République Démocratique du Congo

✍

MINISTERE L’ENSEIGNEMENT, SUPERIEUR, UNIVERSITAIRE, RECHERCHE SCIENTIFIQUE

ET L’INNOVATION(ESURSI)

INSTITUT SUPERIEUR PEDAGOGIQUE TECHNIQUE DE KINSHASA

**ISPT – KIN**

****

SECTION DEPARTEMENT

INFORMATIQUE INFORMATIQUE INDUSTRIELLE

B.P 3287

KINSHASA/GOMBE

SYSTEME : LICENCE-MASTER-DOCTORAT(LMD)

**DEPLOIEMENT D’UN SYSTEME DE DETECTION ET DE PREVENTION D’INTRUSION (IDS/IPS) DEDIE AUX RESEAUX DE TELEVISION**

**«**Cas de la Rtnc gombe**»**

**NDONA TABUKU Pedo**

TFC de fin de cycle présenté et défendu en vue de l’obtention du titre

De licencie en pédagogie et technique appliquées

**Mention : informatique industrielle**

**Quatrième Licence**

Directeur : **Prof. ANGOMA MONGA SINDANI Blaise**

*Docteur en informatique*

Co-directeur : **Ass. MAYI YALEM Didier**

*Licencie en informatique*

**Année académique 2024-2025**

# EPIGRAPHE

« La détection des intrusions est la première ligne de défense dans un monde numérique en constante mutation. Prévenir, c'est bâtir des murs invisibles autour de notre savoir. »

**Émile Verlaine**

# DEDICACE

A mes parents bien aimés papa JEAN NDONA et maman JULIENNE TABUKU, qui se sont donnés corps et âme pour supporter nos études malgré la grande crise économique actuelle et toutes autres charges à leurs têtes, nous disons un grand merci.

A Mon oncle paternelle : ACHILLE NDONA qui est mon tuteur et papa IGNACE NDONA pour le soutien.

# NDONA TABUKU PEDO

# AVANT-PROPOS

Au seuil de la confection de ce travail scientifique sanctionnant le terme de notre cycle de formation universitaire, l’occasion nous est offerte pour remercier ceux qui ont fait à ce que nous arrivons dans ce stade. De prime à bord nous tenons à remercier l’Eternel Dieu tout puissant qui nous a accordé jusqu’ici son souffle de vie.

Nous exprimons nos sentiments de reconnaissance en l’endroit de toutes les autorités tant académiques, scientifiques qu’administratif de l’Institut Supérieur Pédagogique et Technique de Kinshasa, en sigle ISPT.

Ce travail serait privé de son vrai sens n’eût été le concours scientifique et technique de Monsieur ANGOMA MANGO SINDANI Blaise, professeur.Dr en informatique qui en dépit de ses nombreuses occupations, a dû accepter de diriger ce travail du début jusqu’à sa fin et à mon codirecteur MAYI LUKONGO YALEM Didier, Ass. Licencié en informatique

Nos vifs remerciements vont droit à mes Frères et soeurs, plus précisément Junior tabuku, Franck ndona, Rigo ndona, Cecile ndona, Urbain ndona, Joyce Mah, Getro ndona, Fils mpasa , pour votre soutient tant moral, matériel que financier qui ont fait que j’arrive à ce stade.

Aux amis et connaissance : Yahav Mpayi, Joseph Itakala, Joseph Muhigwa, Patthy Edia, Collette Edia, Isaac Anozo, Elie Pabicher, Gloire yanfu, Nicole tabuku.

Que tous ceux qui ne sont pas repris sur cette liste trouvent notre profonde reconnaissance pour tous leurs bienfaits.

# NDONA TABUKU PEDO

# LISTE DES TABLEAUX

[Tableau 3. 1 Choix des matériels 44](#_Toc206638715)

[Tableau 3. 2 Choix des logiciels 44](#_Toc206638716)

[Tableau 3. 3 Plan d'adressage 45](#_Toc206638717)

[Tableau 3. 4 Estimation du coût 56](#_Toc206638718)

# LISTE DES FIGURES

[Figure 1. 1 Classification des réseaux selon l’étendue géographique 8](#_Toc206638727)

[Figure 1. 2 Réseau Peer to Peer (p2p) 11](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638728)

[Figure 1. 3 Réseau administré (client/serveur) 12](#_Toc206638729)

[Figure 1. 4 Routeur 13](#_Toc206638730)

[Figure 1. 5 Concentrateur 13](#_Toc206638731)

[Figure 1. 6 Pont 13](#_Toc206638732)

[Figure 1. 7 Accès Point 13](#_Toc206638733)

[Figure 1. 8 Les couches du Modèle OSI 15](#_Toc206638734)

[Figure 1. 9 Modèle TCP/IP 16](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638735)

[Figure 1. 10 Topologie en Bus 17](#_Toc206638736)

[Figure 1. 11 Topologie en anneau 18](#_Toc206638737)

[Figure 1. 12 Topologie en étoile 18](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638738)

[Figure 1. 13 Câble coaxial 21](#_Toc206638739)

[Figure 1. 14 Câble à paire torsadée 21](#_Toc206638740)

[Figure 1.15 Fibre optique 21](#_Toc206638741)

[Figure 1. 16 Système de détection d’intrusion réseau. 37](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638742)

[Figure 1. 17 Système de détection d’intrusion hôte. 38](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638743)

[Figure 3. 1 Maquette du nouveau système 45](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638744)

[Figure 3.2 Démarrage de PfSense 46](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638745)

[Figure 3. 3 Acceptation de l’installation 46](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638746)

[Figure 3. 4 Installation facile 47](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638747)

[Figure 3. 5 Installation du noyau 47](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638748)

[Figure 3. 6 Partitionnement UFS 47](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638749)

[Figure 3. 7 Progression d’installation 48](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638750)

[Figure 3. 8 Redémarrage du système 48](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638751)

[Figure 3. 9 Configuration des interfaces 48](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638752)

[Figure 3. 10 Choix de l’interface à configurer 49](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638753)

[Figure 3. 11 Propriété des interfaces 49](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638754)

[Figure 3. 12 Accès en mode interface graphique du LAN1 50](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638755)

[Figure 3. 13 Modification du Nom 50](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638756)

[Figure 3. 14 Sélection des Trafics 51](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638757)

[Figure 3. 15 Sélection des interfaces 51](#_Toc206638758)

[Figure 3. 16 L’algorithme de cryptage 52](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638759)

[Figure 3. 17 Affichage des informations du système 52](#_Toc206638760)

[Figure 3. 18 Accès dans le Snort 53](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638761)

[Figure 3. 19 Identification des ports Snort 53](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638762)

[Figure 3. 20 Activation du Snort 53](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638763)

[Figure 3. 21 Ajout de fonctionnalité 53](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638764)

[Figure 3. 22 Activation des paramètres 54](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638765)

[Figure 3. 23 Enregistrement 54](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638766)

[Figure 3. 24 Identification de l'interface Overview 54](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638767)

[Figure 3. 25 Paramètre d'adresse IP 55](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638768)

[Figure 3.26 Paramètre de la Carte 55](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638769)

[Figure 3. 27 Sélection du mode Automatique 55](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638770)

[Figure 3. 28 Vérification d'Adresse IP 56](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638771)

[Figure 3. 29 Test de connectivité 56](file:///E:\TRAVAIL%20SCIENTIFIQUE%202025\TRAVAUX%20SCIENTIFIQUE%20ZONE%20KINSHASA\NDONA%20TABUKU%20PEDO%20T-PEN\TFC%20NDONA%20250.docx#_Toc206638772)

# LISTE DES ABREVEATIONS

|  |  |
| --- | --- |
| **ABREVIATIONS** | **DESCRIPTIONS** |
| **BNC** | Bayonnet Neill-Concelman Connector |
| **CSMA/CD** | carrier sense multiple access with collision |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DNS** | Domaine Name Serveur |
| **DPI** | Direction Provinciale des Impôts |
| **FTP** | File Transfert Protocol |
| **http** | HyperText Transfert Protocol |
| **IEEE** | Institute of Electrical and Electronic Ingeneer |
| **InterNic** | Internet Network Information Center |
| **IP** | Internet Protocol |
| **ISPT** | Institut Supérieur Pédagogique et Technique |
| **IDS** | **Intrusion Detection System** |
| **IPS** | **Intrusion Prevention System** |
| **ISO** | Interconnexion des Systèmes Ouverts |
| **LAN** | Local Area Network |
| **Li-fi** | Light – Fidelity |
| **MAN** | Métropolitain Area Network |
| **OSI** | Open System Interconnexion |
| **PAN** | Personal Area Network |
| **RJ45** | Registered Jack 45 |
| **RTNC** | RadioTélévision Nationale Congolaise |
| **TCP** | Transmission Control Protocol |
| **UDP** | User Datagram Protocol |
| **USB** | Universal Serial Bus |
| **UTP** | Unshielded Twisted Pair |
| **WAN** | Wide Area Network |
| **WI-FI** | Wireless Fidelity |
| **WWW** | World Wide Web |
| **PAN** | Personal Area Network |
| **RJ45** | Registered Jack 45 |
| **TCP** | Transmission Control Protocol |
| **TDMA** | Time Division Multiplexing Access |

# INTRODUCTION GENERALE

## 0.1 Présentation du Sujet

A l'ère du numérique, les réseaux de télévision jouent un rôle crucial dans la diffusion d'informations, de divertissements et de contenus éducatifs. Toutefois, cette transition vers des infrastructures de plus en plus interconnectées expose ces réseaux à des risques de cyberattaques croissants. La Radio-Télévision Nationale Congolaise (RTNC), en tant qu'entité majeure de la communication en République Démocratique du Congo, n'échappe pas à ces menaces.

La sécurité des réseaux de télévision est primordiale non seulement pour la protection des données sensibles, mais aussi pour maintenir la confiance du public et garantir la continuité des services. Les systèmes de Détection et de Prévention d’Intrusion (IDS/IPS) émergent comme des solutions indispensables pour surveiller les activités sur le réseau, détecter les comportements malveillants et prévenir les intrusions avant qu'elles ne causent des dommages.

Cette étude examine le déploiement d'un système IDS/IPS spécifiquement adapté aux besoins et aux défis de RTNC. À travers une analyse des menaces potentielles et des solutions techniques, nous mettrons en évidence l'importance d'une approche proactive en matière de sécurité des réseaux de télévision. Ce faisant, l'objectif est de proposer un cadre qui non seulement renforce la sécurité, mais aussi contribue à l'évolution et à la résilience du secteur audiovisuel face aux défis numériques contemporains.

## 0.2 Choix et intérêt du sujet

### 0.2.1 Choix du sujet

Le choix de se concentrer sur le déploiement d’un système de Détection et de Prévention d’Intrusion (IDS/IPS) dédié aux réseaux de télévision, en particulier dans le cas de la Radiotélévision Nationale Congolaise (RTNC), repose sur plusieurs motivations et enjeux cruciaux.

Le choix de ce sujet s'inscrit dans une volonté d'explorer les meilleures pratiques en matière de sécurité pour les réseaux de télévision, en mettant l'accent sur l'importance stratégique d'un système IDS/IPS pour RTNC. Cette recherche vise à proposer des solutions concrètes et adaptées qui renforceront la sécurité et la résilience de l'institution face aux menaces numériques contemporaines.

La RTNC, en tant qu'institution phare des médias en République Démocratique du Congo, est confrontée à des défis uniques en matière de sécurité des informations. Avec une audience vaste et diversifiée, la protection des contenus diffusés et des données sensibles est essentielle pour maintenir la confiance du public et assurer la qualité des services.

Les réseaux de télévision nécessitent des mesures de sécurité adaptées aux spécificités de leurs opérations. Un IDS/IPS peut fournir des solutions sur mesure pour surveiller les flux de données en temps réel, protéger les infrastructures critiques et garantir l'intégrité des contenus diffusés.

### 0.2.2 Intérêt du sujet

Le déploiement d'un système de détection et de prévention d'intrusion (IDS/IPS) dédié aux réseaux de télévision, comme celui de la RTNC (Radio-Télévision Nationale Congolaise), présente plusieurs intérêts significatifs, tant sur le plan personnel qu'académique.

* **Intérêt professionnel**

La RTNC manipule des informations sensibles et des contenus exclusifs. Un IDS/IPS permet de protéger ces données contre les accès non autorisés et les cyberattaques. La détection proactive des intrusions aide à garantir que les contenus diffusés ne soient pas altérés ou compromis, assurant ainsi la qualité de l'information transmise au public. En assurant la sécurité des transmissions, la RTNC peut renforcer la confiance de son audience dans ses services.

# Intérêt personnel

Participer à un tel projet permet de développer des compétences en cybersécurité, en administration de réseaux et en gestion des systèmes d'information. Travailler sur le déploiement d’une IDS/IPS offre une expérience concrète qui peut s'avérer précieuse pour une carrière dans la sécurité informatique.

# Intérêt scientifique

Ce sujet peut servir de base pour des recherches académiques sur la sécurité des réseaux, permettant d'explorer de nouvelles méthodes de détection et de prévention des intrusions. Ce projet peut encourager des collaborations entre différents domaines, comme l'informatique, les sciences de l'information, et les études médiatiques, enrichissant ainsi le processus d'apprentissage.

**0.3 Problématique**

SHOMBA.K précise que « la problématique est une ensemble des questions posées dans un domaine de la science, en vue d’une recherche des solutions »[[1]](#footnote-1)

La RTNC (Radio-Télévision Nationale Congolaise) fait face à plusieurs défis en matière de sécurité des réseaux, qui compromettent non seulement l'intégrité de ses opérations, mais aussi la confiance du public dans ses diffusions. Ces difficultés incluent entre temps l’augmentation des Cyberattaques comme toute institution médiatique, la RTNC est exposée à un large éventail de cybermenaces, allant des attaques par déni de service (DDoS) aux tentatives d'intrusion ciblées, mettant à mal la continuité de ses services. La RTNC fait face à la vulnérabilité des Systèmes, Les équipements et logiciels utilisés par la RTNC peuvent présenter des failles de sécurité, souvent dues à un manque de mises à jour régulières ou à une connaissance limitée des meilleures pratiques en matière de cybersécurité.

Toutes ces difficultés ne facilitent pas La RTNC, au moyen de son personnel, d’être plus performant. Le fond du problème pour lequel nous voulons des pistes de solutions, peut se formuler dans la question suivante :

- Quel système pouvons-nous mettre en place afin de prévenir toutes éventuelles intrusions au sein de la RTNC ?

## 0.4 Hypothèse

Si à la problématique nous avons posé une question ; nous allons essayer, à ce stade, d’y répondre.

L’hypothèse est une réponse provisoire guidant la recherche susceptible d’être confirmée ou infirmée. Pour le dictionnaire universel, l’hypothèse est définie comme un point de départ d’une démonstration logique posée dans l’énoncé à partir duquel on se propose d’aboutir à la conclusion de la démonstration. En outre, l’hypothèse est la proposition des solutions aux problèmes posés à la problématique.

Nous pensons que Le déploiement d'un système de détection et de prévention d'intrusion au sein de la RTNC pourrait permettre non seulement de renforcer la sécurité des réseaux de télévision contre les cybermenaces, mais aussi pourrait améliorer la protection des données sensibles et de sensibiliser le personnel aux enjeux de la cybersécurité, conduisant ainsi à une réduction significative des incidents de sécurité et à une meilleure continuité des services de diffusion.

## 0.5 Objectifs

Le déploiement d'un système de détection et de prévention d'intrusion (IDS/IPS) dédié aux réseaux de télévision, comme celui de la RTNC (Radio-Télévision Nationale Congolaise), a plusieurs objectifs dont :

* Protéger les informations sensibles et les contenus diffusés contre les accès non autorisés et les fuites de données.
* Sauvegarder les équipements et les réseaux de télévision contre les attaques malveillantes, garantissant ainsi la continuité des services de diffusion.
* Assurer le respect des normes de sécurité et des réglementations en matière de protection des données et de la vie privée

## 0.6 Méthodes et techniques

La réalisation d’un travail scientifique n’est pas un fait hasardeux, c’est ainsi qu’il trouve son mérite sur l’efficacité et la rigueur des méthodes et techniques utilisées. La scientificité d’une recherche, sied à l’utilisation ces dernières.

### 0.6.1 Méthodes

Jean Louis LAUBET Del Bayle pour sa part définit la méthode « comme l’ensemble des opérations intellectuelles permettant d’analyser, de comprendre et d’expliquer la réalité étudiée.[[2]](#footnote-2) Dans le présent travail, nous avons utilisé les méthodes suivantes :

* **Méthode structuro fonctionnelle :**

Elle détermine la structure et les différentes fonctions, elle nous a été utile pour bien comprendre les services ainsi que le rôle de chacun de ses parties ;

* **Méthode descriptive :**

C’est une méthode qui consiste, à décrire le système existant, afin de déceler les anomalies, et proposer une solution adéquate. Elle nous a permis à la description du fonctionnement de la RTNC et son service technique en particulier, afin de déceler des anomalies de l’ancien système, pour tenter d’apporter une solution.

* **Méthode historique :**

C’est une méthode utilisée pour fournir des renseignements sur la genèse d’organisation c’est-à-dire l’histoire de la création. Celle-ci nous a permis d’obtenir les renseignements sur la genèse de la création de la RTNC.

* **Méthode Top-down Network design:**

C’est une approche complémentaire à la méthode Top-Down qui se concentre sur l’optimisation et l’amélioration des réseaux existants. Evaluation de l’infrastructure existante, identification des lacunes, conception des améliorations.

### 0.6.2 Techniques utilisées

Une technique n'est rien d'autre qu'un processus à suivre où en mettre en pratique pour parvenir à un bon résultat attendu par tous. C'est un ensemble des procédés d'un art ou d'un métier c'est pourquoi nous en citerons quelques techniques dans notre recherche scientifique qui sont :

* **L'observation** : Cette technique sera utilisée toujours dans le but de la récolte de données sur le champ de recherche et aussi bien là où nous aurons encore beaucoup plus d'idées cadrant avec notre sujet.
* **La documentation** : Partant de sa définition c'est un ensemble des documents sur les matières que nous chercheurs, voulons bel est bien traité en vue d'atteindre les buts attendus ; d'où il sera impossible de parvenir à contourner cette étape vous étant chercheur, car un travail sans référence n'est pas un travail scientifique.

## 0.7. Délimitation du sujet

Il est affirmé qu'un travail scientifique, pour être bien précis, doit être délimité. Elle est délimitée aussi bien dans l’espace que dans le temps.

### 0.7.1 Spatiale

En ce qui concerne l’espace, le présent travail se limite à la Radio-Télévision Nationale Congolaise.

**0.7.2 Temporelle**

De manière temporelle, pour une période allant de Mars 2025 à Août 2025.

## 0.8 Subdivision du Travail

Hormis l’Introduction et la conclusion générale, Le présent travail est divisé en deux parties de valeurs non négligeables :

* Le premier chapitre « notions fondamentaux sur les réseaux informatique », explique la théorie de réseaux informatique ;
* Le second chapitre « fondements théoriques des systèmes de détection », traite des différents systèmes d’intrusion ;

et de prévention d'intrusion

* Le troisième chapitre « présentation de l’entreprise », parle de la rtnc ;
* Le quatrième chapitre « déploiement du nouveau système », s’occupe de l’implantation du système de prévention et détection d’intrusion au sein de la RTNC.

# CHAPITRE I : NOTIONS FONDAMENTALES SUR LES RESEAUX INFORMATIQUES

# 1.1 Introduction

Dans ce chapitre nous allons parler des généralités sur les réseaux informatiques et la supervision réseau afin expliquer quelques notions indispensables au fonctionnement de ce dernier. Nous allons aussi parler des supports de transmission et ainsi que la sécurité informatique.

## 1.2 Définition

Un réseau informatique est un ensemble équipements informatiques interconnecté entre eux pour un but de se partager les ressources physique et logique.[[3]](#footnote-3)

Dans ce même ranger, nous pouvons définir le réseau informatique comme étant l’ensemble des terminaux misent en commun permettant de se communiquer entre eux.

## 1.3 Classification des réseaux

On peut distinguer différent type de réseaux selon plusieurs critères tels que la taille de réseau, sa vitesse de transfert des données et aussi son étendu.

**1.3.1. Selon l’étendue géographique**

Selon l’étendue géographique que couvre le réseau nous distinguons principalement les réseaux suivants :

* **PAN (Personnal Area Network)**

Le réseau personnel permet aux équipements de communiquer à l’échelle individuelle. Un exemple courant est celui d’un réseau qui relie un ordinateur à une imprimante ou un autre équipement. Ses limites peuvent varier de (de 100 m à 1km).[[4]](#footnote-4)

* **LAN (Local Area Network)**

Un LAN est un réseau local situé dans une zone.

C’est un réseau local servant à relier les équipements informatiques sous une petite distance, souvent c’est entre les équipements disposés dans un ou deux bâtiments séparés par une petite distance.

Ses limites peuvent varier de (de 10 à100 m).

* **MAN (Metropolitan Area Network)**

Lorsqu'un réseau privé ; s'étend sur plusieurs kilomètres, dans une ville par exemple les réseaux locaux sont interconnectés via des liaisons téléphoniques à haut débit ou à l'aide d'équipements spéciaux comme des transmissions hertziennes. Ce type de regroupement de réseaux locaux peut se faire au niveau d'une ville et l'infrastructure du réseau métropolitain peut être privée ou publique. Le réseau métropolitain permet l'interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une zone urbaine dont l’étendue géographique n’excède pas 200 km. Ces réseaux peuvent être privés ou publics. Ils se distinguent aussi par leurs taux d’erreurs de communication.[[5]](#footnote-5)[[6]](#footnote-6)

* **WAN (Wide Area Network)**

Ces réseaux relient plusieurs réseaux locaux en les interconnectant via des lignes louées ou via Internet.

Exemple : les réseaux bancaires qui établissent des liaisons entre les agences et le siège central. Dans le cas de l'utilisation d'Internet, on parle de VPN (Virtual Private Network) puisqu'on utilise alors un réseau public pour faire transiter des informations privées.



Figure 1. 1 Classification des réseaux selon l’étendue géographique

**1.3.2. Selon le media de transmission[[7]](#footnote-7)**

Un support de transmission est un lien entre deux terminaux. Ainsi, compte tenu de media de transmission nous distinguons les réseaux ci-après :

* **Le réseau filaire ou câblé**

Est un réseau dont les terminaux sont reliés par l’entremise des câbles (coaxial, twisted paire, fibre optique, CPL, etc…).

* **Le réseau non filaire**

Un réseau non filaire ou sans fil, est un réseau par lequel les terminaux se communiquent sans liaison physique ou visible (l’air, le vide, faisceau hertzien, ondes radioélectriques, etc…).

### 1.3.3. Selon le débit

Le débit est la vitesse de transmission des informations par unité de temps au sein d’un réseau. Selon le débit nous avons les réseaux ci-après :

* **Les réseaux à faible et moyen débit :** sont les réseaux dont le débit est inférieur à 200 Kbit/seconde.
* **Les réseaux à haut débit** sont les réseaux dont le débit est supérieur à 200 Kbit/seconde mais inférieur à 20 Mbit/seconde.
* **Les réseaux à très haut débit** sont les réseaux dont le débit est supérieur à 20 Mbit/seconde.

1.3.4. Selon le champ d’application[[8]](#footnote-8)

Le champ d’application décrit le contexte dans lequel le réseau est utilisé. En effet, compte tenu de cette rubrique nous distinguons deux principaux types des réseaux :

### 1.3.4.1 Réseau privé

Les réseaux privés concernent en général des réseaux personnels ou les réseaux d’entreprise. Ils sont privés par la nature des données échangées. Cette confidentialité des données est facile à assurer lorsque le réseau n’a que l’étendue limitée de quelques ordinateurs interconnectés ensemble et sont cachés derrière un routeur / pare feu qui contrôle les accès au monde extérieur.

Les réseaux privés sont connectés à Internet par des équipements spéciaux appelés routeurs. Les routeurs sont des équipements qui échangent les données entre les machines du réseau local et les autres réseaux.

Est un réseau où les règles d’accès sont établies afin de reléguer l’accès à quelques privilégiés. Parmi ces réseaux privés nous pouvons citer:

# Intranet

Un intranet est un réseau qui offre des services à une entité de même nature afin d’être en communication. (Exemple : un serveur web et d’autres services misent à la disposition de RTNC Kinshasa et RTNC Bandundu). Il utilise le protocole TCP pour la transmission des informations, comme par exemple l’utilisation de navigateur internet, pour réaliser un système d’informations interne à une organisation ou une entreprise. On peut dire encore que l’intranet est un réseau privé sur le protocole TCP/IP et exploitant les mêmes applications que sur internet.[[9]](#footnote-9)

# Extranet[[10]](#footnote-10)

Un extranet est un réseau qui relie une entreprise à ses partenaires. Nous pouvons dire qu’un extranet fait l’interconnexion de plusieurs intranets au moyen d’un tunnel VPN (exemple : TMB-PEPELE Mobile et ses abonnés).

# Ethernet

Un Ethernet est un réseau qui relie les terminaux en local.

## 1.3.4.2. Réseau public

On parle du réseau Public lorsque les échanges de données n’ont plus le caractère confidentiel des réseaux privés. Un réseau auquel l’accès est relégué à un grand public, et par son intermédiaire, peut se connecter d’autres réseaux. Parmi lesquels on peut citer :

* **Internet** est un acronyme Interconnected Network qui fait l’interconnexion des plusieurs réseaux distants à l’échelle planétaire et qui permet à des terminaux de se communiquer au moyen d’un protocole de communication commun appelé (IP).

## 1.3.5. Selon l’architecture de communication

L’architecture de communication réseau détermine la manière dont les services et les ressources s’échangent entre les terminaux au sein d’un réseau. Il existe deux types d’architecture de réseaux :

Architecture Client/serveur et architecture poste à poste.

# Le réseau Peer to Peer (p2p)

Cette architecture est en fait un réseau sans serveur, constitué de deux ou plusieurs ordinateurs où chaque ordinateur joue à la fois le rôle de serveur et de client. Inversement à une architecture de réseau de type client/serveur, il n’y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela indique notamment que chacun des ordinateurs du réseau est libre de partager ses ressources. Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés. Dans un réseau poste à poste typique, il n’y a pas d’administrateur.

# 1. Avantages de l’architecture poste à poste

1. **Coût réduit** : Il n’existe pas de matériel évolué et donc cher, et en plus il n’y a pas de frais d’administration. Grande simplicité : La gestion et la mise en place du réseau et des machines sont peu compliquées.

# 2. Inconvénients de l’architecture poste à poste

* Ce système n’est pas du tout centralisé, ce qui le rend très difficile à administrer.
* La sécurité est moins facile à assurer, compte tenu des échanges transversaux.
* Aucun maillon du système ne peut être considéré comme fiable

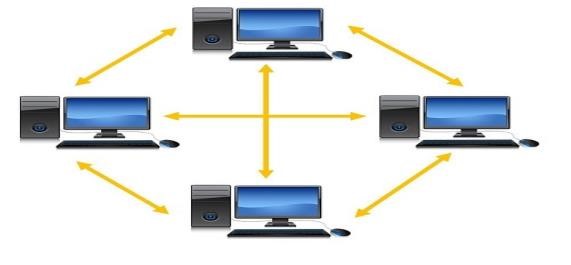


Figure 1. 2 Réseau Peer to Peer (p2p)

#  Le réseau administré (client/serveur)

Un périphérique (appelé serveur) fournit des services à d’autres périphériques (appelés clients) qui lui en font la demande via des requêtes. Le réseau client/serveur correspond à une architecture centralisée des ressources.

L’architecture client/serveur désigne un modèle de communication entre plusieurs ordinateurs d’un réseau. Elle distingue plusieurs postes clients qui communiquent avec un serveur (une machine généralement très puissante en termes de capacités d’entrée/sortie) qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l’heure, des fichiers, des connexions, etc. Les services sont exploités par des programmes appelés programmes clients s’exécutant sur les machines clientes.[[11]](#footnote-11)

# 1. Avantages de l’architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité. Ses principaux atouts sont :

* Ressources centralisées : Étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée afin d’éviter les problèmes de redondance et de contradiction.
* Meilleure sécurité : Car le nombre de points d’entrée permettant l’accès aux données est moins important.
* Administration au niveau serveur : Les clients ayant peu d’importance dans ce modèle ont moins besoin d’être administrés et autres…

# 2. Inconvénients de l’architecture client/serveur

L’architecture client/serveur a tout de même quelques lacunes parmi lesquelles, on peut citer :

* Coût élevé : dû à la technicité du serveur.
* Maillon faible : Le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui.

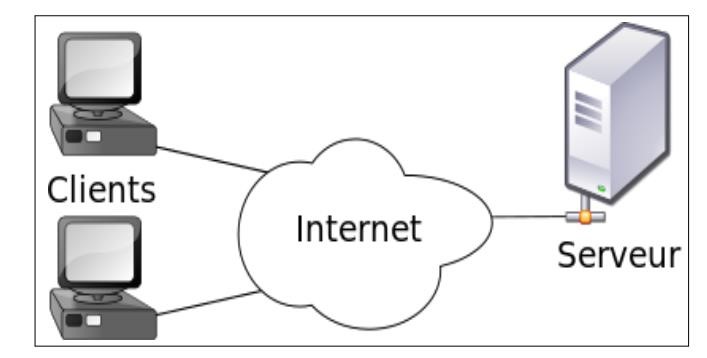


Figure 1. 3 Réseau administré (client/serveur)

## 1.4 Equipement d’interconnexion réseau

Les équipements d’interconnexion peuvent se situer à courte ou à longue distance. Nous présentons aux lignes qui suivent quelques principaux équipements de base utilisés pour mettre en place un réseau :

### 1.4.1. Switch

Le Switch est un équipement utilisé aussi pour interconnecter les ordinateurs dans un réseau. Permettant de relier divers éléments tout en segmentant le réseau, ils sont des hubs améliorés et plus intelligents qui envoi le signal directement à la station concernée.[[12]](#footnote-12)



Figure 1.4 : Switch

### 1.4.2. Routeur

Le routeur est un équipement du réseau capable d’interconnecter deux ou plusieurs réseaux de nature différente. Un routeur permet d’assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu’un paquet de données peut emprunter.[[13]](#footnote-13)



Figure 1. 4 Routeur

### 1.4.3 Hub

Le concentrateur est un équipement permet à connecter les différents équipements en réseaux afin de concentrer les signaux.



Figure 1. 5 Concentrateur

### 1.4.4. Pont (bridge)

Un pont est un Equipment réseau qui sert à relier deux réseaux locaux utilisant les mêmes paramètres (Protocol, paramètres IP, etc…). Il utilise les adresses MAC des équipements pour le transfert des trames.



Figure 1. 6 Pont

### 1.4.5 Point d’accès

Un point d'accès réseau, siglé PA ou AP, dans le domaine des réseaux de télécommunications, est un équipement informatique qui permet de relier les terminaux distants via une onde radio, en suivant une procédure logicielle.[[14]](#footnote-14)



Figure 1. 7 Accès Point

## 1.5 Modèles

Le transfert d’information entre deux logiciels informatiques sur deux équipements réseau différent se base sur deux modèles théoriques : le modèle OSI et le modèle TCP/IP. Ces deux modèles sont plus théoriques.

### 1.5.1 Modèle de référence OSI (Open System Interconnection)

Le modèle OSI est un modèle de référence pour décrire et expliquer les communications dans un réseau. Il décrit sept couches portant les noms de couche physique, liaison, réseau, transport, session, présentation et application. Les divers protocoles qui définissent le réseau et les communications sont donc répartis dans chaque couche, selon leur utilité. Il est d’usage de diviser ces sept couches en deux : les couches basses, qui se limitent à gérer les fonctionnalités de base, et les couches hautes, qui contiennent des protocoles plus élaborés.

# A. Couches basses

Les couches basses, aussi appelées couches matérielles, s’occupent de tout ce qui est traité au bas-niveau, c.à.d. au matériel. Elles permettent d’envoyer un paquet de données sur un réseau et garantir que celui-ci arrive à destination. Elle est généralement prise en charge par le matériel et le système d’exploitation, mais pas du tout par les logiciels réseaux. Les couches basses sont donc des couches assez bas-niveau, peu abstraites et de nombre de trois. Pour résumer, ces trois couches s’occupent respectivement de la liaison point à point (entre deux ordinateurs/équipements réseaux), des ré- seaux locaux, et des réseaux Internet.

1. **La couche physique** : Elle s’occupe de la transmission physique des bits entre deux équipements réseaux. Elle s’occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.
2. **La couche liaison** : Elle s’occupe de la transmission d’un flux de bits entre deux ordinateurs par l’intermédiaire d’une liaison point à point ou d’un bus. Pour simplifier, elle s’occupe de la gestion du réseau local. Elle prend, notamment, en charge les protocoles MAC, ARP, et quelques autres protocoles.
3. **La couche réseau** : Elle s’occupe de tout ce qui a trait à internet : L’identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. C’est notamment cette couche qui s’occupe du routage, à savoir la découverte d’un chemin de transmission entre récepteur et émetteur, le chemin qui passe par une série de machines ou de routeurs qui transmettent l’information de proche en proche. Le protocole principal de cette couche est le protocole IP

# B. Couches hautes

Les couches hautes, aussi appelées couches logicielles, contiennent des protocoles pour simplifier la programmation logicielle. Elles requièrent généralement que deux programmes communiquent entre eux sur le ré- seau. Elles sont implémentées par des bibliothèques logicielles ou directement dans divers logiciels. Le système d’exploitation ne doit pas, en général, implémenter les protocoles des couches hautes. Elles sont au nombre de quatre :

1. **La couche transport** : Elle permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP et UDP.
2. **La couche session** : Comme son nom l’indique, elle permet de gérer les connexions et les déconnexions et la synchronisation entre deux processus.
3. **La couche présentation** : Elle se charge du codage des données à transmettre. Elle s’occupe notamment des conversions de boutisme ou d’alignement, mais aussi du cryptage ou de la compression des données transmises.

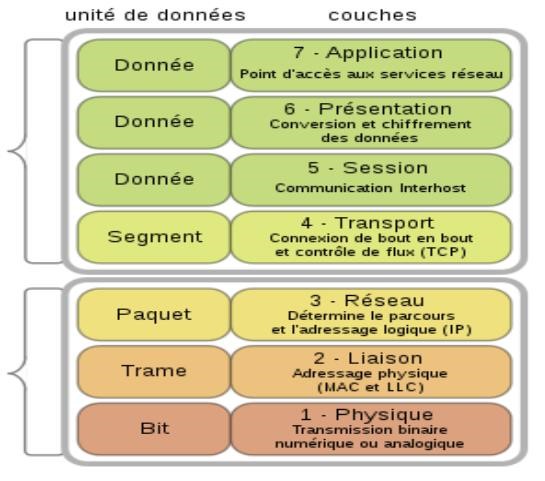


Figure 1. 8 Les couches du Modèle OSI

## 1.5.2 Modèle TCP/IP[[15]](#footnote-15)

Contrairement au modèle OSI, le modèle TCP/IP est né d’une implémentation mais il est inspiré du modèle OSI. Il reprend l’approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. Afin de connaitre les services de chaque couche, elles seront présentées brièvement ci-dessous l’une après l’autre :

1. **Couche application :** Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

1. **Couche transport :** La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L’un de ses protocoles TCP fournit d’excellents moyens de créer avec souplesse des communications réseau fiables.

1. **Couche Internet :** Le rôle de la couche Internet consiste à envoyer des paquets source à partir d’un réseau quelconque de l’inter-réseau et à les faire parvenir à destination indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L’identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.
2. **Couche Accès Réseau** : C’est la couche la plus basse de la pile TCP/IP. Elle contient toutes les spécificités concernant la transmission des données sur un réseau physique.

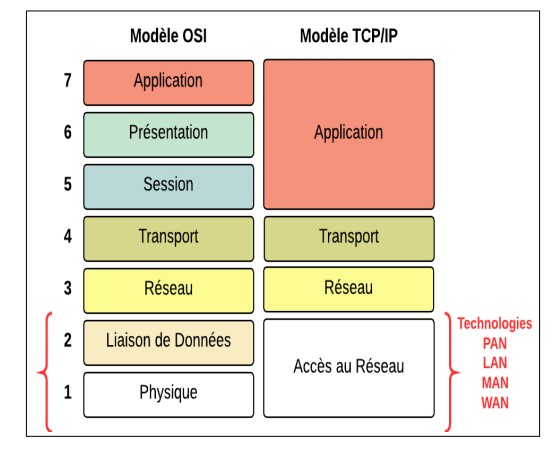


Figure 1. 9 Modèle TCP/IP

# 1.6. Topologie des réseaux

Topologie des réseaux est la manière dont les équipements sont reliés en réseau et se communique en réseau. Les équipements sont connectés dans cette topologie en rapport avec le support de transmission et ils sont en communication grâce aux équipements centraux. Nous avons deux grandes topologies réseaux : topologie réseau et topologie logique.

## 1.6.1 Topologie physique

La topologie Physique est la manière dont les matériels se connectent en réseau. Nous distinguons plusieurs types des topologies physiques mais nous en citerons quelques-unes :

### 1.6.1.1. Topologie en bus

Dans cette topologie, les ordinateurs sont disposés et reliés de part et d’autre d’un câble principal appelé bus. Le support de transmission utilisé dans ce cas est le câble coaxial. Dans cette topologie, lorsqu’un ordinateur envoi une information, tous les autres ordinateurs du réseau reçoivent l’information mais seul la machine à qui l’information est destinée va utiliser.

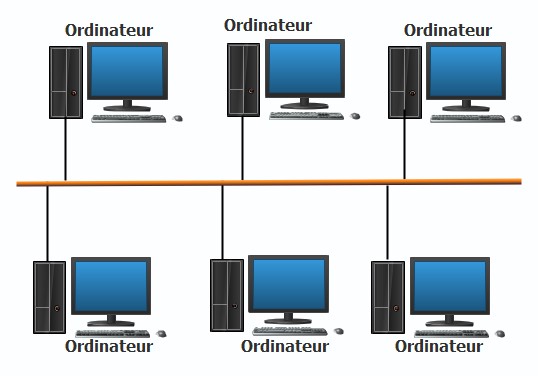


Figure 1. 10 Topologie en Bus

1.6.1.2. Topologie en anneau

Dans cette topologie, les ordinateurs sont connectés à une boucle et communiquent chacun à leur tour. Les informations circulent dans une direction unique, d’un ordinateur à un autre.

Cette Topologie est développée par IBM, elle est principalement utilisée par les réseaux Token Ring. Ce dernier utilise la technique d’accès par jeton. Les informations circulent de station en station, en suivant l’anneau. Un jeton circule autour de l’anneau. La station qui a le jeton émet des données qui font le tour de l’anneau.

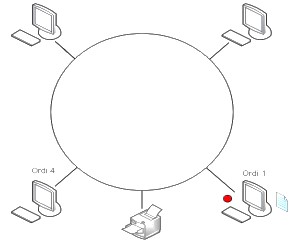


Figure 1. 11 Topologie en anneau

#### 1.6.1.3. Topologie en étoile

Dans cette topologie, les ordinateurs du réseau sont reliés à un équipement central appelé concentrateur (hub) ou un commutateur (Switch).

C’est la topologie la plus courante, notamment avec les réseaux Ethernet RJ-45. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub) ou à celle qui en est le destinataire (Switch).

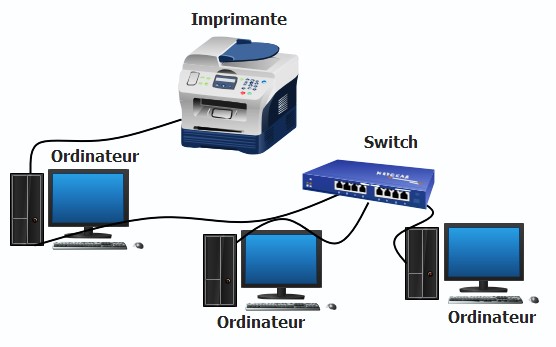
Ce type de réseau est facile à mettre en place et à surveiller. La panne d’une station ne met pas en cause l’ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies. Il est également très facile de rajouter un nœud à un tel réseau puisqu’il suffit de le connecter au concentrateur et le tour est joué.[[16]](#footnote-16)

Figure 1. 12 Topologie en étoile

#### 1.6.2 Topologie Logique

La topologie logique correspond à la manière de faire circuler le signal parmi les composantes physiques. Les topologies logiques les plus connues sont les suivantes :

##### 1.6.2.1. Topologie Ethernet

Cette topologie fait référence à la façon dont les différentes périphéries sont connectées dans un réseau Ethernet. Ethernet est la topologie la plus récente et qui est utilisée partout dans des entreprises et autres. Il est caractérisé par :

* Le débit de 10 Mbits/s à 1Gbit/s ;
* La méthode d’accès suivant la norme IEEE 802.3 (CSMA/CD) ;
* Longueur de trame comprise entre 64 et 1518 Octets ;  Gestion de couches 1 et particulièrement 2 du modèle OSI.

##### 1.6.2.2. Topologie FDDI (Fibre Distributed Data Interface)

Le FDDI a été largement utilisé dans les années 1980 et 1990 pour les réseaux à haut débit, notamment dans les environnements industriels et les réseaux de télécommunications. Cependant, il a été progressivement remplacé par les technologies Ethernet plus récentes et moins coûteuses. Cette topologie fonctionne avec le support de transmission comme la Fibre optique qui a une portée allant jusqu’à 200 km et la vitesse de transfert de donnée peut être au-delà de 100 Mbit/s.

Cette topologie fait appel à un standard de réseau local à haut débit utilisant la fibre optique. La topologie FDDI fonctionne sur base de la transmission en jeton :

* Un jeton circule sur les anneaux pour contrôler l'accès au média.
* Seul le périphérique détenant le jeton peut transmettre des données.

##### 1.6.2.3. Réseau Token Ring

La topologie Token-Ring est utiliser dans de type de réseau local qui utilise un jeton circulant sur un anneau pour contrôler l'accès au média. Voici les principales caractéristiques de cette topologie :

* **Anneau unidirectionnel :** 
  + Les périphériques sont connectés les uns aux autres pour former un anneau unique.
  + Le signal circule dans un seul sens autour de l'anneau.

* Jeton de contrôle d'accès :
  + Un jeton spécial circule sur l'anneau pour contrôler l'accès au réseau.
  + Seul le périphérique détenant le jeton peut transmettre des données.
* Accès déterministe :
  + Grâce au jeton, l'accès au réseau est déterministe et équitable pour tous les périphériques.
* Débit :
  + Le débit typique d'un réseau Token-Ring est de 4 ou 16 Mbit/s.

Cette technologie a été progressivement remplacée par les réseaux Ethernet, plus simples et moins coûteux à mettre en place. Aujourd'hui, la topologie Token-Ring n'est plus largement utilisée.[[17]](#footnote-17)

#### 1.7 Support de Transmission

Une ligne de transmission est une liaison entre deux terminaux. On le désigne généralement par le terme émetteur le terminal qui envoie les données et celui qui les reçoit s’appelle récépteur. Une ligne de communication est un canal servant à transiter les signaux d’un émetteur vers le récepteur.

## 1.7.1 Types de supports de transmission

Les supports de transmissions sont de canaux permettant de faire circuler les informations entre les différents équipements réseaux. On classe généralement ces supports en trois catégories, selon le type de grandeur physique qu’ils permettent de faire circuler, donc de leur constitution physique :

* Les supports filaires : permettent de faire circuler une grandeur électrique sur un câble généralement métallique ;
* Les supports aériens : désigne l’air ou le vide, ils permettent la circulation d’ondes électromagnétiques ou radioélectriques diverses ;
* Les supports optiques permettant d’acheminer des informations sous forme lumineuse.

### 1.7.1.1 Supports filaires

Pour relier les diverses entités d’un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés. Une de ces possibilités est l’utilisation de câbles. Il existe de nombreux types de câbles, mais on distingue généralement :

* Le câble de type coaxial
* La double paire torsadée
* La fibre optique

#### Câble coaxial

Le câble coaxial (en anglais coaxial câble) a longtemps été le câblage de prédilection, pour la simple raison qu’il est peu couteux et facilement manipulable. Un câble coaxial est constitué d’une partie centrale (appelé âme), enveloppé d’un isolant, puis d’un blindage métallique tressé et enfin d’une gaine extérieure.



Figure 1. 13 Câble coaxial

#### Câble à paire torsadée

Le câble à paire torsadée (en anglais twisted-pair câble) est constitué de deux brins de cuivre entrelacés en torsade et recouvert d’isolant.



Figure 1. 14 Câble à paire torsadée

#### Fibre optique

Une fibre optique est un fil en verre de très petite taille à base de silice qui a la propriété d’être un conducteur de la lumière et qui sert dans la transmission de données sous forme lumineuse. Elle constitué de trois grandes parties qui sont :

* Le cœur ;
* Gain optique ;
* Enveloppe protectrice.

Généralement on distingue deux types de fibres optiques qui sont :

* La fibre monomode
* Fibre multimode

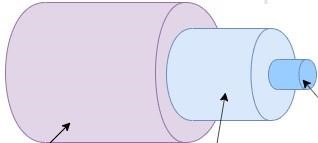


Figure 1.15 Fibre optique

## 1.7.2 Supports non filaires

Pour les transmissions sans fil, l’air représente le support de transmission et le signal transporté est une onde électromagnétique. Les ondes électromagnétiques se propagent dans l’atmosphère où dans le vide. L’absence de support matériel apporte une certaine souplesse et convient aux applications comme la téléphonie ou les télécommunications mobiles, sans la pose couteuse de câble. Les principaux sont :

### Faisceaux hertziens

Un faisceau hertzien est un système de transmission entre deux points fixes, par ondes électromagnétiques très fortement concentrées à l’aide d’antennes directives.

* **Ondes radioélectriques**

Les ondes radioélectriques correspondent à des fréquences comprises entre 10 KHz et 2 GHz. Un émetteur diffuse ces ondes captées par des récepteurs dispersés géographiquement. Contrairement aux faisceaux hertziens, il n’est nécessaire d’avoir une visibilité directe entre émetteur et récepteur, car celui-ci utilise l’ensemble des ondes réfléchies et diffractées.

Les supports de transmission ou lignes de transmission sont des tuyaux qui servent à transporter les informations entre différents points du réseau. Généralement nous distinguons deux grandes familles de supports de transmission, à savoir le support de transmission filaire et le support de transmission non filaire.

#### 1.8. PROTOCOLES RESEAUX[[18]](#footnote-18)

Un protocole réseau est un ensemble de règles et de conventions qui définissent la manière dont les appareils communiquent sur un réseau informatique. Il s'agit d'un langage commun permettant aux différents équipements de se comprendre et d'échanger des informations de manière standardisée. Les principaux rôles d'un protocole réseau sont :

* Définir le format des données à transmettre : la structure des paquets de données, les en-têtes, etc.
* Gérer l'acheminement des données : comment les données sont routées d'un point à un autre sur le réseau.
* Contrôler le flux de données : comment le débit de transmission est régulé pour éviter la congestion.
* Assurer la fiabilité de la transmission : comment les erreurs sont détectées et corrigées.
* Sécuriser les échanges : comment l'authentification, le chiffrement et l'intégrité des données sont garantis.

##### 1.8.1 Protocole TCP (transmission control Protocol)

TCP comble les caractères d’IP lorsque les applications requièrent une grande fiabilité. Ce protocole de transport, lourd et complexe, met en œuvre la détection et correction d’erreurs, gère les contrôles de flux et négocie les conditions du transfert de données entre les deux extrémités de la connexion. L’entité gérée par le TCP s’appelle segment. Une fois le segment fabriqué, le module TCP sollicite le module IP pour le service de transmission, par l’intermédiaire d’une primitive. A l’inverse, lorsque le module IP reçoit un datagramme destiné à la machine concernée et que celui-ci transporte un segment TCP, le module IP extrait le segment du datagramme et en signale l’arrivée au module TCP par la primitive : indication-réception (segment reçu, adresse IP source).

##### 1.8.2 Protocole UDP (user datagram protocole)

UDP est un protocole de transport sans connexion qui permet l’émission de message sans établissement préalable d’une connexion. C’est un protocole non fiable, beaucoup plus simple que TCP, car il n’ajoute aucune valeur ajoutée par apport au service offert par IP. L’utilisateur n’est donc pas assuré de l’arrivée des données dans l’ordre où il les a émises, pas plus qu’il peut être sûr que certaines données ne seront ni perdues, ni dupliquées, puisqu’UDP ne dispose pas de mécanisme de contrôle pour vérifier cela. De ce fait, il n’introduit pas de délai supplémentaire dans la transmission des données entre l’émetteur et récepteur.

##### 1.8.3 Protocole HTTP (Hyper Text Transfert Protocole)

HTTP est le protocole fondamental pour le fonctionnement du World Wide Web, permettant aux navigateurs d'interagir avec les serveurs web. Le protocole HTTP est le standard pour le transfert de données sur le World Wide Web. Il fonctionne selon une architecture client-serveur, où le client (navigateur web) envoie des requêtes HTTP au serveur web, qui renvoie alors des réponses.

Les principales méthodes HTTP sont GET, POST, PUT et DELETE, qui permettent respectivement de récupérer, envoyer, remplacer et supprimer des ressources sur le serveur. Les réponses HTTP sont identifiées par des codes de statut, comme 200 pour le succès, 404 pour une page non trouvée, ou 500 pour une erreur serveur.

#### 1.10 ADRESSAGE IP

Une Adresse IP (Internet Protocole) désigne un numéro unique attribué d’une manière provisoire à un terminal qui veut se connecter en réseau Informatique. Une Adresse IP (Internet Protocole) désigne un numéro unique attribué d’une manière provisoire à un terminal qui veut se connecter en réseau Informatique.

Nous avons deux version d’adresse IP qui sont : la version 4 codé de 32 bits et la version 6 codés de 128 Bits. La version la plus utilisée est la version 4, dans cette version 4 codé sur 32 bites. Chaque machine d’un réseau TCP/IP possède une adresse IP (Internet Protocol). Une adresse IP est constituée d’un groupe de 4 octets soit 4 fois 8 bits, les octets les plus à gauche déterminent l’adresse du réseau et le ou les octets de droite déterminent l’adresse de la machine. Exemple : 192.168.1.5 192.168.1.0 correspond à l’adresse réseau alors que 5 représente l’adresse de l’ordinateur dans le réseau.

Tableau 1.1: Classes d’adresses

|  |  |  |
| --- | --- | --- |
| **classe** | **Plage d’adresse** | **Masque par défaut** |
| **A** | De 1 à 126 | 255.0.0.0 |
| **B** | De 128 à 191 | 255.255.0.0 |
| **C** | De 192 à 223 | 255.255.255.0 |
| **D** | De 224 à 239 | Réservé (multicast) |
| **E** | De 240 à 254 | Réservé à l’IANA |

##### 1.10.1 Adresses particulières

Lorsqu’une machine ne possède pas d’adresse IP et qu’elle doit envoyer un (premier) message pour en obtenir une, elle remplit le champ Adresse du message par « plein 0 » ou 0.0.0.0 en notation décimale pointée. À l’opposé, remplir le champ Adresse par « plein 1 » permet de désigner l’ensemble des machines au sein du réseau dans lequel se trouve la machine.

Ainsi, il existe pour chaque classe d’adresse deux adresses particulières à savoir, l’adresse du réseau et l’adresse de diffusion ou Broadcast address.

* **Adresse du réseau :** elle est obtenue en remplaçant le champ identifiant machine par le plein 0 conformément à la classe. Par exemple : Pour l’adresse 192.168.0.111, de classe C, en remplaçant l’identifiant machine par le plein 0, on obtient 192.168.0.0 qui est l’adresse de ce réseau.
* **Adresse de diffusion** ou Broadcast address, désigne l’ensemble des machines d’un réseau distant. Elle est constituée en remplaçant le champ Identifiant machine par le « plein 1 ». Exemple : L’adresse de diffusion du réseau 192.168.0.0 est 192.168.0.255

##### 1.10.2 Notions de sous-réseaux et masque de sous-réseaux

La hiérarchie à deux niveaux (réseau et machine) de l’adressage IP s’est rapidement révélée insuffisante à cause de la diversité des architectures des réseaux connectés. La notion de sous-réseau (ou subnet), introduite en 1984, a conservé le format de l’adresse IP sur 32 bits.

Dans un réseau subdivisé en plusieurs sous-réseaux, on exploite autrement le champ Identifiant de machine de l’adresse IP. Celui-ci se décompose désormais en un identifiant de sous-réseau et un identifiant de machine.

Remarquons que ce découpage n’est connu qu’à l’intérieur du réseau lui-même. En d’autres termes, une adresse IP, vue de l’extérieur, reste une adresse sur 32 bits avec ses deux champs. On ne peut donc pas savoir si le réseau est constitué d’un seul réseau ou subdivisé en plusieurs sous-réseaux. L’administrateur local choisit le nombre de bits à consacrer à l’identifiant de sous-réseau grâce au masque de sous-réseau (ou Subnet mask). Celui-ci, également codé sur 32 bits, définit le découpage de l’identifiant machine en deux champs (Sous-réseau et Machine).

**1.11 Notion de cryptographie**

La cryptographie est la science et la pratique du chiffrement et du déchiffrement de l'information. Elle vise à assurer la confidentialité, l'intégrité et l'authenticité des données, notamment en empêchant l'accès non autorisé aux informations sensibles

1.11.1 **Principes clés** :

* **Confidentialité :**

Seuls les destinataires autorisés peuvent accéder et comprendre les informations.

* **Intégrité :**

La cryptographie garantit que les données n'ont pas été modifiées ou altérées pendant la transmission ou le stockage.

* **Authentification :**

La cryptographie permet de vérifier l'identité de l'expéditeur et du destinataire, assurant que le message provient bien de la source attendue.

**1.11.2Types de cryptographie**

**1.11.2.1 Cryptographie symétrique**

C’est une méthode qui utilise une seule clé publique pour chiffrer et déchiffrer l’information

* Très rapide et efficace, idéale pour de grandes quantités de données
* Algorithme qu’il utilise sont AES, DES, BlowFish
* **Inconvénients** :

La clé doit être partagée entre les parties, ce qui peut poser un risque si elle est interceptée

**1.11.2.2 Cryptographie asymétrique**

Utilise une paire de clés (publique et privée) dont la clé publique est utilisée pour chiffrer, et une clé privée pour déchiffrer l’informations

* Plus sécurisée pour les échanges sur des réseaux ouverts
* Algorithme qu’il utilise sont : RSA, ECC, DSA
* Permet aussi les signatures numériques pour authentifier l’expéditeur
* **Inconvénients :** plus lente et gourmande en ressources

|  |  |  |
| --- | --- | --- |
| **Critères** | **Symétrique** | **Asymétrique** |
| Nombre de clés | 1 | 2(public + privée |
| Vitesse | Rapide | Plus lente |
| Sécurité du partage | Risqué | Plus sécurisé |
| Cas d’usage | Stockage, VPN, Bases Données | SSL/TLS,email,signatures |
| Scalabilité | Limitée | Élevée |

#### 1.12 Conclusion

Tout au long de ce chapitre nous avions appris les généralités sur les réseaux informatiques, Au chapitre suivant nous allons parler sur les fondements Théoriques des systèmes des systèmes de détection et de prévention d’intrusion. Le prochain chapitre se consacrera sur l’étude des systèmes de détection d’intrusion.

# CHAPITRE 2 : ETUDE DES SYSTEMES DE DETECTION D’INTRUSION (IDS)

# 2.1 Introduction

Dans ce chapitre, nous ferons une étude sur les systèmes de détection d’intrusion IDS/IPS. Identifier un scénario d’attaque d’un réseau et les différents mécanismes de protection contre ces attaques. Malgré leurs grands intérêts, ils présentent des lacunes dues à l’évolution des techniques utilisées par les hackers. Ainsi, dans l’impossibilité de détecter toutes les sortes d’attaques, le système de détection d’intrusion tente de déceler les attaques qui passent inaperçues à travers les mécanismes de sécurité.

**2.2 PRESENTATION DE LA RADIO TELEVISION NATIONALE CONGOLAISE[[19]](#footnote-19)**

* + 1. **Situation géographique**

La RTNC est située dans la commune de Lingwala au croisement des avenues Kabinda et de la Libération (ex. 24 novembre). La Cité de la voix du Peuple abrite ses studios de radio et de télévision ainsi que les bureaux de l’administration centrale.

Elle exercice ses activités sur toute l’étendue du territoire national. Elle peut, moyennant l’autorisation de l’autorité de tutelle, ouvrir des Directions provinciales, des stations, des sous- stations, des agences et des bureaux en tous autres lieux de la République ou à l’étranger.

* + 1. **Aperçu historique**

La Radio Congo-Belge a vu le jour en 1936 à Léopoldville suite à la demande des autorités coloniales. Elle servait comme une station relai qui recevait les émissions de Bruxelles et qui s’adressaient aux africains.

Ce service de radiodiffusion du Congo-Belge fut installé dans l’actuelle commune de la Gombe, jadis appelée KALINA.

En 1937, une station privée Radio-Léo est créée à l’initiative des missionnaires catholiques (les Jésuites) du Collège Albert premier, actuellement BOBOTO, pour une élite africaine toute dévouée à la base de musique classique. En 1940, la guerre oblige le colonisateur belge à

confisquer la station de la radiodiffusion des missionnaires. Ce fut la naissance officielle de la Radio Congo-Belge mais uniquement pour les blancs, aucun Congolais n’avait accès aux émissions de la radio. Le premier janvier 1949 eut lieu l’inauguration de la Radio Congo-Belge pour les africains (Congolais) et elle émettait chaque jour de 17 heures à 22 heures. Cette fois ci, le contenu des programmes était composé des bulletins d’informations et des émissions consacrées au savoir- vivre. Ces émissions étaient en principe diffusées en langues nationales (Lingala, Tshiluba, Swahili et Kikongo) pour la masse (autochtone) et en français pour les évolués.

A l’occasion de l’indépendance du Congo-Belge, te 30 juin 1960, les stations radio Congo-Belge pour africains et Radio Congo Belge pour européens furent fusionnées à une seule station de diffusion « La Radio Télévision Nationale Congolaise », RTNC laquelle fut installée à Léopoldville.

De 1960 à 1965, la radiodiffusion devient l’instrument de l’unité nationale, cela grâce à son impact réel sur la masse. Mais, cela surtout en 1967 grâce à l’installation de plusieurs émetteurs, la radio peut enfin diffuser 24 heures sur 24 et atteindre presque tous les coins du pays. Cette période est caractérisée par l’évolution des mentalités, des conceptions et des intérêts des auditeurs grâce à l’impact de la radiodiffusion. Cette évolution se manifeste sur le plan démographique, intellectuel, social.

La télévision au Congo a vu le jour le 23 novembre 1967. En 1977, le Zaïre s’est doté d’un Complexe de radiodiffusion et de télévision le plus moderne, comprenant, à Kinshasa la Cité de la Voix du peuple (ex- Cité de la Voix du Zaïre), avec sept studios de télévision et quatorze studios de radio, huit stations provinciales reliées par satellite. Comme il était nécessaire de concevoir et de faire fonctionner un outil capable de répondre aux besoins considérables en personnel qualifié pour la RTNC (ex-OZRT), il a été ouvert en janvier 1978 un centre de formation aux métiers de la radio et de la télévision, le studio-école de la Voix du Zaïre (SEVOZA), actuellement Institut Congolais de l’Audiovisuel (I.C.A).

En 1981, l’ordonnance n° 81/050 plaçant la RTNC parmi les entreprises publiques fut signée. A l’avènement de l’Alliance des Forces Démocratiques pour la Libération du Congo AFDL le 17 mai 1997 et surtout la débaptisation du pays (Zaïre en Congo), l’appellation de l’Office Zaïrois de radiodiffusion et de Télévision changera en Radiotélévision Nationale Congolaise.

**2.2.3. Statut et forme juridique**

La Radiotélévision Nationale Congolaise, dans sa configuration actuelle, est un établissement public de l’Etat. Elle est régie par le décret n°09/031 du 02 décembre 2009 qui stipule en ses articles 1 et 2 ce qui suit :

**Article 1er** : L’Office Zaïrois de Radio diffusion et de Télévision, en abrégé « OZRT », créé par l’ordonnance n° 81-050 du 02 avril 1981, est transformé en établissement public à caractère socio-culturel, doté de la personnalité juridique, appelé «Radiotélévision Nationale Congolaise », ci-après dénommé « la R.T.N.C ».Il est régi par la loi n° 08/009 du 07 juillet 2008 portant dispositions générales applicables aux établissements publics et par le présent Décret.

**Article 2** : La RTNC est ainsi subrogée dans les biens, droits, actions, actifs et passifs que détenait l’entreprise publique « Office Zaïrois de Radio diffusion et de Télévision » à la date de la signature du présent Décret. Elle est en outre subrogée, dans les mêmes conditions, purement et simplement, dans le bénéfice et la charge de tous contrats, obligations, engagements, conventions quelconques existant dans le chef de l’entreprise publique « Office Zaïrois de Radiodiffusion et de Télévision ».

L’ensemble des liens corporels et incorporels ainsi que les créances nettes, tels qu’ils ressortent de derniers états financiers certifiés de l’entreprise publique « Office Zaïrois de Radiodiffusion et de Télévision », constituent la dotation de la RTNC.

Le patrimoine de la RTNC est constitué :

* De tous les biens, droits et obligations qui lui sont reconnus conformément à l’article 2 du présent Décret ;
* Des équipements, matériels et autres biens acquis dans le cadre de l’exécution de sa mission ;
* De tous les biens, droits et obligations reconnus à l’Etat Congolais dans le domaine de la radiodiffusion et de télévision, avant et après l’entrée en vigueur de l’Ordonnance n° 81-050 du 02 avril 1981 portant création et statut de « l’Office Zaïrois de Radiodiffusion et Télévision » ; Il peut s’accroître de toute acquisition propre jugée nécessaire pour fonctionnement, des apports ultérieurs que l’Etat pourra lui consentir et des réserves qui pourront lui être incorporées.

Les ressources de la RTNC proviennent

* De la redevance annuelle pour la consommation du service public de radiodiffusion et de télévision ;
* De la gestion du réseau de la télévision numérique terrestre (TNT) ;
* De la publicité, des productions cinématographiques et autres se rapportant à ses missions ;
* De l’administration de son patrimoine et des biens dont la gestion lui est confiée ;
* Des subsides qui lui sont alloués par l’Etat ;
* Des dons, legs et libéralités ;
* Des ressources diverses et exceptionnelles.

**2.2.4. Objectifs poursuivis**

En créant la RTNC, l’Etat lui a confié deux objectifs, à Savoir :

* Un objectif social ;
* Un objectif économique

**2.2.4.1 Objectifs sociaux**

La RTNC a pour objet d’assurer le service public de radiodiffusion et de télévision conformément aux dispositions légales et réglementaires en vigueur.

A cet effet, elle est chargée notamment

* De réaliser la couverture des activités politiques, économiques et sociales ;
* D’élaborer et de mettre en œuvre tout programme d’actions et toute production audiovisuelle en matière de radiodiffusion et de télévision ;
* De mener toute étude ou tout sondage visant l’amélioration qualitative de la radio et de la télévision à l’échelle nationale, régionale et internationale ;
* De réaliser la production nationale des programmes artistiques et éducatifs ; de produire et coproduire des œuvres et documents audiovisuels, de les commercialiser et de les diffuser sur les antennes et par tous les autres moyens audiovisuels, tant dans le pays qu’à l’étranger, pour contribuer au rayonnement de la culture et de la civilisation Congolaise ;
* D’assurer la production cinématographique et d’en assurer la commercialisation ;
* De conclure toute convention pour la production ou l’échange des programmes avec les administrations ou organismes intéressés ;
* De vulgariser les activités et les programmes d’actions des Institutions de la République Démocratique du Congo.

**2.2.4.2 Objectifs économiques**

Depuis 1981 suivant l’ordonnance n° 81/050 créant

L’office, la RTNC a eu pour objectif économique la production, la commercialisation et la vente des espaces publicitaires.

Parmi les missions lui assignées, la RTNC vend tant bien que mal ses services à la radio et la télévision et ce, en diffusant divers communiqués, messages et des spots publicitaires. C’est à travers les activités ci-haut mentionnées que la RTNC apparaît comme une grande entreprise de production, de commercialisation et de vente des espaces publicitaires et des spots.

**2.2.5 Structures organiques & fonctionnelles de la RTNC**

**2.2.5.1** **Structure organique**

L’organigramme est un tableau hiérarchique qui, en

donnant les directions et subdivisions, montre d’une part la répartition des responsabilités et d’autres part la localisation des VERHULST A. Economie de l’Entreprise, éd. Centre de Recherche Pédagogique, Kinshasa, 1981, P. 36

Source : service du Personnel, Direction des Ressources Humaines/RTNC.

**2.2.5.2** **Structure fonctionnelle**

C’est la définition des attributions qu’exercice chaque

Poste de responsabilité dans la structure.

**2.2.5.3** **Le conseil d’administration**

Le conseil d’administration est l’organe de conception,

D’orientation, de contrôle et de décision de la RTNC.

Il définit la politique générale, détermine le programme

d’activités, arrête le budget et approuve les états financiers de fin d’exercice. II fixe l’organigramme de la RTNC et le soumet pour approbation au Ministre de tutelle.

II fixe, sur proposition de la Direction Générale, le cadre

et le statut du Personnel et le soumet pour approbation au Ministre de tutelle. Le Conseil d’Administration est composé de cinq membres au maximum, en ce compris le Directeur Général.

Le Conseil d’Administration se réunit trimestriellement en

séance ordinaire, sur convocation de son Président.

Il peut être convoqué en séance extraordinaire par son Président, sur un ordre du jour déterminé, à la demande du Ministre de tutelle, chaque fois que l’intérêt de la RTNC l’exige.

**2.2.5.4** **La Direction Générale**

La Direction Générale est dirigée par le Directeur Général assisté d’un Directeur Général Adjoint, tous deux nommés, relevés de leurs fonctions et, le cas échéant, révoqués par Ordonnance du président de la République, sur proposition du Gouvernement délibérée en Conseil des Ministres.

Le Directeur Général et le Directeur Général adjoint

sont nommés pour un mandat de cinq ans renouvelable une fois.

Ils ne peuvent être suspendus à titre conservatoire que

par Arrêté du Ministre de tutelle qui en informe le Gouvernement.

La Direction Générale exécute les décisions du Conseil

d’Administration et assure la gestion courante de la RTNC. Elle exécute le budget, élabore les états financiers et dirige l’ensemble des services.

**2.2.5.5** **Le Collège de Commissaires aux Comptes**

Le contrôle des opérations financières de la RTNC est

assuré par un Collège de Commissaires aux Comptes.

Celui-ci est composé de deux personnes issues des

structures professionnelles distinctes et justifiant des connaissances techniques et professionnelles éprouvées.

**2.2.5.6** **Les activités des Directions de l’administration centrale**

Pour accomplir les missions dévolues à l’objet social et

Commercial de sa personnalité juridique, La RTNC agit à travers 20 Directions Centrales subdivisées en Sous-Directions, Services, Sections et Cellules. La RTNC est également représentée dans les chefs- lieux des provinces (stations provinciales).

Ci-dessous, une description sommaire relative aux

activités de chaque Direction.

1. **La Direction Générale**

Cette Direction est chargée de la centralisation des

Documents émanant des autres Directions. C’est aussi le cabinet du Directeur Général de la RTNC.

1. **Direction des Ressources Humaines**

Elle s’occupe de la gestion du Personnel, de l’engagement et du reclassement des agents, de la gestion des approvisionnements (achats, économat et distribution d’outils de travail) ; elle est également chargée du suivi de la carrière des agents et de leur rémunération.

1. **Direction Financière**

* Elle gère les ressources financières de la RTNC. Elle est chargée de
* Dresser les prévisions budgétaires ;
* Normaliser les écritures en matière de paiement de créance et de recouvrement des recettes ;
* Mettre à jour les documents comptables.

1. **Direction Commerciale & Marketing**

Cette Direction est chargée de :

* La commercialisation et la vente des espaces publicitaires que la RTNC met à la disposition des agences publicitaires pour le compte des tiers ;
* La production sur les spots et des émissions à caractère musical pour le compte des agences et des tiers.

Ceux-ci sont destinés à l’antenne radiotélévision pour la

Publicité et la couverture des événements et des manifestations.

1. **Direction de la Redevance**

Pour s’autofinancer, la RTNC a eu l’ingénieuse idée de

Créer la Direction de la redevance sur la radio et la télévision auprès des auditeurs et téléspectateurs de la Voix du peuple.

1. **Direction des programmes radio**

Elle s’occupe de la confection des grilles de

Programmes à la radio, la gestion et la diffusion des programmes à la radio.

1. **Direction des programmes télévisés**

Cette Direction a pour activités essentielles

- la confection et la diffusion des programmes de la télévision

- la gestion de l’antenne télévisée.

1. **Direction des informations radio**

Pour réaliser les missions lui dévolues, elle s’emploie

* Collecter les informations, les traiter et les diffuser sous forme des émissions à produire à la radio ;
* Confectionner les magazines d’informations à la radio.

1. **Direction des informations télévisées**

Elle se charge de la collecte, de l’élaboration, de

l’étude et de la diffusion des informations en langue française à la télévision.

**10.Direction de la RTNC 2**

Considérée comme la deuxième chaîne de la RTNC, elle est chargée de la conception et de la préparation des programmes de télévision pour la culture et l’éducation en générale, les programmes scolaires et des enfants en particulier. Cette chaîne a une vocation provinciale. Elle couvre la ville de Kinshasa.

**11.Direction de Radio Kinshasa**

Cette Direction fait fonctionner la radio de proximité

avec comme mission, aider la RTNC à faire face à la concurrence des radios locales implantées ou opérant à Kinshasa ou ses environs. Elle a une vocation provinciale.

**12.Direction des Langues nationales**

La Direction des Langues nationales se charge aussi de

la collecte, de l’élaboration, de l’étude et de la diffusion des productions et des informations essentiellement en nos langues nationales. C’est-à- dire en swahili, en tshiluba, en lingala et en kikongo.

**13.Direction technique radio**

Comme l’indique bien sa dénomination, elle s’occupe

* De la gestion et de la maintenance des équipements et des installations radio ;
* Du suivi technique de la transmission des informations et l’antenne radio.

**14.Direction technique TV**

Cette Direction s’occupe essentiellement

* De la gestion et de la maintenance des équipements et des installations TV ;
* Du suivi technique de la transmission des programmes à l’antenne.

**15.Direction de l’Intendance Générale**

L’autorité de la RTNC a confié à cette Direction les activités ci-après

* La gestion de l’ensemble des moyens matériels de la RTNC ;
* L’exécution de tous les travaux d’appui pour que les différentes Directions de la RTNC arrivent à réaliser les missions leurs confiées.

**16.Direction de Sports radio TV**

Elle est chargée de la recherche et de la diffusion des informations sportives nationales et internationales.

**17.Direction de Ciné Production**

De part sa domination cette Direction a pour vocation :

* La production des films
* La production des photos d’actualités
* La production des documents visuels destinés à l’antenne TV et la vente.

1. **Direction de la RTNC Records & Médiathèques**

Tout comme la Direction Commerciale et la Direction

de la Redevance qui ont l’objectif de renflouer la caisse de la RTNC, la RTNC Records & Médiathèques se doit de valoriser les productions audiovisuelles de la RTNC. De même elle est chargée de la production des spectacles en concertation avec la Direction Commerciale.

1. **Direction de l’Institut Congolais de l’Audiovisuel (I.C.A)**

Elle s’emploie

* à la formation du Personnel appelé à œuvrer avec radio ou à la télévision ;
* au sondage d’opinions et au recyclage des agents ;
* à l’étude et à la recherche des voies et moyens audiovisuelles en RDC.

1. **Direction Médico-sociale**

Elle s’occupe principalement des œuvres sociales la polyclinique, la cantine, les sports, les enterrements et de tout ce qui touche à la vie sociale de l’agent de sa famille.

**STATIONS PROVINCIALES**

La RTNC est également représentée dans toutes les provinces. Chaque station est dirigée par un Directeur provincial. Il y a 10 stations provinciales :

* station provinciale du Bas-Congo à Matadi
* station provinciale du Bandundu à Bandundu
* station provinciale du l’Equateur à Mbandaka
* station provinciale du Kasaï-Occidental à Kananga
* station provinciale du Katanga à Lubumbashi
* station provinciale du Kasaï-Oriental à Mbuji-Mayi
* station provinciale du Province Orientale à Kisangani
* station provinciale du Sud Kivu à Bukavu
* station provinciale du Nord Kivu à Goma

# 2.3 Définition des systèmes de détection

Un système de détection d’intrusion (IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d’avoir une action de prévention et d'intervention sur les risques d’intrusion. Afin de détecter les attaques que peut subir un système (réseau informatique), il est nécessaire d’utiliser un logiciel spécialisé dont le rôle est de surveiller les données (stockées ou) qui transitent par ce système, et qui est capable de réagir si des données semblent suspectes.[[20]](#footnote-20)

# 2.3. Définition d’un système d’intrusion

Un IDS (Intrusion Detection System) est un ensemble de composants logiciels et/ou matériels dont la fonction principale est de détecter et analyser des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

## 2.3.1. Différents types d'IDS (classification)

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situés à plusieurs niveau (réseau, machine, application, etc.).

## 1. Systèmes de prévention d'intrusion (IPS)

IPS signifie **Intrusion Prévention System**. Ce sont des composants matériels ou logiciels utilisés afin d'empêcher une activité suspecte sur l'environnement cible (réseau, ordinateur, serveur, etc.). Contrairement aux IDS, les IPS sont des systèmes qui peuvent non seulement détecter une intrusion mais aussi la bloquer. Cependant, il faut faire très attention à ne pas bloquer du trafic ou activité légitime.

# 2. Systèmes de détection d'intrusion réseaux (NIDS)

NIDS pour "Network Intrusion Detection System". Les NIDS écoutent passivement tout le trafic transitant le réseau en temps réel, l'analysent et déclenchent des alertes si des paquets semblent suspects ou dangereux. Le NIDS reconnait un trafic suspect ou dangereux en le comparant à sa bibliothèque d'attaques connues. Dans le cas d'un NIPS les paquets malveillants sont non seulement détectés mais aussi arrêtés (bloqués). Les NIDS sont très utilisés et permettent, selon la technologie utilisée, non seulement d'analyser le trafic mais aussi de garder une trace de ce dernier (pcap: PacketCAPture) pendant un certain temps. Il existe deux types de NIDS :

* **NIDS en ligne**: Dans ce type le NIDS analyse un réseau en temps réel. Il analyse les paquets transitant le réseau et applique des règles prédéfinies afin de déterminer s'il s'agit d'une attaque ou non.
* **NIDS hors ligne** (mode tap): Dans ce cas, le NIDS traite les paquets collectés. Ce qui signifie qu'il les passe à travers un certain nombre de processus afin de décider du résultat (attaque ou non).

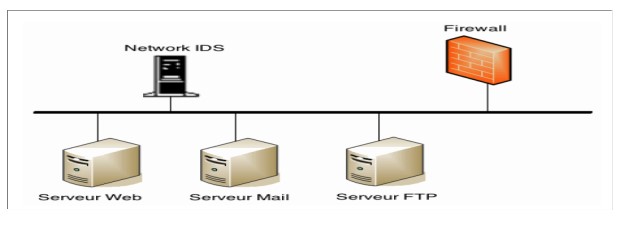


Figure 1. 16 Système de détection d’intrusion réseau.

## 2.3.2 Systèmes de détection d'intrusion de type hôte (HIDS)

HIDS pour "Host Intrusion Detection System". Les HIDS se concentrent principalement sur l'analyse en temps réel de l'activité qui se passe sur une machine donnée, c'est à dire les paquets entrants et sortants de cette machine, ou les logs de cette dernière (appel système, modification de fichiers, authentification aux applications, etc.). Ensuite, le HIDS déclenche une alerte en cas de détection d'activité suspecte. Exemple: l'HIDS prend des captures des fichiers système dans un temps T et les fait correspondre aux précédents fichiers. Si l'HIDS détecte qu'un fichier critique a été modifié ou supprimé, le HIDS déclenche une alerte à l'administrateur réseau ou à l'équipe de sécurité pour enquêter sur le changement effectué. Un HIDS installé sur une machine cible, cette dernière devrait être saine. Si la machine a été compromise avant l'installation d'un HIDS, le système de détection d'intrusion ne sera plus efficace. Les HIDS sont très utilisés sur les machines critiques et peuvent détecter les menaces qu'une solution NIDS pourrait manquer.[[21]](#footnote-21)

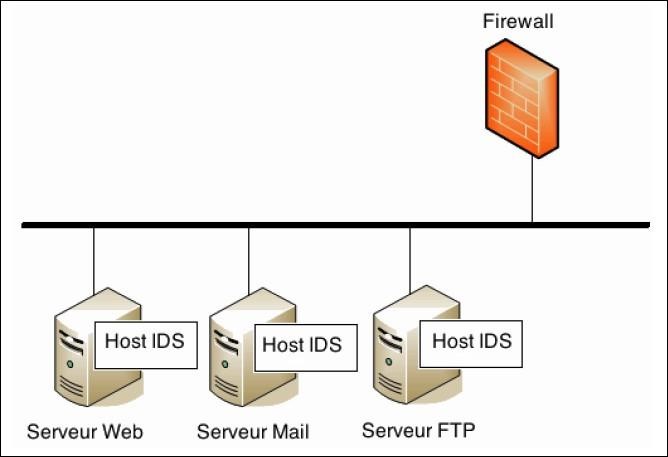


Figure 1. 17 Système de détection d’intrusion hôte.

## 2.3.3 Systèmes de détection d'intrusion hybrides

Les IDS hybrides peuvent être utilisés pour collecter les informations en provenance d'un système HIDS et NIDS, d'où l'appellation "hybride". Prélude est un IDS hybride permettant de collecter et de stocker des informations de différents systèmes relativement variés.[[22]](#footnote-22)

Les systèmes de détections d’intrusions hybrides, rassemblent les caractéristiques de plusieurs systèmes de détections différents. En pratique, on trouve la combinaison des NIDS et HIDS qui permettent de surveiller le réseau et l’hôte.

Les sondes agissent comme un NIDS ou un HIDS Il permet de réunir les informations de diverses sondes placées sur le réseau. L’exemple le plus connu dans le monde Open-Source est Prelude.

* Cet IDS permet de stocker dans une base de données des alertes provenant de différents systèmes relativement variés.
* Utilisant Snort comme NIDS, et d’autres logiciels tels que Samhain en tant que HIDS, il permet de combiner des outils puissants tous ensemble pour permettre une visualisation centralisée des attaques.

# 2.4 Mode de fonctionnement

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion. Il existe deux modes de détection, la détection d'anomalies et la reconnaissance de signatures. D'eux-mêmes, deux types de réponses existent, la réponse passive et la réponse active. Nous allons tout d'abord étudier les modes de détection d'un IDS, avant de présenter les réponses possibles à une attaque.[[23]](#footnote-23)

## 2.4.1 Modes de détection

Nous notons deux modes de détection qui sont :

* La détection d'anomalies
* La reconnaissance de signature

Il faut noter que la reconnaissance de signature est le mode de fonctionnement le plus implémenté par les IDS du marché. Cependant, les nouveaux produits tendent à combiner les deux méthodes pour affiner la détection d'intrusion.

## 2.4.2 Détection d'anomalies[[24]](#footnote-24)

Elle consiste à détecter des anomalies par rapport à un profil "de trafic habituel". La mise en œuvre comprend toujours une phase d'apprentissage au cours de laquelle les IDS vont découvrir le fonctionnement normal des éléments surveillés. Ils sont ainsi en mesure de signaler les divergences par rapport au fonctionnement de référence.

Les modèles comportementaux peuvent être élaborés à partir d'analyses statistiques. Ils présentent l'avantage de détecter des nouveaux types d'attaques. Cependant, de fréquents ajustements sont nécessaires afin de faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes générées.

## 2.4.3 Reconnaissance de signatures[[25]](#footnote-25)

Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce type d'IDS est purement réactif ; il ne peut détecter que les attaques dont il possède la signature.

De ce fait, il nécessite des mises à jour fréquentes. De plus, l'efficacité de ce système de détection dépend fortement de la précision de sa base de signature. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniques dites "d'évasion" qui consistent à maquiller les attaques utilisées. Ces techniques tendent à faire varier les signatures des attaques qui ainsi ne sont plus reconnues par l'IDS.

Une signature permet de définir les caractéristiques d'une attaque, au niveau des paquets (jusqu'à TCP ou UDP) ou au niveau des protocoles (HTTP, FTP...).

* Au niveau paquet, l'IDS va analyser les différents paramètres de tous les paquets transitant et les comparer avec les signatures d'attaques connues.
* Au niveau protocole, l'IDS va vérifier au niveau du protocole si les commandes envoyées sont correctes ou ne contiennent pas d'attaque. Cette fonctionnalité a surtout été développée pour HTTP actuellement. Il faut savoir que les signatures sont mises à jour en fonction des nouvelles attaques identifiées.

**2.5 Systèmes de prévention d’intrusion IPS**

Les IPS ont pour fonction principale d’empêcher toute activité suspecte détectée au sein d’un système, ils sont capables de prévenir une attaque avant qu'elle atteigne sa destination. Contrairement aux IDS, les IPS sont des outils aux fonctions « actives », qui en plus de détecter une intrusion, tentent de la bloquer.

Le principe de fonctionnement d’un IPS est analogue à celui d’un IDS, ajoutant à cela l’analyse des contextes de connexion, l’automatisation d'analyse des logs et la coupure des connexions suspectes. Contrairement aux IDS classiques, aucune signature n'est utilisée pour détecter les attaques. Avant toute action, une décision en temps réel est exécutée (i.e., l'activité est comparée aux règles existantes). Si l'action est conforme à l'ensemble de règles, la permission de l’exécuter sera accordée et l'action sera exécutée. Si l'action est illégale, une alarme est générée. Dans la plupart des cas, les autres détecteurs du réseau (ou une console centrale connectées à l’IPS) en seront aussi informés dans le but d’empêcher les autres ordinateurs d'ouvrir ou d'exécuter des fichiers spécifiques.

# 2.6 Critères de choix d'un IDS

Les systèmes de détection d'intrusion sont devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle. Ils s'intègrent donc toujours dans un contexte et dans une architecture imposante des contraintes très diverses. Certains critères imposant le choix d'un IDS peuvent être dégagés :

* **Fiabilité** : Les alertes générées doivent être justifiées et aucune intrusion ne doit pouvoir lui échapper.
* **Réactivité** : Un IDS doit être capable de détecter les nouveaux types d'attaques le plus rapidement possible ; pour cela il doit rester constamment à jour. Des capacités de mise à jour automatique sont indispensables.
* **Facilité** **de mise en œuvre et adaptabilité** : Un IDS doit être facile à mettre en œuvre, surtout s'adapter au contexte dans lequel il doit opérer. Il est inutile d'avoir un IDS émettant des alertes en moins de 10 secondes si les ressources nécessaires à une réaction ne sont pas disponibles pour agir dans les mêmes contraintes de temps.
* **Performance** : la mise en place d'un IDS ne doit en aucun cas affecter les performances des systèmes surveillés. De plus, il faut toujours avoir la certitude que l’IDS a la capacité de traiter toute l'information à sa disposition (par exemple un IDS réseau doit être capable de traiter l'ensemble du flux pouvant se présenter à un instant donné sans jamais supprimer de paquets) car dans le cas contraire il devient trivial de masquer les attaques en augmentant la quantité d'information.

# 2.7. Sécurité réseau

La sécurité informatique est l’ensemble des moyens mis en œuvre afin de réduire la vulnérabilité d’un système contre les menaces accidentelles ou intentionnelles. Il convient d’identifier les exigences fondamentales en sécurité informatique.[[26]](#footnote-26)

Elles caractérisent ce à quoi s’attendent les utilisateurs de systèmes informatiques en regard de la sécurité. La sécurité d'un réseau informatique peut être définie sur trois niveaux :

* Niveau physique
* Niveau logique
* Niveau réseau

## 2.7.1. Sécurité au niveau physique

La sécurité au niveau physique concerne essentiellement l'accès aux bâtiments et aux équipements qu'ils abritent. À ce niveau l'accès même aux bâtiments doit être défini pour savoir qui y a accès ou non. Car un pirate (ou une personne mal intentionnée) peut avoir besoin d'accéder aux locaux du réseau avant de préparer son attaque depuis l'extérieur.

## 2.7.2. Sécurité au niveau logique

Au niveau logique, la notion de sécurité est plus sensible, les utilisateurs sont en contact direct ou indirect avec le système (données, logiciels, applications, services...).

L'accès au système par tout le monde à un instant voulu peut engendrer des risques qui pourraient exposer ce dernier. Les utilisateurs doivent être « casés » dans des groupes dont chacun a un niveau d'accès bien défini par l'administrateur réseau, suivant les besoins du groupe. Si tout le monde a les mains libres pour accéder au système, une maladresse (erreur) pourrait provoquer des effets très graves et exposer le système à des attaques externes (si le réseau est interconnecté avec l'extérieur par exemple).

# 2.8. Définition d'une intrusion réseau

Une intrusion réseau consiste à se connecter sur un ordinateur ou un réseau distant sans en avoir la permission. Donc c’est la pénétration frauduleuse d’un système. L’intrusion réseau est une des conséquences potentielles de l’existence de failles dans la sécurité d'un réseau informatique. Le but (ou encore actions consécutives) d’une intrusion dépend des motivations du pirate (l'intrus) :

* Accès aux documents confidentiels
* Vols ou destructions de données
* Espionnage : introduction dans le réseau de programmes capables de surveiller les Activités internes du réseau au profit du pirate. Ce qui est très dangereux, car cela peut permettre au pirate d'avoir un control total sur le système dénis de service : il constitue à empêcher aux utilisateurs légitimes du réseau D’exploiter au maximum les ressources de leurs machines par l'envoi de programmes perturbateurs (bugs) ou des pings continus (Ping de la mort).

# 2.9. Quelques techniques d'intrusion[[27]](#footnote-27)

Une intrusion est consécutive à une attaque externe réussie, car avant de pénétrer dans le réseau cible il faut déployer certaines stratégies. On peut répartir les attaques en deux catégories :

## 1. Attaques Passives

Une Attaque passive constitue à écouter le trafic du réseau (ou de la machine) cible, donc l'interface de la machine attaquante (du pirate) est en mode écoute. L'objectif est de découvrir et capturer des trames du réseau cible pour y rechercher des informations particulières : clés de cryptages, login et mots de passe, données. Elle se réalise grâce à des outils tels que : les sniffer, les scanners.

## 2. Attaques actives

Contrairement à une attaque passive, ici l'attaquant n'est plus en mode écoute.Elles consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau, à interroger le réseau (ou la machine) cible, contourner le dispositif de sécurité existant … par diverses méthodes :

* **Deny of service (Dos : Déni de Service) :**
* Une attaque de type Dos consiste à rendre une machine (ou un réseau) « hors service » en lui envoyant des « programmes perturbateurs »
* **Les Virus :** Selon la définition donnée par Fred Cohen, le premier chercheur qui a décrit le phénomène dans une thèse publiée en 1985, un virus est un programme informatique capable d'infecter d'autres programmes en les modifiant afin d'y intégrer une copie de lui-même qui pourra avoir légèrement évolué. A la manière de son frère biologique, il se reproduit rapidement à l'intérieur de l'environnement infecté sans que le porteur (l'utilisateur) en ait conscience.

# 2.10 Conclusion

Dans ce chapitre, il était question de parler sur le système de détection d’intrusion d’où nous avions parlé des outils de l’IDS, IPS et autres… Dans le chapitre suivant, nous présenterons les données de l’entreprise et passer à la proposition de la nouvelle solution.

# CHAPITRE 3 : IMPLEMENTATION DU NOUVEAU SYSTEME

# 3.0. INTRODUCTION

Dans ce chapitre, il sera question de réaliser notre travail qui consiste à mettre en place un réseau local en utilisant le pare-feu Open Source qui est notre solution.

Avant tout, la conception précèdera cette réalisation où nous allons faire le choix de la norme, le plan d’adressage ; le choix des matériels etc.

# 3. 1 CONCEPTION DU NOUVEAU SYSTEME

# 3.1.1 Choix de la norme du réseau local

Comme il s’agit du Réseau Local ave le pare-feu OPEN Source, nous faisons appel à la norme 802.3, qui va nous aider avec le type de topologie qui sera en étoile comme physique et en logique la topologie Ethernet et le câble à paire torsadée.

# 3.1.2 Choix des matériels

|  |  |  |  |
| --- | --- | --- | --- |
| **N°** | **Matériels** | **Qté** | **Description** |
| 01 | Ordinateur | 7 | HP ; CPU i5 ; HDD 1TO ; RAM 8G |
| 02 | Routeur PfSense | 1 | 5 ports dont 4 Ethernet et 1 internet |
| 03 | Onduleur ASI | 2 | MERCURY MP 911010KVA |
| 04 | Câble à paire torsadée | 1carton | Cat 6 UTP |
| 05 | Prises murales Schneider | 18 | RJ45 encastrable |
| 06 | Connecteur RJ45 | 2 paquets | Le connecteur Blindé |
| 07 | Goulottes | 150mm | Manchester Noir |
| 08 | Extincteur | 1 pièce |  |
| 09 | Câble Tie | 2 paquet |  |
| 10 | Imprimante | 3 |  |

Tableau 3. 1 Choix des matériels

# 3.1.3 Choix des logiciels

|  |  |
| --- | --- |
| **Logiciels** | **Caractéristique** |
| Système d’Exploitation | Windows 11 Edition 2022 |
| Antivirus | Symantech |
| Package Office | Microsoft Office 2016 |
| Pfsense Open Source | Edition 3.16 |

Tableau 3. 2 Choix des logiciels

# 

# 3.1.4 Plan d’Adressage

|  |  |  |
| --- | --- | --- |
| Adresse du Réseau | 192.168.10.0 | 255.255.255.0 |
| Adresse de la Passerelle | 192.168.10.1 | 255.255.255.0 |
| Adresse du Début | 192.168.10.2 | 255.255.255.0 |
| Adresse de la Fin | 192.168.10.254 | 255.255.255.0 |
| Adresse de Broadcast | 192.168.10.255 | 255.255.255.0 |

Tableau 3. 3 Plan d'adressage

# 3.1.5 Maquette du réseau (Nouveau Système)

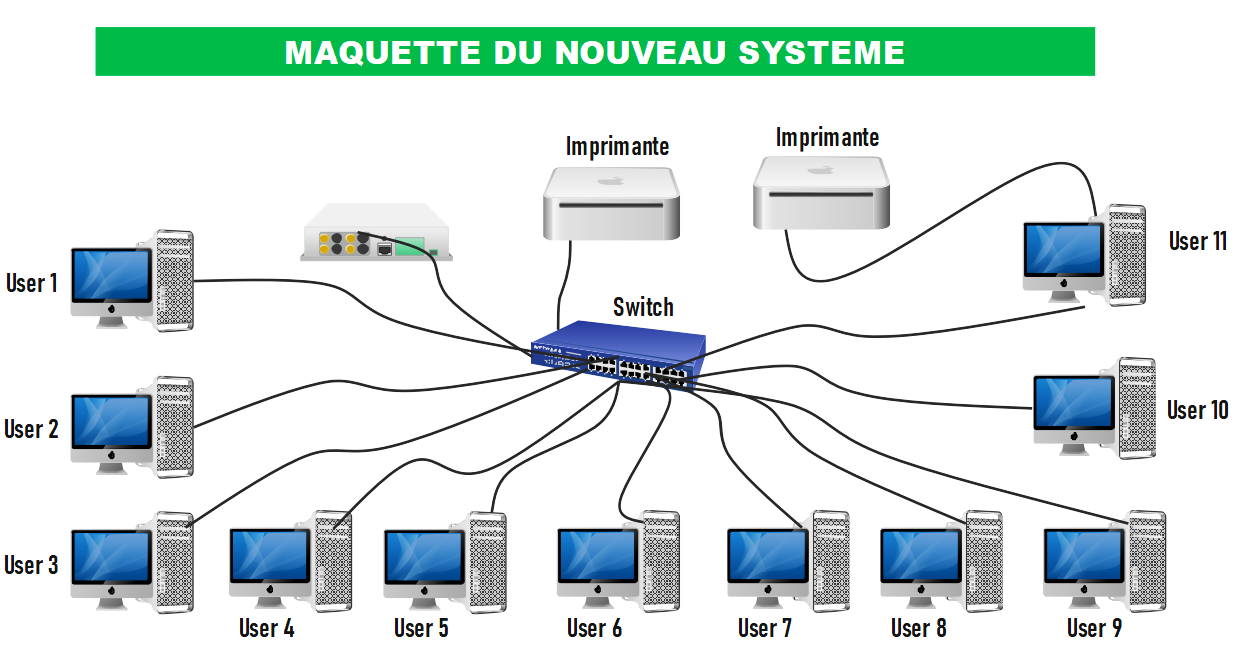
****

Figure 3. 1 Maquette du nouveau système

# 3.2 Installation et configuration du nouveau Système

**3.2 choix de logiciel**

Nous avons Choisir pfsense et Snort parce qu’ils offrent une solution robuste et open source pour la sécurité réseau. Pfsense, en tant que pare-feu, isole et filtre le trafic, tandis que Snort surveille le réseau pour détecter et bloquer les activités malveillantes, créant ainsi une défense en profondeur.

PfSense et Snort forment une combinaison puissante pour la sécurité réseau, offrant une solution open source, flexible et personnalisable pour la détection et la prévention des intrusions.

NB : notre système elle est logique mais lors de l’intrusion il va générer une alerte physique soit par ordinateur serveur ou encore un téléphone par mail de l’administrateur.

**1 Fonctionnalités de pare-feu :**

* **Pare-feu avec état :** PfSense examine chaque paquet réseau et mémorise les informations de connexion pour autoriser automatiquement le trafic de réponse, ce qui assure une sécurité accrue.
* **Règles de pare-feu :** Permet de définir des règles personnalisées pour contrôler le trafic entrant et sortant.
* **Détection d’intrusion :** Intègre des systèmes de détection d'intrusion (IDS/IPS) pour identifier et bloquer les activités suspectes.
* **Filtrage d’URL :** Permet de bloquer l'accès à des sites web indésirables.
* **NAT :** Prend en charge le NAT (Network Address Translation) pour masquer les adresses IP internes et traduire les adresses IP publiques.
* **Équilibrage de charge :** Répartit le trafic réseau entre plusieurs connexions ou serveurs pour améliorer les performances et la disponibilité.

# 3.2.1 Installation du routeur pfSense

Nous allons démarrer l’option du Boot Pfsense :

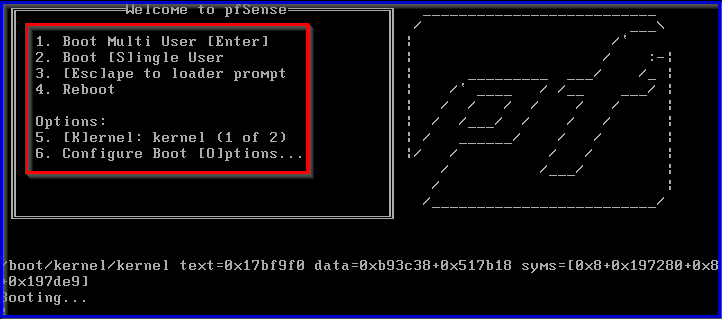


Figure 3.2 Démarrage de PfSense

Nous allons accepter le choix pour valider

Figure 3. 3 Acceptation de l’installation

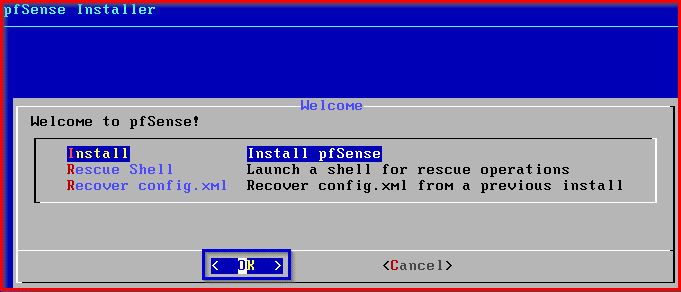
Nous allons opter **install Pfsense** pour commencer notre installation ensuite nous allons valider cette option.

Figure 3. 4 Installation facile

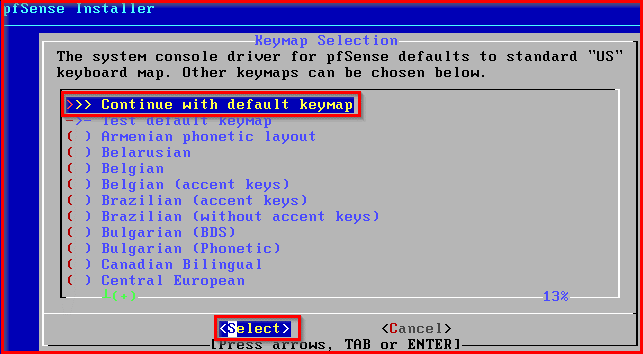
Nous allons laisser l’installation du noyau par défaut ensuite nous allons le sélectionner pour avancer.

Figure 3. 5 Installation du noyau

Nous allons choisir UFS automatique

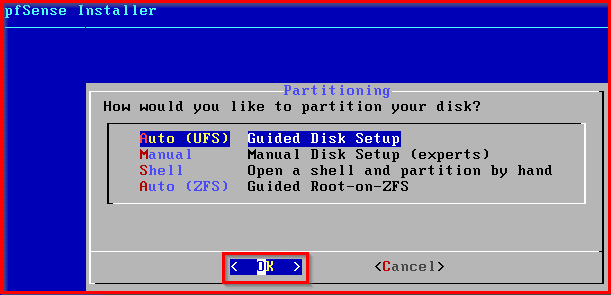


Figure 3. 6 Partitionnement UFS

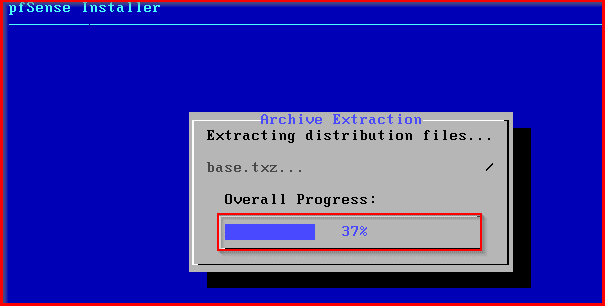
Nous allons patienter pendant l’installation du Routeur Pfsense

Figure 3. 7 Progression d’installation

Nous allons accepter le Reboot pour redémarrer l’image système du Pfsense.

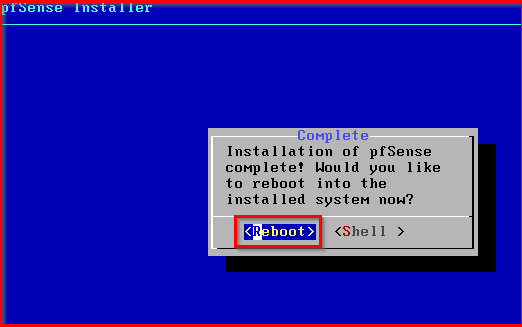


Figure 3. 8 Redémarrage du système

# 

# 3.2.2 Configuration des interfaces réseau

Dans notre cas « le0 » correspond à l’interface WAN par contre le1 correspond au LAN qu’il faudra configurer. Nous allons entrer **«**2 **»** pour lancer la configuration IP d'une interface.

Les deux adresses là sont venues d’une manière automatique et nous allons dans l’obligation de le modifier



Figure 3. 9 Configuration des interfaces

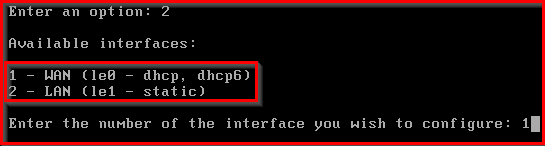
Puis choisir le numéro de l'interface à configurer ;

Figure 3. 10 Choix de l’interface à configurer

Répondre aux questions pour configurer l’interface : adresse IP via DHCP ou adresse IP statique, nombre de bits de sous-réseau etc. La configuration IP d'une interface se termine par une question demandant si nous souhaitons autoriser l'accès en http à l'interface web via cette interface.

Comme vous remarquer, la configuration de des interfaces réseaux de LAN1 sont terminée. Nous allons continuer de la même façon pour les interfaces réseaux de LAN2.

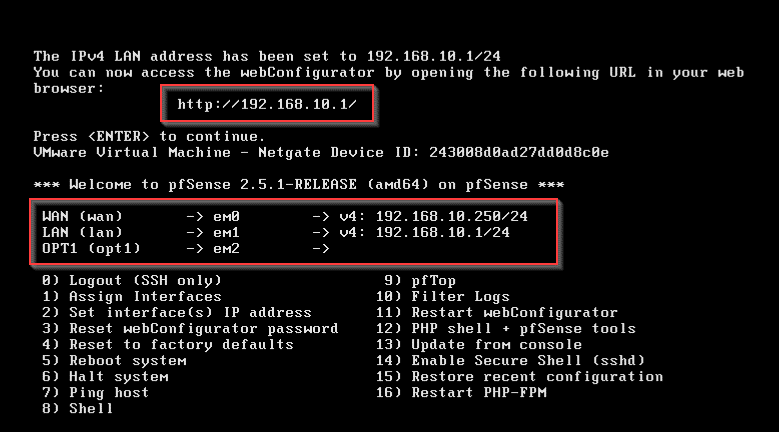


Figure 3. 11 Propriété des interfaces

# 3.2.2.1 Configuration graphique du routeur PFSENS

Nous présenterons la configuration pour notre Routeur qui est PFSENSE.

Nous pouvons accéder à l’interface Web de pfSense à partir d’une machine se trouvant sur le réseau natif LAN du pfSense (par exemple un poste Windows 10 ayant l’adresse IP 192.168.10.1/24 pour le réseau LAN1.

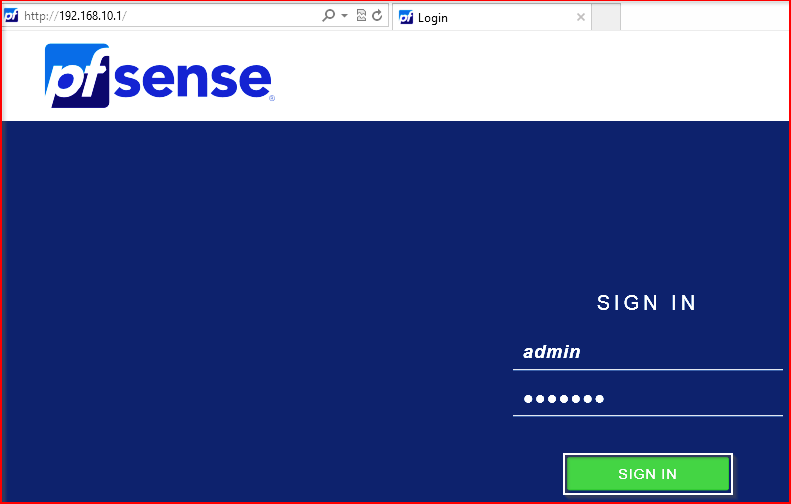


Figure 3. 12 Accès en mode interface graphique du LAN1

Nous mettre le nom du routeur, vu notre cas, nous allons mettre PfSense.

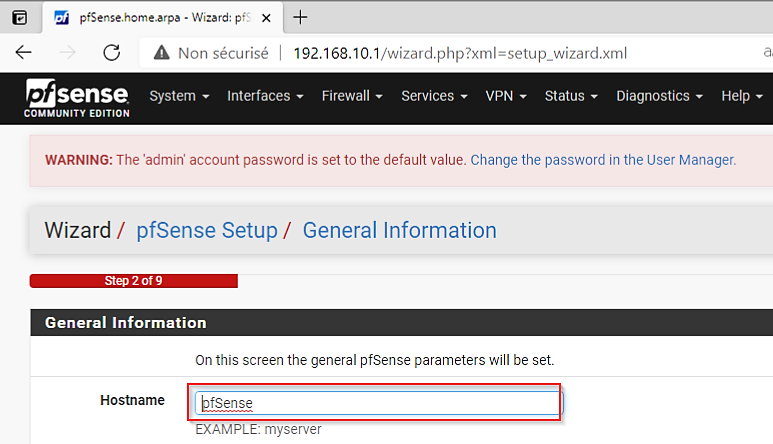


Figure 3. 13 Modification du Nom

A ce niveau, nous allons bloquer tous les trafics des entrées et sorties.

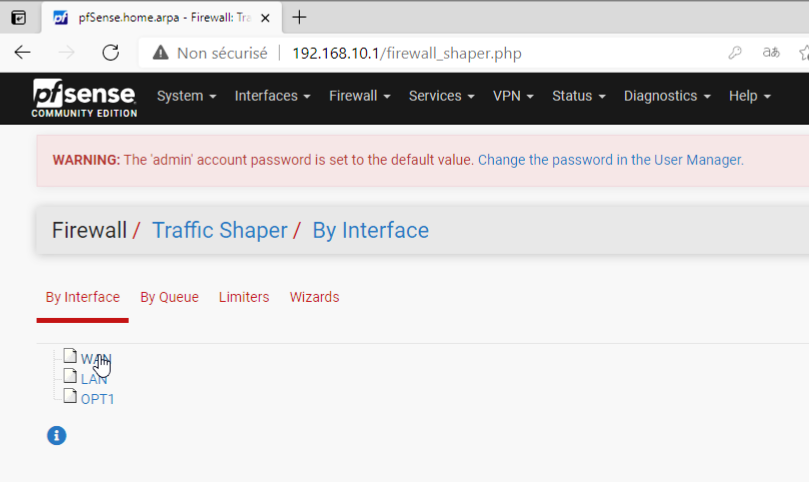


Figure 3. 14 Sélection des Trafics

Assurer que vous avez bien écrit User Name et password qui est ‘Admin et pfSense comme password. Ensuite cliquer sur ‘Sign in’’. Dès la saisi du nom d’utilisateur et du mot de passe, la page d’accueil de PfSense s’affiche.

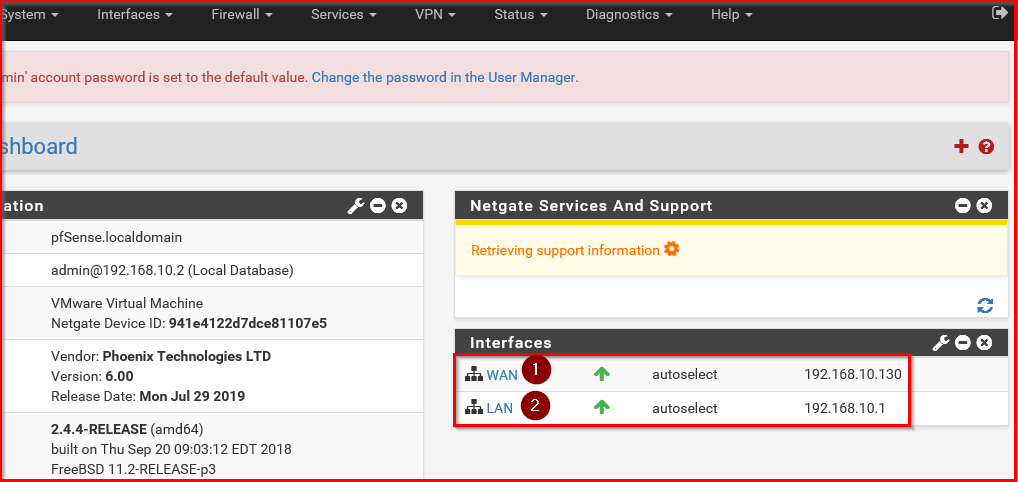


Figure 3. 15 Sélection des interfaces

Cliquer sur le bouton ‘+Add P1. Les éléments à configurer sont les suivants :

* **Key Exchange version :** permet de choisir la version du protocole IKE (Internet Key Exchange). Nous choisissons "IKEv2". Si l'autre pair ne support par l'IKEv2 ou si un doute subsiste, il est recommandé de choisir "Auto".
* **Internet Protocol :** IPv4 ou IPv6 ; dans notre cas, nous choisissons IPv4
* **Remote Gateway :** l'adresse IP publique du site distant. Dans notre cas : 192.168.10.250
* **Authentication Method :** la méthode d'authentification des deux pairs. Deux choix sont possibles : authentification par clé pré-partagée (PSK) ou par certificat (RSA). Le plus simple et le plus courant est de choisir "Mutual PSK" ; ce que nous faisons.
* **My identifier :** notre identifiant unique. Par défaut, il s'agit de l'adresse IP publique. Nous laissons donc la valeur "My IP adresse".
* **Encryptions Algorithme** : l'algorithme de chiffrement. Si les deux parties supportent l'AES-GCM, nous recommandons l'utilisation d'AES256-GCM ou d'AES128GCM ; ce qui permettra de bénéficier d'un bon niveau de chiffrement et sera compatible avec l'accélération.

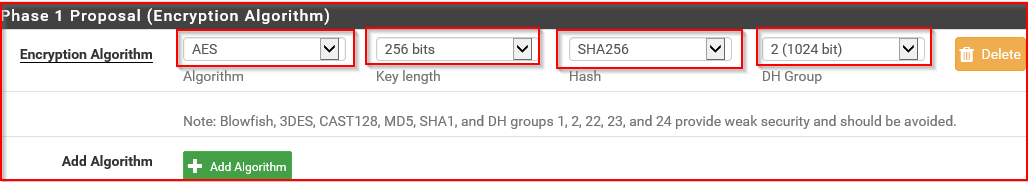


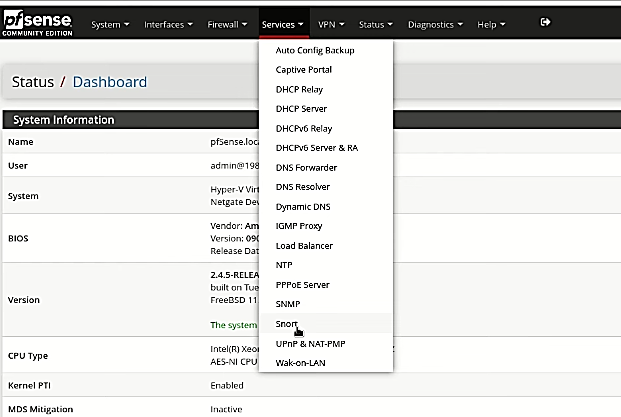
Figure 3. 16 L’algorithme de cryptage

# A ce niveau, nous allons afficher les informations du système

# 

Figure 3. 17 Affichage des informations du système

# A ce niveau, nous allons accéder dans le Snort



# Figure 3. 18 Accès dans le Snort

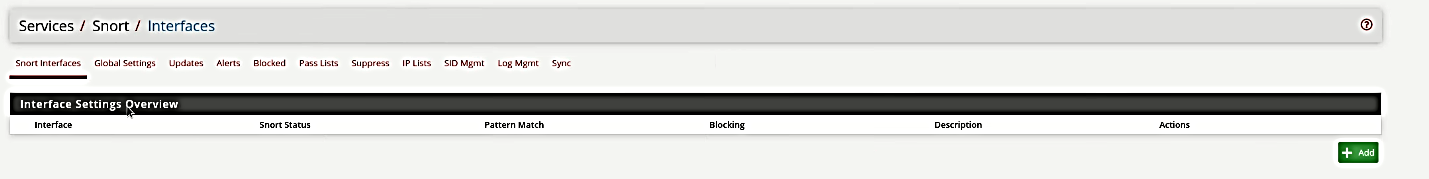
A ce niveau, il y’a aucune interface qui est créer.

Figure 3. 19 Identification des ports Snort

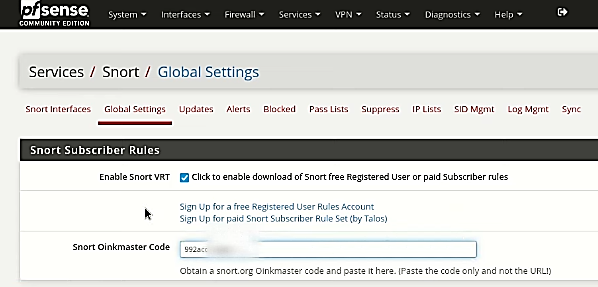
Nous allons activer le **Snort VRT**

Figure 3. 20 Activation du Snort

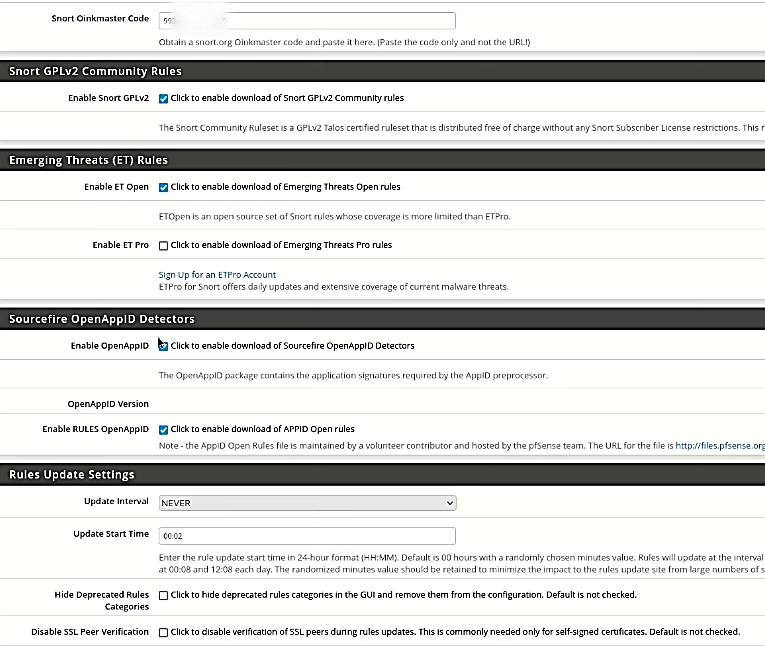
Nous allons activer toutes les fonctionnalités de Snort pour permettre

Figure 3. 21 Ajout de fonctionnalité

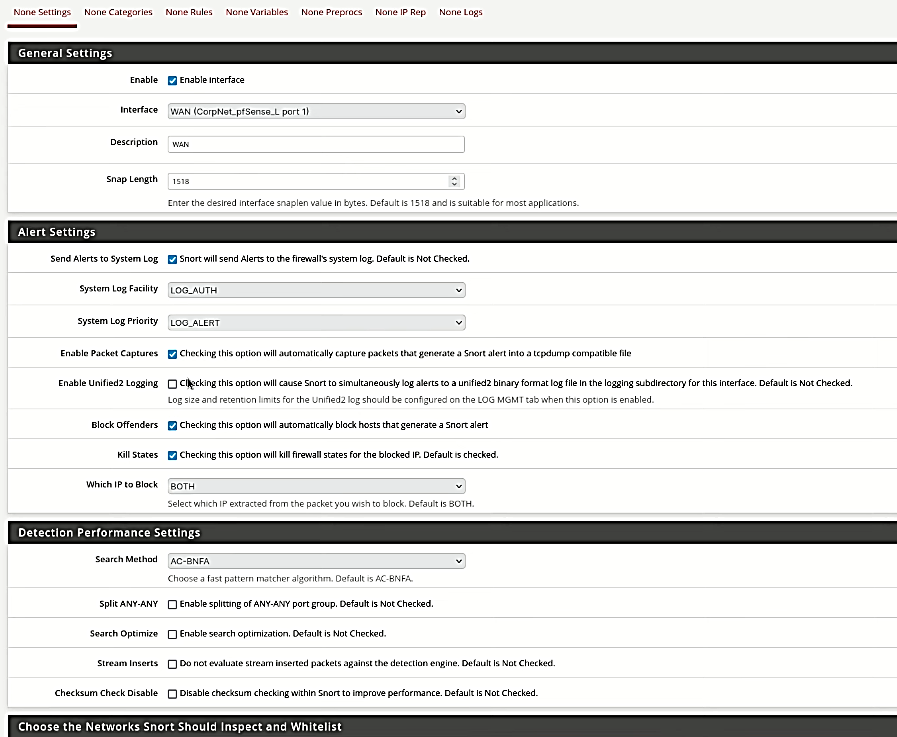
Nous allons activer les alertes des paramètres d’authentification

Figure 3. 22 Activation des paramètres

Après avoir activer, nous allons sauvegarder le paramètre.

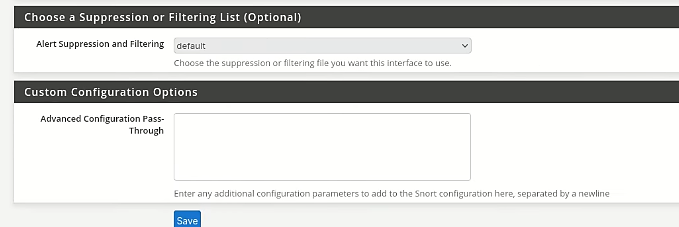


Figure 3. 23 Enregistrement

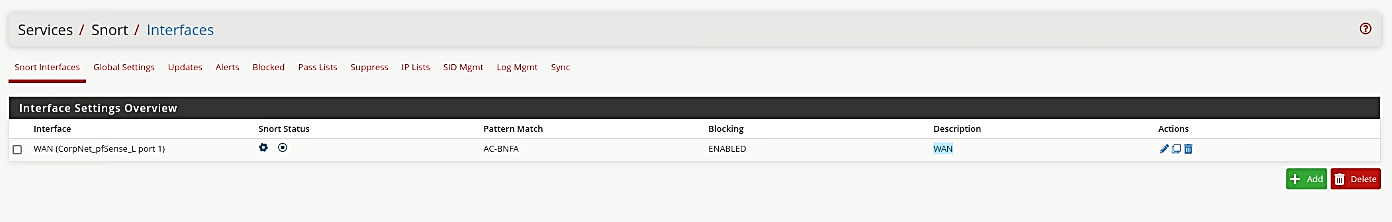
Interface activer de l’interface Overview

Figure 3. 24 Identification de l'interface Overview

# 3.3 ASSIGNATION D’ADRESSE IP

Nous allons se diriger vers la carte réseau de notre machine.

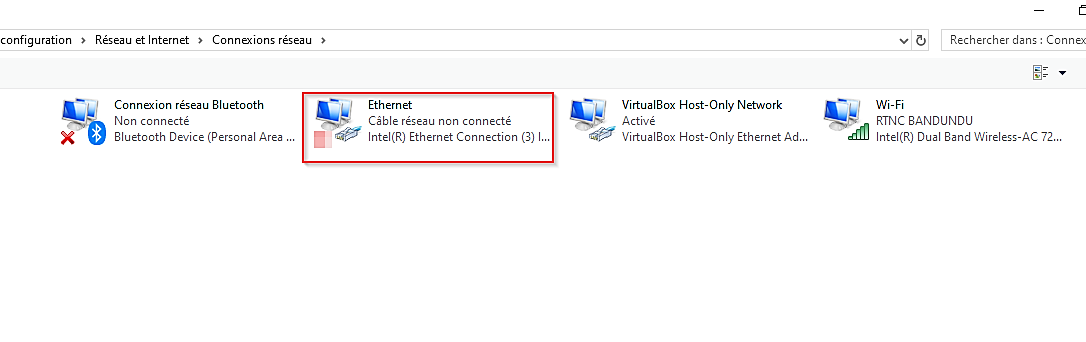


Figure 3. 25 Paramètre d'adresse IP

# Nous allons cliquer sur Protocole Internet Version 4 (TCP/IPv4)

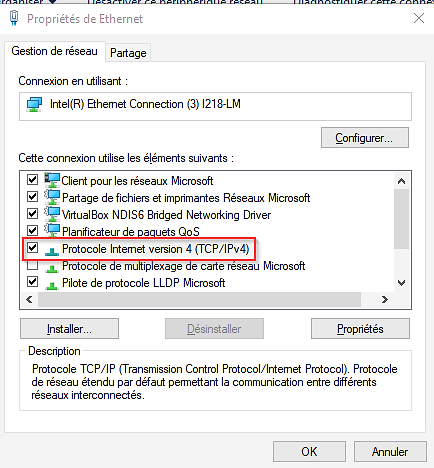


Figure 3.26 Paramètre de la Carte

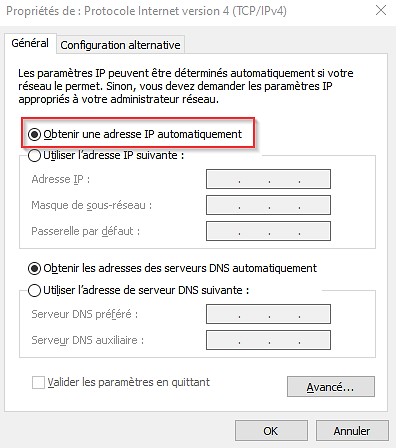
Vu que nous avons activé le paramètre DHCP d’une manière automatique dans notre réseau, nous allons cocher **Obtenir une Adresse IP automatique.**

Figure 3. 27 Sélection du mode Automatique

# 3.4 VERIFICATION D’ADRESSE IP

Nous allons faire le clic droit dans la carte Réseau et ensuite cliquer sur Statut.

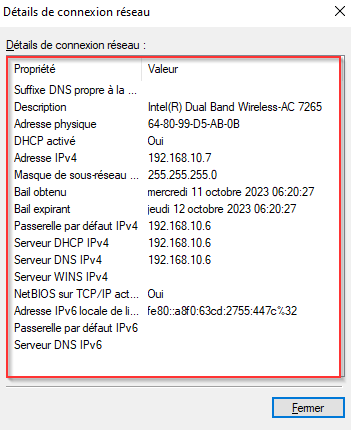


Figure 3. 28 Vérification d'Adresse IP

# 

# 3.5 TEST DE CONNECTIVITE

Pour Tester la connectivité, nous irons dans l’invite de commande. Nous allons faire appel au Packet Internet Grouper (Ping en sigle) suivie de l’adresse du destinataire.

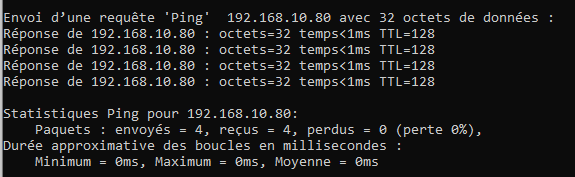
****

Figure 3. 29 Test de connectivité

**CONCLUSION**

# 3.6 Estimation du cout

C’est un tableau qui décrit les différents outils à acheter, le nombre nécessaire, l’imprévu, la quantité totale, le prix unitaire, le prix total.

|  |  |  |  |
| --- | --- | --- | --- |
| **Matériels** | **Qté** | P.U | P.T |
| Ordinateur | 7 Pièces | 500$ | 3 500$ |
| Routeur PfSense | 1 Pièce | 200$ | 200$ |
| Onduleur ASI | 2 Pièces | 500$ | 1000$ |
| Câble à paire torsadée | 2 cartons | 85$ | 170$ |
| Prises murales Schneider | 18 | 4$ | 72$ |
| Connecteur RJ45 | 2 paquets | 15$ | 30$ |
| Goulottes | 150mm | 0.5$ | 75$ |
| Extincteur | 1 pièce | 200$ | 200$ |
| Câble Tie | 2 paquet | 5$ | 10$ |
| Imprimante | 3 Pièces | 250$ | 750$ |
| TOTAL | | | **6 007$** |
| IMPREVU 10% | | | **600,7$** |
| MAIN D’ŒUVRE 30% | | | **1 802,1$** |
| TOTAL GENERAL | | | **8 409,8$** |

Tableau 3. 4 Estimation du coût

**3.6 CONCLUSION**

Dans ce chapitre nous avons effectué des configurations tant matérielles que logicielles qui nous ont permis de mettre en place le nouveau système.

**CONCLUSION GENERALE**

Le présent travail a porté sur le déploiement d'un système de détection et de prévention d'intrusion (IDS/IPS) dédié aux réseaux de télévision, avec un cas d'étude spécifique sur la Radio-Télévision Nationale Congolaise (RTNC).

Face à l'augmentation constante des cybermenaces et à la criticité des infrastructures de diffusion, il est devenu impératif de renforcer la sécurité des réseaux pour garantir la continuité des services et la protection des informations sensibles.

Nous avons mis en évidence la problématique liée à la vulnérabilité des réseaux de télévision de la RTNC face aux cyberattaques, ainsi que l'intérêt majeur de l'implémentation d'une solution IDS/IPS.

Les objectifs fixés pour cette étude comprenaient la protection des informations sensibles, la sauvegarde des équipements et des réseaux, et l'assurance du respect des normes de sécurité. La méthodologie adoptée a permis d'analyser en profondeur les besoins spécifiques de la RTNC, de concevoir une architecture IDS/IPS adaptée et de détailler les étapes de son déploiement. Les configurations matérielles et logicielles ont été présentées, démontrant la faisabilité technique de la solution proposée. L'estimation des coûts a également été fournie, offrant une perspective réaliste sur l'investissement nécessaire.

En somme, ce travail a démontré qu'un système IDS/IPS est une composante essentielle pour la résilience des réseaux de télévision modernes. Son déploiement au sein de la RTNC permettra non seulement de détecter et de prévenir les intrusions, mais aussi de renforcer  
la confiance du public dans la qualité et la sécurité des contenus diffusés. Au-delà de la protection immédiate, cette initiative ouvre la voie à une culture de cybersécurité renforcée au sein de l'institution, essentielle pour faire face aux défis numériques futurs et assurer une diffusion fiable et sécurisée de l'information.

**BIBLIOGRAPHIE**

**ŒUVRES**

* SHOMBA, K., « Méthodologie de la Recherche Scientifique », [Ed. MES], KIN-RDC, 1995, Pp26.
* LAUBET, B., **initiation aux méthodes de recherche en sciences sociales**, éd. Le Harmattan, Paris, 2000, P. 120
* ACISSI., **Sécurité informatique - Ethical Hacking,** Paris: ENI, 2009
* Andrew S. TANENBAUM, “Computer Networks, 3rd Edition” (traduction française ) Practice Hall, avril 1996 Consulté le 02/03/2025
* JEAN-LUC, MONTAGNER, Pratique des réseaux d’entreprise : du câblage l’administration, du réseau local aux réseaux Télécom, Ed. Eyrolles, Paris, 1997
* Dr Nadjia Khatir, Dr Abdelkader Belhadri « Notes de cours sur les réseaux informatiques » Ecole Supérieure en Génie Electrique et Energétique d’Oran, Année Académique 2020-2021, p8
* N. Salmi, A. Abdeli. Réseaux et télétraitements. Pages Bleues, 2016 p20
* GOUPILLE PIERRE A., **Réseau et télécoms**, 3eme édiction, Dunod, 2007, Paris, page.11
* Joseph S. La cybersécurité pour les nuls, First éditions, ENI, Paris, 2020 consulté le 03/03/ 2025
* Jacques p. **Systèmes et réseaux, Réseaux Intranet et Internet**. Paris, Ellipses 2012

**NOTE DES COURS**

* MBIKAYI Jeampy, Note de cours d’administration Réseau. Kinshasa: Mediaspaul, 2013
* MAKANGU Jacob, « **notes de cours réseau 2** » G3 réseau informatique, ISC-Bandundu, année académique 2021 – 2022, p19

**WEBOGRAPHIE**

* Ionos, <<Principaux Réseaux informatiques>> in
* [www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-aconnaitre](http://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre)  consulté le 01/03/2025
* www.memoire-online.fr.www.mise\_en\_d’un-multi\_platform\_network\_au\_seind’une\_entité\_decentralisée/, Consulté le 02/03/2025
* [www.epprendre\_types\_reseaux\_informatique\_mp.fr/%architecture\_reseau\_informatique/](http://www.epprendre_types_reseaux_informatique_mp.fr/%25architecture_reseau_informatique/) , consulté le 05/03/2025
* [www.memoireoneline.com/mise-en-place-d’une-politique-extranet,](http://www.memoireoneline.com/mise-en-place-d’une-politique-extranet) consulté le 6/03/2025
* <https://www.africmemoire.com/part.4-chapitre-iii-presentation-de-la-radio-television-nationale-congolaise-2062.html,consultez> le 17/07/2025 18H50
* [http://web.mit.edu/rhel-doc/OldFiles/4/RH-DOCS/rhel-sg-fr-4/chdetection.html](http://web.mit.edu/rhel-doc/OldFiles/4/RH-DOCS/rhel-sg-fr-4/ch-detection.html) consulté le 20 Avril 2025 à 10H00
* <http://securinet.free.fr/intrusions.html>consulté le 12 Avril 2025 à 15H
* <http://www.tux-planet.fr/utilisation-de-nmap-et-outil-de-detection-des-scans-de-ports/> consulté le 12 Avril 2025 à 15H
* <http://www.linux-france.org/prj/edu/archinet/systeme/ch05s03.html>Consulté le 20 Avril 2025
* <http://www.sestream.com/docCom/Snort.pdf>consulté le 21 Avril 2025
* <http://www.ossir.org/resist/supports/cr/200205/ids-logs.pdf>consulté le 20 Avril 2025
* [http://www.labo-linux.org/articles-fr/surveillance-reseau-avec-snort/installation-et-configurationdesnort](http://www.labo-linux.org/articles-fr/surveillance-reseau-avec-snort/installation-et-configurationde-snort) consulté le 25 Avril 2025
* shttp://www.system-linux.eu/index.php?post/2009/02/23/Compilation-Installation-etConfigurationde-Snort consulté le 28 avril 2025

**TABLE DES MATIERES**

[EPIGRAPHE i](#_Toc206639106)

[DEDICACE ii](#_Toc206639107)

[NDONA TABUKU PEDO ii](#_Toc206639108)

[AVANT-PROPOS iii](#_Toc206639109)

[NDONA TABUKU PEDO iii](#_Toc206639110)

[LISTE DES TABLEAUX iv](#_Toc206639111)

[LISTE DES FIGURES v](#_Toc206639112)

[LISTE DES ABREVEATIONS vi](#_Toc206639113)

[INTRODUCTION GENERALE 1](#_Toc206639114)

[0.1 Présentation du Sujet 1](#_Toc206639115)

[0.2 Choix et intérêt du sujet 1](#_Toc206639116)

[0.2.1 Choix du sujet 1](#_Toc206639117)

[0.2.2 Intérêt du sujet 2](#_Toc206639118)

[0.4 Hypothèse 3](#_Toc206639121)

[0.5 Objectifs 4](#_Toc206639122)

[0.6 Méthodes et techniques 4](#_Toc206639123)

[0.6.1 Méthodes 4](#_Toc206639124)

[0.6.2 Techniques utilisées 5](#_Toc206639125)

[0.7. Délimitation du sujet 5](#_Toc206639126)

[0.7.1 Spatiale 5](#_Toc206639127)

[0.8 Subdivision du Travail 5](#_Toc206639128)

[CHAPITRE I : NOTIONS FONDAMENTALES SUR LES RESEAUX INFORMATIQUES 1.1 Introduction 7](#_Toc206639129)

[1.2 Définition 7](#_Toc206639130)

[1.3 Classification des réseaux 7](#_Toc206639131)

[1.3.3. Selon le débit 9](#_Toc206639132)

[1.3.4.1 Réseau privé 9](#_Toc206639133)

[1.3.4.2. Réseau public 10](#_Toc206639137)

[1.3.5. Selon l’architecture de communication 10](#_Toc206639138)

[1. Avantages de l’architecture client/serveur 11](#_Toc206639143)

[2. Inconvénients de l’architecture client/serveur 12](#_Toc206639144)

[1.4 Equipement d’interconnexion réseau 12](#_Toc206639145)

[1.4.1. Switch 12](#_Toc206639146)

[1.4.2. Routeur 13](#_Toc206639147)

[1.4.3 Hub 13](#_Toc206639148)

[1.4.4. Pont (bridge) 13](#_Toc206639149)

[1.4.5 Point d’accès 13](#_Toc206639150)

[1.5 Modèles 14](#_Toc206639151)

[1.5.1 Modèle de référence OSI (Open System Interconnection) 14](#_Toc206639152)

[B. Couches hautes 15](#_Toc206639154)

[1.5.2 Modèle TCP/IP 16](#_Toc206639155)

[1.6. Topologie des réseaux 17](#_Toc206639156)

[1.6.1 Topologie physique 17](#_Toc206639157)

[1.6.1.1. Topologie en bus 17](#_Toc206639158)

[1.7.1 Types de supports de transmission 20](#_Toc206639159)

[1.7.1.1 Supports filaires 20](#_Toc206639160)

[1.7.2 Supports non filaires 21](#_Toc206639161)

[CHAPITRE 2 : ETUDE DES SYSTEMES DE DETECTION INTRUSION (IDS) 27](#_Toc206639163)

[2.1 Introduction 27](#_Toc206639164)

[2.3 Définition des systèmes de détection 35](#_Toc206639165)

[2.3. Définition d’un système d’intrusion 36](#_Toc206639166)

[2.3.1. Différents types d'IDS (classification) 36](#_Toc206639167)

[1. Systèmes de prévention d'intrusion (IPS) 36](#_Toc206639168)

[2. Systèmes de détection d'intrusion réseaux (NIDS) 36](#_Toc206639169)

[2.3.2 Systèmes de détection d'intrusion de type hôte (HIDS) 37](#_Toc206639170)

[2.3.3 Systèmes de détection d'intrusion hybrides 38](#_Toc206639171)

[2.4 Mode de fonctionnement 38](#_Toc206639172)

[2.4.1 Modes de détection 39](#_Toc206639173)

[2.4.2 Détection d'anomalies 39](#_Toc206639174)

[2.4.3 Reco nnaissance de signatures 39](#_Toc206639175)

[2.6 Critères de choix d'un IDS 40](#_Toc206639176)

[2.7. Sécurité réseau 41](#_Toc206639177)

[2.7.1. Sécurité au niveau physique 41](#_Toc206639178)

[2.7.2. Sécurité au niveau logique 42](#_Toc206639179)

[2.8. Définition d'une intrusion réseau 42](#_Toc206639180)

[2.9. Quelques techniques d'intrusion 43](#_Toc206639181)

[1. Attaques Passives 43](#_Toc206639182)

[2. Attaques actives 43](#_Toc206639183)

[2.10 Conclusion 43](#_Toc206639184)

[CHAPITRE 3 : IMPLEMENTATION DU NOUVEAU SYSTEME 44](#_Toc206639185)

[3.0. INTRODUCTION 44](#_Toc206639186)

[3. 1 CONCEPTION DU NOUVEAU SYSTEME 44](#_Toc206639187)

[3.1.1 Choix de la norme du réseau local 44](#_Toc206639188)

[3.1.2 Choix des matériels 44](#_Toc206639189)

[3.1.3 Choix des logiciels 44](#_Toc206639190)

[3.1.4 Plan d’Adressage 45](#_Toc206639191)

[3.1.5 Maquette du réseau (Nouveau Système) 45](#_Toc206639192)

[3.2 Installation et configuration du nouveau Système 45](#_Toc206639193)

[3.2.1 Installation du routeur pfSense 46](#_Toc206639194)

[3.2.2 Configuration des interfaces réseau 48](#_Toc206639195)

[3.2.2.1 Configuration graphique du routeur PFSENS 50](#_Toc206639196)

[3.3 ASSIGNATION D’ADRESSE IP 55](#_Toc206639219)

[Nous allons cliquer sur Protocole Internet Version 4 (TCP/IPv4) 55](#_Toc206639220)

[3.4 VERIFICATION D’ADRESSE IP 55](#_Toc206639221)

[3.5 TEST DE CONNECTIVITE 56](#_Toc206639222)

[3.6 Estimation du cout 56](#_Toc206639223)

1. SHOMBA, K., « Méthodologie de la Recherche Scientifique », [Ed. MES], KIN-RDC, 1995, Pp26. [↑](#footnote-ref-1)
2. LAUBET, B., **initiation aux méthodes de recherche en sciences sociales**, éd. Le Harmattan, Paris, 2000, P. 120 [↑](#footnote-ref-2)
3. ACISSI., **Sécurité informatique - Ethical Hacking,** Paris: ENI, 2009 [↑](#footnote-ref-3)
4. Ionos, <<Principaux Réseaux informatiques>> in

   [www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-aconnaitre](http://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre)  consulté le 01/03/2025 [↑](#footnote-ref-4)
5. Andrew S. TANENBAUM, “Computer Networks, 3rd Edition” (traduction française [↑](#footnote-ref-5)
6. ) Practice Hall, avril 1996 Consulté le 02/03/2025 [↑](#footnote-ref-6)
7. www.memoire-online.fr.www.mise\_en\_d’un-multi\_platform\_network\_au\_seind’une\_entité\_decentralisée/, Consulté le 02/03/2025 [↑](#footnote-ref-7)
8. [www.epprendre\_types\_reseaux\_informatique\_mp.fr/%architecture\_reseau\_informatique/](http://www.epprendre_types_reseaux_informatique_mp.fr/%25architecture_reseau_informatique/) , consulté le 05/03/2025 [↑](#footnote-ref-8)
9. JEAN-LUC, MONTAGNER, Pratique des réseaux d’entreprise : du câblage

   l’administration, du réseau local aux réseaux Télécom, Ed. Eyrolles, Paris, 1997 [↑](#footnote-ref-9)
10. [www.memoireoneline.com/mise-en-place-d’une-politique-extranet,](http://www.memoireoneline.com/mise-en-place-d’une-politique-extranet) consulté le 6/03/2025 [↑](#footnote-ref-10)
11. Dr Nadjia Khatir, Dr Abdelkader Belhadri « Notes de cours sur les réseaux informatiques » Ecole Supérieure en Génie Electrique et Energétique d’Oran, Année Académique 2020-2021, p8 [↑](#footnote-ref-11)
12. N. Salmi, A. Abdeli. Réseaux et télétraitements. Pages Bleues, 2016 p20 [↑](#footnote-ref-12)
13. GOUPILLE PIERRE A., **Réseau et télécoms**, 3eme édiction, Dunod, 2007, Paris, page.11 [↑](#footnote-ref-13)
14. Joseph S. La cybersécurité pour les nuls, First éditions, ENI, Paris, 2020 consulté le 03/03/ 2025 [↑](#footnote-ref-14)
15. MAKANGU Jacob, « **notes de cours réseau 2** » G3 réseau informatique, ISC-Bandundu, année académique 2021 – 2022, p19 [↑](#footnote-ref-15)
16. Jacques p. **Systèmes et réseaux, Réseaux Intranet et Internet**. Paris, Ellipses 2012 [↑](#footnote-ref-16)
17. MBIKAYI Jeampy, Note de cours d’administration Réseau. Kinshasa: Mediaspaul, 2013 [↑](#footnote-ref-17)
18. EYEME LUNDU E. « TFC, étude comparée sur les protocoles de transport » ISIPA 2014, page 70 [↑](#footnote-ref-18)
19. <https://www.africmemoire.com/part.4-chapitre-iii-presentation-de-la-radio-television-nationale-congolaise-2062.html,consultez> le 17/07/2025 18H50 [↑](#footnote-ref-19)
20. [http://web.mit.edu/rhel-doc/OldFiles/4/RH-DOCS/rhel-sg-fr-4/chdetection.html](http://web.mit.edu/rhel-doc/OldFiles/4/RH-DOCS/rhel-sg-fr-4/ch-detection.html) consulté le 20 Avril 2025 à 10H00 [↑](#footnote-ref-20)
21. <http://securinet.free.fr/intrusions.html>consulté le 12 Avril 2025 à 15H [↑](#footnote-ref-21)
22. <http://www.tux-planet.fr/utilisation-de-nmap-et-outil-de-detection-des-scans-de-ports/> consulté le 12 Avril 2025 à 15H [↑](#footnote-ref-22)
23. <http://www.linux-france.org/prj/edu/archinet/systeme/ch05s03.html>Consulté le 20 Avril 2025 [↑](#footnote-ref-23)
24. <http://www.sestream.com/docCom/Snort.pdf>consulté le 21 Avril 2025 [↑](#footnote-ref-24)
25. <http://www.ossir.org/resist/supports/cr/200205/ids-logs.pdf>consulté le 20 Avril 2025 [↑](#footnote-ref-25)
26. [http://www.labo-linux.org/articles-fr/surveillance-reseau-avec-snort/installation-et-configurationdesnort](http://www.labo-linux.org/articles-fr/surveillance-reseau-avec-snort/installation-et-configurationde-snort) consulté le 25 Avril 2025 [↑](#footnote-ref-26)
27. shttp://www.system-linux.eu/index.php?post/2009/02/23/Compilation-Installation-etConfigurationde-Snort consulté le 28 avril 2025 [↑](#footnote-ref-27)