



**MÉMOIRE DE FIN D'ÉTUDES DU PREMIER CYCLE EN VUE DE L'OBTENTION
DU DIPLÔME DE LICENCE EN INFORMATIQUE**

PARCOURS : ADMINISTRATION DES SYSTÈMES ET RÉSEAUX

THEME :

**ANALYSE CONCEPTUELLE DE LA CONFIGURATION ET
DE LA REDIRECTION DES PORTS DES SERVEURS,
cas de la DGSR**

Présenté par : RAZANAMAHARO Candy Salma Amanda

Membres du jury :

**Président du jury : Madame RATOBIBASINA Mioranavalona Vololonirina
Directrice de l'INSIDE University**

**Encadreur professionnel : Monsieur ANDRIANTSOA Husayn Mozart
Informaticien**

**Encadreur pédagogique : Monsieur RAHARISON Heriniaina
Enseignant formateur à l'INSIDE University**

Avril 2025

AVANT-PROPOS

L'évolution rapide des technologies informatiques et des infrastructures réseau a rendu la gestion des serveurs plus complexe et stratégique. Parmi les nombreux aspects à maîtriser, la configuration et la redirection des ports occupent une place centrale, notamment en ce qui concerne la sécurité et l'optimisation des services. Ce mémoire se penche sur l'analyse conceptuelle de ces processus, en prenant comme étude de cas la Direction Générale de la Sécurité Routière (DGSR).

En tant qu'étudiante en administration des systèmes et réseaux, j'ai toujours été attirée par les problématiques liées à la gestion des infrastructures informatiques et à la cybersécurité. Mon choix de sujet s'inscrit dans une volonté d'approfondir la compréhension des mécanismes de configuration des serveurs et de la manière dont la redirection des ports influence leur accessibilité, leur performance et leur sécurité.

Ce travail est destiné aux étudiants, aux professionnels de l'informatique et aux responsables IT souhaitant mieux appréhender les enjeux techniques et sécuritaires liés à ces opérations. Il repose sur une analyse approfondie, basée sur des recherches théoriques et des observations pratiques effectuées au sein de la DGSR. Grâce à une approche méthodologique rigoureuse, cette étude met en lumière les défis rencontrés dans la mise en place et la gestion des redirections de ports, ainsi que les bonnes pratiques à adopter pour garantir un fonctionnement optimal des serveurs.

L'intérêt de cette recherche ne se limite pas à une simple étude technique, mais vise également à fournir des recommandations concrètes et applicables. J'espère que ce mémoire apportera des éclairages utiles et suscitera l'intérêt des lecteurs, tout en les encourageant à approfondir cette thématique essentielle à la gestion des infrastructures informatiques modernes.

REMERCIEMENTS

Avant toute chose, je tiens à rendre grâce à Dieu Tout-Puissant pour sa bénédiction infinie, sa protection constante et sa guidance qui m'ont accompagné à chaque étape de ce parcours. Sans sa lumière, ce travail n'aurait jamais pu voir le jour.

Je voudrais exprimer ma profonde gratitude à Monsieur RABEZANAHARY Andriamparany, Directeur de l'INSIDE UNIVERSITY, et à Madame RATOBIBASINA Mioranavalona Vololonirina, Directrice de l'INSIDE UNIVERSITY, ainsi qu'à tout le corps professoral de l'institut. Leur soutien sans faille, leur bienveillance et leurs encouragements ont été une source d'inspiration tout au long de mon parcours académique. Grâce à leur vision et leur dévouement, j'ai pu m'épanouir dans un environnement propice à l'apprentissage, et c'est grâce à eux que j'ai pu réaliser ce travail avec passion et détermination.

Je remercie du fond du cœur mon encadreur professionnel, Monsieur ANDRIANTSOA Husayn Mozart, pour son soutien constant, sa générosité dans le partage de son expérience et pour ses conseils avisés. Grâce à lui, j'ai pu aborder ce sujet de manière concrète et le transformer en une véritable expérience d'apprentissage. Sa disponibilité et sa patience ont fait toute la différence.

Un grand merci également à mon encadreur pédagogique, Monsieur RAHARISON Heriniaina, dont l'expertise et la rigueur m'ont permis de franchir chaque étape de cette étude. Ses encouragements et son regard éclairé ont été essentiels pour mener à bien cette recherche.

Je tiens à exprimer ma reconnaissance éternelle à ma famille, dont le soutien a été inestimable. Non seulement ils ont toujours été là pour m'apporter leur soutien moral, mais ils m'ont aussi soutenu financièrement, ce qui m'a permis de poursuivre mes études et de mener à bien ce projet. Leur amour, leur patience et leur générosité ont été mon moteur tout au long de cette aventure. À eux, je dédie une grande partie de cette réussite.

Enfin, à toutes les personnes qui, de près ou de loin, ont participé à la réalisation de ce travail – que ce soit par un mot d'encouragement, un conseil ou un simple geste de soutien, je vous adresse un sincère et chaleureux merci. Vous êtes les véritables artisans de cette réussite.

RESUME

La gestion des infrastructures informatiques représente un enjeu crucial dans un monde de plus en plus connecté, notamment à travers la configuration et la redirection des ports des serveurs, éléments essentiels à la performance et à la sécurité des services en ligne. Cette étude, réalisée dans un contexte virtuel avec pour cas d'étude la Direction Générale de la Sécurité Routière (DGSR), vise à comprendre l'impact de ces configurations sur l'accessibilité et la protection des serveurs. En explorant les notions de ports réseau, de protocoles de communication et de stratégies de redirection, elle met en lumière les défis liés à la virtualisation et les risques de cybersécurité en cas de mauvaise configuration. Grâce à une analyse technique et documentaire, l'étude démontre que l'adoption de bonnes pratiques, comme l'usage de pare-feu, le filtrage des connexions et une attribution réfléchie des ports, améliore considérablement la fiabilité des infrastructures réseau. Elle fournit ainsi des recommandations utiles aux administrateurs système pour une gestion optimisée et sécurisée.

Mots clés : Ports, Redirection, Serveurs, Sécurité, Protocoles, Cybersécurité, Pare-feu, Filtrage, Trafic, Virtualisation, Infrastructures, Réseau.

ABSTRACT

The management of IT infrastructures is a crucial challenge in an increasingly connected world, especially through the configuration and redirection of server ports, which are essential to the performance and security of online services. This study, conducted in a virtual environment using the Directorate General of Road Safety (DGSR) as a case study, aims to understand the impact of these configurations on server accessibility and protection. By exploring the concepts of network ports, communication protocols, and redirection strategies, it highlights the challenges related to virtualization and the cybersecurity risks associated with poor configurations. Through technical and documentary analysis, the study demonstrates that adopting best practices—such as the use of firewalls, connection filtering, and thoughtful port assignment—significantly improves the reliability and security of network infrastructures. It thus provides valuable recommendations for system administrators seeking to optimize and secure their infrastructure management.

Keywords: Ports, Redirection, Servers, Security, Protocols, Cybersecurity, Firewall, Filtering, Traffic, Virtualization, Infrastructure, Network.

LISTE DES TABLEAUX

Tableau 1: Organigramme de la DGSR	12
Tableau 2:Chronogramme de GANTT	19
Tableau 3: Les éléments constitutifs du parc informatique de la société DGSR.....	20

LISTE DES FIGURES

Figure 1: Logo de l'INSIDE University	7
Figure 2:Logo DGSR.....	8
Figure 3: Taux de cyberattaque.....	14
Figure 4: Routeur	21
Figure 5: Switch.....	22
Figure 6: Point d'accès.....	22
Figure 7: câble RJ45	23
Figure 8: câble fibre optique	23
Figure 9: Pare-feu	24
Figure 10: Topologie en étoile	26
Figure 11: Architecture réseau de l'entreprise DGSR.....	28
Figure 12:Logo d'OPNsense	30
Figure 13 : Configuration de la machine virtuelle dans VirtualBox.	32
Figure 14: Menu de démarrage d'opnsense.....	32
Figure 15: Processus d'installation d'opnsense étape 1	33
Figure 16: Processus d'installation d'opnsense étape 2	34
Figure 17: Processus d'installation d'opnsense étape 3	34
Figure 18: Processus d'installation d'opnsense étape 4	35
Figure 19: Processus d'installation d'opnsense étape 5	36
Figure 20: Installation réussi d'opnsense	36
Figure 21: Page de connexion OPNsense.	41
Figure 22: Tableau de bord après connexion.	42
Figure 23: Navigation vers Firewall > NAT > Port Forward.....	42
Figure 24(1/4): Formulaire rempli pour la règle NAT.....	43
Figure 25(2/4): Formulaire rempli pour la règle NAT.....	44
Figure 26(3/4): Formulaire rempli pour la règle NAT.....	44
Figure 27(4/4): Formulaire rempli pour la règle NAT.....	44
Figure 28: Live View montrant le trafic entrant.	46

LISTE DES ANNEXES

Annexe 1:Présentation des protocoles utilisés	X
Annexe 2: Différence entre IP public et IP privée	X
Annexe 3:Différence entre LAN et WAN	XI

LISTE DES ABREVIATIONS

ACM : Automobile Club de Madagascar
DGSR : Direction Générale de la Sécurité Routière
DMZ : Demilitarized Zone (Zone Démilitarisée)
EPIC : Établissement Public à Caractère Industriel et Commercial
FAI : Fournisseur d'Accès à Internet
FTP : File Transfer Protocol (Protocole de Transfert de Fichiers)
HIFI: High Fidelity
HTTP: HyperText Transfer Protocol
HTTPS: HyperText Transfer Protocol Secure
IDS/IPS: Intrusion Detection System / Intrusion Prevention System (Système de Détection et de Prévention d'Intrusion)
IP : Internet Protocol
IT : Information Technology (Technologies de l'Information)
LAN: Local Area Network (Réseau Local)
MAF : Multi-Factor Authentication (Authentification Multi-Facteur)
NAT : Network Address Translation
NTIC : Nouvelles Technologies de l'Information et de la Communication
ONU : Organisation des Nations Unies
PF : Packet Filter (Filtrage de Paquets)
RAM: Random Access Memory
SEG: Système d'Exploitation Général
SSH: Secure Shell
TCP : Transmission Control Protocol (Protocole de Contrôle de Transmission)
UDP : User Datagram Protocol (Protocole de Datagramme Utilisateur)
UNESCO : Organisation des Nations Unies pour l'Éducation, la Science et la Culture
VDI : VirtualBox Disk Image (Image de Disque VirtualBox)
VMS : Virtual Machine System (Système de Machine Virtuelle)
VPN : Virtual Private Network (Réseau Privé Virtuel)
WAN: Wide Area Network
WIFI: Wireless Fidelity

SOMMAIRE

AVANT-PROPOS	I
REMERCIEMENTS	II
RESUME	III
ABSTRACT	IV
LISTE DES TABLEAUX.....	V
LISTE DES FIGURES	VI
LISTE DES ANNEXES.....	VII
LISTE DES ABREVIATIONS	VIII
INTRODUCTION GÉNÉRALE	1
PARTIE I : CADRE GÉNÉRALE	3
CHAPITRE I : PRESENTATION DE L'INSIDE UNIVERSITY	3
CHAPITRE II : PRESENTATION DE L'ENTREPRISE DE STAGE.....	8
CHAPITRE III : METHODOLOGIE	14
PARTIE II : ANALYSE DE L'EXISTANT ET RÉSULTATS	20
CHAPITRE I : MATÉRIELS TECHNOLOGIE ET TOPOLOGIE.....	20
CHAPITRE II : MISE EN PLACE DE L'OUTIL	30
PARTIE III : CADRE PRATIQUE	38
CHAPITRE I : FONCTIONNALITES.....	38
CHAPITRE II : RESULTATS	47
CHAPITRE III : PERSPECTIVE D'AVENIR.....	50
CONCLUSION GÉNÉRALE	52
BIBLIOGRAPHIE.....	IX
ANNEXES	X

INTRODUCTION GÉNÉRALE

Dans un monde où la digitalisation des services ne cesse de croître, la gestion efficace des infrastructures informatiques devient une nécessité incontournable. À l'échelle internationale, la sécurisation et l'optimisation des serveurs sont au cœur des préoccupations des entreprises et institutions publiques. L'augmentation des cyberattaques, la complexité croissante des réseaux et la nécessité d'assurer une accessibilité optimale des services en ligne imposent une maîtrise approfondie de la configuration et de la redirection des ports des serveurs. De nombreux incidents de sécurité liés à une mauvaise gestion des ports ont été recensés dans plusieurs pays, entraînant des fuites de données et des interruptions de service critiques.

À Madagascar, ces défis prennent une importance particulière avec la modernisation des systèmes d'information des administrations et entreprises. L'État malgache, à travers diverses institutions, a entrepris des réformes numériques visant à améliorer la gestion des infrastructures informatiques. La Direction Générale de la Sécurité Routière (DGSR) s'inscrit dans cette dynamique en adoptant des solutions virtualisées pour l'hébergement de ses services numériques. Cependant, la gestion efficace des configurations réseau, en particulier la redirection des ports, demeure un enjeu central pour garantir l'accessibilité et la sécurité des systèmes d'information.

C'est dans ce contexte que s'inscrit cette étude, qui vise à analyser la configuration et la redirection des ports des serveurs en environnement virtuel. La question centrale de cette recherche est la suivante : **comment optimiser la configuration et la redirection des ports des serveurs virtuels pour améliorer la sécurité et la performance des infrastructures informatiques ?**

L'objectif global de cette étude est d'apporter une compréhension approfondie des mécanismes de configuration et de redirection des ports afin d'en optimiser l'usage au sein des infrastructures virtualisées. Pour répondre à cette problématique, plusieurs sous-questions sont abordées : Quels sont les principes fondamentaux de la gestion des ports des serveurs ? Quels sont les risques liés à une mauvaise configuration des ports ? Quelles sont les meilleures pratiques pour sécuriser la redirection des ports dans un environnement virtuel ? Comment la DGSR peut-elle améliorer la gestion des ports de ses serveurs virtualisés ?

Les hypothèses de cette étude reposent sur l'idée que la mise en place d'une gestion rigoureuse des ports, associée à des outils et protocoles adaptés, permet d'améliorer significativement la performance et la sécurité des serveurs. Nous supposons également que l'application des bonnes pratiques en matière de redirection des ports peut réduire les risques d'attaques et optimiser l'accessibilité des services numériques.

Afin de vérifier ces hypothèses, cette étude s'appuiera sur une revue de la littérature, une analyse technique des configurations existantes, ainsi que des recommandations basées sur les meilleures pratiques en matière d'administration réseau.

Ce travail se structure comme suit : après cette introduction, une première partie sera consacrée à la cadre générale. La deuxième partie portera sur l'analyse de l'existant et résultats. Enfin, la dernière sera consacrée à la cadre pratique.

PARTIE I : CADRE GÉNÉRALE

CHAPITRE I : PRESENTATION DE L'INSIDE UNIVERSITY

L'INSIDE University est une université habilitée par l'Etat qui fait la formation de haut niveau et suivant le système LMD. La conférence, atelier de projet et voyage d'étude font partie de leurs activités.

Il y a 3 mentions dans l'INSIDE University. Chaque mention assure la formation initiale menant jusqu'au Master. Le cursus complet des études est subdivisé en 2 cycles, le premier cycle a une durée de six (06) semestres et dont la réussite est sanctionnée par un diplôme de Licence et le second cycle : une durée de quatre (04) semestres et dont la réussite est sanctionnée par un diplôme de Master.

Voici la détaille de chaque mention :

1. GESTION :

La Mention Gestion de l'INSIDE University a pour objectif de préparer des futurs cadres, dirigeants, opérateurs d'entreprise et managers capables de s'adapter au monde des affaires et de se placer au carrefour des enjeux de la compétitivité de l'économie mondiale.

La Mention Gestion de l'INSIDE University a pour vocation de préparer et d'accompagner des collaborateurs capables d'assurer durablement la performance de l'entreprise vis-à-vis de la mondialisation. Elle propose pour cela des itinéraires de formation initiale, diplômante, qualifiante et professionnalisante répondant aux besoins du marché de travail et de notre pays.

INSIDE University formera des étudiants à mobilité intellectuelle efficace, à intensité intellectuelle rigoureuse, dynamique, ayant le sens de défi, compétents aux besoins du monde professionnel. La qualité et l'efficacité de chaque étudiant y seront prépondérantes au cours de la formation. L'aptitude à faire face au changement et la performance de chaque apprenant y seront aiguisées.

La Mention Gestion de l'INSIDE University donne accès à trois parcours :

1.2 Comptabilité finance

C'est un parcours qui prépare les étudiants à être capable de créer sa propre entreprise, maîtriser les techniques comptables et financières, maîtriser les techniques de contrôle budgétaire, maîtriser les techniques d'assurances, maîtriser le rôle du Leadership, concevoir les stratégies de l'entreprise, assurer la Direction d'une entreprise, assurer la Direction commerciale, assurer la Direction financière, assurer la Direction des Ressources Humaines, assurer le rôle d'un auditeur, apprendre à connaître les bases et techniques du contrôle formel des états comptables et valider l'enregistrement des opérations, et de maîtriser les principes de la comptabilité publique et la comptabilité bancaire au sein d'un environnement réglementaire en évolution.

1.3 Marketing et commerce international

C'est un parcours qui prépare les étudiants à être capable de créer sa propre entreprise, connaître et mieux maîtriser l'environnement de vente de l'entreprise, maîtriser les techniques approfondies en Marketing et en Commerce international, assurer la Direction commerciale, assurer la Direction Marketing, assurer le conseil à la vente, apprécier les capacités de vente de l'entreprise, gérer et d'augmenter les ventes, maîtriser la stratégie marketing adoptée dans l'équilibre général de l'entreprise, maîtriser la pénétration des marchés étrangers, maîtriser l'environnement international de l'entreprise, apprécier les capacités à l'import/export de l'entreprise, et assurer le conseil à l'import/export, maîtriser les techniques relatives à la conquête d'un marché à l'étranger, et conduire des projets d'importation et d'exportation au niveau international d'une manière réalisable et fiable.

1.4 Management et développement d'entreprise

C'est un parcours qui prépare les étudiants à être capable de créer sa propre entreprise, mener un projet, maîtriser les techniques de gestion des ressources humaines, maîtriser les systèmes de management de qualité pour améliorer la qualité de service ou de produit au niveau de l'entreprise, maîtriser les principes de la comptabilité publique et la comptabilité bancaire au sein d'un environnement réglementaire en évolution, maîtriser les techniques et les rouages de la gestion de trésorerie de l'entreprise, organiser, gérer, structurer le rôle de l'entreprise dans son environnement, maîtriser le rôle du Leadership, concevoir les stratégies de l'entreprise, assurer la Direction d'une entreprise, assurer la Direction financière, assurer la Direction des Ressources Humaines, assurer la tenue de la comptabilité d'une société, faire un inventaire

comptable, dresser un bilan annuel -d'une société, maîtriser les techniques de transit et douane, maîtriser les techniques de ventes, assister le chef personnel d'une société, assurer le rôle d'un auditeur, apprendre à connaître les bases et techniques du contrôle formel des états comptables et valider l'enregistrement des opérations.

1.5 Débauchés

A la fin de leurs études, les étudiants pourront être responsable Administratif et Financier, responsable Comptabilité, responsable des Ressources Humaines, auditeur, contrôleur de Gestion, responsable Crédit, et responsable Marketing, responsable Communication, responsable Import/Export, transitaire, responsable Publicité, chef de produit...

2. DROIT :

La Mention Droit de l'INSIDE University est une formation qui répond aux besoins de la nation dans la mesure où elle met en exergue le cadre juridique pour contribuer au développement du pays en imposant des règles pour le bon fonctionnement et l'organisation des organismes privés et publics.

La Mention Droit de l'INSIDE University a pour objectif de donner aux étudiants une formation juridique générale de haut niveau comportant l'enseignement de toutes les matières classiques du droit privé et du droit public. INSIDE University vise à insérer les étudiants dans un cursus comportant une dimension nationale et internationale marquée.

La Mention Droit de l'INSIDE University comporte deux parcours le DROIT PRIVE et le DROIT PUBLIC

2.1. Débauchés

La Mention Droit de l'INSIDE University est une mention qui ouvre toutes les portes car les juristes ont une formation polyvalente comme les carrières judiciaires, l'avocat : défense des personnes, des entreprises (en tant qu'avocat d'affaires), ou l'Etat, le magistrat (ou juge), le notaire : intervenant à des moments importants de la vie (mariage, achat d'une maison, rédaction d'un testament, succession, ...). Conseiller des entreprises, le clerc de notaire, l'huissier de justice : recouvrement de créances, constat et état des lieux, le commissaire-priseur : expertise et évaluation des objets, le greffier, les carrières dans l'entreprise, la fonction

juridique pure : contrats, traitement des contentieux, la fonction ressources humaines recrutement, licenciement, formation, négociation collective, le juriste rédacteur : conception et rédaction des ouvrages juridiques dont se servent tous les professionnels du Droit pour travailler, les carrières administratives, la fonction publique locale, nationale ou internationale (Union européenne, ONU, UNESCO, etc.), le juriste d'administration, l'équivalent du juriste d'entreprise, les fonctions d'administration et de gestion dans les services de l'Etat ou des collectivités locales (administrateur, attaché, rédacteur), l'officier de gendarmerie ; officier de police ; commissaire de police ; inspecteur des impôts ; diplomate ; officier des armées ; officier sapeur-pompier professionnel, autres carrières, le juriste d'association, le journaliste, la carrière politique, l'enseignant-chercheur en droit, notamment Maître de conférences ou Professeur.

3. INFORMATIQUE :

L'informatique est actuellement un facteur discriminant social et intellectuel ainsi que garant de développement tant au niveau de l'étudiant que national. La Mention Informatique de l'INSIDE University propose aux jeunes étudiants un produit intervenant dans le domaine de la gestion, de la maintenance et du réseau informatique permettant à l'étudiant d'acquérir de bonnes connaissances concernant la maîtrise de la gestion appliquée à l'informatique et le fonctionnement des systèmes réseaux ainsi que les diverses maintenances matérielles. La Mention Informatique de l'INSIDE University intègre bien évidemment, les techniques d'automatisation, la méthodologie de maintenance, d'assurance qualité et le partage sécurisé par réseaux des données. Une partie des travaux pratiques est adossée à des sites et/ou secteurs professionnels et des laboratoires de recherche.

La Mention Informatique de l'INSIDE University comporte deux parcours :

3.1 Administrations des systèmes et réseaux

Le parcours Administration des Systèmes et Réseaux consiste à vérifier le bon fonctionnement des systèmes informatiques et des réseaux, d'assister les utilisateurs dans l'utilisation des nouvelles technologies ou les dépanner en cas de problème, de gérer l'accès et la sécurité du système. C'est la structuration de l'entreprise par les NTIC et la mise en œuvre des réseaux haut débit. Il constitue l'organe de contrôle et de diffusion de

l'information, de la maintenance des systèmes intelligents en temps réels et de leurs interfaces.

3.2 Génie logiciel et base de données

Le parcours Génie Logiciel et base de données caractérise l'utilisation de l'outil informatique pour simplifier la gestion administrative de l'entreprise et du suivi des activités en passant par l'automatisation des différentes tâches. Il est étroitement lié au système d'informatique de l'entreprise et se rend la forme, pour les grandes entreprises, d'un progiciel de gestion intégré.

3.3 Débauchés

La Mention Informatique de l'INSIDE University forme les étudiants à devenir un architecte d'Applications, architecte de Matériels informatiques, chef de Projet Informatique, développeur Multimédia, administrateur Réseau Informatique, ingénieur Développeur d'Application en Base de Données, ingénieur Développeur d'Application Web, ingénieur d'Etude et de Développement, ingénieur Qualité Logicielle, ingénieur Informaticien, ingénieur en Réseau et Sécurité Informatique, ingénieur en Création de Projet Informatique Electronique, ingénieur Informaticien en Multimédia.

Figure 1: Logo de l'INSIDE University



Source : inside-university.mg

CHAPITRE II : PRESENTATION DE L'ENTREPRISE DE STAGE

Ce chapitre est consacré au statut de la Direction Générale de la Sécurité Routière a son historique ainsi qu'au service fourni par le centre.

1 Statut de la direction générale de la sécurité Routière

La Direction Générale de la Sécurité Routière sise à Alarobia sur la rue Ravoninahitriarivo-Antananarivo. A titre de l'information si après les contacts OPS 033.77.777.03 et l'adresse email du société DGSR a 2 annexes à Betongolo et à Nanisana. La DGSR est un établissement public à caractère industriel et commercial « EPIC » suivant le décret N°2003/856 du 19 Août 2003 portant statut de la DGSR (EPIC) dont nous allons voir son historique.

A compter du 1^{er} Janvier 1989, les centres de Sécurité Routières sont érigés en Direction Générale de la Sécurité Routière, connue sous le sigle DGSR suivant le décret N°89-080 du 24 Mars 1989. En son article 2, le décret N°89-080 du 2 Mars 1989 confère à la DGSR le statut d'établissement Public à caractère Industriel et Commercial (EPIC) bénéficiant de l'autonomie financière et placé sous la tutelle du Ministère de la Défense.

En 1995, la DGSR, organisme rattaché à la Zandarimariam-pirenenana, est placée sous tutelle du Ministère des Forces Armées, suivant le décret N°95-327 du 03 Mai 1995. En 1997 décret N°97-284 du 0 Avril 1997 fixant les attributions du secrétariat d'Etat près du Ministère des forces Armées chargé de la gendarmerie, ainsi que l'organisation générale de son Secrétariat d'Etat qui stipule en son article 13 que la DGSR est un EPIC placée sous tutelle du SEG.

Figure 2:Logo DGSR



Source : dgsrmda.com

2 Historique de la société

La principale activité de la DGSR est d'assurer la sécurité de la circulation routière, essentiellement le contrôle et la vérification de la conformité et de l'état technique des véhicules. Ces activités de la sécurité publique et la sécurité routière font une partie intégrante des missions des gendarmeries auparavant assuré par l'automobile Club de Madagascar (ACM).

2.1 Automobile club de Madagascar

Le 10 Décembre 1959, signature d'une convention par laquelle l'Etat Malagasy a confié le contrôle technique périodique des véhicules automobiles à l'AUTOMOBILE CLUB DE MADAGASCAR (ACM) qui est une association privée reconnue d'utilité publique. Progressivement des centres de sécurité routière, placés sous contrôle administratif et technique du Ministère de l'équipement et des communications (chargé des transports), ont été créés pour être chargé des visites techniques des véhicules automobiles conformément aux dispositions du code de la route.

Une convention du 14 Mai 1968 régit la gérance des centres de sécurité routière qui sont en majorité implanté dans les locaux des travaux publics. L'ensemble des biens mobiliers et immobiliers qui étaient acquis au cours de la gérance de ces centres étaient reconnus propriétés de l'Etat.

2.2 Gendarmerie nationale

Les activités de la DGSR contribuent au financement des missions de la gendarmerie nationale relatives à la sécurité publique et la sécurité routière. Suite à la déficience de l'ACM, la responsabilité des centres de sécurité routières en matière de visite technique a été confiée à la zandarimariam-pirenena suivant le décret N°76-283 du 09 Septembre 1976 ainsi que les textes suivants :

Le 02 Février 1982, parution de l'Instruction Ministérielle N°/MINDEF/SG/DAL/STIM relative aux modalités d'application du décret N°76-283 du 09 septembre 1976, confiant la responsabilité des centres de sécurité routière en matière de visite technique à la zandarimariam-pirenena.

Le 06 Mars 1991, la responsabilité assumée par le Ministère des travaux publics en matière de réception technique des véhicules a été transférée au ministère de la défense en vertu du décret N°88-426 du 033 Novembre 1988.

Le 10 Janvier 1989, parution de l'arrêté 128/89 du ministère de la défense relatif à la réception des véhicules à moteur ou véhicules remorqués ainsi que les éléments de véhicules.

En 2001, décret N°2001/780 du 28 Septembre 2001, portant modification de certaines dispositions du décret N°89-080 du 24 Mars 1989 sur la réorganisation des centres de sécurité routières, notamment en son article 2 stipulant que « La direction Générale de la Sécurité Routière est un établissement public à caractère industriel et commercial doté de la personnalité morale et jouissant de l'autonomie administrative et financière régie par la loi N°98-031 du 20 Janvier 1998 susvisée, placée sous tutelle du secrétariat d'Etat chargé de la gendarmerie.

3 Mission

Depuis sa création, la DGSR a pour mission de protéger la vie humaine d'où le slogan : « Lahitokana ny aina ». A l'entrée du garage de la DGSR est écrit « PREVENTION, PRUDENCE, SECURITE ». Ces trois mots peuvent résumer les objectifs de la DGSR. EN d'autres termes, la DGSR vise surtout à préserver les accidents de la route en assurant la sécurité et l'aptitude d'un véhicule automobile à circuler avec prudence.

4 Activité

Pour réaliser ses missions, la DGSR procède à la visite technique, à la réception technique, à la constatation avant dédouanement et à la contrôle inopiné.

4.1 Visite technique

La visite technique a pour objectif d'assurer un bon état de marché d'un véhicule automobile et remorque afin d'atténuer les risques des accidents. Pour ce faire une attention particulière est portée par les vérificateurs sur la direction, les freins, l'éclairage des signalisations et l'émission de fumées. La visite technique est exigée pour tout véhicule. Les papiers demandés dépendent de la nature du véhicule.

Périodicité de la visite technique :

- Tous les ans pour les véhicules de plus de 5 ans
- Tous les 4 mois pour les véhicules de transport public de personne
- Tous les 6 mois pour les véhicules de transport de marchandises

Les papiers exigés :

D'une manière générale : la carte grise et la carte de visite technique

Pour les véhicules utilitaires on exige en plus :

- Carte violette : -Patente – Licence
- Carnet d'entretien
- Attestation de non-imposition

1. Réception technique

Pour la réception technique, il faut vérifier si les voitures importées sont conformes aux normes techniques avant de leur livrer les papiers afférents. Les différents types de véhicules qui doivent se présenter à la réception technique sont les véhicules à moteur et remorques.

Des véhicules à moteur et remorque :

- Importés, neufs ou d'occasion
- Neuf ou d'occasion ayant subi des aménagements, transformations ou modifications

Les papiers exigés :

- Demande manuscrite adressée à Monsieur le Directeur General de la DGSR
- Photocopie de la carte gris à l'étranger
- Photocopie du certificat pour servir à l'immatriculation (Modèle)
- Photocopie de la déclaration d'importation
- Notice descriptive du véhicule
- Certificat de conformité

2. Constations avant dédouanement

Par un communiqué relatif à l'amélioration de la sécurité des transports routiers daté du 02 Octobre 2003, la Vice-Primature confie aux centre de la sécurité routière l'exécution des constatations techniques que doivent subir à compter du 03 Novembre 2003 les véhicules importés d'occasion de 3.5 tonnes et plus avant leur dédouanement en application du décret N°2003 R 982 du 30 Septembre 2003 modifiant certaines dispositions de l'articles R 66 (nouveau) paragraphe B et C(1^{er} alinéa) ainsi que l'article R 284 R 2 (nouveau) et de l'article 1^{er} du décret N°2000 R 187 du 22 Mars 2000.

Des nouvelles mesures ont été adoptées selon l'Arrêté N°952/2006 du 16 Janvier 2000 sur les contrôles des vitres fumées et la ceintures de sécurité.

3. Contrôle inopiné

En matière de contrôle inopiné, La DGSR a donné un mois de sensibilisation et conscientisation (du 20 Décembre 2018 au 20 Janvier 2019) des usagers (propriétaires et chauffeurs) de bien entretenir et maintenir en bon état de marche leurs véhicules. Mais n'accorde aucune tolérance pour tous véhicules présentant des anomalies génératrices d'accident surtout celle qui touchent le système de freinage, la direction et les pneumatiques. Une fois ce délai expiré, des contrôles plus stricte, sévères, rigoureux seront appliqués aux récalcitrants.

I. Les sièges de la société DGSR à Madagascar

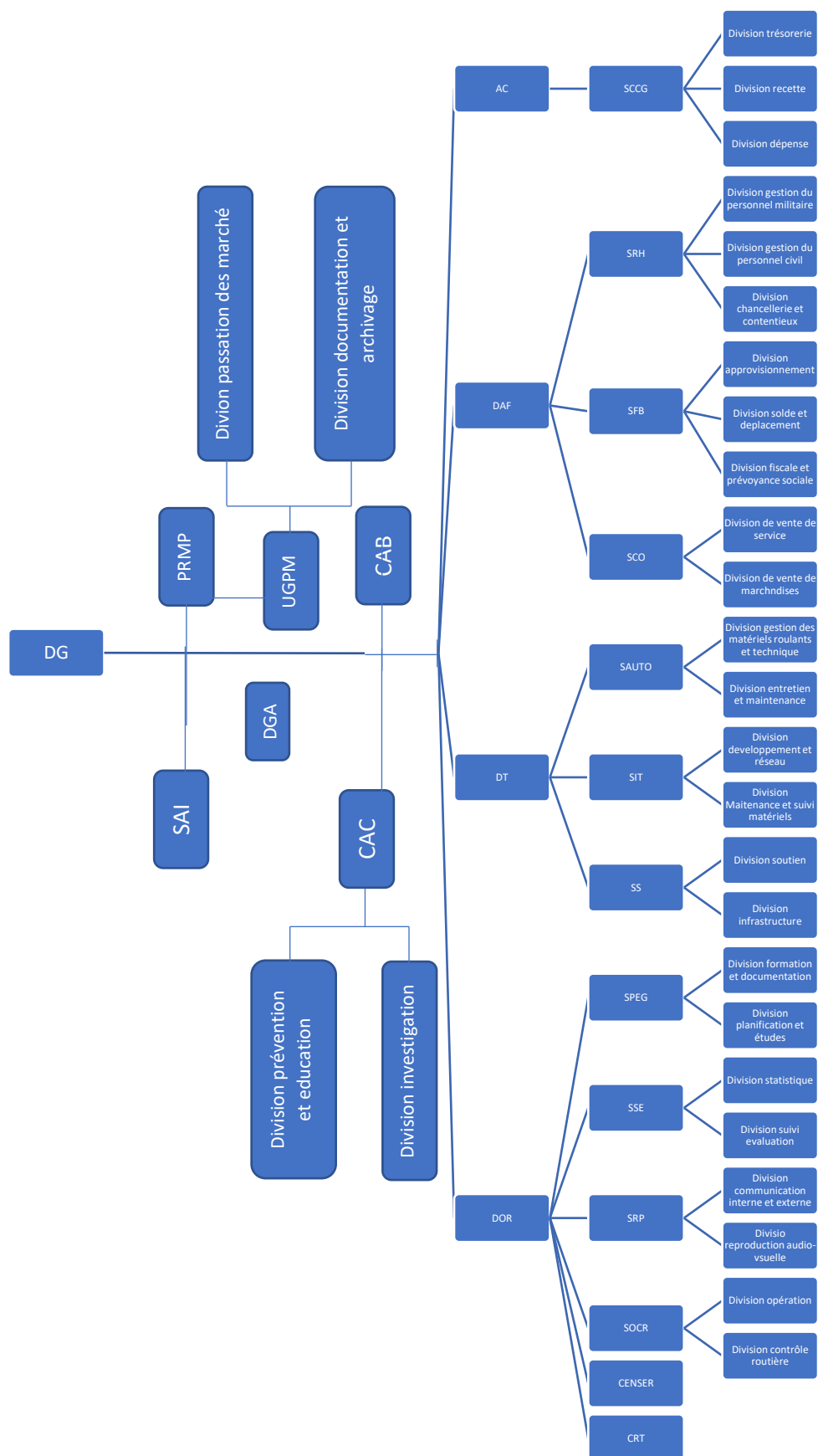
La DGSR se localise dans toute la région de Madagascar dont le principal siège est Antananarivo. Elle est aussi présente dans les locaux suivants :

- Toliara : Ambovombe-Androy, Taolagnaro
- Mahajanga : Antsohihy, Amborovy
- Antsiranana : Antranobozaka, Nosy-Be, Sambava
- Toamasina : Ambatodrazaka, Fénerive-Est, Barikadimy, Moramanga et Antanamborizano
- Fianarantsoa : Besorohitra, Ambositra, Ihosy
- Antananarivo : Ivato, Tsiroanomandidy, Betongolo, By-pass et Antsirabe

II. Organigramme de la DGSR

La structure organisationnelle est une représentation schématique de toute organisation générale mise en place au sein d'un établissement. Cette structure a pour objectif de veiller à une meilleure répartition des tâches entre les différentes responsables hiérarchiques. Ci-après l'organigramme.

Tableau 1: Organigramme de la DGSR



Source : Direction générale de la sécurité routière

CHAPITRE III : METHODOLOGIE

Ce chapitre décrit la méthodologie utilisée pour mener à bien cette analyse. Il est essentiel de comprendre les étapes et les outils adoptés pour évaluer la configuration des serveurs et la redirection des ports au sein de l'infrastructure réseau de la DGSR.

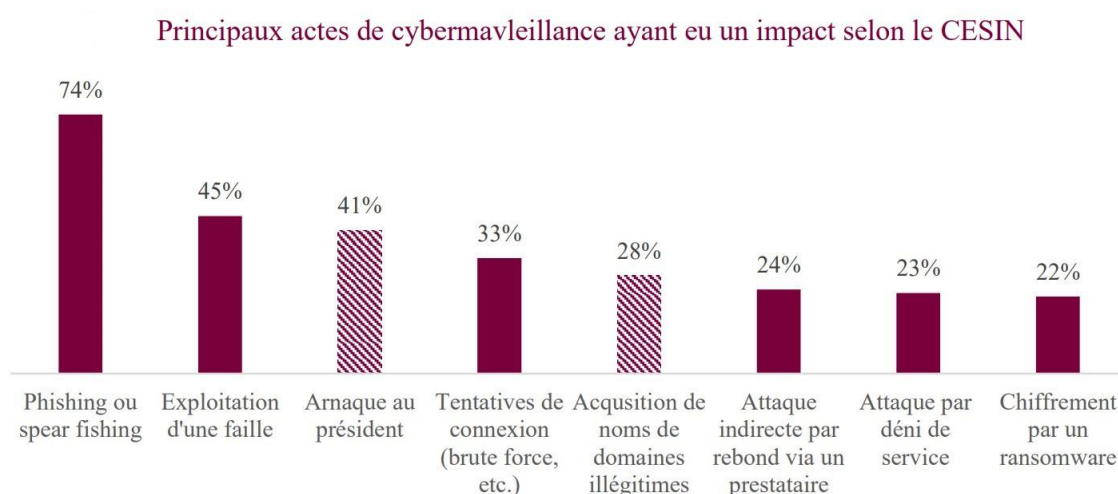
1. CHOIX DU THEME

Le choix du thème est une étape cruciale dans la définition des objectifs de cette étude. Il permet de clarifier les enjeux et de justifier l'importance du sujet choisi. Dans ce cas, l'analyse conceptuelle de la configuration et de la redirection des ports des serveurs à la Direction Générale de la Sécurité Routière (DGSR) a été retenue pour plusieurs raisons, qui seront développées dans les sous-sections suivantes.

1.1 Contextualisation

La cybersécurité est devenue un enjeu majeur tant au niveau national qu'international. Avec l'augmentation des menaces informatiques telles que les cyberattaques, le vol de données et les intrusions non autorisées, la protection des infrastructures réseau est devenue une priorité pour les organisations publiques et privées. La gestion efficace des configurations réseau, notamment la configuration et la redirection des ports, joue un rôle essentiel dans la prévention de ces risques.

Figure 3: Taux de cyberattaque



Source : blodemoderateur.com

Avant de définir un thème précis, il est crucial de comprendre l'état actuel des pratiques en matière de sécurité des réseaux. Cette phase d'analyse permet d'examiner les configurations des serveurs, des pare-feux, ainsi que la gestion des ports dans différents environnements. Bien que de nombreuses infrastructures soient opérationnelles, elles peuvent présenter des vulnérabilités en matière de sécurité et des lacunes dans l'optimisation des ressources.

L'architecture réseau moderne repose souvent sur la virtualisation, une technologie qui divise un serveur physique en plusieurs environnements virtuels autonomes. Chaque serveur virtuel fonctionne comme une machine indépendante, avec son propre système d'exploitation, ses ressources, et ses applications. Cette configuration, bien qu'efficace, nécessite une gestion rigoureuse afin d'éviter des problèmes de performance et des vulnérabilités en matière de sécurité.

La DGSR, joue un rôle essentiel dans la gestion des systèmes d'information de l'état. Cependant, comme toute organisation utilisant des systèmes informatiques, elle est exposée à des risques cybernétiques. L'étude de la configuration et redirection des ports au sein de la DGSR s'avère donc particulièrement pertinente pour évaluer le niveau de sécurité de ses infrastructures et identifier les pistes d'amélioration.

Ainsi, une analyse approfondie des configurations des serveurs et des redirections des ports est indispensable pour renforcer la sécurité et l'efficacité des systèmes d'information, que ce soit dans des contextes nationaux ou internationaux.

1.2 Thème

Le thème de ce projet porte sur la configuration et la redirection des ports dans un environnement virtualisé, un sujet d'une importance croissante face à l'évolution des menaces informatiques. En effet, la gestion des ports constitue un élément clé de la sécurité réseau, car une mauvaise configuration peut ouvrir des failles exploitables par des cyberattaquants. Ce projet vise à démontrer comment des outils de sécurité avancés, tels qu'OPNsense, peuvent être utilisés pour renforcer la sécurité des infrastructures informatiques.

L'objectif est d'explorer les mécanismes de configuration des ports, d'analyser leur impact sur la sécurité du réseau, et de proposer des solutions adaptées aux environnements modernes basés sur la virtualisation. Le choix de ce thème s'explique par la nécessité croissante pour les organisations de sécuriser efficacement leurs systèmes d'information, en particulier dans des contextes où la virtualisation est omniprésente.

Le choix de ce thème est également motivé par les défis actuels auxquels font face les entreprises et les institutions dans la gestion de la sécurité de leurs réseaux. Avec la prolifération des cyberattaques ciblant des infrastructures critiques, il est essentiel de comprendre comment les configurations réseau, notamment la redirection des ports, peuvent devenir des points d'entrée pour des menaces. Ce projet permet ainsi de mettre en lumière l'importance de la sécurisation de ces points névralgiques grâce à des outils performants comme OPNsense, qui offre des solutions adaptées aux environnements virtualisés complexes. Ce travail s'inscrit ainsi dans une démarche visant à sécuriser et améliorer l'infrastructure de la DGSR, en garantissant un meilleur contrôle des ressources informatiques et en réduisant les risques liés aux vulnérabilités réseau.

2. RECHERCHES

La phase de recherche est essentielle pour poser les bases théoriques et pratiques du projet. Elle permet d'identifier les connaissances existantes, de comprendre les enjeux techniques et d'intégrer des solutions déjà éprouvées. Cette section détaille les sources utilisées pour nourrir l'analyse du thème choisi : l'analyse de la configuration et de la redirection des ports des serveurs. Pour ce faire, trois types de recherches ont été réalisées : la recherche bibliographique, la recherche webographie et la recherche médiagraphie.

2.1 Recherche bibliographie

La recherche bibliographique a consisté en une exploration des ouvrages, articles scientifiques et rapports techniques sur la gestion des serveurs, la configuration des ports et la sécurité des réseaux. Cette étape a permis de poser un cadre théorique solide pour comprendre les principes fondamentaux de la gestion des infrastructures réseaux et de la sécurité des données.

Les ouvrages étudiés incluent des manuels sur la sécurité des systèmes d'information, la gestion des serveurs et des réseaux, ainsi que des publications sur les bonnes pratiques en matière de configuration des ports et de pare-feu. Parmi les documents les plus pertinents, on retrouve : *Serveur-cours1.pdf*, mise en place d'une sécurité réseau basé sur le pare-feu OPNsense, *TS2Log-Redirection des ports.pdf*.

Cette recherche bibliographique a donc permis de mieux cerner les enjeux du projet et d'intégrer des concepts théoriques indispensables pour mener à bien l'analyse des configurations de serveurs et des redirections de ports.

2.2 Recherche webographie

La recherche webographique a été un complément essentiel à la recherche bibliographique, car elle permet d'obtenir des informations actualisées sur les pratiques de sécurité des serveurs, la configuration des réseaux et la redirection des ports. En effet, de nombreux experts en cybersécurité, administrateurs systèmes et entreprises spécialisées partagent leurs retours d'expérience et leurs solutions via des blogs, forums et publications en ligne. Voici quelques exemples de ressources web consultées : <https://cours-informatique.fr>, <https://cite-telecom.com>, <https://www.fnac.com>, <https://finevpn.org>, <https://web4.ensiie.fr>

Cette recherche webographie a permis de compléter et d'actualiser les connaissances acquises par la recherche bibliographique. Elle a aussi mis en lumière des solutions techniques récentes et des stratégies de sécurisation innovantes.

2.3 Recherche médiagraphie

La recherche médiagraphie a consisté en l'examen de sources multimédia, telles que des vidéos, des webinaires, des conférences et des podcasts, qui abordent la gestion des serveurs et la sécurité des ports. Ces ressources sont particulièrement utiles pour leur capacité à illustrer de manière visuelle et interactive les concepts techniques, et pour leur accessibilité dans l'acquisition de compétences pratiques. Les principaux types de ressources médiagraphies consultées sont : redirection des ports avec opnsense de Pascal DUVERLIE, How to port forwarding on opnsense firewall (NETVN82).

La recherche médiagraphie a donc apporté un éclairage pratique sur les sujets étudiés, facilitant la compréhension de certains aspects techniques complexes tout en permettant d'entendre des témoignages d'experts dans le domaine.

3. ENTRETIEN

L'entretien professionnel est une étape cruciale dans la collecte d'informations et dans la compréhension des processus en place au sein de l'entreprise de stage.

Entretien professionnelle

L'entretien a été réalisé avec Monsieur ANDRIANTSOA Husayn Mozart à la DGSR. Il est responsable de l'administration des réseaux, et possède une expertise solide dans la gestion des infrastructures IT et la sécurité des réseaux. Avec 12 d'expérience, Il a travaillé sur la configuration des serveurs et la mise en place de solutions de sécurité. Son rôle consiste à

garantir la sécurité des serveurs, la gestion des ports, ainsi que l'optimisation de l'infrastructure réseau, et les activités de cybersécurité, tout en respectant les normes de sécurité en vigueur.

Ce profil est particulièrement pertinent pour le projet, car Monsieur ANDRIANTSOA Husayn Mozart gère directement les configurations des serveurs et est en charge de la mise en place des stratégies de sécurité au sein de la DGSR. Grâce à son expérience et à sa maîtrise des aspects techniques, il a pu fournir des informations détaillées sur les pratiques actuelles utilisées pour la configuration des ports et la gestion des serveurs au sein de l'organisation.

L'entretien s'est concentré sur plusieurs axes afin de comprendre les pratiques et les défis auxquels la DGSR est confrontée dans la gestion des serveurs et des redirections de ports. Voici les principaux points abordés : le responsable a expliqué les décisions prises concernant l'architecture des serveurs de la DGSR. L'entretien a permis de discuter des défis liés à la configuration des redirections de ports et des risques que cela comporte pour la sécurité. Le responsable a décrit les mécanismes et les stratégies déployés pour minimiser ces risques. Le responsable a présenté les outils de gestion des serveurs et des réseaux utilisés au sein de la DGSR. Les contraintes techniques et humaines qui affectent la gestion des serveurs ont été abordées, notamment les enjeux de ressources humaines et les défis liés à la mise à jour des systèmes de sécurité dans un environnement évolutif.

L'entretien avec le responsable technique a été une étape clé du projet. Il a apporté une perspective pratique et une expertise terrain qui complètent et enrichissent les recherches théoriques. Les informations recueillies ont permis de mieux comprendre les défis et les solutions appliquées au sein de la DGSR, tout en validant certaines approches techniques abordées dans les recherches précédentes. Cette discussion a également ouvert la voie à des pistes d'amélioration pour la gestion des serveurs et des ports dans le cadre de la sécurité informatique au sein de l'organisation.

4. CHRONOGRAMME DE GANTT

Le chronogramme de Gantt est un outil visuel permettant de planifier et de suivre l'évolution d'un projet. Il est souvent utilisé pour organiser les différentes tâches et activités à réaliser, en précisant leurs dates de début et de fin. Ce type de graphique aide à visualiser la progression du projet, les dépendances entre les différentes tâches, et les échéances importantes.

Le chronogramme de Gantt pour ce projet a été élaboré afin d'organiser toutes les étapes nécessaires à la réalisation de l'analyse conceptuelle de la configuration et de la redirection des

ports des serveurs de la Direction Générale de la Sécurité Routière (DGSR). Ce plan de travail s'étend sur plusieurs mois et inclut les principales phases du projet, de la recherche à la rédaction finale.

Tableau 2:Chronogramme de GANTT

Activité	S 1	S 2	S 3	S 4	S 5	S 6	S 7	S 8	S 9	S10	S11	S12	S13
Début stage													
Recherche thème													
Recherche bibliographie													
Recherche webographie													
Recherche médiagraphie													
Entretien professionnelle													
Analyse de données													
Rédaction du rapport													

Source : Investigation personnelle

Le chronogramme de Gantt permet de structurer et d'organiser le déroulement du projet en fonction des différentes tâches et de leurs durées respectives. En ayant une vision claire du temps alloué à chaque étape, tu peux suivre les progrès du projet et t'assurer de respecter les délais pour chaque phase. Il est essentiel de respecter ces échéances pour garantir une progression fluide du projet, de la recherche initiale à la rédaction finale.

PARTIE II : ANALYSE DE L'EXISTANT ET RÉSULTATS

CHAPITRE I : MATÉRIELS TECHNOLOGIE ET TOPOLOGIE

Ce chapitre est dédié à la présentation des éléments techniques qui composent l'infrastructure réseau de la DGSR. Il inclut les matériels utilisés, les technologies déployées ainsi que la topologie du réseau en place, afin de comprendre les fondements techniques nécessaires à la gestion de la configuration et à la redirection des ports des serveurs.

1. MATÉRIELS

La DGSR utilise une série de matériels pour assurer la gestion de ses serveurs et de son infrastructure réseau. Ces matériels sont essentiels pour le bon fonctionnement des services et pour la sécurité des données échangées.

1.1. Quelques définitions

Avant d'aborder les aspects techniques du réseau et de son infrastructure, il est essentiel de définir certains termes clés qui seront utilisés tout au long de cette étude. Ces définitions permettent de mieux comprendre le contexte général de l'environnement informatique étudié.

1.1.1. Réseaux informatiques

D'une manière générale, un réseau est un ensemble d'objet interconnecté les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

1.1.2. Parc informatique

L'expression Parc informatique désigne l'ensemble du matériel informatique et des logiciels utilisés au sein de l'entreprise.

Tableau 3: Les éléments constitutifs du parc informatique de la société DGSR

MATÉRIELS	NOMBRES
Source fibre	1
Serveur	2
Routeur	2
Machine clients	41
Coffret	4
Switch	6
Point d'accès wifi	5
Imprimantes	9

Source : Investigation personnelle

Le source fibre est utilisée comme accès internet pour recouvrir le besoin en connexion de l'entreprise.

1.1.3. Serveurs

Un serveur est un ordinateur ou un système informatique qui fournit des services, des ressources ou des informations à d'autres ordinateurs (appelés clients) via un réseau. Les serveurs sont utilisés pour stocker des données, héberger des sites web, ou exécuter des applications pour les utilisateurs.

La DGSR dispose d'un serveur physique unique qui joue un rôle fondamental dans son infrastructure réseau. Cependant, grâce à des technologies de virtualisation, ce serveur physique héberge plusieurs serveurs virtuels. Ces serveurs virtuels permettent d'exécuter plusieurs systèmes distincts sur une seule machine physique, optimisant ainsi l'utilisation des ressources matérielles.

Chaque serveur virtuel est configuré pour effectuer des tâches spécifiques. Par exemple, un serveur virtuel peut être dédié à l'hébergement des sites web, tandis qu'un autre peut gérer les bases de données ou les services internes de l'organisation. Cette approche permet d'assurer une meilleure isolation des services, une gestion centralisée et une flexibilité accrue dans l'utilisation des ressources disponibles.

1.1.4. Gateway

Le Gateway, en informatique est un dispositif matériel et logiciel qui permet de relier deux réseaux informatiques, ou deux réseaux de télécommunications, aux caractéristiques différentes. Pour le cas de DGSR, c'est configurer selon la norme par Telma, le FAI.

1.1.5. Routeur

Un routeur est un dispositif qui permet de connecter plusieurs réseaux entre eux (par exemple, entre le réseau interne de la DGSR et Internet). Il prend en charge la gestion du trafic entrant et sortant, la redirection des paquets et la gestion de la bande passante.

Figure 4: Routeur



Source : Stock.adobe.com

1.1.6. Switch

Un switch est un dispositif réseau qui permet de relier plusieurs équipements (ordinateurs, imprimantes, etc.) au sein du même réseau local (LAN). Contrairement au hub qui diffuse les données à tous les périphériques, le switch transmet les données uniquement à l'équipement concerné, optimisant ainsi les performances du réseau.

Figure 5: Switch



Source : www.ebay.com

1.1.7. Point d'accès

Un point d'accès (Access Point) est un dispositif qui permet aux appareils sans fil de se connecter à un réseau filaire via Wi-Fi. Il sert d'intermédiaire entre les périphériques sans fil (comme les smartphones ou ordinateurs) et l'infrastructure réseau. Les points d'accès peuvent fonctionner en mode autonome, où ils gèrent eux-mêmes la connexion, ou en mode contrôlé, où ils sont gérés par un contrôleur centralisé pour une gestion plus facile de plusieurs appareils.

Figure 6: Point d'accès



Source : www.ebay.com

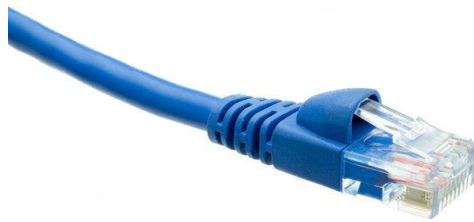
1.1.8. Câble Ethernet

Le câble Ethernet est utilisé pour relier les équipements HIFI et audio-vidéo à une connexion internet de manière fiable.

1.1.8.1. Câble rj45

Le câble rj45 est un type de câble Ethernet utilisé pour transmettre des données sur des réseaux locaux (LAN).

Figure 7: câble RJ45



Source : stock.adobe.com

1.1.8.2. Câble optique

La fibre optique est un fil en verre (silice) ou en plastique très fin, de quelques microns de diamètre. Elle permet de raccorder tous les périphériques à une prise délivrant la fibre.

Figure 8: câble fibre optique



Source : amazon.fr

1.1.9. Authentification

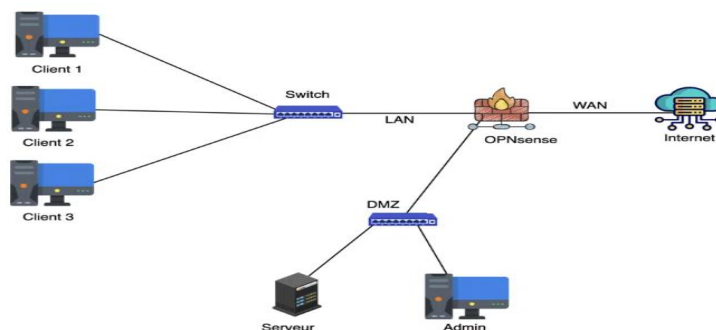
L'authentification consiste à vérifier l'identité d'un utilisateur. L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système) afin d'autoriser l'accès de cette entité à des ressources du système (systèmes, réseaux, applications) conformément au paramétrage du contrôle d'accès.

La Direction Générale de la Sécurité Routière utilise le login et mot de passe encrypté comme méthode d'authentification (Le type d'encryptage n'a pas été divulgué en raison de sécurité).

1.1.10. Pare-feu et équipements de sécurité

La sécurité des réseaux étant une priorité, la DGSR utilise des pare-feux placés entre le réseau interne et externe qui permet de filtrer les connexions non autorisées, bloquer les tentatives d'intrusion et protéger les serveurs sensibles, et le DMZ qui fourni l'accès aux services internet et ce, de façon sécurisée.

Figure 9: Pare-feu



Source : forum.level1techs.com

1.1.11. Port

Un port est un point d'entrée pour la communication réseau, identifié par un numéro. Il permet aux applications d'envoyer et de recevoir des données. Chaque type de service réseau utilise un port spécifique (par exemple, le port 80 pour HTTP, le port 443 pour HTTPS). La gestion des ports est essentielle pour assurer la sécurité et le bon fonctionnement des services.

1.1.12. Configuration des ports

La configuration des ports fait référence à la gestion des points d'accès pour les communications réseau. Chaque port sur un serveur ou un routeur permet de gérer une application spécifique (par exemple, un port pour le serveur web, un autre pour le serveur FTP). La configuration correcte des ports est essentielle pour assurer la sécurité et le bon fonctionnement du réseau.

1.1.13. Redirection des ports

La redirection des ports est une technique utilisée pour diriger le trafic réseau entrant sur un port spécifique d'un serveur vers un autre port ou un autre serveur. Cela permet, par exemple, de rendre certains services accessibles de l'extérieur tout en les protégeant du réseau interne. Elle permet d'optimiser l'accès à divers services, tels que des serveurs web, des serveurs FTP, des serveurs de messagerie ou des applications spécifiques, en dirigeant les connexions vers les bons serveurs internes. Cela réduit l'exposition du réseau et renforce la sécurité en ne permettant l'accès qu'aux ports nécessaires.

Une configuration correcte est essentielle pour éviter les vulnérabilités. Une mauvaise configuration peut exposer l'infrastructure à des risques, tandis qu'une bonne gestion permet de sécuriser l'accès aux services tout en protégeant le réseau interne.

2. TOPOLOGIE DE RESEAU

La topologie du réseau décrit la disposition physique et logique des éléments qui composent le réseau, y compris les connexions entre les serveurs, les routeurs, les switches et les stations de travail. Elle définit la manière dont les données circulent dans le réseau et comment les équipements sont interconnectés.

2.1. Type de topologie

Il existe plusieurs types de topologies réseau, chacune avec ses propres caractéristiques, avantages et inconvénients. Le choix de la topologie dépend généralement des besoins de l'organisation, du budget, de la taille du réseau, ainsi que des performances et de la fiabilité souhaitées. Voici quelques-unes des topologies les plus couramment utilisées.

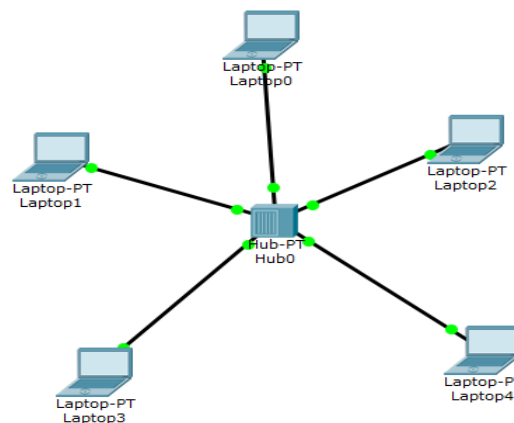
2.1.1. Topologie en bus

La topologie en bus est l'une des structures réseau les plus simples. Elle consiste à connecter tous les périphériques du réseau à un seul câble principal, appelé bus. Les données circulent dans une seule direction sur ce câble, et chaque périphérique reçoit les informations qui lui sont destinées. L'avantage principal de cette topologie réside dans sa simplicité et son coût réduit, car elle nécessite peu de câblage. Cependant, elle présente des inconvénients majeurs : une panne du câble principal entraîne l'arrêt complet du réseau, et la performance diminue à mesure que le nombre de périphériques connectés augmente. Ce type de topologie est souvent utilisé dans les petits réseaux ou les réseaux temporaires.

2.1.2. Topologie en étoile

Dans une topologie en étoile, chaque périphérique est connecté à un dispositif central, tel qu'un commutateur ou un hub. Cette structure est couramment utilisée dans les réseaux modernes, car elle offre une gestion simple et une bonne extensibilité. Si un périphérique tombe en panne, le reste du réseau continue de fonctionner, à condition que le dispositif central soit opérationnel. Cependant, si ce dernier tombe en panne, l'ensemble du réseau est paralysé. Cette topologie est particulièrement adaptée aux entreprises qui recherchent une solution fiable et facilement évolutive.

Figure 10: Topologie en étoile



Source : gitmind.com

2.1.3. Topologie en anneau

La topologie en anneau connecte chaque périphérique à deux autres pour former un cercle. Les données circulent d'un périphérique à l'autre, dans une direction unique (anneau simple) ou dans les deux sens (anneau double), jusqu'à atteindre leur destination. Bien que cette structure offre une transmission efficace et ordonnée, elle est vulnérable : une panne sur un seul périphérique ou un câble peut perturber l'ensemble du réseau. Pour cette raison, elle est de moins en moins utilisée, bien qu'elle ait été populaire dans les anciens réseaux locaux.

2.1.4. Topologie maillée

La topologie maillée est une structure dans laquelle chaque périphérique est connecté à tous les autres. Cela permet une redondance totale et une grande fiabilité, car les données peuvent emprunter plusieurs chemins pour atteindre leur destination. Ce type de topologie est souvent utilisé dans les réseaux critiques, où la fiabilité est essentielle, comme dans les

environnements militaires ou les systèmes de communication d'urgence. Toutefois, le coût élevé et la complexité de l'installation sont des inconvénients majeurs, surtout dans les grands réseaux.

2.1.5. Topologie en arbre

La topologie en arbre est une combinaison de plusieurs topologies en étoile, toutes reliées à un bus central. Elle suit une structure hiérarchique où les périphériques sont organisés en niveaux. Ce type de topologie est fréquemment utilisé dans les grandes organisations, car il permet une gestion efficace et l'expansion du réseau. Cependant, si le câble principal ou le bus central tombe en panne, cela peut affecter l'ensemble du réseau. Elle nécessite également un contrôle rigoureux pour éviter des goulots d'étranglement dans le trafic de données.

2.1.6. Topologie hybride

La topologie hybride combine deux ou plusieurs types de topologies, comme une combinaison d'étoile et de bus ou d'étoile et d'anneau. Cette flexibilité permet d'adapter le réseau aux besoins spécifiques d'une organisation. Bien qu'elle offre une grande souplesse et une meilleure tolérance aux pannes, sa conception et sa maintenance peuvent être complexes et coûteuses. Cette structure est généralement utilisée dans les réseaux de grande taille, où différents départements peuvent avoir des exigences réseau spécifiques.

Compte tenu des avantages et inconvénients de chaque topologie ainsi qu'après avoir analysé, la DGSR a optée pour la topologie en étoile pour son facilité à mettre en œuvre, ses liaisons indépendantes les unes des autres, son facilité d'ajouter un équipement ainsi que pour la centralisation de la supervision et maintenance de réseau.

2.2. Architecture réseau de la DGSR

L'architecture réseau de la Direction Générale de la Sécurité Routière (DGSR) suit un modèle client-serveur, où un serveur physique héberge plusieurs machines virtuelles à l'aide de VirtualBox. Cette solution permet une gestion optimale des ressources tout en réduisant les coûts matériels et de maintenance.

Le serveur physique est équipé d'un processeur Intel Xeon E5-2670 v3 avec 12 cœurs et 24 threads, offrant une capacité de traitement parallèle adaptée à la virtualisation. Il dispose de 16 Go de RAM DDR4, ce qui permet de gérer efficacement plusieurs machines virtuelles. Le stockage est assuré par un disque SSD de 2 To, configuré en RAID 1 pour garantir la rapidité et la sécurité des données.

Les machines virtuelles sont créées à l'aide de VirtualBox, permettant de virtualiser des serveurs pour des services spécifiques. Par exemple, un serveur web est alloué avec 4 Go de RAM et 2 cœurs de CPU, un serveur de base de données avec 16 Go de RAM et 6 cœurs de CPU, et un serveur de gestion interne avec 8 Go de RAM et 4 cœurs de CPU.

Grâce à cette architecture, la DGSR bénéficie d'une grande flexibilité dans la gestion de ses ressources, tout en assurant la sécurité, la haute disponibilité et l'efficacité de ses services.

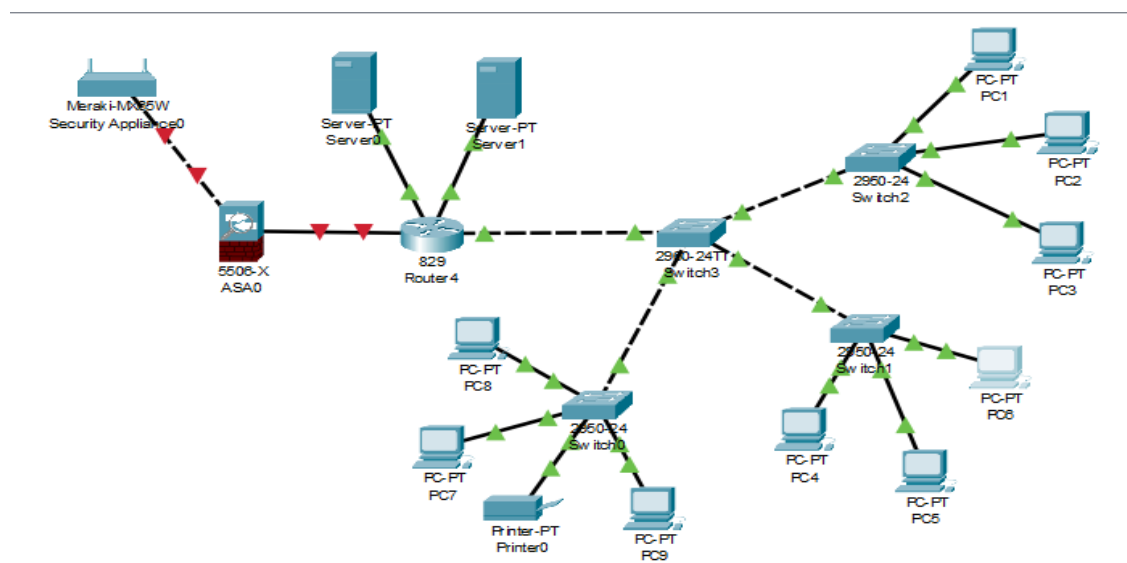
2.2.1. Avantage

Un seul serveur physique permet de centraliser les services, évitant ainsi d'avoir plusieurs machines physiques gourmandes en énergie et en maintenance. En cloisonnant les services dans des machines virtuelles distinctes, un problème affectant un serveur n'impacte pas forcément les autres. L'administration se fait depuis un seul point, simplifiant la maintenance et la supervision et qu'il est facile d'ajouter de nouveaux serveurs virtuels sans investir dans du matériel supplémentaire.

2.2.2. Inconvénients

Si le serveur physique tombe en panne, tous les serveurs virtuels deviennent inaccessibles. Une mauvaise allocation des ressources entre les serveurs virtuels peut entraîner des ralentissements et une gestion avancée des accès et des performances est nécessaire pour assurer la fluidité des services.

Figure 11: Architecture réseau de l'entreprise DGSR



Source : Investigation personnelle

2.2.3. Avantages et inconvénients de la virtualisation des serveurs

L'adoption d'une architecture virtualisée présente plusieurs avantages. Elle permet une meilleure gestion des ressources en allouant dynamiquement la puissance de calcul, la mémoire et le stockage en fonction des besoins des applications. Cette flexibilité améliore les performances et réduit les temps d'arrêt. De plus, la virtualisation facilite la mise en place de sauvegardes et de restaurations rapides en cas de panne. Toutefois, cette solution a aussi des inconvénients. La surcharge du serveur hôte peut entraîner des ralentissements si les ressources ne sont pas bien gérées. Par ailleurs, une panne matérielle affectant le serveur physique peut rendre inaccessibles tous les serveurs virtuels qui y sont hébergés, ce qui impose la mise en place de stratégies de redondance et de sauvegarde pour minimiser les risques.

Conclusion

Les équipements matériels et les technologies utilisés par la DGSR sont essentiels pour assurer la sécurité et le bon fonctionnement de son infrastructure réseau. Une bonne gestion de ces éléments, ainsi que des protocoles associés, est cruciale pour garantir l'intégrité et la confidentialité des données traitées. Les définitions présentées permettent de mieux comprendre le rôle de chaque composant dans l'ensemble de l'infrastructure, ainsi que les interactions entre les différents systèmes utilisés.

CHAPITRE II : MISE EN PLACE DE L'OUTIL

La mise en place de l'outil constitue une étape cruciale pour assurer la sécurité et l'efficacité du réseau. Dans ce chapitre, nous détaillons les étapes nécessaires pour l'installation et la configuration de l'outil retenu pour cette étude, à savoir OPNsense, ainsi que la préparation des machines virtuelles (VMs) indispensables à la simulation de l'environnement réseau. Cette phase de déploiement vise à garantir une infrastructure stable, performante et sécurisée, en tenant compte des meilleures pratiques en matière de cybersécurité.

1. PRESENTATION D'OPNSENSE

OPNsense est un système d'exploitation open-source basé sur FreeBSD, conçu pour offrir des solutions complètes de pare-feu, de routeur et de gestion de réseau dans des environnements professionnels et personnels. OPNsense est une alternative populaire à d'autres solutions de pare-feu comme pfSense, et il est largement utilisé pour protéger les réseaux locaux, contrôler le trafic entrant et sortant, ainsi que pour gérer des configurations complexes telles que le VPN, la détection d'intrusions et l'équilibrage de charge.

L'adoption d'OPNsense par la DGSR repose sur plusieurs raisons essentielles. Tout d'abord, il offre une sécurité avancée grâce à des fonctionnalités robustes. De plus, OPNsense permet une gestion efficace des ports grâce à des options de redirection précises, garantissant un contrôle optimisé du trafic entrant et sortant. Son interface web intuitive facilite grandement la configuration et le suivi du réseau. Enfin, sa compatibilité avec des environnements virtualisés en fait un choix idéal pour la DGSR, dont l'infrastructure repose sur un serveur physique unique hébergeant plusieurs serveurs virtuels, permettant ainsi une intégration fluide et efficace dans cette architecture.

Figure 12:Logo d'OPNsense



Source : anteor.com

2. PREPARATION DE L'ENVIRONNEMENT

Avant de procéder à l'installation d'OPNsense, il est essentiel de préparer l'environnement virtuel afin de créer des conditions optimales pour le déploiement. L'objectif est de simuler un environnement réseau réaliste où OPNsense jouera le rôle de pare-feu et de routeur.

2.1 Prérequis

Avant d'installer OPNsense, il est essentiel de s'assurer que l'on dispose des éléments suivants :

- VirtualBox installé sur l'ordinateur hôte, permettant la création et l'exécution de machines virtuelles.
- L'image ISO d'OPNsense, téléchargeable depuis le site officiel (<https://opnsense.org/download>).
- Une configuration matérielle minimale comprenant au moins 2 Go de RAM, 10 Go d'espace disque et deux interfaces réseau (WAN et LAN).

Ces prérequis garantissent un bon fonctionnement d'OPNsense, notamment pour une utilisation en laboratoire ou en test avant déploiement dans un environnement réel.

2.2 Configuration des machines virtuelles

La première étape consiste à créer plusieurs machines virtuelles distinctes sur le poste hôte : l'une dédiée à l'installation d'OPNsense, qui agira comme pare-feu, et d'autres pour simuler des serveurs virtuels nécessaires à l'infrastructure réseau.

2.3 Création des machines virtuelles

Lors de la création des machines virtuelles, il est important de définir des ressources matérielles adaptées. La machine dédiée à OPNsense nécessite des performances légèrement supérieures à celles des serveurs virtuels, car elle assurera la gestion du trafic réseau.

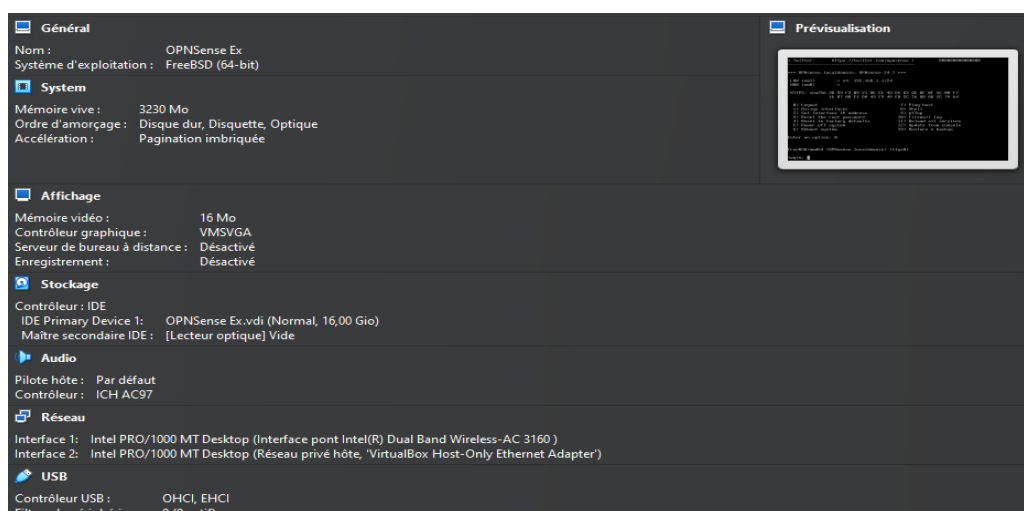
- Lancer VirtualBox et cliquer sur "Nouvelle" pour créer une nouvelle machine virtuelle.
- Nommer la machine (exemple : "OPNsense") et sélectionner FreeBSD (64-bit) comme type de système d'exploitation.
- Allouer la mémoire RAM (au moins 2 Go pour assurer de bonnes performances).
- Créer un disque dur virtuel d'au moins 10 Go, en choisissant le format VDI (VirtualBox Disk Image).

Configurer les interfaces réseau :

- Aller dans Paramètres > Réseau.
- Activer l'adaptateur 1 et le configurer en mode NAT (pour la connexion externe WAN).
- Activer l'adaptateur 2 en mode Réseau interne (pour la connexion LAN entre les machines du réseau virtuel).

Ces configurations permettent à OPNsense de jouer son rôle de pare-feu entre un réseau local et Internet, comme ce serait le cas dans un environnement réel.

Figure 13 : Configuration de la machine virtuelle dans VirtualBox.



Source : Investigation personnelle

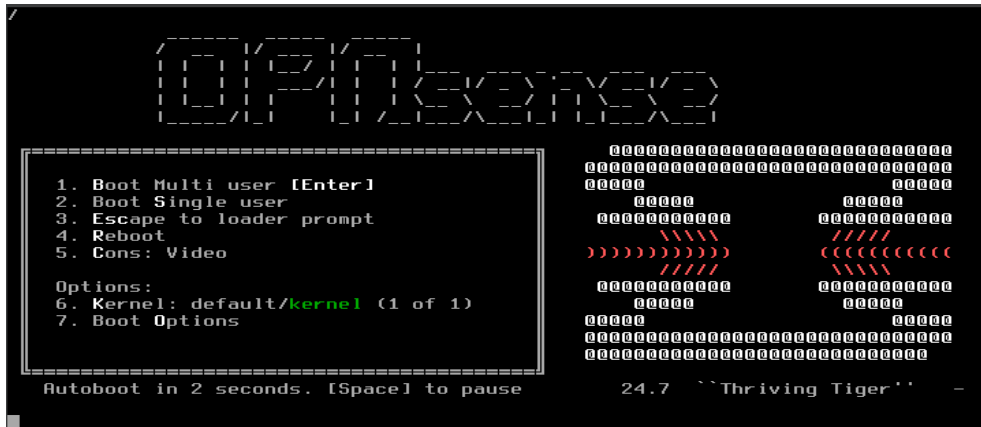
3. INSTALLATION D'OPNSENSE

Une fois la machine virtuelle créée, il est temps d'installer OPNsense en utilisant l'image ISO téléchargée précédemment.

3.1. Sélection de l'ISO d'OPNsense

L'ISO d'OPNsense contient tous les fichiers nécessaires à l'installation du système. Pour l'utiliser, il faut s'assurer qu'il est bien monté dans le lecteur virtuel de la machine. Dans le menu de sélection du disque de démarrage, il suffit d'ajouter l'image ISO et de la choisir comme source principale. Une fois cette sélection effectuée, le programme d'installation démarre automatiquement, permettant d'accéder à l'interface de démarrage d'OPNsense.

Figure 14: Menu de démarrage d'opnsense



Source : Investigation personnelle

3.2. Lancement du processus d'installation

L'installation d'OPNsense se fait via une interface en ligne de commande. Pour commencer, il faut se connecter avec les identifiants par défaut : Nom d'utilisateur : installer, Mot de passe : opnsense.

Une fois connecté, l'utilisateur accède au menu principal du programme d'installation. Il doit ensuite sélectionner l'option Install OPNsense pour initier le processus d'installation sur le disque dur virtuel.

Figure 15: Processus d'installation d'opnsense étape 1

```
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/ufs/OPNsense_Install
Tue Mar  4 14:06:25 UTC 2025

*** OPNsense.localdomain: OPNsense 24.7 ***

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      -> v4/DHCP4: 192.168.56.106/24

HTTPS: sha256 18 82 8F 0B D0 D3 DD 5E 5A EE 1F C7 93 94 AF 4C
              62 BD 34 8E 27 3D C2 35 3C F8 31 CB 08 99 B8 CC
SSH:  SHA256 YnvXTeu7vPg5UF2epky4Lc0u0e40uHX15rSdLxcC4M0 (ECDSA)
SSH:  SHA256 orSNgyi7EpW1rWhT3+4BrGD/pE8KKeaF+QXCjJAIn/w (ED25519)
SSH:  SHA256 YjQQwR7HK0yVnom+zJZhEx9zqiQi9Tg1JcBmqL0TNiY (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

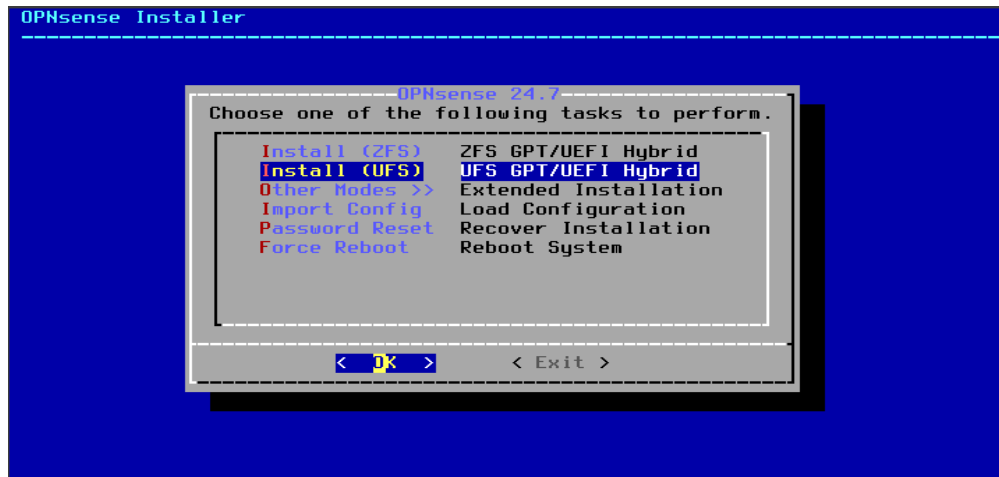
Source : Investigation personnelle

3.3. Type d'installation

L'installateur d'OPNsense demande alors à l'utilisateur de choisir un disque sur lequel le système sera installé. Dans un environnement virtualisé, il est important de sélectionner le disque dédié à la machine. L'installation peut être réalisée automatiquement en utilisant une

partition GPT/UEFI, ou bien en mode manuel pour une configuration plus avancée. Une fois le disque sélectionné, l'utilisateur valide son choix pour lancer l'installation.

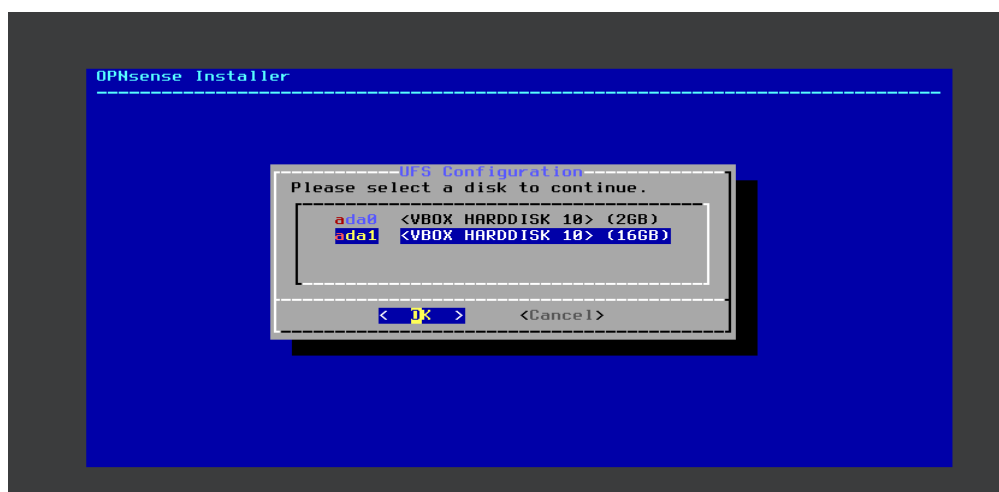
Figure 16: Processus d'installation d'opnsense étape 2



3.4. Sélection du disque

Lors de l'installation d'OPNsense, il est nécessaire de sélectionner le disque cible, généralement identifié sous FreeBSD par des noms tels que ada0, ada1, etc. En choisissant ada1, l'installation s'effectuera sur ce disque, entraînant l'effacement de ses données.

Figure 17: Processus d'installation d'opnsense étape 3

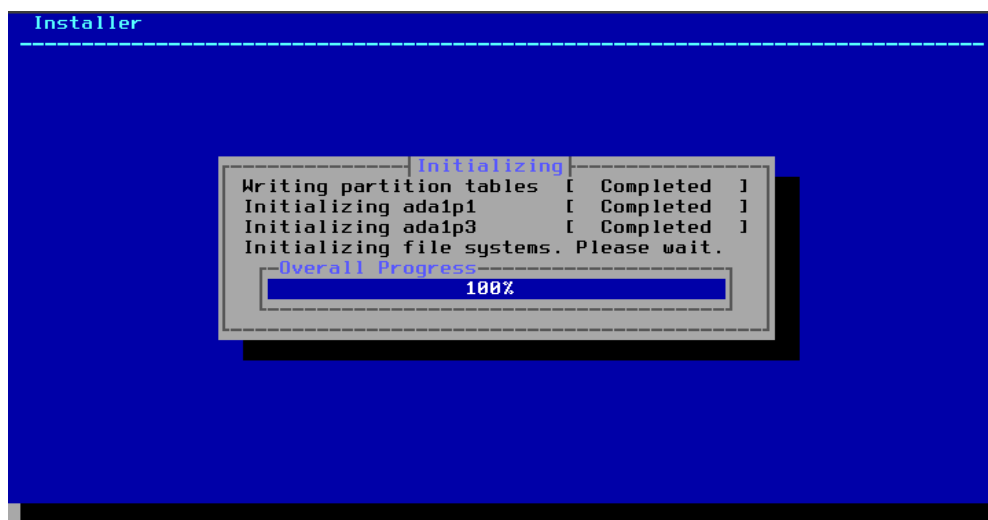


Source : Investigation personnelle

3.5. Formatage des fichiers

Après la sélection du disque, le programme d'installation procède au formatage et à la copie des fichiers nécessaires au fonctionnement d'OPNsense. Cette étape peut prendre quelques minutes, selon la vitesse du disque virtuel et les performances de la machine hôte. Il est important de ne pas interrompre ce processus, car cela pourrait entraîner des erreurs et nécessiter une réinstallation complète.

Figure 18: Processus d'installation d'opnsense étape 4



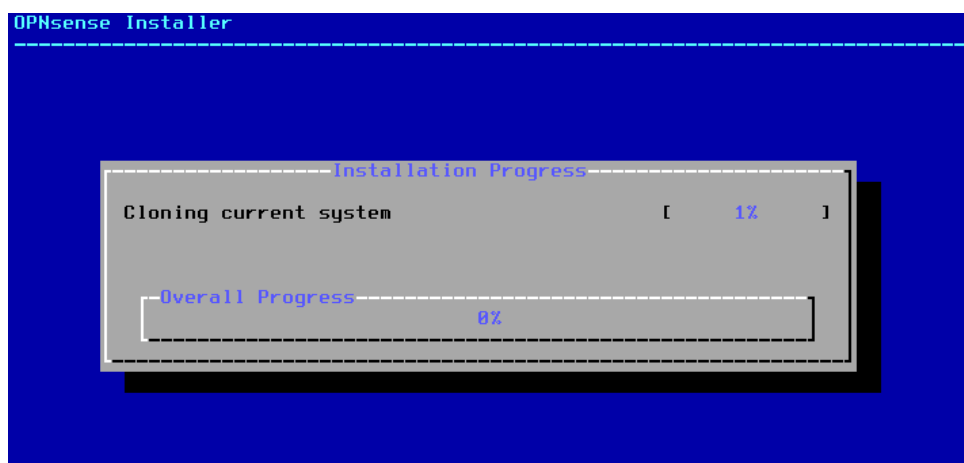
Source : Investigation personnelle

3.6. Copie des fichiers système

Une fois le disque sélectionné, le processus d'installation d'OPNsense démarre par la copie des fichiers système. Cette étape, appelée "**Cloning system current**", consiste à dupliquer l'image du système d'exploitation sur le disque choisi.

L'opération peut prendre quelques minutes en fonction des performances du disque et de l'environnement d'installation. Une fois terminée, l'installateur passe aux configurations finales avant le redémarrage du système.

Figure 19: Processus d'installation d'opnsense étape 5



Source : Investigation personnelle

3.7. Retrait du support d'installation et redémarrage

Lorsque l'installation est finalisée, il est nécessaire de retirer l'image ISO du lecteur virtuel pour éviter un redémarrage sur le programme d'installation. Une fois l'ISO retirée, l'utilisateur peut sélectionner l'option Reboot System pour redémarrer la machine. Après le redémarrage, OPNsense démarre normalement et affiche une interface en ligne de commande permettant d'effectuer les configurations réseau et de sécuriser le pare-feu.

Figure 20: Installation réussie d'opnsense

```
>>> Invoking start script 'freebsd'
>>> Invoking start script 'syslog'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK

>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Wed Nov 27 08:10:46 UTC 2024

*** OPNsense.localdomain: OPNsense 24.7 ***

LAN (em1)      -> v4: 192.168.1.1/24
WAN (em0)      -> v4/DHCP4: 192.168.12.123/24

HTTPS: sha256 3D 93 F3 09 21 AE EE 43 D5 D3 8E AF 0F 5C 00 F7
              16 B7 8B E1 D8 43 E9 49 EA CC 76 8B 8A 2C 79 64

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

Source : Investigation personnelle

L'installation d'OPNsense est rapide et simple, grâce à son interface conviviale. Après le redémarrage, le système est prêt à être configuré pour une gestion efficace du réseau.

3.8. Mise à jour du système

Avant de procéder à des configurations avancées, il est recommandé de mettre à jour le firmware d'OPNsense pour bénéficier des dernières améliorations de sécurité et de performance.

Conclusion

L'installation et la configuration d'OPNsense dans un environnement virtualisé avec VirtualBox offrent un excellent moyen d'explorer les fonctionnalités de cet outil sans nécessiter de matériel dédié. Cette approche permet aux administrateurs de tester différentes configurations, d'analyser le comportement du pare-feu et d'expérimenter des scénarios de sécurité avant une éventuelle mise en production.

Grâce à sa flexibilité et à ses nombreuses options de gestion, OPNsense s'impose comme une solution fiable pour le contrôle et la sécurisation des réseaux. Son interface web ergonomique facilite son utilisation, rendant les opérations de filtrage et de surveillance accessibles à tous.

PARTIE III : CADRE PRATIQUE

CHAPITRE I : FONCTIONNALITES

Dans ce chapitre, l'accent est mis sur la redirection des ports, une fonctionnalité essentielle pour assurer l'accessibilité des services tout en maintenant un niveau de sécurité élevé au sein de l'infrastructure réseau de la DGSR. L'objectif est d'expliquer en détail son fonctionnement, son utilité et son impact sur la gestion du trafic entrant et sortant. Cette analyse permettra ainsi de mieux comprendre les enjeux techniques et sécuritaires associés à la redirection des ports et d'illustrer son rôle central dans l'architecture réseau de la DGSR.

1. Introduction à la redirection des ports et son importance

Dans le domaine de la gestion des réseaux, la redirection des ports est une fonctionnalité incontournable, utilisée pour contrôler, filtrer et sécuriser les flux de données entre un réseau interne et des connexions extérieures. Elle permet à une organisation d'exposer certains services en ligne tout en maintenant un niveau de sécurité optimal. Dans un environnement où plusieurs serveurs et applications doivent être accessibles à distance, la redirection des ports joue un rôle fondamental dans la gestion de l'accessibilité et la sécurisation des ressources sensibles.

Concrètement, cette technique consiste à rediriger une requête reçue sur un port spécifique d'un pare-feu ou d'un routeur vers une machine spécifique à l'intérieur du réseau. Par exemple, lorsqu'un utilisateur externe tente d'accéder à un service hébergé localement sur un serveur web, il envoie une requête à l'adresse IP publique de l'organisation sur un port donné (par exemple, le port 80 pour le HTTP ou le port 443 pour le HTTPS). Grâce à la redirection des ports, le pare-feu peut acheminer cette requête vers le serveur interne correspondant, garantissant ainsi une connectivité fluide et sécurisée.

Dans le cadre du projet de la DGSR, la redirection des ports est essentielle pour assurer la disponibilité des services sans compromettre la sécurité du réseau interne. Elle permet notamment de restreindre l'accès aux ressources aux seules adresses IP autorisées, tout en optimisant la gestion du trafic entrant.

2. La fonctionnalité de la redirection des ports dans opnsense

OPNsense est une solution de pare-feu open-source largement utilisée dans l'administration des réseaux en raison de sa flexibilité, de son interface intuitive et de ses fonctionnalités avancées de filtrage et de gestion du trafic. Il repose sur Packet Filter (PF), un moteur de pare-feu puissant qui assure la gestion des flux entrants et sortants avec une grande précision.

Lorsqu'un paquet de données arrive sur une interface réseau d'OPNsense, plusieurs étapes sont suivies avant qu'il ne soit transmis à sa destination finale :

2.1 Vérification des règles NAT

Dans un réseau sécurisé, la gestion du trafic entrant est essentielle pour assurer un bon fonctionnement des services et une protection contre les menaces. OPNsense, en tant que pare-feu avancé, vérifie systématiquement si une règle de redirection des ports s'applique à une connexion entrante avant d'autoriser son passage vers le réseau interne. Cette vérification permet de s'assurer que le trafic est bien dirigé vers la bonne machine et que les connexions non autorisées sont bloquées.

Le contrôle des accès est un élément clé dans l'application des règles NAT. Seul le trafic autorisé est redirigé, ce qui réduit considérablement les risques d'intrusions. Grâce à cette vérification, OPNsense optimise la gestion des connexions entrantes et garantit que seuls les services nécessaires sont accessibles. Cela améliore également la sécurité en évitant l'exposition directe des machines internes aux attaques potentielles provenant d'Internet.

2.1.1 Filtrage du trafic

Lorsqu'une règle de redirection des ports est active, OPNsense analyse chaque paquet entrant pour vérifier si ses caractéristiques correspondent aux critères définis, tels que l'adresse IP source, l'adresse IP de destination, le protocole utilisé et le port cible. Après cette vérification, il applique les règles de filtrage configurées afin de décider si la connexion doit être autorisée ou bloquée.

Ce filtrage empêche les connexions non autorisées et protège les services internes contre d'éventuelles attaques. Il permet également une meilleure gestion du trafic en limitant les requêtes inutiles qui pourraient surcharger le réseau. Grâce à cette approche, seules les connexions respectant les critères définis par l'administrateur réseau sont autorisées, garantissant ainsi un contrôle strict de l'accès aux services.

Par exemple, si une entreprise héberge un serveur web sur son réseau local à l'adresse IP 192.168.1.100 sur le port 80 et souhaite le rendre accessible depuis Internet via le port 8080, elle configure une règle NAT sur OPNsense. Lorsqu'un utilisateur externe tente d'accéder à ce service en tapant l'adresse publique suivie du port 8080 dans son navigateur, OPNsense examine d'abord l'adresse IP source de la requête et vérifie si elle est autorisée. Ensuite, il analyse le protocole utilisé, dans ce cas HTTP, pour s'assurer qu'il correspond à la règle

définie. Si toutes les conditions sont remplies, OPNsense redirige automatiquement le trafic vers le serveur web interne.

2.1.2 Transmission du paquet

Si le paquet satisfait aux critères établis par les règles NAT et de filtrage, OPNsense assure sa transmission vers le serveur interne correspondant. Cette transmission garantit l'intégrité des données, en veillant à ce qu'aucune modification non autorisée ne soit apportée au paquet. Elle permet également d'appliquer des restrictions spécifiques, comme l'accès limité à certaines plages horaires ou à des adresses IP spécifiques. Cela est particulièrement utile pour les entreprises qui souhaitent sécuriser leurs services tout en assurant un accès fluide aux utilisateurs légitimes.

Un autre exemple courant concerne l'accès à un serveur SSH interne. Si un utilisateur distant envoie une requête pour se connecter à ce serveur via le port 2222 de l'adresse IP publique, OPNsense analyse d'abord la requête et vérifie si elle respecte les règles de filtrage. Ensuite, il modifie l'adresse de destination du paquet afin de rediriger la connexion vers le serveur interne configuré sur l'adresse 192.168.1.50 avec le port 22. Une fois cette redirection effectuée, la session reste sécurisée grâce aux restrictions imposées par l'administrateur réseau, telles que l'autorisation d'accès uniquement depuis certaines adresses IP approuvées.

Grâce à ce fonctionnement, OPNsense permet de contrôler précisément quel service est accessible et par qui, réduisant ainsi les risques d'attaques malveillantes comme les tentatives d'intrusion ou le scanning de ports.

3. Mise en œuvre de la redirection des ports dans opnsense

L'implémentation de la redirection des ports repose principalement sur la configuration de règles NAT dans OPNsense.

3.1 Création et configuration des règles NAT

La redirection de port ou le port Forwarding est une fonctionnalité essentielle d'OPNsense permettant de rediriger le trafic entrant d'un port spécifique vers une machine du réseau interne. Cette configuration est particulièrement utile pour héberger des services accessibles depuis l'extérieur, comme un serveur web, SSH, ou un serveur de jeux.

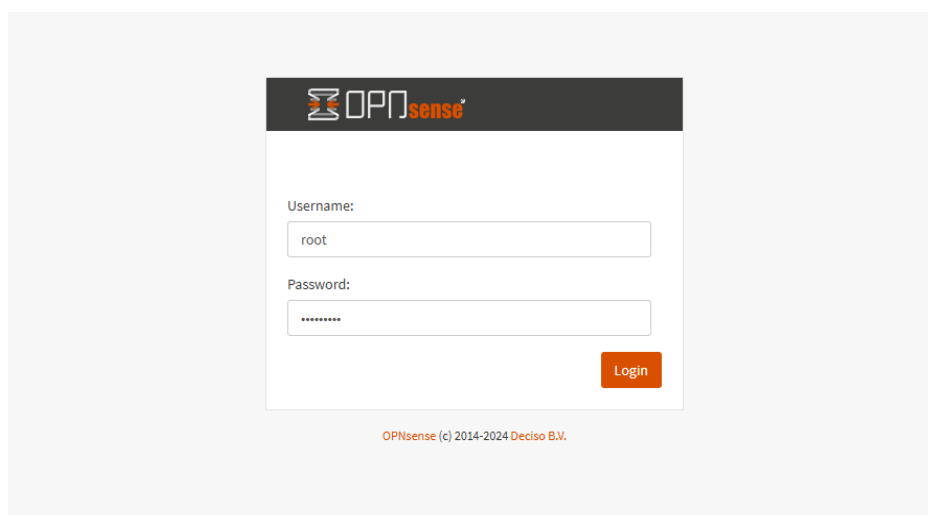
Dans cette section, nous allons voir comment configurer une règle NAT étape par étape en utilisant l'interface graphique d'OPNsense.

3.1.1 Accéder à l'interface opnsense

Avant de configurer les règles NAT, il est essentiel d'accéder à l'interface d'administration d'OPNsense. Pour cela, ouvrez un navigateur web et saisissez l'adresse IP du pare-feu OPNsense dans la barre d'adresse (exemple : `https://192.168.1.1`). Cette adresse correspond à l'interface de gestion du pare-feu, permettant d'accéder aux différentes configurations.

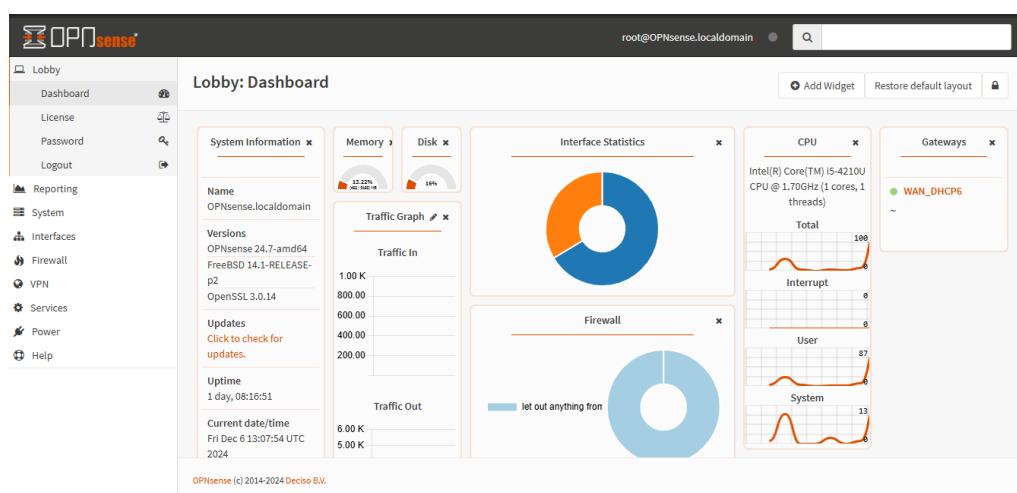
Une fois la page de connexion affichée, entrez les identifiants administrateur. Par défaut, le nom d'utilisateur est root et le mot de passe est opnsense. Après authentification, l'interface d'administration s'ouvre, donnant accès aux réglages nécessaires pour configurer les règles NAT.

Figure 21: Page de connexion OPNsense.



Source : Investigation personnelle

Figure 22: Tableau de bord après connexion.

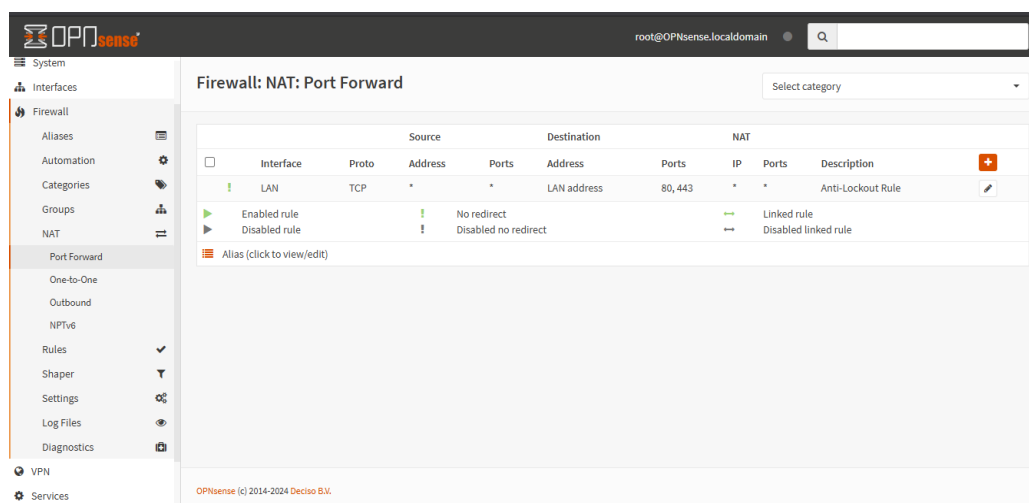


Source : Investigation personnelle

3.1.2 Accéder aux règle NAT

Les règles NAT se trouvent dans le menu pare-feu d'OPNsense. Elles permettent de définir comment le trafic doit être redirigé vers une machine interne. Dans le menu latéral, clique sur "Firewall" > "NAT" puis sélectionne l'onglet "Port Forward".

Figure 23: Navigation vers Firewall > NAT > Port Forward.



Source : Investigation personnelle

3.1.3 Création d'une règle NAT pour la redirection des ports

Une fois dans la section NAT, nous allons créer une règle de redirection de port pour permettre l'accès à un service interne depuis l'extérieur.

1. Clique sur "Add" pour ajouter une nouvelle règle.
2. Remplis les champs comme suit :
 - Interface : WAN (car le trafic provient d'Internet).
 - Protocol : TCP ou UDP (selon le service que tu veux rediriger).
 - Destination : WAN Address (adresse publique du pare-feu).
 - Destination Port Range : Sélectionne le port externe (ex : 80 pour HTTP).
 - Redirect Target IP : Saisis l'adresse IP locale du serveur cible (ex : 192.168.12.132).
 - Redirect Target Port : Saisis le port du service sur le serveur interne (ex : 80 pour HTTP).
3. Coche la case "Add associated filter rule" pour autoriser automatiquement le trafic.
4. Clique sur "Save" et ensuite "Apply Changes" pour appliquer la configuration.

Figure 24(1/4): Formulaire rempli pour la règle NAT.

The screenshot displays the OPNsense web interface. The top header shows the OPNsense logo and the user 'root@OPNsense.localdomain'. The left sidebar contains a navigation menu with options: System, Interfaces, Firewall (selected), Aliases, Automation, Categories, Groups, NAT, Port Forward (selected), One-to-One, Outbound, NPTv6, Rules, Shaper, Settings, Log Files, and Diagnostics. The main content area is titled 'Firewall: NAT: Port Forward' and contains the 'Edit Redirect entry' form. The form includes the following fields and values:

Field	Value
Disabled	☐ Disable this rule
No RDR (NOT)	☐
Interface	LAN
TCP/IP Version	IPv4
Protocol	TCP
Source	Advanced
Destination / Invert	☐
Destination	LAN address

Figure 25(2/4): Formulaire rempli pour la règle NAT.

Figure 26(3/4): Formulaire rempli pour la règle NAT.

Figure 27(4/4): Formulaire rempli pour la règle NAT.

Firewall: NAT: Port Forward

Select category

The NAT configuration has been changed.
 You must apply the changes in order for them to take effect.

Apply changes

	Source			Destination		NAT				
☐	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description	☐ ☐ ☐ ☐ ☐
☒	LAN	TCP	*	*	LAN address	80, 443	*	*	Anti-Lockout Rule	☐
☐	LAN	TCP	*	*	LAN address	8085	192.168.12.132	8085	redirection vers le serveur web	☐ ☐ ☐ ☐ ☐

Source : Investigation personnelle

3.1.4 Vérification et testes

Une fois la règle NAT créée, il est essentiel de vérifier que la redirection fonctionne correctement afin d'assurer l'accessibilité du service tout en garantissant la sécurité du réseau. Cette étape permet de s'assurer que les paquets sont bien dirigés vers la machine cible et que le service est opérationnel depuis l'extérieur.

3.1.4.1 Test depuis une machine externe

Pour valider la configuration, il est recommandé d'effectuer des tests à partir d'une machine externe au réseau local.

Dans le cas d'un serveur web, l'utilisateur peut ouvrir un navigateur et saisir l'adresse IP publique suivie du port redirigé. Par exemple, si le serveur est censé être accessible sur le port 8085, il suffit d'entrer l'URL suivante dans la barre d'adresse du navigateur : 192.168.1.1:8085. Si la redirection fonctionne correctement, la page web du serveur doit s'afficher sans erreur. En cas d'échec, il est nécessaire de vérifier la configuration du NAT, l'état du pare-feu ainsi que l'accessibilité du service sur la machine cible.

Pour un service SSH, la connexion peut être testée en tentant d'accéder au serveur via la commande suivante : `ssh user@[adresse_IP_publicue]`. Si la connexion est établie avec succès et qu'il est possible de s'authentifier sur le serveur distant, cela signifie que la règle NAT est correctement appliquée. Dans le cas contraire, il convient d'examiner les éventuels blocages au niveau du pare-feu ou de la configuration SSH du serveur.

Ces tests sont cruciaux pour s'assurer du bon fonctionnement des règles NAT et pour identifier d'éventuelles erreurs de configuration ou restrictions empêchant la redirection des paquets.

3.2 Vérification avec les logs opnsense

Une fois la redirection des ports configurée, il est important de vérifier que le trafic est bien redirigé vers l'IP interne prévue. OPNsense offre un outil de journalisation permettant de suivre en temps réel l'activité du pare-feu et de s'assurer que les règles NAT fonctionnent comme prévu.

Pour effectuer cette vérification, il faut accéder à l'interface d'administration d'OPNsense, puis naviguer vers Firewall > Log Files > Live View. Cet outil affiche les connexions entrantes et sortantes, y compris celles affectées par les règles de redirection des ports.

Dans Live View, il est possible de rechercher des logs spécifiques en filtrant par adresse IP source, adresse IP de destination ou port utilisé. Par exemple, si une règle NAT a été configurée pour rediriger le trafic entrant sur le port 8085 vers un serveur interne, il faut observer si des paquets correspondant à cette règle apparaissent dans les logs et s'ils sont bien transmis à l'IP interne cible.

Figure 28: Live View montrant le trafic entrant.

Interface	Time	Source	Destination	Proto	Label
WAN	2025-02-04T08:42:27	[fe80:a0027ff:fe33:e7dd]:28412	[2604:1380:4601:5501::2:1]:53	udp	let out anything from firewall host itself
WAN	2025-02-04T08:42:27	[fe80:a0027ff:fe33:e7dd]:28358	[2001:4100:700:335d:8:53]	udp	let out anything from firewall host itself
WAN	2025-02-04T08:42:27	[fe80:a0027ff:fe33:e7dd]:45280	[2604:1380:2:6002::41:1]:53	udp	let out anything from firewall host itself
WAN	2025-02-04T08:42:27	192.168.1.100:25139	185.209.85.151:53	udp	let out anything from firewall host itself (force gw)
WAN	2025-02-04T08:42:27	192.168.1.100:25497	23.150.41.54:53	udp	let out anything from firewall host itself (force gw)
WAN	2025-02-04T08:42:26	192.168.1.100:55544	102.130.49.148:53	udp	let out anything from firewall host itself (force gw)
WAN	2025-02-04T08:42:26	[fe80:a0027ff:fe33:e7dd]:33601	[2001:43f8:d60:300::201]:53	udp	let out anything from firewall host itself
WAN	2025-02-04T08:42:26	[fe80:a0027ff:fe33:e7dd]:32984	[2a03:7900:104:1::2]:53	udp	let out anything from firewall host itself
WAN	2025-02-04T08:42:26	192.168.1.100:48892	185.209.85.151:53	udp	let out anything from firewall host itself (force gw)
lan	2025-02-04T08:42:26	fe80:81ef:da96:b83:1cf	fe80:a0027ff:fe33:a41f	ipv6-icmp	IPv6 RFC4890 requirements (ICMP)
WAN	2025-02-04T08:42:26	[fe80:a0027ff:fe33:e7dd]:30834	[2604:1380:2:6002::41:1]:53	udp	let out anything from firewall host itself

Source : Investigation personnelle

CHAPITRE II : RESULTATS

Après avoir mis en place la redirection des ports à l'aide d'OPNsense, il est essentiel d'analyser les résultats obtenus afin d'évaluer l'efficacité de cette configuration. Ce chapitre présente les impacts de la redirection des ports sur la sécurité et la performance du réseau de la DGSR. Nous examinerons les améliorations observées en matière de gestion du trafic, de protection contre les menaces extérieures, ainsi que les bénéfices apportés en termes d'optimisation du réseau.

1. Amélioration de la gestion du trafic

L'un des premiers résultats observés après l'implémentation de la redirection des ports concerne l'optimisation de la gestion du trafic réseau. Grâce à OPNsense, il est désormais possible de mieux structurer les flux entrants et sortants, en attribuant des règles précises de redirection en fonction des besoins de la DGSR.

Avant la mise en place de cette solution, le réseau présentait des problèmes de congestion et des difficultés d'acheminement des paquets, ce qui pouvait ralentir les services et engendrer des pertes de connexion. Avec OPNsense, chaque port est configuré pour diriger les connexions vers les bons services ou machines, garantissant ainsi une fluidité optimale du trafic.

En segmentant les flux et en appliquant des politiques de redirection adaptées, la DGSR bénéficie d'une gestion plus fine de son réseau. Cela permet notamment d'éviter les conflits d'adressage IP et d'assurer une meilleure répartition de la bande passante entre les différentes applications et utilisateurs.

2. Renforcement de la sécurité du réseau

Un autre avantage majeur de la redirection des ports est le renforcement significatif de la sécurité du réseau. Avant l'implémentation de cette solution, certaines ressources de la DGSR étaient directement exposées à Internet, augmentant ainsi le risque d'intrusion et de cyberattaques. Grâce aux règles de filtrage et de redirection des ports, seules les connexions autorisées peuvent désormais accéder aux services internes.

OPNsense offre la possibilité de restreindre l'accès aux ports en fonction de l'adresse IP source, du protocole utilisé et des plages horaires définies. Cette approche permet de minimiser la surface d'attaque en limitant l'exposition des services sensibles. De plus, en couplant la redirection des ports avec un pare-feu et un système de détection des intrusions, il devient plus facile d'identifier et de bloquer les tentatives d'accès non autorisées.

Un autre aspect sécuritaire important est la mise en place de logs et d'alertes en temps réel. Chaque tentative de connexion suspecte est enregistrée, permettant aux administrateurs réseau de réagir rapidement en cas de menace potentielle. Ce suivi proactif améliore considérablement la résilience du réseau face aux cyberattaques.

3. Optimisation des performances des services internes

Outre la gestion du trafic et la sécurité, la redirection des ports a permis d'améliorer les performances globales des services internes de la DGSR. En redirigeant les connexions vers les bonnes machines et en évitant les goulots d'étranglement, les temps de réponse des applications critiques ont été réduits.

Auparavant, l'accès à certains services internes pouvait être lent ou instable en raison d'une mauvaise gestion des flux. Avec la nouvelle configuration, les requêtes sont traitées plus rapidement, ce qui améliore l'expérience utilisateur et la productivité des employés.

L'impact est également visible sur l'équilibrage de charge entre les différents serveurs. En attribuant des ports spécifiques à certaines ressources stratégiques, il devient possible de mieux répartir la charge de travail, réduisant ainsi les risques de surcharge et de défaillance des services.

4. Réduction des erreurs de configurations et facilité de maintenance

Avant la mise en place de la redirection des ports via OPNsense, la gestion des accès réseau était souvent sujette à des erreurs de configuration. Des ports ouverts inutilement ou mal redirigés pouvaient engendrer des dysfonctionnements, compromettant ainsi la stabilité du réseau.

Grâce à OPNsense, l'administration des ports est désormais centralisée et simplifiée. L'interface graphique intuitive permet de visualiser en un coup d'œil les règles en place, facilitant ainsi les modifications et les ajustements en cas de besoin. Cette centralisation réduit également les erreurs humaines et garantit une meilleure cohérence des configurations réseau.

De plus, la possibilité de sauvegarder et de restaurer les configurations apporte une flexibilité précieuse en cas de nécessité de rollback. Si un problème survient après une modification, il est possible de revenir rapidement à un état stable, minimisant ainsi les interruptions de service.

Conclusion

L'implémentation de la redirection des ports avec OPNsense a apporté des améliorations significatives à la DGSR, tant sur le plan de la gestion du trafic que de la sécurité et des performances. En structurant les flux réseau de manière optimale, la DGSR bénéficie d'une infrastructure plus robuste et mieux sécurisée contre les menaces potentielles.

Les résultats obtenus démontrent l'importance d'une gestion rigoureuse des accès réseau pour garantir la stabilité et la sécurité des services. Grâce aux fonctionnalités avancées d'OPNsense, il est désormais possible de contrôler finement les connexions et de prévenir les risques liés aux intrusions et aux erreurs de configuration. Cette approche permet à la DGSR de disposer d'un réseau fiable, performant et sécurisé, en adéquation avec ses besoins opérationnels.

CHAPITRE III : PERSPECTIVE D'AVENIR

Après avoir mis en place la redirection des ports via OPNsense et analysé les résultats obtenus, il est important d'envisager les perspectives d'avenir pour améliorer et pérenniser cette solution. Ce chapitre explore les évolutions possibles, les améliorations techniques envisageables et les recommandations pour garantir une gestion réseau encore plus efficace et sécurisée au sein de la DGSR.

1. Renforcement de la sécurité

Bien que la redirection des ports permette de mieux gérer les accès au réseau et de limiter l'exposition des services, il est essentiel de renforcer davantage la sécurité en intégrant d'autres solutions complémentaires.

Une amélioration essentielle serait l'intégration d'un système de détection et de prévention des intrusions (IDS/IPS), notamment Snort, dans OPNsense pour renforcer la sécurité du réseau. Cet outil analyse en temps réel les paquets circulant sur le réseau, identifie les tentatives d'intrusion et bloque automatiquement les connexions suspectes. Grâce à sa base de signatures régulièrement mise à jour, Snort est capable de détecter une large gamme de menaces, allant des attaques par force brute aux exploits connus. Son intégration permet ainsi de protéger efficacement l'infrastructure tout en offrant une visibilité détaillée sur les événements de sécurité.

Par ailleurs, l'utilisation d'une authentification multi-facteurs (MFA) pour l'accès aux services critiques renforcerait la protection des comptes administratifs et éviterait les risques liés aux compromissions de mots de passe. Cette méthode de sécurité ajouterait une couche supplémentaire de vérification avant d'autoriser une connexion.

Enfin, il serait pertinent d'envisager l'adoption d'un système de VPN (Virtual Private Network) pour les connexions à distance. En chiffrant le trafic réseau, le VPN garantirait une meilleure confidentialité et empêcherait l'interception des données par des tiers malveillants.

2. Automatisation et supervision avancée du réseau

À mesure que les infrastructures réseau évoluent, il devient indispensable de mettre en place des solutions permettant d'automatiser certaines tâches de gestion et de surveiller en temps réel l'état du réseau.

L'intégration d'outils de monitoring avancés, comme Zabbix ou Prometheus, permettrait aux administrateurs de la DGSR de suivre en permanence les performances du réseau, de

détecter rapidement les anomalies et de réagir efficacement en cas de panne. Grâce aux tableaux de bord dynamiques et aux alertes automatisées, la supervision du réseau serait facilitée et les temps d'indisponibilité réduits.

En parallèle, l'automatisation des configurations via des scripts ou des outils comme Ansible pourrait permettre de simplifier la gestion des règles de redirection des ports. Cela éviterait les erreurs humaines et assurerait une uniformité dans l'application des politiques de sécurité sur l'ensemble des équipements.

3. Scalabilité et adaptation aux besoins futur

Avec l'évolution constante des besoins de la DGSR, il est primordial de concevoir une infrastructure réseau capable de s'adapter aux changements et aux nouvelles exigences.

L'une des pistes d'amélioration serait l'adoption d'une architecture réseau plus flexible, notamment en intégrant des technologies comme le cloud computing. En utilisant des solutions cloud ou des infrastructures hybrides, il serait possible d'étendre facilement les capacités du réseau sans nécessiter d'investissements matériels trop lourds.

Par ailleurs, à mesure que le volume de trafic augmente, il serait judicieux d'optimiser les performances en mettant en place un équilibrage de charge plus avancé. En répartissant le trafic de manière intelligente entre plusieurs serveurs ou passerelles, on éviterait les risques de congestion et d'engorgement du réseau.

Enfin, pour anticiper les besoins futurs, il serait recommandé de former régulièrement les administrateurs réseau sur les nouvelles technologies et pratiques en matière de cybersécurité. Une veille technologique active permettrait à la DGSR d'être toujours à jour face aux nouvelles menaces et d'adopter des solutions innovantes pour protéger son infrastructure.

Conclusion

Les perspectives d'avenir incluent donc l'intégration de systèmes complémentaires de protection, l'optimisation de la supervision du réseau et l'adaptation aux évolutions technologiques. En mettant en place ces améliorations, la DGSR pourra disposer d'une infrastructure réseau encore plus performante, sécurisée et évolutive, capable de répondre aux défis de demain.

CONCLUSION GÉNÉRALE

En conclusion, cette étude a permis d'explorer en profondeur la configuration et la redirection des ports des serveurs dans un environnement virtualisé, en prenant comme cas d'étude la Direction Générale de la Sécurité Routière (DGSR). Il a été démontré que la gestion des ports joue un rôle crucial dans la sécurité, l'accessibilité et la performance des services informatiques. Une mauvaise configuration peut entraîner des vulnérabilités exploitables par des cyberattaques, tandis qu'une gestion optimisée améliore non seulement la performance du réseau, mais aussi la protection des données sensibles. Dans un contexte où la transformation numérique s'accélère et où les cybermenaces deviennent de plus en plus sophistiquées, la mise en place de stratégies efficaces en matière de redirection des ports devient indispensable pour garantir la continuité des services et la confidentialité des informations.

L'analyse menée dans cette étude a mis en évidence les principes fondamentaux de la gestion des ports, les risques associés à une configuration inadéquate, ainsi que les meilleures pratiques pour sécuriser leur redirection. L'évaluation des méthodes appliquées à la DGSR a révélé des axes d'amélioration, notamment dans l'adoption de politiques de filtrage plus rigoureuses, l'automatisation des configurations pour minimiser les erreurs humaines, et l'intégration de solutions de surveillance continue permettant de détecter toute activité suspecte en temps réel.

Cependant, cette étude se limite à un cadre spécifique, et elle ouvre la voie à de futures recherches. Il serait pertinent d'approfondir l'impact des nouvelles technologies, telles que l'intelligence artificielle et les systèmes d'automatisation, sur la gestion des ports des serveurs. Ces technologies offrent des solutions innovantes pour sécuriser et optimiser la configuration des infrastructures réseau. **Comment l'intelligence artificielle et les systèmes d'automatisation, pourraient-elles révolutionner la gestion des ports et des configurations réseau, et ainsi améliorer encore la sécurité et l'efficacité des infrastructures informatiques dans les années à venir ?**

BIBLIOGRAPHIE

1. SUPPORT DE COURS

Monsieur RAHARISON Heriniaina, « **Réseaux Client/Serveur** », Niveau L3, 2023-2024

Monsieur RANDRIAMAMONJY Liantsoa Joharinirina, « **Technique de décision** », Niveau L3, 2023-2024

2. OUVRAGES ET ARTICLES

Olivier Bonaventure, « Réseaux : Concepts et protocoles », publié en 2011

José Dordoigne, "Réseaux informatiques - Notions fondamentales (10^e édition)" en février 2025

Mathieu Nebra, "Conception et administration de réseaux", publié en 2016

Laurent Bloch, "La sécurité des systèmes d'information", publié en 2013

3. WEBOGRAPHIE

<https://docs.opnsense.org>, consulté le 25 Novembre 2024 à 08 :35

<https://cours-informatique.fr>, consulté le 02 Décembre 2024 à 11 :45

<https://www.fnac.com>, consulté le 19 Décembre 2024 à 09 :12

<https://finevpn.org>, consulté le 08 Janvier 2025 à 09 :30

<https://web4.ensiie.fr>, consulté le 18 Janvier 2025 à 08 :00

<https://forum.opnsense.org>, consulté le 27 Janvier 2025 à 10 :10

ANNEXES

Annexe 1:Présentation des protocoles utilisés

TCP (Transmission Control Protocol) est un protocole orienté connexion qui assure une transmission fiable des données entre un client et un serveur. Il est utilisé pour les services nécessitant un contrôle d'intégrité des données, comme SSH, HTTP, et FTP.

UDP (User Datagram Protocol) est un protocole sans connexion qui est plus rapide mais moins fiable que TCP. Il est souvent utilisé pour les applications en temps réel, comme les jeux en ligne, le streaming vidéo et DNS.

Protocole	Fiabilité	Utilisation principale
TCP	Oui	Web, SSH, Email, FTP
UDP	Non	Streaming, VoIP, DNS

Annexe 2: Différence entre IP public et IP privée

Critères	IP publique	IP privée
Visibilité	Accessible sur Internet	Restreinte à un réseau local
Fourniture	Assignée par un FAI	Gérée par un routeur ou DHCP
Exemple d'IP	102.55.66.77	192.168.1.10
Utilisation	Serveurs, sites web, connexions à distance	Réseau domestique, entreprise, appareils internes

Relation entre IP publique et privée : la NAT

Les réseaux utilisent un mécanisme appelé **NAT (Network Address Translation)** pour permettre aux appareils avec des IP privées d'accéder à Internet via une seule IP publique. Par exemple un routeur avec l'IP publique 197.45.30.1 peut avoir plusieurs appareils connectés en IP privée (192.168.1.10, 192.168.1.20...). Lorsqu'un appareil local veut accéder à Internet, le routeur traduit son IP privée en IP publique. De l'extérieur, tout le réseau semble utiliser 197.45.30.1, mais en interne, chaque appareil garde son IP privée.

Annexe 3: Différence entre LAN et WAN

Critères	Réseau LAN	Réseau WAN
Portée	Zone locale (bâtiments, bureau)	Zone étendu (pays, monde)
Vitesse	Très rapide (100 Mbps-plusieurs Gbps)	Très rapide (10Mbps-plusieurs Gbps)
Latence	Faible	Elevée
Coût	Faible	Elevée
Connexion	Ethernet, WIFI	Fibre optique, satellite, 4G/5G
Sécurité	Facile à gérer	Plus complexe à sécuriser

Les réseaux LAN et WAN sont souvent interconnectés. Par exemple, dans une entreprise : chaque bureau a un réseau LAN local pour les ordinateurs et imprimantes. Tous ces LAN sont reliés entre eux via un WAN d'entreprise. Internet (WAN) permet aux employés de se connecter à distance via un VPN.

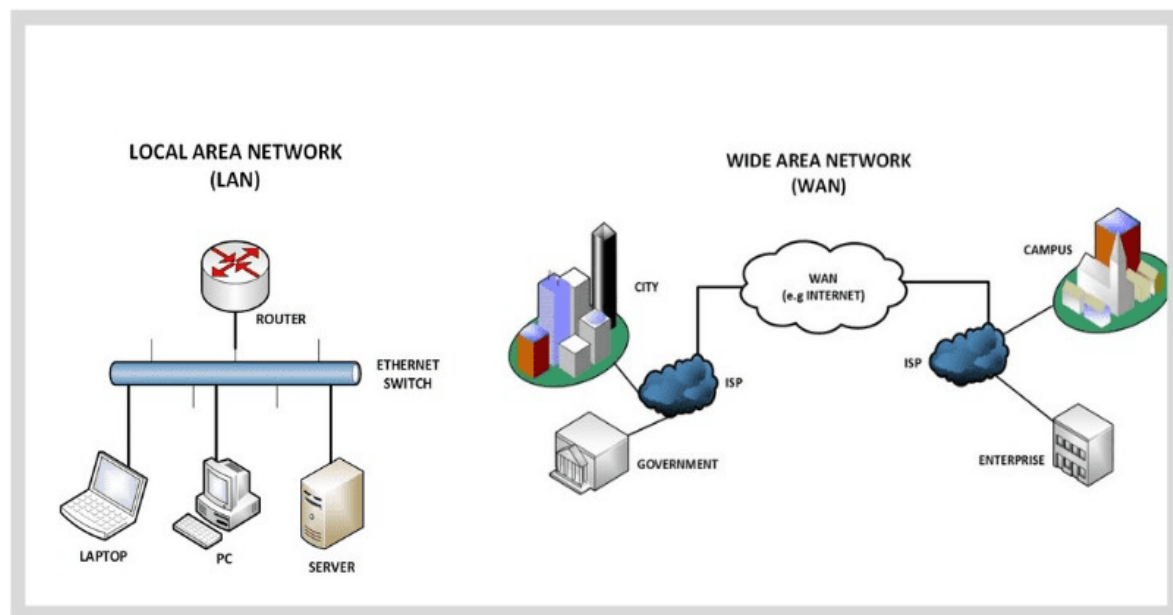


TABLE DES MATIERES

AVANT-PROPOS.....	I
REMERCIEMENTS	II
RESUME	III
ABSTRACT	IV
LISTE DES TABLEAUX.....	V
LISTE DES FIGURES	VI
LISTE DES ANNEXES.....	VII
LISTE DES ABREVIATIONS	VIII
INTRODUCTION GÉNÉRALE	1
PARTIE I : CADRE GENERALE	3
CHAPITRE I : PRESENTATION DE L'INSIDE UNIVERSITY.....	3
1. GESTION :	3
1.2 Comptabilité finance.....	4
1.3 Marketing et commerce international.....	4
1.4 Management et développement d'entreprise.....	4
1.5 Débauchés	5
2. DROIT :	5
2.1. Débauchés	5
3. INFORMATIQUE :	6
3.1 Administrations des systèmes et réseaux	6
3.2 Génie logiciel et base de données	7
3.3 Débauchés	7
CHAPITRE II : PRESENTATION DE L'ENTREPRISE DE STAGE.....	8
1 Statut de la direction générale de la sécurité Routière	8
2 Historique de la société	9
2.1 Automobile club de Madagascar	9

2.2	Gendarmerie nationale	9
3	Mission	10
4	Activité	10
4.1	Visite technique	10
	Périodicité de la visite technique :	10
CHAPITRE III : METHODOLOGIE		14
1.	CHOIX DU THEME	14
1.1	Contextualisation	14
1.2	Thème	15
2.	RECHERCHES.....	16
2.1	Recherche bibliographie.....	16
2.2	Recherche webographie.....	17
2.3	Recherche médiagraphie	17
3.	ENTRETIEN	17
	Entretien professionnelle.....	17
4.	CHRONOGRAMME DE GANTT.....	18
PARTIE II : ANALYSE DE L’EXISTANT ET RESULTATS		20
CHAPITRE I : MATERIELS TECHNOLOGIE ET TOPOLOGIE.....		20
1.	MATERIELS.....	20
1.1.	Quelques définitions.....	20
1.1.1.	Réseaux informatiques	20
1.1.2.	Parc informatique	20
1.1.3.	Serveurs	21
1.1.4.	Gateway	21
1.1.5.	Routeur	21
1.1.6.	Switch	22
1.1.7.	Point d’accès	22
1.1.8.	Câble Ethernet.....	23

1.1.9.	Authentification.....	23
1.1.10.	Pare-feu et équipements de sécurité	24
1.1.11.	Port.....	24
1.1.12.	Configuration des ports	24
1.1.13.	Redirection des ports	25
2.	TOPOLOGIE DE RESEAU	25
2.1.	Type de topologie	25
2.1.1.	Topologie en bus.....	25
2.1.2.	Topologie en étoile.....	26
2.1.3.	Topologie en anneau	26
2.1.4.	Topologie maillée.....	26
2.1.5.	Topologie en arbre	27
2.1.6.	Topologie hybride	27
2.2.	Architecture réseau de la DGSR.....	27
2.2.1.	Avantage	28
2.2.2.	Inconvénients.....	28
2.2.3.	Avantages et inconvénients de la virtualisation des serveurs.....	29
CHAPITRE II : MISE EN PLACE DE L'OUTIL		30
1.	PRESENTATION D'OPNSENSE.....	30
2.	PREPARATION DE L'ENVIRONNEMENT	31
2.1	Prérequis.....	31
2.2	Configuration des machines virtuelles	31
2.3	Création des machines virtuelles	31
3.	INSTALLATION D'OPNSENSE.....	32
3.1.	Sélection de l'ISO d'OPNsense	32
3.2.	Lancement du processus d'installation	33
3.3.	Type d'installation	33
3.4.	Sélection du disque.....	34

3.5.	Formatage des fichiers.....	35
3.6.	Copie des fichiers système.....	35
3.7.	Retrait du support d'installation et redémarrage.....	36
3.8.	Mise à jour du système	37
PARTIE III : CADRE PRATIQUE		38
CHAPITRE I : FONCTIONNALITES.....		38
1.	Introduction à la redirection des ports et son importance	38
2.	La fonctionnalité de la redirection des ports dans opnsense.....	38
2.1	Vérification des règles NAT	39
2.1.1	Filtrage du trafic	39
2.1.2	Transmission du paquet	40
3.	Mise en œuvre de la redirection des ports dans opnsense	40
3.1	Création et configuration des règles NAT	40
3.1.1	Accéder à l'interface opnsense.....	41
3.1.2	Accéder aux règle NAT.....	42
3.1.3	Création d'une règle NAT pour la redirection des ports	43
3.1.4	Vérification et testes.....	45
3.1.4.1	Test depuis une machine externe.....	45
3.2	Vérification avec les logs opnsense	45
CHAPITRE II : RESULTATS		47
1.	Amélioration de la gestion du trafic	47
2.	Renforcement de la sécurité du réseau	47
3.	Optimisation des performances des services internes.....	48
4.	Réduction des erreurs de configurations et facilité de maintenance	48
Conclusion		49
CHAPITRE III : PERSPECTIVE D'AVENIR.....		50
1.	Renforcement de la sécurité.....	50
2.	Automatisation et supervision avancée du réseau.....	50

3. Scalabilité et adaptation aux besoins futur.....	51
Conclusion	51
CONCLUSION	52
BIBLIOGRAPHIE.....	IX
1. SUPPORT DE COURS	IX
2. OUVRAGES ET ARTICLES	IX
3. WEBOGRAPHIE	IX
ANNEXES	X