Ministère de l'enseignement supérieur et de la recherche scientifique

Université Mouloud Mammeri Tizi-Ouzou

Faculté de Génie Electrique et d'Informatique

Département d'Informatique

MEMOIRE

En vue de l'obtention du Diplôme du Master académique en Informatique

Option : Systèmes Informatiques

Théme

Mise en place d'un IDS pour sécuriser un réseau en utilisant Snort

Réalisé par :

SELMANI Elgharbi

Soutenue le : 08/12/2020 devant le jury composé de :

M^{r}	SADOU Samir	**Président**
M^{elle}	YESLI Yasmine	**Examinatrice**
M^{me}	BOURKACHE Ghenima	**Promotrice**

Année Universitaire
2019/2020

Remerciements

Je souhaite adresser mes remerciements les plus sincères aux personnes qui m'ont apportés leur aide et qui ont contribués à l'élaboration de ce mémoire.

Je tiens à remercier ma promotrice Madame BOURKACHE Ghenima pour l'orientation, la confiance et la patience qui ont donnés un apport considérable, sans lesquels ce travail n'aurait pas vu le jour.

Je remercie très sincèrement, les membres de jury d'avoir bien voulu accepter de faire partie de la commission d'examinateur, et consacré leurs temps à la lecture de ce mémoire.

Sans oublier de remercier les enseignants qui ont contribué à notre formation et appuyé notre cursus universitaire, et le personnel administratif de département d'informatique.

Et finalement, je tiens à remercier toute personne qui a contribué de n'importe qu'elle manière à l'élaboration de ce mémoire.

Merci à tous et à toutes.

Sommaire

Introduction générale

Introduction générale

Avec l'évolution des techniques de communication, les systèmes d'information et réseaux informatiques sont aujourd'hui de plus en plus ouverts sur le monde extérieur notamment avec Internet. Cette ouverture facilite la vie pour l'humain en lui offrant divers services, et relie des centaines de millions de machines à Internet un peu partout dans le monde. Cependant, cette interconnexion des machines permet également aux utilisateurs malveillants d'utiliser ces ressources et profiter de ses vulnérabilités à des fins abusives, par exemple : rendre un service web hors ligne.

La sécurité de nos jours est un problème d'une importance capitale, elle est devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers. Différents mécanismes ont été mis en place pour faire face à ces problèmes de sécurité, comme les antivirus, les pare-feux, le cryptage, mais ces mécanismes ont des limites face au développement rapide des techniques de piratage. Pour éviter ces limites, l'utilisation des systèmes de détection d'intrusion s'impose.

Les systèmes de détection d'intrusions ont été conçus pour une surveillance continue, et la découverte des violations de la politique de sécurité, ainsi l'identification de toute activité non autorisée dans un réseau.

C'est dans cette optique que s'inscrit notre mémoire. À savoir l'étude des systèmes de détection d'intrusions, et sa mise en place pour sécuriser un réseau informatique. Ce mémoire est structuré en quatre chapitres comme suit :

Le premier chapitre est consacré à la présentation des généralités sur les réseaux informatiques.

Dans le second chapitre, nous présentons les menaces informatiques, les logiciels malveillants, et les mécanismes de sécurité.

Dans le troisième chapitre, nous présentons les **IDS** et les **IPS** en donnant leur architecture et le principe de leur fonctionnement, et la différence entre un **IDS** et un **IPS**.

Le quatrième chapitre est consacré à la mise en place de notre IDS, notamment l'étudie des trois architectures de sécurité pour l'emplacement de l'IDS, la présentation des différents outils utilisés, le choix de la bonne architecture, la mise en place de la solution et les tests.

Enfin, nous terminons le mémoire par une conclusion générale.

Chapitre I : Généralités sur les réseaux informatiques

I.1 Introduction

Les réseaux informatiques permettent à leur origine de relier des terminaux passifs à de gros ordinateurs centraux. Ces derniers autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banque, gestion, commerce, base de données, recherche…etc.) et des particuliers (messagerie, loisirs…etc.).

I.2 Définition

Un réseau est un ensemble de moyens matériels et logiciels géographiquement dispersés destinés à offrir un service, comme le réseau téléphonique, ou à assurer le transport de données. Les techniques à mettre en œuvre diffèrent en fonction des finalités du réseau et de la qualité de service désirée. [2]

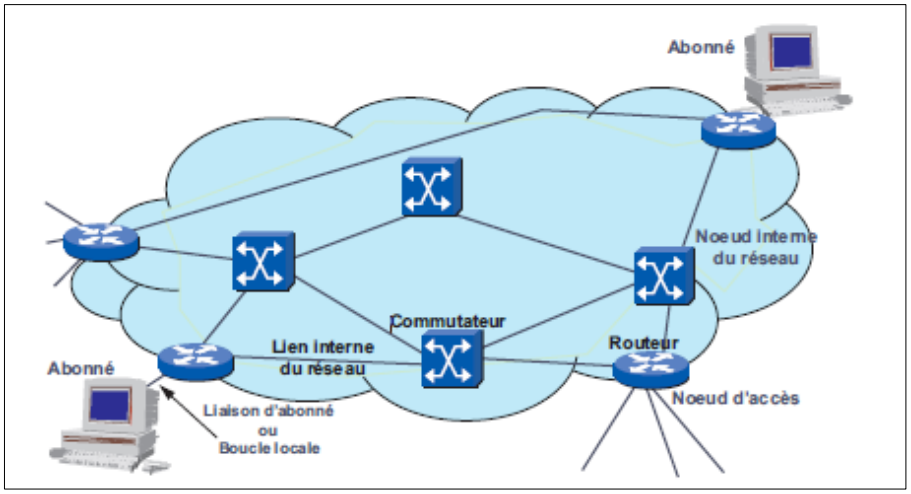


Figure 1 : Le réseau ensemble de ressources mises en commun

I.3 Intérêts des réseaux

Un ordinateur est une machine permettant de manipuler des données. L'homme, un être de communication, a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile. Un réseau permet: [13]

- Le partage de fichiers, d'applications et de ressources.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, ...).
- La communication entre processus (entre des machines industrielles).

- La garantie de l'unicité de l'information (bases de données).
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).
- Les réseaux permettent aussi de standardiser les applications, on parle généralement de *groupware*. Par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

I.4 Classification des réseaux selon leur étendue

Suivant la distance qui sépare les ordinateurs, on distingue plusieurs catégories de réseaux :

- PAN : Personal Area Network (Réseau Personnel)
- LAN : Local Area Network (Réseau Local)
- MAN : Metropolitan Area Network (Réseau Métropolitain)
- WAN : Wide Area Network (Réseau Etendu)

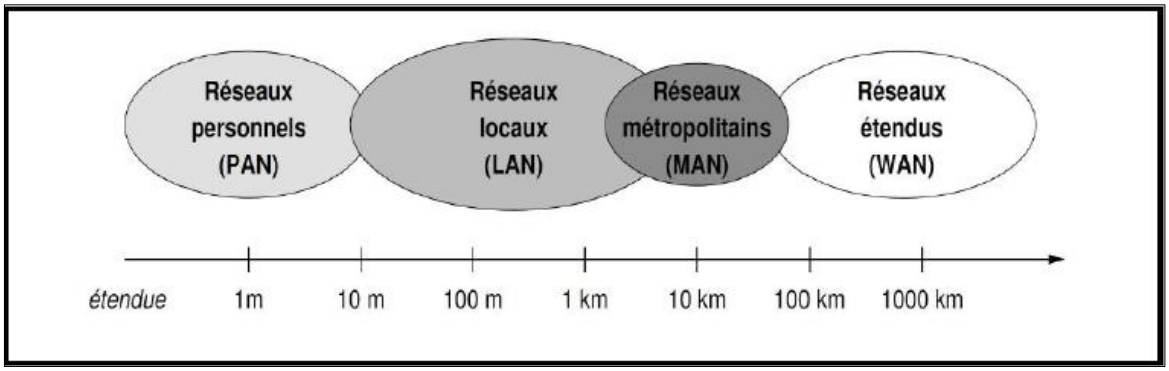


Figure 2 : Classification des réseaux [4]

I.4.1 PAN

La plus petite taille de réseau ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tels que GSM, portable, organiseur etc.… d'un même utilisateur [4].

I.4.2 LAN

LAN signifie *Local Area Network* (en français *Réseau Local*). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un

réseau ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs. [5]

I.4.3 MAN

Les MAN (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. [5]

I.4.4 WAN

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet. [5]

I.5 Les topologies des réseaux

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé **topologie physique**. On distingue généralement les topologies suivantes : [6]

- Topologie en bus
- Topologie en étoile
- Topologie en anneau
- Topologie maillée
- Topologie en arbre

La **topologie logique**, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

I.5.1 Topologie en bus

Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. [6]

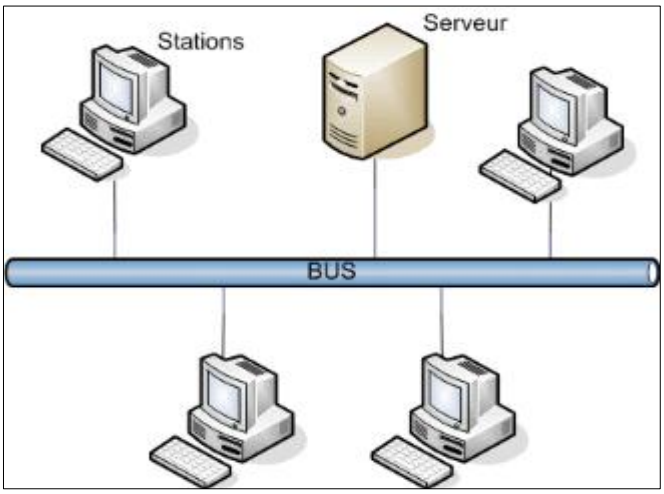


Figure 3 : Typologie en bus

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté. [6]

I.5.2 Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais *hub*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions. [6]

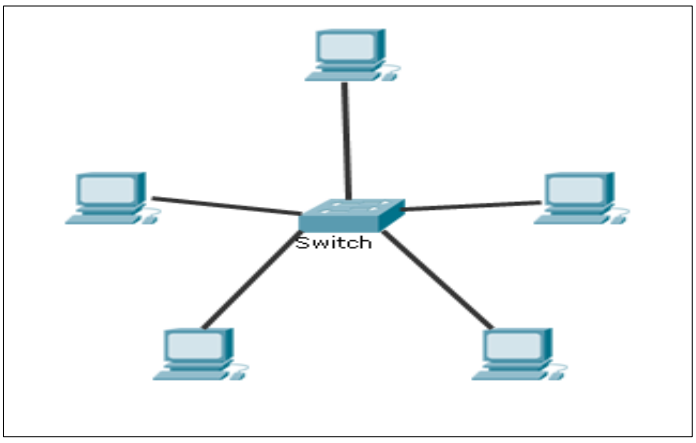


Figure 4 : Topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est

possible. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub). [6]

I.5.3 Topologie en anneau :

Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

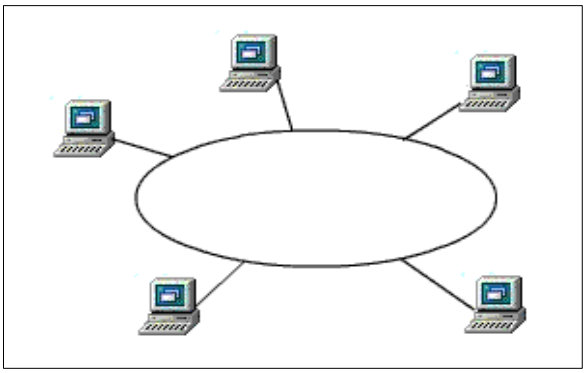


Figure 5 : Topologie en anneau

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole. Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et **FDDI**. [6]

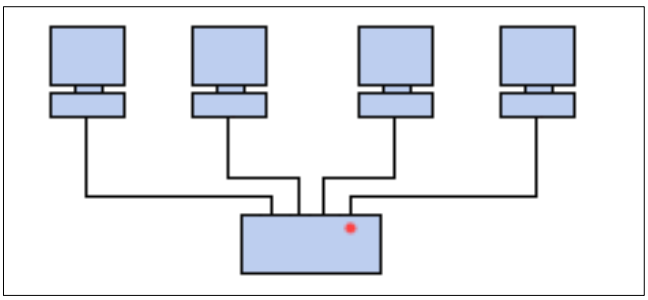


Figure 6 : Répartiteur

I.5.4 Topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons de point à point. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé. Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). [7]

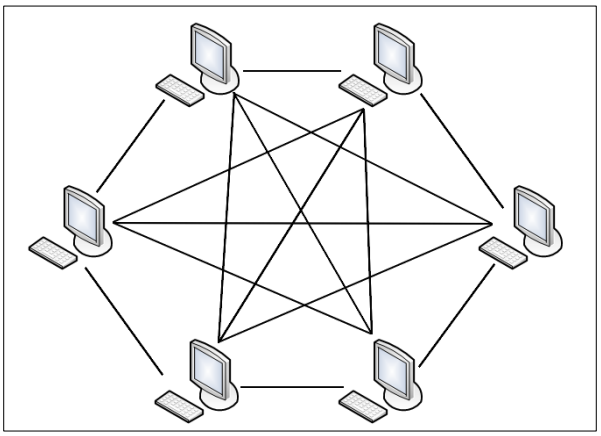


Figure 7 : Topologie maillée

L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties. L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée.

I.5.5 Topologie en arbre

Aussi connu sous le nom de topologie **hiérarchique**, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence. [7]

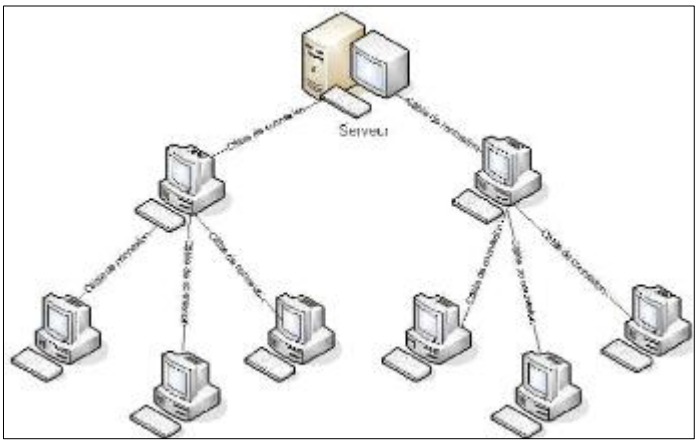


Figure 8 : Topologie en arbre

I.6 Les Modèles OSI et TCP/IP

Pour assurer le bon fonctionnement d'un réseau, il faut réunir les supports physiques nécessaires et prévoir une bonne architecture logicielle et une normalisation de celle-ci s'impose. Deux familles d'architectures ont vu le jour : La première s'appelle le **Modèle OSI**. La seconde sur laquelle ils sont basés les réseaux IP, est **l'architecture TCP/IP**.

I.6.1 Le modèle OSI (Open System Interconnexion)

Ce modèle est une norme définie par ISO (International Organization for Standardization). Fondé sur un principe énoncé par JULES CESAR « Diviser pour mieux régner ». Ce modèle est composé de sept couches (elles seront détaillées ultérieurement) : **couche physique, couche liaison de données, couche réseau, couche session, couche transport, couche présentation et couche application.** [8]

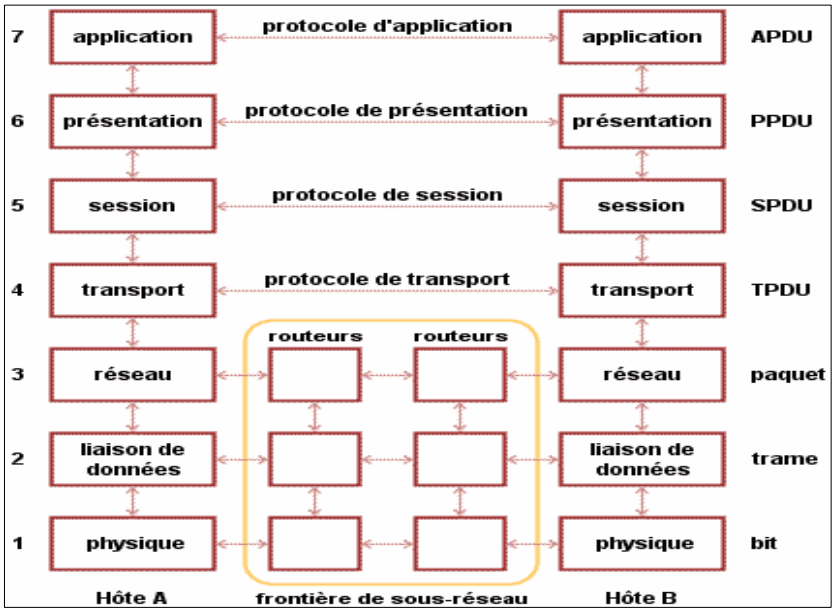


Figure 9 : Modèle de référence OSI

Ce modèle permet la communication entre plusieurs équipements et systèmes hétérogènes. Cette communication passe donc par un ensemble de couches empilées : [8]

- Chaque couche a un rôle précis (conversion, routage, découpage, vérification…etc.).
- Chaque couche dialogue avec la couche juste au-dessus et celle au-dessous : elle fournit des services à la couche dessus et utilise les services de la couche dessous.
- Chaque couche encapsule les données venant de la couche dessus en y ajoutant des propres informations avant de les passer à la couche dessous (opération inverse dans l'autre sens).
- Les données traversent les couches vers le bas quand elles sont envoyées et elles remontent les couches à la réception.

Décrivons maintenant le rôle de chaque couche [9] :

1. **La couche Physique :** La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1).

2. **Couche liaison de données :** Cette couche s'occupe de la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.
3. **Couche réseaux :** elle traite la partie de données utiles contenue dans la trame. Elle connaît l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage et le routage.
4. **Couche transport :** en charge de la liaison d'un bout à l'autre. Cette couche s'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.
5. **Couche session :** en charge d'établir et maintenir des sessions (c'est-à-dire débuter le dialogue entre machines, vérifier que l'autre machine est prête à communiquer, s'identifier, etc…).
6. **Couche présentation :** en charge de convertir les données en information compréhensible par les applications et les utilisateurs ; syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression…etc.
7. **Couche application :** c'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers, l'émulation de terminaux, …etc.

Au niveau de chaque couche un ensemble de protocoles est intégré.

Protocole réseau : est un ensemble de règles et de procédures permettant de définir un type de communication particulier entre les machines (exemple **: HTTP, FTP, TCP, IP, ICMP**,…etc.).

I.6.2 Le modèle TCP/IP

Le nom TCP/IP provient des deux protocoles principaux étroitement liés : TCP (*Transmission Control Protocol*) et IP (*Internet Protocol*). Ce modèle est celui adopté par le réseau mondial Internet. Il est basé sur 4 couches : [10]

1. **Couche accès réseau :** La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.
2. **Couche Internet :** La couche Internet est la couche "la plus importante" car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces

paquets indépendamment les uns des autres jusqu'à destination. Les paquets sont alors rassemblés par cette couche.

3. **Couche transport :** Son rôle est le même que celui de la couche transport du modèle OSI. Officiellement, cette couche n'a que deux implémentations :
    a. **TCP**, un protocole orienté connexion qui assure le contrôle des erreurs
    b. **UDP**, un protocole non orienté connexion dont le contrôle d'erreur est peu fiable.
4. **Couche application :** Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles.

On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches (Présentation et Session), et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

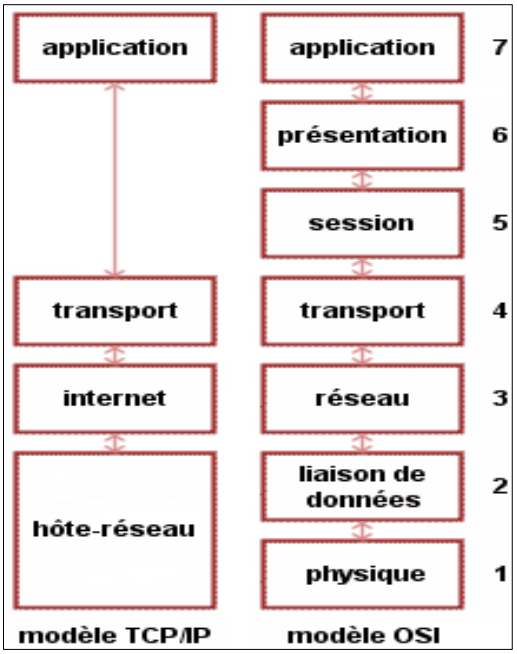


Figure 10 : Modèle TCP/IP et OSI

I.7 Conclusion

TCP/IP est le protocole utilisé dans le réseau Internet. Mais malheureusement, la suite de protocoles TCP/IP, développée sous le parrainage du département américain de la défense, ne serait pas parfaite. Il existerait des problèmes de sécurité inhérents à la conception du protocole ou à la plupart des implémentations TCP/IP. Les pirates utilisent ces vulnérabilités pour effectuer diverses attaques sur les systèmes, d'où le problème de la sécurité réseau.

Chapitre II : Sécurité Informatique

II.1 Introduction

La sécurité informatique joue un rôle majeur dans les technologies numériques modernes, avec l'augmentation de la demande d'internet dans différents domaines (sanitaire, social, éducatif, militaire…), les besoins en sécurité sont de plus en plus importants, le développement des applications et des sites tel que : le commerce électronique, le paiement en ligne ou la vidéoconférence, implique de nouveaux besoins comme l'identification des entités communicantes, l'intégrité des messages échangés, la confidentialité de la transaction, l'authentification des entités, l'anonymat du propriétaire du certificat, l'habilitation des droits, la procuration, …etc.

II.2 Objectifs de sécurité

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime par les objectifs (services) de sécurité suivant : [11]

- **Disponibilité :** est la propriété qui permet de garantir l'accès aux ressources. Exemples de ressources : serveur, réseau, donnée …
    - Il ne suffit pas qu'une ressource soit disponible. Elle doit être utilisable avec des temps de réponse acceptables.
    - Un service doit être assuré avec un minimum d'interruption (continuité de service).
    - La disponibilité est obtenue, par exemple, par une certaine redondance ou duplication des ressources.
- **Intégrité :** est lié au fait que des ressources ou services n'ont pas été altérés (détruits ou modifiés) tant de façon intentionnelle qu'accidentelle.
    - Il est indispensable de se protéger contre la modification des données lors de leur stockage, de leur traitement ou de leur transfert.
    - En télécommunication, **le contrôle d'intégrité** consiste à vérifier que les données n'ont pas été modifiées tant de façon intentionnelle (attaques informatiques) qu'accidentelle durant la transmission.
- **Confidentialité :** c'est la propriété qui garantit que les informations transmises ne sont compréhensibles que par les entités autorisées.
    - Deux actions complémentaires permettent d'assurer la confidentialité des données :
        - Limiter et contrôler l'accès aux données afin que seules les personnes autorisées puissent les lire.

        - Transformer les données par des techniques de chiffrement pour qu'elles deviennent inintelligibles aux personnes qui n'ont pas les moyens de les déchiffrer.
    - Le chiffrement des données (ou cryptographie) contribue à en assurer la confidentialité des données et à en augmenter la sécurité des données lors de leur transmission ou de leur stockage.
- **Authentification :** c'est la propriété qui consiste à vérifier l'identité d'une entité avant de lui donner l'accès à une ressource.
    - L'entité devra prouver son identité : Exemples : mot de passe, empreinte biométrique.
    - Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification et l'authentification (pas d'accès anonyme aux ressources).
- **Non répudiation :** est le fait de ne pourvoir nier qu'un évènement (action transaction) a eu lieu.
    - Par exemple, la non répudiation permet d'avoir une preuve comme quoi un utilisateur a envoyé (ou reçu) un message particulier. Ainsi, l'utilisateur ne peut nier cet envoi (ou réception).

II.3 Attaques

II.3.1 Définition

Une attaque peut être définie par : n'importe quelle action qui tente d'exploiter une (ou plusieurs) vulnérabilité(s) dans un système pour violer un ou plusieurs besoins de sécurité et est généralement préjudiciable. [13][14]

II.3.2 Objectifs des attaques

Les objectifs des attaques visent : [14]

- **Interception :** Une tierce partie non autorisée obtient un accès à un actif. C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.
- **Modification :** Une tierce partie non autorisée obtient accès à un actif et le modifie. Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de

données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.

- **Fabrication :** Une tierce partie non autorisée insère des faux objets dans un système. C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrement à un fichier.
- **Interruption :** Un actif du système est détruit ou devient indisponible ou inutilisable. C'est une attaque portée à la disponibilité. La destruction d'une pièce matérielle, la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples.

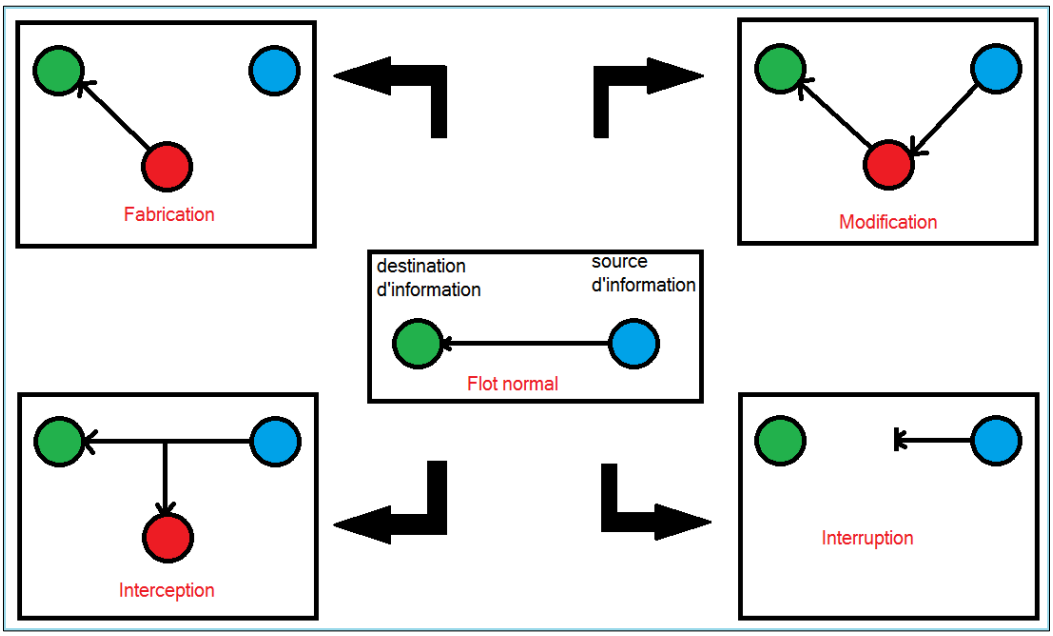


Figure 11 : Les objectifs des attaques

II.3.3 La reconnaissance passive

Il s'agit d'une phase d'attaques où l'intrus n'effectue pas une action pour collecter les informations. Il se restreint à observer passivement les événements afin d'en tirer les conclusions. Une des attaques les plus répandues est l'écoute du trafic (sniffing).

Le principe consiste à installer une sonde sur le réseau pour capter le trafic et le sauvegarder dans des fichiers journaux. L'analyse de ces fichiers permet de connaître les machines installées sur le réseau et de déterminer les ports ouverts et les systèmes d'exploitation utilisés. L'attaque est considérée lente si l'attaquant cherche une information précise sur une machine particulière du réseau. En revanche elle est si discrète qu'il est difficile de la détecter. [15]

II.3.4 La reconnaissance active

L'objectif de la reconnaissance active est similaire à celui de la reconnaissance passive. Il s'agit d'acquérir des informations utiles sur le réseau cible. La reconnaissance active parait néanmoins plus fructueuse puisque l'attaquant ne se restreint pas à inspecter les données échangées entre les différents hôtes. Cependant, il initie lui-même des connections réseaux pour tester le comportement des machines. Il cherche des informations précises concernant les hôtes accessibles, l'emplacement des routeurs et des pare feux, les systèmes d'exploitation, les ports ouverts, les services fournis et les versions des applications exécutées. Parmi les techniques les plus utilisées pour acquérir ces informations nous évoquons les utilitaires **PING**, **NsLookup**, **DIG**, **Traceroute.** [15]

II.4 Les techniques d'attaque

II.4.1 Spoofing

Nous trouvons 3 attaques **Spoofing** principales : [8]

- **Spoofing IP :** Le spoofing IP est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement, il s'agit d'une mascarade de l'adresse IP au niveau des paquets émis, c'est-à-dire une modification des paquets envoyés afin de faire croire au destinataire qu'ils proviennent d'une autre machine.
- **Spoofing ARP :** Le spoofing ARP est une technique qui modifie le cache ARP. Le cache ARP contient une association entre les adresses matérielles des machines et les adresses IP, l'objectif du pirate est de conserver son adresse matérielle, mais d'utiliser l'adresse IP d'un hôte approuvé. Ces informations sont simultanément envoyées vers la cible et vers le cache. A partir de cet instant, les paquets de la cible seront routés vers l'adresse matérielle du pirate.
- **Spoofing DNS :** Le système DNS (Domain Name System) a pour rôle de convertir un nom de domaine en son adresse IP et réciproquement, à savoir : convertir une adresse IP en un nom de domaine. Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émises par une victime. Il existe deux types de méthode :
    - **DNS ID spoofing** L'attaquant essaie de répondre à un client en attente d'une réponse d'un serveur DNS, avec une fausse réponse et avant que le serveur DNS ne réponde.

- **DNS Cache Poisoning** L'attaquant essaie d'empoisonner le cache (table de correspondance IP- NomMachine) du serveur DNS avec d'autres informations.

II.4.2 Attaque l'homme du milieu (Man In The Middle)

L'attaque de l'homme du milieu ou Man In The Middle (MITM), est une attaque utilisant au moins trois ordinateurs. Deux ordinateurs communiquent ensemble, un troisième au milieu casse la liaison entre les deux ordinateurs, et se fait passer pour l'autre entité, il intercepte et envoie les communications et peut de plus les modifier. [20]

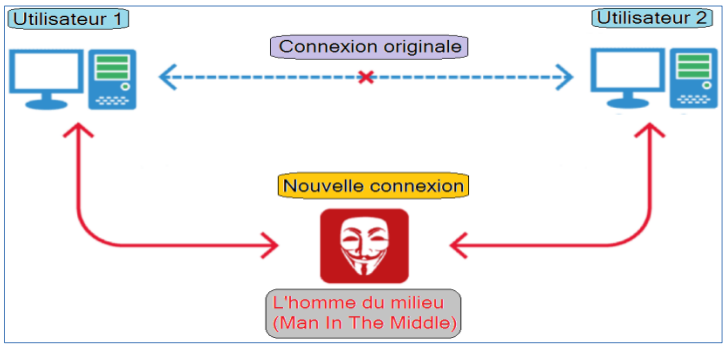


Figure 12 : Simuler le scénario de l'attaque MITM

La plupart des attaques de type ***man in the middle*** consistent à écouter le réseau à l'aide d'outils d'écoute du réseau comme ***wireshark*** (un analyseur de paquets. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques).

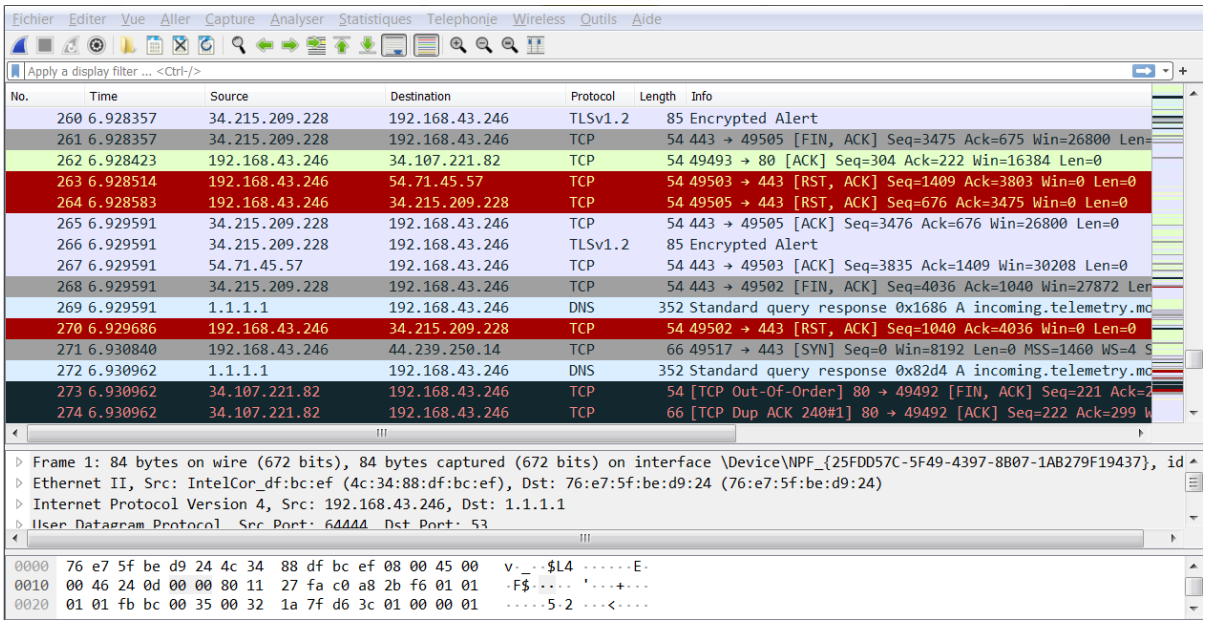


Figure 13 : Capture de l'outil wireshark

II.4.3 Sniffing

Consiste à configurer la carte réseau pour récupérer l'ensemble des données transmises par le biais d'un réseau de la couche 2 à la couche 7 du modèle OSI, et utiliser ces données pour d'autres attaques. [20]

II.4.4 DoS et DDoS

- **DoS (Denial of Service) :** Un DoS (Denial of Service) est une attaque de déni de service. Le but d'un déni de service est de faire tomber un serveur. L'attaque par **Syn flood** (consiste à envoyer une grande quantité de requête de type Syn) est l'une des attaques les plus répandues, elle consiste à demander des connexions et ne pas y répondre. Lors d'une demande de connexion, le serveur est en attente et bloque pendant un certain temps une partie de ses ressources pour cette nouvelle connexion. Le but est l'envoyer plus de demandes de connexion qu'il ne peut en traiter dans un temps donné. Le serveur ne pourra plus subvenir au besoin des vrais clients. [20]
- **DDoS (Distributed Denial of Service):** Le DDoS (Distributed Denial of Service) est similaire au DoS, mais l'attaque se fait à partir de plusieurs machines. Une attaque DoS est simple à contrôler, il suffit d'établir une règle dans le pare-feu afin de bloquer l'adresse IP attaquante. Dans le cas d'un DDoS cela se complique énormément. [20]

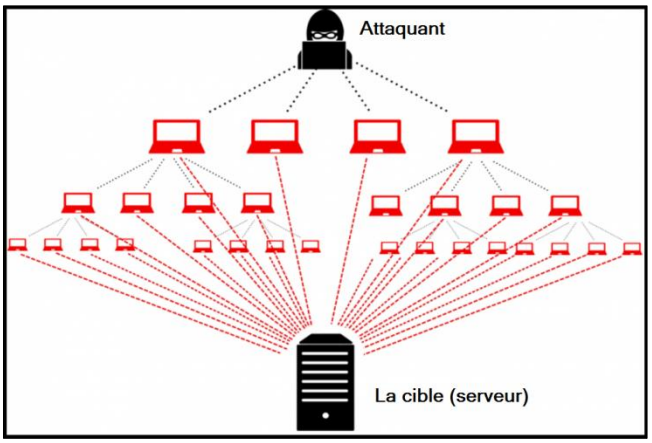


Figure 14 : Architecture attaque DDoS

II.4.5 Attaques virales

Il existe principalement quatre types de menaces distinctes : [21]

- **Les virus :** Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire, Et qui lorsqu'on le lance, se charge en mémoire et exécute les instructions que son auteur a programmées.

- **Les vers :** Un ver est un programme qui peut se reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (clé USB, disque dur, programme hôte…) pour se propager ; un ver est donc un **virus réseau.**
- **Les chevaux de Troie :** On appelle **cheval de Troie** (Trojan horse) un programme informatique ouvrant une porte dérobée (Backdoor) dans un système pour faire y entrer un hacker ou d'autres programmes indésirables. Un cheval de Troie peut par exemple : voler des mots de passe, copier des données sensibles, contrôle un terminal à distance…etc.

II.4.6 Attaque par faille matérielle

Les failles matérielles sont rares mais lorsque l'une d'entre elles est révélée, elle peut s'avérer très dangereuse, et nous trouvons : [21]

- Les routeurs

  La plupart des routeurs sont accessibles via des interfaces texte comme **Telnet** et web (serveur HTML). Une faille se matérialise souvent dans leur microcode : serveur HTML mal conçu, système de mots de passe défaillant ou même porte dérobée non documentée par le constructeur.
- Les processeurs

  Exploiter la technologie de virtualisation intégrées aux nouveaux processeurs, En 2006 une chercheuse polonaise *Joanna Rutkowska*. Cette dernière est arrivée à créer un compte administrateur sur un PC tournant sous Windows Vista. Son rootkit, appelé *Blue Pill*.

II.4.7 Attaque de mot de passe

Nous trouvons l'utilisation du mot de passe presque partout, c'est pour ça les pirates ont couru pour trouver une faille ou une solution pour casser ce niveau de sécurité. Nous trouvons trois méthodes populaires : [21]

- **Attaque par force brute :** On appelle ainsi **attaque par force brute** (brute force cracking, ou parfois attaque exhaustive) le cassage d'un mot de passe en testant tous les mots de passe possibles, et cette attaque avait perdu de son intérêt notamment face à des outils de cryptage de plus en plus perfectionnés.
- **Attaque par dictionnaire :** La plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes.

- **Attaque par réinitialisation de mot de passe :** Cette attaque est principalement utilisée pour prendre le contrôle de compte de services en ligne. Le principe consiste à solliciter le service en ligne pour lui demander la réinitialisation du mot de passe d'un compte. Le pirate a alors plusieurs méthodes à sa disposition :
  - Grâce à des recherches sur le détenteur du compte, deviner les réponses qui permettent de réinitialiser le mot de passe. Les questions de type (nom du chien, de sa grand-mère…) sont des informations pouvant être retrouvées notamment sur les réseaux sociaux.
  - Intercepter l'e-mail de réinitialisation s'il connaît le compte de secours.
  - Créer lui-même un message qui renverra l'internaute vers la page de réinitialisation, page qui sera contrefaite.

II.5 Mécanismes de sécurité

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Et nous trouvons plusieurs mécanismes de sécurité :

II.5.1 Pare-feu (firewall)

Le pare-feu ou **Firewall** en anglais, c'est un mécanisme indispensable dans la sécurité informatique des entreprises et même dans des simples ordinateurs. Le Pare-feu propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau. Et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec les activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux. [16]

II.5.1.1 Fonctionnement du Pare-feu

Un système Pare-feu ou Firewall contient un ensemble de règles prédéfinies permettant, d'autoriser la connexion (Allow), de bloquer la connexion (Deny), de rejeter la demande de connexion sans avertir l'émetteur (drop). [16]

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politique de sécurité permettant : [16]

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées (tout ce qui n'est pas explicitement autorisé est interdit).
- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Un système Firewall fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données échangé entre une machine du réseau interne et une machine extérieure. Les en-têtes systématiquement analysés par le firewall sont :

Adresse IP de machine émettrice

Adresse IP de machine réceptrice

Type de paquet (TCP, UDP, etc…)

Numéro de **port** (un numéro associé à un service ou une application réseau.).

II.5.1.2 Les Firewalls BRIDGE

Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de Firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le Firewall est indétectable pour un pirate. En effet, quand une requête ARP est émise sur le câble réseau, le Firewall ne répondra jamais. Ses adresses **Mac** (12 chiffres hexadécimaux « 48bits » identifiant une interface réseau) ne circuleront jamais sur le réseau, et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Et ces Firewalls se trouvent typiquement sur les **switchs** (Un commutateur réseau « en anglais switch », est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels). [16]

- **Inconvénients :**
  - Possibilité de le contourner (il suffit de passer outre ses règles).
  - Configuration souvent contraignante.
  - Les fonctionnalités présentes sont très basiques (filtrages sur adresse IP, port).
- **Avantage :**
  - Impossible de l'éviter (les paquets passeront par ses interfaces).
  - Coûteux.

II.5.2 Antivirus

Les antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus

sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais parfois, ce nettoyage simple n'est pas possible. [17]

II.5.3 Systèmes de détection d'intrusions IDS

Un système de détection d'intrusion **(ou 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 connaissance sur les tentatives réussies comme échouées des intrusions. [12]

II.5.4 Système de prévention d'intrusion IPS

Un système de prévention d'intrusion **(ou IPS : Intrusion Prevention System)** est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. [12]

II.5.5 Cryptographie

La cryptographie est une science basée sur les mathématiques, et aussi une des disciplines de la cryptologie s'attachant à protéger des messages (assurant la confidentialité, l'authenticité et l'intégrité) avec un algorithme de chiffrement, Chiffrer un message consiste de le rendre inintelligible, sauf pour celui qui possède le moyen (une clé) de le déchiffrer. [8]

- **La cryptographie Symétrique :** Aussi appelé chiffrement à clé secrète, il consiste à utiliser la même clé pour le chiffrement et le déchiffrement. [18]

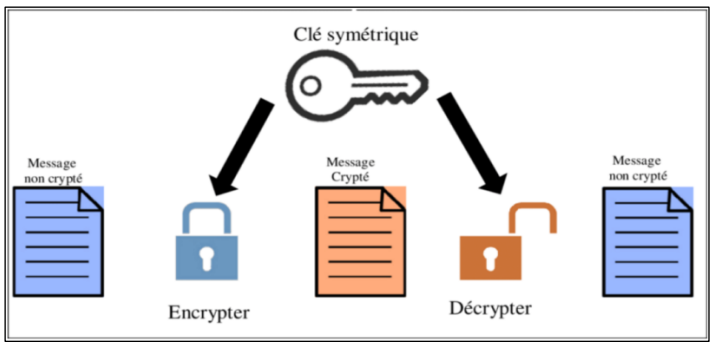


Figure 15 : Cryptage Décryptage Symétrique [40]

- **La cryptographie Asymétrique :** Ce chiffrement est aussi appelé chiffrement à clés publiques. Le principe de l'algorithme de ce chiffrement est qu'il s'agit d'une fonction unidirectionnelle à trappe. Une telle fonction a la particularité d'être facile à calculer dans un sens, mais difficile voire quasi impossible dans le sens inverse. La seule manière de pouvoir réaliser le calcul inverse est de connaître une trappe. Une trappe

pourrait par exemple être une faille dans e générateur de clés. Cette faille peut être soit intentionnelle de la part du concepteur ou accidentelle. [18]

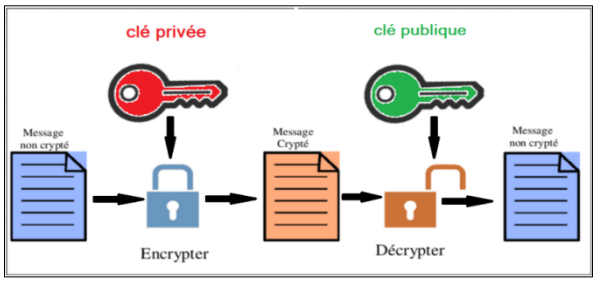


Figure 16 : Cryptage Décryptage Asymétrique

- **Signature électronique :** Signature électronique ou numérique est un code digital permet à la personne qui reçoit une information de contrôler l'authenticité de son origine. Et également de vérifier que l'information en question est intacte. Aussi, les signatures électroniques permettent l'authentification et le contrôle de l'intégrité et également la non répudiation.
- **Certificat :** Certificat est Document électronique, carte d'identité émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique l'encryptions et fournit des informations de gestion sur le certificat et le détenteur.

Issued To

Common Name (CN)	*.facebook.com
Organization (O)	Facebook, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	0A:A9:4B:5A:FA:70:A3:70:97:9A:C5:06:47:EF:AC:9C

Issued By

Common Name (CN)	DigiCert SHA2 High Assurance Server CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

Period of Validity

Begins On	November 2, 2020
Expires On	January 31, 2021

Fingerprints

SHA-256 Fingerprint	EE:DE:3E:39:07:A3:76:47:93:C9:0C:41:17:9E:D6:E7: 22:06:7E:52:B8:8D:99:BC:5A:35:98:0E:B8:A1:FC:06
SHA1 Fingerprint	F7:72:F3:5C:71:1D:95:E1:59:C6:FD:49:D5:B2:E9:F0:05:2F:60:97

Figure 17 : Certificat de Facebook.com

II.5.6 VPN

De nos jours, les cybers attaques se sont multipliées, y compris envers les particuliers. Ces derniers ont décidé de s'armer d'une protection efficace comme le VPN pour faire face aux hackers. Un VPN (Virtual Private Network) ou Réseau Privé Virtuel en français est une connexion inter-réseau permettant de relier 2 réseaux locaux différents de façon sécurisé par un protocole de **tunnelisation**.

La tunnelisation est un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie. [19]

II.6 Conclusion

Dans ce chapitre, nous avons présentés une introduction générale sur la sécurité informatique, et compris que la majorité des menaces se trouvent dans les réseaux locaux et nos appareils personnels, et faire prendre conscience des attaques que nous pouvons rencontrer, nous distinguons deux types de reconnaissances (attaques) passive et active. Nous avons aussi présenté des solutions contre ces menaces avec des mécanismes comme les IDS, et nous verrons cela en détail dans le chapitre suivant.

Chapitre III : Etude des Système de Détection et Prévention d'Intrusions (IDS/IPS)

III.1 Introduction

De nos jours, l'ouverture des systèmes d'information des entreprises à des échanges externes avec le réseau mondial internet donnent aux utilisateurs malveillants des moyens supplémentaires et un élargissement dans leur terrain de jeu afin d'y attaquer et menacer ces entreprises facilement.

C'est bien d'avoir un système qui joue un rôle pour surveiller la circulation des données échangées entre le réseau de l'entreprise et le réseau externe, et qui serait capable de réagir en temps réel si des données semblent suspectes. Les systèmes de détection et prévention d'intrusions (IDS/IPS) conviennent parfaitement pour réaliser ces tâches.

III.2 Définition de l'IDS

Un IDS ou (**I**ntrusion **D**etection **S**ystem) ou le système de détection des intrusions, est un logiciel ou un matériel qui automatise des surveillances et détecter les signes des intrusions. Placée judicieusement sur un réseau ou un système. Pour automatiser la surveillance et repérer les activités douteuses ou anormales sur cette cible et alerter les responsables de sécurité. De cette façon, on peut obtenir une connaissance des tentatives réussies (ou non) d'attaque ou d'intrusion sur le système. [22]

III.2.1 Les différents types d'IDS

Les différents IDS se caractérisent par leur domaine de surveillance (surveillance d'un hôte « HIDS », surveillance d'un segment du réseau « NIDS », surveillance d'une application « AIDS »). Il existe trois grandes familles distinctes d'IDS :

- **IDS sur l'hôte ou HIDS (Host IDS) :** Le HIDS c'est un système de détection d'intrusion qu'il s'attache à surveiller le fonctionnement ou l'état de la machine sur laquelle il est installé, afin de détecter les attaques. Il analyse exclusivement l'information concernant cet hôte, avec la vérification des journaux systèmes, il contrôle l'accès aux appels systèmes, il étudie l'intégrité des systèmes de fichiers. Comme il n' pas à contrôler le trafic du réseau mais seulement les activités d'un hôte ils se montrent habituellement plus précis sur les types d'attaques subies. [23][35]
- **IDS sur réseau ou NIDS (Network IDS) :** Son rôle est l'analyse et l'interprétation des paquets circulant sur le réseau. Pour faire ça, un logiciel de protection est installé uniquement à des points spécifiques du réseau, comme les serveurs qui établissent l'interface entre l'environnement extérieur et le segment de réseau à protéger. Cette interface doit être configuré en mode furtif (ou stealth mode), de façon à être invisibles

aux autres machines. Pour obtenir ce mode il faut configurer la carte de réseau d'NIDS en mode promiscuité, c'est-à-dire le mode dans lequel la carte réseau lit l'ensemble du trafic, de plus, aucune adresse IP n'est configurée. [23][28]

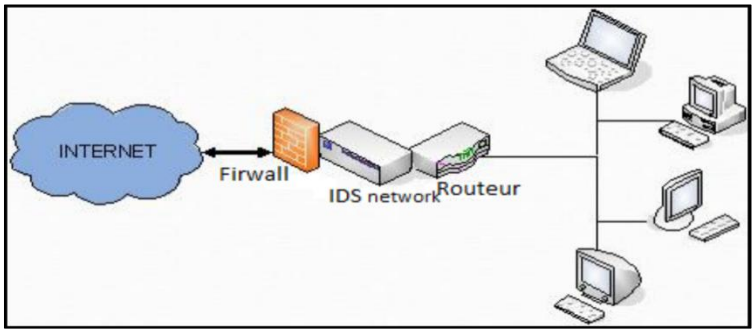


Figure 18 : Exemple d'NIDS [36]

- **IDS basé application ou AIDS (Application based IDS) :** un sous-groupe des HIDS. Il contrôle l'interaction entre un utilisateur et un programme en analysant les fichiers log afin de fournir plus d'informations sur les activités d'une application particulière. Puisque il opère entre un utilisateur et un programme, il est facile de filtrer tout comportement notable. [35]
- **IDS Hybride :** IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et lier les informations d'origines multiples. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, ou chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus exactes. [36]

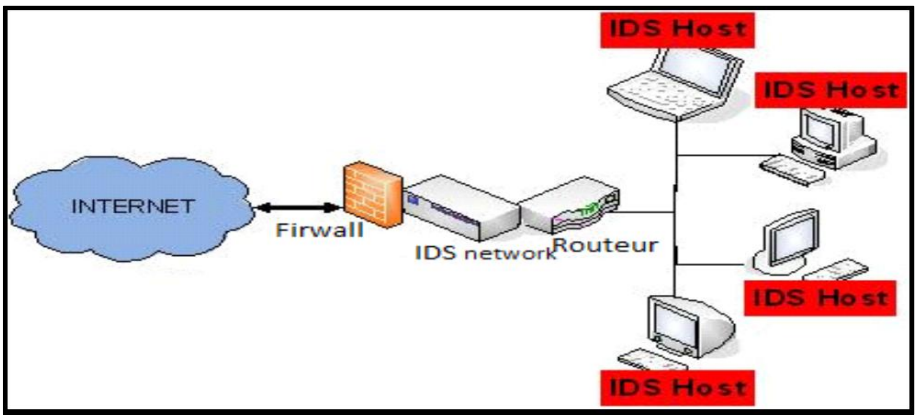


Figure 19 : Exemple d'Hybride [36]

Cependant vu que le secteur des IDS est en plein développement, de nouveaux types d'IDS sont conçus actuellement, comme les IDS basés sur la pile, qui étudie la pile d'un

système, ou les nœuds réseau IDS (Node Network IDS en abrégé NNIDS). Ce nouveau type d'IDS fonctionne comme les NIDS classiques, c'est-à-dire il analyse les paquets du trafic réseau. Cependant, il ne s'intéresse qu'aux paquets destinés à un nœud du réseau. Une autre différence entre le NNIDS et le NIDS est que le NIDS fonctionne en mode "promiscuous", ce qui n'est pas le cas du NNIDS. Celui-ci n'étudie que les paquets à destination d'une adresse ou d'une plage d'adresses. [35]

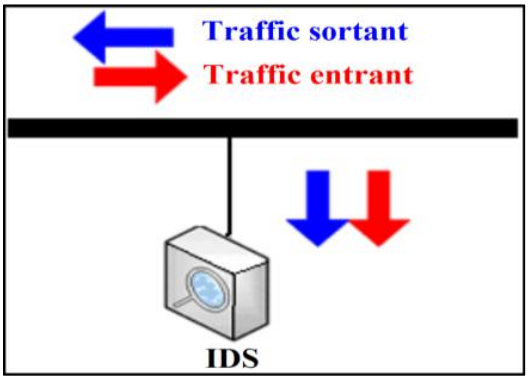


Figure 20 : Emplacement d'un IDS au niveau d'un système informatique [35]

III.2.2 Architecture d'un IDS

Nous nous intéressons maintenant à l'architecture et les modules de base d'un IDS. On retrouve souvent les IDS placés en première ligne du réseau à sécuriser, pour qu'il examine tous les paquets entrants ou sortants. Il réalise un ensemble d'analyses de détection sur chaque paquet individuel ainsi sur les conversations et motifs du réseau. En visualisant chaque transaction dans la figure suivante :

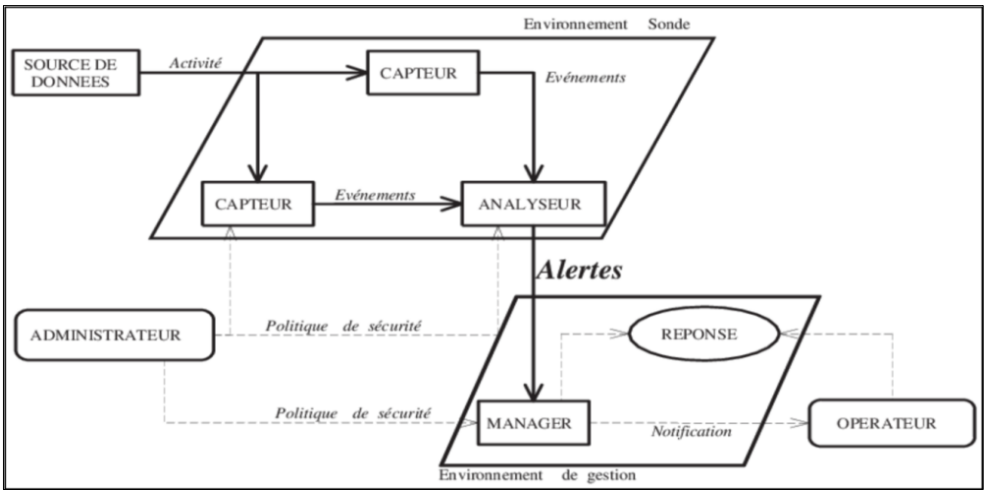


Figure 21 : Schéma d'architecture IDWG d'un IDS [24]

Un IDS est composé de plusieurs éléments dont chacun accompli un rôle bien précis, on trouve :

- **Capteur :** ou le c**ollecteur des données (Sensors),** observe l'activité du système et génère des évènements qui renseignent de l'évolution de l'état du système en filtrant des données provenant d'une source de données. [24]
- **Analyseur :** Les analyseurs reçoivent comme entrée les données qui proviennent d'un ou plusieurs collecteurs ou à partir d'autres analyseurs qui auraient au préalable procédés à un premier traitement des données **[25].** Il génère des alertes lorsque le flux d'évènements fourni par le(s) capteur(s) contient des éléments caractéristiques d'une activité malveillante.
- **Manager :** Le manager collecte les alertes produites par l'analyseur, et les transmit ensuite à l'opérateur sous forme de notifications afin de lui permettre de gérer les alertes reçues et prendre des décisions. **[24]**
- **Opérateur :** Personne chargée de l'utilisation de manager associé à l'IDS. Elle décide sur la réaction à prendre en cas d'alerte.
- **Administrateur :** Une personne chargée de mettre en place la politique de sécurité et configure les IDS et par conséquent de déployer et de configurer les IDS **[24]**, via les interfaces utilisateur.
- **Interface utilisateur :** C'est un module qui permet à l'IDS d'interagir avec l'utilisateur (généralement un administrateur système), pour pouvoir configurer et fixer quelques paramètres en relation avec la politique de sécurité qu'on veuille mettre en œuvre. [25]

III.2.3 Fonctionnement d'un IDS

Nous nous intéressons maintenant au fonctionnement d'un IDS, nous commençons par les méthodes d'analyse, après les techniques de détection.

III.2.3.1 Les méthodes d'analyse

Avec la localisation de l'analyse des données on peut faire une distinction entre les IDS :

- **Analyse centralisée :** certains IDS ont une architecture multi-capteurs. Ils centralisent les événements (ou alertes) pour analyse au sein d'une seule machine. L'intérêt principal de cette architecture est de faciliter la corrélation entre événements puisqu'on dispose alors d'une vision globale. Par contre, la charge des calculs ainsi que la charge réseau peuvent être lourdes et risquent de constituer un goulet d'étranglement. [26]
- **Analyse locale :** si l'analyse du flot d'événements est effectuée au plus près de la source de données (généralement en local sur chaque machine disposant d'un capteur), on minimise le trafic réseau et chaque analyseur séparé dispose de la même puissance

de calcul. En contrepartie, il est impossible de croiser des événements qui sont traités séparément et l'on risque de passer à côté de certaines attaques distribuées. [26]

- **Analyse distribuée :**
  - **Partiellement distribuée :** dans ce cas un nombre limité de nœuds peuvent exécuter des tâches d'analyse locale et de détection mais ils sont commandés par un nœud maître, celui-ci collabore avec d'autres nœuds maîtres pour superviser la détection globale sous forme d'une structure hiérarchique. [27]
  - **Entièrement distribuée :** la collecte d'informations, l'analyse et la détection ainsi que les alertes seront réalisées au niveau local de chaque nœud. Mais dans le cas d'information incomplète ou bien suspicion les nœuds peuvent déclencher des procédures de collaboration supervisées par des nœuds maitres. [27]

III.2.3.2 Les techniques de détection

Le trafic réseau est généralement constitué de datagrammes IP. Un NIDS est capable de capturer les paquets lorsqu'ils circulent sur les liaisons physiques sur lesquelles il est connecté. Pour que le NIDS détecte les intrusions à travers les paquets qui circulent sur le réseau, il peut appliquer les techniques suivantes :

- **Approche comportementale :** Cette technique consiste à détecter une intrusion en fonction du comportement de l'utilisateur ou d'une application, autrement dit c'est créer un modèle basé sur le comportement habituel du système et surveiller toute déviation de ce comportement. [36]
- **Approche par scénario ou par signature :** Cette technique s'appuie sur les connaissances des techniques utilisées par les attaquants contenues dans la base de donnée, elle compare l'activité de l'utilisateur à partir de la base de donnée, ensuite elle déclenche une alerte lorsque des événements hors profil se produisent [36]. Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues, et cette approche est très similaire à celle des outils antivirus et présente les même inconvénients que celle-ci, il nécessite des mises à jour quotidiennes. [30]
- **Vérification de la pile protocolaire :** par exemple « *Ping-Of-Death* » ont recours à des violations des protocoles TCP, IP, UDP, ICMP dans le but d'attaquer une machine. Une simple vérification protocolaire de nombre d'intrusions peut mettre en évidence les paquets invalides et signaler ce type de techniques très usitées. [29]

- **Vérification des protocoles applicatifs** : Cette technique est rapide (il n'est pas nécessaire de chercher des séquences d'octets sur l'exhaustivité de la base de signatures), élimine en partie les fausses alertes et s'avère donc plus efficiente. Beaucoup d'intrusions utilisent des comportements protocolaires invalides, comme par exemple « WinNuke », qui utilise des données NetBIOS invalides (ajout de données OOB data). Dans le but de détecter efficacement ce type d'intrusions, le NIDS doit ré-implémenter une grande variété de protocoles applicatifs. [29]

III.2.3.3 Comportement après détection

On peut classer les IDS par type de réaction lorsqu'une attaque est détectée :

- **Passive :** La plupart des systèmes de détection d'intrusion n'apportent qu'une réponse passive à l'intrusion. Lorsqu'une attaque est détectés, ils génèrent une alarme et notifient l'administrateur système par e-mail, message dans une console, voire même par beeper. C'est alors lui qui devra prendre les mesures qui s'imposent. [26]
- **Active :** D'autres systèmes de détection d'intrusions peuvent, en plus de la notification à l'opérateur, prendre automatiquement des mesures pour stopper l'attaque en cours [26], et dans ce cas il devient un IPS.

III.2.4 Points forts

Le positionnement des sondes réseaux de l'IDS et la configuration des interfaces réseaux, joue un rôle majeur sur l'étude de l'efficacité des protections mises en place, et avoir des avantages indispensable, comme : [23]

- L'invisibilité des dispositifs pour les attaquants.
- Conçu pour la surveillance continue sur le réseau.
- Diminue le travail manuel de la sécurité, en réduisant le coût dans les entreprises.
- Les systèmes de détection d'intrusions peuvent analyser tout le trafic, et relever des attaques même qu'ils n'en sont pas la cible directe.
- Il n'est pas nécessaire de surveiller le réseau en permanence pour être au courant de ce qui se passe par les responsables de sécurité.
- Les IDS détectent les intrusions et renvoient des alertes et notifications avec nombreuses informations détaillées (type supposé d'attaque, la source, la destination), tout cela permet une bonne compréhension sur les attaques.
- Contient des outils de filtrage très intéressants qui nous permettent de faire du contrôle par protocole (ICMP, TCP, UDP), adresse IP, suivi de connexion.

- L'emplacement d'une sonde dans le côté extérieur du firewall, permet de détecter les tentatives d'attaques dirigées contre le réseau surveillé, et une autre dans le côté intérieur de firewall, pour remonter les attaques qui ont réussi à passer le firewall.
- Suivre une attaques sur un réseau, voir si elle arrive jusqu'à sa victime, en suivant quel parcours,…etc.
- Définir des périmètres de surveillance d'une sonde sur des entrées uniques vers plusieurs domaines de collision (par exemple à l'entrée d'un commutateur), pour réduire le nombre de sondes, garder l'efficacité de la sécurité, efficacité de la répétition les alertes et les notifications.

III.2.5 Points faibles

Les IDS basés sur une bibliothèque de de signatures d'attaque connues, cette bibliothèque devra être mise à jour à chaque nouvelle attaque sera affichées. Si l'attaque ne contient pas la signature d'une attaque spécifique et récente, cette dernière passera au travers des mailles du filet et la sécurité des données et le réseau en général sera menacé. [36]

Nous trouvons d'autres points faibles, et sont classées comme suit : [23]

- **Besoin de connaissances en sécurité**
  - La mise en place de sonde sécurité fait appel à de bonnes connaissances en sécurité.
  - L'exploitation des remontées d'alertes nécessite des connaissances plus pointues.
  - La configuration, et l'administration des IDS nécessitent beaucoup de temps, et de connaissances.
  - L'intervention humaine est toujours indispensable, pour prendre les décisions critiques et finales.
- **Problème de positionnement des sondes**
  - Avec fonctionnement en mode promiscuité. Les sondes captent tout le trafic, et même si un Ping flood, les sondes NIDS le captureront aussi et donc en subiront les conséquences, comme si l'attaque leur était directement envoyée. Les DoS classiques seront donc très nocifs pour les sondes NIDS.
  - Le point fort de certains IDS qui est d'archiver aussi le contenu des trames ayant levées une alerte, peut aussi s'avérer un point faible. Un hôte flood avec un paquet chargé de 64000 octets, vont faire exploser la taille des fichiers de logs des sondes en quelques minutes.

- **Problèmes intrinsèques à la plateforme**
  - Beaucoup d'IDS sont des logiciels reposant sur un système d'exploitation non dédié aux IDS.
  - La faiblesse d'un IDS est liée à la faiblesse de la plate-forme.
  - Une saturation de la mémoire, de la carte réseau, ou du processeur porte atteinte directement au bon fonctionnement de tout le système.

III.3 Définition d'IPS

Un système de prévention d'intrusions (IPS) est un composant logiciel et/ou matériel dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. Les IPS rejettent de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue. En effet, le concept d'IPS avant tout été conçu pour lever les limitations des IDS en matière de réponses passives à des attaques. Il ne s'agit plus seulement de détecter une attaque en cours, mais d'empêcher que celle-ci puisse seulement débuter. Pour cette raison qu'un système IPS est obligatoirement placé en ligne pour pouvoir réagir aux attaques (figure 22). [35]

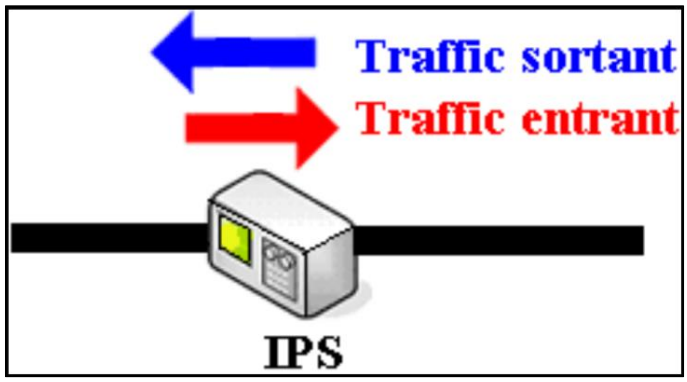


Figure 22 : Emplacement d'un IPS au niveau d'un système informatique [35]

III.3.1 Les différents types d'IPS

Comme pour les IDS, les IPS peuvent être orientés hôtes (Host IPS), réseaux (Network IPS) ou noyau (kernel IPS). Mais, il n'existe pas d'IPS destiné à surveiller une application.

- **IPS orienté hôte (HIPS) :** un IPS basé hôte est un agent installé sur le système bloquant les comportements anormaux tels que la lecture ou l'écriture de fichiers protégés. L'accès à des ports non autorisés, une tentative de débordement de pile, un accès à certaines zones de la base de registres. En effet, un HIPS analyse exclusivement l'information concernant cet hôte pour le protéger des comportements

dangereux. Les HIPS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédantes des données importantes pour l'entreprise. [35]

- **IPS orienté réseau (NIPS) :** Le rôle d'un IPS basé réseau est d'analyser les paquets circulant dans le réseau. La principale différence entre un NIDS et NIPS tient principalement en deux caractéristiques. Le positionnement en coupure sur le réseau du NIPS, et non plus seulement en écoute comme pour le NIDS et la possibilité de bloquer immédiatement les intrusions quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce. Ce qui induit que le NIPS est constitué d'une technique de filtrage de paquets et de moyens de blocage. En effet, le positionnement en coupure, tel un firewall, est le seul mode permettant d'analyser les données entrantes ou sortantes et de réduire dynamiquement les paquets intrusifs avant qu'ils n'atteignent leurs destinations. [35]
- **IPS orienté noyau (KIPS) :** leur particularité est de s'exécuter dans le noyau d'une machine, pour y bloquer toute activité suspecte. Le KIPS peut reconnaître des motifs caractéristiques du débordement de mémoire, et peut ainsi interdire l'exécution du code. Il peut également interdire le système d'exploitation d'exécuter un appel système qui ouvrirait un terminal de commande. Puisqu'un KIPS analyse les appels systèmes, il ralentit l'exécution. C'est pour-ça sont moins utilisés. [36]

III.3.2 Architecture fonctionnelle d'IPS

Le fonctionnement d'un IPS est similaire à celui d'IDS. Il capture le trafic du réseau puis l'analyse. Mais au lieu d'alerter l'utilisateur d'une intrusion ou d'une attaque, l'IDS réagit automatiquement sans l'intervention de l'utilisateur, et bloque directement les intrusions en supprimant les paquets illégitimes. Pour informer l'utilisateur, l'IPS peut aussi remplir un fichier de journalisation qui contiendra la liste des paquets supprimés et éventuellement un message indiquant la raison de cette suppression. [36]

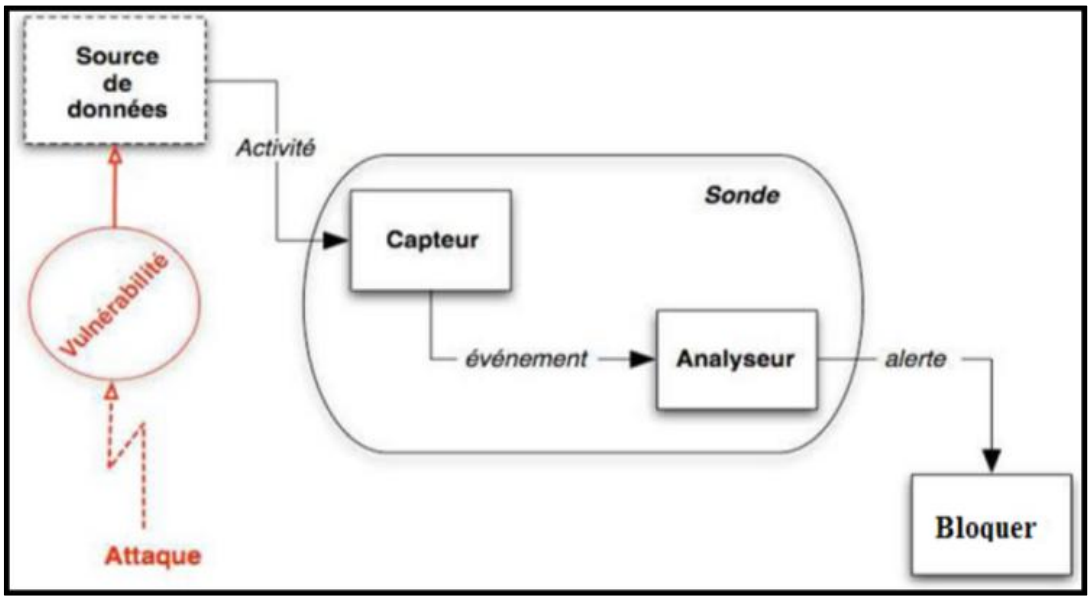


Figure 23 : Architecture fonctionnelle d'un IPS [36]

L'IPS détecte et produit des alertes en raison d'un certain nombre des facteurs qui sont classifiées dans une des limites suivantes : [36]

- ✓ **Vrai positif :** Une situation dans laquelle une signature met le feu correctement quand le trafic intrusif est détecté sur le réseau, ceci représente l'opération normale et optimale.
- ✓ **Faux positif :** Une situation dans laquelle d'utilisation d'une activité normale déclenche une alerte ou une réponse, ceci représente une erreur.
- ✓ **Vrai négatif :** Une situation dans laquelle une signature ne met pas un signe pendant l'utilisation normal de trafic sur le réseau. Aucune activité malveillante. Ceci représente une opération normale et optimale.
- ✓ **Faux négatif :** Une situation dans laquelle le système détection ne détecte pas le trafic intrusif bien qu'il y a une activité malveillante, mais le système de sécurité ne réagit pas, dans ce cas représente une erreur.

III.3.3 Points forts

- ✓ La plupart des logiciels IPS sont multi-plateforme (Linux, FreeBSD, Windows ... etc.).
- ✓ Empêche la transmission des paquets en fonction de ses règles tous comme un pare-feu bloque le trafic en se basant sur les adresses IP.
- ✓ La liberté de création des règles pour les actions à exécuter.
- ✓ Démineur le coût, pour installer plusieurs
- ✓ Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN, IDS, anti-virus, anti-spam, etc.

- ✓ Peut détecter des attaques sur plusieurs différents types des logiciels d'exploitation et d'applications, selon l'ampleur de sa base de données. [36]
- ✓ Un dispositif simple peut analyser le trafic pour une grande échelle des centres serveurs sur le réseau, qui fait au NIPS une bonne solution qui diminue le coût d'entretien et de déploiement.
- ✓ Un simple dispositif peut analyser le trafic et sécurisé un large réseau, qui fais au l'IPS ou NIPS une bonne solution qui diminue le coût d'entretien et le déploiement. [36]

III.3.4 Points faibles

- L'IPS peuvent couper les connexions suspectes ou même, pour une attaque externe, reconfigurer le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Toutefois, il apparaît que ce type de fonctionnalité automatique est potentiellement dangereux car il peut mener à des dénis de service provoqués par l'IDS. Un attaquant déterminé peut, par exemple, tromper l'IDS en usurpant des adresses du réseau local qui seront alors considérées comme la source de l'attaque par l'IDS. Il est préférable de proposer une réaction facultative à un opérateur humain (qui prend la décision finale). [26]
- La consommation des ressources (mémoire, CPU)
- Paralyse le réseau **(Faux positif).**

III.4 La différence entre IDS et IPS

Les IDS et IPS lisent tous les deux les paquets réseau et comparent le contenu à une base de menaces connues. La principale différence entre les deux tient à ce qui se passe ensuite.

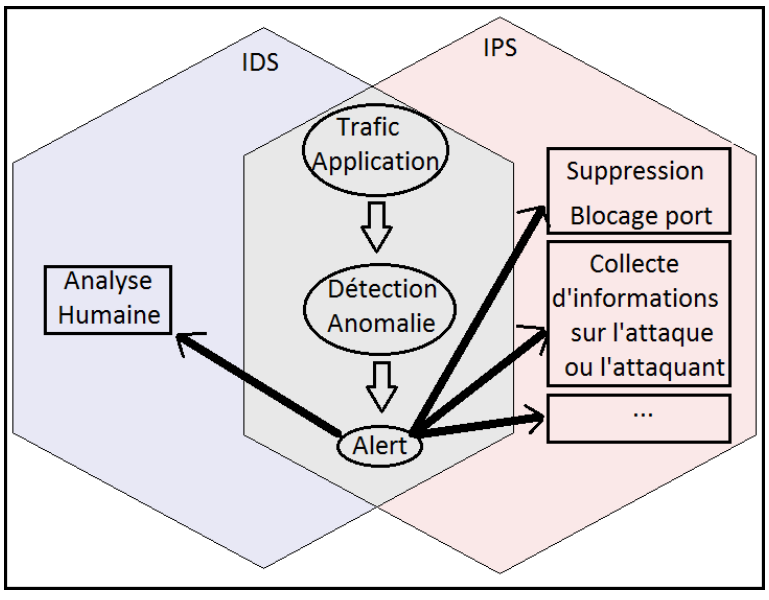


Figure 24 : Différence entre IDS et IPS

IDS	IPS
• Les IDS sont des outils de détection et de surveillance qui n'engagent pas d'action de leur propre fait. • Il est nécessaire qu'un humain ou un autre système prenne ensuite le relais pour examiner les résultats et déterminer les actions à mettre en œuvre, ce qui peut représenter un travail à temps complet selon la quantité quotidienne de trafic généré. • L'IDS ne modifie en aucune façon les paquets réseau.	• Les IPS constituent un système de contrôle qui accepte ou rejette un paquet en fonction d'un ensemble de règles. • L'IDS constitue un très bon outil, qui pourra l'utiliser dans le cadre de ses enquêtes sur les incidents de sécurité. • l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

De nombreux fournisseurs d'IDS/IPS ont intégré de nouveaux systèmes IPS à des pare-feu, afin de créer une technologie appelée **UTM** (*Unified Threat Management*). Cette technologie combine en une seule entité les fonctionnalités de ces deux systèmes similaires. Certains systèmes intègrent dans une même entité les fonctionnalités d'un IDS et d'un IPS. [39]

III.5 Conclusion

Dans ce chapitre, nous avons montré les notions des systèmes de détection et prévention d'intrusions, et leurs architectures, ainsi que leurs fonctionnements. Nous avons compris que les IDS/IPS sont des outils indispensables à la bonne sécurité d'un réseau, et capables de satisfaire les besoins de presque tous les types d'utilisateurs. Comme tous les outils technologiques, les IDS ont des limites et des faiblesses que seule une analyse humaine peut compenser, et les IPS ont des limites et des faiblesses que ne peut pas empêcher toutes les attaques non connues, et ils peuvent paralyser tout un système. Mais avec le temps, ces outils deviennent chaque jour meilleurs grâce à l'expérience acquise.

Chapitre IV : Mise en place et Test

IV.1 Introduction

Nous allons présenter dans ce chapitre, les différentes architectures d'un réseau d'entreprise standard, le choix de l'architecture du réseau à sécuriser, ensuite nous allons présenter les outils utilisés ainsi que les étapes de l'installation et de la configuration de PfSense et Snort. À la fin, nous allons présenter des tests en lançant quelques attaques à partir de divers endroits du réseau et voir l'efficacité du système avec la détection de ces attaques.

IV.2 L'architecture réseau de l'entreprise

Grâce à un réseau informatique d'entreprise, les collaborateurs peuvent accéder à Internet, et partager entre eux des données confidentielles. La mise en place et la configuration du réseau dans une entreprise jouent un rôle fondamental pour la facilité du travail et est une étape essentielle dans la sécurité.

Dans cette partie, nous allons présenter les zones réseaux de l'entreprise, et les sécuriser avec un système de détection d'intrusion Snort qui tourne sur la plateforme PfSense, sur trois types d'architectures différentes.

IV.2.1 Les zones réseaux de l'entreprise

Le réseau standard de l'entreprise est divisée en deux sous réseaux, un réseau local virtuel (LAN), qu'est lui-même divisé en trois sous-réseaux (zones), et le réseau externe WAN (internet), qui lui permet d'échanger des données entre le réseau LAN et l'internet.

IV.2.1.1 Zone WORK

C'est ici où se passe la majorité des travaux de l'entreprise, dans cette zone qui est le cœur de l'entreprise, on trouve des imprimantes, téléphones fixes, postes de travail, ainsi le(s) poste(s) administrateur(s) avec un privilège très haut qui lui permet de contrôler les serveurs de la zone DMZ, les routeurs, firewall, IDS, et presque la totalité du réseau de l'entreprise.

IV.2.1.2 Zone PUBLIC

Ce sont des domaines d'utilisation publics des entreprises comme le foyer, le but de cette zone est de laisser un espace pour les employés afin d'utiliser leurs propres machines (les ordinateurs portables (PC), Smartphones, tablette… etc.) pour un besoin personnel, et c'est pour cela qu'il faut isoler cette zone de la zone WORK pour avoir une bonne sécurité.

IV.2.1.3 Zone DMZ

La zone démilitarisée **(ou en anglais: demilitarized zone)** c'est l'endroit où se trouvent les serveurs (web, vpn, proxy ...etc.), qui sont utilisés pour fournir des services

(Comme: les sites web, proxy, vpn, vps … etc.) aux utilisateurs hors de l'entreprise (hors du réseau LAN), car cette zone est accessible via Internet.

La zone démilitarisée peut-être une méthode de sécurité, car elle joue un rôle d'un pont entre le réseau Internet (WAN) et les autres réseaux locaux de l'entreprise, pour ne pas permettre aux attaquants externes de pénétrer le cœur de l'entreprise comme la zone WORK.

IV.2.1.4 Zone WAN

C'est la zone qui permet d'accéder et partager les données à l'extérieur de l'entreprise, et bénéficier de l'Internet. La connexion dans cette zone est reliée avec des fibres optiques pour avoir un grand débit, et la majorité des entreprises utilisent les fibres ou l'agrégation de plusieurs interfaces réseaux en une interface logique (**Bonding**).

IV.2.2 Architecture centralisée

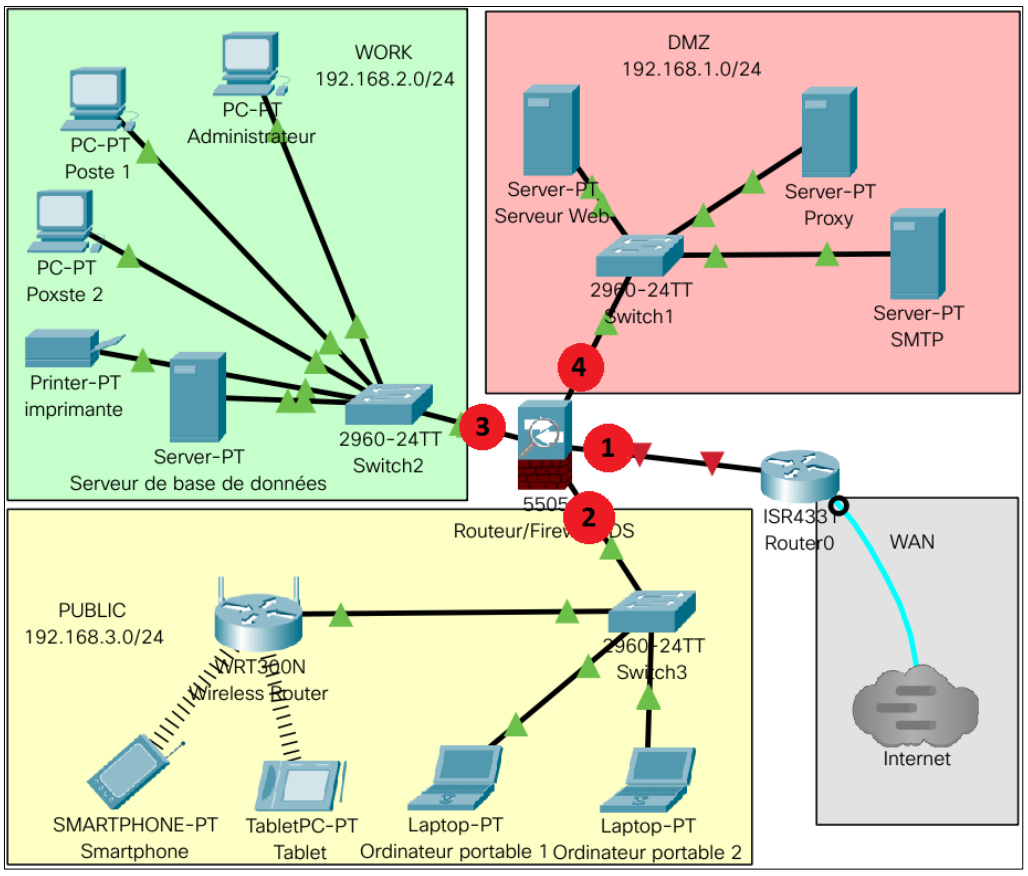


Figure 25 : Architecture centralisée

Comme le montre la **Figure 25,** tous les réseaux locaux (DMZ, WORK et PUBLIC) sont reliés directement à un **serveur de contrôle (nœud central)**, et chaque sous-réseau local est connecté à une des interfaces du nœud central, qui est à son tour connecté à Internet (WAN) via un routeur.

NB : Serveur de contrôle c'est une machine ou ordinateur puissant où on va installer PfSense et leurs services (firewall, routeur et SNORT).

Exemple : **ASA:** (**Adaptive Security Appliance)** la famille de dispositifs de sécurité Cisco protège les réseaux d'entreprises et les centres de données de toutes tailles. Il offre aux utilisateurs un accès hautement sécurisé aux données et aux ressources réseau à tout moment, en tout lieu, en utilisant n'importe quel appareil. (The Cisco ASA Family of security devices protects corporate networks and data centers of all sizes. It provides users with highly secure access to data and network resources - anytime, anywhere, using any device **[31]**).

- **Positionnement des IDS dans l'architecture centralisée :**

  Les cercles rouge sur la figure 25 sont les positions des IDS :

  - **Position (1):** la première idée qui vienne à notre tête, c'est de placer l'IDS dans cette position, elle couvre toute l'architecture, et détecte toutes les attaques frontales. Ainsi, énormément d'alertes seront remontées ce qui va consommer beaucoup de ressource et rendra les logs difficilement consultables.
  - **Position (2):** placer un IDS dans cette position, ne lui permet pas de détecter les attaques frontales, et il couvrira juste la zone PUBLIC, avec moins de consommation de ressources, et son utilité est faible, car ne sécurise pas les zones WORK et DMZ.
  - **Position (3):** l'installation d'un IDS dans cette position, joue un rôle important, car il couvre une zone essentielle, et il va minimiser beaucoup les erreurs humaines (les mauvaises activités involontaires ou intentionnelles des employés).
  - **Position (4):** elle sécurise juste la zone DMZ, et elle ne prend pas en considération le flux qui passe vers la zone PUBLIC et WORK. Dans le sous-réseau DMZ, c'est mieux d'installer un HIDS sur les serveurs que d'utiliser un NIDS, s'il y a un petit nombre de serveurs, car c'est une zone automatisée, ne contient pas des activités humaines.

Existe trois solutions pour équiper cette architecture avec un système de détection d'intrusions pour sécuriser toute l'entreprise:

- Placer une seule sonde, dans la position (1).
- Placer les sondes sur les positions une, deux et trois.
- Placer les sondes sur toutes les positions, qui vont coûter très cher, et satureront le serveur central.

- **Les Avantages de l'architecture centralisée :**
  - La facilité d'installation et la mise en place.
  - Tout le flux entrant et sortant de l'entreprise passe par une seule machine, qui va donner un seul endroit à visiter pour contrôler le flux.
- **Les inconvénients d'architecture centralisée :**
  - Si le nœud central tombe en panne, toute l'architecture tombe en panne.
  - Comme le traitement des paquets nécessite une mémorisation des connexions en cours, il existe des attaques sur ces équipements visant à saturer leur mémoire.
  - Si un attaquant contrôle le nœud central il va avoir entre ses mains le contrôle de toutes les zones (WORK, PUBLIC et DMZ) de l'entreprise.
  - Une bande passante limitée, car le nœud central contrôle tout le trafic.

IV.2.3 Architecture décentralisée

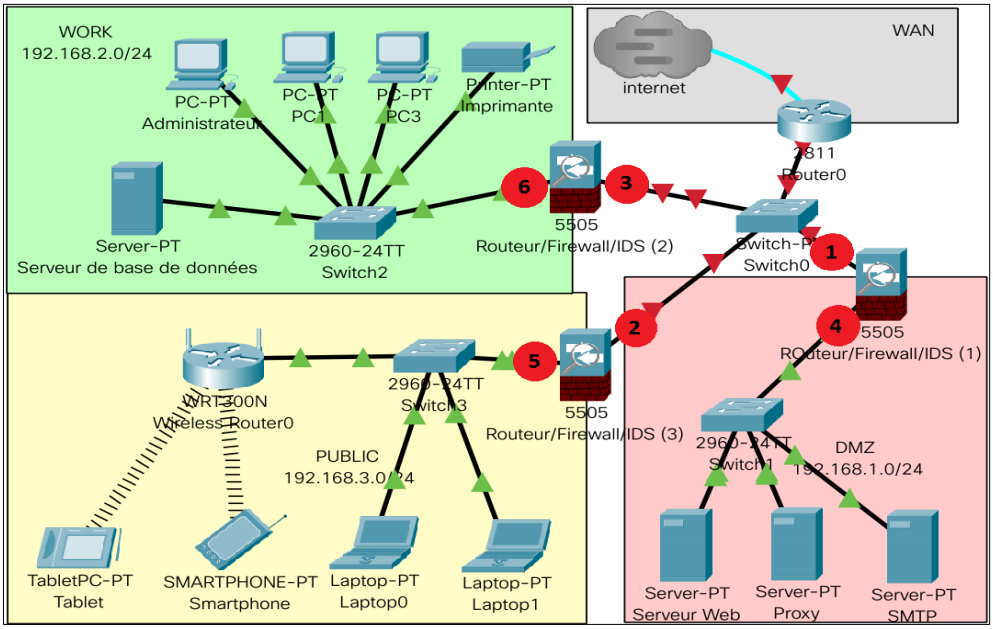


Figure 26 : Architecture décentralisée

Comme le montre la Figure 26. C'est une architecture qui consiste à isoler chaque zone avec son propre serveur de contrôle, et chaque serveur de contrôle est connecté directement au réseau WAN via le même routeur.

- **Positionnement des IDS dans l'architecture décentralisée:**

  Il existe plusieurs endroits stratégiques où il convient de placer un IDS dans cette architecture. Depuis la figure 26:

  - **Position (1):** sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur. Ainsi, beaucoup d'alertes seront remontées ce

qui rendra les logs difficilement consultables, et tout ce travail, c'est pour sécuriser seulement la zone DMZ, et est équivalent à un tiers (1/3) du réseau de l'entreprise.

- **Position (2):** les inconvénients de positionner un IDS dans ce point plus beaucoup que ses avantages, car il produit les mêmes inconvénients que la position (1), et ne couvre pas les zones essentielles de l'entreprise, comme la zone DMZ et WORK.
- **Position (3):** cette position est équivalente à la position (1), sauf que la zone sécurisée ici ce n'est pas la DMZ, mais c'est la zone WORK, où il y a beaucoup d'erreurs humaines.
- **Position (4):** si l'IDS est placé dans la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence, mais nous ne pouvons pas faire un diagnostic sur toutes les menaces qui visent l'entreprise depuis l'extérieur. Les logs seront ici plus clairs à consulter, car les attaques légères ne seront pas enregistrées.
- **Position (5):** cette position ne couvre que la zone PUBLIC, et ne détecte pas les attaques frontales.
- **Position (6):** le positionnement de l'IDS dans la zone WORK, peut rendre compte des attaques internes, provenant du réseau local de l'entreprise. Ce pourrait être une bonne idée de mettre un IDS à cet endroit, étant donné le fait que la majorité des attaques proviennent de l'intérieur. De plus, si des chevaux de Troie (Trojans) ont contaminé la zone WORK, ils pourront être ici facilement identifiés pour être ensuite éradiqués.

Le nombre minimum d'IDS qu'il faut placer dans cette architecture pour sécuriser toutes les zones est trois, et ils fonctionneront à toutes leurs capacités.

- **Les Avantages d'architecture décentralisée :**
  - Diminuer le flux contrôlé (au lieu de surcharger un seul serveur de contrôle par tout le flux, nous décentralisons le flux sur trois serveurs de contrôle).
  - La tolérance aux pannes, si un des trois serveurs de contrôle tombe en panne, le réseau sera rétrogradé, mais ce n'est pas une panne totale.
- **Les inconvénients d'architecture décentralisée :**
  - La difficulté de la mise en place et l'installation.
  - La difficulté de contrôler trois serveurs de contrôle.
  - La redondance des règles de configurations firewall et IDS.
  - Difficile de choisir les bonnes positions pour l'IDS.
  - Positionner plusieurs IDS pour sécuriser toute l'entreprise.

- Un coût élevé pour mettre en place trois serveurs de contrôle, et positionner l'IDS sur toutes les positions.
- Noyade dans toutes les notifications et logs produits par les IDS.
- Les mêmes alertes apparaissent sur la plupart des systèmes de détection d'intrusions.

IV.2.4 Architecture hybride :

C'est une combinaison entre l'architecture centralisée et décentralisée comme le montre la **Figure 27** suivante, tel qu'on décentralise le contrôle de réseau DMZ et les deux réseaux WORK et PUBLIC avec les trois étapes suivantes :

- Mettre en place un **serveur_de_contrôle_1** qui connecte le réseau Internet à la zone démilitarisée (DMZ).
- Nous centralisons les deux zones WORK et PUBLIC qui sont connectées à un autre **serveur_de_contrôle_2** via deux interfaces réseaux.
- Connecter l'interface WAN de **serveur_de_contrôle_2** à la zone démilitarisée, et avoir un accès à ses services, ainsi que l'accès à Internet.

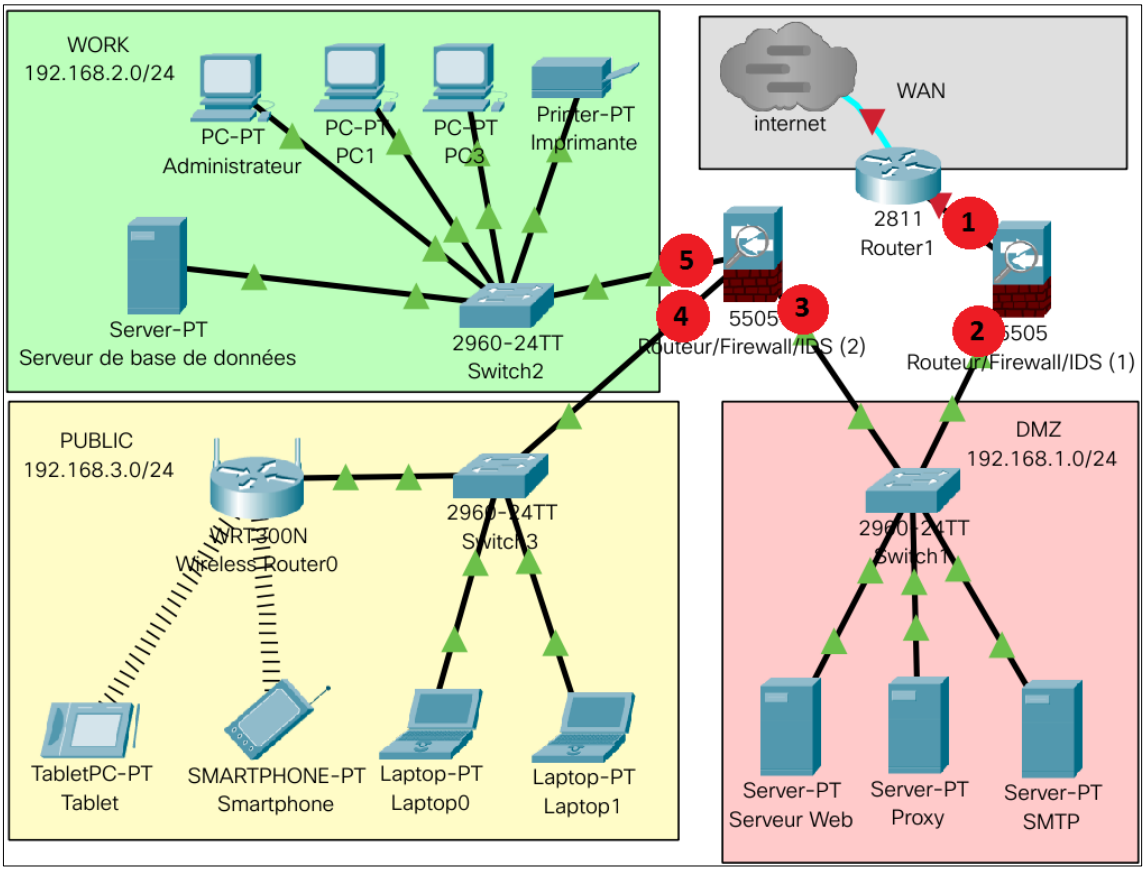


Figure 27 : Architecture hybride

- **Positionnement des IDS dans l'architecture hybride:**

  Il existe plusieurs endroits stratégiques où il convient de placer un IDS dans cette architecture. Depuis la figure 27:

  - **Position (1)**: c'est une position d'entrée de l'entreprise, et est équivalente à la position (1) de l'architecture centralisée.
  - **Position (2)**: placer un IDS sur cette position, il lui permet de capturer toutes les attaques passées par le pare-feu, et sécurise toute l'architecture, même les serveurs de la zone démilitarisée.
  - **Position (3)**: c'est une position proche à la position (2), sauf que ne contrôle pas les menaces destinées vers la zone DMZ, ainsi les menaces qui sortent de cette dernière. Alors c'est mieux de placer l'IDS sur la deuxième position que cette position.
  - **Position (4)**: placer un IDS dans cette position, couvre bien la zone WORK, et ne consomme pas beaucoup de ressources, car le flux entrant analysé, passe par plusieurs barrages (deux pare-feu et les IPS placés dans les positions une deux et trois) et diminue le volume des données.
  - **Position (5):** un IDS placé dans cette position, il lui permet de sécuriser et couvrir la zone PUBLIC, et détecter les données sortantes, potentiellement dangereuses dans le cas où un intrus s'infiltre dans cette zone.

Existe trois solutions pour équiper cette architecture avec un système de détection d'intrusions pour sécuriser toutes l'entreprise :

- Positionner un IDS dans la position (1), qui va générer les mêmes avantages et les inconvénients de la position (1) de l'architecture centralisée.
- Positionner 3 IDS dans les positions (1) (4) et (5), et c'est le bon choix.

- **Les Avantages d'architecture hybride :**
  - Mettre le réseau DMZ au milieu (entre les deux zones WORK et PUBLIC) ajoute un autre mur de sécurité contre les zones WORK et PUBLIC.
  - Tout le flux des deux zones (WORK et PUBLIC) passe par la zone automatisée DMZ, qui va masquer le cœur de l'entreprise (la zone WORK) au réseau WAN pour éviter les attaques directes.
  - Distribuer le flux de contrôle qui va diminuer la surcharge sur les nœuds de contrôle, car le **serveur_de_contrôle_1** ne contrôle que le flux de réseau DMZ et laisse le contrôle de flux des zones WORK et PUBLIC pour le **serveur_de_contrôle_2.**
  - Éviter la redondance des règles de configuration.

- Si le **serveur_de_contrôle_1** tombe en panne, le réseau interne de l'entreprise reste fonctionnel, et si le **serveur_de_contrôle_2** tombe en panne, on va garder les services de domaine DMZ fonctionnels pour les clients qui se trouvent dans le réseau WAN avec le premier **serveur_de_contrôle_1**.
- Seulement deux IDS pour contrôler trois zones, qui vont diminuer le coût par rapport à l'architecture décentralisé.

➢ Les inconvénients d'architecture hybride :

- Un coût de plus par rapport à l'architecture centralisée.
- Si le premier serveur de contrôle tombe en panne, tous le réseau perdent la connexion internet.

IV.3 Présentations des outils utilisés

IV.3.1 VirtualBox

C'est un logiciel libre de virtualisation publié par Oracle sous la licence publique générale GNU version 2, et c'est une solution pour pouvoir exécuter d'autres systèmes d'exploitation sur une seule machine et faire un test d'un réseau réel dans un seul ordinateur, écrit avec les langages **Python**, **assembleur**, **C** et **C++**. Il marche sur les trois plateformes (Linux, Windows, macOS).

IV.3.2 Pfsense

Le projet pfSense est une distribution de pare-feu réseau gratuite, basée sur le système d'exploitation **FreeBSD** avec un noyau personnalisé et comprenant des progiciels gratuits **[32]**

Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des paquets (logiciels) supplémentaires, et désinstaller des paquets et faire d'autres fonctionnalités. Le nom de ce gestionnaire de paquets est **pkg**, et dans pfsense on peut installer les paquets avec une ligne de commande **« pkg install <nom de paquet> »**, ou par la page d'administrateur depuis un navigateur.

Plusieurs services peuvent être gérés par pfSense, et ces services peuvent être arrêtés ou activés depuis une interface graphique. Voici une liste des services proposés par Pfsense :

- VPN client PPTP, VPN site à site OpenVPN et IPSec.
- Gestion des VLAN.
- Filtrage d'URL.
- Serveur DHCP.

- Partage de bande passante Traffic Shaper (régulation de flux est le contrôle du volume des échanges sur un réseau informatique dans le but d'optimiser ou de garantir les performances).
- Répartition de charge avec répartition de charge (LoadBalancer).
- IDS-IPS Snort.

IV.3.3 LOIC

Low **O**rbit **I**on **C**annon (**LOIC**), qui peut être traduit par « canon à ion en orbite basse » est un outil de pression réseau open source, écrit en C#. LOIC est basé sur le projet LOIC de Praetox. **LOIC** est à des fins éducatives uniquement, destiné à aider les propriétaires de serveurs à développer une attitude de «défense contre les pirates». Cet outil est livré sans aucune garantie. « Vous ne pouvez pas utiliser ce logiciel à des fins illégales ou contraires à l'éthique. Cela comprend les activités qui donnent lieu à une responsabilité pénale ou civile. En aucun cas, le concédant ne sera responsable des activités ou des méfaits du licencié. » [41]

LOIC est une application de test de réseau, cette application tente d'attaquer par déni de service (**Dos**), le site ciblé en inondant le serveur avec des paquets TCP ou des paquets UDP.

IV.3.4 Snort

IV.3.4.1 Définition de Snort

Snort est un hybride d'IPS et d'IDS utile et efficace, et est un projet Open Source le plus avancé au monde. Il utilise une série de règles qui aident à définir l'activité réseau malveillante et utilise ces règles pour trouver les paquets qui leur correspondent à eux et génère des alertes pour les utilisateurs. Il peut également être déployé en ligne pour arrêter ces paquets [33]. Snort peut être téléchargé et configuré pour une utilisation personnelle et professionnelle, c'est un outil multi-plateformes (Linux, Windows, FreeBSD).

Snort a trois utilisations principales:

- un renifleur de paquets comme tcpdump.
- un enregistreur de paquets - ce qui est utile pour le débogage du trafic réseau.
- un système de prévention des intrusions réseau à part entière.

IV.3.4.2 Fonctionnement de Snort

Le fonctionnement de Snort, consiste à passer les données par 4 blocs, qui ont des rôles complémentaires décrits comme suit :

- Bloc 1 (sniffer de paquets) : consiste d'intercepter toutes les trames qui circulent sur le réseau, et les lire avec un décodeur qui se base sur la librairie "libpcap".
- Bloc 2 (préprocesseur) : il peut repérer les malformations, anomalies… etc. et les réparer.
- Bloc 3 (moteur de détection) : il se base sur les flux normalisés et réassemblés pour repérer d'éventuelles.
- Bloc 4 (les événements) : sont inscrits (logs au format unifié, BDD… etc.).

Snort utilise des règles dans leur moteur de détection, pour reconnaître les intrusions. Nous pouvons télécharger ces règles prédéfinies via le site officiel, ou programmer nos propres règles, via un langage simple et léger de description, qui est flexible et assez puissant. [38]

- **La structure des règles :** Les règles de Snort doivent être écrites sur une seule ligne, car l'analyseur de règles de Snort ne sait pas comment traiter des règles sur plusieurs lignes. Les règles Snort sont divisées en deux sections logiques :
  - La section entête de règle : contient l'action de la règle (alert, log, pass…etc), le protocole, les adresses IP source et destination avec les masques réseau, et les ports source et destination.
  - La section options de la règle : contient les messages d'alerte et les informations sur les parties du paquet qui doivent être inspectés pour déterminer si l'action de la règle doit être acceptée. Voici une règle d'exemple :

```
alert tcp any any -> 193.194.82.178/20 3036 (content:"|00 01 86 a5|"; msg:
"mountd access";)
```

- **Les entêtes de règle :** L'entête de règle contient l'information qui définit le "qui, où, et quoi" d'un paquet. Nous trouvons dans l'entête :
  - **L'action de règle :** c'est le premier élément dans l'entête. L'action de règle dit à Snort quoi faire quand il trouve un paquet qui correspond aux critères de la règle. Il y a cinq actions accessibles par défaut dans Snort :
    - alert - génère une alerte.
    - log - journalise le paquet.
    - pass - ignore le paquet.
    - activate – active une autre règle dynamique (dynamic).
    - Dynamic – reste passive jusqu'à être activée par une règle activate.
  - **Les protocoles :** spécifier le protocole à analyser (TCP, UDP, ICMP, ARP...ect).

- **La section des adresses :** s'occupe comme information de l'adresse IP et le masque de réseau, pour une règle donnée. Le mot clé "any" peut être utilisé pour définir n'importe quelle adresse.
- **Les numéros de ports :** les numéros de port peuvent être spécifiés en plusieurs façons représentées comme suit : [38]

log udp any any -> 192.168.1.0/24 1:1024 journalise le trafic udp provenant de tout port et à destination de ports dans l'intervalle de 1 à 1024
log tcp any any -> 192.168.1.0/24 :6000 journalise le trafic tcp depuis tout port et allant vers les ports inférieurs ou égaux à 6000
log tcp any :1024 -> 192.168.1.0/24 500: journalise le trafic tcp depuis les ports privilégiés inférieurs ou égaux à 1024 allant vers les ports supérieurs ou égaux à 500
log tcp any any -> 192.168.1.0/24 !6000:6010 journalise le trafic udp provenant de tout port et à destination tout port sauf l'intervalle de 6000 à 6010

- **Les variables :** Ce sont de simples substitutions des variables fixées avec le mot clé var, et sa structure est : var <nom de variable> <valeur de variable>.

Voici un exemple d'une variable :

```
var Mon_Reseau [192.168.3.0/10.5.32.0/22]
```

Ces règles peuvent être modifiées de plusieurs façons. Nous pouvons définir des méta-variables en utilisant l'opérateur "$". Celles-ci peuvent être utilisées avec les opérateur de modification de variables, "?" et "-".

- "$var" défini la méta-variable.
- "$(var)" replace avec le contenu de variable "var".
- "$(var:-défaut)" remplace avec le contenu de variable "var" ou avec "défaut" si "var" est indéfini.
- "$(var:?message)" remplace avec le contenu de la variable "var » ou affiche le message d'erreur "message" et quitter.

Voici un exemple d'une variable :

```
var MY_NET $(MY_NET:-192.168.1.0/24)
```

```
log tcp any any -> $(MY_NET:?MY_NET is undefined!) 23
```

- **Les inclusions :** Le mot clé include permet à d'autres fichiers de règles d'être inclus dans le fichier de règles indiqué sur la ligne de commande. Format :

```
include: <répertoire/nom du fichier include>
```

- **Options de règle générale**
  - **msg :** indique au moteur de journalisation le message à imprimer avec un vidage de paquets. C'est une simple chaîne de texte qui utilise le \ comme caractère d'échappement pour indiquer un caractère discret.
  - **reference :** Le mot-clé reference permet aux règles d'inclure des références à des systèmes d'identification d'attaques externes. Le plugin prend actuellement en charge plusieurs systèmes spécifiques ainsi que des URL uniques. Ce plugin doit être utilisé par les plugins de sortie pour fournir un lien vers des informations supplémentaires sur l'alerte produite. [42]
  - **sid :** Le mot-clé sid est utilisé pour identifier de manière unique les règles de Snort. Ces informations permettent aux plugins de sortie d'identifier facilement les règles.
  - **threshold :** peut être inclus dans le cadre d'une règle ou vous pouvez utiliser des threshold autonomes faisant référence au générateur et au SID auxquels ils sont appliqués. Par exemple, une règle pour détecter un trop grand nombre de tentatives de mot de passe de connexion peut nécessiter plus de 5 tentatives. Dans le threshold nous trouvons quatre paramètres (**type, track, count** et seconds**)** et leur format est : threshold : **type** <limit|threshold|both>**, track** <by_src|by_dst>**, coutn** <c>**, seconds** <s>**;**

Options	description
type limit|threshold|both	- **limit** : Lance des alertes pour les **c** premiers évènements pendant l'intervalle de temps, puis ignore les événements pour le reste de l'intervalle de temps - **threshold :** lance les alertes toutes les **c** fois que nous voyons cet événement pendant l'intervalle de temps.

	- **Both** : Saisissez les deux alertes une fois par intervalle de temps après avoir vu **c** occurrences de l'événement, puis ignorez tout événement supplémentaire pendant l'intervalle de temps.
track by_src|by_dst	le débit est suivi soit par l'adresse IP source, soit par l'adresse IP de destination. Cela signifie que le nombre est maintenu pour chaque adresse IP source unique ou pour chaque adresse IP de destination unique. Les ports ou toute autre chose ne sont pas suivis.
count c	nombre de règles correspondant en **s** secondes qui entraîneront le dépassement de la limite *event_filter*. **c** doit être une valeur différente de zéro.
seconds s	période de temps (en secondes) sur laquelle le compte est accumulé. **s** doit être une valeur différente de zéro.

IV.3.5 Nmap

Nmap (Network Mapper) est un outil open source d'exploration réseau et d'audit de sécurité. Il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique. Nmap innove en utilisant des paquets IP bruts (raw packets) pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques. Nmap est généralement utilisé pour les audits de sécurité, mais de nombreux gestionnaires des systèmes et de réseau l'apprécient pour des tâches de routine comme les inventaires de réseau, la gestion des mises à jour planifiées ou la surveillance des hôtes et des services actifs [34].

Nmap c'est un outil populaire et multi plateformes (Linux, Windows, macOS, FreeBSD, NetBSD, OpenBSD, Solaris), et marche avec des lignes de commandes (avec terminal sous Linux ou CMD pour la plateforme Windows) qui donne une difficulté d'utilisation pour les utilisateurs qui n'aiment pas les lignes de commandes, c'est à cause de

ce problème que les développeurs de Nmap ont créé une interface graphique d'utilisateur (GUI: graphical user interface).

IV.4 Mise en place

IV.4.1 Choix de l'architecture

Nous avons présenté les trois architectures standard de l'entreprise (centralisé, décentralisé, hybride), et comme notre thème est basé sur la sécurité et la mise en place de notre système de détection d'intrusions IDS, nous avons opté pour l'architecture hybride à cause de ses avantages sur la sécurité.

Le but de cette architecture hybride est de gagner les avantages des autres architectures mentionnées dans la partie (**IV.2)**, et avec cet emplacement (centraliser les zones WORK et PUBLIC avec un seul serveur de contrôle, et isoler le réseau DMZ avec son propre serveur de contrôle) nous pouvons diminuer les inconvénients, et ajouter d'autres avantages.

Parmi les avantages de cette architecture par rapport aux autres architectures, est de faire passer le flux entrant par plusieurs barrières de sécurité, pour un meilleur filtrage. Comme le montre la figure suivante :

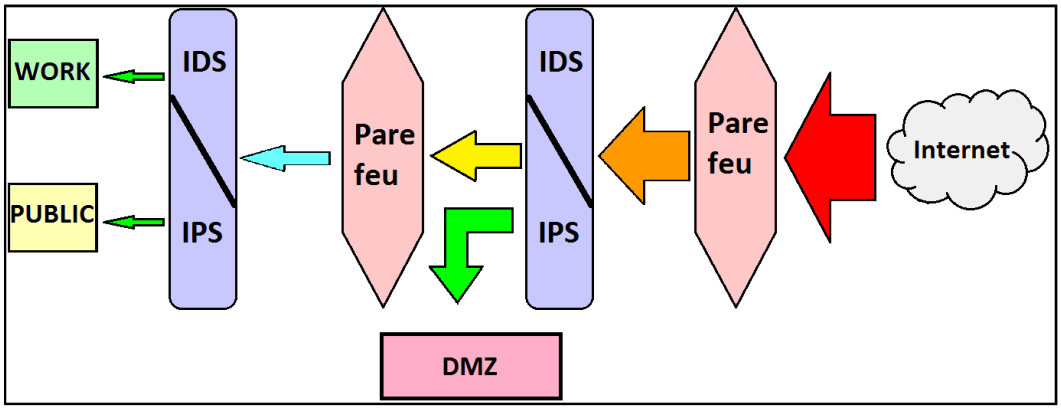


Figure 28 : Topologie de l'architecture hybride

Le principe de cette architecture est d'installer quatre barrières de sécurité obligatoires (deux pare-feu et deux IDS/IPS), et une autre optionnelle (passer le trafic par un Proxy ou un vpn), comme le montre la figure suivante :

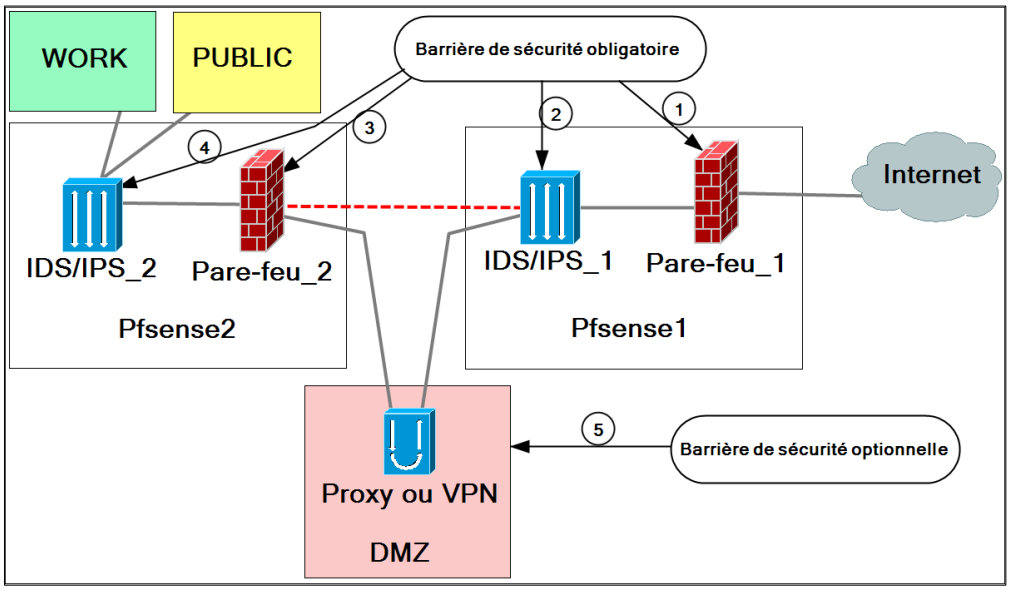


Figure 29 : Structure interne du réseau hybride

Comme le montre la figure précédente, toutes les communications qui circulent entre le réseau Internet et les deux zones (WORK et PUBLIC), passe obligatoirement par quatre points de contrôle qui sont placés en série, et qui ont des rôles complémentaires décrits comme suit :

- **Barrière 1 :** la configuration de **pare-feu_1**, permet le passage des requêtes SYN de synchronisations entrantes, et bloque les paquets et domaines indésirables selon la politique de chaque entreprise, il permet cela de réduire le volume du trafic entrant, et faciliter l'analyse du flux de données sur la prochaine barrière, et d'éviter la surcharge sur le serveur.
- **Barrière 2 :** après avoir franchi la première barrière et réduire le volume des données, dans cette deuxième barrière où l'IDS/IPS intervient, dont son rôle est d'analyser le flux reçu à partir de la première barrière, en comparant les paquets réseau à une base de données de *cybermenaces*, et de bloquer les paquets potentiellement dangereux, en réduisant ainsi le volume du trafic une deuxième fois pour la prochaine barrière.
- **Barrière 3 :** dans cette barrière, nous trouvons le **pare-feu_2** qui protège les zones inaccessibles via Internet (WORK et PUBLIC), et avec sa configuration qui lui permet aussi de bloquer les requêtes (SYN), qui ont traversé le **Pare-feu_1**, et destinées à pénétrer les zones (WORK et PUBLIC), plus d'autres paquets selon la configuration des besoins de l'entreprise, cela réduit le flux une troisième fois pour la prochaine barrière.

- **Barrière 4** : une dernière barrière qui protège les deux zones WORK et PUBLICE des menaces Internet, et aussi considéré comme la première barrière contre les attaques qui proviennent de la zone PUBLIC, dans le cas où un intrus s'infiltre dans cette zone.

Toutes les alertes et les notifications produites par les deux IDS, sont transférées vers la machine de l'administrateur situé dans la zone du travail (WORK).

Selon la politique de l'entreprise, une simple configuration d'un Proxy ou un VPN dans la zone DMZ, elle permet d'ajouter une cinquième barrière de sécurité considérée comme optionnelle :

- **Barrière 5 :** son rôle est de sécurité et surveiller les échanges des données entrantes et surtout sortantes.

IV.4.2 Installation et configuration de Pfsense

Avant de lancer l'installation et la configuration des outils, nous présentons ci-dessous la configuration théorique de notre réseau virtuel :

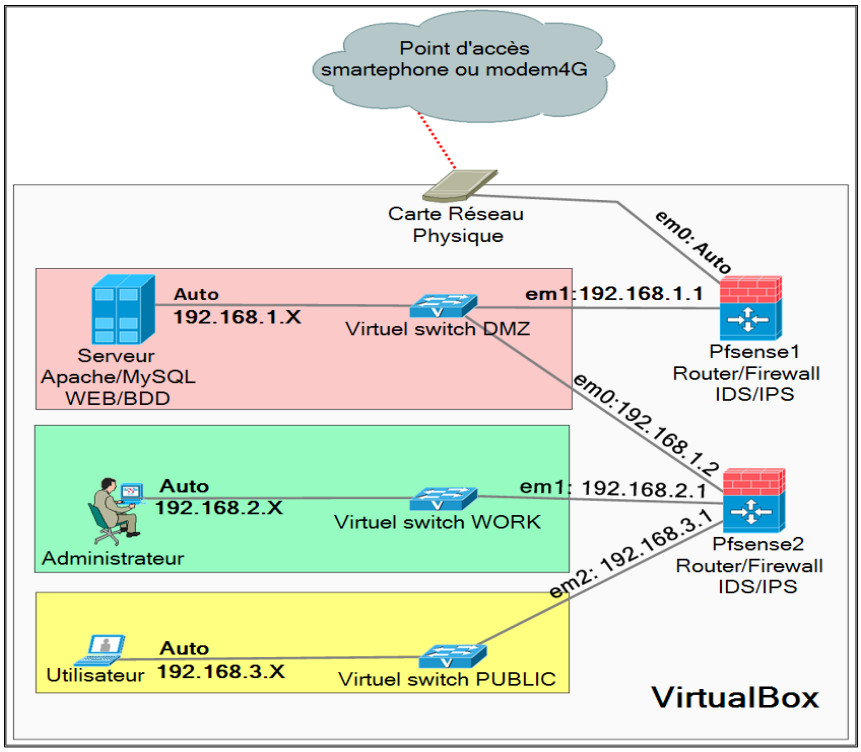


Figure 30 : Configuration du réseau virtuel

- En réalité l'adresse **IP** de l'interface **em0** de **Pfsense1**, c'est l'adresse publique fournie par le **ISP**, et dans notre test le ISP c'est la machine physique (faire un pont entre em0 de Pfsense1 et l'interface de la machine physique.

- L'adresse réseau de la zone démilitarisée (DMZ) est 192.168.1.0/24, et une passerelle (192.168.1.1) attribuée à l'interface **em1** de **Pfsense1**, et le serveur DHCP de cette zone est installé sur le **pfsense1**.
- L'adresse réseau de la zone WORK est 192.168.2.0/24, et une passerelle (192.168.2.1) attribuée à l'interface **em1** de **Pfsense2**.
- L'adresse du réseau la zone PUBLIC est 192.168.3.0/24, et une passerelle (192.168.3.1) attribuée à l'interface **em2** de **Pfsense2**.
- L'adresse **IP** de l'interface **em0** de **Pfsense2** est attribuée automatiquement par le serveur DHCP de la zone DMZ.
- serveur DHCP des deux zones WORK et PUBLIC, est installé sur le **Pfsense2**.
- Installer une machine virtuelle **Debian** dans la zone DMZ qui va jouer le rôle des serveurs **WEB** et **BDD** (base de données) avec les services **NGINX** et **MySQL**.

IV.4.2.1 Installation de Pfsense

La première étape, est de télécharger le fichier ISO et nous choisissons la bonne l'architecture du fichier depuis le site officiel (**https://www.pfsense.org/download/**), dans notre test nous allons utiliser l'architecture AMD64 (64 bits).

Après avoir téléchargé le fichier nous lançons le Virtualbox et suivons les étapes suivantes pour installer le **Pfsense1**:

- ✓ Créer une nouvelle machine du type **BSD** et version FreeBSD (64 bits).
- ✓ Ajouter le fichier téléchargé de Pfsense comme CD de boot.
- ✓ Dans l'onglet réseau (Networks), nous activons deux adaptateurs réseaux, attacher le premier à une interface réseau physique avec l'option adaptateur avec pont (**Bridged Adapter**), et pour le deuxième adaptateur on sélectionne réseau interne (**internal network**) avec le nom DMZ, après nous lançons la machine et nous choisissons les étapes par défaut.

Les étapes d'installation de deuxième Pfsense1 sont les mêmes, sauf que dans l'onglet réseau nous activons trois adaptateurs réseaux, nous attachons le premier adaptateur au réseau interne DMZ, le deuxième au réseau WORK, et le troisième au réseau PUBLIC.

IV.4.2.2 Configuration de Pfsense1 et Pfsense2

À la fin de l'installation et le lancement de **Pfsense1** et **Pfsense2**, la première chose que nous devons faire est de configurer les interfaces réseau des deux serveurs. Depuis la console de **Pfsense1**, nous choisissons l'option numéro 2 (**Set interfaces ip address**) et nous

sélectionnons l'interface réseau numéro 1 (**em0**) et nous acceptons la configuration IP via le **DHCP**.

Avec la même option, nous sélectionnons l'interface numéro 2 (**em1**) pour configurer le sous-réseau DMZ avec une adresse IP (192.168.1.1) pour l'interface **em1** comme une passerelle ce réseau DMZ, et donner l'intervalle [192.168.1.3, 192.168.1.30] des adresses IP pour le DHCP.

Figure 31 : configuration les l'interfaces em0 et em1 de Pfsense1

Depuis la console de **Pfsense2**, nous choisissons l'option numéro 2 pour voir les trois interfaces (em0, em1 et em2) et suivons ces étapes pour les configurer:

- Sélectionner l'interface numéro 1 (em0), et donner l'adresse IP 192.168.1.2 avec un masque réseau 24, et la passerelle 192.168.1.1 (interface em0 de Pfsense1).
- Sélectionner l'interface numéro 2 (em1), et donner l'adresse IP 192.168.2.1 comme passerelle pour le réseau WORK et masque réseau 24, et un intervalle [192.168.2.2 – 192.168.2.30] des adresses IP pour le DHCP.
- Sélectionner l'interface numéro 3 (em3), et donner l'adresse IP 192.168.3.1 comme une passerelle pour le réseau PUBLIC, et un intervalle [192.168.3.2 – 192.168.3.30] des adresses IP pour le DHCP.

Figure 32 : Configuration les l'interfaces em0, em1, em2 de Pfsense2

Accéder à l'interface web en entrant l'adresse IP du côté LAN de Pfsense dans un navigateur sur la machine de l'administrateur, dans notre cas : 192.168.2.1 pour Pfsense1 et 192.168.1.1 pour Pfsense2. Dont les identifiants sont (**admin, pfsense**).

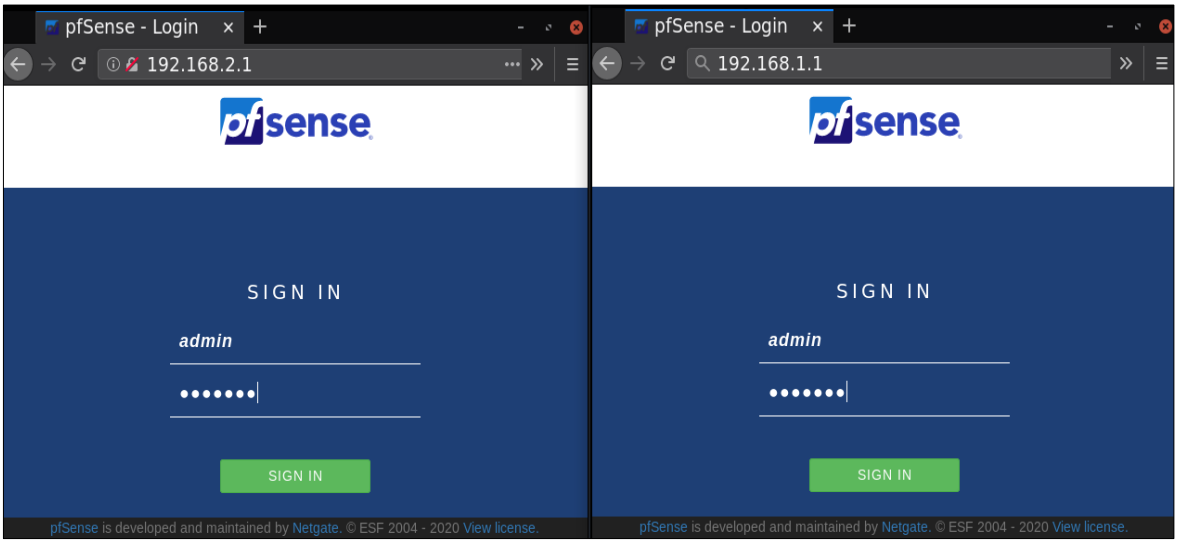


Figure 33 : L'interface web de Pfsense

Pour rendre la zone DMZ accessible via le réseau externe, nous devons configurer la table NAT sur le Pfsense1. Ouvrez les ports sur l'interface WAN et associez-les à l'adresse de serveur. Dans notre cas, l'adresse du serveur est 192.168.1.3.

Règles

	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
☐	WAN	TCP	*	*	WAN address	10 - 60000	192.168.1.3	10 - 60000		

Figure 34 : Configuration de la table NAT

IV.4.3 Installation et configuration de Snort sous Pfsense

IV.4.3.1 Installation de Snort

Nous pouvons installer snort sur les deux serveurs de contrôle (Pfsense1 et Pfsense2) avec la ligne de commande « **pkg install pfSense-pkg-snort** », ou avec l'interface graphique du navigateur sur la machine de l'administrateur dans la zone WORK, on utilise l'adresse 192.168.1.1 pour le Pfsense1, et 192.168.2.1 pour le Pfsense2, et allez vers (Système → Gestionnaire de paquets → Paquets disponibles → Install).

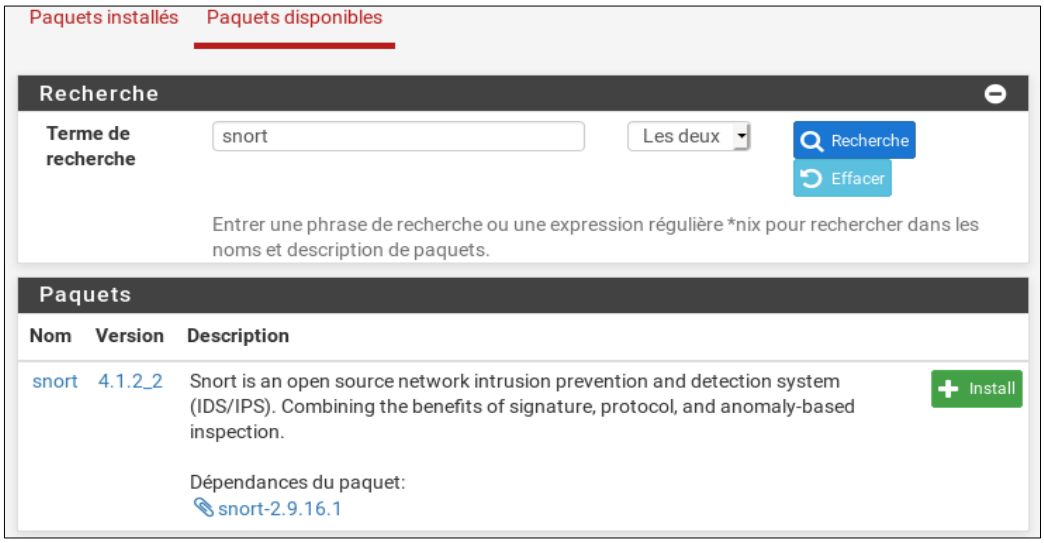


Figure 35 : Installation des paquets de SNORT

IV.4.3.2 Configuration de Snort

Snort utilise des règles pour effectuer ses analyses. Pour utiliser ces règles, nous avons procédé par la création d'un compte sur https://www.snort.org/users/sign, afin de pouvoir récupérer le code Oinkcode pour prédéfinir ses règles en temps voulu.

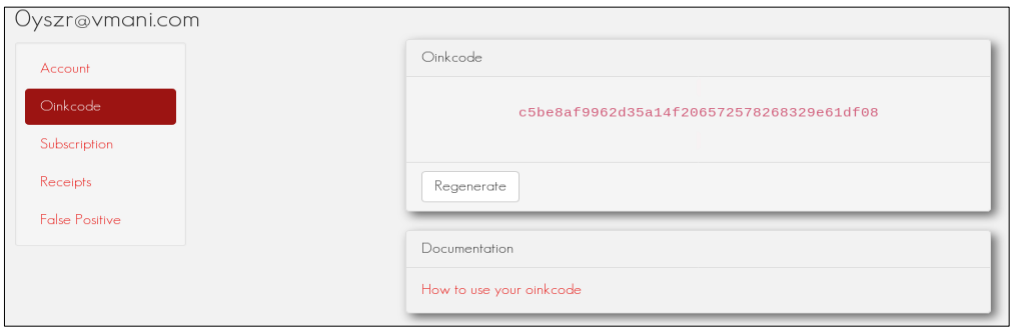


Figure 36 : Code Oinkcode délivré après inscription sous Snort

Allons ensuite dans l'onglet **Services>Snort<Global Settings** sur le premier pfsense, et nous collons le code Oinkmaster après l'acivation de **Snort VRT**, en suite activer **GPL2** (une liste de règles de certifié et distribué gratuitement sans aucune restriction de licence d'abonné snort), **OpenAppID** (plugin de sécurité réseau pour la couche application), et modifier que ce qui est nécessaire :

Figure 37 : La configuration de l'importer les règles de Snort

Nous validons, ensuite nous lançon la mise à jour depuis l'onglet « Updates ».

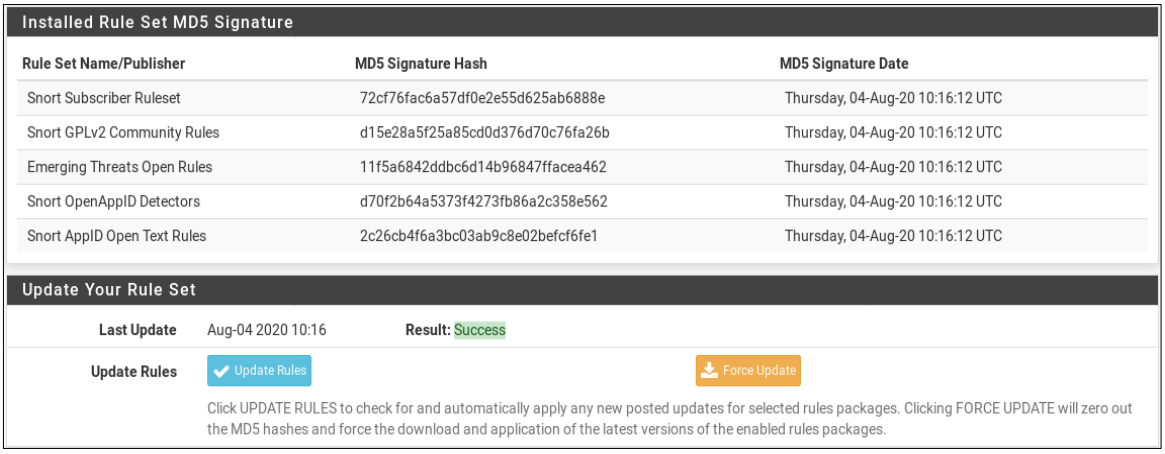


Figure 38 : Télécharger les règles de Snort

Nous passons maintenant à la configuration des interfaces sur Pfsense1 et Pfsense, qui seront les capteurs de Snort, dans l'onglet Services>Snort>Interface>Snort Interfaces, et nous sélectionnons l'interface LAN (em1), et nous activons l'option Search Optimize pour optimiser les performances dans la détection.

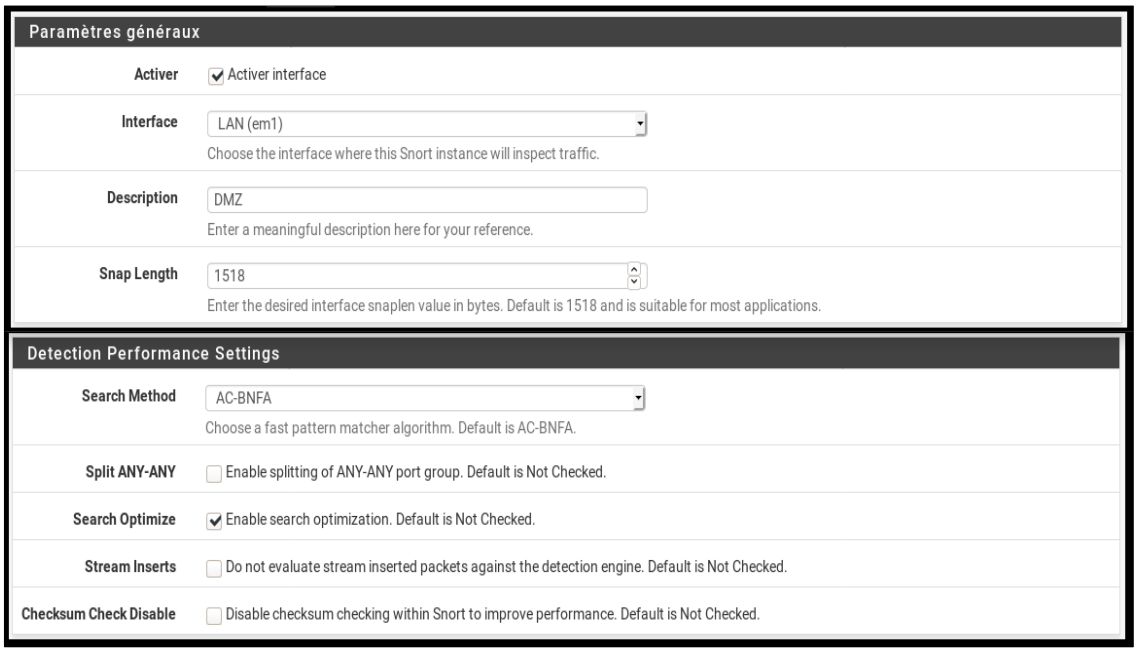


Figure 39 : Activation de l'interface em1 sur Pfsense1

Nous suivons les mêmes étapes pour configurer les deux interfaces (em1 et em2) de Pfsense2, comme le montre la figure suivante :

Figure 40 : Activer les interfaces em1 et em2 sur Pfsense2

La configuration des interfaces est désormais terminée. Maintenant nous passons à la programmation des règles, pour détecter les attaques **Dos** produites par l'outil **LOIC** et le **scanne** avec **Nmap,** pour saisir ces règles, on va dans l'onglet **Snort Interfaces -> LAN**

Règles sur le **pfsense1**, et nous choisissons **custom.rules** de la liste **Category Selection,** et nous écrivons les règles suivantes :

alert tcp $EXTERNAL_NET any -> $HOME_NET any (**msg**:"une attaque DOS"; **flags**:S threshold:type both, **track** by_src, **count** 180, **seconds** 60; sid:15031996; rev:1;)	Quand cette règle détecte 180 tentatives (**count 180**) de demandes de connexion (**flags:S**) depuis une seule machine source (**track by_src**) pendant une durée de 60 secondes (**seconds 60**) (l'équivalent de 3 tentatives/s), elle lancera une alerte avec un message « une attaque DOS » (msg:"une attaque DOS").
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (**msg**:"ET SCAN Suspicious inbound to mySQL port 3306"; **flow**:to_server; **flags**:S; threshold: type limit, **count** 5, **seconds** 60, **track** by_src; reference:url,doc.emergingthreats.net /2010937; classtype:bad-unknown; sid:2010937; rev:3; metadata:created_at 2010_07_30, former_category HUNTING, updated_at 2018_03_27;)	Cette règles tirée de la librairie de Snort, et elle détecte les requêtes suspectes le scanne le port 3306 (le port utilisé par le servcie mySQL) **($HOME_NET 3306**), on suit les 5 tentatives (**count 5**) de connexion (**flags:S**) de l'adresse source (**track by_src**) vers le serveur (**flow:to_server**) pendant une durée de 60 secondes (**seconds 60**), et lancer une alerte avec le message « ET SCAN Suspicious inbound to mySQL port 3306 » (**msg**:"ET SCAN Suspicious inbound to mySQL port 3306").

alert tcp $EXTERNAL_NET any -> $HOME_NET 5432 (msg:"ET SCAN Suspicious inbound to PostgreSQL port 5432"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; reference:url,doc.emergingthreats.net/2010939; classtype:bad-unknown; sid:2010939; rev:3; metadata:created_at 2010_07_30, former_category HUNTING, updated_at 2018_03_27;)	Cette règle tirée de la librairie de Snort, et elle détecte les requêtes suspectes le scanne le port 5432 (le port utilisé par PostgreSQL)
alert tcp $EXTERNAL_NET any -> $HOME_NET 1433 (msg:"ET SCAN Suspicious inbound to MSSQL port 1433"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; reference:url,doc.emergingthreats.net/2010935; classtype:bad-unknown; sid:2010935; rev:3; metadata:created_at 2010_07_30, former_category HUNTING, updated_at 2018_03_27;)	Cette règles tirée de la librairie de Snort, et elle détecte les requêtes suspectes le scanne le port 1433 (le port utilisé par MSSQL)
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820	Cette règles tirée de la

(msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5; metadata:created_at 2010_07_30, updated_at 2010_07_30;)	librairie de Snort, et elle détecte les requêtes suspectes le scanne les ports [5800-5820] (les ports utilisés par VNC <Virtual Neetwork Computing>)
alert tcp $EXTERNAL_NET any -> $HOME_NET 1521 (msg:"ET SCAN Suspicious inbound to Oracle SQL port 1521"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; reference:url,doc.emergingthreats.net/2010936; classtype:bad-unknown; sid:2010936; rev:3; metadata:created_at 2010_07_30, former_category HUNTING, updated_at 2018_03_27;)	Cette règles tirée de la librairie de Snort, et elle détecte les requêtes suspectes le scanne le port 1521 (le port utilisé par Oracle SQL)

Pour les règles des interfaces sur Pfsense2, nous changeons juste :

- Sur la sonde position 4 de notre architecture hybride (voir la figure 27), la variable **$EXTERNAL_NET** avec 192.168.3.0/24 (le réseau de la zone PUBLIC), et la variable **$HOME_NET** avec 192.168.1.0/24 (le réseau de la zone DMZ).
- Sur la sonde position 5 de notre architecture hybride (voir la figure 27), la variable **$EXTERNAL_NET** avec 192.168.3.0/24 (le réseau de la zone PUBLIC), et la variable **$HOME_NET** avec 192.168.2.0/24 (le réseau de la zone DMZ).

EXEMPLE :

- alert tcp 192.168.3.0/24 any -> 192.168.1.0/24 any 3306 (**msg**:"ET SCAN Suspicious inbound to mySQL port 3306"; ……
- alert tcp 192.168.3.0/24 any -> 192.168.2.0/24 any 3306 (**msg**:"ET SCAN Suspicious inbound to mySQL port 3306";……

IV.5 Test

Dans cette section, nous allons lancer deux types attaques (attaque active "**Dos"** utilisant l'outil **LOIC** et attaque passive "**scanne"** utilisant l'outil **Nmap)**, de deux endroits différents (zone WAN et zone PUBLIC), comme le montre la figure ci-dessous :

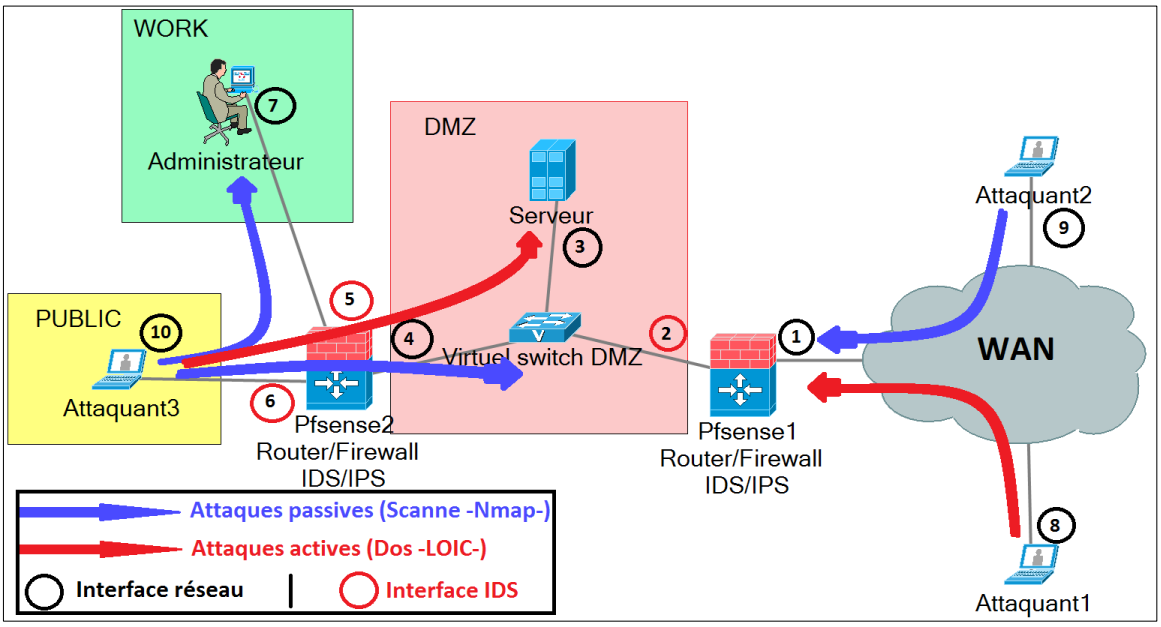


Figure 41 : Maquette d'attaque active (Dos) et passive (Scan)

Les cercles dans la figure 41, sont les interfaces réseau des machines, et pour chacune de ces interfaces a une adresse IP. Comme le montre dans le tableau suivant :

ID	IP	Description
1	10.5.2.88	L'adresse IP de l'interface réseau **em0** de Pfsense1.
2	192.168.1.1	L'adresse IP de l'interface réseau **em1** de Pfsense1 (passerelle de la zone DMZ), capteur de IDS/IPS (1).
3	192.168.1.3	L'adresse IP de L'interface réseau de serveur (mySQL, Nginx, …)
4	192.168.1.2	L'adresse de l'interface réseau **em0** de Pfsense2.
5	192.168.2.1	L'adresse IP de l'interface réseau **em1** de Pfsense2 (passerelle de la zone WORK), capteur (1) de IDS/IPS (2).
6	192.168.3.1	L'adresse IP de l'interface réseau **em2** de Pfsense2 (passerelle de la zone PUBLIC), capteur (2) de IDS/IPS (2).
7	192.168.2.10	L'adresse IP de l'interface réseau de l'ordinateur **Administrateur**.
8	10.5.2.89	L'adresse IP de l'attaquant1
9	10.5.2.90	L'adresse IP de l'attaquant2
10	192.168.3.3	L'adresse IP de l'attaquant3

IV.5.1 Test de l'attaque active Dos

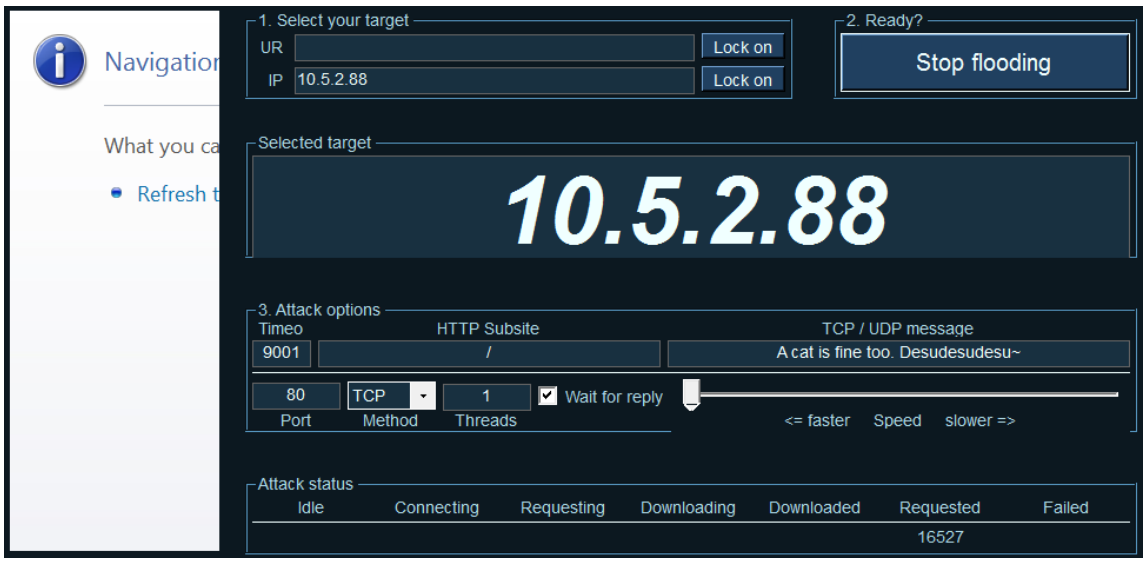


Figure 42 : Attaque Dos via la zone WAN par l'attaquant1

3 Entries in Active Log

Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description
2020-11-17 15:48:10	⚠	0	TCP		10.5.2.89	49217	192.168.1.3	80	1:15031996	une attaque DOS

Figure 43 : Détection de l'attaque Dos de l'attaquant1 par IDS 1

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Supprimer
1	10.5.2.89	(http_inspect) PROTOCOL-OTHER HTTP server response before client request -- 2020-11-17 15:48:10 (http_inspect) UNKNOWN METHOD -- 2020-11-17 15:48:10 une attaque DOS -- 2020-11-17 15:48:10	✖

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

Figure 44 : Blocage de l'adresse IP de l'attaquant1 par IPS 1

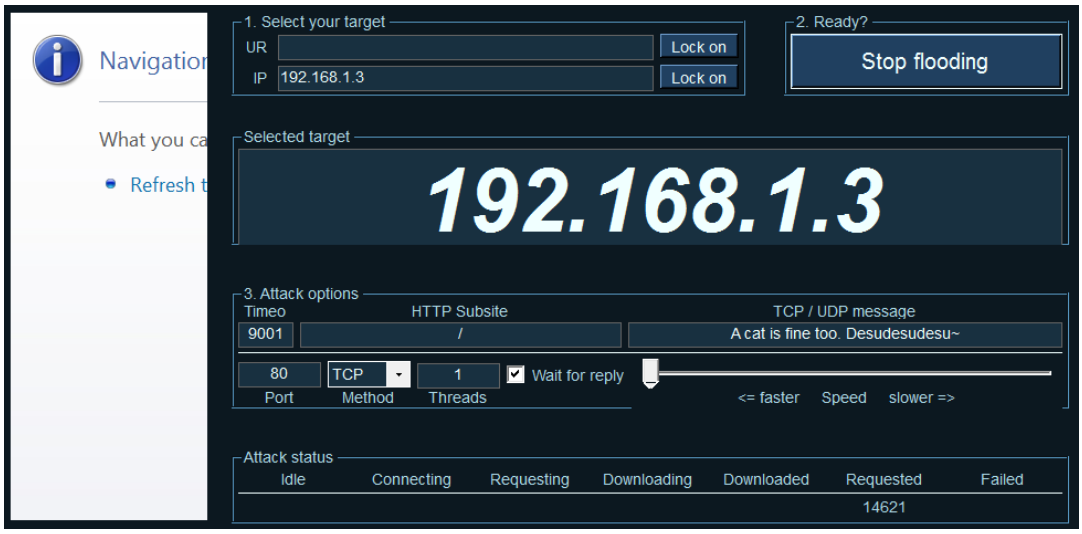


Figure 45 : Attaque Dos via la zone PUBLIC par l'attaquant2

2020-11-18 01:54:10	⚠	0	TCP	192.168.3.3	59887	192.168.1.3	89	1:15031996	une attaque DOS

Figure 46 : Détection de l'attaque Dos de l'attaquant2 par IDS 2

IV.5.1 Test de l'attaque passive Scanne

```
userone@kali:~$ sudo nmap 10.5.2.88
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-17 10:09 EST
Nmap scan report for 10.5.2.88
Host is up (0.00083s latency).
Not shown: 980 closed ports
PORT      STATE    SERVICE
1/tcp     filtered tcpmux
3/tcp     filtered compressnet
4/tcp     filtered unknown
6/tcp     filtered unknown
7/tcp     filtered echo
9/tcp     filtered discard
22/tcp    open     ssh
80/tcp    open     http
3306/tcp  open     mysql
60020/tcp filtered unknown
60443/tcp filtered unknown
61532/tcp filtered unknown
61900/tcp filtered unknown
62078/tcp filtered iphone-sync
63331/tcp filtered unknown
64623/tcp filtered unknown
64680/tcp filtered unknown
65000/tcp filtered unknown
65129/tcp filtered unknown
65389/tcp filtered unknown
MAC Address: 08:00:27:65:C2:31 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
userone@kali:~$
```

Figure 47 : Le scanne via la zone WAN par l'attaquant2

5 Entries in Active Log

Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description
2020-11-17 16:09:09	⚠	2	TCP	Potentially Bad Traffic	10.5.2.90	34325	192.168.1.3	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2020-11-17 16:09:09	⚠	2	TCP	Attempted Information Leak	10.5.2.90	34325	192.168.1.3	5815	1:2002910	ET SCAN Potential VNC Scan 5800-5820
2020-11-17 16:09:09	⚠	2	TCP	Potentially Bad Traffic	10.5.2.90	34325	192.168.1.3	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2020-11-17 16:09:09	⚠	2	TCP	Potentially Bad Traffic	10.5.2.90	34325	192.168.1.3	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2020-11-17 16:09:09	⚠	2	TCP	Potentially Bad Traffic	10.5.2.90	34325	192.168.1.3	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306

Figure 48 : Détection de l'attaque scanne de l'attaquant1 par IDS 1

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Supprimer
1	10.5.2.90	ET SCAN Suspicious inbound to mySQL port 3306 -- 2020-11-17 16:09:09 ET SCAN Suspicious inbound to PostgreSQL port 5432 -- 2020-11-17 16:09:09 ET SCAN Suspicious inbound to MSSQL port 1433 -- 2020-11-17 16:09:09 ET SCAN Potential VNC Scan 5800-5820 -- 2020-11-17 16:09:09 ET SCAN Suspicious inbound to Oracle SQL port 1521 -- 2020-11-17 16:09:09	

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

Figure 49 : Blocage de l'adresse IP de l'attaquant2 par IPS 1

```
userone@kali:~$ sudo nmap 192.168.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-17 19:48 EST
Nmap scan report for Pfsense1.localdomain (192.168.2.1)
Host is up (0.00050s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 192.168.2.10
Host is up (0.00079s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.26 seconds
userone@kali:~$
```

Figure 50 : Le scanne de zone WORK via la zone PUBLIC par l'attaquant3

Interface to Inspect: LAN (em1) — Choose interface.. | Auto-refresh view | 250 — Alert lines to display. | Enregistrer

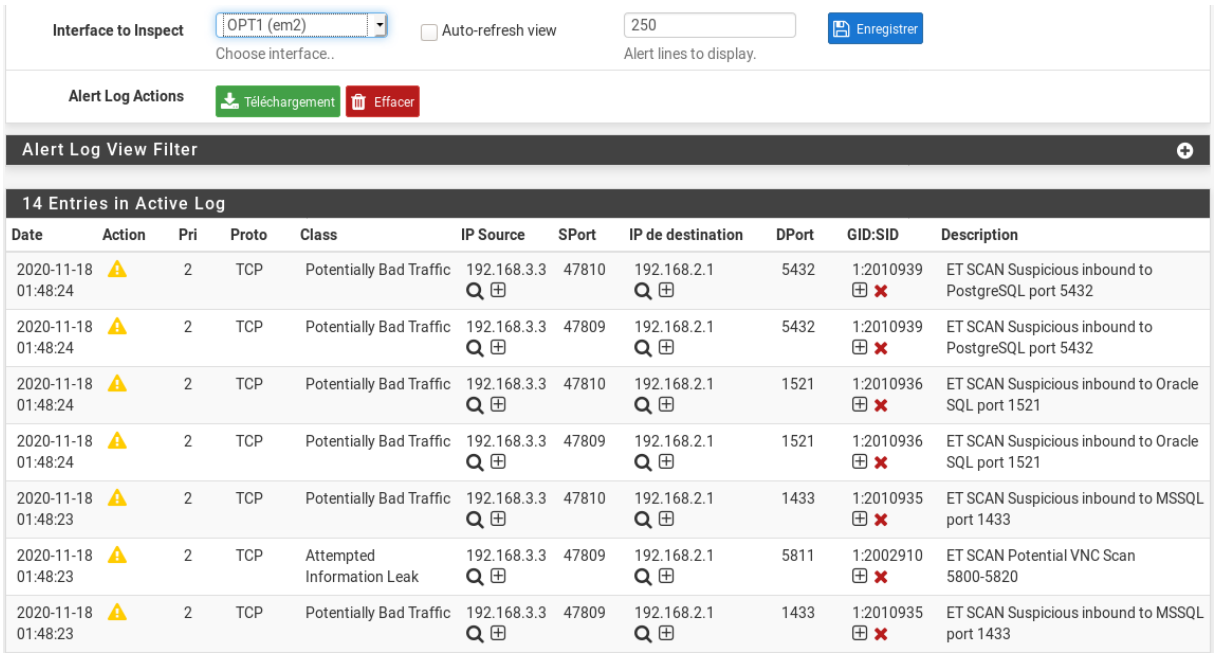
Alert Log Actions: Téléchargement | Effacer

Alert Log View Filter

24 Entries in Active Log

Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description
2020-11-18 01:48:21		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.10	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2020-11-18 01:48:21		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.10	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2020-11-18 01:48:20		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.10	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2020-11-18 01:48:20		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.10	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306
2020-11-18 01:48:02		2	TCP	Potentially Bad Traffic	192.168.3.3	46950	192.168.2.10	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2020-11-18 01:48:02		2	TCP	Attempted Information Leak	192.168.3.3	46950	192.168.2.10	5811	1:2002910	ET SCAN Potential VNC Scan 5800-5820
2020-11-18 01:48:02		2	TCP	Potentially Bad Traffic	192.168.3.3	46950	192.168.2.10	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2020-11-18 01:48:02		2	TCP	Potentially Bad Traffic	192.168.3.3	46950	192.168.2.10	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432

Figure 51 : Détection de l'attaque scanne de l'attaquant3 par IDS2 capteur1



Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description
2020-11-18 01:48:24		2	TCP	Potentially Bad Traffic	192.168.3.3	47810	192.168.2.1	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2020-11-18 01:48:24		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.1	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2020-11-18 01:48:24		2	TCP	Potentially Bad Traffic	192.168.3.3	47810	192.168.2.1	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2020-11-18 01:48:24		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.1	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2020-11-18 01:48:23		2	TCP	Potentially Bad Traffic	192.168.3.3	47810	192.168.2.1	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2020-11-18 01:48:23		2	TCP	Attempted Information Leak	192.168.3.3	47809	192.168.2.1	5811	1:2002910	ET SCAN Potential VNC Scan 5800-5820
2020-11-18 01:48:23		2	TCP	Potentially Bad Traffic	192.168.3.3	47809	192.168.2.1	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433

Figure 52 : Détection de l'attaque scanne de l'attaquant3 par IDS2 capteur1

2020-11-18 01:54:11		2	TCP	Potentially Bad Traffic	192.168.3.3	59888	192.168.1.1	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306
2020-11-18 01:54:11		2	TCP	Potentially Bad Traffic	192.168.3.3	59888	192.168.1.2	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306
2020-11-18 01:54:11		2	TCP	Potentially Bad Traffic	192.168.3.3	59887	192.168.1.2	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306
2020-11-18 01:54:11		2	TCP	Potentially Bad Traffic	192.168.3.3	59887	192.168.1.1	3306	1:2010937	ET SCAN Suspicious inbound to mySQL port 3306
2020-11-18 01:54:10		2	TCP	Attempted Information Leak	192.168.3.3	59887	192.168.1.3	5802	1:2002910	ET SCAN Potential VNC Scan 5800-5820
2020-11-18 01:54:10		2	TCP	Potentially Bad Traffic	192.168.3.3	59887	192.168.1.3	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2020-11-18 01:54:10		2	TCP	Potentially Bad Traffic	192.168.3.3	59887	192.168.1.3	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2020-11-18 01:54:10		2	TCP	Potentially Bad Traffic	192.168.3.3	59887	192.168.1.3	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432

Figure 53 : Détection de l'attaque scanne de l'attaquant3 sur la zone DMZ par IDS2

IV.6 Conclusion

Dans ce chapitre, nous avons étudié les principales zones réseaux d'une entreprise sur trois types d'architectures (centralisée, décentralisée et hybride), et illustré l'installation et le mécanisme de fonctionnement de Snort. Nous avons vu à la fin, comment Snort a pu stopper une attaque passive (scanne avec Nmap) et active (Dos) avec succès.

Conclusion générale

Conclusion générale

L'évolution des réseaux informatiques et l'ouverture de ces réseaux rendent l'accès aux informations plus simples et plus rapides, et les rend plus vulnérables. D'où la nécessité de mettre en place toute une politique de sécurité. La sécurité des réseaux informatique est un des problèmes les plus sérieux que connaissent les entreprises.

Sur le réseau Internet, les pirates informatiques exploitent et développent de plus en plus de nouvelles stratégies, afin d'atteindre leurs objectifs sans se faire détecter. D'où la nécessité de mettre en place toute une politique de sécurité pour se prévenir. Les systèmes de détection d'intrusions ne représentent qu'une petite partie de cette politique.

Ce mémoire nous a permis d'acquérir une certaine maitrise et un certain bagage dans le domaine de la sécurité informatique, et nous a permis de découvrir les systèmes de détection et de prévention d'intrusions.

Nous avons étudié les fonctionnements de'IDS et d'IPS, et comment les positionner sur différents types d'architectures réseaux (centralisée, décentralisée, et hybride), ainsi nous avons pris le snort comme exemple qui est un très bon outil pour la détection et la prévention d'intrusion, il effectue en temps réel des analyses du trafic de réseau, et garantie une sécurité continue, et nous avons appris comment le manipuler sous la plateforme Pfsense, ce qui nous a offert l'occasion de travailler sous l'environnement FreeBSD.

Le résultat des tests de notre système est satisfaisant, mais cela ne veut pas dire que notre système est parfaitement efficace, car aucun système de sécurité permettant de garantir une sécurité totalement fiable à 100%.

Bibliographie

[1] Les 10 Cyber attaques qui ont marqué 2019, https://www.globalsecuritymag.fr/Les-10-Cyberattaques-qui-ont,20191219,94070.html.

[2] C.Servin « Réseaux et Télécoms Cours et Exercices corrigés », Dunod, 2003.

[3] Dean .T (2001). Réseaux Informatique. Edition RYNALD GOULET.

[4] Mr Abdellaoui Mohammed El Amine, Mr Benhamou Aboubakr: « Application mobile de la voIP sur un réseau Wifi ». Mémoire de Master, spécialité Réseaux et Systèmes de télécommunication. Faculté de technologie. Université de Tlemcen. Juin 2014.

[5] https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/types.htm

[6] https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/topologi.htm

[7] https://www.fichier-pdf.fr/2015/04/20/topologie-des-reseaux/?

[8] Melle Rebiha HADAOUI : « Un IDS basé sur un algorithme inspiré du fonctionnement de colonies des fourmis ». Mémoire de Magister. Faculté des Sciences, Département d'informatique. Université M'hamed BOUGARA de Boumerdes. 2009.

[9] Pierre Erny. (1998). « Les réseaux informatiques d'entreprise ».

[10] G.Valet, (Janvier 2012). Cours « Réseaux, TCP/IP ». Lycée Polyvalent Diderot.

[11] S.Belattaf, « Sécurité Informatique ». Cours LICENCE3 -2017/2018 –UMMTO.

[12] Elies Jebri, « Introduction à la sécurité », support de cours, 2008.

[13] MESSOUAF Sonia : « Génération automatique des scénarios d'attaques dans les systèmes informatiques ». Mémoire de fin de cycle master en informatique, Option : Réseaux et Systèmes Distribués. 2012-2013

[14] Amiri khadidja, Tabti Fatima Djihane : « Détection des Cyber-attaques dans un réseau IP ». Mémoire de fin d'étude. 2016-2017

[15] Tarek ABBES : « Classification du trafic et optimisation des règles de filtrage pour la détection d'intrusion ».Thèse. 2004

[16] Hamzata Guey : « Mise en place d'un IDS en utilisant Snort ». Licence en informatique et reseau.2010.

[17] Guillaume CHARPENTIER, Olivier MONTIGNY, Mathieu ROUSSEAU : « Virus / antivirus- Nouvelles technologies Réseaux. 2004.

[18] Raphael Yende : « support de cours de sécurité informatique et crypto ».Support de cours. 2018

[19] Melle BELHARIZI Asmaà « La sécurité réseau, étude le cas de service Openvpn ».Mémoire licence en Informatique. 2013

[20] ACISSI « Sécurité informatique Ethical Hacking Apprendre l'attaque pour mieux se défendre ». Octobre 2009.

[21] Jean-François PILLOU, Jean-Philippe BAY « Tout sur la sécurité informatique 4e édition». Dunod. 2016.
[22] M. Tran Van Tay « Le Sèstème de détection des intrusions et le système d'empêchement des intrusions (ZERO DAY) », Rapport de stage de fin d'études, Février 2005, Université du Québec à Montéal.
[23] Nicolas Baudoin, Marion Karle « NT Réseaux IDS et IPS », 2003/2004.
[24] M. ABBAS Massinissa, M. AOUADI Djamel « Détection d'intrusion dans les réseaux LAN :IDS Snort sous LINUX », Mémoire de fin de cycle Master, Université Abderrahmane Mira de Béjaïa, 2016/2017.
[25] Landry Ndjate, « Mise en place d'un crypto système pour la sécurité des données et la détection d'intrusion dans un supermarché ». Graduat, 2014, Université Notre Dame du Kasayi
[26] C. MICHEL : « Langage de description d'attaque pour la détection d'intrusion par corrélation d'évènements ou d'alertes en environnement réseau hétérogène ». Thèse de doctorat. Université de Rennes 1. Décembre 2003
[27] Z. ABDELHALIM. Recherche et détection des patterns d'attaques dans les réseaux IP à haut débit. Thèse de doctorat. Université d'Evry Val d'Essonne. Janvier 2011.
[28] https://www.lemagit.fr/definition/HIDS-NIDS
[29] https://www.commentcamarche.net/contents/237-systemes-de-detection-d-intrusion-ids
[30] https://www.securiteinfo.com/conseils/choix_ids.shtml
[31] https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html
[32] https://www.pfsense.org/getting-started/
[33] https://www.snort.org/
[34] https://nmap.org/man/fr/index.html
[35] SOUROUR MEHAROUECH « Optimisation de la Fiabilité et la Pertinence des Systèmes de Détection et Prévention d'Intrusions », Thèse de Doctorat, 2009/2010. école supérieure des Communications de Tunis Université 7 Novembre à Carthage.
[36] Melle BELKHTMI Keltouma, Mlle BENAMARA Ouarda. « Mise en place d'un système de détection et de prévention d'intrusion », Mémoire de fin d'étude Master. 2015/2016. Université A/Mira de Béjaïa.
[37] Dany Fernandes, Papa Amadou Sarr, « La protection des réseaux contre les attaques DOS », 2010, Université PARIS DESCARTES
[38] http://www.madchat.fr/reseau/ids%7Cnids/L'%E9criture%20de%20r%E8gles%20Snort.htm
[39] https://blog.varonis.fr/ids-et-ips-en-quoi-sont-ils-differents/
[40] https://www.researchgate.net
[41] Le manuel officiel du logiciel **LOIC** (README), sur le site github. URL: https://github.com/NewEraCracker/LOIC/
[42] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

Liste des figures

Liste des abréviations

VPN	Virtual Private Network
DMZ	Demilitarized zone
FreeBSD	Free Berkeley Software Distribution
BSD	Berkeley Software Distribution
Nmap	Network Mapper
PPTP	Point-to-Point tunneling Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ISP	Internet Service Provider
DHCP	Dynamic Host Configuration Protocol
UTM	Unified Threat Management
OSI	Open Systems Interconnection
IP	Internet Protocol
NAT	Network Address Translation
DNS	Domain Name System
IDS	Intrusion Detection System
HIDS	Host Intrusion Detection System
NIDS	Network Intrusion Detection System
AIDS	Application Intrusion Detection System
IPS	Intrusion Detection System
HIPS	Host Intrusion Detection System
NIPS	Network Intrusion Detection System
KIPS	Kernel Intrusion Detection System
SYN	synchronize
TCP	Transmission Control Protocol
UDP	User Dataram Protocol
ICMP	Internet Control Message Protocol
PAN	Personal Area Network
LAN	Local Area Network

MAN	Metropolitan Area Network
WAN	Wide Area Network
DOS	Denial Of Service
DDOS	Distributed Denial Of Service
LOIC	Low Orbit Ion Cannon
ASA	Adaptive Security Appliance
CD	Compact Disc
BDD	Base De Données
SQL	Structured Query Language
IDWG	Intrusion Detection exchange format Working Group