



Master : Cryptologie Et Sécurité Informatique



المكتب الوطني للمطارات
Office National Des Aéroports

Aéroport d'Al Hoceima Chérif El Idrissi

Rapport De Stage



Réalisée par :

ELMNAJJA DINA

Encadré par :

M. HAOUZI BAHI Abdelmoula "Chef du service Technique Navigation"

Mlle. EZ-ZGHOULI Oumaima "Ingénieur en Electronique de la Sécurité de la Circulation Aérienne"

Année universitaire :2024/2025

TABLE DES MATIÈRES

Remercierement	9
Résumé	10
Abstract	11
Introduction	12
Partie I : Cadre Général Du Projet	15
Chapitre I : Présentation de l'organisme d'accueil	15
I. Office Nationale des aéroports	15
1. Présentation de l'ONDA	15
2. Missions de l'ONDA	15
3. Définition des Services Aériens	16
4. Activités De l'ONDA	16
5. Organigramme de l'ONDA	16
II. Pôle de la Navigation Aérienne (PNA)	17
1. Présentation du PNA	17
2. Missions du PNA	17
3. Organigramme de PNA	17
III. Aéroport Al Hoceïma - Cherif-Al-Idrissi	18
1. Présentation de l'aéroport	18
2. Organigramme de l'aéroport	18
3. Service Technique Navigation	19
IV. Service technique de la navigation aérienne	19
V. Généralités sur Les systèmes CNS	19
Conclusion	21
Chapitre II : Contexte général du Projet	22
Introduction	22
I. Contexte général du Projet	22
1. Etude de l'existant	22
2. Problématique	23
3. Objectifs du Projet	23

II. Cahier des charges	24
1. Études et réalisations préalables	24
2. Acteurs Du Projet	24
3. Contraintes techniques	24
III. Planification du projet	24
1. Diagramme des Tâches	24
2. Diagramme de GANTT	25
Conclusion	26
Chapitre II : Equipements du RINAM	28
Introduction	28
I. Composition et caractéristiques techniques	28
1. Routeur Cisco ISR4451	28
2. Switch Catalyst 3850	29
3. PC LMS	29
II. Maintenance Préventive des Équipements RINAM	30
Conclusion	30
Partie II : Etat De L'art	32
Chapitre I : Etude des Solutions de Sécurité Existant en terme du RINAM	32
Introduction	32
I. Solutions de Sécurité Existants	32
1. Solutions de Sécurité	32
2. Protocoles de Sécurité Réseau pour les Aéroports	33
3. Tableau Comparatif des Protocoles de Sécurité	35
II. Solutions de Sécurité sur le Marché pour les Aéroports	35
III. Solution Proposée	36
IV. Protocole IPsec	36
1. Fonctionnement d'IPsec	36
2. Modes de Fonctionnement	36
3. Présentation d'IPsec	37
4. Mécanismes d'Authentification et de Chiffrement d'IPsec	38
5. Intégration d'IPsec dans les protocoles de communication réseau (IPv4, IPv6)	39
6. Cas d'Utilisation Appropriés pour IPsec	39
V. Protocole SSH	40
1. Sécurité et Tunnellisation avec SSH	40
2. Fonctionnement de SSH	40
3. Utilisations Pratiques du Protocole SSH	42
4. Port de Protocole SSH	42
Conclusion	42
Partie III : Conception Et Réalisation	45
Introduction	45

Chapitre I : Conception du Système	45
I. Conception du Système	45
1. Architecture du Réseau	45
II. VPN (Virtual Private Network)	45
1. Types de VPN	46
2. VPN Site-à-Site	46
III. Techniques de Cryptage	47
1. Cryptage Symétrique	47
2. Cryptage Asymétrique	48
3. Hachage	48
Chapitre II : Réalisation et implémentation	50
I. Environnement de Test	50
1. GNS3	50
2. Wireshark	51
3. VirtualBox	52
4. Logiciel Snort	53
4.1. Définition	53
4.2. Fonctionnalités	53
4.3. Composants de Snort	53
4.4. Mode de Fonctionnement	54
4.5. Architecture de Snort	54
II. Représentation Visuelle	55
1. Scénarios de Simulation	55
III. Configuration	56
1. Configuration des Machines	56
2. Configuration des Routeurs	62
Routeur 1	62
Routeur 2	63
Routeur 3	64
Routeur 4	65
3. Configuration de l'Interface Loopback0	65
IV. Configuration de VPN-IPSec	66
1. Choix des Algorithmes de Chiffrement	66
2. Définition des Clés de Sécurité	68
3. Configuration des Politiques de Sécurité	68
4. Configuration des Interfaces Et Listes d'Accès	70
5. Utilisation d'ISPF	73
6. Tests de connectivité	74
7. Détection de Snort	75
V. Présentation Visuelle de SSH	78
1. Configuration	79
2. Configuration d'une Connexion Sécurisée avec PuTTY via SSH	83
3. Authentification via SSH	84
4. Vérification des Sessions SSH et Chiffrement	85
Conclusion	86
Conclusion	88
Bibliographie	89

TABLE DES FIGURES

1	Organigramme de l'ONDA	17
2	Organigramme du PNA	18
3	Organigramme de l'aéroport d'al Hoceima	19
4	Organisation des Tâches	25
5	Diagramme de GANTT	26
6	Cisco 4451-X ISR et leur Ports	29
7	Switch Catalyst 3850 et leur Ports	29
8	Affichage de PC LMS	30
9	Modes d'IPSec	37
10	AH	37
11	Esp	38
12	Cryptage Symétrique	47
13	Cryptage Asymétrique	48
14	Schéma de hachage	49
15	Logo du GNS3	51
16	Logo de Wireshark	51
17	Logo du VirtualBox	52
18	Logo de Snort	53
19	Schéma de simulation d'un Réseau Virtuel	55
20	Configuration de PC1	56
21	Configuration de PC2	56
22	Configuration de PC3	57
23	Configuration de PC4	57
24	Configuration de PC5	58
25	Configuration de PC6	58
26	Configuration de PC7	59
27	Configuration de PC8	59
28	Configuration de PC9	60
29	Configuration de Ununtu VM	60
30	Configuration de Linux VM	61
31	Configuration de R1	62
32	Configuration de R2	63
33	Configuration de R3	64
34	Configuration de R4	65
35	Configuration de l'Interface Loopback0	65

36	Configuration VPN-IPSec de R1	67
37	Configuration VPN-IPSec de R1	68
38	Configuration VPN-IPSec de R1	68
39	Configuration VPN-IPSec de R1	70
40	Configuration VPN-IPSEC de R2	71
41	Configuration VPN-IPSEC de R3	72
42	Configuration VPN-IPSEC de R4	73
43	Configuration d'ISPF	73
44	Configuration de ospf de R2	74
45	Configuration de ospf de R3	74
46	Configuration de ospf de R4	74
47	Ping Ubuntu vers Linux	75
48	Initialisation de Snort	75
49	Validation de Snort	76
50	Initialisation de Snort	76
51	Commencement des paquets	77
52	Affichage de la detection de Snort	78
53	Simulation de ssh	78
54	Configuration ssh de R1	79
55	Configuration des interfaces de R1	81
56	Configuration des interfaces de R2	82
57	Connexion Sécurisée avec PuTTY	83
58	Authentification ssh	84
59	Commande show run	84
60	Commande show ssh	86

LISTE DES TABLEAUX

1	Comparaison entre les protocoles de Sécurité	35
---	--	----



REMERCIEREMENT

Je commence par exprimer ma profonde gratitude envers Dieu, le tout-puissant, le Très-Haut, pour Ses innombrables bénédictions. Sans Son soutien, rien n'aurait été possible.

Je tiens à exprimer ma profonde gratitude à mes parents pour leur soutien indéfectible et leurs encouragements constants tout au long de ce projet. Leur amour et leur confiance en moi ont été des sources inestimables de motivation.

Je remercie également chaleureusement M. Haouzi Bahi Abdelmoula, Chef du Service Technique Navigation, pour sa précieuse assistance et son expertise qui ont grandement contribué à la réalisation de ce projet. Sa disponibilité et ses conseils ont été essentiels.

Un grand merci à Mlle. Ez-Zghouli Oumaima, Ingénieur en Électronique de la Sécurité de la Circulation Aérienne, pour son aide technique et son soutien moral. Sa collaboration et son professionnalisme ont été déterminants dans l'avancement de ce projet.

Je souhaite également adresser mes remerciements à toutes les personnes qui ont contribué, que ce soit par leur reconnaissance ou leur soutien moral. Votre aide a été précieuse et je vous en suis profondément reconnaissant.



RÉSUMÉ

Mon stage s'est déroulé au sein de l'Office National Des Aéroports (ONDA), où j'ai travaillé sur la sécurité du Réseau IP de la Navigation Aérienne Marocaine (RINAM). Ce réseau est essentiel pour assurer les communications et la transmission des données liées à la gestion du trafic aérien.

L'objectif principal de ce projet était de renforcer la sécurité du RINAM en proposant et en mettant en œuvre des solutions de sécurité adaptées. Cela a inclus une analyse approfondie de l'architecture du réseau, la détection des vulnérabilités, et l'application de mesures de sécurité, telles que la mise en place du protocole IPsec VPN pour sécuriser la communication entre différentes machines virtuelles, ainsi que l'utilisation du protocole SSH pour renforcer la sécurité des accès distants aux équipements réseau.

À travers ce projet, j'ai pu proposer des améliorations pour garantir la résilience du réseau face aux cybermenaces et assurer la continuité des services de navigation aérienne, tout en respectant les normes internationales en matière de sécurité aéroportuaire.



ABSTRACT

My internship took place at the Office National Des Aéroports (ONDA), where I worked on securing the Moroccan Air Navigation IP Network (RINAM). This network is essential for ensuring communications and data transmission related to air traffic management.

The main objective of this project was to strengthen the security of the RINAM by proposing and implementing appropriate security solutions. This included an in-depth analysis of the network architecture, the detection of vulnerabilities, and the application of security measures such as implementing the IPsec VPN protocol to secure communication between different virtual machines, as well as using the SSH protocol to enhance the security of remote access to network equipment.

Through this project, I was able to propose improvements to ensure the network's resilience against cyber threats and to maintain the continuity of air navigation services, while adhering to international airport security standards.



INTRODUCTION

Dans le contexte aéroportuaire, la sécurité des réseaux de communication est primordiale pour garantir le bon déroulement des opérations aériennes et la sécurité des passagers. Le Réseau IP de la Navigation Aérienne Marocaine (RINAM) joue un rôle central dans cette infrastructure critique.

En tant qu'élément clé du système de navigation aérienne au Maroc, le RINAM est chargé de transporter des données IP et Transporter des données IP, notamment le trafic IP des radars et des divisions télécoms. Il assure également la sauvegarde de l'architecture VPN-IAM de la division de traitement de l'information et établit des connexions essentielles avec divers sites partenaires, tant locaux qu'internationaux.

La sécurité de ce réseau est vitale pour préserver l'intégrité des données de navigation aérienne, assurer une communication fluide entre les différentes parties prenantes, et protéger contre les cybermenaces qui pourraient compromettre les opérations aériennes. Dans ce cadre, les défis en matière de cybersécurité sont considérables, et il est impératif de mettre en place des mesures robustes pour prévenir les attaques et les intrusions.

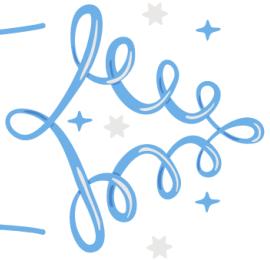


OBJECTIF

L'objectif principal de ce projet est de renforcer la sécurité du réseau complexe en identifiant les vulnérabilités potentielles et en évaluant les mesures nécessaires pour protéger l'intégrité des données et des communications. Je vise à proposer des solutions efficaces pour assurer la résilience du RINAM face aux menaces, tout en garantissant la continuité et la fiabilité des services de navigation aérienne essentiels au bon fonctionnement de l'aéroport.

À cette fin, j'ai défini deux objectifs spécifiques : d'une part, déployer le protocole IPsec VPN entre les deux VMs, Linux et Ubuntu, afin de sécuriser leur communication ; et d'autre part, implémenter le protocole SSH sur un routeur dans une autre simulation pour garantir la sécurité à distance. Ces mesures permettront d'améliorer la protection des échanges de données et de renforcer les mécanismes de sécurité dans le réseau.





Partie I

Cadre Général Du Projet

CHAPITRE I : PRÉSENTATION DE L'ORGANISME D'ACUEIL

Introduction

Je vais aborder une approche générale sur le sujet de mon stage afin de situer le contexte du projet. Tout d'abord, je décrirai l'environnement d'accueil. Ensuite, je présenterai le cahier des charges et l'architecture du système étudié, et j'établirai une planification des tâches.

I. Office Nationale des aéroports

1. Présentation de l'ONDA



L'Office National des Aéroports (O.N.D.A) est un établissement semi-public doté de la personnalité morale et de l'autonomie financière. Il est placé sous la tutelle technique du ministère du Transport et de la Logistique.

Créé en 1979 sous le nom de l'Office des Aéroports de Casa (OAC), cet organisme a été établi pour répondre aux nouveaux besoins d'exploitation et de gestion, en tenant compte de la complexité des équipements techniques et des innovations dans le secteur aéronautique. La publication de la loi 14-89 a conduit à la transformation de l'OAC en Office National des Aéroports.

2. Missions de l'ONDA

Les missions de l'ONDA sont regroupées en 4 axes :

- La garantie de la sécurité de la navigation aérienne au niveau des aéroports et de l'espace aérien, sous juridiction nationale.

-
- L'aménagement, l'exploitation, l'entretien et le développement des aéroports civils de l'État. L'embarquement, le débarquement, le transit et l'acheminement à terre des voyageurs, des marchandises et du courrier transportés par air, ainsi que tout service destiné à la satisfaction des besoins des usagers et du public.
 - La liaison avec les organismes et les aéroports internationaux afin de répondre aux besoins du trafic aérien.
 - La formation d'ingénieurs de l'aéronautique civile, de contrôleurs et d'électroniciens de la sécurité aérienne.

3. Définition des Services Aériens

L'OACI ('Organisation de l'Aviation Civile Internationale) a défini en 1952 les services aériens réguliers internationaux comme étant une série de vols possédant chacune les caractéristiques suivantes :

- les vols s'accomplissent à travers l'espace aérien de plus d'un État (transport de passagers, de courrier ou de marchandises) ;
- les vols sont accessibles au public ;
- les vols sont assurés suivant un horaire publié et avec une régularité et une fréquence telle que cette suite constitue une série systématique de vols.

Les services de transport aérien non réguliers ne font pas l'objet d'une définition propre et s'entendent par conséquent tous les services de transport aérien ne relevant pas de la définition des vols réguliers.

4. Activités De l'ONDA

Les activités de l'ONDA consistent en deux types :

- Les activités aéronautiques représentant l'essentiel des recettes sous forme de redevances de diverses natures ayant comme sous-jacent commun le trafic aéroportuaire et de survol de manière extensive (passagers, avions...) ;
- Les activités extra-aéronautiques générant des recettes de nature concessionnelles.

5. Organigramme de l'ONDA

L'organigramme de l'ONDA se compose de plusieurs directions, toutes encadrées par la direction générale des Aéroports Nationaux afin de décentraliser les pouvoirs et les services.

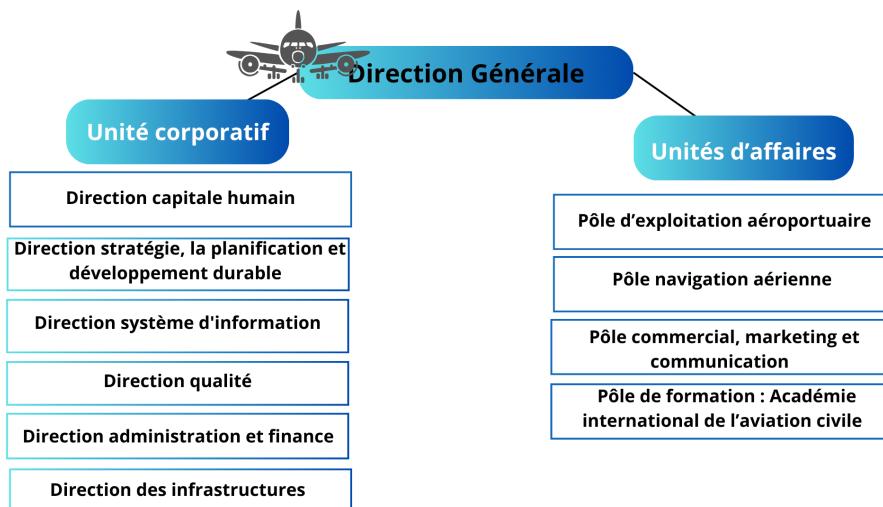


FIGURE 1 – Organigramme de l'ONDA

II. Pôle de la Navigation Aérienne (PNA)

1. Présentation du PNA

Le Pôle de la Navigation Aérienne (PNA) est une entité spécialisée au sein de l'ONDA, chargée de la gestion et de la supervision des activités liées à la navigation aérienne. Il assure la sécurité, la régulation et le contrôle du trafic aérien, en coordination avec les infrastructures aéroportuaires et les services de météorologie.

2. Missions du PNA

Le Pôle de la Navigation Aérienne a pour missions :

- Assurer la sécurité et la régularité du trafic aérien,
- Définir et mettre en œuvre le dispositif de navigation aérienne de l'Office, répondant aux exigences de sécurité et de service de tous les usagers aériens (aviation commerciale, aviation générale, aviation militaire),
- Fournir un soutien permanent aux entités opérationnelles de la Navigation Aérienne par le biais de procédures et de normes de contrôle aérien, ainsi que d'autres moyens appropriés.

3. Organigramme de PNA

La figure suivante représente l'organigramme du PNA :

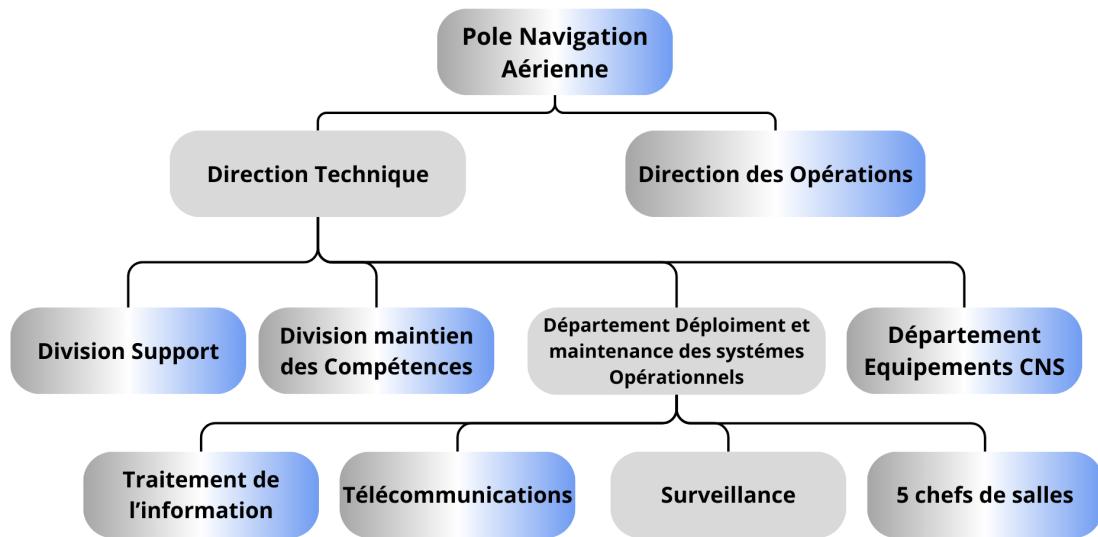


FIGURE 2 – Organigramme du PNA

III. Aéroport Al Hoceïma - Cherif-Al-Idrissi

1. Présentation de l'aéroport

L'aéroport Al Hoceima - Cherif Al Idrissi est un aéroport international situé à 17 km au sud de la ville d'Al Hoceima, dans le nord du Maroc. Il est géré par l'Office National des Aéroports (ONDA) et dispose de deux terminaux, capables d'accueillir jusqu'à 300 000 passagers par an. Ses équipements de radionavigation comprennent des systèmes VOR, DME, et NDB. L'aéroport occupe une place importante dans la région, facilitant le transport aérien pour les habitants et les touristes.

2. Organigramme de l'aéroport

L'organigramme de l'aéroport Al Hoceima - Cherif Al Idrissi est organisé sous la supervision directe du Commandant. Le Commandant est responsable de plusieurs services clés, comme illustré dans l'image :

- Service Exploitation Aéroportuaire
- Service Technique Navigation, en lien avec la section Entretien des infrastructures, de l'électricité et de l'électromécanique.
- Service Gestion de la Sécurité, Sécurité, Qualité & Environnement, en lien avec la section Sécurité.
- Service Navigation Aérienne

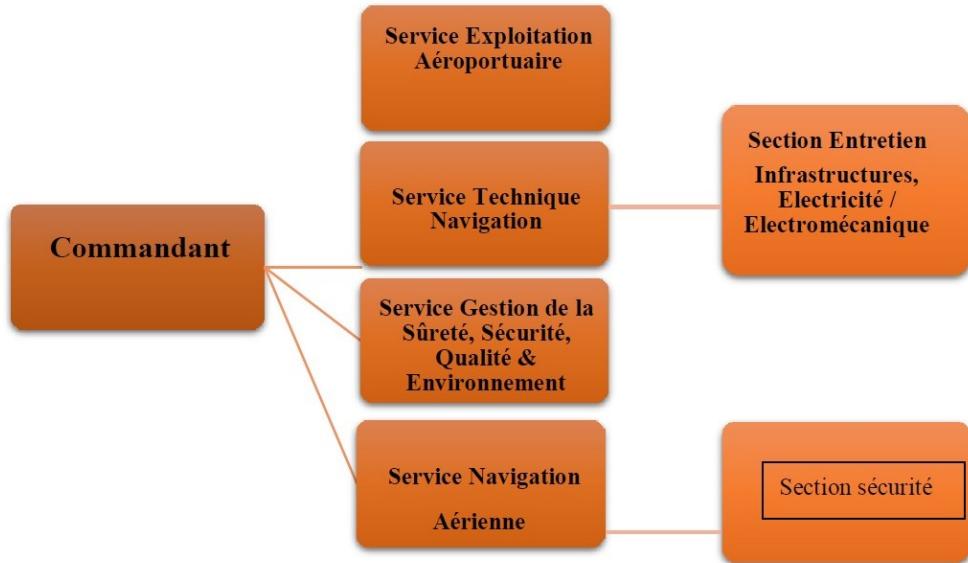


FIGURE 3 – Organigramme de l'aéroport d'al Hoceima

3. Service Technique Navigation

Le Service Technique Navigation est un service central à l'aéroport, chargé de la gestion des infrastructures techniques et des systèmes de radionavigation. En collaboration avec la Section Entretien Infrastructures, Électricité/Electromécanique, ce service assure le bon fonctionnement des équipements essentiels à la navigation aérienne tels que le VOR, DME et NDB.

IV. Service technique de la navigation aérienne

J'ai effectué mon stage au sein du service technique navigation et plus précisément dans la section Electronique de la sécurité aérienne, qui assume les fonctions suivantes :

- **Maintenance des Équipements** : Supervision et maintenance des systèmes de navigation aérienne, comme les radars, les balises, et les systèmes de communication.
- **Développement Technologique** : Recherche et mise en œuvre de nouvelles technologies pour améliorer la sécurité et l'efficacité du trafic aérien.
- **Ingénierie et Infrastructure** : Conception, construction et entretien des infrastructures nécessaires à la navigation aérienne.
- **Support Technique** : Assistance technique aux contrôleurs aériens et autres personnels opérationnels pour garantir le bon fonctionnement des systèmes de navigation.

V. Généralités sur Les systèmes CNS

Les systèmes CNS (Communication, Navigation, Surveillance) sont essentiels pour assurer la sécurité et l'efficacité des opérations aériennes.

C : Communication

Le service de communication englobe les radiocommunications et télécommunications, telles que l'ATN (Aeronautical Telecommunications Network), qui regroupe les communications VHF-UHF, les liaisons réseau entre centres de contrôle, et les échanges de données de gestion du trafic aérien.

Le Voice Communication System (VCS) est un système crucial pour la gestion des communications ATC (Air Traffic Control). Basé sur la technologie Voice-over-IP, il assure une interconnexion efficace entre divers systèmes de communication, y compris les radios UHF et VHF, les téléphones et les interphones. Le VCS comprend plusieurs éléments, dont :

- Le poste opérateur, qui constitue l'interface Homme/Machine,
- Le système radio, incluant les serveurs de commutation et les sous-systèmes d'interface radio,
- La chaîne téléphonique et la chaîne radio,
- Un système de supervision pour la maintenance et la configuration.

N : Navigation

Les systèmes de radionavigation comprennent des installations telles que l'ILS (Instrument Landing System), le VOR (VHF Omnidirectional Range) et le DME (Distance Measuring Equipment), qui sont essentiels pour la navigation aérienne :

- **VOR** : Système de positionnement radioélectrique utilisant les fréquences VHF, qui aide les aéronefs à se positionner en naviguant autour des balises VOR.
- **DME** : Permet de mesurer la distance entre un aéronef et une balise au sol en chronométrant le temps nécessaire à un signal radioélectrique pour faire le trajet aller-retour.
- **ILS** : Système d'atterrissement aux instruments qui offre une approche de précision. Il comprend un Localizer (LOC) pour déterminer l'écart de l'avion par rapport à l'axe de la piste et un Glide Path pour l'écart par rapport à la pente d'approche.

S : Surveillance

Les systèmes de surveillance sont cruciaux pour permettre aux contrôleurs aériens de connaître la localisation des aéronefs, ce qui est indispensable pour la gestion du trafic aérien. Ils incluent :

- **Radars Primaires** : Fonctionnent sur le principe de la réflexion des ondes radioélectriques par les aéronefs pour les localiser, sans besoin d'équipement à bord.
- **Radars Secondaires** : Composés d'un interrogateur au sol et d'un transpondeur à bord de l'aéronef, permettant l'échange de réponses pour la localisation précise des aéronefs.

À l'aéroport d'Al Hoceima, où je réalise mon stage, il existe uniquement les systèmes de communication et de navigation. Ces systèmes jouent un rôle crucial en permettant des communications claires et fiables entre les pilotes et les contrôleurs aériens, ainsi qu'en facilitant la navigation précise des aéronefs dans l'espace aérien.

L'absence de système de surveillance signifie qu'il est encore plus important d'optimiser et de maintenir les systèmes de communication et de navigation pour garantir la sécurité et l'efficacité des opérations aériennes à l'aéroport.

Conclusion

En conclusion, cette section a permis de poser les bases nécessaires pour bien comprendre le contexte dans lequel s'inscrit le projet de stage. En présentant l'Office National des Aéroports (ONDA) et ses missions, ainsi que les différentes entités et services impliqués dans la navigation aérienne au Maroc, notamment à l'aéroport d'Al Hoceima, j'ai pu mettre en lumière l'importance cruciale des systèmes de communication et de navigation dans le bon fonctionnement des opérations aériennes. Ce cadre général constitue une fondation solide pour la suite du projet, qui se concentrera sur l'analyse des systèmes existants, la formulation du cahier des charges, et la planification des tâches à réaliser.

CHAPITRE II : CONTEXTE GÉNÉRAL DU PROJET

Introduction

Pendant mon stage, j'ai eu l'opportunité d'explorer et d'analyser le fonctionnement de l'architecture du RINAM (Réseau IP de la Navigation Aérienne Marocaine) au sein de l'aéroport. Cette étude m'a permis de comprendre en profondeur comment ce réseau opère dans un environnement aéroportuaire. J'ai ensuite travaillé sur **l'étude et la mise en œuvre de solutions de sécurité du RINAM**, visant à renforcer la protection et l'intégrité du réseau dans ce contexte spécifique.

I. Contexte général du Projet

1. Etude de l'existant

La sécurité, dans le contexte des systèmes d'information et des réseaux, se réfère à l'ensemble des mesures, pratiques et technologies mises en place pour protéger les informations et les infrastructures contre les risques de perte, de vol, d'accès non autorisé, de modification ou de destruction. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des données, ainsi que la continuité des services et la résilience face aux menaces et aux attaques.

L'application des solutions de sécurité sur le réseau RINAM est essentielle pour renforcer la protection du réseau et garantir la sécurité des opérations aériennes, il est impératif d'implémenter des mesures de sécurité robustes pour protéger ce réseau contre les menaces potentielles.

1.1. RINAM

RINAM (le Réseau IP de la Navigation Aérienne Marocaine) est un réseau essentiel pour la sécurité de la navigation aérienne. Le réseau IP de l'ONDA permet une communication fluide entre les tours de contrôle, les avions et les systèmes de gestion du trafic aérien. Cette communication est cruciale pour coordonner les vols, éviter les collisions et gérer les situations d'urgence de manière efficace.

Le RINAM est principalement utilisé pour transmettre les informations radar aux destinations nécessaires et fournir un service de liaison longue distance aux systèmes

de navigation aérienne. Avant son extension, le réseau IP national de l'ONDA, qui partageait les données radar, les données de vol et les communications vocales pour la navigation aérienne, se composait d'un réseau fédérateur et d'un réseau d'accès.

2. Problématique

La problématique principale est la suivante :

Comment renforcer la sécurité du RINAM pour protéger les informations critiques de navigation aérienne contre les cyberattaques, tout en assurant une communication efficace et ininterrompue entre les différents acteurs de la gestion du trafic aérien ?

Cette question soulève plusieurs défis spécifiques, liés aux points faibles identifiés dans la sécurité du réseau RINAM :

- **Protection des Données Sensibles** : Les informations critiques telles que les données radar et les communications vocales doivent être protégées contre les risques d'interception et de falsification. L'absence de mesures de chiffrement adéquates pourrait exposer ces données sensibles à des cyberattaques, compromettant ainsi la sécurité des opérations aériennes.
- **Prévention des Attaques par Déni de Service (DoS)** : Le réseau pourrait être vulnérable aux attaques par déni de service, qui visent à saturer les ressources du système et à perturber les communications et les opérations de contrôle du trafic aérien. La capacité à détecter et à atténuer ces attaques est cruciale pour maintenir la continuité des services.
- **Robustesse des Protocoles de Sécurité** : La mise en place de protocoles de sécurité robustes est essentielle pour garantir l'intégrité et la confidentialité des données échangées sur le réseau. Des protocoles insuffisamment sécurisés peuvent créer des failles exploitables par des attaquants pour accéder aux informations critiques.
- **Gestion des Accès et des Identités** : Il est crucial de mettre en œuvre une gestion efficace des accès et des identités pour garantir que seules les personnes autorisées puissent accéder aux informations et aux systèmes critiques. Une gestion des identités défaillante peut conduire à des accès non autorisés et à des compromissions de la sécurité.
- **Surveillance et Réponse aux Incidents** : La surveillance continue du réseau et une réponse rapide aux incidents de sécurité sont nécessaires pour minimiser l'impact des attaques potentielles. L'absence de mécanismes de détection et de réponse efficaces peut retarder la réaction face aux menaces, augmentant ainsi les risques pour la sécurité du réseau.

Aborder ces défis est essentiel pour garantir non seulement la sécurité et la résilience du RINAM, mais également la sécurité globale de la navigation aérienne marocaine. En traitant ces vulnérabilités, le projet vise à établir une infrastructure de communication sécurisée et fiable pour la gestion du trafic aérien.

3. Objectifs du Projet

Analyse des Systèmes Actuels

- Étudier les solutions de sécurité en place au sein du RINAM.

-
- Identifier les vulnérabilités et les points faibles de ces systèmes pour comprendre les besoins spécifiques de sécurité.

Implémentation des Solutions de Sécurité

- **Application du protocole VPN IPsec :** Mise en place du protocole IPsec pour sécuriser la communication entre les machines virtuelles (VM) Linux et Ubuntu. Cette configuration assure que les données échangées entre ces VMs sont protégées contre les interceptions et les modifications.
- **Configuration de SSH pour la sécurité à distance :** Implémentation du protocole SSH sur un routeur dans une autre simulation pour permettre une gestion sécurisée à distance. Cette configuration assure une connexion sécurisée et authentifiée pour l'administration des équipements réseau.

II. Cahier des charges

1. Études et Réalisations Préalables

Le présent cahier des charges a pour objectif l'implémentation de solutions de sécurité adaptées au RINAM. Le projet débutera par une étude approfondie des outils de sécurité existants afin d'identifier leurs défaillances et de proposer des améliorations. L'analyse des besoins vise à préciser les objectifs de sécurité à atteindre et à clarifier les attentes pour affiner le périmètre du projet.

2. Acteurs Du Projet

- **Maitre d'ouvrage :** est l'Aeroport Cherif Al Idrissi représenté par :

M. HAOUZI BAHI Abdelmoula "Chef du service Technique Navigation"

Mlle. EZ-ZGHOULI Oumaima "Ingénieur en Electronique de la Sécurité de la Circulation Aérienne"

- **Maitre d'œuvre :** est la faculté des sciences et techniques d'Al hoceima représentée par un élève "première année master de cryptologie et sécurité informatique" :

Mlle. ELMNAJJA Dina.

3. Contraintes Techniques

III. Planification du projet

mon Projet de Stage s'étale sur une période de 1 mois (8/08 - 6/09), et pour garantir son avancement et sa réussite, une planification des tâches rigoureuses, soignée et réaliste est nécessaire. Le tableau ci-dessous représente

1. Diagramme des Tâches

J'ai découpé le projet en 5 tâches Principales, chacune étant décomposée en sous-tâches.



Nom de la tâche	Durée	Début	Fin	
Identification du projet à réaliser	<ul style="list-style-type: none"> Présentation du projet par l'encadrant Déterminer les objectifs du projet Identification et analyse de la problématique Élaboration du cahier des charges 	<ul style="list-style-type: none"> 7 jours 2 jours 2 jours 2 jours 1 jours 	<ul style="list-style-type: none"> 8 Août 2024 8 Août 2024 10 Août 2024 12 Août 2024 14 Août 2024 	<ul style="list-style-type: none"> 15 Août 2024 10 Août 2024 12 Août 2024 14 Août 2024 15 Août 2024
Étude fonctionnelle du projet	<ul style="list-style-type: none"> Spécifications des besoins fonctionnelles Spécifications des modules de base 	<ul style="list-style-type: none"> 5 jours 3 jours 2 jours 	<ul style="list-style-type: none"> 16 Août 2024 16 Août 2024 19 Août 2024 	<ul style="list-style-type: none"> 21 Août 2024 19 Août 2024 21 Août 2024
Étude technique du projet	<ul style="list-style-type: none"> Étudier les différents protocoles disponibles. Définir des critères de sélection basés sur les besoins spécifiques du RINAM Sélectionner un ensemble de protocoles qui répondent le mieux aux critères définis. 	<ul style="list-style-type: none"> 5 jours 1 jours 2 jours 2 jours 	<ul style="list-style-type: none"> 21 Août 2024 21 Août 2024 22 Août 2024 24 Août 2024 	<ul style="list-style-type: none"> 26 Août 2024 22 Août 2024 24 Août 2024 26 Août 2024
L'implémentation et le Test	<ul style="list-style-type: none"> Créer un modèle du réseau RINAM dans GNS3, incluant les différents composants et topologies du réseau de l'aéroport. Implémenter les protocoles de sécurité sélectionnés dans l'environnement simulé. Conduire une série de tests pour évaluer la performance des protocoles 	<ul style="list-style-type: none"> 5 jours 1 jours 2 jours 2 jours 	<ul style="list-style-type: none"> 26 Août 2024 26 Août 2024 27 Août 2024 29 Août 2024 	<ul style="list-style-type: none"> 31 Août 2024 27 Août 2024 29 Août 2024 31 Août 2024
Préparation de la soutenance	<ul style="list-style-type: none"> Rédaction du rapport de stage Préparation de la présentation finale 	<ul style="list-style-type: none"> 33 jours 31 jours 2 jours 	<ul style="list-style-type: none"> 8 Août 2024 8 Août 2024 1 Septembre 2024 	<ul style="list-style-type: none"> 3 Septembre 2024 1 Septembre 2024 3 Septembre 2024

FIGURE 4 – Organisation des Tâches

2. Diagramme de GANTT



Le diagramme de Gant en gestion de projet et en ordonnancement. C'est un outil efficace pour représenter visuellement l'état d'avancement et la succession des différentes activités (tâches ou opérations) qui constituent un ordonnancement ou la gestion d'un projet.

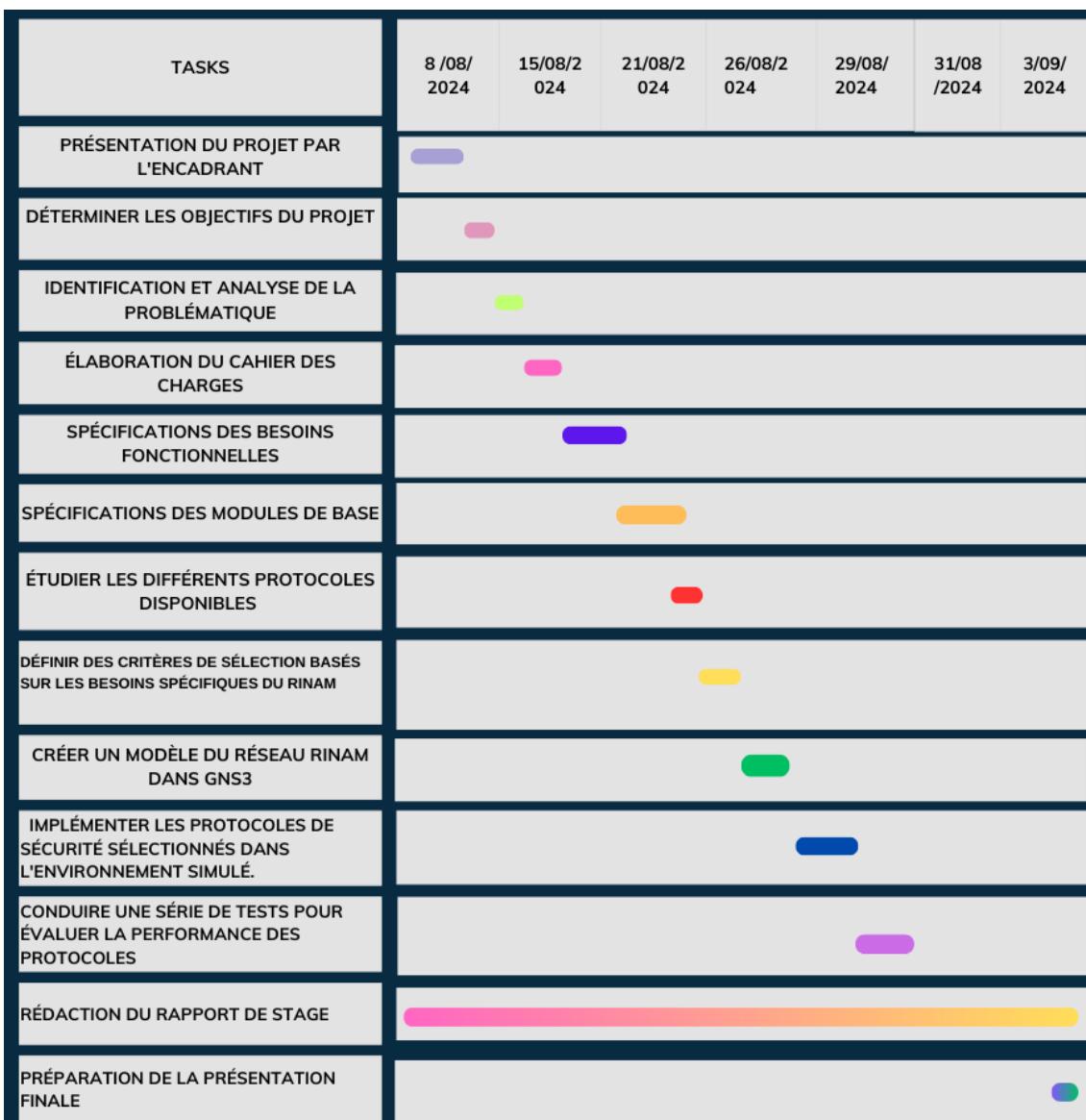
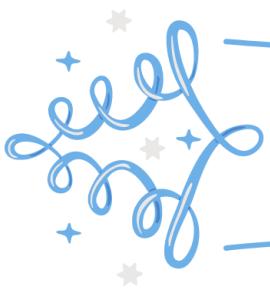


FIGURE 5 – Diagramme de GANTT

Conclusion

L'étude approfondie de l'architecture et des mécanismes de sécurité du RINAM (Réseau IP de la Navigation Aérienne Marocaine) a mis en lumière l'importance cruciale de ce réseau pour la sécurité et la coordination du trafic aérien au sein de l'aéroport. Le projet, centré sur le renforcement de la sécurité du RINAM, a permis d'identifier des vulnérabilités clés nécessitant des solutions adaptées pour protéger les informations critiques et garantir une communication fiable et sécurisée. L'analyse des systèmes existants, la définition des objectifs de sécurité, ainsi que la planification rigoureuse des tâches sont des étapes déterminantes pour la réussite de ce projet, qui vise à établir une infrastructure de communication résiliente et conforme aux normes internationales de sécurité aéronautique.



Partie II

Etat De L'art

CHAPITRE I : EQUIPEMENTS DU RINAM

Introduction

Dans le cadre de mon projet d'étude et d'implémentation des solutions de sécurité pour le RINAM (Réseau IP de la Navigation Aérienne Marocaine), l'objectif principal est de comprendre l'architecture du RINAM et d'implémenter des solutions de sécurité adaptées. Le réseau IP National de l'ONDA (Office National Des Aéroports) est conçu pour couvrir toutes les plateformes et services de la Navigation aérienne, en utilisant un mécanisme de tunnel (généralement MPLS). Ce réseau permet l'interconnexion de LAN situés sur différents sites et plateformes, qui apparaissent comme un seul LAN Ethernet. À l'aéroport d'Al Hoceima, la liaison IP est assurée avec le CRCNSA Casablanca via :

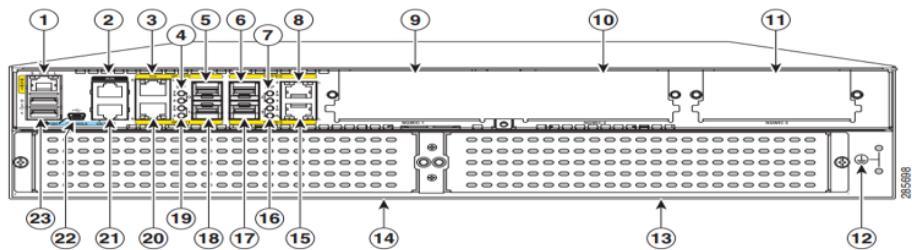
- 4 liaisons E&M
- 1 liaison FXS
- 1 liaison E1

I. Composition et caractéristiques techniques

1. Routeur Cisco ISR4451

Le routeur Cisco 4451-X ISR est un élément clé de l'infrastructure. Il est équipé de deux blocs d'alimentation et prend en charge les modules suivants :

- Modules d'interface réseau (NIM)
- Modules de service (SM-X, comme SM-X-1T3/E3)
- Modules serveur de la série E

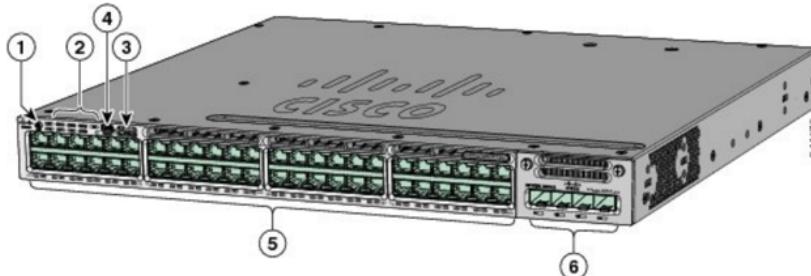


1	GE 0 management port	2	Auxiliary port
3	RJ-45 Gigabit Ethernet port (GE 0/0/0)	4	LEDs for the GE 0/0/0 interface (See Table 1-1 for detailed LED information)
5	SFP/Gigabit Ethernet port (GE 0/0/0)	6	SFP/Gigabit Ethernet port (GE 0/0/2)
7	LEDs for the GE 0/0/2 interface	8	RJ-45 Gigabit Ethernet port (GE 0/0/2)
9	NIM slot 1 (shown with slot divider removed).	10	NIM slot 2 (shown with slot divider removed).
11	NIM slot 3	12	Ground connection
13	Enhanced Service Module (SM-X) 2	14	Enhanced Service Module (SM-X) 1
15	RJ-45 Gigabit Ethernet port GE 0/0/3	16	LEDs for the GE 0/0/3 interface
17	SFP/Gigabit Ethernet GE 0/0/3	18	SFP Gigabit Ethernet GE 0/0/1
19	LEDs for the GE 0/0/1 interface	20	RJ-45 Gigabit Ethernet port GE 0/0/1
21	Serial console port	22	USB Type B mini port
23	USB 0 and USB 1		

FIGURE 6 – Cisco 4451-X ISR et leur Ports

2. Switch Catalyst 3850

Le Switch Catalyst 3850 est utilisé pour gérer et sécuriser les communications au sein du réseau.



1	Mode button	4	USB mini-Type B (console) port
2	Status LEDs	5	10/100/1000 PoE+ ports
3	USB Type A storage port	6	Network module

FIGURE 7 – Switch Catalyst 3850 et leur Ports

3. PC LMS

La configuration matérielle et logicielle minimale requise pour l'agent PC LMS est la suivante :

- Processeur : Processeur double cœur 2 GHz ou plus rapide
- RAM : 4 Go

- Espace disque dur : 500 Go
- Carte graphique et écran : 1400 x 900 pixels
- Système d'exploitation : CentOS Linux v7

Le logiciel NetArt ATC permet de surveiller la disponibilité des périphériques réseau Cisco, incluant leurs interfaces IP, ports voix, alimentations, et ventilateurs. Il fournit une vue d'ensemble de l'état des canaux de communication de bout en bout via une console Web intuitive. En cas de dysfonctionnement, il identifie l'appareil défaillant, facilitant ainsi l'intervention de l'équipe de maintenance.

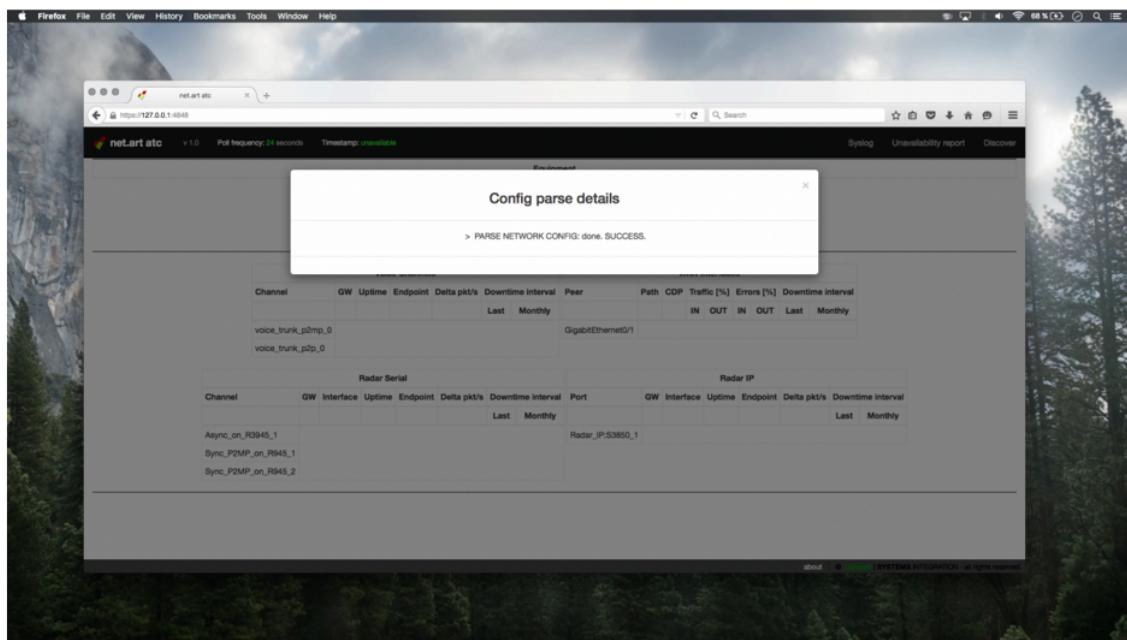


FIGURE 8 – Affichage de PC LMS

II. Maintenance Préventive des Équipements RINAM

La maintenance préventive, essentielle pour assurer la sécurité et la fiabilité du système, comprend :

- Vérification régulière du fonctionnement de l'application.
- Contrôle visuel des équipements clés comme le Routeur Cisco 4451 ISR et le Switch Catalyst 3850, incluant la vérification des ports, voyants, alimentation, et ventilateur.

Conclusion

Le projet d'étude et d'implémentation des solutions de sécurité pour le RINAM (Réseau IP de la Navigation Aérienne Marocaine) m'a permis de comprendre en profondeur l'architecture complexe de ce réseau critique. L'analyse des équipements, tels que le routeur Cisco ISR4451 et le switch Catalyst 3850, a révélé l'importance d'une infrastructure robuste et sécurisée pour assurer la continuité des services de navigation aérienne.

La mise en place de mesures de sécurité adaptées, associée à une maintenance préventive rigoureuse, est essentielle pour garantir la fiabilité et la sécurité du RINAM. Ces efforts sont primordiaux pour prévenir les interruptions de service et assurer une communication fluide entre les différentes plateformes aéroportuaires.

À travers cette étude, j'ai pu non seulement acquérir des compétences techniques spécifiques, mais aussi comprendre l'importance stratégique de la sécurité des réseaux dans le domaine de la navigation aérienne. Ce projet constitue une étape clé dans mon parcours professionnel, et les connaissances acquises me serviront dans mes futures contributions à la sécurité des infrastructures critiques.

CHAPITRE II : ETUDE DES SOLUTIONS DE SÉCURITÉ EXISTANTS

Introduction

Les aéroports doivent aujourd’hui garantir un niveau de sécurité optimal tout en relevant de nombreux défis dans ce domaine. Les responsables sont tenus de jouer plusieurs rôles cruciaux, notamment en matière de sécurité, de sûreté, de communications et d’automatisation des bâtiments. De plus, ils doivent se conformer à des exigences de plus en plus strictes. Pour répondre à ces défis, les aéroports mettent en œuvre diverses solutions de sécurité intégrées et sophistiquées, assurant ainsi une protection complète et efficace des installations, des passagers et du personnel.

I. Solutions de Sécurité Existants

1. Solutions de Sécurité

- **Cryptage des Communications** : Utilisation de protocoles de cryptage avancés pour protéger les données radar, les données de vol et les communications vocales contre les interceptions non autorisées.
 - **Avantages** : Assure la confidentialité et l’intégrité des données transmises ; protège contre les écoutes et les manipulations.
 - **Inconvénients** : Peut entraîner une latence dans la communication ; nécessite une gestion rigoureuse des clés de cryptage.
- **Pare-feu et Systèmes de Détection d’Intrusion** : Déploiement de pare-feu robustes et de systèmes de détection et de prévention des intrusions (IDS/IPS) pour surveiller et contrôler le trafic réseau, bloquant ainsi les tentatives d’accès non autorisées.
 - **Avantages** : Offre une protection proactive contre les menaces ; surveille en temps réel le trafic réseau.
 - **Inconvénients** : Peut générer des faux positifs, entraînant des interruptions inutiles ; nécessite une configuration et une maintenance régulières.

-
- **Authentification et Gestion des Accès** : Mise en place de mécanismes d'authentification forte et de gestion des accès pour s'assurer que seules les personnes autorisées peuvent accéder aux systèmes et aux informations critiques.
 - **Avantages** : Réduit le risque d'accès non autorisé ; améliore la traçabilité et l'audit des accès.
 - **Inconvénients** : Peut être complexe à implémenter et à gérer ; nécessite une sensibilisation des utilisateurs pour être efficace.
 - **Surveillance et Réponse aux Incidents** : Implémentation de solutions de surveillance continue et de gestion des incidents de sécurité pour détecter et répondre rapidement aux menaces potentielles, minimisant ainsi l'impact des cyberattaques.
 - **Avantages** : Permet une réaction rapide aux incidents de sécurité ; aide à réduire les dommages et les temps d'arrêt.
 - **Inconvénients** : Peut nécessiter des ressources importantes pour une surveillance continue ; risque de surcharge d'informations si mal géré.
 - **Réseaux Privés Virtuels (VPN)** : Utilisation de VPN pour sécuriser les communications entre les différents acteurs de la gestion du trafic aérien, assurant ainsi la confidentialité et l'intégrité des données transmises.
 - **Avantages** : Offre une communication sécurisée sur des réseaux non sécurisés ; facile à déployer et à utiliser.
 - **Inconvénients** : Peut ralentir la vitesse de connexion ; vulnérable aux attaques si les protocoles de sécurité ne sont pas correctement configurés.
 - **Mise à Jour et Gestion des Patches** : Application régulière de mises à jour et de patches de sécurité pour corriger les vulnérabilités connues et protéger les systèmes contre les menaces émergentes.
 - **Avantages** : Maintient les systèmes à jour et sécurisés ; réduit le risque d'exploitation des vulnérabilités.
 - **Inconvénients** : Peut causer des interruptions lors de l'application des mises à jour ; nécessite une gestion rigoureuse pour être efficace.
 - **Formation et Sensibilisation à la Sécurité** : Organisation de programmes de formation et de sensibilisation pour le personnel afin de renforcer la culture de sécurité et de réduire les risques liés aux erreurs humaines.
 - **Avantages** : Augmente la vigilance et la réactivité du personnel face aux menaces de sécurité ; réduit les risques d'erreurs humaines.
 - **Inconvénients** : Nécessite des ressources pour l'organisation et la mise en œuvre des formations ; l'efficacité dépend de l'engagement du personnel.

2. Protocoles de Sécurité Réseau pour les Aéroports

Les aéroports utilisent divers protocoles de sécurité réseau pour assurer la protection de leurs systèmes. Voici une présentation détaillée de plusieurs protocoles clés, suivie d'une comparaison sous forme de tableau.

- **TLS (Transport Layer Security)** : Protocole cryptographique qui assure la sécurité des communications sur un réseau informatique en chiffrant les données échangées entre les serveurs et les clients. Utilisé pour sécuriser les connexions HTTPS.

-
- **Avantages** : Assure la confidentialité et l'intégrité des données ; protège contre les attaques de type "man-in-the-middle".
 - **Inconvénients** : Peut introduire une latence ; nécessite des certificats valides et une gestion rigoureuse des clés.
 - **IPsec (Internet Protocol Security)** : Suite de protocoles utilisée pour sécuriser les communications sur un réseau IP en chiffrant et en authentifiant les paquets de données au niveau de la couche réseau.
 - **Avantages** : Offre une protection complète au niveau du réseau ; efficace pour sécuriser les VPNs.
 - **Inconvénients** : Peut être complexe à configurer ; peut introduire une surcharge sur les performances du réseau.
 - **SNMPv3 (Simple Network Management Protocol version 3)** : Protocole de gestion réseau qui offre des mécanismes de sécurité améliorés, y compris l'authentification, la confidentialité et l'intégrité des données.
 - **Avantages** : Permet une gestion sécurisée des équipements réseau ; protège contre les accès non autorisés.
 - **Inconvénients** : Peut être difficile à configurer correctement ; nécessite une bonne gestion des communautés de sécurité.
 - **BGP (Border Gateway Protocol) avec RPKI (Resource Public Key Infrastructure)** : Protocole de routage utilisé pour échanger des informations de routage entre différents systèmes autonomes ; RPKI est utilisé pour sécuriser les annonces de routage.
 - **Avantages** : Améliore la sécurité du routage Internet ; réduit le risque de détournement de route.
 - **Inconvénients** : Complexité de mise en œuvre ; nécessite une gestion continue des certificats RPKI.
 - **SSH (Secure Shell)** : Protocole cryptographique utilisé pour établir des connexions sécurisées à distance entre un utilisateur et un serveur. Il utilise le chiffrement pour protéger les données échangées contre l'écoute clandestine et offre des mécanismes d'authentification basés sur des clés publiques et privées.
 - **Avantages** : Assure la confidentialité des données échangées ; permet une gestion à distance sécurisée et un transfert de fichiers en toute sécurité ; offre des capacités de tunnelling pour contourner les restrictions réseau.
 - **Inconvénients** : Peut nécessiter une configuration correcte pour assurer une sécurité optimale ; les pare-feu peuvent bloquer les connexions SSH si elles ne sont pas correctement configurées.

3. Tableau Comparatif des Protocoles de Sécurité

Protocole	Avantages	Inconvénients
TLS	Confidentialité et intégrité des données Protection contre les attaques "man-in-the-middle"	Latence Gestion des certificats
IPsec	Protection réseau Sécurisation des VPNs	Complexité de configuration Surcharge réseau
SNMPv3	Gestion sécurisée Protection contre accès non autorisés	Configuration Gestion des communautés
BGP avec RPKI	Sécurité du routage Réduction détournement	Complexité Gestion des certificats
SSH	Confidentialité et intégrité des données Gestion à distance Transfert sécurisé de fichiers Accès aux services dans le cloud	Installation de logiciels supplémentaires Configuration des clés

TABLE 1 – Comparaison entre les protocoles de Sécurité

II. Solutions de Sécurité sur le Marché pour les Aéroports

Pour répondre aux défis croissants en matière de sécurité, les aéroports se tournent vers une gamme de solutions de sécurité avancées disponibles sur le marché. Ces solutions comprennent :

- **Systèmes de Surveillance Vidéo Intelligents** : Utilisation de caméras de surveillance haute définition couplées à des logiciels d'analyse vidéo pour détecter des comportements suspects et réagir rapidement aux incidents.
- **Contrôle d'Accès Electronique** : Mise en place de systèmes de contrôle d'accès électroniques qui utilisent des cartes à puce, des biométries et d'autres technologies pour restreindre l'accès aux zones sensibles.
- **Détection d'Intrusion** : Utilisation de capteurs avancés et de systèmes d'alarme pour surveiller et protéger les périmètres et les installations contre les intrusions non autorisées.
- **Sécurité des Réseaux Informatiques** : Mise en œuvre de solutions de cybersécurité pour protéger les réseaux et les systèmes informatiques contre les cyberattaques, incluant les pare-feu, les systèmes de détection et de prévention des intrusions (IDS/IPS) et les solutions de chiffrement des données.
- **Gestion Intégrée des Bâtiments** : Utilisation de systèmes de gestion des bâtiments qui intègrent la sécurité, la surveillance, le contrôle d'accès et d'autres fonctions pour une gestion centralisée et efficace.
- **Scanners et DéTECTEURS Avancés** : Installation de scanners de bagages et de détecteurs de métaux avancés pour assurer une inspection minutieuse et rapide des passagers et de leurs bagages.

-
- **Systèmes de Communication Sécurisés** : Déploiement de systèmes de communication sécurisés pour assurer une coordination efficace entre les différents acteurs de la sécurité aéroportuaire.

III. Solution Proposée

Dans le cadre de l'implémentation des solutions de sécurité pour le Réseau IP de la Navigation Aérienne Marocaine (RINAM), j'ai identifié les protocoles IPsec et SSH comme des solutions appropriées pour assurer la sécurité des communications.

IPsec, ou Internet Protocol Security, est un ensemble de protocoles développés pour sécuriser les communications au niveau du réseau en fournissant des mécanismes de chiffrement et d'authentification. Cette solution est particulièrement adaptée aux exigences de sécurité du RINAM, qui nécessitent une protection robuste des données échangées entre les différents dispositifs du réseau de navigation aérienne. Le choix d'IPsec repose sur sa capacité à garantir la confidentialité, l'intégrité et l'authenticité des données, tout en étant conforme aux normes de sécurité internationales.

En complément, SSH (Secure Shell) est utilisé pour sécuriser les accès et les communications à distance avec les systèmes critiques du RINAM. SSH assure le chiffrement des données, protège contre les écoutes clandestines et garantit l'intégrité des informations échangées. Bien que SSH soit particulièrement efficace pour la gestion sécurisée à distance et la protection des communications de données.

Dans la section suivante, nous examinerons en détail le fonctionnement d'IPsec et de SSH, en mettant en lumière leurs mécanismes de sécurité, leurs protocoles associés, et les avantages qu'ils offrent pour la protection des communications au sein du RINAM.

IV. Protocole IPsec

1. Fonctionnement d'IPsec

IPsec fonctionne en sécurisant les paquets de données IP par l'utilisation de deux principaux protocoles : le protocole de sécurité des paquets (ESP) et le protocole d'authentification des en-têtes (AH). Le protocole ESP fournit des services de chiffrement et d'authentification des données, garantissant ainsi la confidentialité et l'intégrité des informations échangées. Le protocole AH, quant à lui, assure l'intégrité des en-têtes des paquets et vérifie l'authenticité des sources.

2. Modes de Fonctionnement

IPsec peut fonctionner en deux modes : le mode transport et le mode tunnel. En mode transport, seul le contenu des paquets est chiffré, tandis qu'en mode tunnel, l'ensemble du paquet, y compris l'en-tête, est chiffré. Le choix entre ces modes dépend des besoins spécifiques en matière de sécurité et de configuration du réseau.

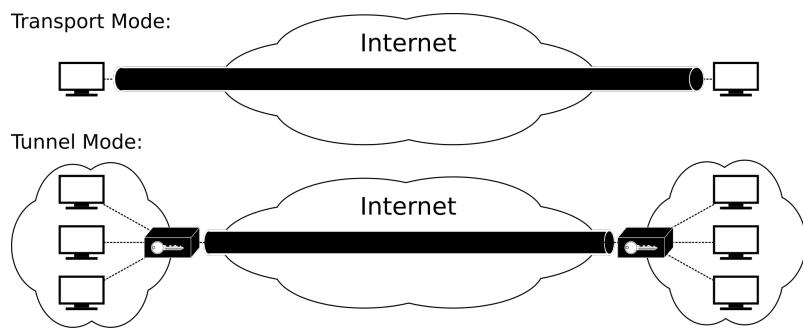


FIGURE 9 – Modes d'IPSec

3. Présentation d'IPsec

L'architecture d'IPsec repose sur plusieurs composants clés, notamment l'Authentication Header (AH), Encapsulating Security Payload (ESP) et Internet Key Exchange (IKE), chacun ayant un rôle spécifique dans la sécurisation des communications réseau.

Protocole Authentication Header (AH) :

Fournit l'authentification de données et l'intégrité, mais n'offre pas de confidentialité (pas de chiffrement). Il ajoute un en-tête supplémentaire au paquet IP d'origine avec une somme de contrôle basée sur le contenu.

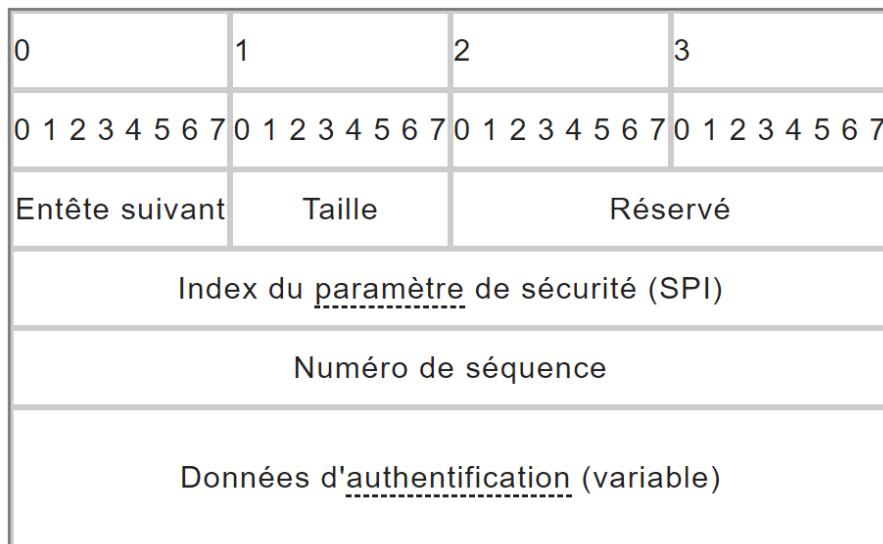


FIGURE 10 – AH

Protocole Encapsulating Security Payload (ESP) :

Assure la confidentialité, l'authentification et l'intégrité des données en chiffrant et en ajoutant un en-tête ESP aux paquets IP.

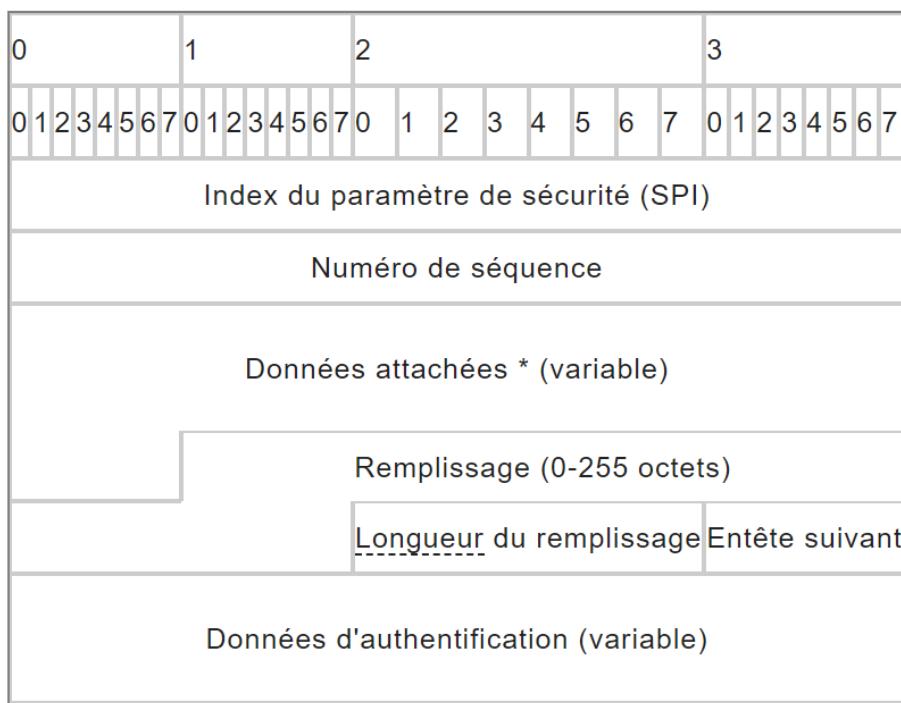


FIGURE 11 – Esp

Internet Key Exchange (IKE) :

Protocole pour négocier et établir des associations de sécurité entre les appareils.

4. Mécanismes d'Authentification et de Chiffrement d'IPsec

- **Authentification**

IPsec propose plusieurs mécanismes d'authentification afin de vérifier l'identité des parties impliquées dans la communication et de prévenir les attaques de type "homme du milieu" (MITM). L'authentification peut être réalisée en utilisant des méthodes basées sur des clés partagées, telles que le HMAC (Code d'Authentification de Message basé sur un Hachage), où un HMAC est calculé sur les données échangées à l'aide d'une clé partagée. Une autre méthode d'authentification courante est l'utilisation de certificats numériques, où les parties s'authentifient mutuellement en présentant des certificats émis par une autorité de certification (CA) de confiance.

- **Chiffrement**

IPsec fait appel à des algorithmes de chiffrement pour sécuriser le contenu des paquets IP lors de leur transmission à travers le réseau. Parmi les algorithmes de chiffrement couramment utilisés dans IPsec, on trouve le DES (Standard de Chiffrement des Données), le 3DES (Triple DES), l'AES (Standard de Chiffrement Avancé) et le Blowfish. IPsec offre la possibilité d'utiliser deux modes de chiffrement : le mode transport, où seules les données utiles sont chiffrées, et le mode tunnel, où l'intégralité du paquet IP est encapsulée et chiffrée.

5. Intégration d'IPsec dans les protocoles de communication réseau (IPv4, IPv6)

- **IPv4**

IPv4 est le protocole de communication fondamental utilisé pour le routage des données sur Internet. IPsec, un protocole de sécurité intégré à IPv4, offre des options de sécurisation des communications entre hôtes ou entre passerelles. Il peut être configuré en mode transport ou tunnel. Dans le mode transport, seules les données utiles sont chiffrées ou authentifiées, tandis que dans le mode tunnel, l'intégralité du paquet IP est protégée. IPsec est largement utilisé pour établir des réseaux privés virtuels (VPN), sécuriser les connexions entre les sites distants et protéger les données sensibles contre les menaces.

- **IPv6**

IPv6 intègre nativement IPsec, simplifiant ainsi sa mise en œuvre dans les réseaux utilisant ce protocole. Les en-têtes d'authentification (AH) et de sécurité encapsulée (ESP) sont pris en charge par défaut dans IPv6. L'utilisation d'IPsec est fortement encouragée pour assurer la sécurité des communications sur les réseaux IPv6, offrant ainsi une protection essentielle contre les menaces potentielles.

6. Cas d'Utilisation Appropriés pour IPsec

IPsec trouve des applications variées dans divers environnements réseau

VPN (Virtual Private Network) :

IPsec est largement utilisé pour sécuriser les connexions VPN, offrant une solution fiable pour permettre aux utilisateurs distants d'accéder en toute sécurité aux ressources réseau de leur organisation via Internet. Il établit des tunnels cryptés entre les périphériques clients et le réseau privé, assurant ainsi la confidentialité et l'intégrité des données échangées.

Connexions site à site :

IPsec est également déployé pour sécuriser les communications entre les différents sites d'une même organisation. Ces tunnels IPsec garantissent un transfert sécurisé des données sensibles entre les passerelles des sites distants, protégeant ainsi les informations confidentielles contre les menaces potentielles sur le réseau.

Télétravail :

Dans le contexte du télétravail, IPsec permet aux employés distants de se connecter en toute sécurité au réseau de leur entreprise depuis des emplacements externes. En sécurisant le trafic entre les appareils des employés et le réseau de l'entreprise, IPsec assure que les communications et les données restent protégées contre les menaces en ligne.

Communications inter-systèmes :

IPsec peut être déployé pour sécuriser les communications entre différents systèmes informatiques au sein d'un même réseau local. En configurant des politiques IPsec sur les hôtes individuels, il est possible d'assurer la confidentialité et l'intégrité des données échangées entre ces systèmes, protégeant ainsi contre les intrusions et les attaques malveillantes.

Voix sur IP (VoIP) :

IPsec est souvent utilisé pour sécuriser les communications vocales en cryptant le trafic vocal entre les appareils. Cela garantit que les informations échangées restent confidentielles, ce qui est crucial pour les organisations traitant des informations sensibles ou privées par le biais de communications vocales.

V. Protocole SSH

Le protocole Secure Shell (SSH) est une méthode permettant d'envoyer en toute sécurité des commandes à un ordinateur sur un réseau non sécurisé. SSH a recours à la cryptographie pour authentifier et chiffrer les connexions entre les appareils. SSH permet également la tunnelling, ou le transfert de port, c'est-à-dire que les paquets peuvent traverser des réseaux qu'il ne pourrait pas traverser autrement. SSH est souvent utilisé pour contrôler des serveurs à distance, dans le but de gérer l'infrastructure et de transférer des fichiers.

1. Sécurité et Tunnelling avec SSH

Connexions chiffrées à distance : SSH établit une connexion entre l'appareil d'un utilisateur et une machine éloignée, souvent un serveur. Il utilise le chiffrement pour brouiller les données qui traversent la connexion. Quiconque intercepterait les données ne trouverait que des données statiques, c'est-à-dire des données aléatoires qui n'ont aucun sens tant qu'elles ne sont pas déchiffrées. (Les méthodes de chiffrement appliquées par SSH rendent le déchiffrement extrêmement difficile pour les personnes extérieures).

Possibilité de tunnelling : dans le domaine des réseaux, la tunnelling est une méthode permettant de faire transiter un paquet au travers d'un réseau en utilisant un protocole ou suivant un itinéraire qu'il ne pourrait normalement pas emprunter. La tunnelling consiste à envelopper les paquets* de données avec des informations supplémentaires, appelées en-têtes, afin de modifier leur destination. Les tunnels SSH ont recours à une technique appelée redirection de port pour transférer des paquets d'une machine à l'autre. La redirection de port est expliquée plus en détail ci-dessous.

2. Fonctionnement de SSH

TCP/IP

SSH s'exécute parallèlement à la suite de protocoles TCP/IP, sur laquelle repose une grande partie du site Internet. TCP signifie Transmission Control Protocol et IP Internet Protocol. TCP/IP associe ces deux protocoles afin de formater, acheminer et distribuer les paquets. IP indique, entre autres informations, l'adresse IP à laquelle un paquet doit être envoyé (à l'image d'une adresse postale), tandis que TCP indique

le port vers lequel un paquet doit être envoyé pour chaque adresse IP (comme l'étage d'un bâtiment ou un numéro d'appartement).

TCP est un protocole de couche de transport : il prend en charge le transport et la distribution des paquets. En général, des protocoles supplémentaires sont utilisés en plus de TCP/IP afin de préparer les données transmises dans un format utilisable par l'application. SSH est un de ces protocoles. (Autres exemples : HTTP, FTP et SMTP).

Cryptographie à clé publique

SSH est « sécurisé » car il intègre le chiffrement et l'authentification dans le cadre d'un processus appelé cryptographie à clé publique. La cryptographie à clé publique est un moyen de chiffrer des données ou de les signer avec deux clés différentes. Une des deux clés, la clé publique, est accessible à tous. L'autre, la clé privée, est gardée secrète par son propriétaire. Les deux clés étant strictement associées, pour établir l'identité du propriétaire de la clé, il est nécessaire d'avoir en sa possession la clé privée qui correspond à la clé publique.

Ces clés « asymétriques », appelées ainsi parce qu'elles ont des valeurs différentes, permettent également aux deux parties de la connexion de négocier des clés symétriques identiques et partagées pour un chiffrement supplémentaire du canal. Une fois cette négociation terminée, les deux parties utilisent les clés symétriques pour chiffrer les données qu'elles échangent.

Dans une connexion SSH, les deux parties disposent d'une paire de clés publique/-privée, et chaque partie authentifie l'autre à l'aide de ces clés. C'est ce qui distingue SSH de HTTPS, qui, dans la plupart des cas, ne vérifie que l'identité du serveur web dans le cadre d'une connexion client-serveur. (Parmi les autres différences, citons le fait que HTTPS ne permet généralement pas au client d'accéder à la ligne de commande du serveur et que les pare-feu bloquent parfois SSH, mais presque jamais HTTPS).

Authentification

Bien que la cryptographie à clé publique permette d'authentifier les appareils connectés selon SSH, un ordinateur correctement sécurisé exigera toujours l'authentification de la personne qui utilise SSH. Il s'agit souvent de saisir un nom d'utilisateur et un mot de passe.

Une fois l'authentification établie, la personne peut exécuter des commandes sur la machine distante comme si elle le faisait sur sa propre machine en local.

Tunnellisation SSH, ou redirection de port

La redirection de port est comparable au transfert d'un message entre deux personnes. Bob peut envoyer un message à Alice, qui le transmet à son tour à Dave. De la même manière, la redirection de port transfère les paquets destinés à une adresse IP et à un port d'une machine donnée vers une adresse IP et un port d'une autre machine.

Imaginons par exemple qu'un administrateur veuille apporter une modification à un serveur situé dans un réseau privé dont il assure la gestion, et qu'il veuille le faire à partir d'un site distant. Pour des raisons de sécurité, ce serveur ne reçoit que des paquets provenant d'autres ordinateurs au sein du réseau privé. L'administrateur a alors la possibilité de se connecter à un deuxième serveur au sein du réseau, un serveur qui reçoit sans problème du trafic provenant d'Internet, et d'utiliser la redirection de port SSH pour se connecter au premier serveur. Du point de vue du premier serveur, les paquets de l'administrateur proviennent de l'intérieur du réseau privé.

Utilisation du protocole SSH

Le protocole SSH est présent dans les systèmes d'exploitation Linux et Mac. Sur les machines Windows, il arrive qu'il soit nécessaire d'installer une application client SSH. Sur les ordinateurs Mac et Linux, les utilisateurs peuvent ouvrir l'application Terminal et saisir directement les commandes SSH.

3. Utilisations Pratiques du Protocole SSH

Techniquement, SSH peut transmettre n'importe quelle donnée arbitraire sur un réseau, et la tunnelling SSH peut être mise en place pour une multitude d'objectifs. Toutefois, les cas d'utilisation les plus courants de SSH sont les suivants :

- Gestion à distance des serveurs, de l'infrastructure et des ordinateurs des collaborateurs
- Transfert de fichiers en toute sécurité (SSH est plus sûr qu'un protocole non chiffré tel que FTP)
- Accès à des services dans le cloud sans exposer les ports d'une machine locale à l'Internet
- Connexion à distance aux services d'un réseau privé
- Contournement des restrictions d'un pare-feu

4. Port de Protocole SSH

Le port 22 est le port par défaut pour le protocole SSH. Parfois, les pare-feu bloquent l'accès à certains ports sur les serveurs situés derrière le pare-feu, mais laissent le port 22 ouvert. SSH est donc utile pour accéder à des serveurs de l'autre côté du pare-feu : les paquets dirigés vers le port 22 ne sont pas bloqués et peuvent ensuite être transférés vers n'importe quel autre port.

Conclusion

En conclusion, l'étude des solutions de sécurité pour le RINAM met en évidence la nécessité de mettre en œuvre des protocoles robustes et adaptés aux exigences spécifiques du domaine aéronautique. Parmi les diverses solutions disponibles, le protocole IPsec se distingue par sa capacité à garantir la confidentialité, l'intégrité, et l'authenticité des communications au sein du réseau. Ce protocole est particulièrement pertinent pour sécuriser les échanges de données critiques entre les dispositifs du RINAM, en offrant une protection complète contre les menaces potentielles.

En complément, le protocole SSH (Secure Shell) joue également un rôle crucial dans la sécurisation des communications et la gestion à distance des serveurs et infrastructures. SSH permet de garantir la confidentialité et l'intégrité des données échangées, tout en offrant des fonctionnalités telles que la redirection de ports pour accéder aux services d'un réseau privé ou pour contourner les restrictions d'un pare-feu. SSH est particulièrement adapté pour les transferts de fichiers sécurisés et l'accès à des services dans le cloud sans exposer les ports d'une machine locale à l'Internet.

En combinant IPsec et SSH, il est possible de créer une architecture de sécurité robuste qui répond aux exigences spécifiques du RINAM, en garantissant à la fois la protection des communications réseau et la gestion sécurisée des systèmes distants.



Partie III

Conception Et Réalisation

CHAPITRE I : CONCEPTION DU SYSTÈME

Introduction

I. Conception du Système

1. Architecture du Réseau

L'architecture du Réseau IP de la Navigation Aérienne Marocaine (RINAM) est conçue pour assurer une communication sécurisée et efficace entre les différents acteurs du trafic aérien :

- **Nœuds de Communication** : Les tours de contrôle, les stations radar et les centres de gestion du trafic aérien (ATC) sont les principaux nœuds de communication. Chaque nœud est équipé de routeurs et de commutateurs configurés pour gérer le trafic de données de manière sécurisée.
- **Réseau Fédérateur** : Un réseau central reliant tous les noeuds de communication. Ce réseau utilise des liens à haute bande passante et des technologies de redondance pour garantir la disponibilité continue des services.
- **Réseaux d'Accès** : Ces réseaux relient les équipements des utilisateurs finaux (comme les contrôleurs aériens) au réseau fédérateur. Ils incluent des dispositifs de sécurisation comme des pare-feu et des systèmes de détection d'intrusion (IDS/IPS).
- **Connexions VPN** : Les connexions VPN (réseaux privés virtuels) sont utilisées pour sécuriser les communications entre les différents nœuds. Chaque connexion VPN est chiffrée pour assurer la confidentialité des données échangées.

II. VPN (Virtual Private Network)

Un VPN (réseau privé virtuel) est une technologie qui crée une connexion sécurisée et cryptée sur un réseau moins sécurisé, comme Internet. Il permet aux utilisateurs de protéger leurs données et de masquer leur adresse IP, créant ainsi un réseau privé qui garantit la confidentialité et l'intégrité des informations échangées.

1. Types de VPN

VPN Site-à-Site

Connecte plusieurs réseaux privés situés dans différents endroits via Internet. Les routeurs ou pare-feu sur chaque site établissent une connexion sécurisée, permettant aux dispositifs des différents sites de communiquer comme s'ils étaient sur le même réseau local.

Utilisation : Idéal pour connecter des bureaux distants ou des sites d'une entreprise. Il est souvent utilisé pour relier des succursales d'une entreprise à son siège social ou à d'autres bureaux.

VPN Client-à-Site (ou VPN Accès Distant)

Permet à un utilisateur individuel de se connecter à un réseau privé via une connexion Internet sécurisée. Le client VPN installé sur l'ordinateur de l'utilisateur se connecte au serveur VPN, offrant un accès sécurisé au réseau de l'entreprise.

Utilisation : Principalement utilisé par des employés qui travaillent à distance et ont besoin d'accéder au réseau interne de leur entreprise.

VPN MPLS (Multiprotocol Label Switching)

Utilise des labels pour diriger le trafic de données à travers un réseau MPLS. Il peut être utilisé pour créer des réseaux privés virtuels entre plusieurs sites.

Utilisation : Souvent utilisé par les grandes entreprises pour gérer des réseaux complexes avec des exigences élevées en matière de performance et de sécurité.

VPN SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Utilise des protocoles SSL/TLS pour sécuriser les communications entre le client VPN et le serveur VPN. Ce type de VPN est généralement utilisé pour les accès distants via un navigateur web.

Utilisation : Pratique pour les utilisateurs qui ont besoin d'accéder à des applications web ou des services spécifiques de manière sécurisée.

2. VPN Site-à-Site

Un VPN site-à-site est une solution de VPN qui connecte des réseaux entiers situés à différents emplacements. Voici comment cela fonctionne et ses principales caractéristiques :

- **Configuration :** Deux ou plusieurs dispositifs de réseau, généralement des routeurs ou des pare-feu, sont configurés pour établir une connexion VPN. Chaque site possède un dispositif VPN qui chiffre le trafic sortant et le décrypte à son arrivée au site distant.
- **Tunnel VPN :** Crée un "tunnel" sécurisé à travers lequel les données sont envoyées entre les sites. Ce tunnel est chiffré pour garantir que les données ne puissent pas être lues par des parties non autorisées.

- **Utilisation** : Permet aux bureaux d'une entreprise, aux succursales ou aux sites distants de communiquer comme s'ils faisaient partie du même réseau local. Cela facilite la communication et le partage de ressources entre les sites tout en assurant la sécurité des données.
- **Avantages** :
 - **Sécurité** : Le chiffrement protège les données en transit contre les interceptions et les attaques.
 - **Intégration Transparente** : Les utilisateurs des différents sites peuvent accéder aux ressources du réseau comme s'ils étaient au même emplacement.
 - **Économie** : Réduit les coûts de communication en utilisant des connexions Internet plutôt que des lignes dédiées coûteuses.

III. Techniques de Cryptage

1. Cryptage Symétrique

Le cryptage symétrique utilise une clé unique pour à la fois chiffrer et déchiffrer les données. Ce type de cryptographie est rapide et efficace, ce qui le rend idéal pour traiter de grandes quantités de données. Dans le cadre d'IPsec, des algorithmes comme AES (Advanced Encryption Standard) et 3DES (Triple Data Encryption Standard) sont employés pour protéger la confidentialité des données transmises sur un VPN. Une clé secrète partagée entre les parties est utilisée pour garantir que seules les personnes autorisées puissent accéder aux informations. De même, SSH utilise des algorithmes symétriques tels que AES pour chiffrer les données échangées pendant la session. Ce chiffrement symétrique assure que les informations restent confidentielles et protégées contre les interceptions non autorisées.

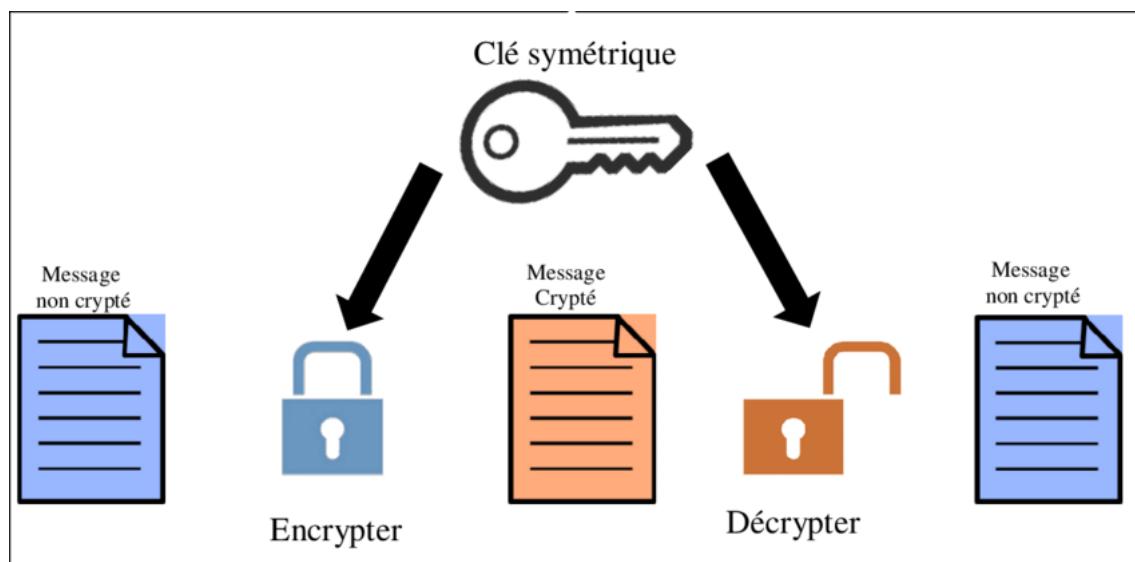


FIGURE 12 – Cryptage Symétrique

2. Cryptage Asymétrique

Le cryptage asymétrique, également connu sous le nom de cryptographie à clé publique, utilise une paire de clés distinctes : une clé publique pour le chiffrement et une clé privée pour le déchiffrement. La clé publique est accessible à tous, tandis que la clé privée reste secrète. Cette approche est principalement utilisée pour sécuriser l'échange de clés et l'authentification. Dans IPsec, le cryptage asymétrique est utilisé principalement lors de l'échange de clés à travers le protocole IKE (Internet Key Exchange), qui utilise des algorithmes comme RSA pour établir des connexions sécurisées. SSH, quant à lui, utilise le cryptage asymétrique pour authentifier les parties communicantes au début d'une session. Cela implique l'utilisation de clés publiques et privées pour vérifier l'identité des utilisateurs et des serveurs.

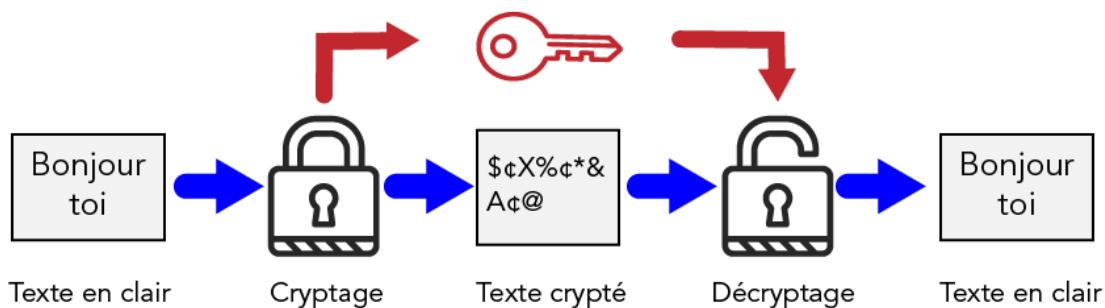


FIGURE 13 – Cryptage Asymétrique

3. Hachage

Le hachage est une technique irréversible qui transforme des données en une chaîne de caractères fixe appelée "empreinte" ou "hachage", à l'aide d'une fonction de hachage. Cette empreinte est unique pour chaque ensemble de données différent, et même une petite modification des données produira une empreinte complètement différente. Les fonctions de hachage, telles que SHA-1 et SHA-256, sont utilisées dans IPsec pour assurer l'intégrité des données et vérifier les messages via le protocole AH (Authentication Header). Elles garantissent que les données n'ont pas été altérées lors de la transmission. SSH utilise également des fonctions de hachage pour vérifier l'intégrité des messages échangés et pour créer des empreintes de clés, assurant ainsi une communication sécurisée et vérifiable entre le client et le serveur.



FIGURE 14 – Schéma de hachage

CHAPITRE II : RÉALISATION ET IMPLÉMENTATION

Introduction

Dans ce chapitre, j'aborderai la réalisation du système de communication sécurisé du Réseau IP de la Navigation Aérienne Marocaine (RINAM). L'objectif est de concevoir une architecture réseau robuste et adaptée aux besoins spécifiques de la navigation aérienne. Le RINAM se caractérise par une infrastructure complexe reliant divers noeuds critiques tels que les tours de contrôle, les stations radar, et les centres de gestion du trafic aérien (ATC). Ces noeuds sont interconnectés via un réseau fédérateur utilisant des technologies avancées pour garantir la disponibilité et la sécurité des communications. Ce chapitre se focalisera également sur les outils de simulation et de test, notamment GNS3 et VirtualBox, choisis pour leur capacité à reproduire fidèlement les conditions opérationnelles du RINAM et à tester les configurations réseau dans un environnement contrôlé.

I. Environnement de Test

Dans cette partie, je présenterai l'environnement technique.

1. GNS3

GNS3 (Graphical Network Simulator-3) est un simulateur de réseau open-source qui permet aux utilisateurs de concevoir, configurer, tester et dépanner des réseaux virtuels en utilisant des routeurs, des commutateurs et d'autres dispositifs réseau réels ou simulés. GNS3 est largement utilisé par les professionnels de l'informatique, les ingénieurs réseau et les étudiants pour pratiquer et développer leurs compétences en conception et en gestion de réseaux.



FIGURE 15 – Logo du GNS3

Ses Caractéristiques principales :

- **Simulation de Dispositifs Réels** : GNS3 permet de simuler des équipements réels, tels que les routeurs et les commutateurs Cisco, à l'aide d'images IOS (Internetwork Operating System) fournies par l'utilisateur.
- **Émulation de Logiciels** : En plus de simuler du matériel, GNS3 peut également émuler divers logiciels de réseau, comme des serveurs ou des applications spécifiques.
- **Interface Graphique** : GNS3 offre une interface graphique intuitive pour créer des topologies de réseau en glissant-déposant les dispositifs sur un tableau de conception.
- **Intégration avec du Matériel Réel** : GNS3 peut être connecté à du matériel réseau physique pour permettre des tests dans des environnements hybrides, combinant dispositifs réels et simulés.
- **Support Multiplateforme** : Le logiciel est compatible avec plusieurs systèmes d'exploitation, y compris Windows, macOS, et Linux.
- **Communauté Active** : GNS3 dispose d'une large communauté d'utilisateurs qui contribuent à son développement, partagent des configurations, et offrent du support à d'autres utilisateurs.

2. Wireshark

Wireshark est un outil de capture et d'analyse de paquets réseau open-source. Il permet aux utilisateurs d'intercepter et d'inspecter le trafic réseau en temps réel ou à partir de fichiers de capture préalablement enregistrés. Wireshark prend en charge une large gamme de protocoles réseau, ce qui en fait un outil polyvalent pour le dépannage, la sécurité réseau, la surveillance de la performance et la compréhension du comportement du réseau. Les fonctionnalités de filtrage avancées de Wireshark permettent aux utilisateurs de cibler et d'examiner spécifiquement les paquets qui les intéressent, tandis que ses capacités de décodage détaillé fournissent des informations précieuses sur les échanges de données au sein du réseau.



FIGURE 16 – Logo de Wireshark

3. VirtualBox

VirtualBox est un logiciel de virtualisation open-source développé par Oracle qui permet aux utilisateurs de créer et de gérer des machines virtuelles (VMs) sur leurs ordinateurs. Une machine virtuelle est un environnement logiciel qui émule un ordinateur physique, permettant ainsi d'exécuter plusieurs systèmes d'exploitation sur une seule machine physique sans avoir besoin de redémarrer ou de partitionner le disque dur.



FIGURE 17 – Logo du VirtualBox

Ses Caractéristiques principales :

- **Multiplateforme** : VirtualBox fonctionne sur plusieurs systèmes d'exploitation hôtes, tels que Windows, macOS, Linux, et Solaris. Il permet d'exécuter des systèmes d'exploitation invités tels que Windows, Linux, macOS, Solaris, et autres distributions Unix.
- **Support de Multiple OS Invités** : Vous pouvez exécuter différents systèmes d'exploitation en même temps sur un même hôte. Par exemple, un utilisateur sous Windows peut exécuter une VM sous Linux ou macOS à l'intérieur de VirtualBox.
- **Snapshots** : VirtualBox permet de prendre des "instantanés" de l'état actuel d'une VM, ce qui permet de revenir rapidement à un état antérieur en cas de besoin. Cela est particulièrement utile lors de la réalisation de tests ou d'expériences qui pourraient affecter le système invité.
- **Partage de Fichiers** : VirtualBox permet de configurer des dossiers partagés entre l'hôte et la VM, facilitant le transfert de fichiers entre les deux environnements.
- **Réseautage** : VirtualBox offre une gamme d'options de configuration réseau, y compris NAT (Network Address Translation), pontage (bridged networking), et réseau interne (internal networking), permettant aux VMs de communiquer entre elles ou avec des appareils externes.
- **Support pour les Extensions** : VirtualBox propose des extensions comme les "Guest Additions" qui améliorent l'intégration entre l'hôte et l'invité, offrant des fonctionnalités supplémentaires comme un meilleur support graphique, le redimensionnement dynamique de la fenêtre de la VM, et le partage du presse-papiers.
- **Portabilité** : Les VMs créées avec VirtualBox peuvent être exportées sous forme de fichiers OVA (Open Virtual Appliance), permettant de les déplacer et de les importer facilement sur d'autres installations de VirtualBox ou même d'autres logiciels de virtualisation.

Dans VirtualBox, j'utilise deux machines virtuelles, l'une exécutant Ubuntu et l'autre Linux.

Ubuntu est une distribution Linux basée sur Debian, reconnue pour sa convivialité et sa large communauté de support. Elle est souvent choisie pour sa facilité d'utilisation, son interface utilisateur intuitive, et sa compatibilité avec une vaste gamme de logiciels.

Linux, quant à lui, fait référence au noyau qui est au cœur de nombreuses distributions, y compris Ubuntu. Le noyau Linux gère les ressources matérielles de l'ordinateur et assure l'interaction entre le matériel et les logiciels.

Windows 7 est un système d'exploitation de Microsoft utilisé ici pour tester la compatibilité et les configurations spécifiques dans un environnement Windows.

Ces trois environnements permettent de simuler et de tester des configurations réseaux sécurisées, comme l'intégration de VPNs, dans un cadre virtuel.

4. Logiciel Snort

4.1. Définition

Snort est un système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) gratuit et open-source¹ créé en 1998 par Martin Roesch.

Développé à l'origine par la société Sourcefire, il est aujourd'hui maintenu par Cisco Systems à la suite du rachat de Sourcefire en 2013.



FIGURE 18 – Logo de Snort

4.2. Fonctionnalités

- **Détection d'Intrusion** : Snort permet de détecter les tentatives d'intrusion en comparant le trafic réseau aux signatures connues de menaces.
- **Analyse de Paquets** : Il peut analyser en profondeur les paquets pour identifier des anomalies ou des activités suspectes.
- **Génération d'Alertes** : Lorsqu'une menace est détectée, Snort génère des alertes en temps réel, permettant aux administrateurs de réagir rapidement.

4.3. Composants de Snort

- **Preprocessor** : Ce module prépare les paquets pour l'analyse en les normalisant et en les décodant. Il est également capable de détecter certains types d'anomalies avant que les paquets ne soient envoyés au moteur de détection.

-
- **Detection Engine** : C'est le cœur de Snort. Le moteur de détection compare les paquets aux règles définies pour identifier les menaces. Si une correspondance est trouvée, une alerte est générée.
 - **Output Plugins** : Ces plugins gèrent la manière dont les résultats et les alertes sont enregistrés ou signalés. Snort peut les enregistrer dans des fichiers journaux, les envoyer à une base de données, ou encore déclencher des notifications.

4.4. Mode de Fonctionnement

- **Mode Sniffer** : Capture et affiche le trafic réseau en temps réel, utile pour l'analyse initiale du réseau.
- **Mode Packet Logger** : Enregistre le trafic réseau capturé dans des fichiers pour une analyse ultérieure, facilitant ainsi l'audit et la recherche d'incidents.
- **Mode IDS** : Analyse le trafic en temps réel et génère des alertes pour toute activité suspecte ou malveillante, permettant une réponse rapide.

4.5. Architecture de Snort

L'architecture de Snort se compose de plusieurs composants intégrés pour capturer, analyser et détecter les menaces dans le trafic réseau. Elle commence par la capture des paquets à l'aide de la bibliothèque 'libpcap', permettant d'intercepter les données sur les interfaces réseau. Ces paquets sont ensuite décodés pour extraire les informations essentielles des en-têtes de protocole (comme IP, TCP, UDP).

Les paquets passent ensuite par des preprocessors, qui les préparent pour l'analyse en normalisant les données, détectant les anomalies et résassemblant les paquets fragmentés. Le moteur de détection, situé au cœur de Snort, compare ensuite les paquets aux règles prédéfinies, recherchant des signatures d'attaques ou des comportements suspects.

Enfin, les résultats de cette analyse sont gérés par des output plugins, qui permettent d'enregistrer les alertes et les détails des paquets dans des fichiers journaux ou de les transmettre en temps réel à des systèmes de gestion de sécurité pour une réponse rapide. Cette architecture modulaire et détaillée permet à Snort d'être un outil puissant pour la surveillance proactive et la protection des réseaux.

II. Représentation Visuelle d'IPSEC

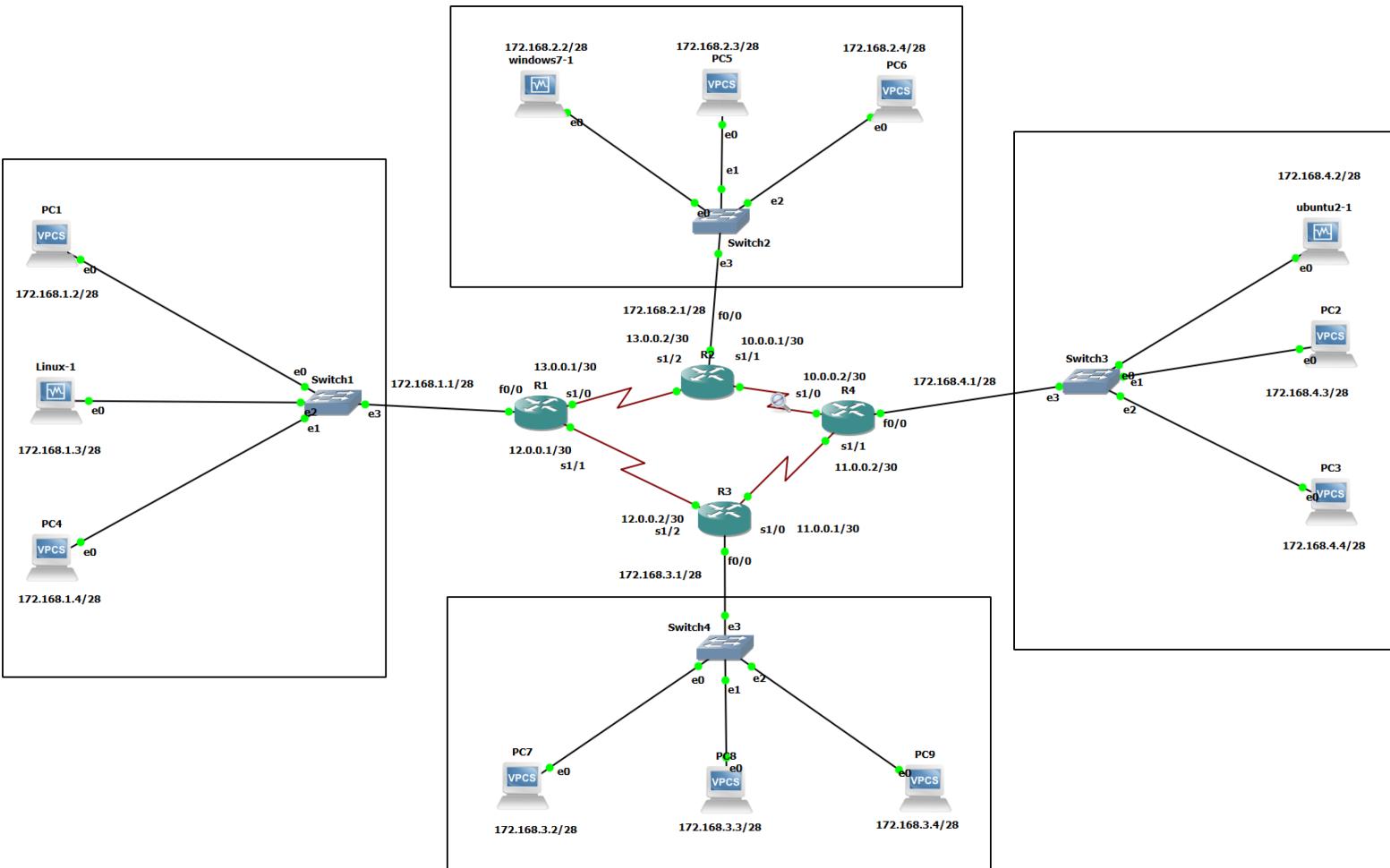


FIGURE 19 – Schéma de simulation d'un Réseau Virtuel

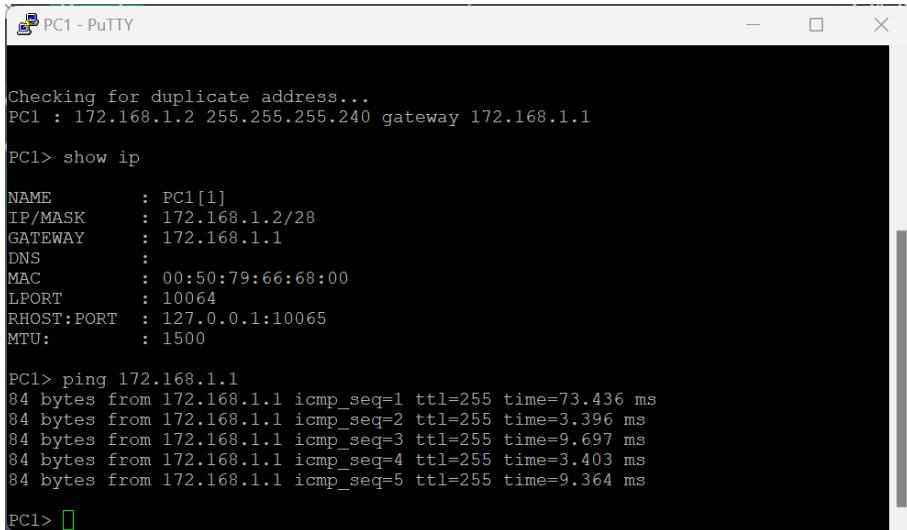
1. Scénarios de Simulation

je décris la simulation de la connexion entre deux machines virtuelles (VMs), l'une fonctionnant sous Linux et l'autre sous Ubuntu. L'objectif principal est de configurer les VMs pour permettre une communication sécurisée en utilisant le protocole IPsec et de vérifier cette sécurité à l'aide de Wireshark.

III. Configuration des Paramètres

1. Configuration des Machines

PC1



```
PC1 - PuTTY

Checking for duplicate address...
PC1 : 172.168.1.2 255.255.255.240 gateway 172.168.1.1

PC1> show ip

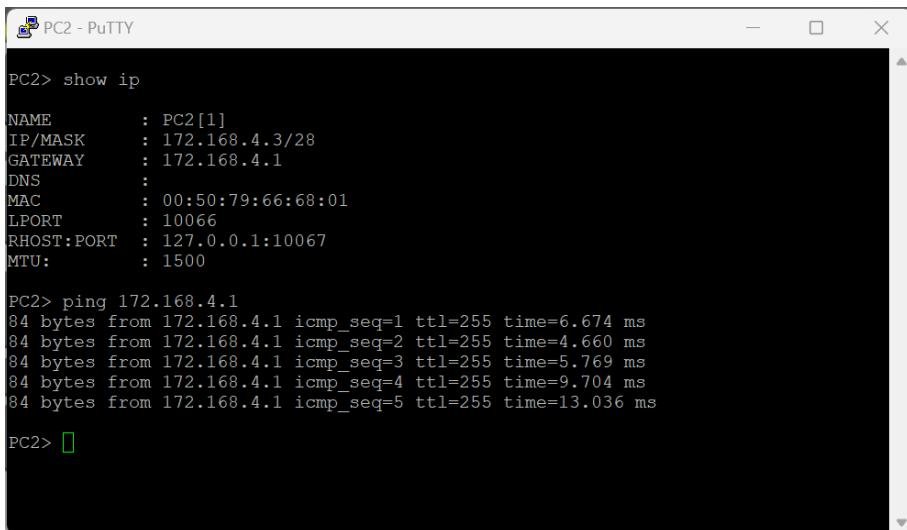
NAME      : PC1[1]
IP/MASK   : 172.168.1.2/28
GATEWAY   : 172.168.1.1
DNS       :
MAC       : 00:50:79:66:68:00
LPORT     : 10064
RHOST:PORT: 127.0.0.1:10065
MTU:      : 1500

PC1> ping 172.168.1.1
84 bytes from 172.168.1.1 icmp_seq=1 ttl=255 time=73.436 ms
84 bytes from 172.168.1.1 icmp_seq=2 ttl=255 time=3.396 ms
84 bytes from 172.168.1.1 icmp_seq=3 ttl=255 time=9.697 ms
84 bytes from 172.168.1.1 icmp_seq=4 ttl=255 time=3.403 ms
84 bytes from 172.168.1.1 icmp_seq=5 ttl=255 time=9.364 ms

PC1>
```

FIGURE 20 – Configuration de PC1

PC2



```
PC2 - PuTTY

PC2> show ip

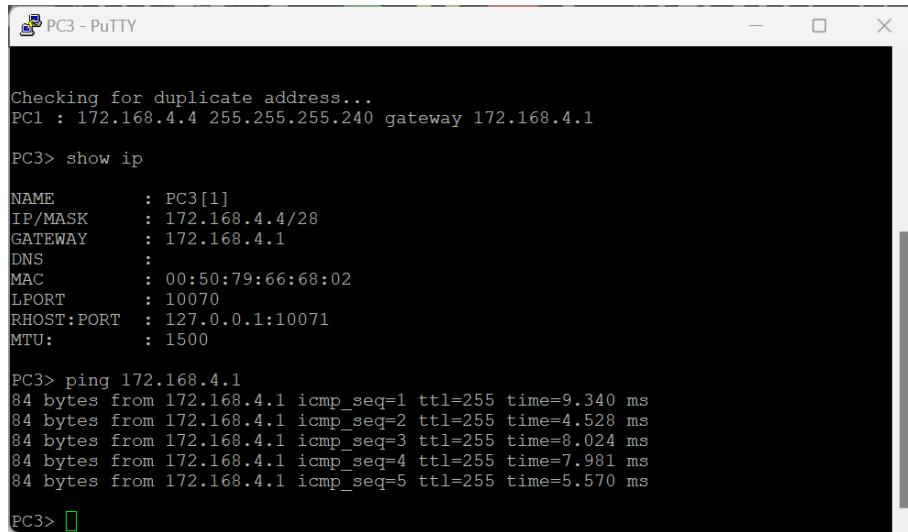
NAME      : PC2[1]
IP/MASK   : 172.168.4.3/28
GATEWAY   : 172.168.4.1
DNS       :
MAC       : 00:50:79:66:68:01
LPORT     : 10066
RHOST:PORT: 127.0.0.1:10067
MTU:      : 1500

PC2> ping 172.168.4.1
84 bytes from 172.168.4.1 icmp_seq=1 ttl=255 time=6.674 ms
84 bytes from 172.168.4.1 icmp_seq=2 ttl=255 time=4.660 ms
84 bytes from 172.168.4.1 icmp_seq=3 ttl=255 time=5.769 ms
84 bytes from 172.168.4.1 icmp_seq=4 ttl=255 time=9.704 ms
84 bytes from 172.168.4.1 icmp_seq=5 ttl=255 time=13.036 ms

PC2>
```

FIGURE 21 – Configuration de PC2

PC3



```
PC3 - PuTTY

Checking for duplicate address...
PC1 : 172.168.4.4 255.255.255.240 gateway 172.168.4.1

PC3> show ip

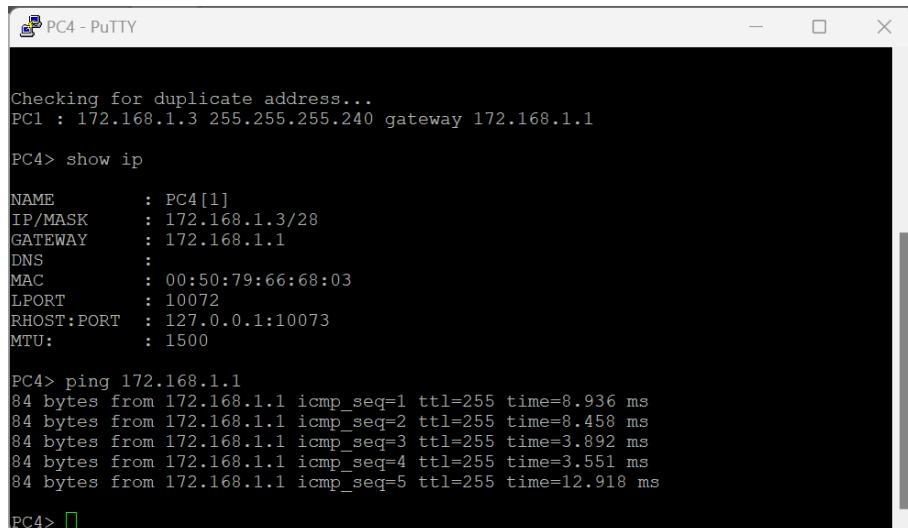
NAME      : PC3[1]
IP/MASK   : 172.168.4.4/28
GATEWAY   : 172.168.4.1
DNS       :
MAC       : 00:50:79:66:68:02
LPORT     : 10070
RHOST:PORT: 127.0.0.1:10071
MTU:      : 1500

PC3> ping 172.168.4.1
84 bytes from 172.168.4.1 icmp_seq=1 ttl=255 time=9.340 ms
84 bytes from 172.168.4.1 icmp_seq=2 ttl=255 time=4.528 ms
84 bytes from 172.168.4.1 icmp_seq=3 ttl=255 time=8.024 ms
84 bytes from 172.168.4.1 icmp_seq=4 ttl=255 time=7.981 ms
84 bytes from 172.168.4.1 icmp_seq=5 ttl=255 time=5.570 ms

PC3>
```

FIGURE 22 – Configuration de PC3

PC4



```
PC4 - PuTTY

Checking for duplicate address...
PC1 : 172.168.1.3 255.255.255.240 gateway 172.168.1.1

PC4> show ip

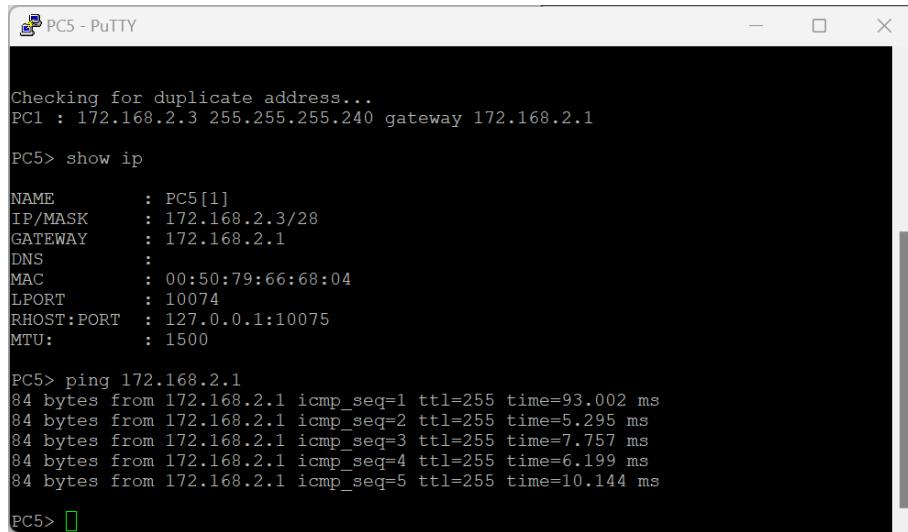
NAME      : PC4[1]
IP/MASK   : 172.168.1.3/28
GATEWAY   : 172.168.1.1
DNS       :
MAC       : 00:50:79:66:68:03
LPORT     : 10072
RHOST:PORT: 127.0.0.1:10073
MTU:      : 1500

PC4> ping 172.168.1.1
84 bytes from 172.168.1.1 icmp_seq=1 ttl=255 time=8.936 ms
84 bytes from 172.168.1.1 icmp_seq=2 ttl=255 time=8.458 ms
84 bytes from 172.168.1.1 icmp_seq=3 ttl=255 time=3.892 ms
84 bytes from 172.168.1.1 icmp_seq=4 ttl=255 time=3.551 ms
84 bytes from 172.168.1.1 icmp_seq=5 ttl=255 time=12.918 ms

PC4>
```

FIGURE 23 – Configuration de PC4

PC5



```
PC5 - PuTTY

Checking for duplicate address...
PC1 : 172.168.2.3 255.255.255.240 gateway 172.168.2.1

PC5> show ip

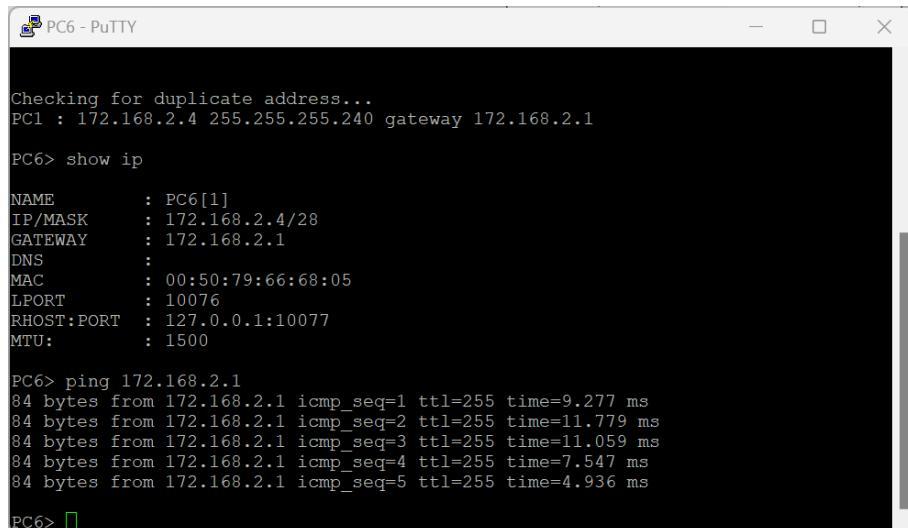
NAME      : PC5[1]
IP/MASK   : 172.168.2.3/28
GATEWAY   : 172.168.2.1
DNS       :
MAC       : 00:50:79:66:68:04
LPORT     : 10074
RHOST:PORT: 127.0.0.1:10075
MTU:      : 1500

PC5> ping 172.168.2.1
84 bytes from 172.168.2.1 icmp_seq=1 ttl=255 time=93.002 ms
84 bytes from 172.168.2.1 icmp_seq=2 ttl=255 time=5.295 ms
84 bytes from 172.168.2.1 icmp_seq=3 ttl=255 time=7.757 ms
84 bytes from 172.168.2.1 icmp_seq=4 ttl=255 time=6.199 ms
84 bytes from 172.168.2.1 icmp_seq=5 ttl=255 time=10.144 ms

PC5>
```

FIGURE 24 – Configuration de PC5

PC6



```
PC6 - PuTTY

Checking for duplicate address...
PC1 : 172.168.2.4 255.255.255.240 gateway 172.168.2.1

PC6> show ip

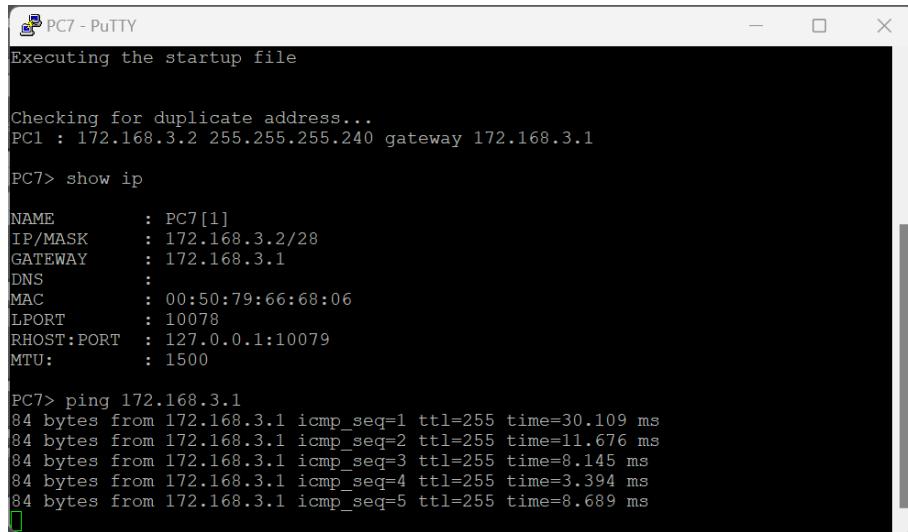
NAME      : PC6[1]
IP/MASK   : 172.168.2.4/28
GATEWAY   : 172.168.2.1
DNS       :
MAC       : 00:50:79:66:68:05
LPORT     : 10076
RHOST:PORT: 127.0.0.1:10077
MTU:      : 1500

PC6> ping 172.168.2.1
84 bytes from 172.168.2.1 icmp_seq=1 ttl=255 time=9.277 ms
84 bytes from 172.168.2.1 icmp_seq=2 ttl=255 time=11.779 ms
84 bytes from 172.168.2.1 icmp_seq=3 ttl=255 time=11.059 ms
84 bytes from 172.168.2.1 icmp_seq=4 ttl=255 time=7.547 ms
84 bytes from 172.168.2.1 icmp_seq=5 ttl=255 time=4.936 ms

PC6>
```

FIGURE 25 – Configuration de PC6

PC7



```
PC7 - PuTTY
Executing the startup file

Checking for duplicate address...
PC1 : 172.168.3.2 255.255.255.240 gateway 172.168.3.1

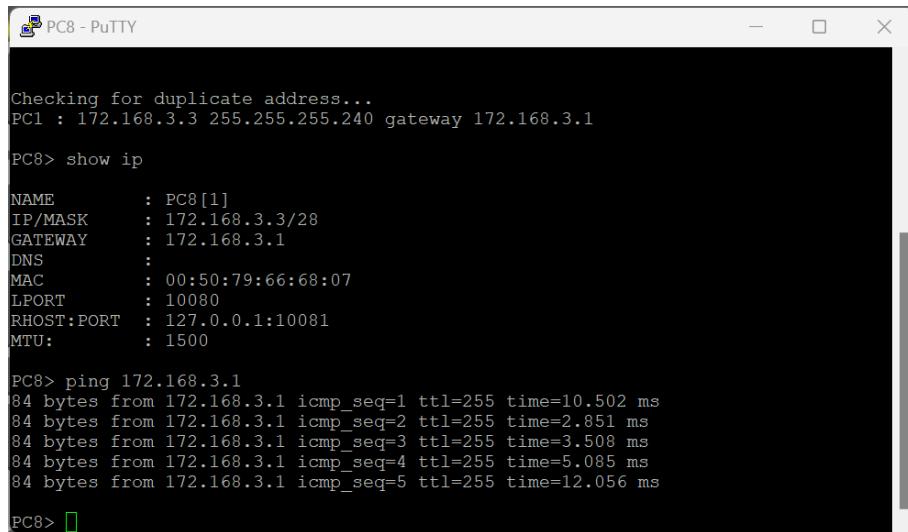
PC7> show ip

NAME      : PC7[1]
IP/MASK   : 172.168.3.2/28
GATEWAY   : 172.168.3.1
DNS       :
MAC       : 00:50:79:66:68:06
LPORT     : 10078
RHOST:PORT : 127.0.0.1:10079
MTU:      : 1500

PC7> ping 172.168.3.1
84 bytes from 172.168.3.1 icmp_seq=1 ttl=255 time=30.109 ms
84 bytes from 172.168.3.1 icmp_seq=2 ttl=255 time=11.676 ms
84 bytes from 172.168.3.1 icmp_seq=3 ttl=255 time=8.145 ms
84 bytes from 172.168.3.1 icmp_seq=4 ttl=255 time=3.394 ms
84 bytes from 172.168.3.1 icmp_seq=5 ttl=255 time=8.689 ms
```

FIGURE 26 – Configuration de PC7

PC8



```
PC8 - PuTTY
Executing the startup file

Checking for duplicate address...
PC1 : 172.168.3.3 255.255.255.240 gateway 172.168.3.1

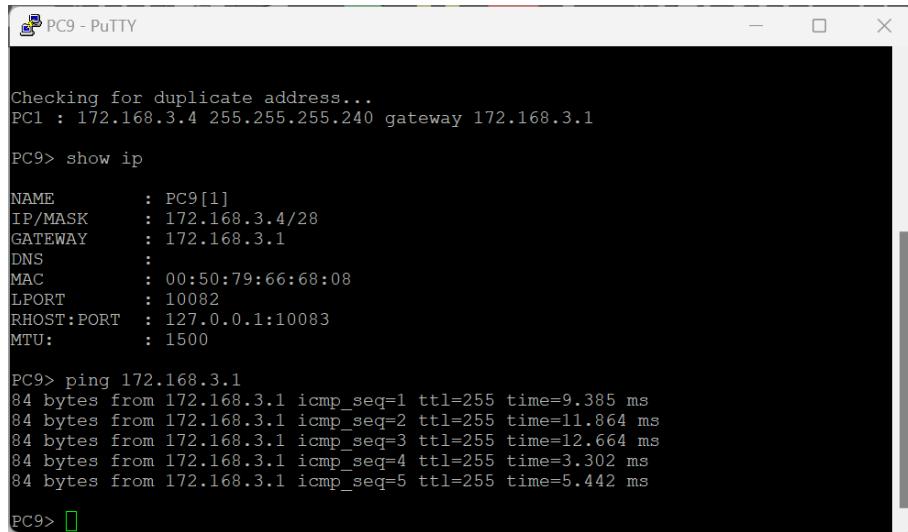
PC8> show ip

NAME      : PC8[1]
IP/MASK   : 172.168.3.3/28
GATEWAY   : 172.168.3.1
DNS       :
MAC       : 00:50:79:66:68:07
LPORT     : 10080
RHOST:PORT : 127.0.0.1:10081
MTU:      : 1500

PC8> ping 172.168.3.1
84 bytes from 172.168.3.1 icmp_seq=1 ttl=255 time=10.502 ms
84 bytes from 172.168.3.1 icmp_seq=2 ttl=255 time=2.851 ms
84 bytes from 172.168.3.1 icmp_seq=3 ttl=255 time=3.508 ms
84 bytes from 172.168.3.1 icmp_seq=4 ttl=255 time=5.085 ms
84 bytes from 172.168.3.1 icmp_seq=5 ttl=255 time=12.056 ms
```

FIGURE 27 – Configuration de PC8

PC9



```
PC9 - PuTTY

Checking for duplicate address...
PC1 : 172.168.3.4 255.255.255.240 gateway 172.168.3.1

PC9> show ip

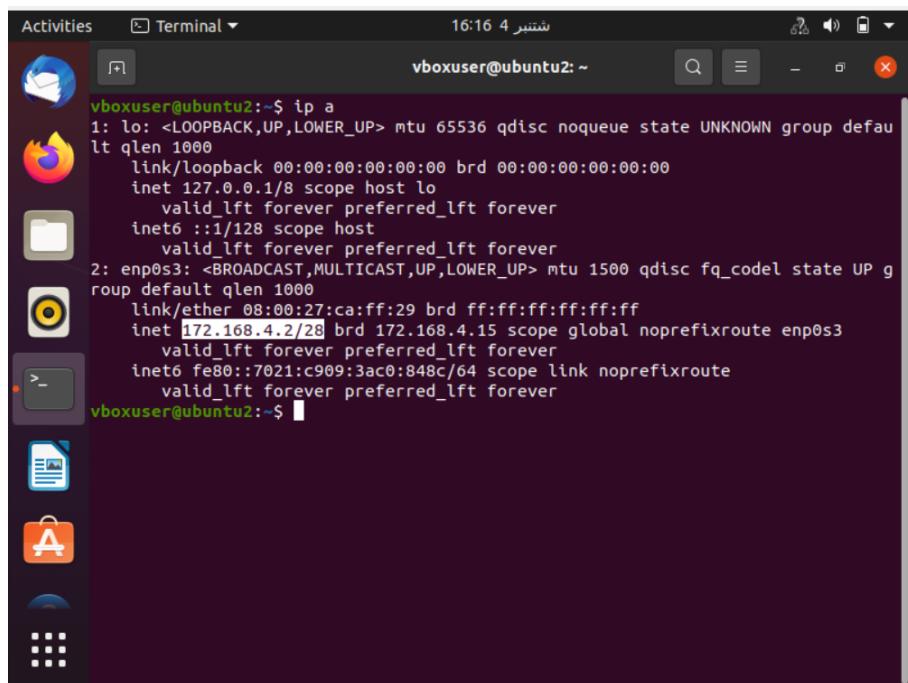
NAME      : PC9[1]
IP/MASK   : 172.168.3.4/28
GATEWAY   :
DNS       :
MAC       : 00:50:79:66:68:08
LPORT     : 10082
RHOST:PORT: 127.0.0.1:10083
MTU:      : 1500

PC9> ping 172.168.3.1
84 bytes from 172.168.3.1 icmp_seq=1 ttl=255 time=9.385 ms
84 bytes from 172.168.3.1 icmp_seq=2 ttl=255 time=11.864 ms
84 bytes from 172.168.3.1 icmp_seq=3 ttl=255 time=12.664 ms
84 bytes from 172.168.3.1 icmp_seq=4 ttl=255 time=3.302 ms
84 bytes from 172.168.3.1 icmp_seq=5 ttl=255 time=5.442 ms

PC9>
```

FIGURE 28 – Configuration de PC9

Ubuntu VM



```
Activities Terminal ١٦:١٦ شنبه ٤
vboxuser@ubuntu2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ca:ff:29 brd ff:ff:ff:ff:ff:ff
    inet 172.168.4.2/28 brd 172.168.4.15 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::7021:c909:3ac0:848c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
vboxuser@ubuntu2:~$
```

FIGURE 29 – Configuration de Ununtu VM

Linux VM

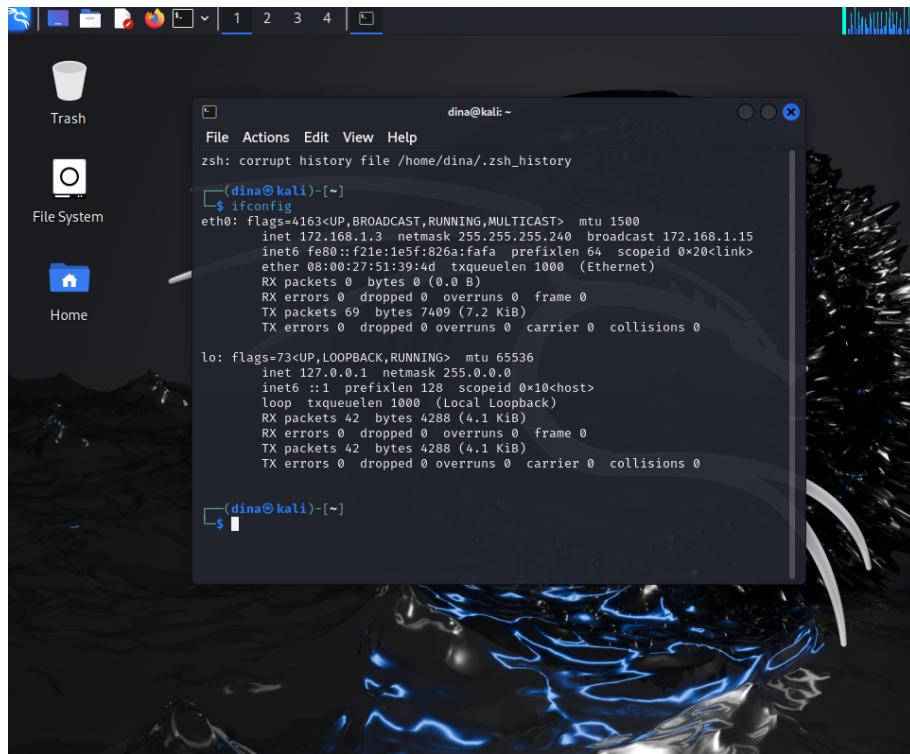


FIGURE 30 – Configuration de Linux VM

2. Configuration des Routeurs

Routeur 1

```
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 172.168.1.1 255.255.255.240
R1#
*Aug 25 13:47:37.127: %SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 172.168.1.1 255.255.255.240
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
*Aug 25 13:49:03.875: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Aug 25 13:49:04.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#int s1/0
R1(config-if)#ip address 13.0.0.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#int s1
*Aug 25 13:49:48.727: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config)#int s1
*Aug 25 13:49:49.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config)#int s1/1
R1(config-if)#ip address 12.0.0.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
*Aug 25 13:50:17.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R1(config-if)#exit
R1(config)#do wr
*Aug 25 13:50:19.311: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R1(config)#do wr
Building configuration...
[OK]
R1(config)#

```

```
*Aug 26 18:35:21.679: %LINK-5-CHANGED: Interface Serial1/2, changed state to administratively down
*Aug 26 18:35:21.707: %LINK-5-CHANGED: Interface Serial1/3, changed state to administratively down
*Aug 26 18:35:21.943: %OSPF-5-ADJCHG: Process 1, Nbr 172.168.3.1 on Serial1/1 from LOADING to FULL, Loading Done
R1#
R1#
R1#
R1#
R1#show ip int brief
Interface          IP-Address      OK? Method Status      Prot
octl
FastEthernet0/0     172.168.1.1    YES  NVRAM   up           up
Serial1/0          13.0.0.1       YES  NVRAM   up           up
Serial1/1          12.0.0.1       YES  NVRAM   up           up

```

FIGURE 31 – Configuration de R1

Routeur 2

```
R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip address 172.168.2.1 255.255.255.240
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
*Aug 25 13:45:51.851: %LINK-3-UPDOWN: Interface FastEthernet0/
0, changed state to up
*Aug 25 13:45:52.851: %LINEPROTO-5-UPDOWN: Line protocol on In-
terface FastEthernet0/0, changed state to up
R2(config)#int s1/1
R2(config-if)#ip address 10.0.0.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#int s
*Aug 25 13:46:15.907: %LINK-3-UPDOWN: Interface Serial1/1, cha-
nged state to up
R2(config)#int s1
*Aug 25 13:46:16.911: %LINEPROTO-5-UPDOWN: Line protocol on In-
terface Serial1/1, changed state to up
R2(config)#int s1/2
R2(config-if)#ip address 13.0.0.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#do wr
Building configuration...
```

```
R2#show ip int brief
Interface          IP-Address      OK? Method Status
      Protocol
FastEthernet0/0    172.168.2.1    YES manual up
                  up
Serial1/0          unassigned     YES unset  administ
relatively down   down
Serial1/1          10.0.0.1       YES manual up
                  down
Serial1/2          13.0.0.2       YES manual up
                  up
Serial1/3          unassigned     YES unset  administ
relatively down   down
R2#
```

FIGURE 32 – Configuration de R2

Routeur 3

```
R3#enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/0
R3(config-if)#ip address 172.168.3.1 255.255.255.240
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#int s1/0
R3(config-if)#ip address 11.0.0.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#int
*Aug 25 13:51:11.311: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R3(config)#int s1
*Aug 25 13:51:12.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R3(config)#int s1/2
R3(config-if)#ip address 12.0.0.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
*Aug 25 13:51:36.115: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R3(config-if)#exit
R3(config)#do
*Aug 25 13:51:37.607: %LINK-3-UPDOWN: Interface Serial1/2, changed state to up
R3(config)#do wr
*Aug 25 13:51:38.611: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed state to up
R3(config)#do wr
Building configuration...
[OK]
```

```
R3#show ip int brief
Interface          IP-Address      OK? Method Status
                  Protocol
FastEthernet0/0    172.168.3.1    YES manual up
                   up
Serial1/0          11.0.0.1       YES manual up
                   down
Serial1/1          unassigned     YES unset  adminis
tratively down down
Serial1/2          12.0.0.2       YES manual up
                   up
Serial1/3          unassigned     YES unset  adminis
tratively down down
R3#
```

FIGURE 33 – Configuration de R3

Routeur 4

```
R4#enable
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#int f0/0
R4(config-if)#ip address 172.168.4.1 255.255.255.240
R4(config-if)#no shut
R4(config-if)#
*Aug 25 13:52:30.011: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Aug 25 13:52:31.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R4(config-if)#exit
R4(config)#int s1/0
R4(config-if)#ip address 10.0.0.2 255.255.255.252
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#int s1
*Aug 25 13:52:58.711: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R4(config)#int s1/1
*Aug 25 13:52:59.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R4(config)#int s1/1
R4(config-if)#ip address 11.0.0.2 255.255.255.252
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#do w
*Aug 25 13:53:20.711: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R4(config)#do wr
Building configuration...
```

```
R4#show ip int brief
Interface          IP-Address      OK? Method Status       Prot
octl
FastEthernet0/0    172.168.4.1    YES manual up        up
Serial1/0          10.0.0.2       YES manual up        up
Serial1/1          11.0.0.2       YES manual up        up
Serial1/2          unassigned     YES unset administratively down down
Serial1/3          unassigned     YES unset administratively down down
R4#
```

FIGURE 34 – Configuration de R4

3. Configuration de l'Interface Loopback0

```
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
```

FIGURE 35 – Configuration de l'Interface Loopback0

L'interface Loopback0, configurée avec l'adresse IP 1.1.1.1 et le masque de sous-réseau 255.255.255.255, joue un rôle crucial dans la stabilité et la gestion des routeurs dans un réseau. Contrairement aux interfaces physiques, l'interface

Loopback est une interface virtuelle qui reste toujours active tant que le routeur est en fonctionnement. Cela la rend particulièrement utile pour plusieurs raisons :

- **Identification Stable** : L'adresse IP attribuée à Loopback0 fournit une identification stable et unique pour le routeur, indépendamment des changements ou des pannes des interfaces physiques. Elle est souvent utilisée comme adresse de source pour les protocoles de routage, assurant ainsi une identification constante du routeur dans le réseau.
- **Test et Dépannage** : L'interface Loopback est utilisée pour les tests et le dépannage. Comme elle est toujours opérationnelle, elle permet de tester la connectivité et la communication du routeur même si ses interfaces physiques sont en panne.
- **Routage et Protocoles** : Dans les protocoles de routage comme OSPF, l'adresse IP de l'interface Loopback est souvent utilisée comme identifiant de routeur (Router ID). Cela permet de maintenir une stabilité dans la désignation du routeur, même en cas de changement dans les interfaces physiques.
- **Gestion Réseau** : L'utilisation de l'adresse IP Loopback dans les configurations VPN ou pour les communications inter-routeurs assure une gestion plus efficace et une meilleure fiabilité des opérations de routage.

IV. Configuration de VPN-IPSec

Dans cette section, je décris la mise en place du VPN-IPSec pour sécuriser la communication entre les deux machines virtuelles (VMs). Le VPN-IPSec est une solution de sécurité qui chiffre le trafic réseau pour assurer la confidentialité et l'intégrité des données échangées.

1. Choix des Algorithmes de Chiffrement

Dans cette section, je configure les algorithmes de chiffrement, de hachage, et le groupe Diffie-Hellman pour sécuriser les communications :

```

R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr ?
  3des Three key triple DES
  aes AES - Advanced Encryption Standard.
  des DES - Data Encryption Standard (56 bit key
s).

R1(config-isakmp)#encr aes
R1(config-isakmp)#hash ?
  md5 Message Digest 5
  sha Secure Hash Standard

R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group ?
  1 Diffie-Hellman group 1 (768 bit)
  14 Diffie-Hellman group 14 (2048 bit)
  15 Diffie-Hellman group 15 (3072 bit)
  16 Diffie-Hellman group 16 (4096 bit)
  2 Diffie-Hellman group 2 (1024 bit)
  5 Diffie-Hellman group 5 (1536 bit)

R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 86400

```

FIGURE 36 – Configuration VPN-IPSec de R1

- **Commande : crypto isakmp policy 10**

Cette commande crée une politique ISAKMP avec une priorité de 10. ISAKMP est responsable de la négociation des paramètres de sécurité entre les pairs VPN.

ISAKMP est un protocole utilisé pour établir des associations de sécurité (SA) et gérer les clés cryptographiques entre les pairs dans un réseau VPN. Cette commande commence la configuration de la politique ISAKMP avec le numéro de priorité 10. Si plusieurs politiques sont définies, celles avec le numéro de priorité le plus bas seront préférées.

- **Commande : encr aes**

Le chiffrement AES (Advanced Encryption Standard) est sélectionné pour garantir la confidentialité des données échangées.

AES (Advanced Encryption Standard) est un algorithme de chiffrement utilisé pour sécuriser les données en les transformant en un format illisible sans la clé de déchiffrement appropriée.

- **Commande : hash md5**

L'algorithme MD5 est choisi pour assurer l'intégrité des données, en générant une empreinte numérique pour chaque message.

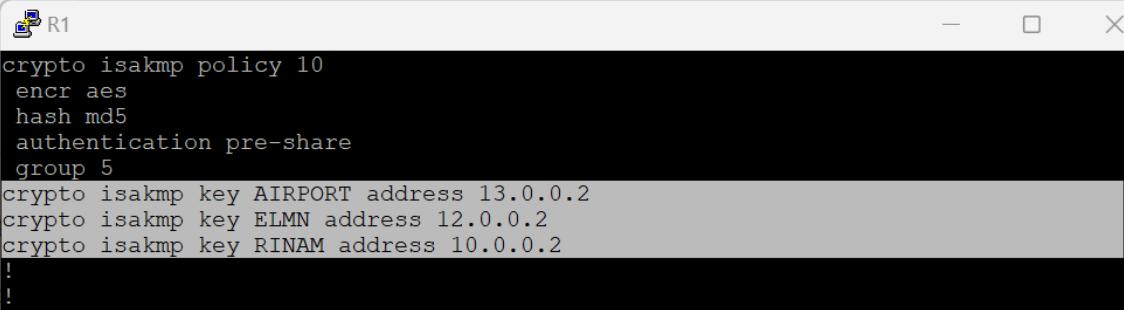
MD5 (Message Digest 5) est un algorithme de hachage qui prend des données et les condense en une empreinte numérique de 128 bits. Il est utilisé pour assurer l'intégrité des données en vérifiant que celles-ci n'ont pas été altérées.

- **Commande : group 5**

Le groupe Diffie-Hellman 5 (1536 bits) est sélectionné pour la génération des clés partagées de manière sécurisée.

Diffie-Hellman est un protocole cryptographique permettant d'échanger des clés de manière sécurisée sur un canal non sécurisé. Le groupe 5 (1536 bits) offre un bon compromis entre sécurité et performance pour la génération des clés.

2. Définition des Clés de Sécurité



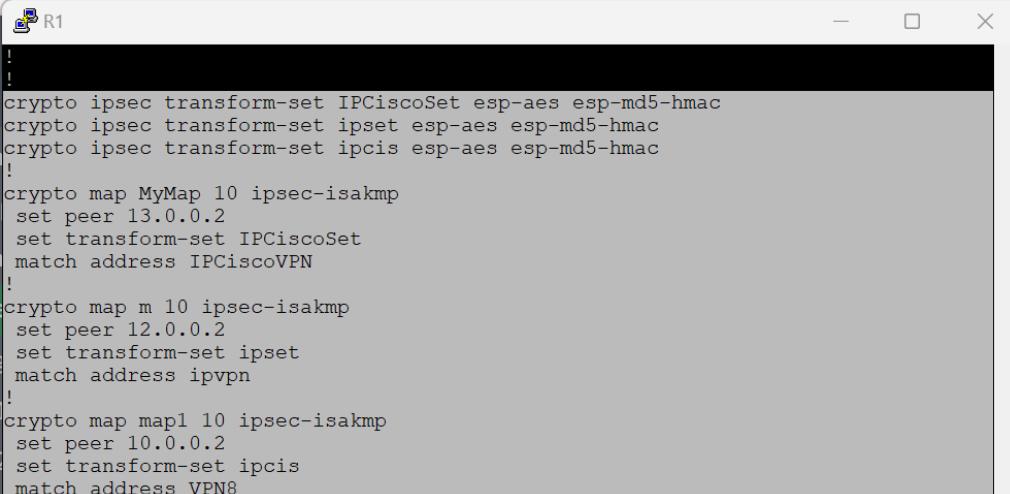
```
!R1
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 5
crypto isakmp key AIRPORT address 13.0.0.2
crypto isakmp key ELMN address 12.0.0.2
crypto isakmp key RINAM address 10.0.0.2
!
```

FIGURE 37 – Configuration VPN-IPSec de R1

Cette section se concentre sur la définition des clés prépartagées utilisées pour l'authentification entre les pairs VPN :

- **crypto isakmp key AIRPORT address 13.0.0.2** : Cette commande configure la clé pré-partagée (pre-shared key) pour le pair ayant l'adresse IP 13.0.0.2. Le mot clé AIRPORT est la clé partagée utilisée pour établir la connexion sécurisée avec ce pair. Dans ce contexte, l'adresse 13.0.0.2 correspond au routeur R2.
- **crypto isakmp key ELMN address 12.0.0.2** : cette commande configure la clé pré-partagée pour le pair ayant l'adresse IP 12.0.0.2, avec la clé partagée ELMN. Ici, l'adresse 12.0.0.2 correspond au routeur R3.
- **crypto isakmp key RINAM address 10.0.0.2** : De la même manière, cette commande configure la clé pré-partagée pour le pair ayant l'adresse IP 10.0.0.2, avec la clé partagée RINAM. Ici, l'adresse 10.0.0.2 correspond au routeur R4.

3. Configuration des Politiques de Sécurité



```
!R1
!
!
crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac
crypto ipsec transform-set ipset esp-aes esp-md5-hmac
crypto ipsec transform-set ipcis esp-aes esp-md5-hmac
!
crypto map MyMap 10 ipsec-isakmp
  set peer 13.0.0.2
  set transform-set IPCiscoSet
  match address IPCiscoVPN
!
crypto map m 10 ipsec-isakmp
  set peer 12.0.0.2
  set transform-set ipset
  match address ipvpn
!
crypto map map1 10 ipsec-isakmp
  set peer 10.0.0.2
  set transform-set ipcis
  match address VPN8
```

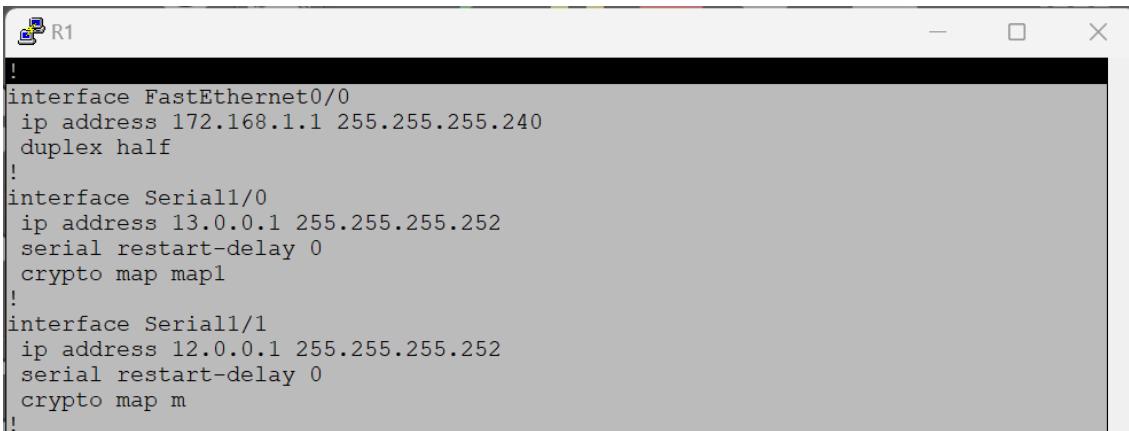
FIGURE 38 – Configuration VPN-IPSec de R1

Cette section porte sur la configuration des ensembles de transformation IPsec, du mode tunnel, et de l'application de ces configurations à une carte crypto :

- **crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac** : Cette commande crée un ensemble de transformations (transform-set) nommé **IPCiscoSet**, qui spécifie les protocoles de sécurité utilisés dans la phase 2 d'IPsec. AES est utilisé pour le chiffrement, et MD5 est utilisé pour l'intégrité avec HMAC. Cet ensemble de transformations définit les paramètres de sécurité pour les connexions IPsec.
- **crypto ipsec transform-set ipset esp-aes esp-md5-hmac** : Un autre ensemble de transformations nommé **ipset** est créé avec les mêmes algorithmes de sécurité. Cet ensemble peut être utilisé pour différents tunnels IPsec, fourni ainsi une certaine flexibilité dans les configurations.
- **crypto map MyMap 10 ipsec-isakmp** : Cela crée une carte de crypto (crypto map) nommée **MyMap**, associée à la politique ISAKMP définie. Le numéro **10** est la séquence de la carte, indiquant l'ordre dans lequel elle est appliquée. Cette carte est utilisée pour associer le trafic réseau aux paramètres de sécurité spécifiés.
- **set peer 13.0.0.2** : Le pair à l'adresse **13.0.0.2** est spécifié comme destination pour ce tunnel IPsec. Cela signifie que tout le trafic associé à cette carte de crypto sera envoyé vers le routeur R2.
- **set transform-set IPCiscoSet** : La carte de crypto utilise l'ensemble de transformations **IPCiscoSet** pour ce tunnel. Cela signifie que les paramètres de sécurité définis dans **IPCiscoSet** (chiffrement AES et intégrité MD5) seront appliqués au trafic traversant ce tunnel.
- **match address IPCiscoVPN** : Cette commande associe la carte de crypto à une liste d'accès (access list) nommée **IPCiscoVPN**, qui définit le trafic qui sera chiffré. Seul le trafic correspondant aux critères de cette liste d'accès sera inclus dans le tunnel IPsec.
- **crypto map m 10 ipsec-isakmp** : Une autre carte de crypto est créée, nommée **m**, pour une connexion IPsec avec l'adresse **12.0.0.2**. Cette carte fonctionne de manière similaire à la carte **MyMap**, mais est utilisée pour un autre tunnel.
- **set peer 12.0.0.2** : Le pair à l'adresse **12.0.0.2** est spécifié comme destination pour ce tunnel IPsec. Cela signifie que ce tunnel IPsec sera établi avec le routeur R3.
- **set transform-set ipset** : Cette carte de crypto utilise l'ensemble de transformations **ipset** pour ce tunnel, qui utilise également AES pour le chiffrement et MD5 pour l'intégrité.
- **match address ipvpn** : Cette commande associe la carte de crypto à une liste d'accès nommée **ipvpn**, qui définit le trafic qui sera chiffré pour ce tunnel. Comme pour **IPCiscoVPN**, seul le trafic correspondant à cette liste sera chiffré dans le tunnel IPsec.
- **crypto map map1 10 ipsec-isakmp** : Crée une crypto map nommée **map1** avec une priorité 10.
- **set peer 10.0.0.2** : Spécifie l'adresse IP du routeur distant, **10.0.0.2**, qui correspond à R4.

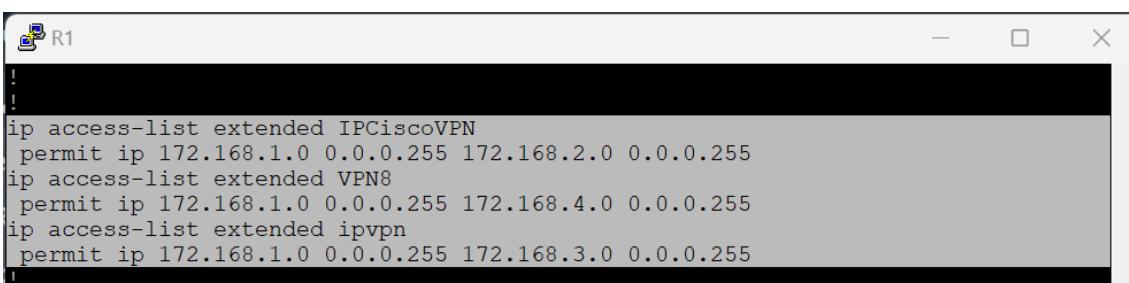
- **set transform-set ipc1s** : Associe le **transform-set ipc1s** pour ce tunnel VPN.
- **match address VPN8** : Indique que cette crypto map va chiffrer le trafic défini par la liste d'accès VPN8.

4. Configuration des Interfaces Et Listes d'Accés



```

R1
interface FastEthernet0/0
 ip address 172.168.1.1 255.255.255.240
 duplex half
!
interface Serial1/0
 ip address 13.0.0.1 255.255.255.252
 serial restart-delay 0
 crypto map map1
!
interface Serial1/1
 ip address 12.0.0.1 255.255.255.252
 serial restart-delay 0
 crypto map m
!
```

```

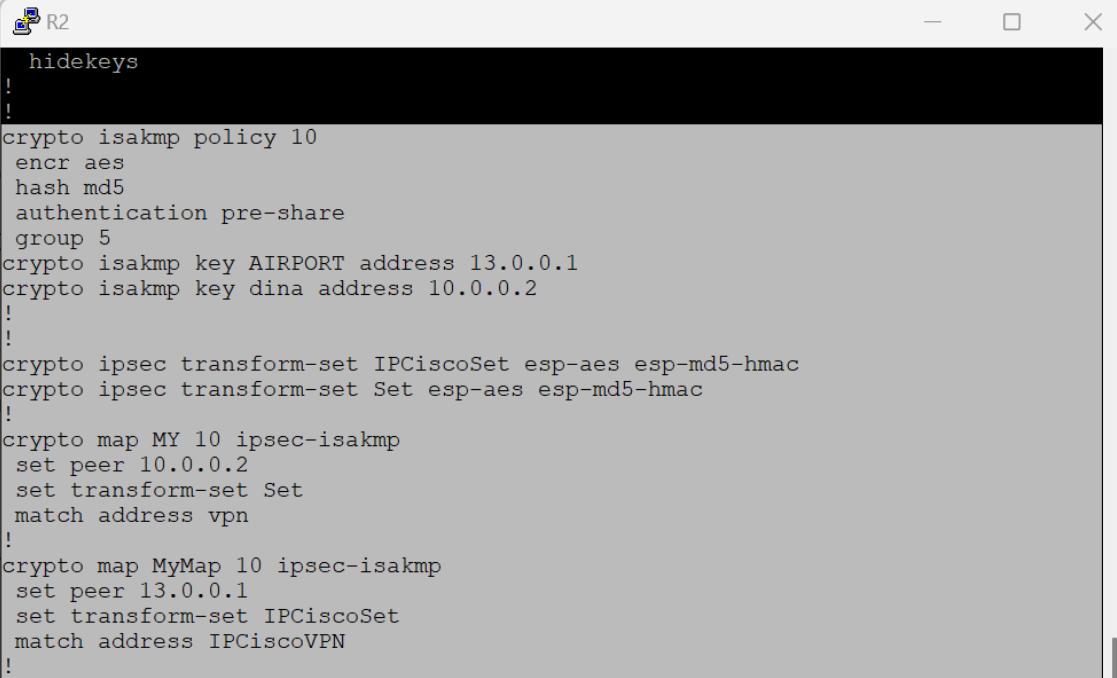
R1
ip access-list extended IPCiscoVPN
 permit ip 172.168.1.0 0.0.0.255 172.168.2.0 0.0.0.255
ip access-list extended VPN8
 permit ip 172.168.1.0 0.0.0.255 172.168.4.0 0.0.0.255
ip access-list extended ipvpn
 permit ip 172.168.1.0 0.0.0.255 172.168.3.0 0.0.0.255
!
```

FIGURE 39 – Configuration VPN-IPSec de R1

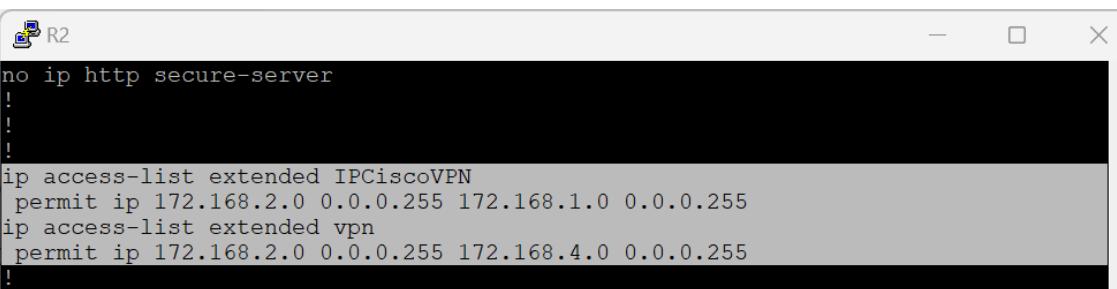
- **ip access-list extended IPCiscoVPN** : Cette commande crée une liste d'accès étendue nommée IPCiscoVPN. Une liste d'accès (ACL) est utilisée pour filtrer le trafic réseau en spécifiant quelles adresses IP sont autorisées à communiquer entre elles.
- **permit ip 172.168.1.0 0.0.0.255 172.168.2.0 0.0.0.255** : Cette règle permet le trafic entre les sous-réseaux 172.168.1.0/24 et 172.168.2.0/24. Le 0.0.0.255 est un masque générique qui correspond à un sous-réseau /24.
- **ip access-list extended ipvpn** : Une autre ACL étendue est créée, nommée ipvpn, pour gérer un trafic différent.
- **permit ip 172.168.1.0 0.0.0.255 172.168.3.0 0.0.0.255** : Cette règle permet le trafic entre les sous-réseaux 172.168.1.0/24 et 172.168.3.0/24.
- **ip access-list extended VPN8** : Crée une ACL étendue nommée VPN8.
- **permit ip 172.168.1.0 0.0.0.255 172.168.4.0 0.0.0.255** : Cette règle permet le trafic IP entre les sous-réseaux 172.168.1.0/24 et 172.168.4.0/24.

Pour les autres routeurs voici leur configurations complètes :

VPN-IPSEC de R2



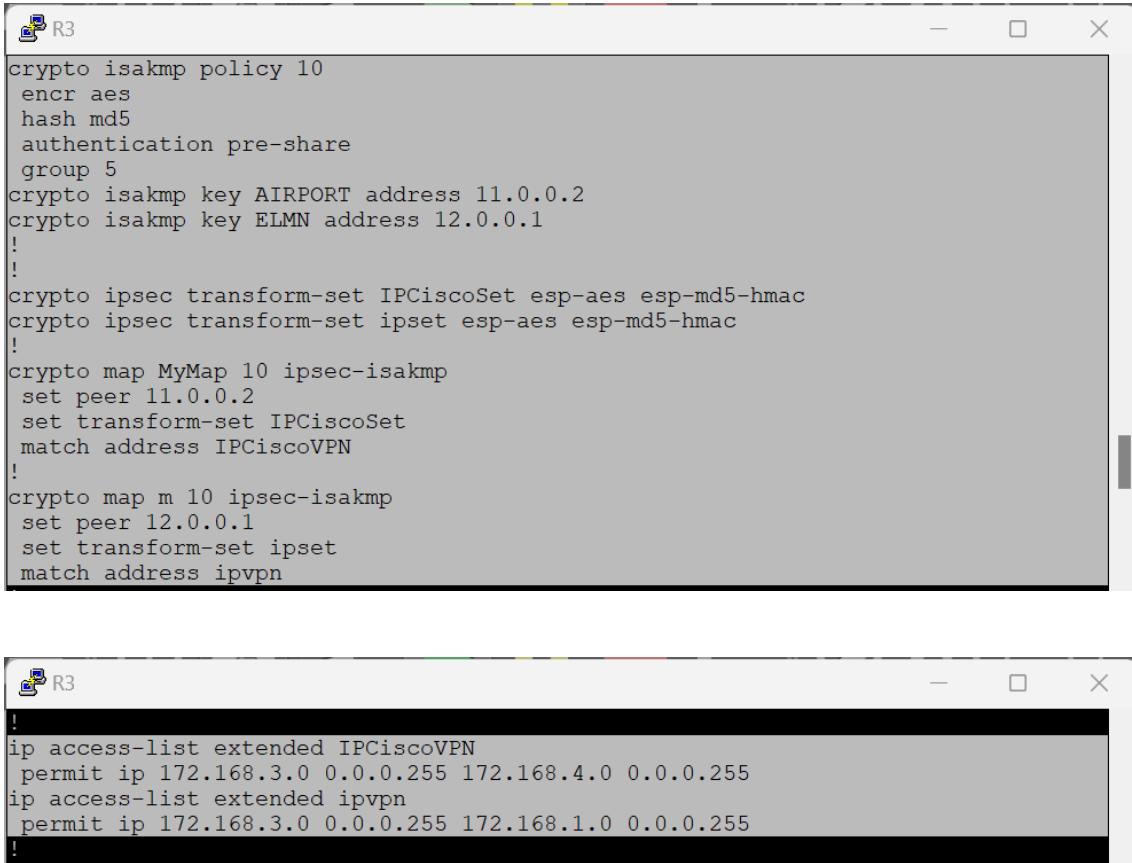
```
R2
hidekeys
!
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 5
crypto isakmp key AIRPORT address 13.0.0.1
crypto isakmp key dina address 10.0.0.2
!
crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac
crypto ipsec transform-set Set esp-aes esp-md5-hmac
!
crypto map MY 10 ipsec-isakmp
  set peer 10.0.0.2
  set transform-set Set
  match address vpn
!
crypto map MyMap 10 ipsec-isakmp
  set peer 13.0.0.1
  set transform-set IPCiscoSet
  match address IPCiscoVPN
!
```

```
R2
no ip http secure-server
!
!
ip access-list extended IPCiscoVPN
  permit ip 172.168.2.0 0.0.0.255 172.168.1.0 0.0.0.255
ip access-list extended vpn
  permit ip 172.168.2.0 0.0.0.255 172.168.4.0 0.0.0.255
!
```

FIGURE 40 – Configuration VPN-IPSEC de R2

VPN-IPSEC de R3



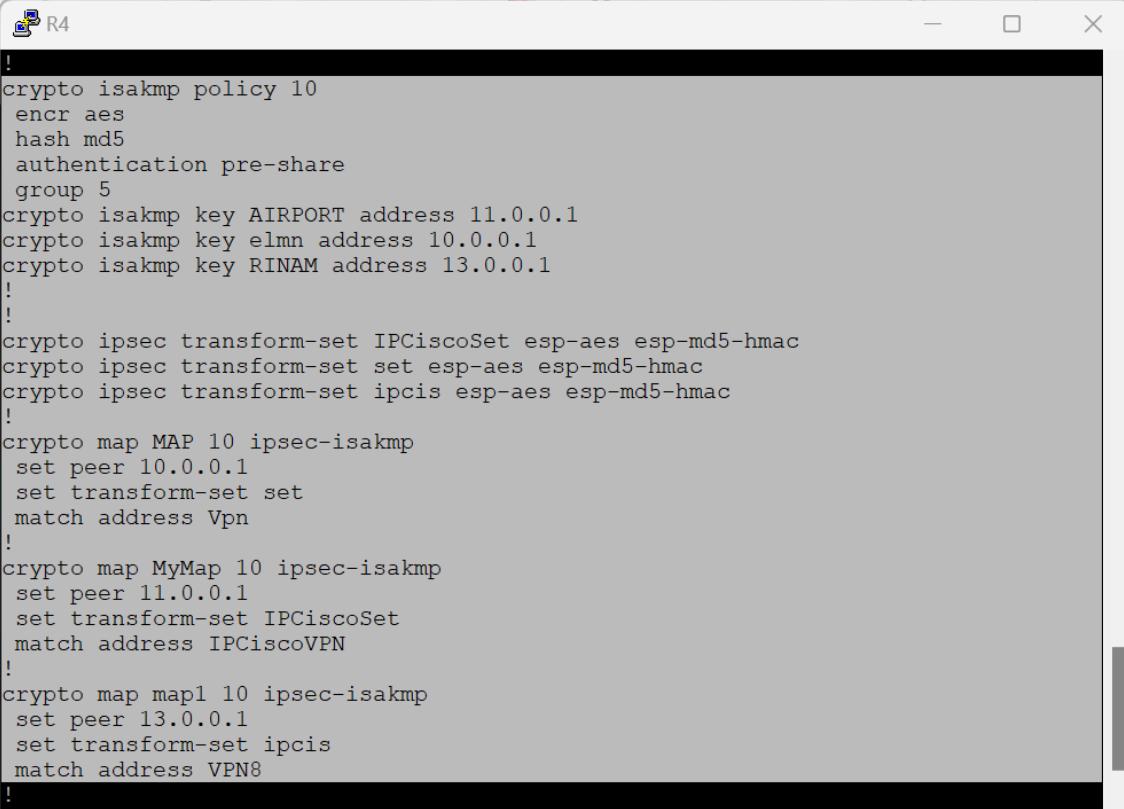
The image shows two terminal windows side-by-side, both titled 'R3'. The left window displays the configuration for a VPN-IPSEC setup. It includes sections for ISAKMP policies (policy 10), IPsec transform sets (IPCiscoSet and ipset), and crypto maps (MyMap and m). The right window shows the configuration of IP access lists (extended ACLs) for the VPN.

```
crypto isakmp policy 10
  encr aes
  hash md5
  authentication pre-share
  group 5
crypto isakmp key AIRPORT address 11.0.0.2
crypto isakmp key ELMN address 12.0.0.1
!
!
crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac
crypto ipsec transform-set ipset esp-aes esp-md5-hmac
!
crypto map MyMap 10 ipsec-isakmp
  set peer 11.0.0.2
  set transform-set IPCiscoSet
  match address IPCiscoVPN
!
crypto map m 10 ipsec-isakmp
  set peer 12.0.0.1
  set transform-set ipset
  match address ipvpn

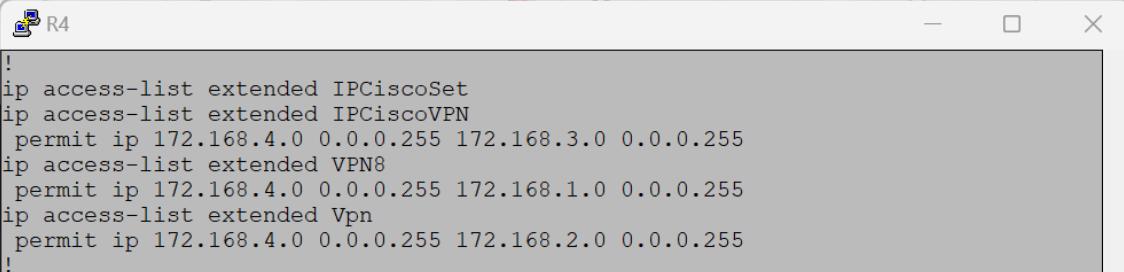
ip access-list extended IPCiscoVPN
  permit ip 172.168.3.0 0.0.0.255 172.168.4.0 0.0.0.255
ip access-list extended ipvpn
  permit ip 172.168.3.0 0.0.0.255 172.168.1.0 0.0.0.255
!
```

FIGURE 41 – Configuration VPN-IPSEC de R3

VPN-IPSEC de R4



```
!crypto isakmp policy 10
encr aes
hash md5
authentication pre-share
group 5
crypto isakmp key AIRPORT address 11.0.0.1
crypto isakmp key elmn address 10.0.0.1
crypto isakmp key RINAM address 13.0.0.1
!
!
crypto ipsec transform-set IPCiscoSet esp-aes esp-md5-hmac
crypto ipsec transform-set set esp-aes esp-md5-hmac
crypto ipsec transform-set ipcis esp-aes esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 10.0.0.1
set transform-set set
match address Vpn
!
crypto map MyMap 10 ipsec-isakmp
set peer 11.0.0.1
set transform-set IPCiscoSet
match address IPCiscoVPN
!
crypto map map1 10 ipsec-isakmp
set peer 13.0.0.1
set transform-set ipcis
match address VPN8
!
```



```
!
ip access-list extended IPCiscoSet
ip access-list extended IPCiscoVPN
permit ip 172.168.4.0 0.0.0.255 172.168.3.0 0.0.0.255
ip access-list extended VPN8
permit ip 172.168.4.0 0.0.0.255 172.168.1.0 0.0.0.255
ip access-list extended Vpn
permit ip 172.168.4.0 0.0.0.255 172.168.2.0 0.0.0.255
!
```

FIGURE 42 – Configuration VPN-IPSEC de R4

5. Utilisation d'ISPF



```
!
router ospf 1
log-adjacency-changes
network 1.1.1.1 0.0.0.0 area 0
network 12.0.0.0 0.0.0.3 area 0
network 13.0.0.0 0.0.0.3 area 0
!
```

FIGURE 43 – Configuration d'ISPF

Dans ma simulation, j'ai configuré OSPF (Open Shortest Path First) sur les routeurs en utilisant des commandes spécifiques pour établir des adjacences et définir

les réseaux. La commande `router ospf 1` initie le processus de configuration OSPF et assigne un identifiant de processus à l'instance OSPF. En ajoutant la commande `log adjacency-changes`, je m'assure que les changements dans les adjacences OSPF sont enregistrés, ce qui facilite le suivi des modifications dans la topologie du réseau. Les commandes `network` spécifient les réseaux inclus dans le processus OSPF, avec les masques de sous-réseau inversés, pour chaque réseau, en les associant à une aire OSPF spécifique (dans ce cas, l'aire 0). Par exemple, `network 1.1.1.1 0.0.0.0 area 0` indique que le réseau 1.1.1.1 est dans l'aire OSPF 0, tandis que `network 12.0.0.0 0.0.0.3 area 0` et `network 13.0.0.0 0.0.0.3 area 0` ajoutent des réseaux supplémentaires à la même aire. Cette configuration permet d'assurer une communication efficace et une mise à jour cohérente des tables de routage entre les routeurs OSPF.

Pour les trois autres routeurs dans ma simulation, voici les configurations ajoutées :

```
!
router ospf 1
log adjacency-changes
network 2.2.2.2 0.0.0.0 area 0
network 10.0.0.0 0.0.0.3 area 0
network 13.0.0.0 0.0.0.3 area 0
!
```

FIGURE 44 – Configuration de ospf de R2

```
!
router ospf 1
log adjacency-changes
network 3.3.3.3 0.0.0.0 area 0
network 11.0.0.0 0.0.0.3 area 0
network 12.0.0.0 0.0.0.3 area 0
!
```

FIGURE 45 – Configuration de ospf de R3

```
!
router ospf 1
log adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 10.0.0.0 0.0.0.3 area 0
network 11.0.0.0 0.0.0.3 area 0
!
```

FIGURE 46 – Configuration de ospf de R4

6. Tests de connectivité

Pour tester la connectivité entre les machines virtuelles Ubuntu et Linux, j'ai utilisé la commande ‘ping’ pour m'assurer que les deux machines pouvaient communiquer via le VPN IPsec configuré. Après avoir confirmé la connectivité, j'ai lancé Wireshark pour capturer le trafic réseau. En filtrant les paquets IPsec, j'ai pu observer que le trafic était bien sécurisé, comme l'indiquent les paquets ESP (Encapsulating Security Payload). Cette analyse a confirmé que la connexion entre les

deux machines est protégée par le VPN IPsec, assurant ainsi la sécurité des données échangées.

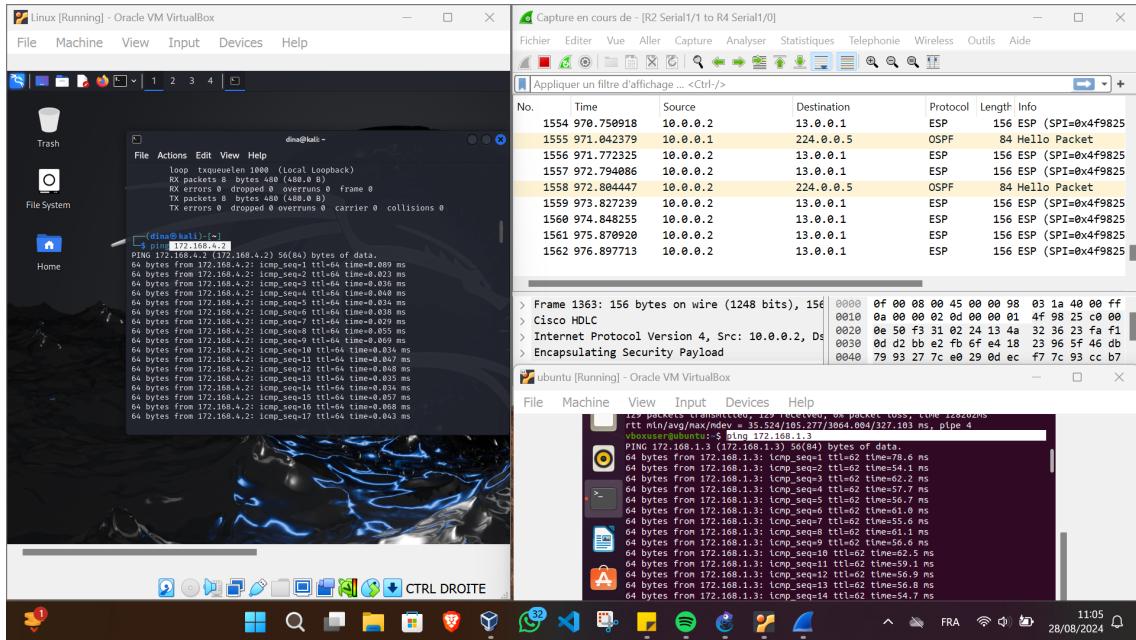


FIGURE 47 – Ping Ubuntu vers Linux

7. Détection de Snort

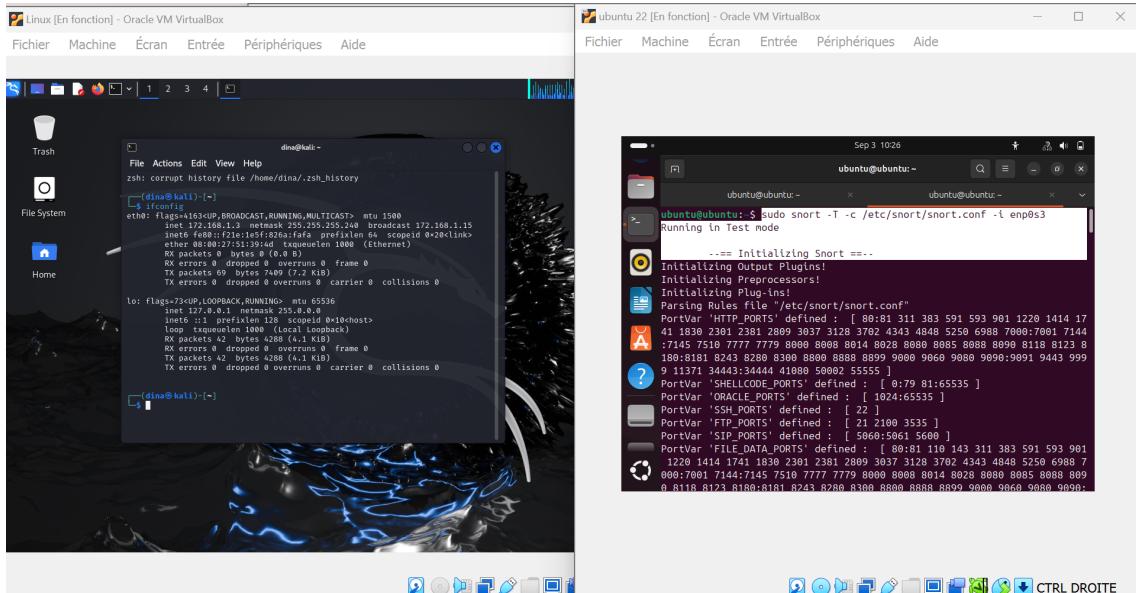


FIGURE 48 – Initialisation de Snort

```
sudo snort -T -c /etc/snort/snort.conf -i enp0s3 :
```

La capture montre l'exécution de Snort, un système de détection d'intrusion réseau, en mode test. La commande signifie :

- sudo : Exécuter la commande en tant qu'administrateur.

- **snort -T** : Lancer Snort en mode test, où il initialise tous les composants sans surveiller activement le trafic.
- **-c /etc/snort/snort.conf** : Utiliser le fichier de configuration spécifié.
- **-i enp0s3** : Spécifier l'interface réseau **enp0s3** pour surveiller le trafic.

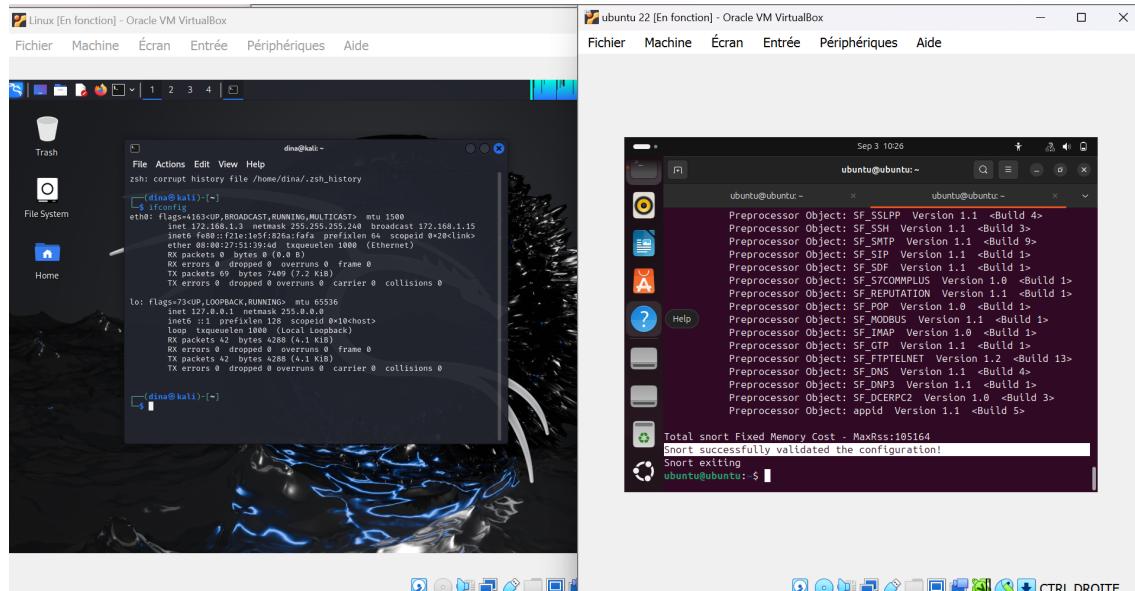


FIGURE 49 – Validation de Snort

La fenêtre de terminal en Ubuntu montre l'exécution de Snort en mode test avec plusieurs messages liés aux préprocesseurs de Snort, confirmant que Snort a correctement validé la configuration avec le message "**Snort successfully validated the configuration !**".

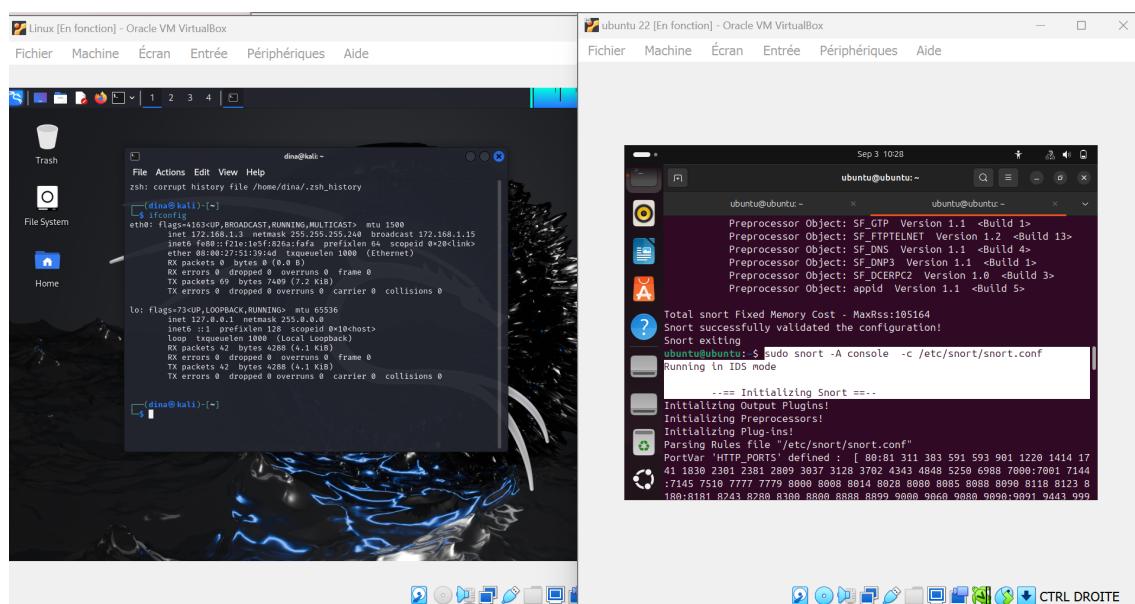


FIGURE 50 – Initialisation de Snort

Le terminal affiche la commande sudo snort -A console -c /etc/snort/snort.conf, ce qui exécute Snort en mode IDS (Intrusion Detection System) avec les messages de sortie directement dans la console. L'initialisation de Snort se déroule avec succès, indiquant que les plugins et preprocessors sont en cours de chargement et que le fichier de règles de Snort est en cours d'analyse.

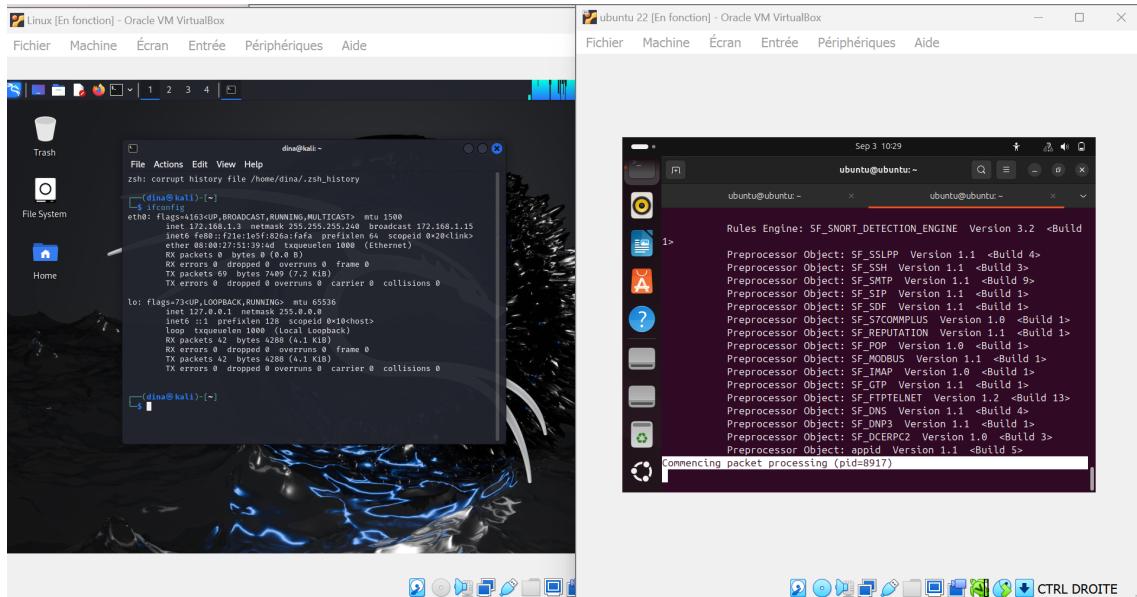


FIGURE 51 – Commencement des paquets

Message "Connecting packet preprocessing" :

Ce message indique que Snort est en train de passer à la phase de prétraitement des paquets. Cela signifie que le système est en train de préparer les données du réseau pour une analyse plus approfondie en utilisant les règles et les configurations définies.

Et lorsque l'on fait le ping, la détection donne le résultat suivant :

The image shows two terminal windows side-by-side. The left window is titled 'ubuntu 22 [En fonction] - Oracle VM VirtualBox' and displays a log of network traffic analysis. The right window is titled 'virtualBox' and shows a command-line interface with a list of ICMP sequence numbers and times.

```

ubuntu@ubuntu:~$ Commencing packet processing (pid=5866)
09/04/12:31:05.842821 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
09/04/12:31:05.974409 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IGMP} 0.0.0.0 -> 22.4.0.22
09/04/12:31:06.429402 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/04/12:31:06.470360 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
09/04/12:31:06.578256 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IGMP} 0.0.0.0 -> 22.4.0.22
09/04/12:31:06.701588 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16

```

```

dina@kali:~$ 
m 10.0.2.15: icmp_seq=17 ttl=64 time=0.069 ms
m 10.0.2.15: icmp_seq=18 ttl=64 time=0.051 ms
m 10.0.2.15: icmp_seq=19 ttl=64 time=0.051 ms
m 10.0.2.15: icmp_seq=20 ttl=64 time=0.123 ms
m 10.0.2.15: icmp_seq=21 ttl=64 time=0.040 ms
m 10.0.2.15: icmp_seq=22 ttl=64 time=0.051 ms
m 10.0.2.15: icmp_seq=23 ttl=64 time=0.051 ms
m 10.0.2.15: icmp_seq=24 ttl=64 time=0.059 ms
m 10.0.2.15: icmp_seq=25 ttl=64 time=0.069 ms
m 10.0.2.15: icmp_seq=26 ttl=64 time=0.069 ms
m 10.0.2.15: icmp_seq=27 ttl=64 time=0.072 ms
m 10.0.2.15: icmp_seq=28 ttl=64 time=0.058 ms
m 10.0.2.15: icmp_seq=29 ttl=64 time=0.058 ms
m 10.0.2.15: icmp_seq=30 ttl=64 time=0.038 ms
m 10.0.2.15: icmp_seq=31 ttl=64 time=0.082 ms
m 10.0.2.15: icmp_seq=32 ttl=64 time=0.075 ms
m 10.0.2.15: icmp_seq=33 ttl=64 time=0.075 ms
m 10.0.2.15: icmp_seq=34 ttl=64 time=0.183 ms
m 10.0.2.15: icmp_seq=35 ttl=64 time=0.084 ms
m 10.0.2.15: icmp_seq=36 ttl=64 time=0.084 ms
m 10.0.2.15: icmp_seq=37 ttl=64 time=0.039 ms
m 10.0.2.15: icmp_seq=38 ttl=64 time=0.096 ms
m 10.0.2.15: icmp_seq=39 ttl=64 time=0.038 ms
m 10.0.2.15: icmp_seq=40 ttl=64 time=0.036 ms
m 10.0.2.15: icmp_seq=41 ttl=64 time=0.038 ms
m 10.0.2.15: icmp_seq=42 ttl=64 time=0.052 ms

```

FIGURE 52 – Affichage de la détection de Snort

V. Présentation Visuelle de SSH

Cette simulation montre comment SSH peut être utilisé pour sécuriser l'accès à différents segments du réseau. Dans un environnement de production, cette méthode permettrait aux administrateurs réseau de se connecter à distance de manière sécurisée à des routeurs ou à d'autres machines sur des réseaux différents, assurant ainsi la confidentialité et l'intégrité des données transmises.

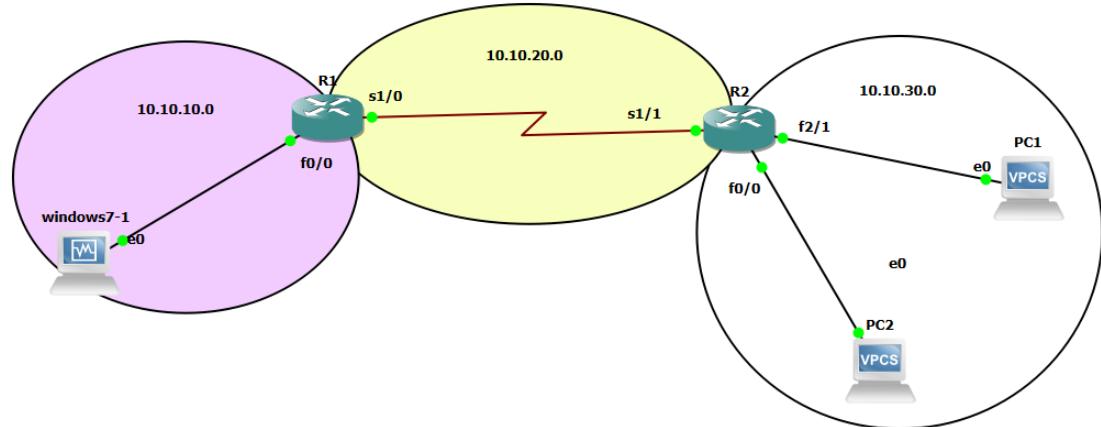
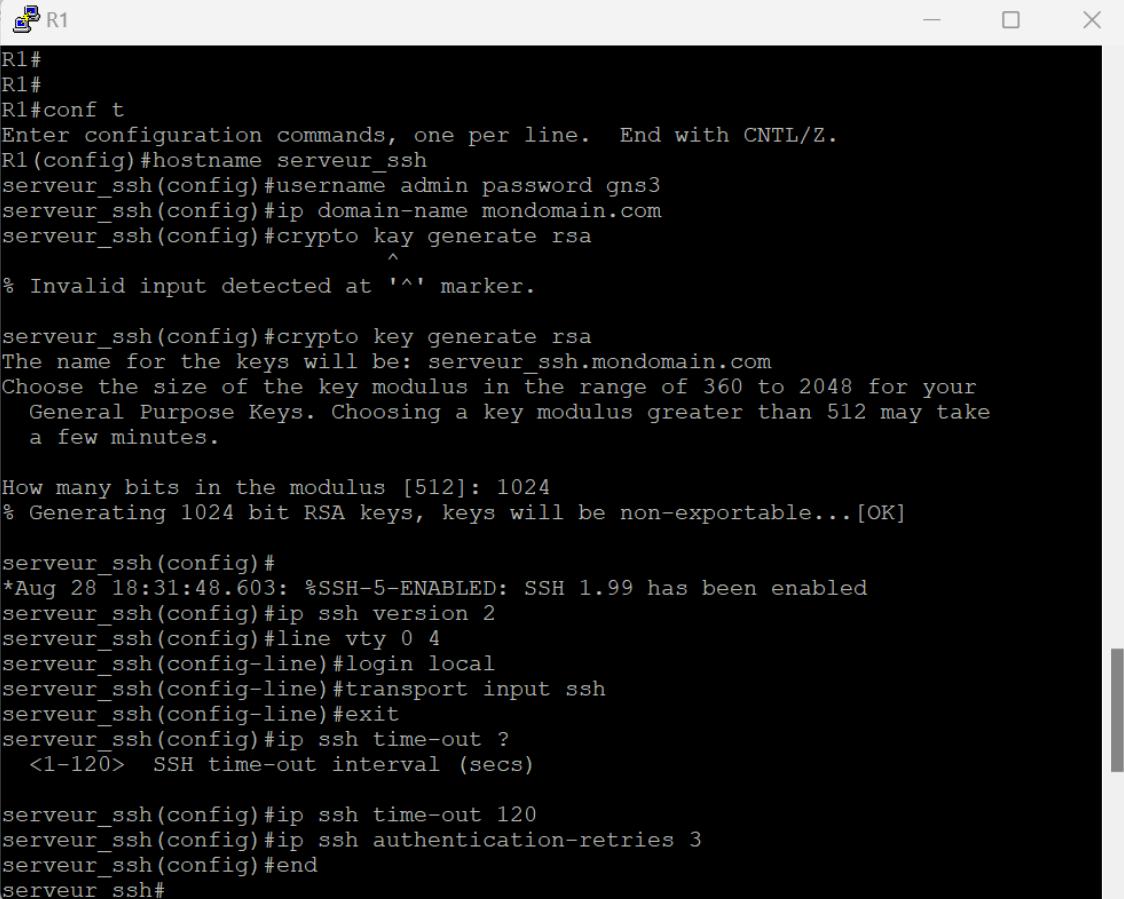


FIGURE 53 – Simulation de ssh

1. Configuration



```
R1#  
R1#  
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#hostname serveur_ssh  
serveur_ssh(config)#username admin password gns3  
serveur_ssh(config)#ip domain-name mondomain.com  
serveur_ssh(config)#crypto key generate rsa  
          ^  
% Invalid input detected at '^' marker.  
  
serveur_ssh(config)#crypto key generate rsa  
The name for the keys will be: serveur_ssh.mondomain.com  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.  
  
How many bits in the modulus [512]: 1024  
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]  
  
serveur_ssh(config)#  
*Aug 28 18:31:48.603: %SSH-5-ENABLED: SSH 1.99 has been enabled  
serveur_ssh(config)#ip ssh version 2  
serveur_ssh(config)#line vty 0 4  
serveur_ssh(config-line)#login local  
serveur_ssh(config-line)#transport input ssh  
serveur_ssh(config-line)#exit  
serveur_ssh(config)#ip ssh time-out ?  
<1-120>  SSH time-out interval (secs)  
  
serveur_ssh(config)#ip ssh time-out 120  
serveur_ssh(config)#ip ssh authentication-retries 3  
serveur_ssh(config)#end  
serveur_ssh#
```

FIGURE 54 – Configuration ssh de R1

- **username admin password gns3 :**
Crée un utilisateur nommé "admin" avec le mot de passe "gns3". Cet utilisateur sera utilisé pour l'authentification SSH.
- **ip domain-name mondomain.com :**
Définit le nom de domaine du routeur comme "mondomain.com". Ce nom de domaine est nécessaire pour générer les clés RSA pour SSH.
- **crypto key generate rsa :**
Cette commande génère une paire de clés RSA pour le protocole SSH. RSA (Rivest-Shamir-Adleman) est un algorithme de chiffrement qui permet de sécuriser les communications.
- **1024 (réponse à l'invite) :**
Spécifie la taille de la clé RSA en bits. Ici, une clé de 1024 bits est choisie, ce qui offre un bon équilibre entre sécurité et performance.
- **ip ssh version 2 :**
Force l'utilisation de la version 2 de SSH, qui est plus sécurisée et recommandée par rapport à la version 1.
- **line vty 0 4 :**

Accède à la configuration des lignes virtuelles (VTY) du routeur, qui sont utilisées pour les connexions Telnet ou SSH.

- **login local :**

Configure le routeur pour utiliser les comptes d'utilisateurs locaux (comme celui créé avec `username admin`) pour l'authentification sur les lignes VTY.

- **transport input ssh :**

Limite les connexions à ces lignes VTY au seul protocole SSH, désactivant ainsi l'accès via Telnet, qui est moins sécurisé.

- **exit :**

Sort de la configuration des lignes VTY et retourne au mode de configuration globale.

- **ip ssh time-out 120 :**

Définit le délai d'expiration de la session SSH à 120 secondes. Si l'utilisateur ne parvient pas à s'authentifier dans ce délai, la session est fermée.

- **ip ssh authentication-retries 3 :**

Limite le nombre de tentatives d'authentification SSH à 3. Après 3 échecs, la session est coupée, ce qui aide à prévenir les attaques par force brute.

- **end :**

Quitte le mode de configuration globale et retourne au mode d'exécution privilégiée.

Ensuite, je configure les adresses IP de chaque interface

```
R1
serveur_ssh#
serveur_ssh#conf t
Enter configuration commands, one per line. End with CNTL/Z.
serveur_ssh(config)#int f0/0
serveur_ssh(config-if)#ip add 10.10.10.1 255.255.255.0
serveur_ssh(config-if)#no shut
serveur_ssh(config-if)#do wr
Building configuration...
[OK]
serveur_ssh(config-if)#exit
serveur_ssh(config)#enable secret gns3
serveur_ssh(config)#exit
serveur_ssh#
*Aug 28 20:43:02.363: %SYS-5-CONFIG_I: Configured from console by console
serveur_ssh#
serveur_ssh#
serveur_ssh#conf t
Enter configuration commands, one per line. End with CNTL/Z.
serveur_ssh(config)#int s1/0
serveur_ssh(config-if)#ip add 10.10.20.1 255.255.255.0
serveur_ssh(config-if)#no shut
serveur_ssh(config-if)#int s1
*Aug 28 20:44:00.747: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
serveur_ssh(config-if)#int s1
*Aug 28 20:44:01.751: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
changed state to up
serveur_ssh(config-if)#exit
serveur_ssh(config)#exit
serveur_ssh#show
*Aug 28 20:44:20.531: %SYS-5-CONFIG_I: Configured from console by console
serveur_ssh#show ip int brief
Interface          IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0    10.10.10.1    YES NVRAM   up           up
Serial1/0          10.10.20.1    YES manual  up           up
Serial1/1          unassigned    YES NVRAM   administratively down down
```

FIGURE 55 – Configuration des interfaces de R1

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s1/1
R2(config-if)#ip add 10.10.20.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int
*Aug 28 20:45:31.503: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R2(config-if)#
*Aug 28 20:45:32.507: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1,
changed state to up
R2(config-if)#exit
R2(config)#int f2/1
R2(config-if)#ip add 10.10.30.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#do wr
*Aug 28 20:46:01.643: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
*Aug 28 20:46:02.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/1, changed state to up
R2(config)#do wr
Building configuration...
[OK]
R2(config)#exit
R2#show
*Aug 28 20:46:11.891: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip int brief
Interface          IP-Address      OK? Method Status       Prot
ocol
FastEthernet0/0    unassigned     YES unset  administratively down down
Serial1/0          unassigned     YES unset  administratively down down
Serial1/1          10.10.20.2   YES manual up           up
Serial1/2          unassigned     YES unset  administratively down down
Serial1/3          unassigned     YES unset  administratively down down
FastEthernet2/0    unassigned     YES unset  administratively down down
FastEthernet2/1    10.10.30.1   YES manual up           up
```

FIGURE 56 – Configuration des interfaces de R2

2. Configuration d'une Connexion Sécurisée avec PuTTY via SSH

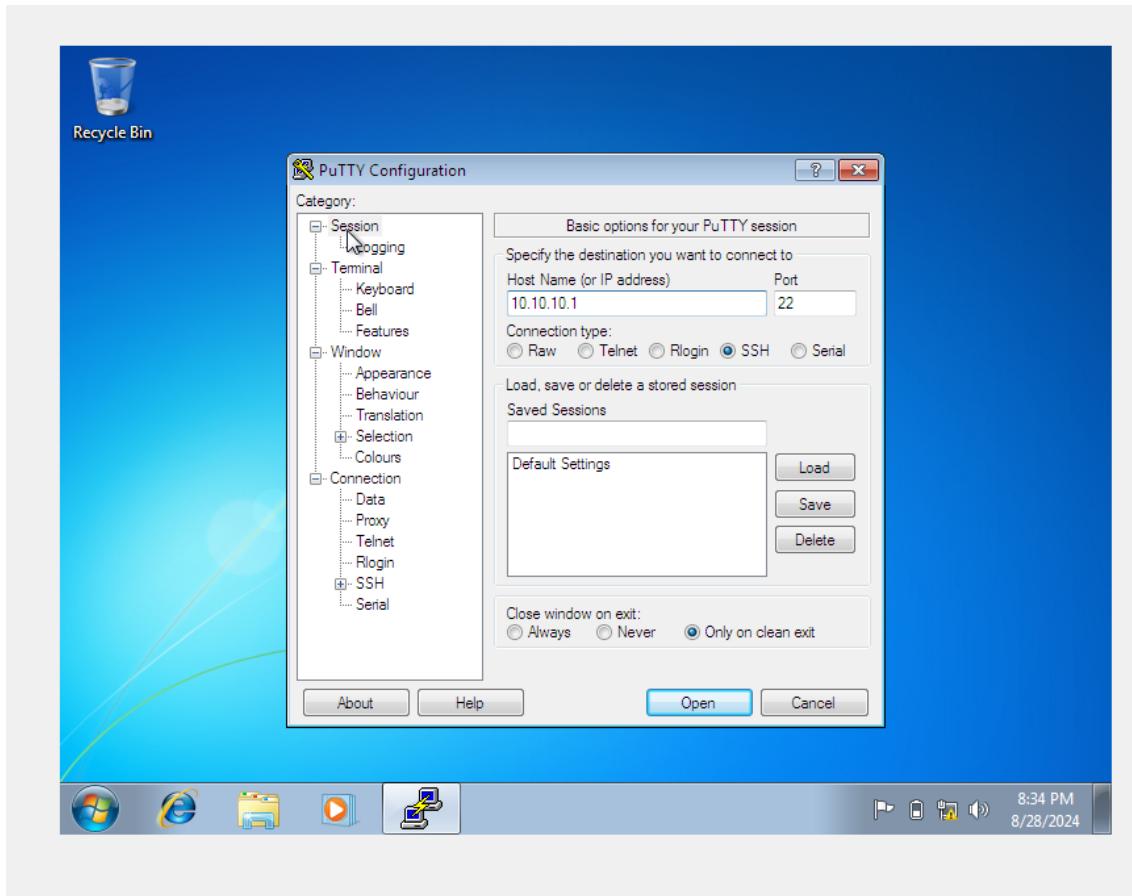


FIGURE 57 – Connexion Sécurisée avec PuTTY

Dans le cadre de l'utilisation de SSH avec PuTTY, un logiciel populaire utilisé pour établir des connexions réseau sécurisées, j'ai configuré une session pour me connecter de manière sécurisée à un serveur distant. PuTTY permet de se connecter à des serveurs en utilisant différents protocoles, notamment SSH, qui assure une communication cryptée. J'ai saisi l'adresse IP '10.10.10.1' dans le champ "Host Name (or IP address)" et spécifié le port '22', qui est le port par défaut pour les connexions SSH. Ensuite, j'ai sélectionné l'option "SSH" sous "Connection type" pour garantir que la communication se ferait de manière sécurisée. J'ai également la possibilité de sauvegarder cette configuration dans "Saved Sessions" pour ne pas avoir à ressaïrir ces informations lors des futures connexions. Enfin, en cliquant sur "Open", j'ai initié la connexion SSH, ouvrant ainsi une fenêtre de terminal où je peux interagir avec le serveur distant via la ligne de commande.

3. Authentication via SSH

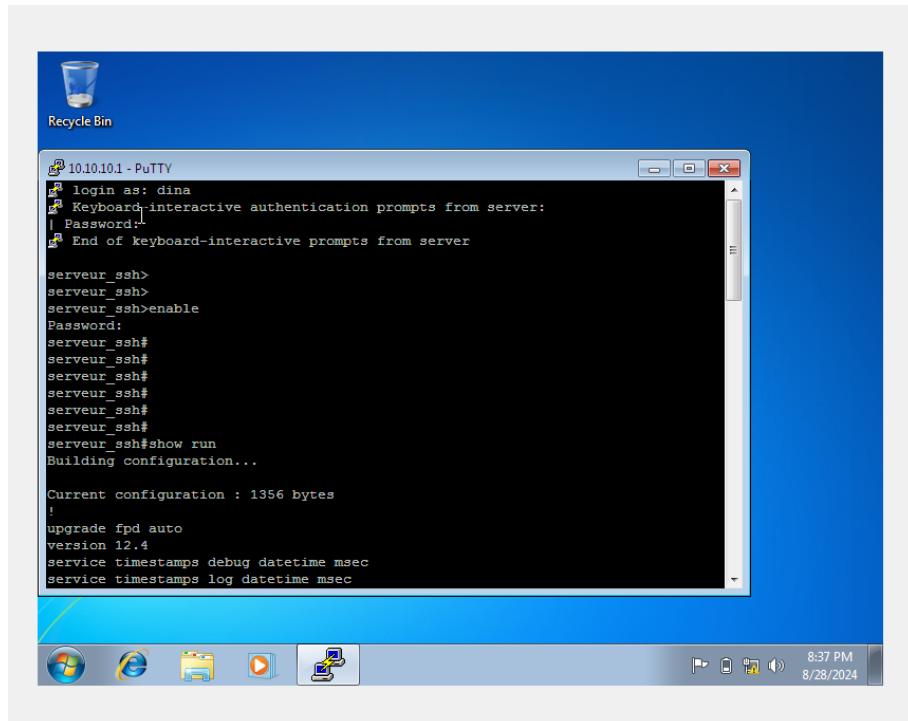


FIGURE 58 – Authentification ssh

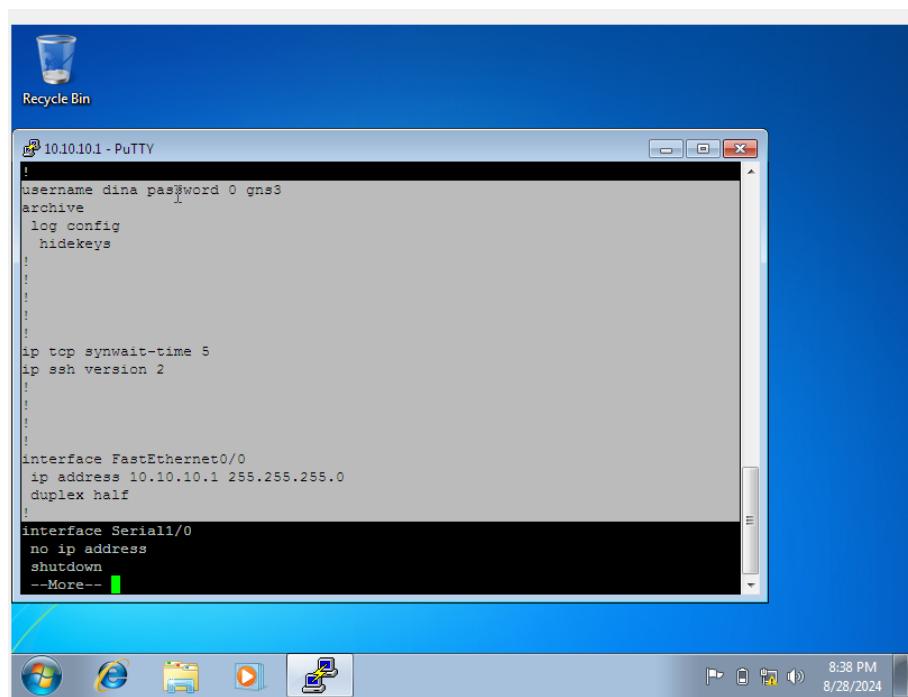


FIGURE 59 – Commande show run

Dans cette deuxième étape, après avoir configuré PuTTY et cliqué sur Open, une connexion SSH est établie avec le serveur distant à l'adresse IP 10.10.10.1. La fenêtre de terminal s'ouvre et vous êtes invité à vous connecter en tant qu'utilisateur

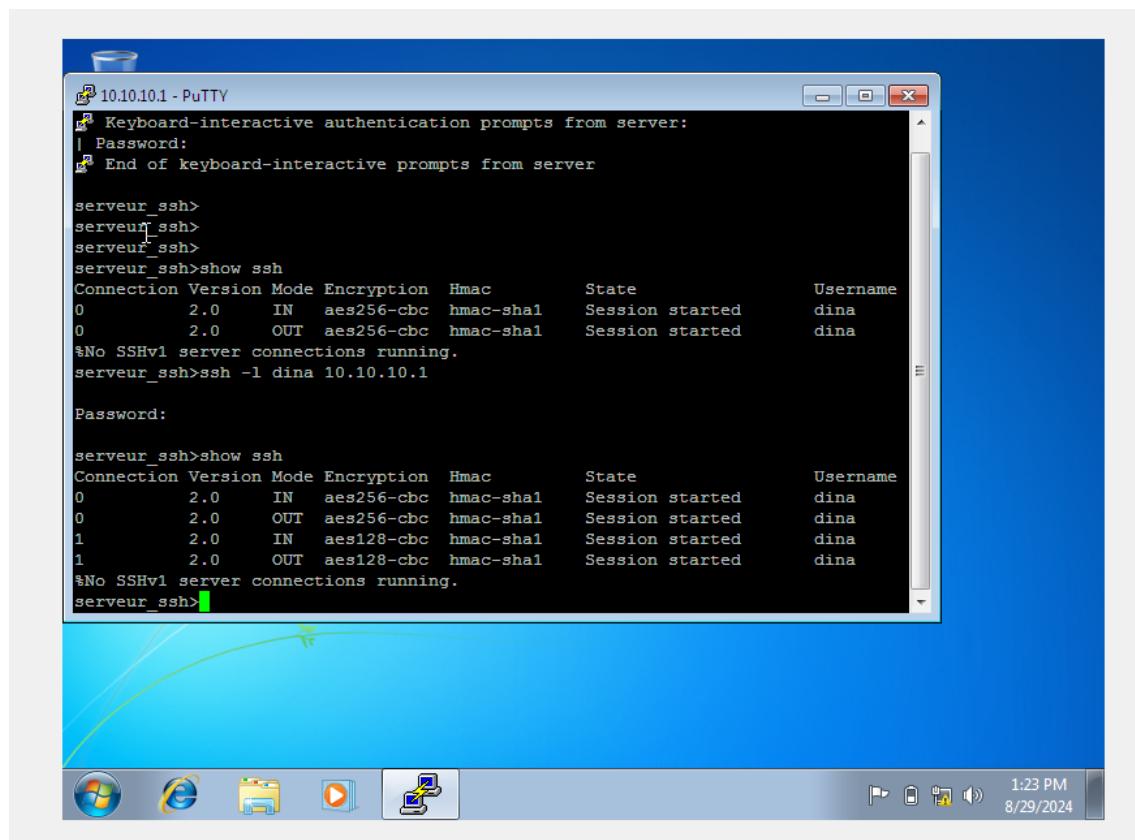
avec le message `login as:`. Dans cet exemple, l'utilisateur a saisi `dina` comme nom d'utilisateur.

Ensuite, le serveur engage une authentification interactive via le clavier, demandant le mot de passe associé à l'utilisateur `dina`. Une fois le mot de passe entré correctement, l'authentification est réussie, et vous accédez à l'interface en ligne de commande du serveur, comme indiqué par le prompt `serveur_ssh>`.

L'utilisateur passe ensuite en mode privilégié en tapant la commande `enable`, ce qui demande à nouveau un mot de passe pour obtenir des droits d'administration. Après avoir entré le mot de passe, le prompt change pour `serveur_ssh#`, indiquant que l'utilisateur dispose désormais des priviléges d'administration pour exécuter des commandes plus avancées sur le serveur.

Par exemple, l'utilisateur exécute la commande `show run` pour afficher la configuration en cours du serveur. Cela permet de voir les paramètres actuels et de vérifier la configuration du système. Le terminal affiche alors la configuration actuelle du serveur, y compris des détails tels que la version du logiciel et les services actifs.

4. Vérification des Sessions SSH et Chiffrement

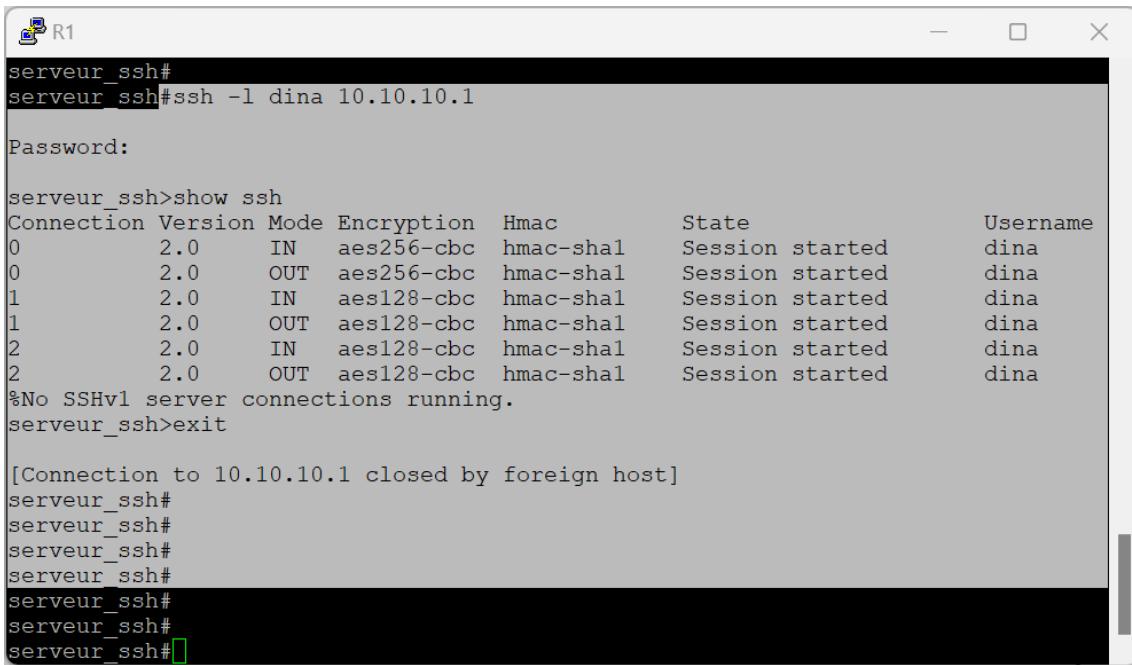


```
10.10.10.1 - PuTTY
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

serveur_ssh>
serveur_ssh>
serveur_ssh>
serveur_ssh>show ssh
Connection Version Mode Encryption Hmac      State          Username
0        2.0    IN   aes256-cbc  hmac-sha1  Session started  dina
0        2.0    OUT  aes256-cbc  hmac-sha1  Session started  dina
%No SSHv1 server connections running.
serveur_ssh>ssh -l dina 10.10.10.1

Password:

serveur_ssh>show ssh
Connection Version Mode Encryption Hmac      State          Username
0        2.0    IN   aes256-cbc  hmac-sha1  Session started  dina
0        2.0    OUT  aes256-cbc  hmac-sha1  Session started  dina
1        2.0    IN   aes128-cbc  hmac-sha1  Session started  dina
1        2.0    OUT  aes128-cbc  hmac-sha1  Session started  dina
%No SSHv1 server connections running.
serveur_ssh>
```



```
R1
serveur_ssh#
serveur_ssh#ssh -l dina 10.10.10.1
Password:
serveur_ssh>show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes256-cbc hmac-sha1 Session started dina
0 2.0 OUT aes256-cbc hmac-sha1 Session started dina
1 2.0 IN aes128-cbc hmac-sha1 Session started dina
1 2.0 OUT aes128-cbc hmac-sha1 Session started dina
2 2.0 IN aes128-cbc hmac-sha1 Session started dina
2 2.0 OUT aes128-cbc hmac-sha1 Session started dina
%No SSHv1 server connections running.
serveur_ssh>exit
[Connection to 10.10.10.1 closed by foreign host]
serveur_ssh#
serveur_ssh#
serveur_ssh#
serveur_ssh#
serveur_ssh#
serveur_ssh#
serveur_ssh#
serveur_ssh#
```

FIGURE 60 – Commande show ssh

Dans cette étape, après s'être connecté au serveur via SSH, l'utilisateur a exécuté la commande `show ssh` pour afficher les sessions SSH actives sur le serveur. Cette commande montre les détails des connexions SSH en cours, y compris la version du protocole, le mode de connexion (entrée ou sortie), le type de chiffrement utilisé (comme `aes256-cbc` et `aes128-cbc`), l'algorithme HMAC (comme `hmac-sha1`), l'état de la session (par exemple, "Session started"), et le nom d'utilisateur associé (`dina`).

Ensuite, l'utilisateur tente d'établir une nouvelle session SSH vers le même serveur (10.10.10.1) avec la commande `ssh -l dina 10.10.10.1`. Après avoir saisi le mot de passe, la commande `show ssh` est exécutée à nouveau pour vérifier les nouvelles connexions. Cette fois, on voit deux sessions supplémentaires utilisant le chiffrement `aes128-cbc`, indiquant que l'utilisateur a bien établi une nouvelle session SSH avec des paramètres de chiffrement différents.

Cette étape permet de vérifier que les sessions SSH sont correctement établies et que le chiffrement est en place pour sécuriser la communication entre l'utilisateur et le serveur.

Conclusion

Dans ce chapitre, nous avons exploré la configuration et l'utilisation du protocole SSH pour sécuriser les connexions réseau, en particulier via l'application PuTTY. Nous avons commencé par configurer les lignes virtuelles (VTY) du routeur pour garantir une authentification sécurisée en utilisant des comptes d'utilisateurs locaux et en limitant les connexions aux protocoles sécurisés comme SSH. Ensuite, nous avons configuré une connexion SSH à un serveur distant en utilisant PuTTY, assurant ainsi une communication chiffrée entre l'utilisateur et le serveur.

L'authentification via SSH a été réalisée avec succès, permettant à l'utilisateur d'accéder à des privilèges d'administration sur le serveur. Nous avons également vérifié les sessions SSH actives et les paramètres de chiffrement en cours, confirmant que la sécurité était bien en place.

Cette démarche souligne l'importance de sécuriser les accès aux serveurs et aux équipements réseau, en particulier dans des environnements critiques où la protection des données et des communications est primordiale. En utilisant des protocoles sécurisés comme SSH, les administrateurs réseau peuvent s'assurer que les connexions sont protégées contre les tentatives d'intrusion et que les communications restent confidentielles.

CONCLUSION

le stage a permis de mettre en lumière plusieurs axes d'amélioration concrets pour renforcer la résilience du réseau RINAM face aux menaces de cybersécurité. Tout d'abord, des vulnérabilités ont été identifiées au niveau de la transmission des données et des communications entre les différentes infrastructures. L'implémentation du protocole IPsec VPN a permis de chiffrer les communications entre les machines virtuelles, garantissant ainsi que les données échangées restent confidentielles et intégrales tout au long de leur transit. De plus, l'intégration de SSH pour les accès distants a apporté un niveau supplémentaire de sécurité en limitant l'accès non autorisé aux équipements réseau.

Ces solutions ont non seulement permis de corriger les failles actuelles, mais elles ont aussi assuré la conformité avec les normes internationales de sécurité aéronautique, telles que celles fixées par l'Organisation de l'Aviation Civile Internationale (OACI). Ainsi, le RINAM bénéficie désormais d'une infrastructure plus robuste, capable de résister aux attaques externes et internes, tout en maintenant un haut niveau de performance et de disponibilité. Ces améliorations garantissent non seulement la sécurité des communications, mais aussi la continuité des services critiques, essentiels pour la gestion du trafic aérien et la coordination entre les différentes entités aéroportuaires.

En somme, les résultats obtenus lors de ce stage contribuent significativement à la modernisation du réseau RINAM et à sa préparation face aux futures évolutions technologiques et réglementaires en matière de cybersécurité.

BIBLIOGRAPHIE

- [1] Airport security solutions to manage incidents, support the business, and improve security [Lien](#)
- [2] Projet de Fin d'Etudes - Design of a remote site allowing Radar and Radio data exchange with the CRCSNA of CASA and AGADIR on the ONDA IP network- Mr. SEHTOUT Abdelilah et Mr. ARJA Hatim
- [3] Projet de Fin d'Etudes - Conception et réalisation d'une application de supervision du réseau RINAM-M.CHOUGDALI SALLAMI
- [4] Projet de Fin d'Etudes - Etude de la mise en œuvre d'une solution de cybersécurité pour les systèmes de surveillance - M. Sallami CHOUGDALI
- [5] Projet de Fin d'Etudes -Réalisation d'une application de supervision des liaisons IP des données RADAR et ADS-B en provenance des sites RADAR - M.LAGLIL Rida et Mme.HALLOU Amal