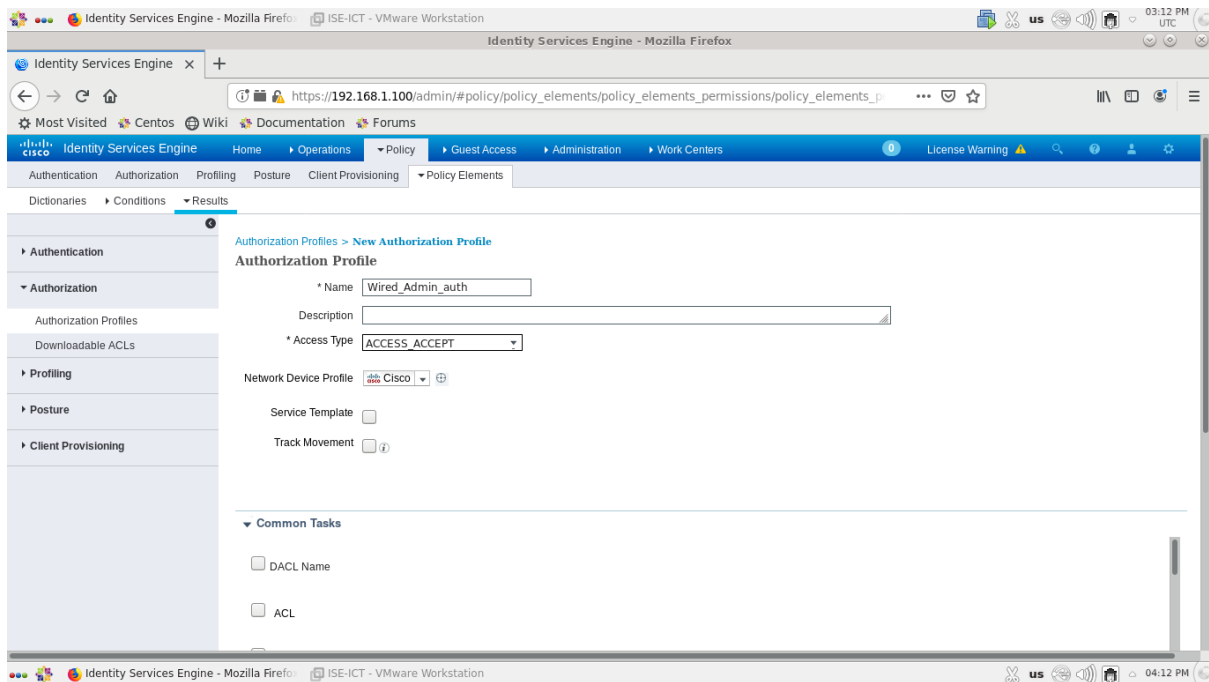


Figure 4.52 : Etape 1.3 de l'ajout de politiques d'autorisation 802.1X.

Etape 1.4. Nous avons cliqué sur “Submit” pour appliquer les changements.

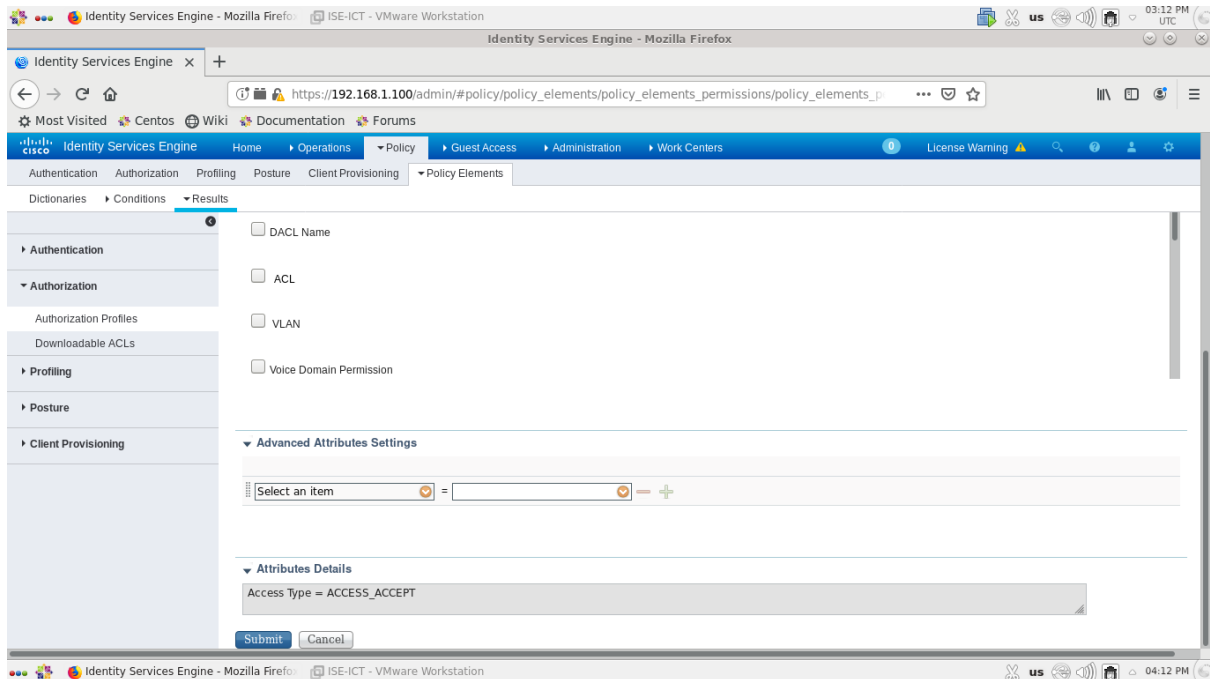


Figure 4.53 : Etape 1.4 de l'ajout de politiques d'autorisation 802.1X.

Etape 1.5. Nous avons ajouté un deuxième profil d'autorisation 802.1X en remplissant le champ “Name” par “Wired_Client_auth”.

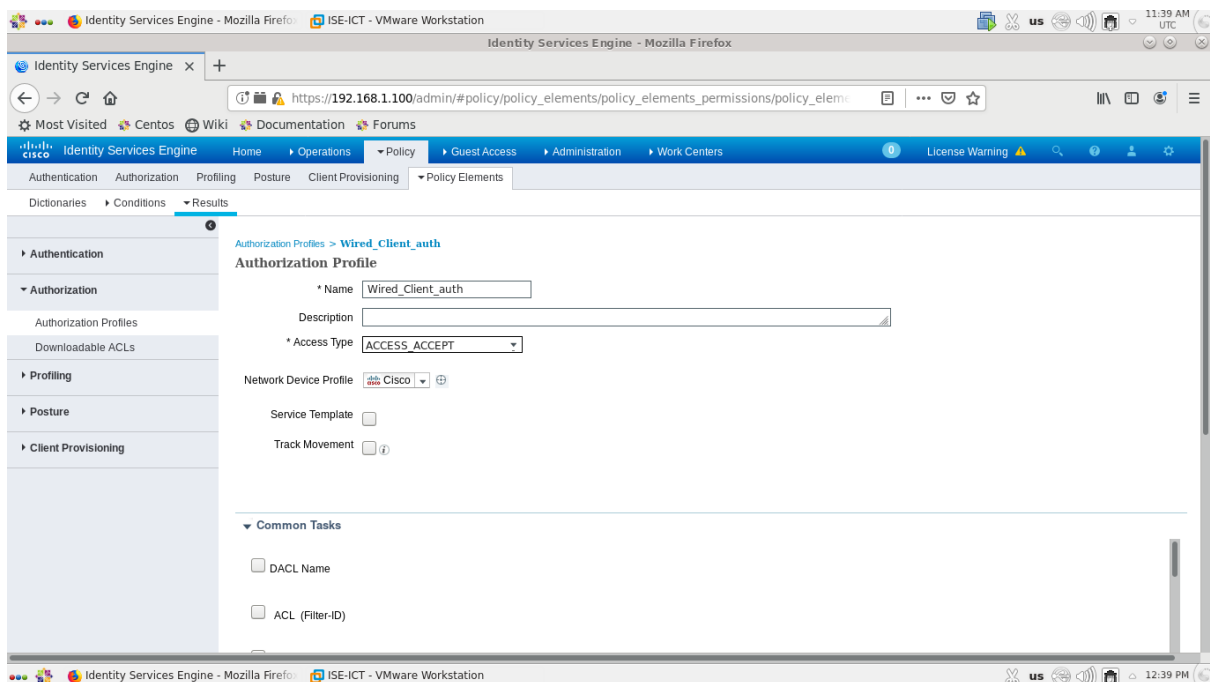


Figure 4.54 : Etape 1.5 de l'ajout de politiques d'autorisation 802.1X.

Etape 1.6. Nous avons cliqué sur “Submit” pour appliquer les changements.

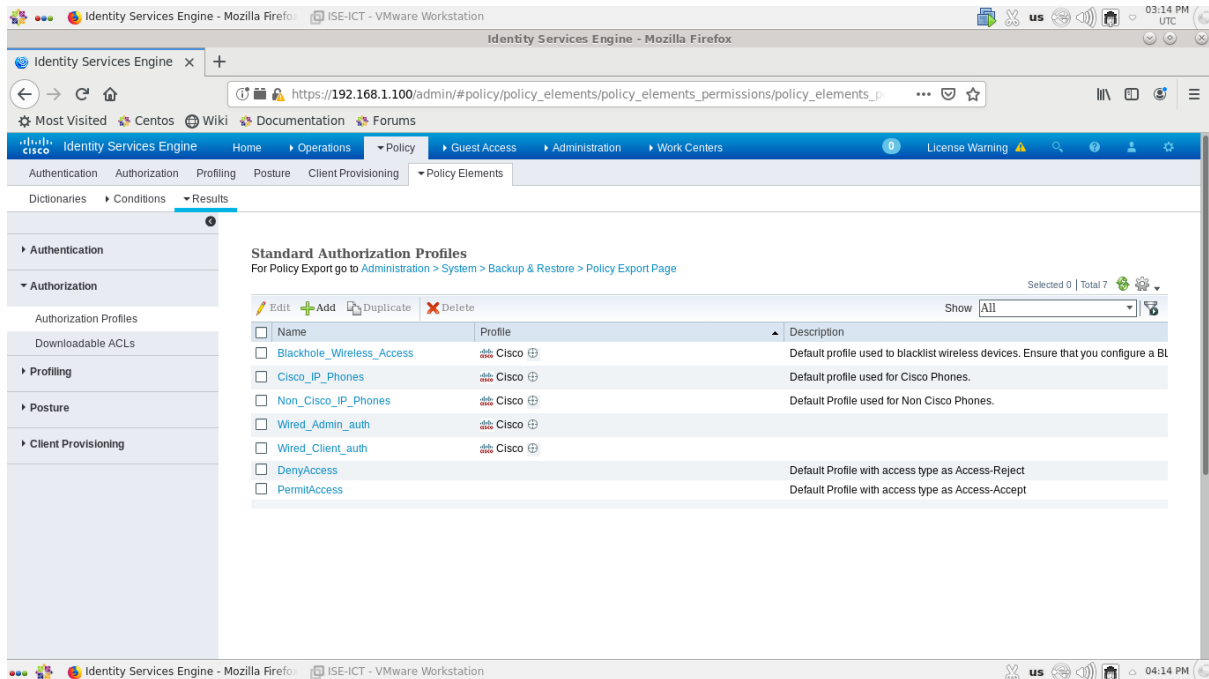


Figure 4.55 : Etape 1.6 de l'ajout de politiques d'autorisation 802.1X.

Etape 2. Nous avons cliqué sur : “Policy” > “Authorization”, l'écran suivant apparaîtra.

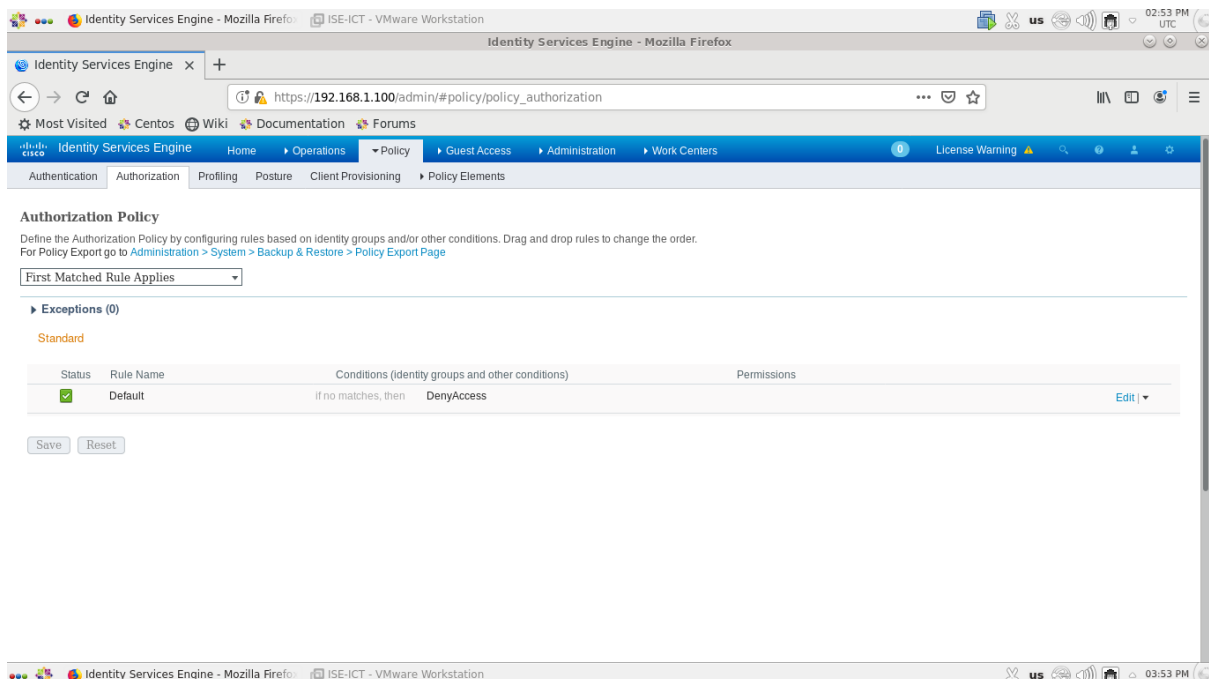


Figure 4.56 : Etape 2 de l'ajout de politiques d'autorisation 802.1X.

Etape 3. Nous avons ajouté une première règle en cliquant sur la flèche qui se trouve à côté de l’option “*Edit*” et nous avons choisi l’option “*Insert New Rule Below*”.

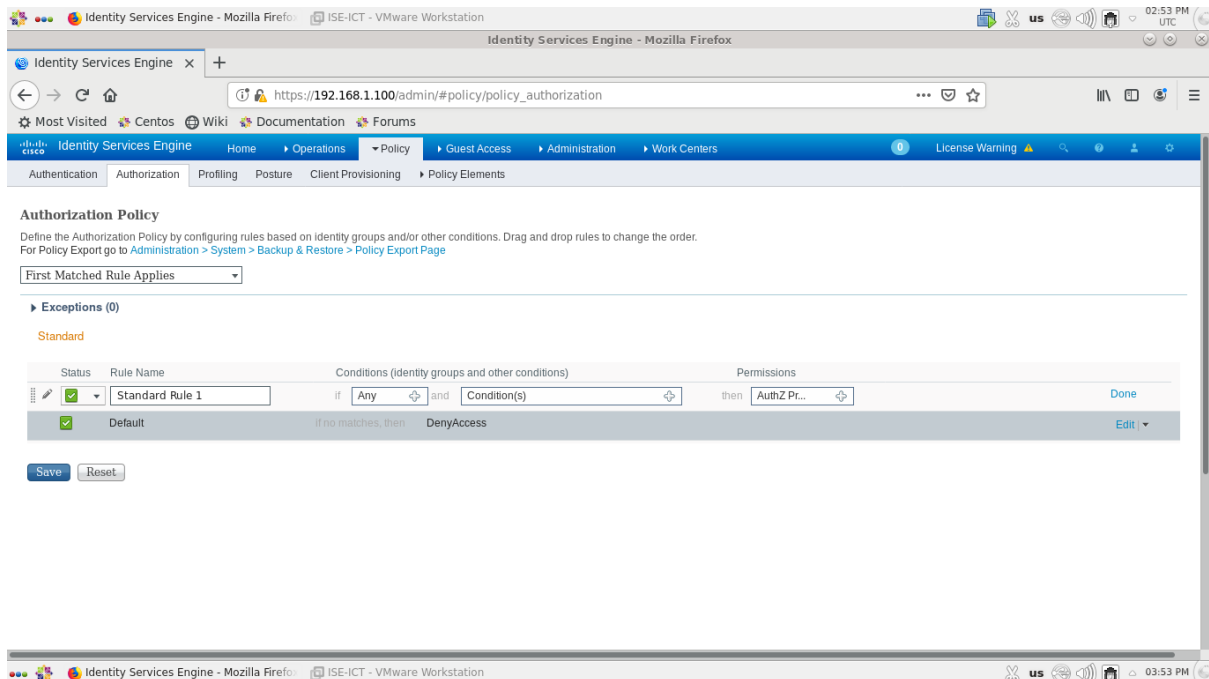


Figure 4.57 : Etape 3 de l’ajout de politiques d’autorisation 802.1X.

Etape 4. Nous avons changé le nom de la règle par “*Admin_Rule*”.

Etape 5. Nous avons choisi le groupe d’identité d’utilisateurs associé à cette règle en cliquant sur “*Any*” > “*Any*” > “*User Identity Groups*” > “*Administrateur*”.

Etape 6. Nous avons choisi la condition associée à ce groupe en cliquant sur “*Condition(s)*” > “*Select Existing Condition from Library*” > “*Select Condition*” > “*Compound Condition*” > “*Wired_802.1X*”.

Etape 7. Nous avons choisi le profil d’autorisation associé à cette règle en cliquant sur “*AuthZ Profiles*” > “*Select an item*” > “*Standard*” > “*Wired_Admin_auth*”.

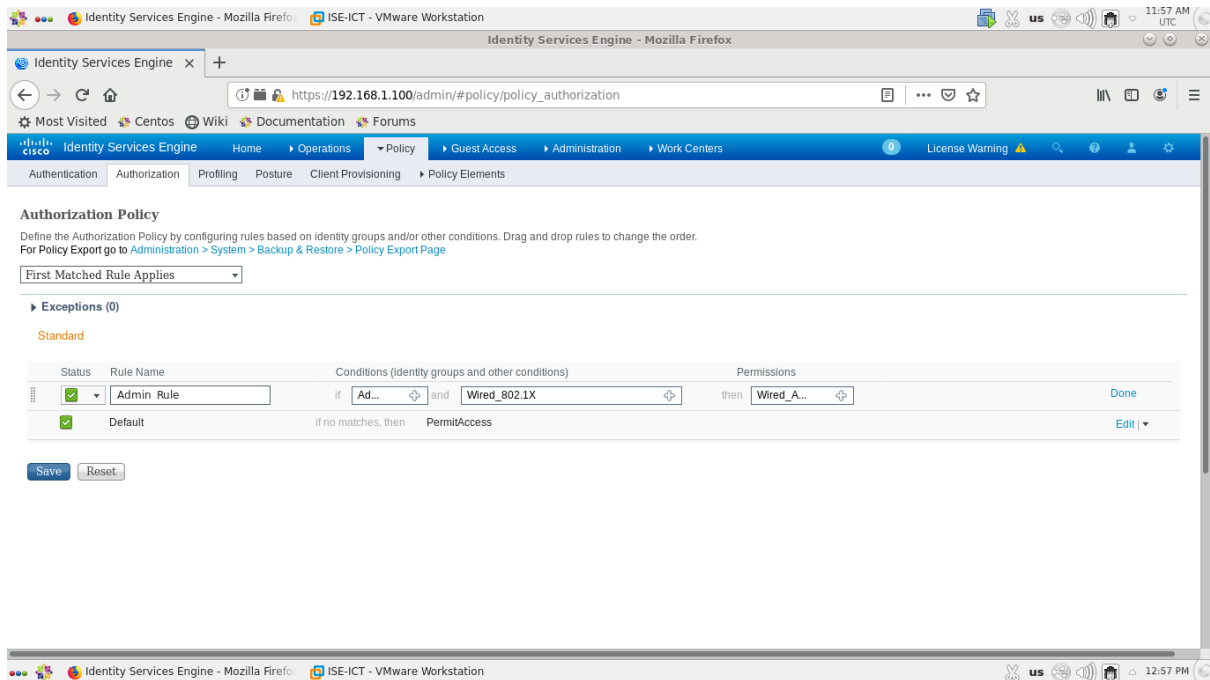


Figure 4.58 : Etape 7 de l'ajout de politiques d'autorisation 802.1X.

Etape 8. Nous avons cliqué sur **“Done”** et nous avons ajouté une deuxième règle en cliquant sur la flèche qui se trouve à côté de l'option **“Edit”** et nous avons choisi l'option **“Insert New Rule Below”**.

Etape 9. Nous avons changé le nom de la règle par **“Client_Rule”**.

Etape 10. Nous avons choisi le groupe d'identité d'utilisateurs associé à cette règle en cliquant sur **“Any” > “Any” > “User Identity Groups” > “Client”**.

Etape 11. Nous avons choisi la condition associée à ce groupe en cliquant sur **“Condition(s)” > “Select Existing Condition from Library” > “Select Condition” > “Compound Condition” > “Wired_802.1X”**.

Etape 12. Nous avons choisi le profil d'autorisation associé à cette règle en cliquant sur **“AuthZ Profiles” > “Select an item” > “Standard” > “Wired_Client_auth”** et nous avons cliqué sur **“Done”**.

Etape 13. Nous avons cliqué sur “Save”.

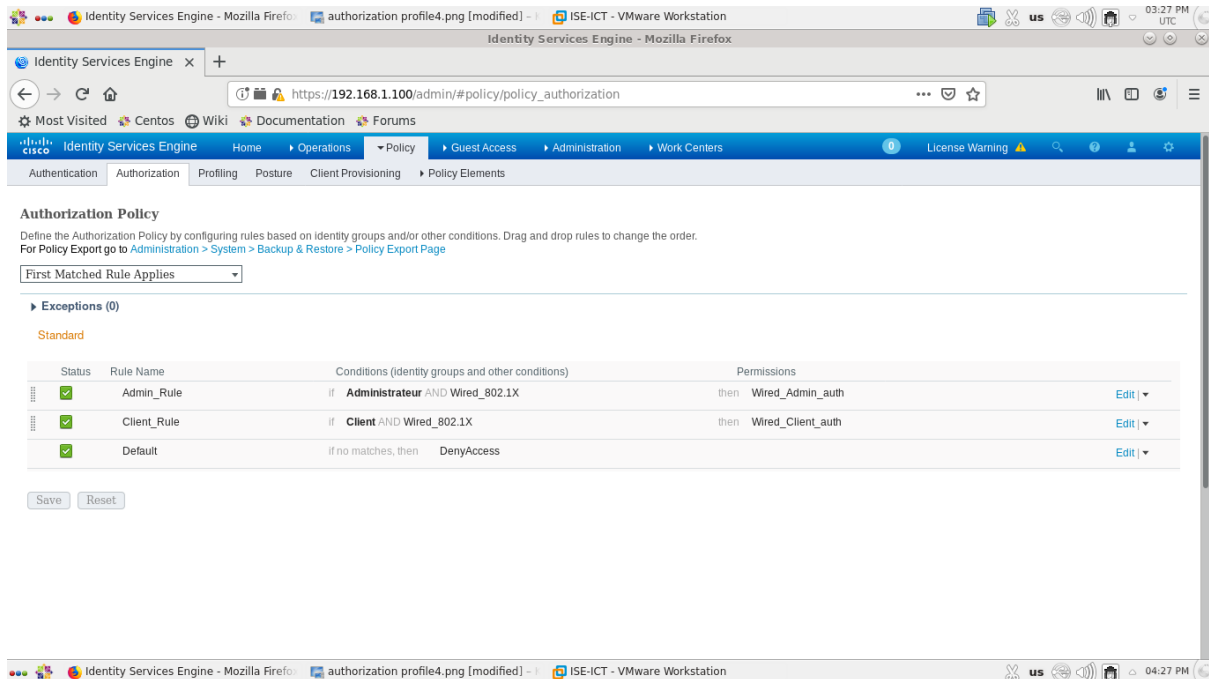


Figure 4.59 : Etape 13 de l'ajout de politiques d'autorisation 802.1X.

4.3.3.2.7.2. Politique d'autorisation MAB

Afin d'ajouter des politiques d'autorisation MAB, nous avons suivi les étapes suivantes :

Etape 1. Tout d'abord, nous avons ajouté un groupe d'identité de point final “*Endpoint identity Groups*”. Pour cela nous avons suivi les sous-étapes suivantes :

Etape 1.1. Nous avons cliqué sur : “*Administration*” > “*Identity Management*” > “*Groups*” > “*Endpoint identity Groups*”, l'écran suivant apparaîtra.

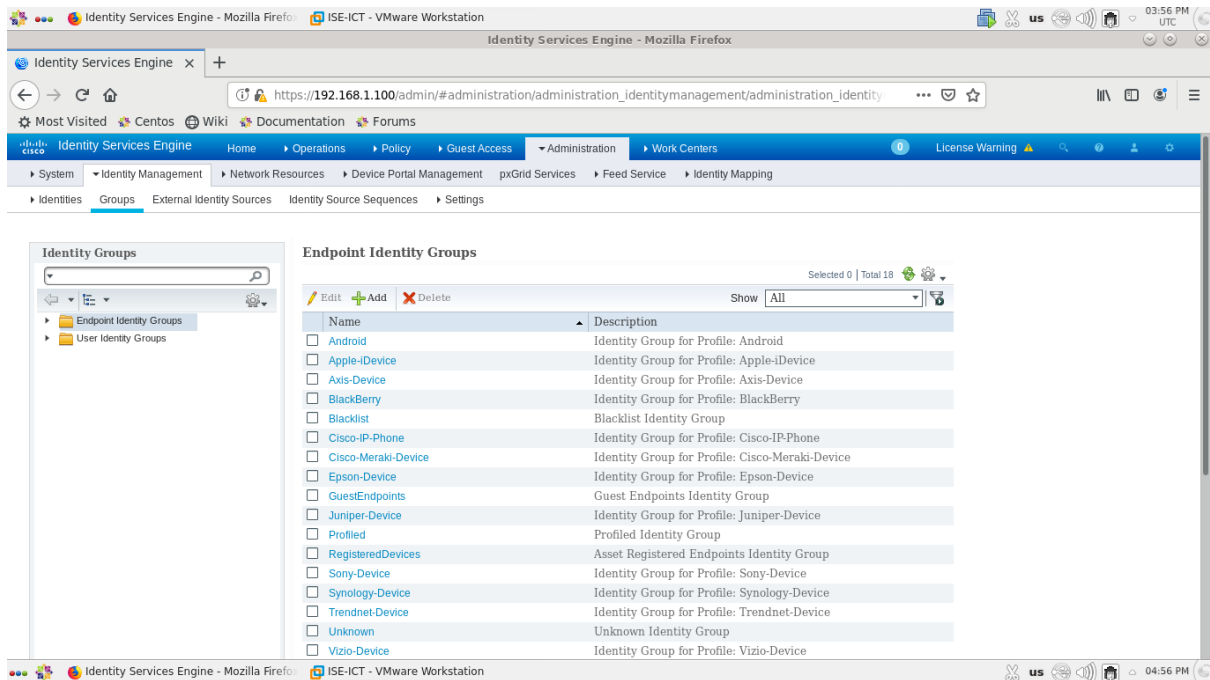


Figure 4.60 : Etape 1.1 de politique d'autorisation MAB.

Etape 1.2. Nous avons cliqué sur “ADD”.

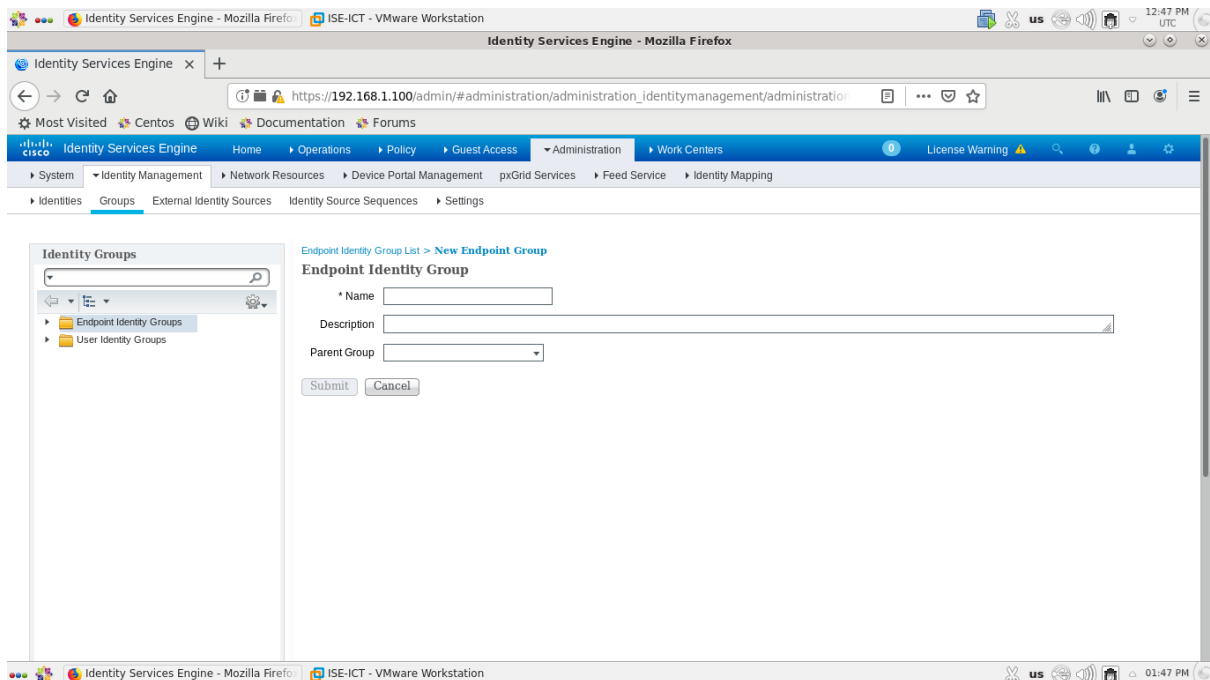


Figure 4.61 : Etape 1.2 de politique d'autorisation MAB.

Etape 1.3. Nous avons ajouté un nouveau groupe en remplissant le champ “Name” par “MAC_Groupe”.

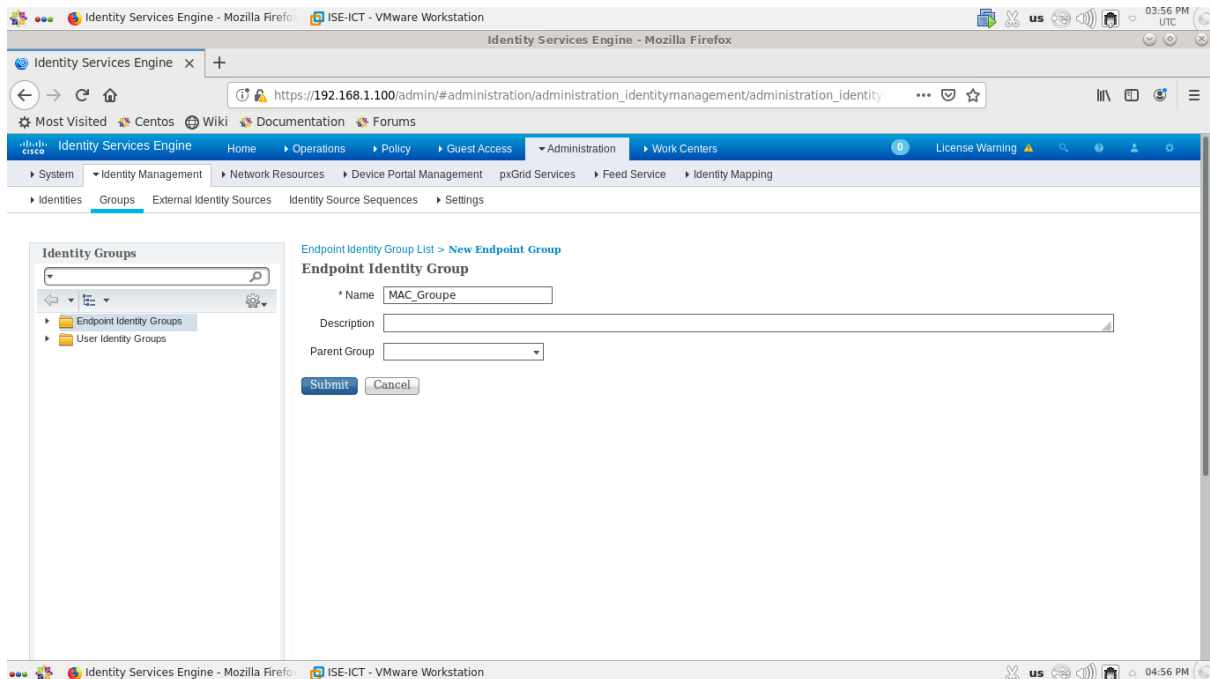


Figure 4.62 : Etape 1.3 de politique d'autorisation MAB.

Etape 1.4. Nous avons cliqué sur “Submit” pour appliquer les changements.

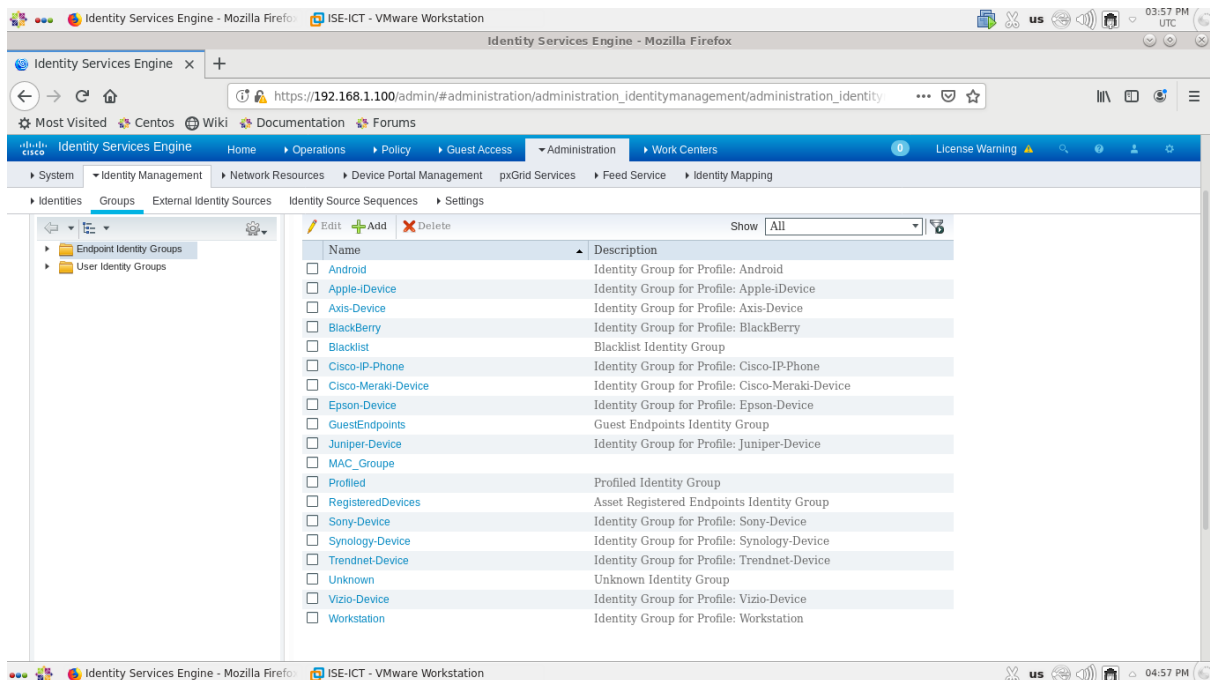


Figure 4.63 : Etape 1.4 de politique d'autorisation MAB.

Etape 2. Nous avons ajouté un point final en suivant les sous étapes suivantes :

Etape 2.1. Nous avons cliqué sur : *“Administration”* > *“Identity Management”* > *“Identities”* > *“Endpoints”*, l’écran suivant apparaîtra.

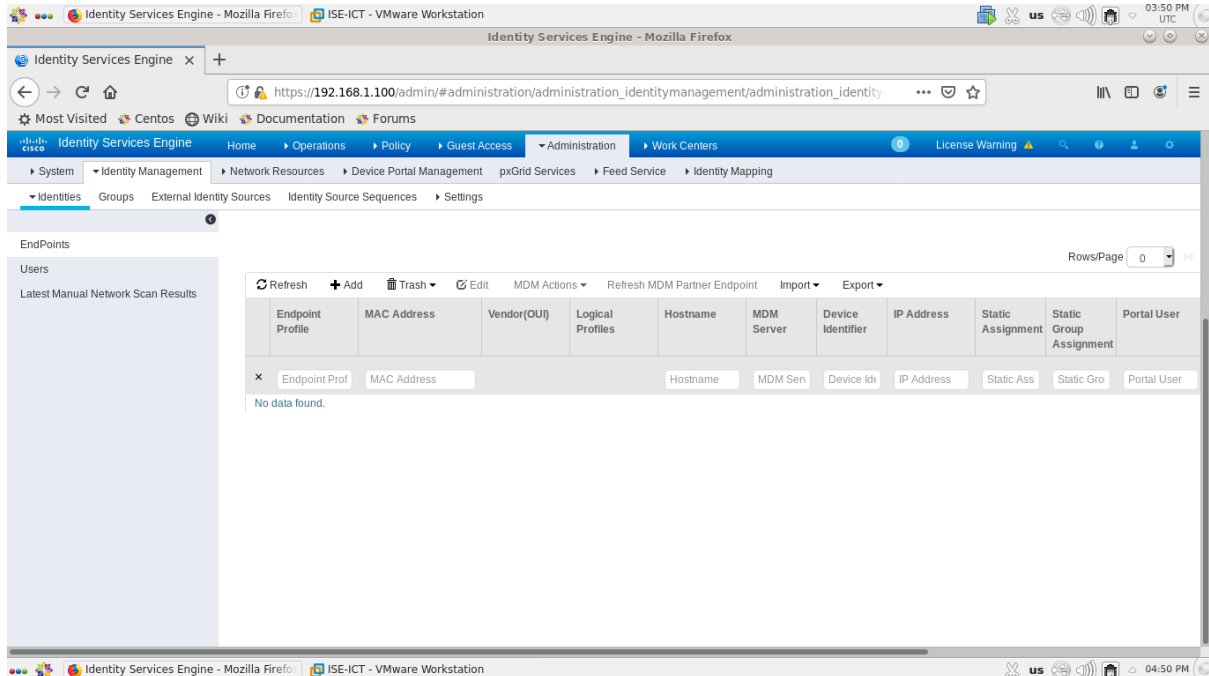


Figure 4.64 : Etape 2.1 de politique d'autorisation MAB.

Etape 2.2. Nous avons cliqué sur *“ADD”*.

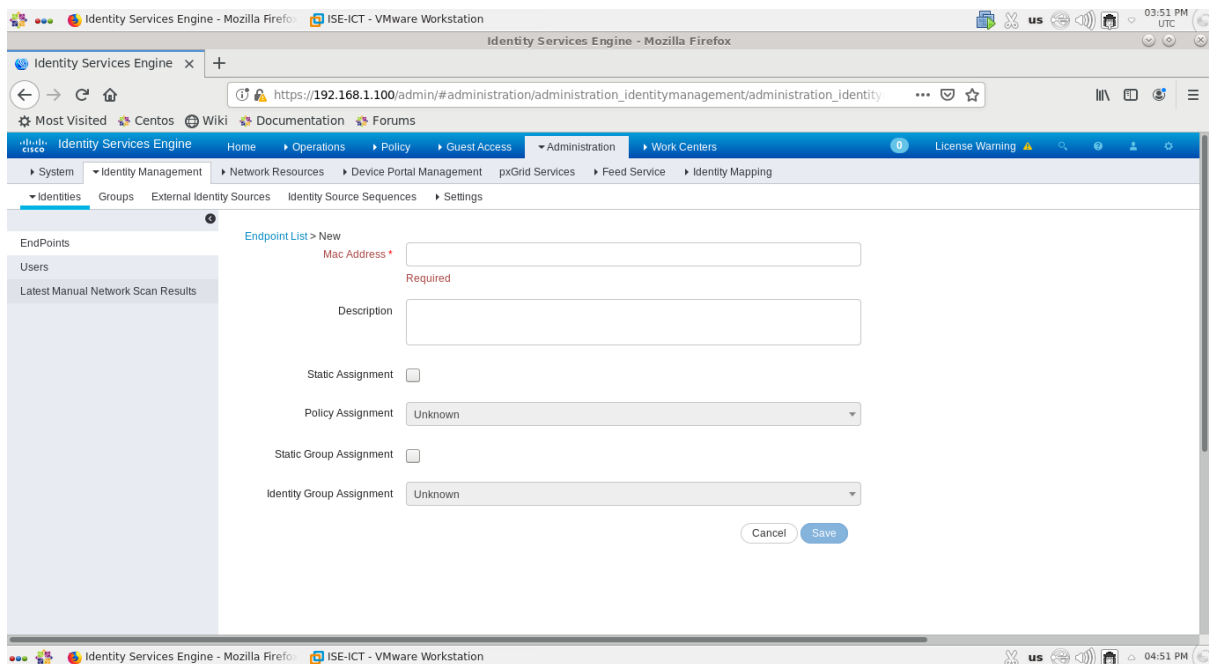


Figure 4.65 : Etape 2.2 de politique d'autorisation MAB.

Etape 2.3. Nous avons ajouté le point final en remplissant le champ **“Mac Address”** par l’adresse Mac correspondante **“Adresse Mac du client Linux”**.

Etape 2.4. Nous avons coché l’option **“Static Group Assignment”** et nous avons affecté cette adresse au groupe d’identité **“MAC_Groupe”**.

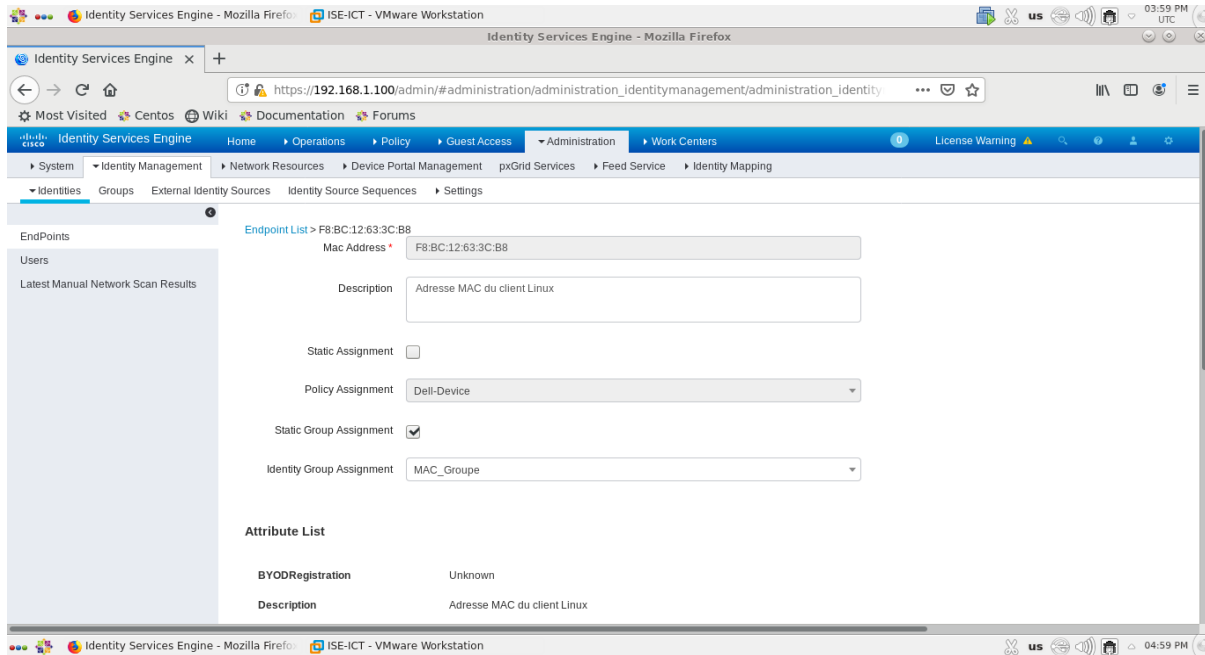


Figure 4.66 : Etape 2.4 de politique d'autorisation MAB.

Etape 2.5. Nous avons cliqué sur **“save”** pour appliquer les changements.

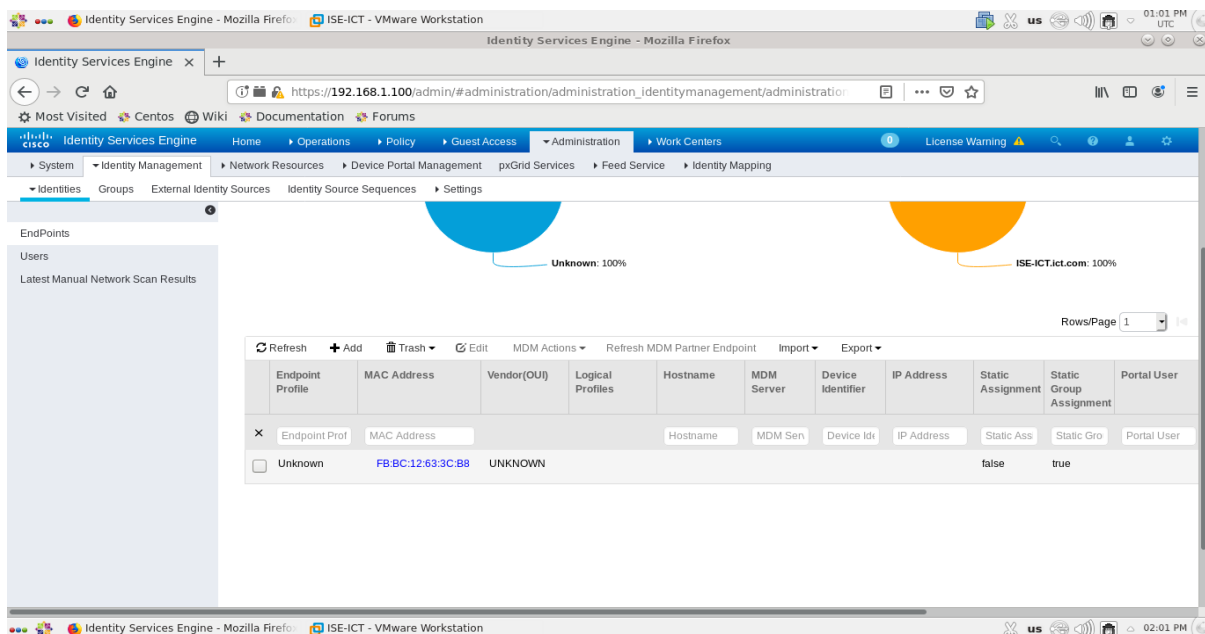


Figure 4.67 : Etape 2.5 de politique d'autorisation MAB.

Etape 3. Nous avons cliqué sur : **“Policy”** > **“Authorization”**, et nous avons ajouté une nouvelle règle en cliquant sur la flèche qui se trouve à côté de l’option **“Edit”** et nous avons choisi l’option **“Insert New Rule Below”**.

Etape 4. Nous avons changé le nom de la règle par **“MAB_Rule”**.

Etape 5. Nous avons choisi le groupe d’identité associé à cette règle en cliquant sur **“Any”** > **“Any”** > **“Endpoint Identity Groups”** > **“MAC_Groupe”**.

Etape 6. Nous avons choisi la condition associée à ce groupe en cliquant sur **“Condition(s)”** > **“Select Existing Condition from Library”** > **“Select Condition”** > **“Compound Condition”** > **“Wired_MAB”**.

Etape 7. Nous avons choisi le profil d’autorisation associé à cette règle en cliquant sur **“AuthZ Profiles”** > **“Select an item”** > **“Standard”** > **“PermitAccess”** et nous avons cliqué sur **“Done”**.

Etape 8. Nous avons cliqué sur **“Save”**.

The screenshot shows the Identity Services Engine (ISE) web interface. The browser address bar displays `https://192.168.1.100/admin/#policy/policy_authorization`. The navigation menu includes **Authentication**, **Authorization**, **Profiling**, **Posture**, **Client Provisioning**, and **Policy Elements**. The main content area is titled **Authorization Policy** and includes a dropdown menu for **First Matched Rule Applies** set to **Standard**. Below this, there is a table of rules:

| Status | Rule Name | Conditions (Identity groups and other conditions) | Permissions | |
|--------|-------------|---|------------------------|----------|
| ✓ | Admin_Rule | if Administrateur AND Wired_802.1X | then Wired_Admin_auth | Edit ▼ |
| ✓ | Client_Rule | if Client AND Wired_802.1X | then Wired_Client_auth | Edit ▼ |
| ✓ | MAB_Rule | if MAC_Groupe AND Wired_MAB | then PermitAccess | Edit ▼ |
| ✓ | Default | if no matches, then | DenyAccess | Edit ▼ |

At the bottom of the table, there are **Save** and **Reset** buttons.

Figure 4.68 : Etape 8 de politique d’autorisation MAB.

4.3.3.2.8. Les tests d'authentification

4.3.3.2.8.1. Test de l'authentification 802.1X

Afin de tester l'authentification **802.1X**, nous avons suivi les étapes suivantes :

Etape 1. Nous avons configuré l'adresse IPv4 du client automatiquement.

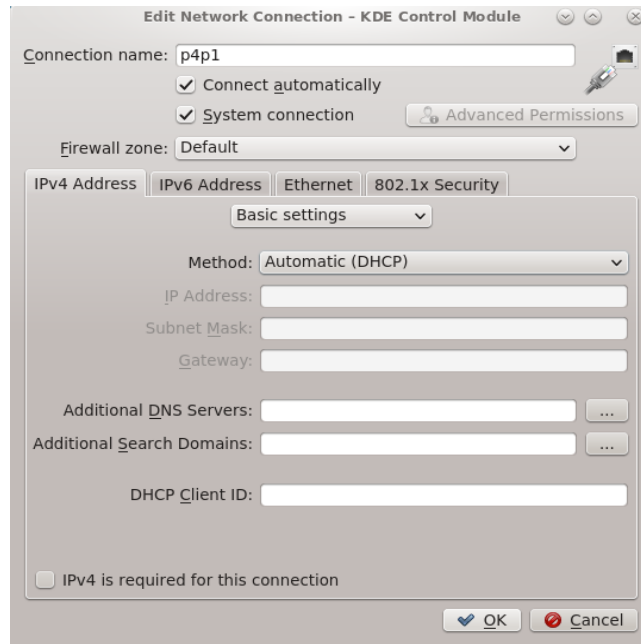


Figure 4.69 : Etape 1 de test de l'authentification 802.1X.

Etape 2. Nous avons choisi la méthode d'authentification **EAP** et nous avons rempli les informations des utilisateurs.

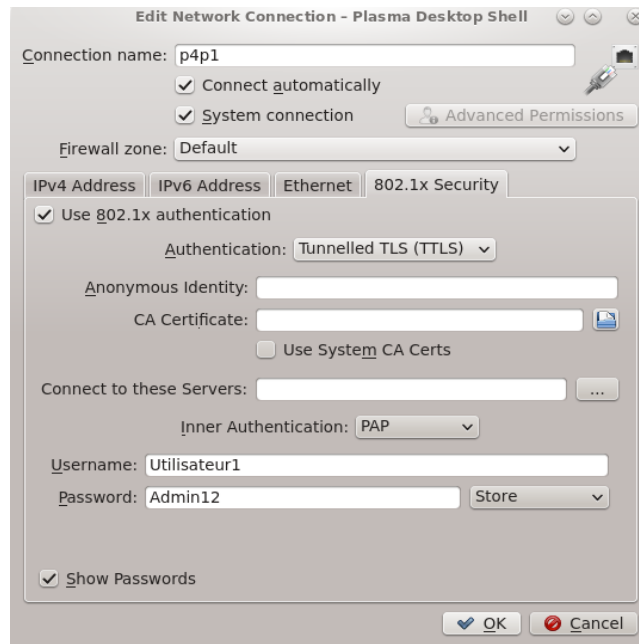


Figure 4.70 : Etape 2.a de test de l'authentification 802.1X (Utilisateur1).

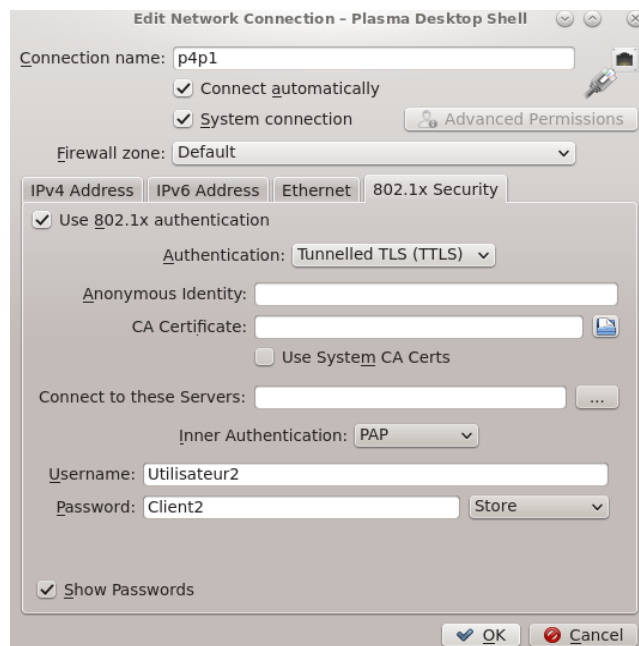


Figure 4.71 : Etape 2.b de test de l'authentification 802.1X (Utilisateur2).

Etape 3. En Utilisant l'outil **Putty**, nous avons connecté au switch d'accès et testé l'authentification du premier utilisateur « **Utilisateur1** ».

```
Authentificateur(config-if)#
*Mar 1 01:08:08.498: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to down
*Mar 1 01:08:11.023: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to up
*Mar 1 01:08:11.124: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A0100000007003E64C2
*Mar 1 01:08:11.174: %DOT1X-5-SUCCESS: Authentication successful for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A0100000007003E64C2
*Mar 1 01:08:11.174: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A0100000007003E64C2
*Mar 1 01:08:11.576: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A0100000007003E64C2
*Mar 1 01:08:12.029: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/11, changed state to up
Authentificateur(config-if)#
```

Figure 4.72 : Etape 3 de test de l'authentification 802.IX.

Etape 4. Nous avons fait un test de troubleshooting au niveau de port connecté au client en utilisant la commande suivante :

```
SW#show authentication sessions interface gigabitEthernet 0/11
```

```
Authentificateur#
Authentificateur#show authentication session int g0/11
      Interface: GigabitEthernet0/11
      MAC Address: f8bc.1263.3cb8
      IP Address: 192.168.1.1
      User-Name: Utilisateur1
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: N/A
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA80A01000000007003E64C2
      Acct Session ID: 0x00000009
      Handle: 0x62000008

Runnable methods list:
  Method  State
  dot1x   Authc Success

Authentificateur#
```

Figure 4.73 : Etape 4 de test de l'authentification 802.IX.

Etape 5. Nous avons testé l'authentification du deuxième utilisateur « **Utilisateur2** » et nous avons fait le test de troubleshooting.

```
Authentificateur(config-if)#
*Mar 1 01:10:56.832: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to down
*Mar 1 01:10:59.332: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to up
*Mar 1 01:10:59.416: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A01000000080040F638
*Mar 1 01:10:59.533: %DOT1X-5-SUCCESS: Authentication successful for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A01000000080040F638
*Mar 1 01:10:59.533: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A01000000080040F638
*Mar 1 01:11:00.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/11, changed state to up
*Mar 1 01:11:00.380: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A01000000080040F638
Authentificateur(config-if)#
```

Figure 4.74 : Etape 5.a de test de l'authentification 802.1X.

```
Authentificateur#show authentication session int g0/11
      Interface: GigabitEthernet0/11
      MAC Address: f8bc.1263.3cb8
      IP Address: 192.168.1.1
      User-Name: Utilisateur2
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: N/A
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA80A01000000080040F638
      Acct Session ID: 0x0000000A
      Handle: 0xAE000009

Runnable methods list:
      Method      State
      dot1x      Authc Success

Authentificateur#
```

Figure 4.75 : Etape 5.b de test de l'authentification 802.1X.

Etape 6. Nous avons vérifié l’authentification au niveau du serveur ISE en allant à “Operations” > “RADIUS LiveLog”.

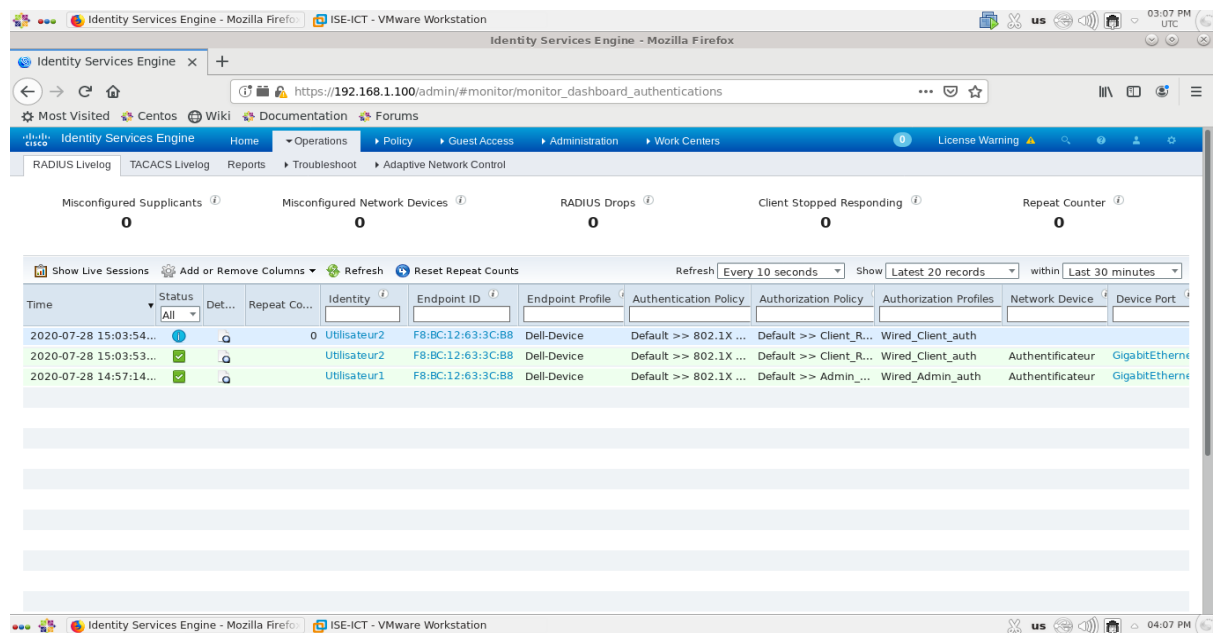


Figure 4.76 : Etape 6 de test de l’authentification 802.1X.

Remarquez-vous que les deux utilisateurs ont été authentifiés avec succès.

4.3.3.2.8.2. Test de l’authentification MAB

Afin de tester l’authentification **MAB**, nous avons suivi les étapes suivantes :

Etape 1. Nous avons désactivé la méthode d’authentification choisie.



Figure 4.77 : Etape 1 de test de l’authentification MAB.

Etape 2. En Utilisant l’outil **Putty**, nous avons connecté au switch d’accès et nous avons testé l’authentification « **MAB** ».

```

Authentificateur#
*Mar 1 01:18:02.806: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to down
*Mar 1 01:18:03.175: %SYS-5-CONFIG I: Configured from console by console
*Mar 1 01:18:05.255: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to up
*Mar 1 01:18:06.262: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/11, changed state to up
Authentificateur#
*Mar 1 01:19:03.287: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:35.898: %DOT1X-5-FAIL: Authentication failed for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:35.898: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:35.898: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:35.898: %AUTHMGR-5-START: Starting 'mab' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:36.502: %MAB-5-SUCCESS: Authentication successful for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:36.502: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
*Mar 1 01:20:36.971: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000A004775FB
Authentificateur#
Authentificateur#

```

Figure 4.78 : Etape 2 de test de l’authentification MAB.

Etape 3. Nous avons fait le test de troubleshooting.

```

Authentificateur#sh authentication sessions int G0/11
      Interface: GigabitEthernet0/11
      MAC Address: f8bc.1263.3cb8
      IP Address: 192.168.1.1
      User-Name: F8-BC-12-63-3C-B8
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: N/A
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA80A010000000A004775FB
      Acct Session ID: 0x0000000C
      Handle: 0xD200000B

Runnable methods list:
      Method      State
      dot1x      Failed over
      mab        Authc Success

Authentificateur#

```

Figure 4.79 : Etape 3 de test de l’authentification MAB.

Etape 4. Nous avons vérifié l'authentification au niveau du serveur ISE.

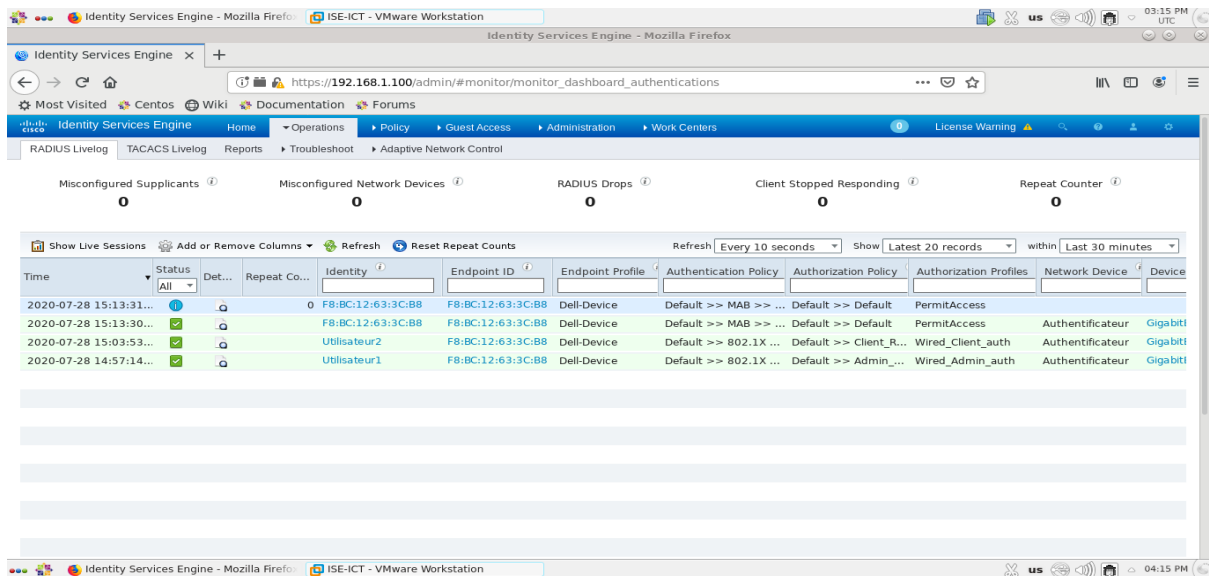


Figure 4.80 : Etape 4 de test de l'authentification MAB.

Remarquez-vous que l'authentification a été réalisée avec succès.

4.4. Configuration des variables 802.1X

Afin d'avoir une dynamique d'accès au réseau, il est recommandé d'utiliser les variables dynamiques qui permettent de l'optimiser et parmi ces variables, nous avons les suivantes :

4.4.1. Affectation des VLANs « *VLAN Assignment* »

4.4.1.1. Configuration de l'affectation des VLANs

Pour configurer ce type de variables dynamiques au niveau de serveur ISE, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : **“Policy”** > **“Policy Elements”** > **“Results”** > **“Authorization”** > **“Authorization Profiles”**.

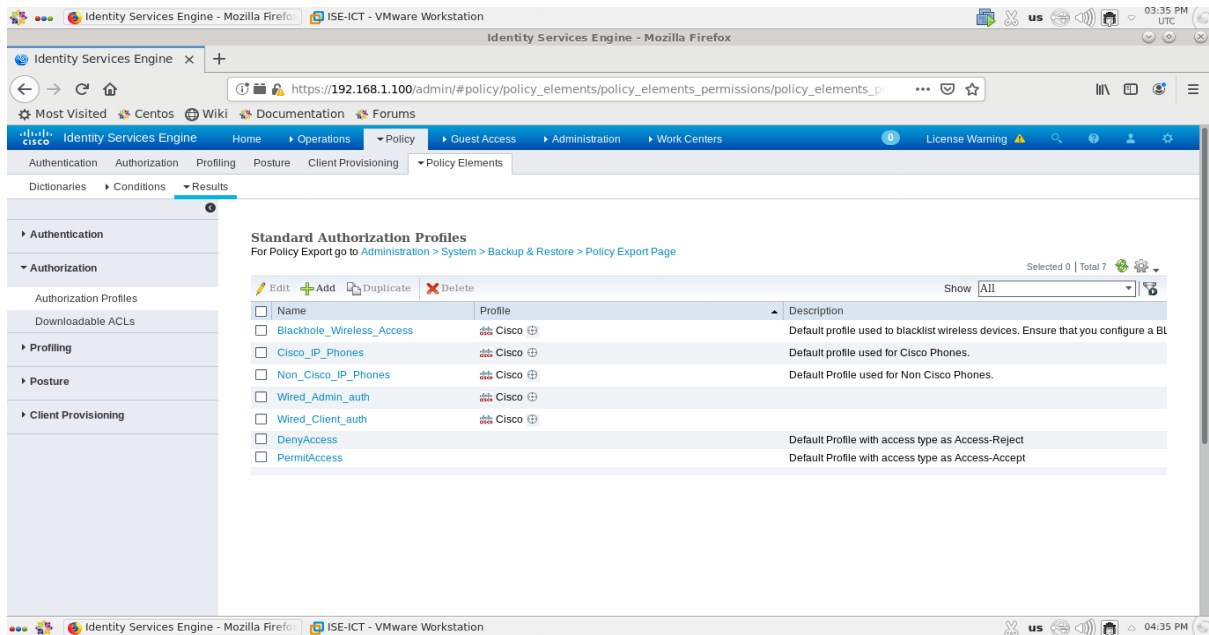


Figure 4.81 : Etape 1 de configuration de l'affectation des VLANs.

Etape 2. Nous avons cliqué sur le profil du premier utilisateur **“Wired_Admin_auth”** et nous sommes allés à la section **“Common Tasks”**.

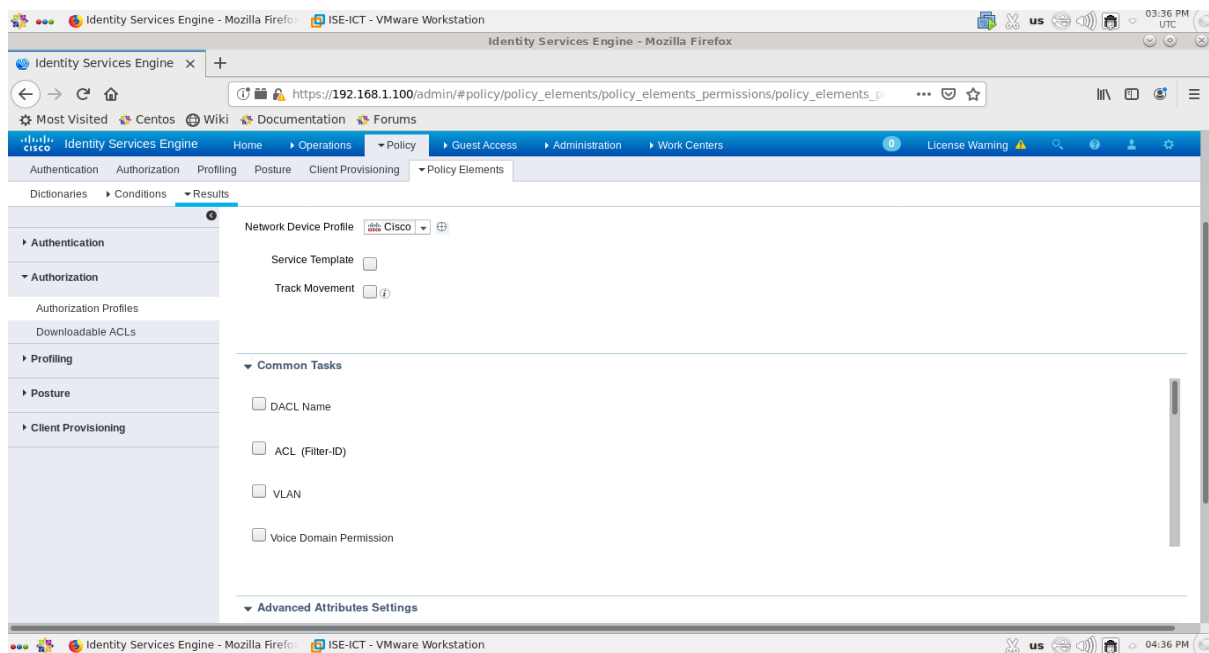


Figure 4.82 : Etape 2 de configuration de l'affectation des VLANs.

Etape 3. Nous avons coché l'option **“VLAN”** et nous avons rempli le champ **“ID/Name”** par la valeur **“10”**.

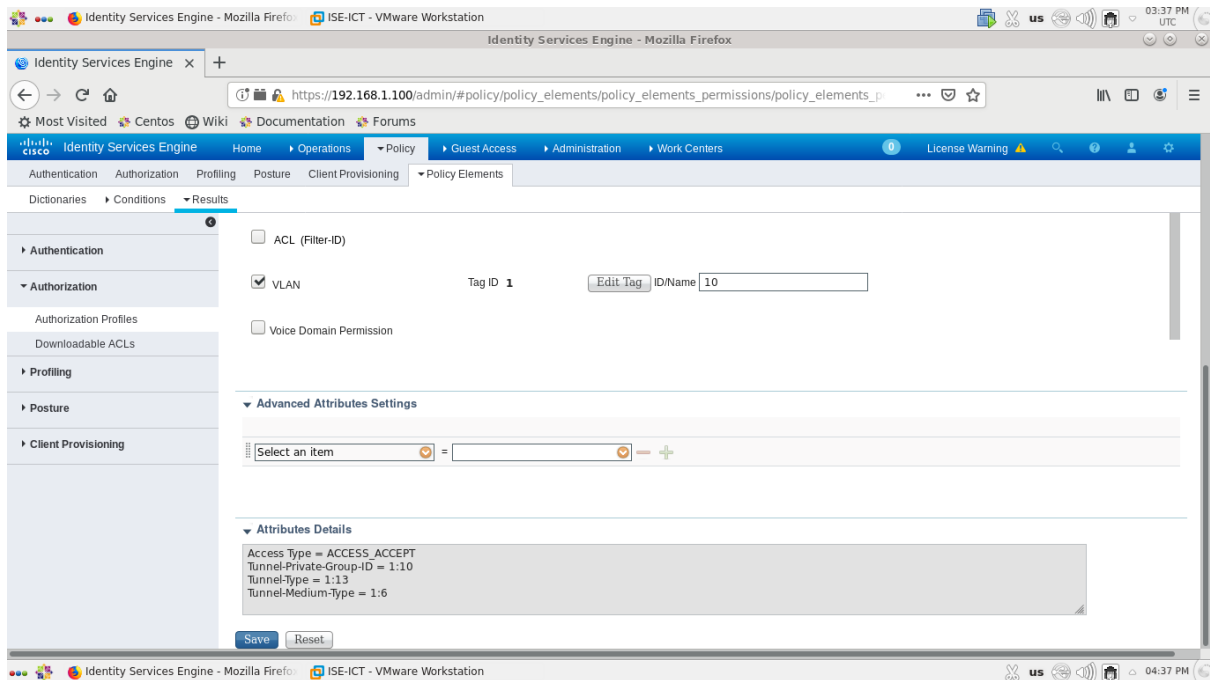


Figure 4.83 : Etape 3 de configuration de l'affectation des VLANs.

Etape 4. Nous avons sauvegardé la configuration en cliquant sur “Save”.

Etape 5. Nous avons répété les mêmes étapes pour le deuxième utilisateur mais cette fois-ci en remplissant le champ “ID/Name” par la valeur “20” et nous avons sauvegardé la configuration.

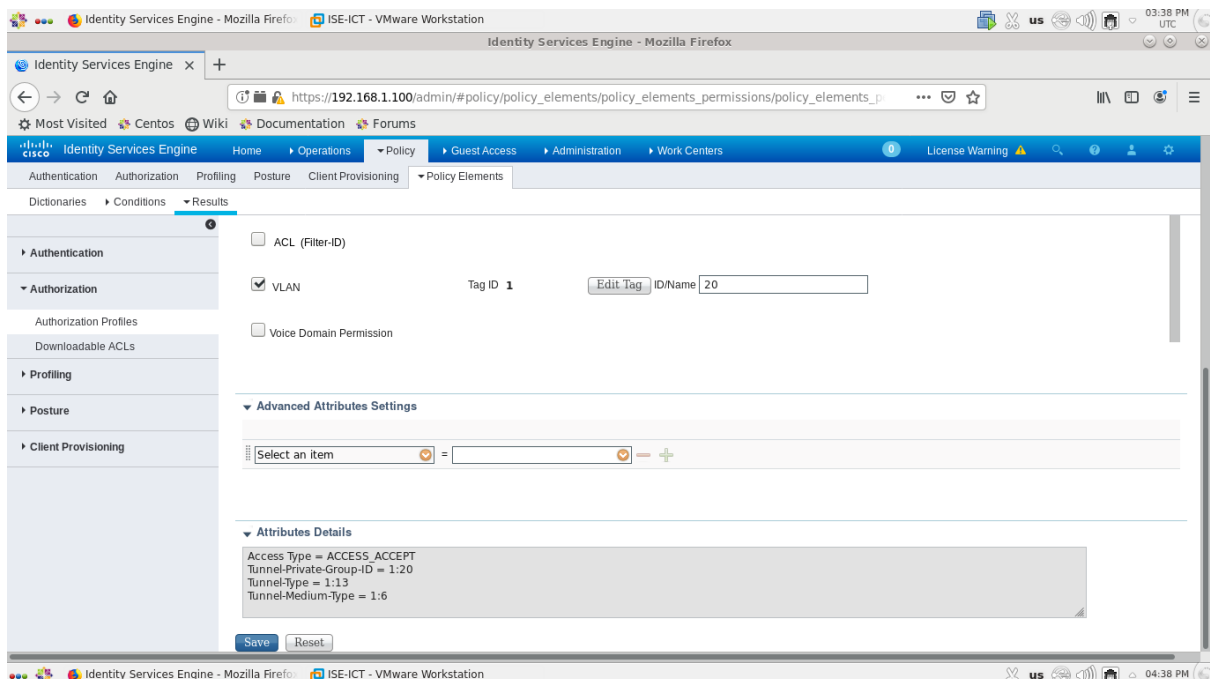


Figure 4.84 : Etape 5 de configuration de l'affectation des VLANs.

4.4.1.2. Tests de configuration

Afin de tester l'affectation des VLANs, nous avons suivi les étapes suivantes :

Etape 1. Nous avons configuré l'adresse IPv4 du client automatiquement.

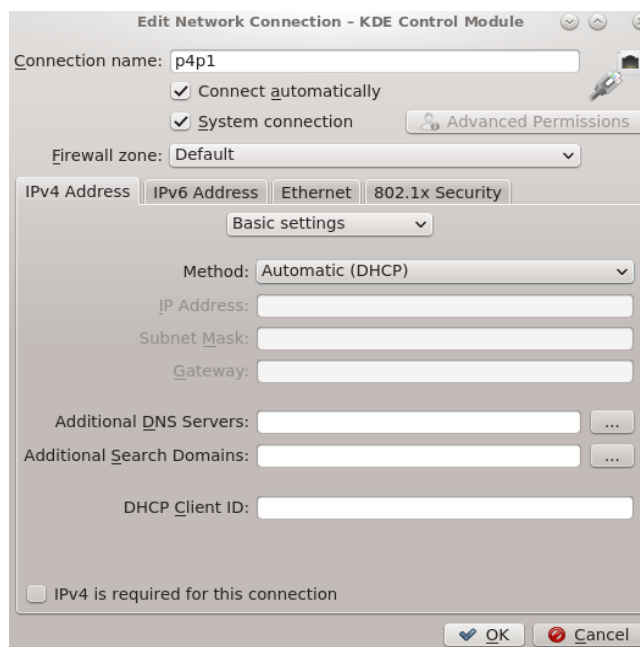


Figure 4.85 : Etape 1 de test de configuration de l'affectation des VLANs.

Etape 2. Nous avons réactivé l'authentification **802.1X** au niveau du client pour le premier utilisateur « **Utilisateur1** ».

Etape 3. Nous avons connecté au switch d'accès et nous avons testé l'authentification du premier utilisateur « **Utilisateur1** ».

```

Authentificateur#
*Mar 1 01:35:09.294: %SYS-5-CONFIG I: Configured from console by console
*Mar 1 01:35:12.205: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000F0056EE8D
*Mar 1 01:35:12.264: %DOT1X-5-SUCCESS: Authentication successful for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000F0056EE8D
*Mar 1 01:35:12.264: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000F0056EE8D
*Mar 1 01:35:12.264: %AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi0/11 AuditSessionID COA80A010000000F0056EE8D
*Mar 1 01:35:12.969: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000000F0056EE8D
*Mar 1 01:35:42.304: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Authentificateur#
Authentificateur#
Authentificateur#

```

Figure 4.86 : Etape 3 de test de configuration de l'affectation des VLANs.

Etape 4. Nous avons fait le test de troubleshooting.

```

Authentificateur#sh authentication sessions int G0/11
      Interface: GigabitEthernet0/11
      MAC Address: f8bc.1263.3cb8
      IP Address: 192.168.10.2
      User-Name: Utilisateur1
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: 10
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA80A010000000F0056EE8D
      Acct Session ID: 0x00000011
      Handle: 0x81000010

Runnable methods list:
      Method      State
      dot1x      Authc Success
      mab         Not run

Authentificateur#

```

Figure 4.87 : Etape 4 de test de configuration de l'affectation des VLANs.

Etape 5. Nous avons réactivé l'authentification **802.1X** au niveau du client pour le deuxième utilisateur « **Utilisateur2** ».

Etape 6. Nous avons connecté au switch d'accès et nous avons testé l'authentification du deuxième utilisateur « **Utilisateur2** ».

```

Authentificateur#
*Mar 1 01:37:30.835: %SYS-5-CONFIG I: Configured from console by console
*Mar 1 01:37:31.121: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to down
*Mar 1 01:37:33.520: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to up
*Mar 1 01:37:33.620: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000001000594983
*Mar 1 01:37:33.679: %DOT1X-5-SUCCESS: Authentication successful for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000001000594983
*Mar 1 01:37:33.679: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (f8bc.1263.3cb8) on I
Authentificateur#interface Gi0/11 AuditSessionID COA80A010000001000594983
*Mar 1 01:37:33.679: %AUTHMGR-5-VLANASSIGN: VLAN 20 assigned to Interface Gi0/11 AuditSessionID COA80A010000001000594983
*Mar 1 01:37:33.964: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA80A010000001000594983
*Mar 1 01:37:34.526: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/11, changed state to up
Authentificateur#
Authentificateur#

```

Figure 4.88 : Etape 6 de test de configuration de l'affectation des VLANs.

Etape 7. Nous avons fait le test de troubleshooting.

```

Authenticateur#sh authentication sessions int G0/11
      Interface: GigabitEthernet0/11
      MAC Address: f8bc.1263.3cb8
      IP Address: 192.168.20.2
      User-Name: Utilisateur2
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: 20
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA80A010000001000594983
      Acct Session ID: 0x00000012
      Handle: 0xAB000011

Runnable methods list:
      Method      State
      dot1x      Authz Success
      mab        Not run

Authenticateur#
  
```

Figure 4.89 : Etape 7 de test de configuration de l'affectation des VLANs.

Etape 8. Nous avons vérifié l'authentification au niveau du serveur ISE.

| Time | Status | Det... | Repeat Co... | Identity | Endpoint ID | Endpoint Profile | Authentication Policy | Authorization Policy | Authorization Profiles | Network Device | Device Port |
|------------------------|---------------|--------|--------------|--------------|-------------------|------------------|-----------------------|------------------------|------------------------|----------------|------------------|
| 2020-07-28 15:31:08... | Authz Success | | 0 | Utilisateur2 | F8-BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Client_R... | Wired_Client_auth | Authenticateur | GigabitEthern... |
| 2020-07-28 15:30:28... | Authz Success | | 0 | Utilisateur2 | F8-BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Client_R... | Wired_Client_auth | Authenticateur | GigabitEthern... |
| 2020-07-28 15:24:49... | Authz Success | | 0 | Utilisateur1 | F8-BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Admin_... | Wired_Admin_auth | Authenticateur | GigabitEthern... |
| 2020-07-28 15:13:30... | Authz Success | | 0 | Utilisateur2 | F8-BC:12:63:3C:B8 | Dell-Device | Default >> MAB >> ... | Default >> Default | PermitAccess | Authenticateur | GigabitEthern... |
| 2020-07-28 15:03:53... | Authz Success | | 0 | Utilisateur2 | F8-BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Client_R... | Wired_Client_auth | Authenticateur | GigabitEthern... |
| 2020-07-28 14:57:14... | Authz Success | | 0 | Utilisateur1 | F8-BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Admin_... | Wired_Admin_auth | Authenticateur | GigabitEthern... |

Figure 4.90 : Etape 8 de test de configuration de l'affectation des VLANs.

Remarquez-vous que l'affectation des VLANs a été réalisée avec succès.

4.4.2. Liste de contrôle d'accès téléchargeable « *DACLs* »

4.4.2.1. Configuration des DACLs

Pour configurer ce type de variables dynamiques au niveau de serveur ISE, nous avons suivi les étapes suivantes :

Etape 1. Nous avons cliqué sur : “*Policy*” > “*Policy Elements*” > “*Results*” > “*Authorization*” > “*Downloadable ACLs*”.

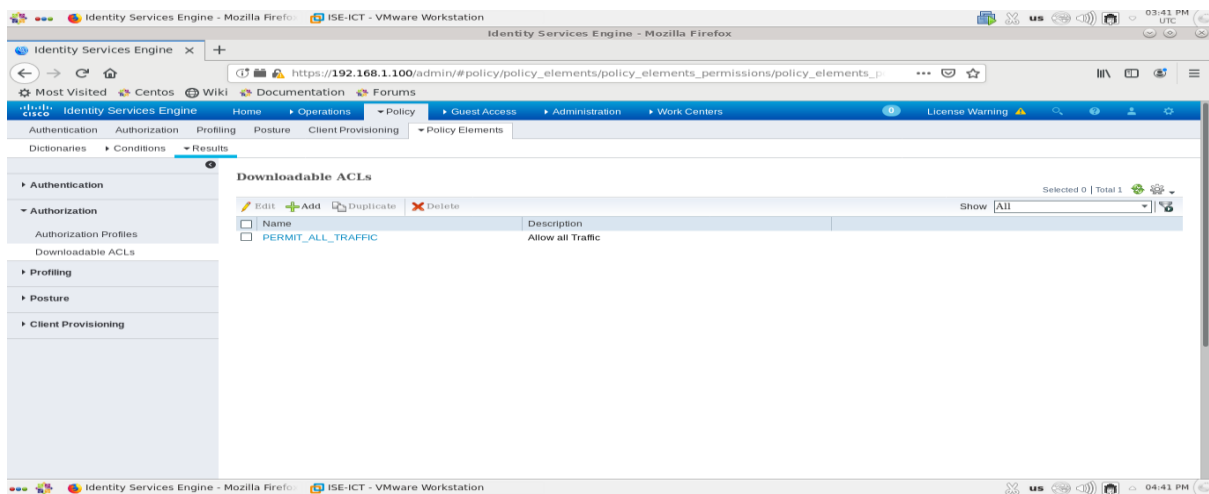


Figure 4.91 : Etape 1 de configuration des DACLs.

Etape 2. Nous avons cliqué sur : “*ADD*”.

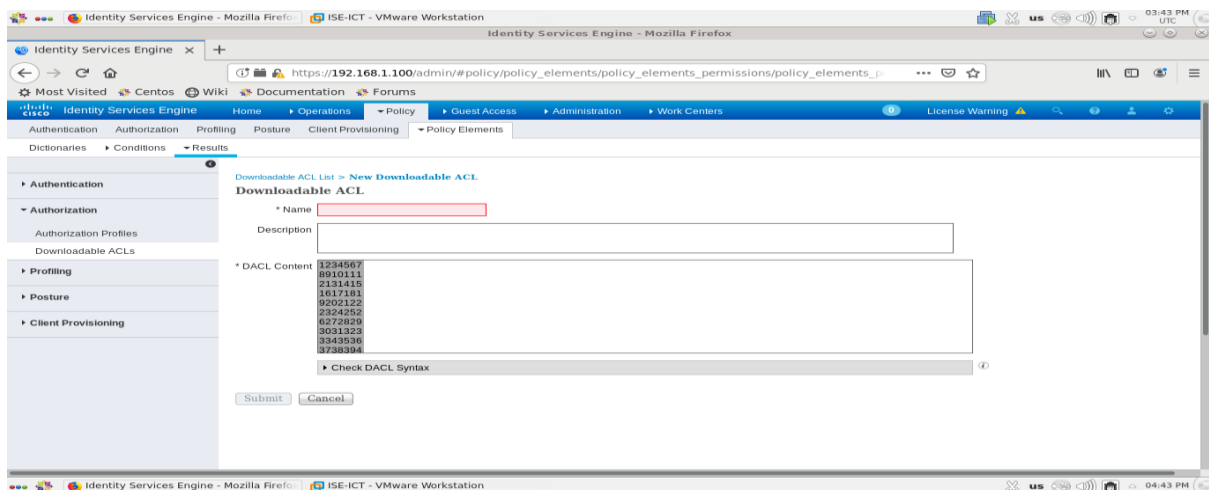


Figure 4.92 : Etape 2 de configuration des DACLs.

Etape 3. Nous avons créé une DACL pour « **Utilisateur1** » en remplissant les champ “**Name**” et “**DACL Content**” par ses informations appropriées et nous l’avons validée, puis nous avons cliqué sur “**Submit**” pour appliquer les changements.

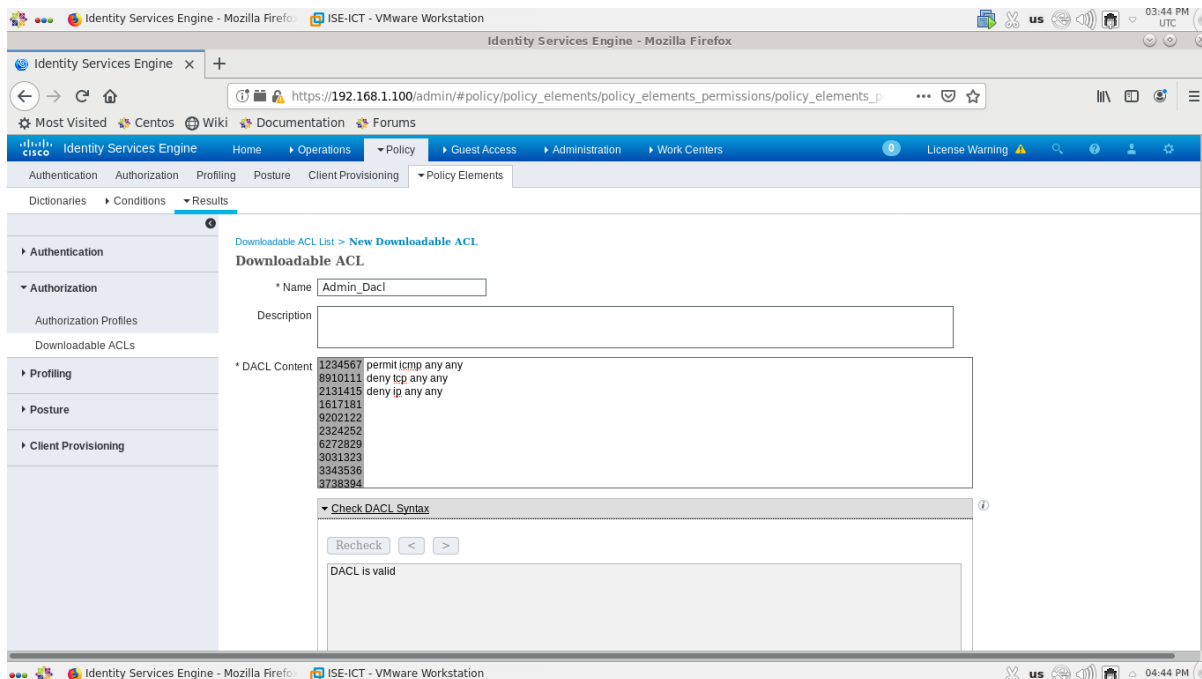


Figure 4.93 : Etape 3 de configuration des DACLs.

Etape 4. Nous avons créé une deuxième DACL pour « **Utilisateur2** » en remplissant les champ “**Name**” et “**DACL Content**” par ses informations appropriées et nous l’avons validée, puis nous avons cliqué sur “**Submit**” pour appliquer les changements.

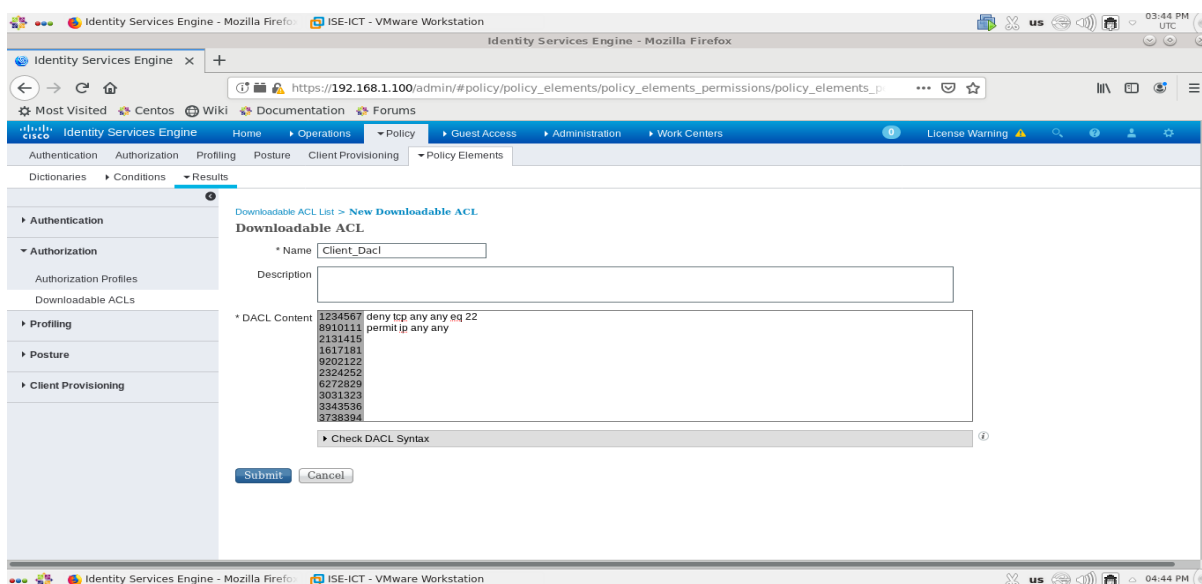


Figure 4.94 : Etape 4.a de configuration des DACLs.

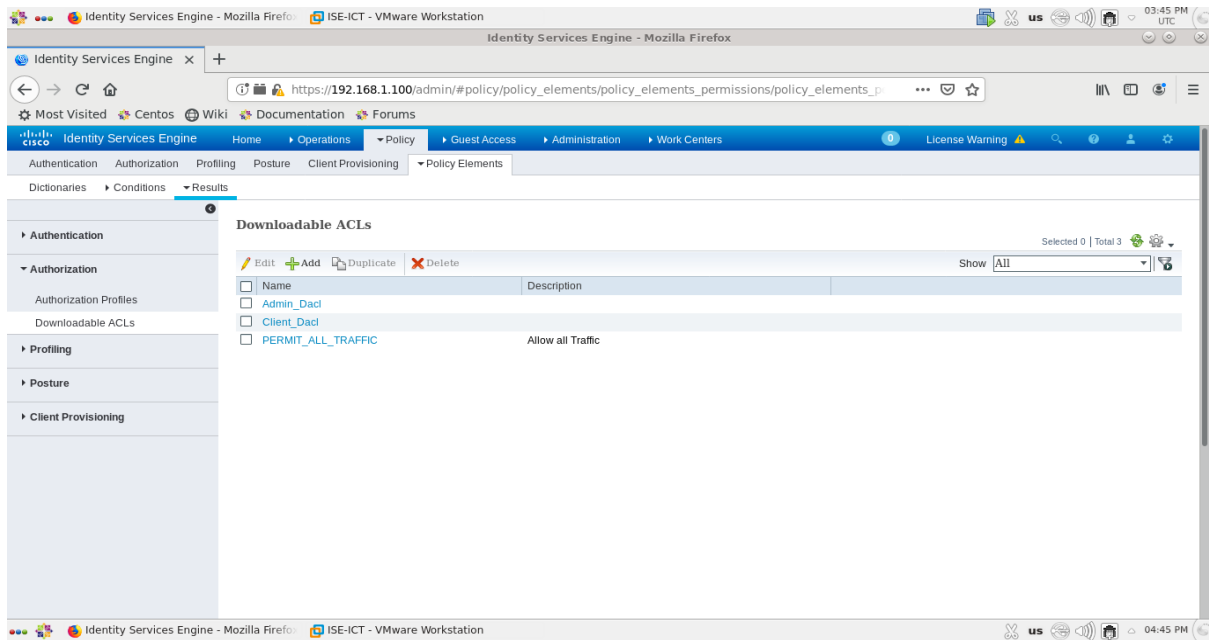


Figure 4.95 : Etape 4.b de configuration des DACLs.

Etape 5. Nous avons cliqué sur : **“Policy”** > **“Policy Elements”** > **“Results”** > **“Authorization”** > **“Authorization Profiles”**.

Etape 6. Nous avons cliqué sur le profil du premier utilisateur **“Wired_Admin_auth”**.

Etape 7. Nous sommes allés à la section **“Common Tasks”** et nous avons coché l’option **“DACL Name”** puis nous avons choisi la DACL du premier utilisateur **“Admin_Dacl”**.

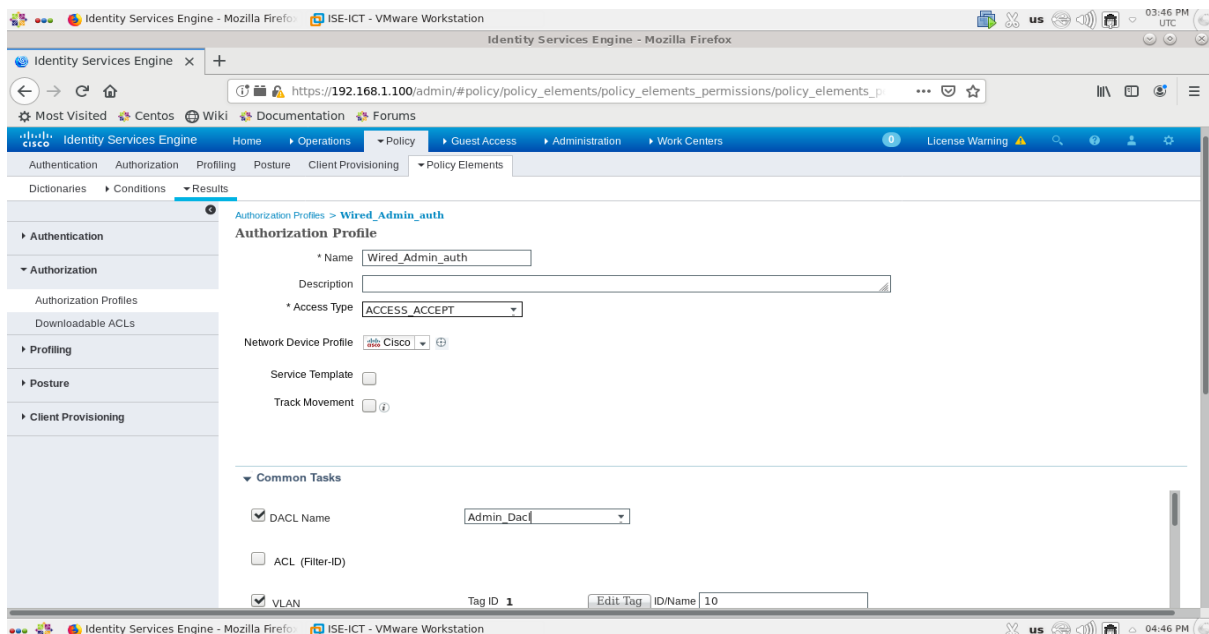


Figure 4.96 : Etape 7 de configuration des DACLs.

Etape 8. Nous avons cliqué sur **“Submit”** pour appliquer les changements.

Etape 9. Nous avons cliqué sur le profil du deuxième utilisateur **“Wired_Client_auth”**.

Etape 10. Nous sommes allés à la section **“Common Tasks”** et nous avons coché l’option **“DACL Name”** puis nous avons choisi la DACL du deuxième utilisateur **“Client_Dacl”**.

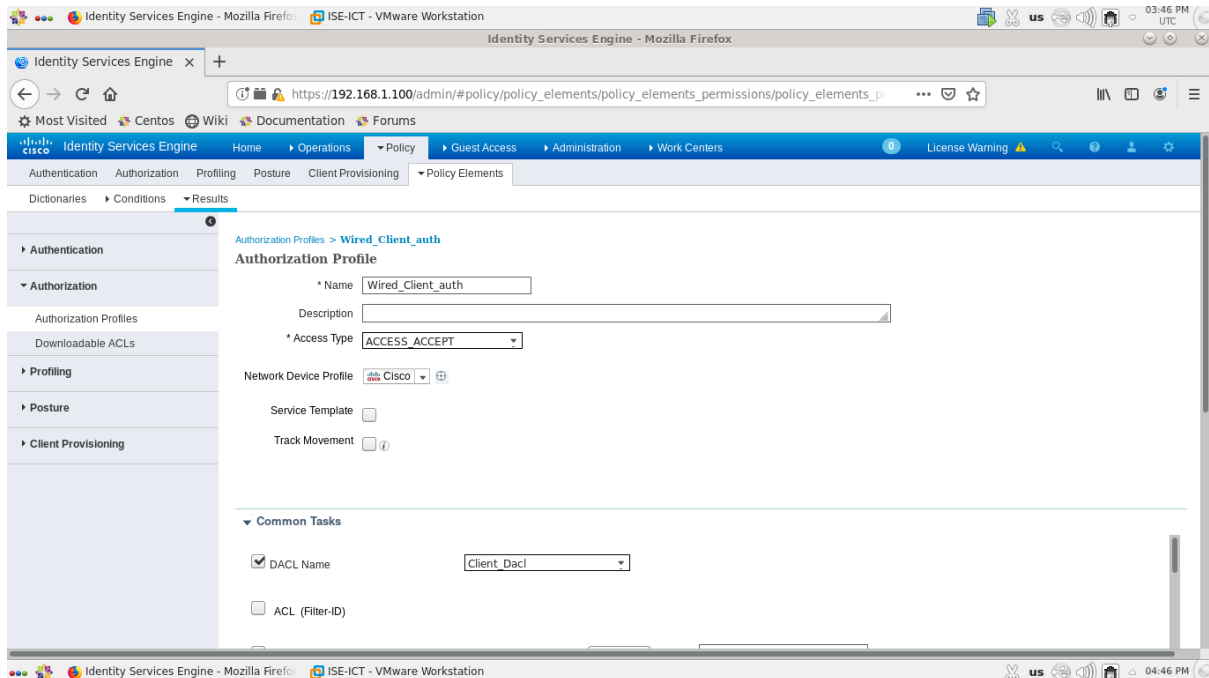


Figure 4.97 : Etape 10 de configuration des DACLs.

Etape 11. Nous avons cliqué sur **“Submit”** pour appliquer les changements.

4.4.2.2. Tests de configuration

Etape 1. Nous avons fait le test de troubleshooting pour le premier utilisateur « **Utilisateur1** » en utilisant la commande suivante :

```
sw#show access-lists
```

```
Authentificateur#  
Authentificateur#sh access-lists  
Extended IP access list Auth-Default-ACL-OPEN  
 10 permit ip any any  
Extended IP access list xACSACLx-IP-Admin_Dacl-5flef64c (per-user)  
 10 permit icmp any any  
 20 deny tcp any any  
 30 deny ip any any  
Authentificateur#  
Authentificateur#
```

Figure 4.98 : Etape 1 de test de configuration de DACLs.

Etape 2. Nous avons fait le test de troubleshooting pour le deuxième utilisateur « Utilisateur2 ».

```
Authentificateur#  
Authentificateur#show access-lists  
Extended IP access list Auth-Default-ACL-OPEN  
 10 permit ip any any  
Extended IP access list xACSACLx-IP-Client_Dacl-5flef682 (per-user)  
 10 deny tcp any any eq 22  
 20 permit ip any any  
Authentificateur#  
Authentificateur#
```

Figure 4.99 : Etape 2 de test de configuration de DACLs.

Etape 3. Nous avons vérifié le téléchargement des DACLs au niveau du serveur ISE.

| Time | Status | Det... | Repeat Co... | Identity | Endpoint ID | Endpoint Profile | Authentication Policy | Authorization Policy | Authorization Profiles | Network D |
|------------------------|--------|--------|--------------|----------------------------------|-------------------|------------------|-----------------------|------------------------|------------------------|-----------|
| 2020-07-28 15:40:05... | 🟢 | 🔒 | 0 | Utilisateur1 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Admin_... | Wired_Admin_auth | Authentic |
| 2020-07-28 15:40:05... | 🟢 | 🔒 | | #ACSACL#-IP-Admin_Dacl-5f1ef64c | | | | | | Authentic |
| 2020-07-28 15:40:05... | 🟢 | 🔒 | | Utilisateur1 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Admin_... | Wired_Admin_auth | Authentic |
| 2020-07-28 15:36:19... | 🟢 | 🔒 | | #ACSACL#-IP-Client_Dacl-5f1ef682 | | | | | | Authentic |
| 2020-07-28 15:30:28... | 🟢 | 🔒 | | Utilisateur2 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Client_R... | Wired_Client_auth | Authentic |
| 2020-07-28 15:24:49... | 🟢 | 🔒 | | Utilisateur1 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Admin_... | Wired_Admin_auth | Authentic |
| 2020-07-28 15:13:30... | 🟢 | 🔒 | | F8:BC:12:63:3C:B8 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> MAB >> ... | Default >> Default | PermitAccess | Authentic |
| 2020-07-28 15:03:53... | 🟢 | 🔒 | | Utilisateur2 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Client_R... | Wired_Client_auth | Authentic |
| 2020-07-28 14:57:14... | 🟢 | 🔒 | | Utilisateur1 | F8:BC:12:63:3C:B8 | Dell-Device | Default >> 802.1X ... | Default >> Admin_... | Wired_Admin_auth | Authentic |

Figure 4.100 : Etape 3 de test de configuration de DACLs.

Remarquez-vous que le téléchargement des DACLs a été fait avec succès.

4.4.3. Restricted / Failed VLAN & Guest VLAN

4.4.3.1. Configuration de Restricted & Guest VLAN

Ces variables dynamiques sont configurées au niveau de switch d'accès, et pour les configurer ; nous avons suivi les étapes suivantes :

Etape 1. Nous avons configuré le VLAN Restricted en utilisant les commandes suivantes :

```
!
interface gigabitEthernet 0/11
    authentication host-mode single-host
    authentication event fail retry 2 action authorize vlan 2
!
```

Etape 2. Nous avons configuré le VLAN Guest en utilisant les commandes suivantes :

```
!  
dot1x guest-vlan supplicant  
interface gigabitEthernet 0/11  
    authentication event no-response action authorize vlan 3  
    exit  
!
```

4.4.3.2. Tests de configuration

4.4.3.2.1. VLAN Restricted

Etape 1. Au niveau de client, nous avons changé la configuration du premier utilisateur « **Utilisateur1** » en entrant un faux mot de passe.

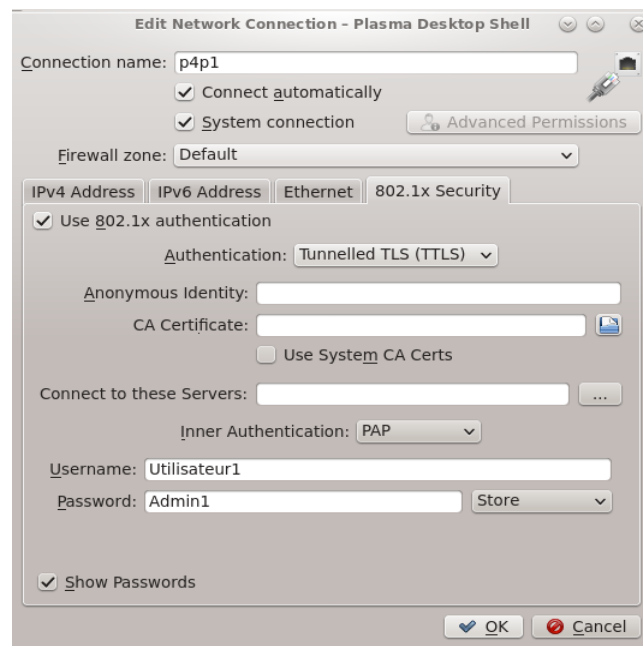


Figure 4.101 : Etape 1 de test de configuration de VLAN Restricted.

Etape 2. Au niveau de switch d'accès, nous avons désactivé et réactivé le port `gigabitEthernet 0/11`.

```

Authentificateur(config-if)#
*Mar 1 00:24:31.781: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to down
*Mar 1 00:24:34.322: %LINK-3-UPDOWN: Interface GigabitEthernet0/11, changed state to up
*Mar 1 00:24:34.423: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.473: %DOT1X-5-FAIL: Authentication failed for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.473: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.524: %DOT1X-5-FAIL: Authentication failed for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.524: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.574: %DOT1X-5-FAIL: Authentication failed for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.574: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:34.574: %AUTHMGR-5-VLANASSIGN: VLAN 2 assigned to Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:35.279: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:35.279: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client (f8bc.1263.3cb8) on Interface Gi0/11 AuditSessionID COA8010A0000000A00167746
*Mar 1 00:24:35.329: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/11, changed state to up
Authentificateur(config-if)#
Authentificateur(config-if)#

```

Figure 4.102 : Etape 2 de test de configuration de VLAN Restricted.

Etape 3. Nous avons fait le test de troubleshooting.

```

Authentificateur#sh authentication sessions interface G0/11
      Interface: GigabitEthernet0/11
      MAC Address: f8bc.1263.3cb8
      IP Address: 192.168.2.2
      User-Name: Utilisateur1
      Status: Authz Success
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Authorized By: Auth Fail Vlan
      Vlan Policy: 2
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA8010A0000000A00167746
      Acct Session ID: 0x0000000C
      Handle: 0xA900000B

Runnable methods list:
      Method      State
      dot1x      Authc Failed
      mab         Not run

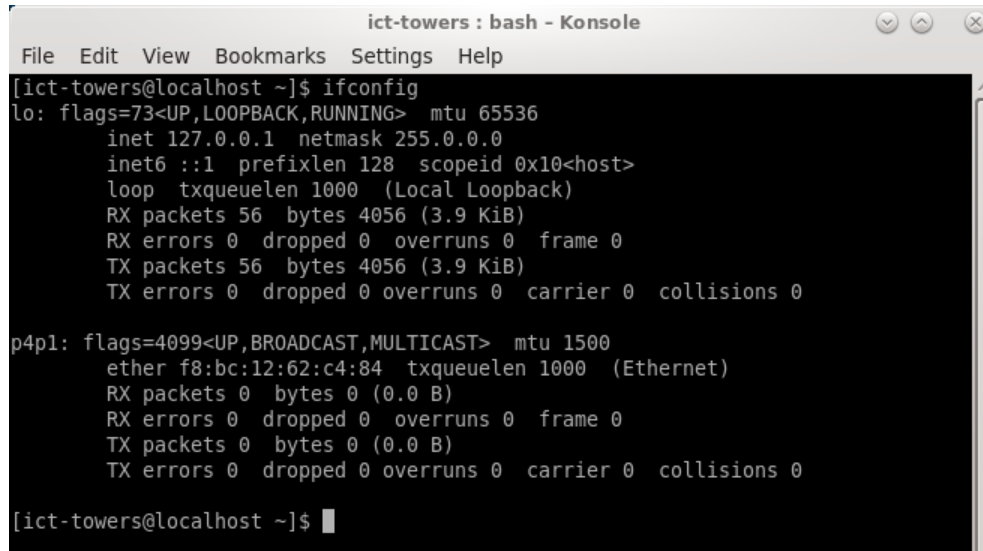
Authentificateur#

```

Figure 4.103 : Etape 3 de test de configuration de VLAN Restricted.

4.4.3.2.2. VLAN Guest

Etape 1. Nous avons changé le client pour obtenir une nouvelle adresse **MAC**.



```
ict-towers : bash - Konsole
File Edit View Bookmarks Settings Help
[ict-towers@localhost ~]$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
  inet6 ::1 prefixlen 128 scopeid 0x10<host>
  loop txqueuelen 1000 (Local Loopback)
  RX packets 56 bytes 4056 (3.9 KiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 56 bytes 4056 (3.9 KiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

p4p1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
  ether f8:bc:12:62:c4:84 txqueuelen 1000 (Ethernet)
  RX packets 0 bytes 0 (0.0 B)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 0 bytes 0 (0.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[ict-towers@localhost ~]$
```

Figure 4.104 : Etape 1 de test de configuration de VLAN Guest.

Etape 2. Nous avons désactivé la méthode d'authentification **802.1X**.

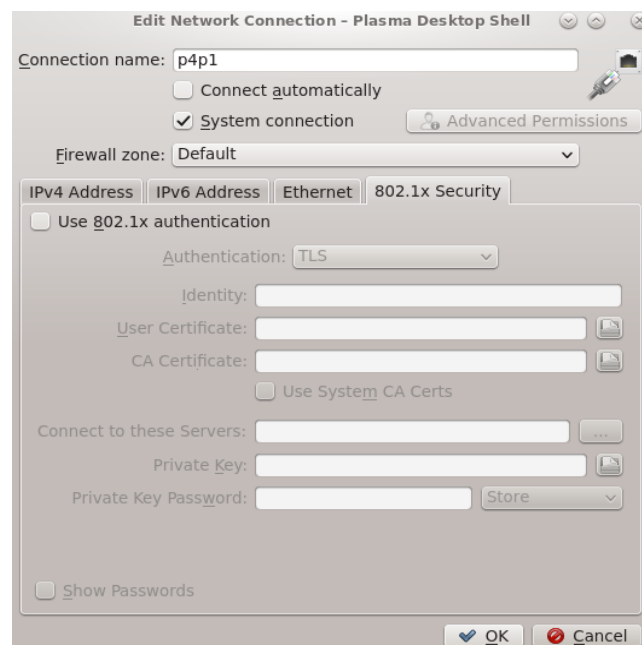


Figure 4.105 : Etape 2 de test de configuration de VLAN Guest.

Etape 3. Nous avons configuré l'adresse IPv4 du client automatiquement.

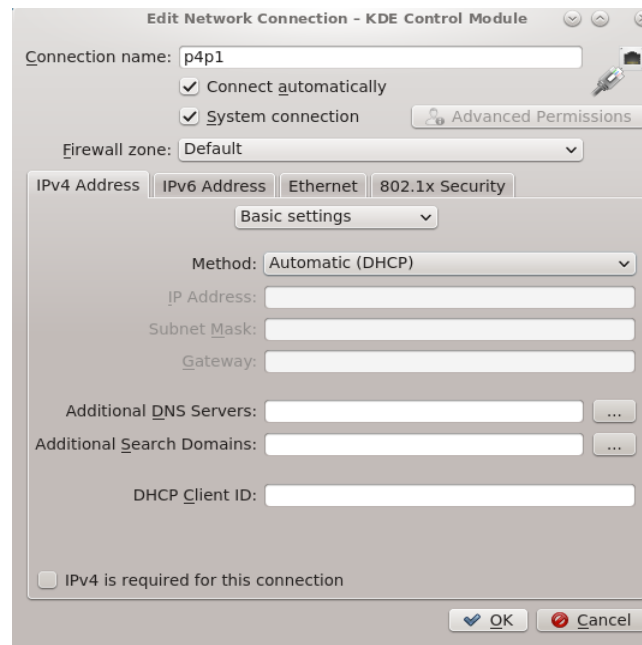


Figure 4.106 : Etape 3 de test de configuration de VLAN Guest.

Etape 4. Au niveau de switch d'accès, nous avons désactivé et réactivé le port gigabitEthernet 0/11.

```

Authentificateur#
Authentificateur#
*Mar 1 00:51:27.620: %AUTHMGR-5-START: Starting 'dot1x' for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.230: %DOT1X-5-FAIL: Authentication failed for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.230: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.230: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.230: %AUTHMGR-5-START: Starting 'mab' for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.247: %MAB-5-FAIL: Authentication failed for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.247: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'mab' for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.247: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.247: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (f8bc.1262.c484) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.247: %AUTHMGR-5-VLANASSIGN: VLAN 3 assigned to Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
*Mar 1 00:53:00.549: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (Unknown MAC) on Interface Gi0/11 AuditSessionID COA8010A00000010002E3287
Authentificateur#
Authentificateur#
Authentificateur#

```

Figure 4.107 : Etape 4 de test de configuration de VLAN Guest.

Etape 5. Nous avons fait le test de troubleshooting.

```
Authentificateur#sh authentication sessions interface G0/11
  Interface: GigabitEthernet0/11
  MAC Address: Unknown
  IP Address: 192.168.3.2
  User-Name: UNRESPONSIVE
  Status: Authz Success
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Authorized By: Guest Vlan
  Vlan Policy: 3
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: COA8010A00000010002E3287
  Acct Session ID: 0x00000012
  Handle: 0xF9000011

Runnable methods list:
  Method   State
  dot1x    Failed over
  mab      Failed over

Authentificateur#
```

Figure 4.108 : Etape 5 de test de configuration de VLAN Guest.

4.4.4. Les Timers

4.4.4.1. Configuration de timers

Les timers sont configurés au niveau de switch d'accès, et pour les configurer ; nous avons utilisé les étapes suivantes :

```
!
interface gigabitEthernet 0/11
  dot1x timeout quiet-period 10
  dot1x timeout tx-period 5
  dot1x timeout supp-timeout 5
  dot1x timeout server-timeout 5
  dot1x max-reauth-req 2
exit
!
```

4.4.4.2. Test de timers

Nous avons fait le test de trouble shooting en utilisant la commande « *show dot1x all* »

```
Authentificateur#show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3

Dot1x Info for GigabitEthernet0/11
-----
PAE                       = AUTHENTICATOR
QuietPeriod               = 10
ServerTimeout            = 5
SuppTimeout              = 5
ReAuthMax                 = 2
MaxReq                   = 2
TxPeriod                 = 5

Authentificateur#
Authentificateur#
```

Figure 4.109 : Test de timers.

4.5. Conclusion

L'implémentation du modèle AAA et de la méthode de sécurité 802.1X ainsi ses fonctionnalités et variables dynamiques montre l'utilité de ce modèle et l'importance de cette méthode de sécurité ainsi son déploiement dans tout réseau actuel.

CONCLUSION GENERALE

A cause de l'augmentation du nombre d'attaques, des méthodes de sécurité ont été développées et la gestion des accès est devenue très importante.

Pour répondre à la problématique posée dans l'introduction générale, nous avons présenté dans ce mémoire l'avantage d'utiliser le modèle AAA assurant la protection des ressources du réseau contre les attaques et la gestion inappropriée. Il permet d'authentifier les utilisateurs du réseau, de leur autoriser certains services et de collecter des informations sur l'utilisation de ressources. Ce modèle a été complété par le protocole 802.1X permettant une authentification centralisée des utilisateurs et une assurance de la dynamique et de la mobilité des accès au réseau

L'implémentation du modèle AAA et de la méthode de sécurité 802.1X a été réalisée avec succès dans un environnement réel à l'établissement ICT-TOWERS de Sidi Bel Abbès et d'Alger avec des équipements du constructeur Cisco.

Notre implémentation a commencé par la configuration du « Port-Based Authentication » puis a été complétée par la méthode d'authentification de secours MAB et a été terminée par la configuration des variables dynamiques de 802.1X permettant d'offrir une connectivité limitée aux utilisateurs du réseau.

La suite de ce travail consiste à essayer de tester ces mécanismes, étudiés théoriquement et implémentés pratiquement, dans un réseau sans fil et à les déployer dans un réseau fonctionnel.

Bibliographie

- [1] EBEL F., BAUDRU S., CROCFER R., PUCHE D., HENNECART J., LASSON S., et al. (2009). « *Sécurité informatique-Ethical Hacking-Apprendre l'attaque pour mieux se défendre* ». Editions ENI.
- [2] IPSpecialist LTD. (2018). « *CCNA Security (IINS 210-260) Technology Workbook With Practice Exam Questions* ». IPSpecialist LTD.
- [3] SANTOS O. (2020). « *CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide* ». Cisco Press.
- [4] MCMILLAN T. (2018) *CCNA security study guide exam 210-260* ». John Wiley & Sons.
- [5] CANAVAN J. E. (2001) « *Artech House telecommunications library* ». Artech House. Inc. Norwood. MA.
- [6] SADIQUI A. (2019). « *Sécurité des réseaux informatiques* ». ISTE Group.
- [7] KRAWETZ N. (2006). « *Introduction to Network Security (Networking Series)* ». Charles River Media. Inc. Rockland. MA.
- [8] WorkSmartr, "Colorful cybersecurity know what red blue and yellow mean", <https://worksmartr.com/colorful-cybersecurity-know-what-red-blue-and-yellow-mean-6a895865fd5>, page consultée le 05 avril 2020.
- [9] Massachusetts Institute of Technology, "Red Hat Enterprise Linux 4: Guide de sécurité", <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/s1-sgs-ov-controls.html>, page consultée le 04 mai 2020.
- [10] WATKINS M., WALLACE K. (2008). « *CCNA Security Official Exam Certification Guide Exam* ». Cisco Press.
- [11] SUPINFO, "Le protocole de sécurité AAA", <https://www.supinfo.com/articles/single/10150-protocole-securite-aaa>, page consultée le 16 mai 2020.

- [12] VACHON B. (2016). « *CCNA Security (210-260) Portable Command Guide (2nd Edition)* ». Cisco Press.
- [13] SlideServe, "Authentication, Authorization, and Accounting", <https://fr.slideserve.com/sorley/authentication-authorization-and-accounting>, page consultée le 01 juin 2020.
- [14] THAKUR K., PATHAN A. S. K., (2020) « *Cybersecurity Fundamentals A Real-World Perspective* ». CRC Press.
- [15] CIAMPA M. (2018). « *Comptia Security+ Guide to Network Security Fundamentals* ». Cengage Learning.
- [16] COBB C. (2004). « *Cryptography for dummies* ». John Wiley & Sons.
- [17]ANSSI, "Recommandations de sécurité relatives aux mots de passe", https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf, page consultée le 20 juillet 2020.
- [18] PILLOU J. F., BAY J. P. (2016). « *Tout sur la sécurité informatique* ». Dunod.
- [19] SANTUKA V., BANGA P., CARROLL B. J. (2010). « *AAA identity management security* ». Cisco Press.
- [20] Cisco Systems, Inc. (2019) « *Security Configuration Guide, Cisco IOS XE Gibraltar 16.11.x (Catalyst 9300 Switches)* ». Cisco Systems, Inc.
- [21] WOLAND A., HEFFNER C., REDMON K. (2015). « *CCNP security SISAS 300-208 official cert guide* ». Cisco Press.
- [22] IpCisco, "AAA PROTOCOLS RADIUS AND TACACS", <https://ipcisco.com/aaa-protocols-radius-and-tacacs/>, page consultee le 20 août 2020.
- [23] YOUM H. Y. (2009). « *Extensible authentication protocol overview and its applications* ». IEICE transactions on information and systems, 92(5). 766-776.
- [24] PRAKASH A., KUMAR U. (2018). « *Authentication protocols and techniques: a survey* ». Int. J. Comput. Sci. Eng. 6(6). 1014-1020.

[25] GEIER J. (2008). « *Implementing 802.1 X security solutions for wired and wireless networks* ». John Wiley & Sons.

[26] intel, "Présentaion de 802.1X est des types d'EAP ", <https://www.intel.fr/content/www/fr/fr/support/articles/000006999/network-and-i-o/wireless-networking.html>, page consultee le 29 août 2020.

[27] PORTER T., GOUGH M. (2007). « *How to cheat at VoIP security* ». Syngress.

[28] Llorens C., Levier L., Valois D. (2011). « *Tableaux de bord de la sécurité réseau* ». Editions Eyrolles.