Liste des figures

Liste des abréviations

DMZ : Demilitarized Zone

IDS : Intrusion Detection System

IPS : Intrusion Prevention System

VPN : Virtual Private Network

DoS : Denial of Services

DDoS : Distributed Denial of Services

NIDS : Network based Intrusion Detection System

HIDS : Host based Intrusion Transmission System

INTERNET : Interconnected Network

IP : Internet Protocol

TCP : Transmission Control Protocol

LAN : Local Area Network

WAN : Wide Area Network

WWW : World Wide Web

Snort : The open source network Intrusion Detection System

Sommaire

Introduction Générale

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plupart raccordés à Internet. Cette ouverture à Internet pour faciliter la communication engendre malheureusement des vulnérabilités ou des failles menaçant ainsi la sécurité informatique. Des utilisateurs avec de mauvaises intentions peuvent exploiter les vulnérabilités des réseaux et systèmes pour fomenter leurs attaques.

La sécurité informatique ou plus simplement sécurité des systèmes d'information (SSI), est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique pouvant être exploitée par un attaquant et porter atteinte à son fonctionnement normal, à l'intégrité ou à la confidentialité des données de ce système.

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais l'utilisateur reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé.

Pour faire face à ces problèmes de sécurité informatique, différents dispositifs ont été mis en place pour détecter et prévenir les attaques sur les systèmes informatiques comme les antivirus, les pare-feux qui paraissent limités face à l'expansion grandissante des techniques de piratage, d'où le besoin de mettre en place un système de détection d'intrusion.

Le mémoire est structuré en trois chapitres :

- Dans le premier chapitre nous allons faire une étude générale sur les réseaux informatiques.
- Dans le deuxième chapitre, nous allons faire une étude théorique sur les systèmes de détection d'intrusion.
- Dans le dernier chapitre nous allons mettre en place un système de détection d'intrusion.

Chapitre I :
Généralités sur les réseaux informatiques

I. Introduction

Le réseau est un ensemble d'objets connectés ou maintenus en liaison. Auparavant les différentes communications entre différentes machines étaient juste destinées au transport de données informatique alors qu'aujourd'hui les réseaux permettent le partage des ressources tel que la parole et la vidéo.

Dans ce premier chapitre, nous décrivons les notions théoriques de base sur les réseaux informatiques en général. Pour ce faire, dans un premier temps nous ferons un petit historique sur les réseaux, puis nous verrons quelques fondamentaux sur les réseaux et la sécurité des données.

II. Historique

Peu après la seconde guerre mondiale, nous sommes à la naissance de la micro-informatique. Seules les grandes entreprises pouvaient se doter de matériel informatique. Le seul moyen d'échanger des données de station à station était la disquette. Pour un même département, cela ne posait guère de problèmes. Cependant, la chose devenait plus compliquée lorsqu'il s'agissait d'un bureau situé à un autre étage, ou dans un autre bâtiment. La taille des entreprises croissant au fil du temps, il a fallu envisager un autre mode d'échange des données.

Vers 1960, des ingénieurs, tant du secteur militaire qu'industriel se sont penché sur ce problème. Le consortium D.I.X. (Digital, Intel, Xerox) a effectué des recherches et est parvenu à développer un moyen de communication de poste à poste plus direct. Leur travail a abouti à la naissance de ce que nous appelons aujourd'hui communément carte réseau. L'appellation correcte de ce type de matériel est carte d'interface réseau.

Les réseaux primitifs se composaient d'un ordinateur central et de terminaux. Ces stations étaient dépourvues de disques durs et servaient à l'échange pur et simple de caractères avec le poste central. Digital et IBM sont parmi les pionniers avec leur système DECnet qui est une architecture réseau en couches, qui constituera un ancêtre de nos réseaux actuels.

Un problème existait néanmoins, chaque fabricant usait de protocoles et de standards propriétaires. Il était donc impossible de faire communiquer des machines de fabricants différents.

La guerre froide couvant, le département américain de la défense étudia un moyen de communication fiable et à même de fonctionner en temps de guerre. Ils créèrent le réseau ARPAnet (Advanced Research Projects Agency Network) qui est le premier réseau à transfert de paquets. ARPAnet interconnectait différents points stratégiques par un réseau câblé et reliait le Royaume-Uni par satellite.

C'est aussi la naissance d'un protocole de communication devenu au fil du temps incontournable : TCP/IP. Grâce à ce protocole, les données peuvent atteindre leur destination indépendamment du média. Si un média est hors d'usage, les données sont acheminées malgré tout via un autre. Outre le protocole, TCP/IP désigne aussi un modèle de conception de réseaux en 4 couches.

III. Les réseaux

1. Classification des réseaux

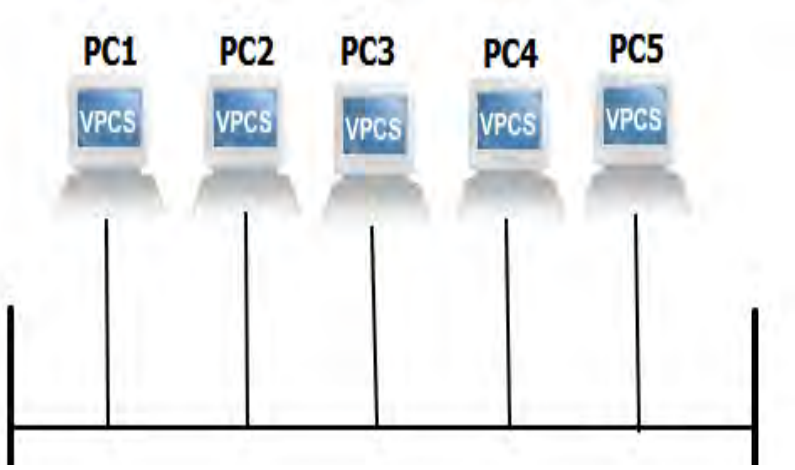
1.1. Classification selon l'architecture

1.1.1. Réseau poste à poste

Dans une architecture d'égal à égal contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Donc chaque machine du réseau est libre de partager ses ressources.
L'architecture réseau poste à poste a des avantages :
- Un coût réduit car on a juste besoin de ressources pour le matériel, le câblage, la maintenance.

- La simplicité pour mettre en place l'architecture.

L'architecture réseau poste à poste a aussi des inconvénients :
- C'est un système qui n'est pas centralisé
- La sécurité peu présente
- Aucun maillon du système n'est fiable



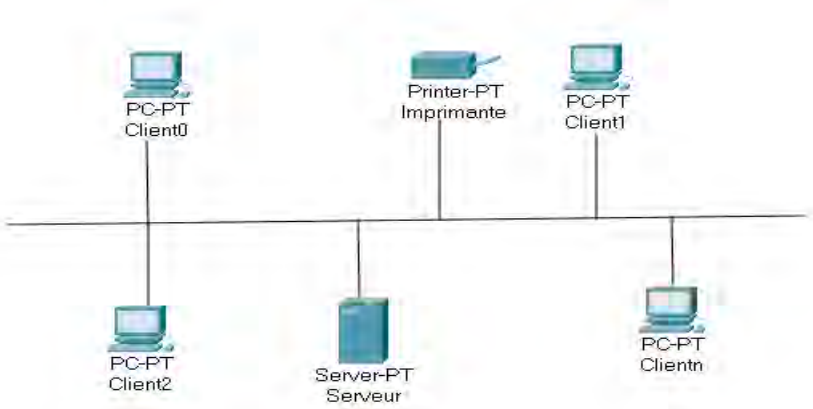
Architecture réseau poste à poste

1.1.2. Réseau client/serveur

De nombreuses applications fonctionnent selon un environnement client/serveur cela signifie que des machines clientes contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée- sortie, qui leur fournit des services. Ces services fournissent des données telles que des mises à jour, des fichiers, l'heure etc.

L'architecture réseau client/serveur a des avantages :
- Des ressources centralisées.
- Une meilleure sécurité car les points d'entrée permettant l'accès au réseau sont moins nombreux.
- Une administration centralisée
- Un réseau évolutif

L'architecture réseau client/serveur a aussi des inconvénients :
- Coût élevé dû aux technicités du serveur
- Le serveur est le maillon faible du serveur étant donné que tout le réseau est architecturé autour de lui.



Architecture réseau client/serveur

1.2. Classification selon la topologie

Une topologie de réseau informatique correspond à l'architecture physique ou logique de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux.

La topologie physique c'est la représentation spatiale des équipements du réseau.

La topologie logique définie la façon dont les données transitent dans les lignes de communication.

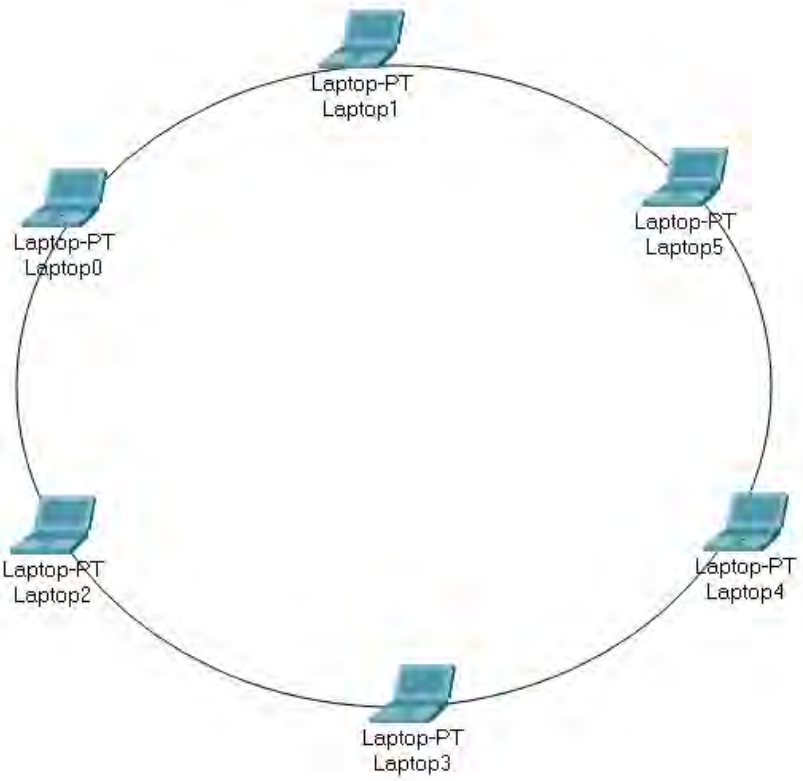
Les architectures suivantes sont utilisées dans des réseaux informatiques d'entreprise. La topologie d'un réseau correspond à son architecture physique et donc leur structure détermine leur type.

Il existe 2 modes de propagation classant ces topologies :

- Le mode de diffusion **:** Dans ce mode de fonctionnement un seul support de transmission est utilisé. En effet le message est envoyé sur le réseau, ainsi tous les équipements du réseau sont capables de voir le message et d'analyser selon l'adresse du destinataire si le message lui est destiné ou non.

Les topologies en anneau et en bus utilisent ce mode de propagation.

On parle de topologie en anneau quand tous les équipements du réseau sont connectés en chaine les uns aux autres par une liaison bipoint de la dernière à la première. Chaque station joue le rôle de station intermédiaire. Chaque station qui reçoit une trame, l'interprète et la réémet à la station suivante de la boucle si c'est nécessaire. La défaillance d'un hôte rompt la structure d'un réseau en anneau si la communication est unidirectionnelle.

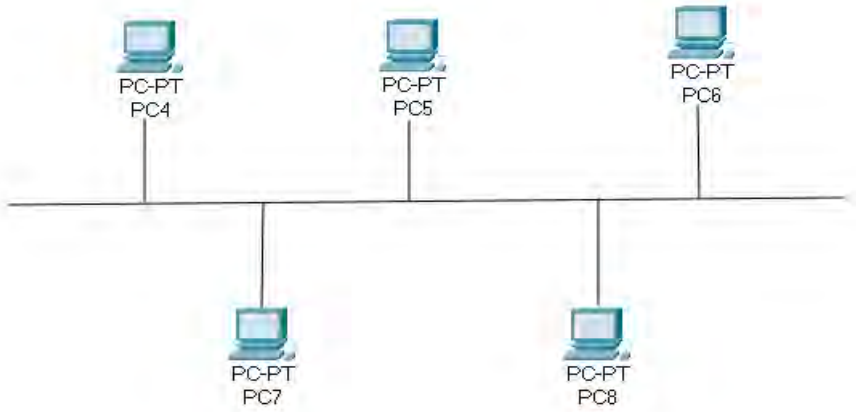


Architecture réseau en anneau

On parle de topologie en bus lorsque celle-ci est représentée par un cablage unique des unités réseaux. Le coût pour un tel réseau n'est pas élevé et la defaillance d'un nœud ne scinde pas le réseau en deux sous réseaux. Les caractéristiques de la topologie en bus sont les suivantes :

- Lorsque le support est en panne, c'est l'ensemble du réseau qui ne fonctionne pas.

- Lorsqu'une station est défectueuse et ne transmet plus sur le réseau, elle ne perturbe pas le réseau.
- Le signal émis par une station ne se propage que dans un seul sens.
- Si la transmission est bidirectionnelle, toutes les stations connectées reçoivent les signaux émis sur le bus en même temps.
- Le bus dans le cas de câbles coaxiaux, est terminé à ses extrémités par des adaptateurs d'impédance appelés aussi bouchons pour éliminer les réflexions du signal.

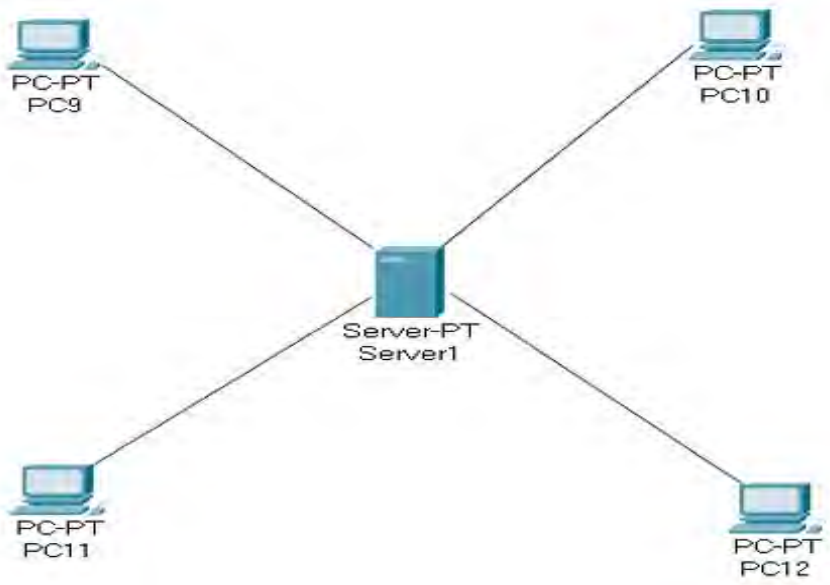


Architecture réseau en bus

- Le mode point à point **:** Dans ce mode, le support physique ne relie qu'une paire d'unités seulement. Pour que deux unités réseaux communiquent, elles passent obligatoirement par un intermédiaire appelé le nœud.

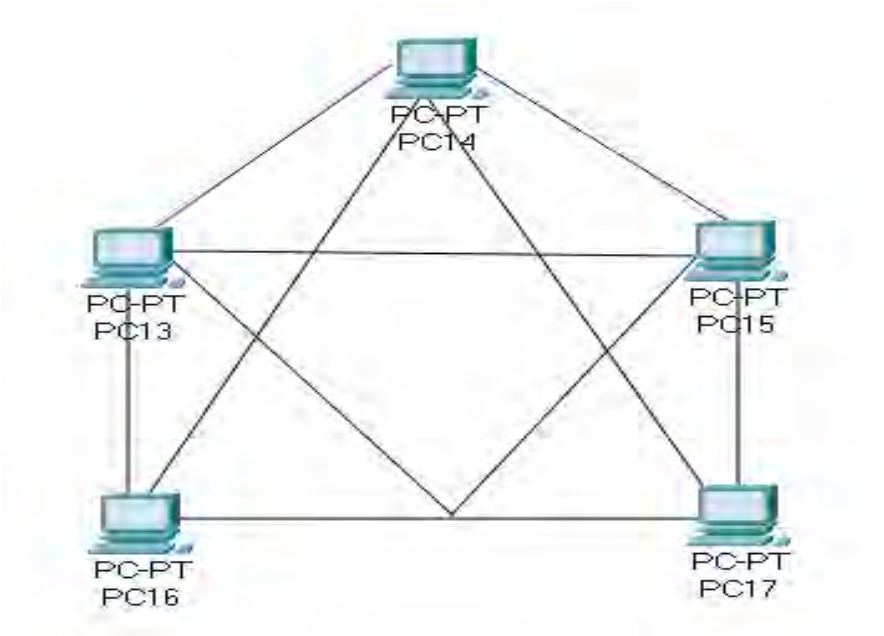
Les topologies en étoile et en maille utilisent ce mode de propagation.

La topologie réseau en étoile est la topologie la plus courante. Elle a aussi l'avantage d'être facile à dépanner et très facile à gérer. En effet, la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central qui est souvent un concentrateur ou un hub et plus souvent un commutateur ou un switch sur les réseaux modernes relie tous les nœuds et constitue aussi le point unique de défaillance. Et donc une panne au niveau de l'équipement central rend le réseau totalement inutilisable. L'inconvénient principal de cette topologie réside dans la longueur des câbles utilisés.



Architecture réseau en étoile

Une topologie maillée correspond à plusieurs liaisons point à point. Dans une telle topologie, chaque terminal est relié à tous les autres. L'inconvénient est le le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux est important. En effet s'il y'a N terminaux, le nombre de liaisons nécessaires est de $\frac{N(N-1)}{2}$.



Architecture réseau en maille

1.3. Classification selon l'étendu du réseau

Un réseau informatique fait référence à des systèmes informatiques indépendants qui sont reliés entre eux pour que l'échange de données entre ces systèmes soient réalisables. Et pour cela en plus d'une connexion physique il faudrait une connexion logique des systèmes en réseau.

ET cette connexion logique est mise en place en utilisant des protocoles de communication telle que le protocole TCP.

Les réseaux sont mis en place en général pour le transfert de données d'un système à un autre ou de fournir des ressources partagées ou des services comme par exemple les serveurs, les bases de données ou une imprimante sur le réseau. Il est possible de différencier et de catégoriser les réseaux selon leur taille et la portée du réseau informatique :

- Personal Area Network (PAN) ou réseau personnel
- Local Area Network (LAN) ou réseau local
- Metropolitan Area Network (MAN) ou réseau métropolitain
- Wide Area Network (WAN) ou réseau étendu
- Global Area Network (GAN) ou réseau global

Pour la connexion physique entre ces types de réseau peut être une connexion câblée c'est-à-dire filaire ou réalisée à l'aide de la technologie sans fil.

1.3.1. Personal Area Network (PAN) ou réseau personnel

Pour permettre l'échange de données des appareils modernes tels que les tablettes, les ordinateurs portables ou les smartphones, il faut un réseau adapté. Ces appareils peuvent être connectés en utilisant un Personal Area Network on parle aussi de réseau domestique.

Les techniques de transmission courantes dans un tel réseau sont souvent l'USB ou le FireWire. Le réseau personnel sans fil (WPAN pour Wireless Personal Area Network) repose sur des technologies comme le Bluetooth, USB sans fil, ZigBee …

Un réseau personnel sans fil réalisé par l'intermédiaire d'un Bluetooth est appelé Piconet. Les WPAN et les PAN ne couvrent en général que quelques mètres et ne sont pas adaptés pour faire communiquer des appareils dans des bâtiments différents.

En plus de faire communiquer plusieurs appareils entre eux, un réseau personnel permet aussi la connexion à d'autres réseaux, le plus souvent plus grands. Dans ce cas on parle de liaison montante ou de Uplink. Les PAN sont généralement utilisés pour relier des appareils pour un usage récréatif par exemple les écouteurs sans fil, les consoles de jeux vidéo, les appareils photos.

1.3.2. Local Area Network (LAN) ou réseau local

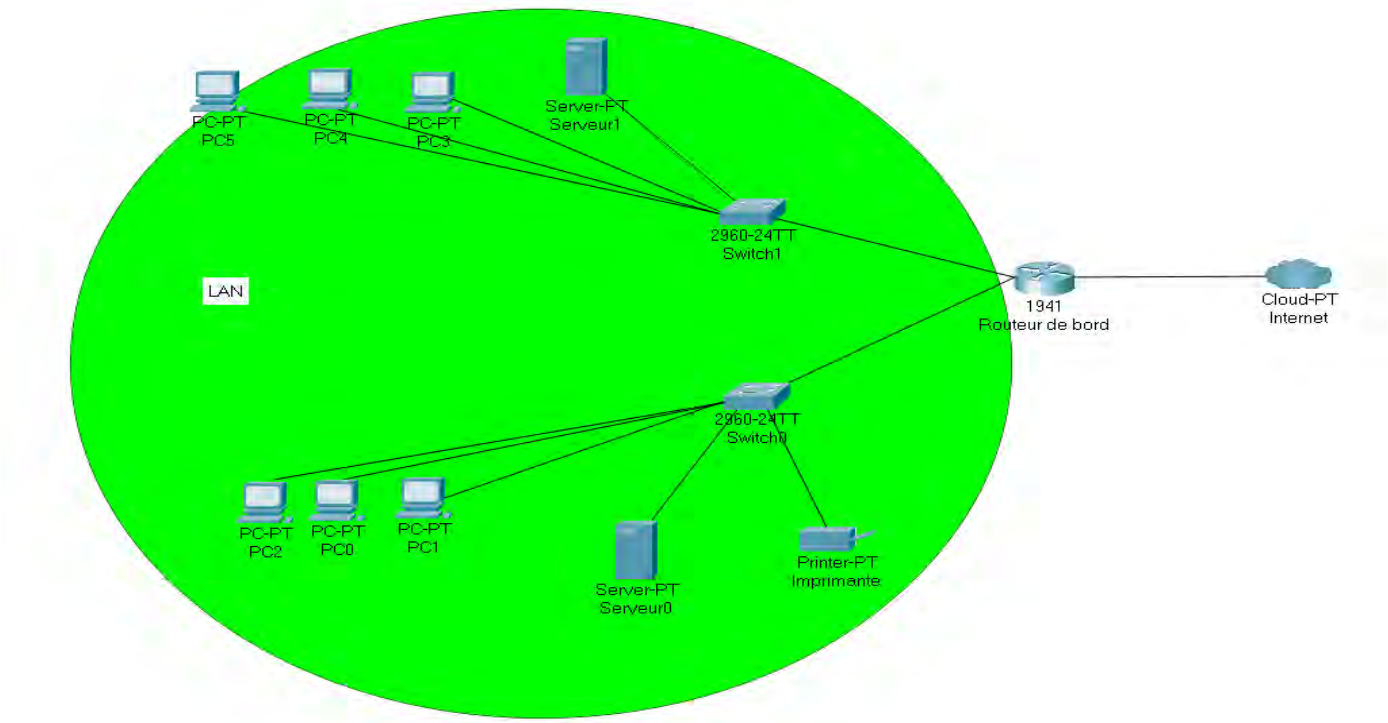
Si nous devions réunir plusieurs machines sur un réseau, cela se fait généralement dans un réseau local ou LAN. En effet un LAN permet de relier plusieurs centaines d'appareils au sein d'un entreprise.

Une norme très répandue pour les réseaux locaux câblés est le protocole Ethernet. Les autres technologies moins fréquentées et parfois même obsolète sont Arcnet, FDDI et Token Ring. Les données transitant dans le réseau sont transmises via des câbles de cuivre ou des câbles de fibres optiques.

Si plus de deux ordinateurs sont imbriqués ensemble dans un réseau local, des composants supplémentaires comme un hub (ou concentrateur), bridge (pont) ou un switch (commutateur réseau) sont nécessaires et agissent alors comme des éléments de couplage et des nœuds de distribution. Un LAN est conçu pour permettre un transfert rapide de grandes quantités de données. Selon la structure du réseau et du moyen de transmission utilisé, un débit de données de 10 à 1000 Mbit/s est courant. Les réseaux locaux permettent un échange d'informations confortable entre les différents périphériques qui sont connectés au réseau. Dans le contexte d'une entreprise, il est courant que plusieurs ordinateurs de travail partagent des serveurs de fichiers, des imprimantes réseau ou des applications sur le LAN.

Les WLAN ou réseau local sans fil sont des réseaux locaux implémenté par radio. Communément le terme WIFI est utilisé pour désigner un WLAN

Les réseaux locaux sans fil permettent l'intégration facile des appareils dans le réseau domestique ou d'entreprise mais le débit des données transmises sur un réseau sans fil est inférieur à celui d'une connexion Ethernet.



1.3.3. Metropolitan Area Network (MAN) ou réseau métropolitain

Un Metropolitan Area Network (MAN) ou réseau métropolitain, est un réseau de télécommunication à large bande qui relie plusieurs LAN géographiquement à proximité. Il s'agit en règle générale de différentes branches d'une société qui sont reliées à un MAN via des lignes loués. Les routeurs de haute performance et les connexions de fibres optiques hautes performances sont utilisés ce qui permet de fournir un débit de données beaucoup plus élevé que l'Internet. La vitesse de transmission entre deux nœuds éloignés est comparable à la communication dans un réseau local. L'infrastructure pour le MAN est assurée par les opérateurs de réseaux internationaux. En tant que réseau métropolitain, les villes câblées peuvent être intégrées dans les réseaux étendus : WAN (Wide Area Networks) et sur le plan international au niveau des GAN (Global Area Networks).

Metro-Ethernet est une technologie de transmission spéciale disponible pour le MAN qui peut être utilisé pour construire de puissants réseaux métropolitains (MEN ou Metro Ethernet Network) basés sur Carrier Ethernet (CE1.0) ou Carrier Ethernet (CE 2.0).

Une norme pour les grands réseaux de radio régionaux, que l'on nomme Wireless Metropolitan Area Network (WMAN) a été développée avec IEEE 802.16. La technologie connue sous le nom de WiMAX (Worldwide Interoperability for Microwave Access) permet de mettre en place ce que l'on appelle des bornes Wifi ou WLAN hotspots. Ce sont plusieurs points d'accès Wifi travaillant ensemble dans différents endroits. La norme commune de transmission DSL est techniquement disponible que lorsque des câbles en cuivre ont été posés.

1.3.4. Wide Area Network (WAN) ou réseau étendu

Alors que les réseaux métropolitains relient des zones qui se trouvent proches les unes des autres dans des zones rurales ou urbaines, les WAN (Wide Area Network) ou réseaux étendus couvrent des vastes zones géographiques à l'échelle d'un pays ou d'un continent par exemple. En principe, le nombre de réseaux locaux ou d'ordinateurs connectés à un réseau étendu est illimité.

Alors que les réseaux locaux (LAN) et MAN peuvent être réalisés en raison de la proximité géographique des ordinateurs connectés ou des réseaux sur la base d'Ethernet, les réseaux étendus utilisent des techniques comme IP/MPLS (Multiprotocol Label Switching), PDH (Plesiochrone Digitale Hierarchie), SDH

(Synchrone Digitale Hierarchie), SONET (Synchronous Optical Network), ATM (Asynchronous Transfer Mode) et encore rarement l'obsolète X.25.

Les réseaux étendus sont généralement détenus par une organisation ou une entreprise et sont donc exploités en privé ou loués. En outre, les fournisseurs de services Internet utilisent des WAN pour connecter les réseaux locaux d'entreprises et les clients à Internet.

1.3.5. Global Area Network (GAN) ou réseau global

Un réseau mondial comme Internet est appelé GAN (Globe Area Network). Les entreprises actives au niveau international maintiennent également des réseaux isolés qui couvrent plusieurs WAN et permettant ainsi de connecter des machines d'entreprises dans le monde. Les GAN utilisent des câbles sous-marins pour faire transiter les données ou des transmissions par satellite.

2. Le modèle OSI

2.1. Définition

Imaginons que nous puissions communiquer à chaque instant, quand nous le voulons, avec n'importe qui dans le monde, c'est ce que nous propose Internet. Il n'est pas facile de s'exprimer lorsque nous sommes un petit groupe de dix personnes, difficile lorsque nous sommes cent, et quasiment impossible quand nous sommes mille. Internet se propose donc de relever le défi de pouvoir communiquer tous ensemble, en même temps, et ce, quand nous le souhaitons. Bien sûr pour arriver à cette prouesse, il a fallu créer un système de communication complexe permettant aux machines de parler entre elles.

Et c'est dans ce contexte qu'en 1984 le modèle OSI a vu le jour.
Le modèle OSI est né quand nous avons commencé à avoir une certaine expérience des communications entre ordinateurs. Il tient donc compte des communications existantes, mais aussi des communications futures et de leurs évolutions potentielles.

Son objectif est de normaliser les communications pour garantir un maximum d'évolutivité et d'interopérabilité entre les ordinateurs. Le modèle OSI est une norme qui préconise comment les ordinateurs devraient communiquer entre eux.

2.2. Les couches du modèle OSI

Le modèle OSI est un modèle en couches. Cela veut dire qu'il est découpé en plusieurs morceaux appelés couches, qui ont chacune un rôle défini, comme nous le montre le schéma suivant :

Les différentes couches du modèle OSI

La couche 1 ou couche physique : La couche physique est la première couche du modèle OSI. La couche physique est chargée de la transmission effective des signaux électriques, radiofréquences ou optiques entre les interlocuteurs.
Son service est généralement limité à l'émission et la réception d'un bit ou d'un train de bits continu (notamment pour les supports synchrones comme la fibre optique). Les matériels associés à la couche 1 est le hub, la carte réseau, la prise RJ45, la fibre optique.

La couche 2 ou couche liaison de données : La couche liaison de données est la deuxième couche du modèle OSI. Elle permet de connecter des machines ente elles sur un réseau local. Elle a aussi pour rôle secondaire de détecter les erreurs de transmission. Le matériel utilisé pour la couche 2 est le commutateur ou le switch

La couche 3 ou couche réseau : La couche réseau permet d'interconnecter les réseaux entre eux mais aussi permet de fragmenter les paquets. Le matériel utilisé au niveau de la couche 3 est le routeur.

La couche 4 ou couche transport : C'est au niveau de la couche 4 que sont gérées les connexions applicatives, la couche transport permet aussi de garantir les connexions.

La couche 5 ou couche session : Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle…). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

La couche 6 ou couche présentation : Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

La couche 7 ou couche applicative : Elle permet de représenter les applications pour lesquelles nous allons mettre en œuvre des communications. Elle est donc le point de contact entre l'utilisateur et le réseau.

Couche 1 ou couche physique	Rôle : Offre un support de transmission pour la communication	Matériel associé : Concentrateur, prise RJ45, fibre optique.
Couche 2 ou couche liaison de données	Rôle : Permet de connecter les machines entre elles sur un réseau local	Matériel associé : Switch, commutateur
Couche 3 ou couche réseau	Rôle : Interconnecter les réseaux entre eux	Matériel associé : Routeur
Couche 4 ou couche transport	Rôle : Gérer les connexions applicatives	Matériel associé : Aucun
Couche 5 ou couche session	Rôle : Organiser et synchroniser les échanges entre taches distantes	Matériel associé : Aucun
Couche 6 ou couche présentation	Rôle : Rendre l'information compatible entre taches communicantes	Matériel associé : Aucun
Couche 7 ou couche applicative	Rôle : Représenter les applications	Matériel associé : Aucun

Tableau récapitulatif des différentes couches du modèle OSI

3. Le TCP/IP

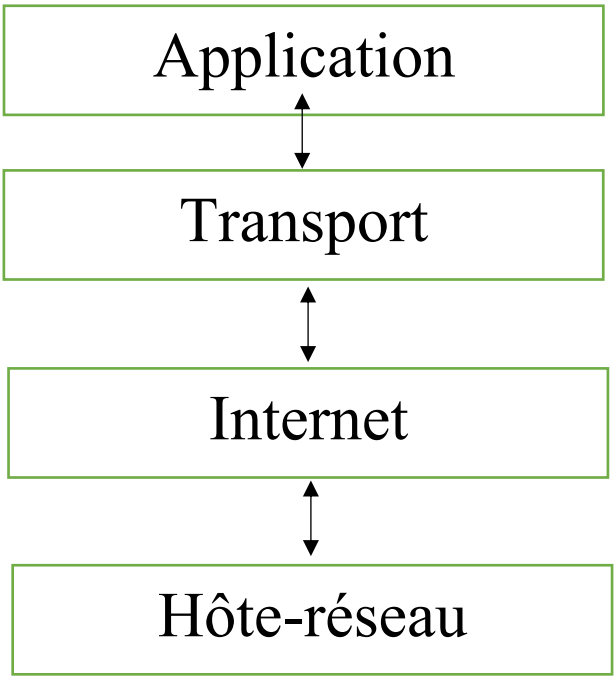
3.1. Définition

Le TCP/IP (Transmission contrôle protocole/Internet protocole) est dérivé de l'APRANET et deviendra plus tard connu sous le nom de worldwide internet.

Transmission contrôle protocol/Internet protocol est un protocole utilisé sur le réseau internet pour transmettre des données entre deux machines. TCP est un protocole de transport, prend en charge l'ouverture et le contrôle de la liaison entre deux ordinateurs. IP est un protocole de routage assure le routage des paquets de données. Le protocole IP est comme un langage universel permettant à deux machines de communiquer entre elles peu importe leur système d'exploitation.

3.2. Les couches du TCP/IP

Le TCP/IP est un modèle en 4 couches représentées sur la figure suivante :



Les différentes couches du modèle TCP/IP

La couche hôte-réseau : Couche assez sombre, le modèle TCP/IP en dit peu sur cette couche, excepté que l'hôte doit se connecter au réseau depuis certains protocoles de sorte à pouvoir envoyer des paquets IP à travers le réseau.

La couche internet : Le but de cette couche est de permettre d'injecter des paquets dans n'importe quel réseau et de faire en sorte qu'ils arrivent à destination. Tous les paquets ne prendront pas le même chemin pour arriver à bon port, mais ceci n'est pas un problème. S'ils arrivent dans le désordre, un protocole, placé dans une couche supérieure, se chargera de les ordonner.
C'est dans la couche internet qui définit le format officiel des paquets et son protocole : le protocole IP pour Internet Protocol. La fonction de la couche internet est de délivrer les paquets IP au bon endroit. Vous l'aurez compris, le routage des paquets est ici très critique et on souhaite éviter une éventuelle congestion. On peut faire l'analogie avec la couche réseau du modèle OSI.

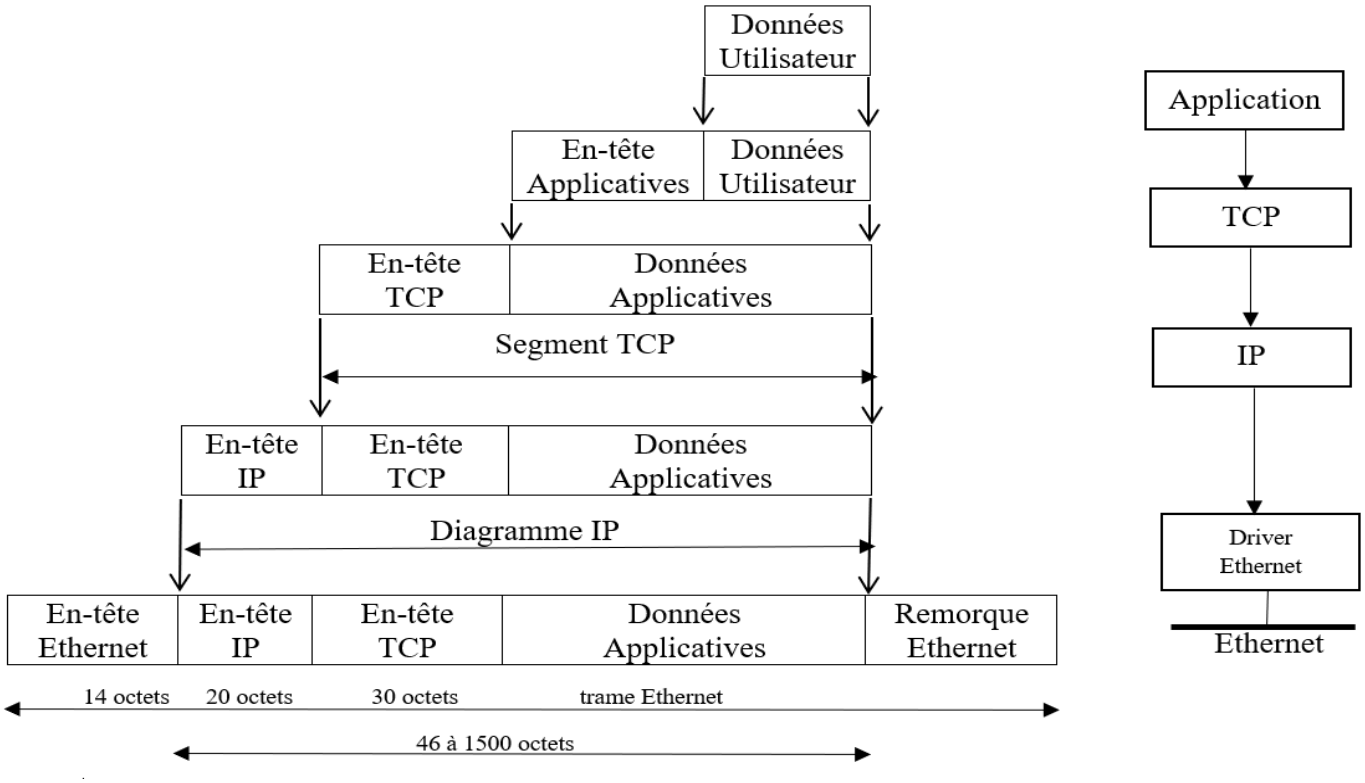
La couche transport : Tout comme pour le modèle OSI, la couche de transport permet aux hôtes source et destination de faire une conversation. C'est dans cette couche ci que sont définis deux protocoles end-to-end pour le transport : TCP, protocole fiable qui nécessite une connexion entre la source et la destination. Le protocole permet de délivrer un flux d'octets, le tout sans erreurs. Le flux d'octets est d'abord découpé en messages, puis les passe les uns après les autres à la couche Internet. Le destinataire réassemble ensuite les messages reçus. Le protocole TCP dispose également de mécanismes de contrôle pour éviter qu'un émetteur trop rapide n'inonde un receveur trop lent. UDP (User Datagram Protocol), protocole non fiable qui ne nécessite pas de connexion préalable (sans négociation). Ce protocole ne dispose pas de mécanisme de contrôle de flux. Ce protocole est surtout utilisé dans une architecture de clients/serveur voir de requête-réponse, pour la VOIP, les jeux en ligne, les appels vidéo. En effet on peut envoyer des plus grosses quantités de données d'un seul coup par rapport au TCP et on part du principe, lors de l'usage de l'UDP, que si on perd quelques paquets ce n'est pas trop grave. On préfère par exemple avoir une conversation téléphonique hachurée qu'avec du délai.
La couche application : Le modèle TCP/IP n'a pas besoin des couches Session ni Présentation. La couche application contient des protocoles haut-niveaux : FTP pour le transfert de fichiers, SMTP pour les mails, HTTP pour le WWW, DNS pour les noms de domaine...

4. Encapsulation des données

L'encapsulation, en informatique et spécifiquement pour les réseaux informatiques, est un procédé consistant à inclure les données d'un protocole dans un autre protocole.

Par exemple, l'Internet est basé sur l'Internet Protocol version 4 et la plupart des applications utilisent aussi bien l'UDP (User Datagram Protocol) que le TCP (Transmission Control Protocol). Ainsi un fragment de donnée est encapsulé dans un datagramme UDP qui lui-même est encapsulé dans un paquet IP, ce dernier étant alors envoyé via un protocole de la couche de liaison (par exemple Ethernet). La couche de liaison est responsable de la transmission physique des données ; IP ajoute l'adressage des ordinateurs individuels ; UDP ajoute « l'adressage des applications » (c'est-à-dire le port spécifiant le service comme un service web ou un serveur TFTP).

Le modèle OSI et la suite des protocoles Internet utilisent l'encapsulation.



Les différentes couches du modèle TCP/IP

5. Le routage IP

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Le routage est une tâche exécutée dans de nombreux réseaux, tels que le réseau téléphonique, les réseaux de données électroniques comme Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire où l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants. C'est grâce à ça que par exemple les mails sont envoyés aux bons destinataires.
Et pour ce faire différents mécanismes sont utilisés :

- Table de routage ou table d'acheminement : Elle se situe au niveau de chaque nœud et fournit l'information nécessaire pour atteindre le prochain nœud jusqu'à la destination.

- Algorithme de routage : C'est une fonction distribuée sur chaque nœud et qui a pour objectif de calculer les routes optimales pour atteindre une destination.

- Protocoles de routage : Elles permettent l'échange des informations de routes calculées par les algorithmes de routage et qui permettent la mise à jour dynamique des tables de routage.

Le routage est réalisé par trois fonctions :

- Le relayage ou forwading : Il permet de calculer le port de sortie en analysant l'adresse de destination du paquet, en consultant la table de routage.

- La commutation ou switching : Elle permet le transfert du ou des fragments de paquet d'un port d'entrée vers un port de sortie à travers un bus.

- L'ordonnancement ou scheduling : Il permet la détermination de l'ordre d'émission des paquets sur la liaison de sortie.

Il existe deux types de routage :

5.1. Les types de routage

Le routage statique : Nous parlons de routage statique lorsque les routeurs du réseau sont configurés un à un. En effet les routes que les paquets doivent suivre sont configurées manuellement permettant ainsi d'acheminer les paquets à leur destination.

Dans le routage statique, l'administrateur réseau doit paramétrer les routeurs pour leur donner des ordres de routage. C'est long, fastidieux et ne convient que pour de petites infrastructures.

Le routage dynamique : Le routage statique ou routage adaptatif est un processus au cours duquel un routeur transmet des données via différentes routes ou vers différentes destinations en fonction de l'état des circuits de communication dans un système.

Et donc dans le routage dynamique les mises à jour se font façon dynamique. Si la configuration du réseau change souvent pour des raisons diverses, alors il faut, pour maintenir le routage dans les bonnes conditions, que chaque routeur adapte sa table de routage à la nouvelle configuration. Cela n'est possible qu'à travers un processus automatique. C'est le rôle des protocoles de routage dynamique.

	Routage statique	Routage dynamique
Mise en œuvre dans des	Petits réseaux	Grands réseaux
Configuration	Manuel	Automatique
Les routes	Défini par l'utilisateur	Les itinéraires sont mis à jour en fonctions du changement de topologie
La construction de la table de routage	Les routes sont remplies à la main	Les routes sont remplies dynamiquement dans la table
Algorithme de routage	N'utilise pas d'algorithmes de routage complexe	Utilise des algorithmes de routage complexe pour effectuer des opérations de routage
Sécurité	Fournit une haute sécurité	Moins de sécurité en raison de l'envoi de diffusions et de multidiffusions
Echec du lien	L'échec de liaison bloque le routage	L'échec de liaison n'affecte pas le routage

Table de comparaison entre les deux types de routage

6. Les protocoles de communication

Un protocole est une méthode standard qui permet la communication entre des processus, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers, d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs etc.

6.1. Protocole ARP

Le protocole ARP qui signifie Address Resolution Protocol (Protocole de résolution d'adresse) permet de traduire une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse de protocole de couche liaison (typiquement une adresse MAC). Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche liaison (couche 2 du modèle OSI).

6.2. Protocole DHCP

Le protocole DHCP qui signifie Dynamic Host Configuration Protocol (Protocole de Configuration Dynamique des Hôtes) est un protocole réseau permettant l'attribution automatique d'une adresse IP et d'un masque d'une machine dans un réseau.

DHCP peut aussi configurer l'adresse de la passerelle par défaut, des DNS (Domain Name Serveur ou serveur de nom de domaine) etc.

6.3. Protocole FTP

Le protocole FTP qui signifie File Transfer Protocol (Protocole de Transfert de Fichier) est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

6.4. Protocole HTTP

Le protocole HTTP qui signifie HyperText Transfer Protocol (Protocole de Transfert Hypertexte) est un protocole de communication client-serveur développé pour le World Wide Web.

HTTP est un protocole de la couche application. Il peut fonctionner sur n'importe quelle connexion fiable, dans les faits on utilise le protocole TCP comme couche de transport. Un serveur http utilise par défaut le port 80.

6.5. Protocole HTTPS

Le protocole HTTP qui signifie HyperText Transfer Protocol Secure (Protocole de Transfert Hypertexte sécurisé) est un protocole de communication client-serveur. Le protocole HTTPS est donc la version sécurisée du protocole HTTP. En effet la communication entre le client et le serveur est chiffrée. Empêchant donc qu'un tiers non autorisé écoute la communication.
Le serveur Web est authentifié par le fait qu'en tout début de communication, un certificat est envoyé au client Web pour attester de la crédibilité du domaine. Cette mesure contribue à combattre les tromperies résultant de faux sites Web.
Le protocole HTTPS utilise par défaut le port 443.

6.6. Protocole RIP

Comme toujours, pour qu'une communication puisse s'établir, chaque interlocuteur doit parler la même langue. Il a été donc nécessaire de concevoir un protocole.

Le protocole RIP qui signifie Rounting Information Protocol (Protocole d'Information de Routage) est un protocole de type vecteur de distance s'appuyant sur l'algorithme de détermination des routes décentralisé Bellman-Ford. Il permet à chaque routeur de communiquer avec les routeurs voisins.

La métrique utilisée est la distance qui sépare un routeur d'un réseau IP déterminé quant au nombre de sauts.

Pour chaque réseau IP connu, chaque routeur conserve l'adresse du routeur voisin dont la métrique est la plus petite. Ces meilleures routes sont diffusées toutes les 30 secondes.

6.7. Protocole Telnet

Le protocole Telnet pour Terminal Network est un protocole utilisé sur tout réseau TCP/IP, permettant de communiquer avec un serveur distant en échangeant des lignes de texte et en recevant des réponses également sous forme de texte.

Créé en 1969, Telnet est un moyen de communication très généraliste et bidirectionnel. Il appartient à la couche application du modèle OSI et du modèle ARPA.

Il était notamment utilisé pour administrer des serveurs UNIX distants ou de l'équipement réseau. Notons néanmoins que le protocole Telnet n'est pas sécurisé car les messages sont échangés en clairs.

Le protocole Telnet repose sur trois concepts fondamentaux :

- Le paradigme du terminal réseau virtuel
- Le principe d'options négociées
- Les règles de négociation

En bref le protocole Telnet est un protocole de transfert de données non sûr, les données qu'il véhicule circulent en clair sur le réseau. Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.

6.8. Protocole DNS

Le protocole DNS qui signifie Domain Name System (Système de noms de domaine) , est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements. En fournissant dès les premières années d'Internet, autour de 1985, un service distribué de noms, le DNS a été un composant essentiel du développement du réseau.

Au niveau protocolaire, seules les adresses IP sont utilisées pour déterminer les partenaires d'une communication. Mais dans l'usage courant d'Internet, on utilise des noms pour joindre des machines sur le réseau : c'est plus facile à manipuler que les adresses IP car par exemple dans un réseau où les adresses IP peuvent être distribuées dynamiquement et par conséquent seront difficiles à retenir.

Le protocole et le système DNS permet de résoudre des noms en adresses IP. DNS est une sorte de service mondial de correspondance entre des noms et des adresses IP, mais uniquement ; plus précisément, DNS est un système d'interrogation d'un registre à portée mondiale.

Les leaders du marché IT recommandent son usage pour déployer leurs solutions.

6.9. Protocole UDP

Le User Datagram Protocol, abrégé en UDP (protocole de datagramme utilisateur), est un protocole permettant l'envoi sans connexion de datagrammes dans des réseaux basés sur le protocole IP. Afin d'atteindre les services souhaités sur les hôtes de destination, le protocole utilise des ports qui constituent un élément essentiel de l'entête UDP. À l'instar de nombreux autres protocoles de réseau, l'UDP fait partie de la suite des protocoles Internet**.** Il intervient au niveau de la couche transport et joue ainsi le rôle d'intermédiaire entre la couche réseau et la couche application.

Le User Datagram Protocol est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, quatrième couche de ce modèle, comme TCP. Il a été défini par David P. Reed et est détaillé dans la RFC 768.

Le rôle de ce protocole est de permettre la transmission de données (sous forme de datagrammes) de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Aucune communication préalable n'est requise pour établir la connexion, au contraire de TCP (qui utilise le procédé de handshaking). UDP utilise un mode de transmission sans connexion.

L'intégrité des données est assurée par une somme de contrôle sur l'en-tête. L'utilisation de cette somme est cependant facultative en IPv4 mais obligatoire avec IPv6. Si un hôte n'a pas calculé la somme de contrôle d'un datagramme émis, la valeur de celle-ci est fixée à zéro. La somme de contrôle inclut également les adresses IP de la source et de la destination.

6.10. Protocole SSH

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

La sécurité joue toujours un rôle majeur sur Internet, c'est pourquoi le protocole de sécurité SSH est fermement intégré dans la pile de protocoles TCP/IP**.** Le protocole SSH permet aux utilisateurs d'établir une connexion sécurisée entre deux ordinateurs. Le protocole réseau est utilisé depuis 1995 et a été depuis lors révisé et actualisé à plusieurs reprises.

Par défaut le protocole SSH utilise le port 22.

6.11. Protocole IP

Internet Protocol est un protocole sans connexion qui, en tant qu'élément central de la famille des protocoles Internet (un ensemble d'environ 500 protocoles réseau), est responsable de l'adressage et de la fragmentation des paquets de données dans les réseaux numériques. Avec le protocole de transport TCP (Transmission Control Protocol), l'IP constitue la base de l'Internet. Pour envoyer un paquet de l'expéditeur au destinataire, le protocole IP définit une structure de paquets qui résume les informations envoyées. Le protocole détermine la manière dont les informations sur la source et la destination des données sont décrites et sépare ces informations des données informatives dans l'en-tête IP. Ce type de format de paquet est également connu sous le nom de datagramme IP.

En 1974, l'Institute of Electrical and Electronics Engineers (IEEE) a publié un document de recherche des informaticiens américains Robert Kahn et Vint Cerf qui décrivait un modèle de protocole pour une connexion mutuelle de paquets de réseau basé sur ARPANET, le prédécesseur d'Internet. En plus du

protocole de contrôle de transmission TCP, le composant principal de ce modèle était le protocole IP, qui, en plus d'une couche d'abstraction spéciale, permettait la communication à travers différents réseaux physiques. Au cours des années suivantes, de plus en plus de réseaux de recherche ont été consolidés sur la base de cette combinaison de protocoles TCP/IP, qui a finalement été spécifiée en 1981 comme standard dans le RFC 791.

6.12. Protocole SSL

SSL signifie Secure Sockets Layer. En bref, il s'agit d'une technologie standard destinée à la sécurité de la connexion Internet et à la protection des données sensibles qui sont transmises entre deux systèmes, empêchant les criminels de lire et de modifier les informations transférées, y compris d'éventuelles informations personnelles. Les deux systèmes peuvent être un serveur et un client (par exemple, un site d'achat et un navigateur) ou un serveur et un autre serveur (par exemple, une application avec des informations personnelles identifiables ou des informations de paie).

Il agit en veillant à ce que les données transférées entre les utilisateurs et les sites, ou entre les deux systèmes restent impossibles à lire. SSL utilise l'algorithme de chiffrement pour brouiller les données en transit, empêchant les pirates de les lire lorsqu'elles sont envoyées via la connexion. Ces informations peuvent être sensibles ou personnelles, et inclure des numéros de cartes de crédit ou d'autres informations financières, des noms et des adresses.

6.13. Protocole POP3

POP3 est un protocole de transmission qui permet à un client de courrier électronique de récupérer le courrier électronique à partir d'un serveur.
POP3 est le bon choix pour vous si vous faîtes attention au temps passé en ligne pour des raisons de coût. Avec cette procédure, les emails sont toujours transmis du serveur à l'appareil local. Si vous ne recevez et ne lisez vos emails que sur un ordinateur spécifique, vous pouvez utiliser POP3 sans hésitation.
Cependant, si vous voulez gérer vos emails en ligne et accéder à votre compte email à partir de différents appareils, IMAP est le bon choix.

6.14. Protocole IMAP

Au sens strict, Interactive Message Access Protocol, devenu IMAP 4 Internet Message Access Protocol est un protocole qui permet d'accéder à ses courriers électroniques directement sur les serveurs de messagerie. Son fonctionnement est donc à l'opposé de POP qui, lui, récupère les messages (depuis le poste de travail) et les stocke localement via un logiciel spécialisé (par défaut, ce client supprime sur le serveur les messages récupérés). L'évolution des différentes versions d'IMAP (IMAP 4) en fait aujourd'hui un protocole permettant également de récupérer les messages localement.

7. Les équipements réseaux

Les équipements d'interconnexion d'un réseau informatique sont les briques constitutives des réseaux informatiques physiques.

L'interconnexion des réseaux c'est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques comme le concentrateur, le routeur etc. Ces périphériques servent aussi à interconnecter les ordinateurs d'une organisation, d'un campus, d'un établissement scolaire, d'une entreprise.

Dans ce cas, des équipements spécifiques sont nécessaire. Lorsqu'il s'agit de deux réseaux de meme type, il suffit de faire passer les trames de l'un vers l'autre. Dans le cas de deux réseaux qui utilisent des protocoles

différents, il est nécessaire de procéder à une conversion de prototype avant de transporter les trames (paquets de données).

7.1. Commutateur (switch)

Les commutateurs jouent généralement un rôle plus intelligent que les concentrateurs. Un commutateur est un dispositif multiport qui améliore l'efficacité du réseau. Le commutateur gère des informations de routage limitées sur les nœuds du réseau interne et permet des connexions à des systèmes tels que les concentrateurs ou les routeurs. Les brins des réseaux locaux sont généralement connectés à l'aide de commutateurs. En général, les commutateurs peuvent lire les adresses matérielles des paquets entrants afin de les transmettre à la destination appropriée.

7.2. Routeur

Les routeurs contribuent à transmettre des paquets vers leurs destinations en traçant un chemin dans l'océan des équipements réseau interconnectés, à l'aide de différentes topologies de réseau. Les routeurs sont des appareils intelligents qui stockent des informations sur les réseaux auxquels ils sont connectés. La plupart des routeurs peuvent être configurés de manière à fonctionner comme pare-feu à filtrage de paquets et utilisent des listes de contrôle des accès (ACL). Les routeurs, conjointement avec une unité de service de canal/unité de service de données (CSU/DSU), servent également à traduire le tramage LAN en tramage WAN. Ceci est nécessaire car les réseaux locaux (LAN) et les réseaux étendus (WAN) utilisent des protocoles différents. De tels routeurs sont appelés routeurs frontières. Ils assurent la connexion externe d'un réseau local à un réseau étendu, et ils fonctionnent à la frontière de votre réseau.

7.3. Pont (bridge)

Les ponts servent à connecter deux ou plusieurs hôtes ou segments de réseau. Le rôle fondamental des ponts dans l'architecture réseau est de stocker et de transférer les trames entre les différents segments qu'ils relient. Ils utilisent les adresses MAC (contrôle d'accès au support) des équipements pour le transfert des trames. En examinant l'adresse MAC des appareils connectés à chaque segment, les ponts peuvent transmettre les données ou les empêcher de traverser. Les ponts peuvent également être utilisés pour connecter deux réseaux locaux physiques en un réseau local logique plus grand.

7.4. Passerelle (Gateway)

Les passerelles opèrent généralement au niveau des couches Transport et Session du modèle OSI. Au niveau de la couche Transport et des couches supérieures, de nombreux protocoles et standards issus de différents fournisseurs sont utilisés ; les passerelles servent à les gérer. Les passerelles assurent la traduction entre des technologies réseau telles que l'interconnexion des systèmes ouverts (OSI) et TCP/IP (protocole de contrôle de transmission/protocole Internet). Ainsi, les passerelles connectent deux ou plusieurs réseaux autonomes, chacun ayant ses propres algorithmes de routage, protocoles, topologie, service de noms de domaine, procédures et politiques d'administration réseau.

7.5. Modem

Les modems (modulateurs-démodulateurs) servent à transmettre des signaux numériques via des lignes téléphoniques analogiques. Les signaux numériques sont donc convertis par le modem en signaux analogiques de différentes fréquences et transmis à un autre modem au lieu de réception. Le modem récepteur effectue la transformation inverse et fournit une sortie numérique au dispositif qui y est connecté, généralement un ordinateur. Les données numériques sont habituellement transférées vers/depuis le modem via une liaison série et une interface standard RS-232. De nombreuses compagnies téléphoniques offrent des services DSL et de nombreux câblo-opérateurs utilisent des modems comme terminaux finaux pour

l’identification et la reconnaissance des utilisateurs individuels. Les modems opèrent à la fois sur les couches Physique et Liaison de données.

7.6. Un répétiteur

Un répéteur est un appareil électronique qui amplifie le signal qu’il reçoit. Vous pouvez considérer un répéteur comme un appareil qui reçoit un signal et le retransmet à un niveau plus élevé ou à une puissance supérieure, afin qu’il puisse couvrir de plus longues distances, plus de 100 mètres pour les câbles LAN standard. Les répéteurs opèrent sur la couche Physique.

7.7. Un point d’accès

Même si un point d’accès peut techniquement comporter une connexion câblée ou sans fil, il s’agit généralement d’un dispositif sans fil. Un point d’accès fonctionne au niveau de la deuxième couche OSI, la couche Liaison de données, et il peut fonctionner soit comme un pont reliant un réseau câblé standard à des appareils sans fil ou comme un routeur transmettant des données d’un point d’accès à un autre.

7.8. Un concentrateur (hub)

Les concentrateurs connectent plusieurs équipements du réseau informatique. Un concentrateur sert également de répéteur, en ce sens qu’il amplifie les signaux, qui se détériorent après avoir parcouru de longues distances sur les câbles de connexion. Le concentrateur est le plus simple de la famille des équipements de connexion réseau, car il connecte des composants LAN ayant des protocoles identiques.

7.9. Un serveur

Un serveur informatique est un dispositif informatique qui offre des services à un ou plusieurs clients. Les services les plus courants sont :

- L’accès aux informations
- Le courrier électronique
- Le partage de périphériques
- Le commerce électronique
- Le stockage en base de données
- La gestion de l’authentification et du contrôle d’accès
- Le jeu et la mise à disposition de logiciels applicatifs

En fonctionnement, un serveur répond automatiquement à des requêtes provenant d’autres dispositifs informatiques (les clients), selon le principe dit client-serveur. Le format des requêtes et des résultats est normalisé, se conforme à des protocoles réseaux et chaque service peut être exploité par tout client qui met en œuvre le protocole propre à ce service.

Les serveurs sont utilisés par les entreprises, les institutions et les opérateurs de télécommunication. Ils sont courants dans les centres de traitement de données et le réseau Internet.

7.10. Carte réseau

La carte réseau est l'interface entre votre ordinateur et le réseau. Elle reçoit les données émises par l'ordinateur et les transfère vers un autre appareil présent sur le réseau, contrôle l'ensemble de ces données et les flux échangés. Elle reçoit également des informations depuis le réseau et les transcrit pour que celles-ci soient lues et traitées par votre ordinateur. Elle assure donc les échanges et les transferts entre votre PC et les autres appareils présents sur le réseau.

IV. La sécurité des systèmes d'information

La sécurité des systèmes d'information est un large terme qui réunit les moyens humains, technologiques, organisationnels qui tentent de garantir certaines propriétés d'un système d'information.

1. Objectif de la sécurité sur les systèmes d'information

Pour sécuriser un système d'information il faut assurer :

- La disponibilité des données : La disponibilité des données consiste à assurer l'accès en temps réel aux ressources du système d'information.

- L'intégrité des données : L'intégrité des données consiste à préserver l'état des données afin de garantir et préserver la validité et l'exactitude des données.

- La confidentialité des données : La confidentialité des données consiste à la protection de toutes les données stockées ou transitant contre l'interception ou la lecture par des personnes non-autorisées.

-La non-répudiation : La non-répudiation est le fait de s'assurer qu'aucune partie ayant participé à une transaction ne peut pas nier y avoir participé.

2. Quelques notions sur la sécurité informatique

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information.

Assurer la sécurité du système d'information est une activité du management du système d'information.

2.1. Vulnérabilité

On appelle vulnérabilité l'existence d'une faiblesse dans un système d'information se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent. Par exemple, une erreur d'implémentation d'une application, est exploitée pour pénétrer notre système d'information (vol d'information, refus de service, etc.). Elle peut être également provenir d'une mauvaise configuration.

2.2. Menace

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, que ce soit interne ou externe à l'entreprise. La probabilité qu'elle soit une faille de sécurité, est évaluée par des études statistiques même si elle est difficile à réaliser.

2.3. Risque

Les menaces engendrent des risques et des coûts humains et financiers : perte de confidentialité des données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété. Les risques peuvent survenir si les systèmes menacés présentent des vulnérabilités.

2.4. Attaque

Une attaque est le résultat de l'exploitation d'une faille. Une attaque réussie sur un système d'information peut entrainer chez la structure une perte de notoriété, une mauvaise réputation, une diminution de chiffre d'affaires, le vol d'information.

2.5. Intrusion

L'intrusion est une opération qui consiste à accéder, sans autorisation, aux données d'un système informatique ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place.

Une intrusion informatique peut être perpétrée pour diverses raisons, notamment pour modifier ou voler de l'information confidentielle, fausser, contaminer ou détruire les données du système.

2.6. Exploits

C'est une porte ou faille utilisée pour pénétrer un système d'information.

Que ce soit à distance (remote exploit) ou sur la machine sur laquelle cet exploit est exécuté (local exploit), le but de cette manœuvre est de s'emparer des ressources d'un ordinateur ou d'un réseau, d'accroitre le privilège d'un logiciel ou d'un utilisateur sur la machine cible, ou encore d'effectuer une attaque par déni de service.

2.7. Zero-Day attaque

Une attaque qui exploite une vulnérabilité d'un système avant la mise à jour de ce dernier.

2.8. Le malware

C'est le terme que l'on utilise pour désigner les menaces informatiques visant à nuire un ordinateur, un téléphone ou tout autre appareil connecté. Peu importe sa forme, il a pour tâche de voler, effacer ou corrompre des données et les réseaux.

2.9. Le virus

Le virus est un type de malware caché dans un logiciel légitime. Lorsqu'on l'exécute, le virus se propage et infecte les appareils.

2.10. Le vers

Le vers informatique se répand sur internet. Il peut s'installer sur un ordinateur à partir d'un courriel, d'un fichier téléchargé ou par messagerie instantanée. Il est beaucoup plus courant que le virus aujourd'hui.

2.11. Le cheval de Troie

Appelé aussi logiciel espion, le cheval de Troie est un logiciel malveillant qui s'insinue dans l'ordinateur de sa victime en secret et peut faire ce qu'il veut sans qu'on soupçonne quoi que ce soit : filmer l'utilisateur à son insu, enregistrer ses mots de passe etc.

2.12. Hacher

Il existe huit types de hackers :

- Les Black Hats : Leurs objectifs est de cracker, détruire un système, voler des informations, provoquer l'arrêt d'un système.

- Les White Hats : Leurs objectifs est d'attaquer un système pour ensuite proposer des recommandations pour améliorer la sécurité.

- Les Grey Hats : Attaque pour détruire ou pour défendre un système.

- Les suicide hackers : Ils attaquent pour détruire un système critique.

- Les script kiddies : Leurs buts est de voler des scripts, des outils, des logiciels et des données d'un système.

- Les spy hackers : Ils sont employés par une entreprise pour qu'ils attaquent leur système.

- Les cyber terroristes : Ils attaquent avec comme motivation la religion ou la politique.

- Les Sponsor hackers : Ils sont employés par une entreprise pour pénétrer le système d'une autre entreprise.

2.13. Contre mesure

C'est les capacités à disposition et les mesures mises en place pour se défendre contre les intrusions.

2.14. Cryptographie

La cryptographie est une discipline de la cryptologie s'attachant à protéger des messages pour assurer la confidentialité, l'authenticité et l'intégrité en s'aidant souvent de secrets ou clés.

2.14.1. Chiffrement

Le chiffrement ou cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.

Ce principe est généralement lié au principe d'accès conditionnel.

Notons qu'il existe deux types de chiffrement :

- Le chiffrement à clé symétrique ou à clé secrète

- Le chiffrement à a clé asymétrique

2.14.2. Déchiffrement

C'est de retrouver, le message clair à partir d'un message chiffré.

2.14.3. Clé

La clé, utilisée à un algorithme permet le chiffrement ou le déchiffrement d'un message. La clé est souvent partagée entre l'émetteur et le récepteur et implémentée dans les opérations de chiffrement et de déchiffrement.

2.15. Cryptanalyse

La cryptanalyse est la science qui consiste à retrouver le message clair à partie d'un message chiffré sans avoir à sa possession la clé de chiffrement.

2.16. Cryptologie

La cryptologie qui signifie étymologiquement la science du secret, est considérée comme une science que depuis peu de temps. Elle englobe la cryptographie et la cryptanalyse.

3. Politiques de sécurité

C'est un document qui définit l'ensemble des normes et configurations à respecter dans le système d'information.

3.1. But de la politique de sécurité

Le but donc d'une politique de sécurité est de fixer des principes visant à garantir la protection des ressources informatiques et des télécommunications en tenant compte des intérêts de l'organisation et de la protection des utilisateurs.

Les ressources du parc informatique doivent être protégées afin de garantir la confidentialité, la disponibilité et l'intégrité des informations qu'elles traitent, dans le respect de la législation en vigueur.

3.2. Périmètre et domaine d'application

La politique de sécurité s'applique à toute personne qui utilise les ressources du parc informatique de l'organisation.

3.3. Utilisation des ressources informatiques et accès utilisateurs

Les ressources du parc informatique sont destinées à des fins strictement professionnels.

Les ressources informatiques et de télécommunications autorisées sont définies de manière exhaustives par l'organe compétent désigné.

3.4. Mesures en cas de violation

La violation volontaire ou par négligence des règles issues de la politique de sécurité peut entrainer la prise de mesures par le service compétent permettant d'éviter la répétition de la violation.

3.5. Communication

La politique de sécurité informatique de l'organisation, ainsi que les règles et procédures qui en découlent sont communiquées à l'ensemble du personnel, et font partie intégrante du statut du personnel, ainsi qu'aux intervenants extérieurs avant leur première intervention.

4. Quelques attaques sur les réseaux

Man-in-the-Middle : L'attaque de l'homme du milieu (HDM) ou man-in-the-middle attack (MITM), parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été

compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre.

ARP poisonning : Connu aussi sous le nom de ARP Spoofing, ARP Poisoning est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi. Cette technique permet à l'attaquant de détourner des flux de communications transitant entre une machine cible et une passerelle : routeur, box, etc. L'attaquant peut ensuite écouter, modifier ou encore bloquer les paquets réseaux.

5. Quelques attaques sur les hôtes

DoS : Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (DDoS).

Backdoor Attack : Une attaque par porte dérobée utilise un type spécifique de malware afin que les pirates puissent éviter les procédures normales d'authentification pour accéder à un système cible.
Par conséquent, les auteurs peuvent passer par toutes les ressources telles que les serveurs de fichiers et les bases de données pour émettre des commandes et modifier les paramètres du système sans être découverts.

6. Menaces sur les applications

SQL injection : La faille injection SQL est méthode d'exploitation de faille de sécurité d'une application interagissant avec une base de données. Elle permet d'injecter dans la requête SQL en cours un morceau de requête non prévu par le système et pouvant en compromettre la sécurité.

XSS : Les attaques de script cross-site (XSS) sont des attaques de type injection dans lesquelles des scripts malveillants sont injectés dans des sites web et pourtant dignes de confiance. Les attaques XSS se produisent lorsqu'un attaquant utilise une application Web pour envoyer du code malveillant, généralement sous la forme d'un script coté navigateur, à un utilisateur final diffèrent.

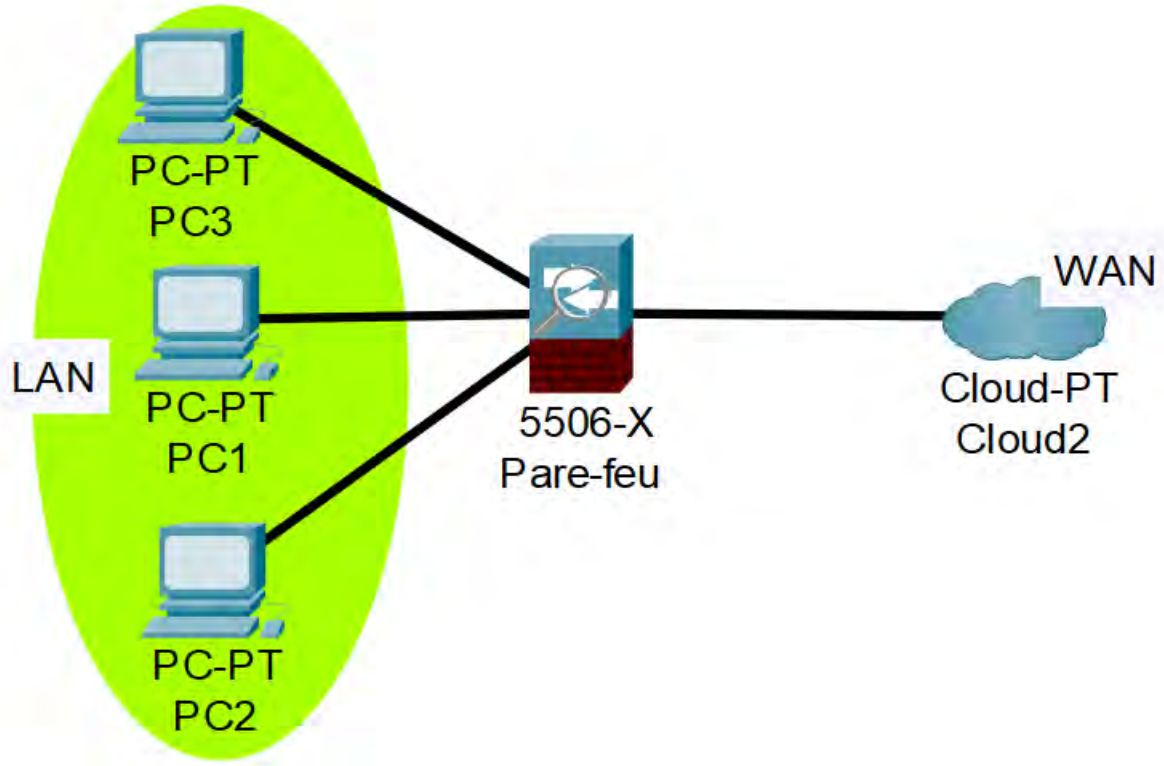
7. Les contres mesures

7.1. Antivirus

Logiciel censé protéger un ordinateur contre les logiciels néfastes ou fichiers potentiellement indésirables. L'antivirus ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.

7.2. Pare-Feu

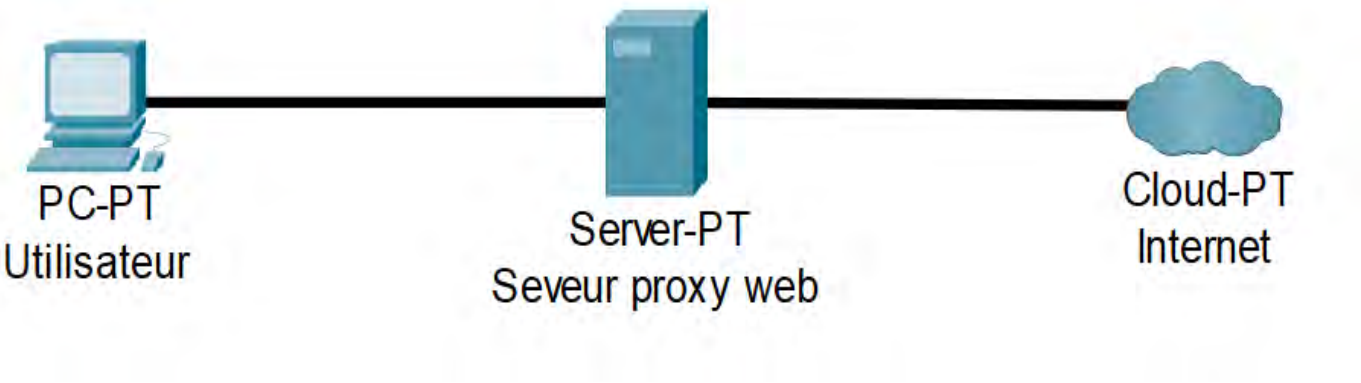
Un pare-feu est un logiciel et/ou matériel qui filtre et protège un système en bloquant les connexions venant de l'extérieur (entrées) ou de l'intérieur (sorties) pour empêcher ou autoriser l'accès à des services Web. Il permet aussi de faire de la translation d'adresse pour servir de routeur.



Exemple d'emplacement d'un pare-feu dans un réseau

7.3. Serveur de proxy

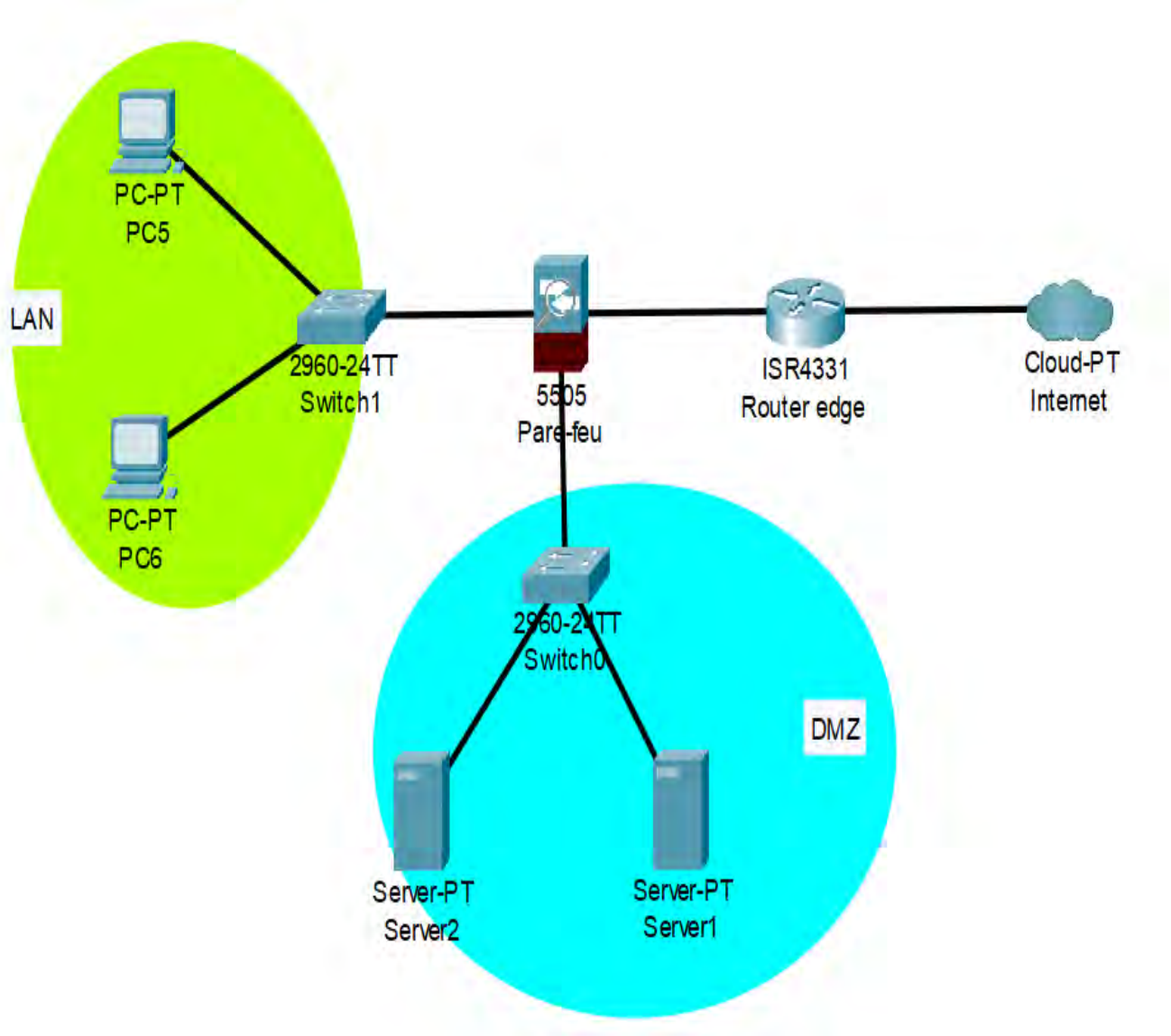
Un serveur proxy joue le rôle de passerelle entre Internet et l'utilisateur. Le serveur proxy fournit différents services. Il assure la sécurité et la confidentialité des données, selon le type d'utilisation, les besoins ou la politique de sécurité de l'organisation.



Exemple de serveur proxy dans un réseau

7.4. Zone démilitarisée (DMZ)

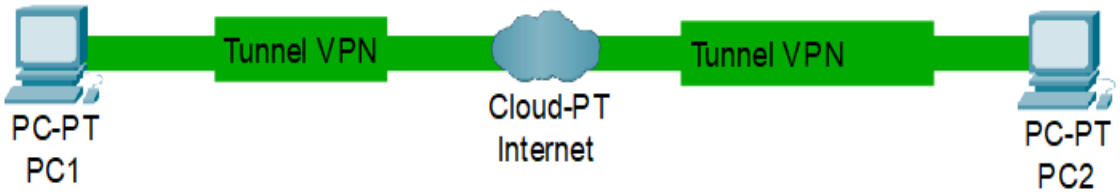
Une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis internet, et qui n'ont pas besoin d'accéder au réseau local.



Emplacement d'un DMZ dans un réseau

7.5. Réseau privé virtuel (VPN)

Un réseau privé virtuel est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics. Le terme VPN est notamment utilisé dans le télétravail.



Exemple d'un tunnel VPN

V. Conclusion

Dans ce chapitre, dans une première partie, nous avons défini des notions sur les réseaux informatiques en général en les classant suivant leur architecteur, leur topologie et leur étendu.

Dans une deuxième partie, nous avons vu quelques protocoles de communications dans les réseaux informatiques ensuite les outils utilisés pour la mise en œuvre de ces protocoles.

Et enfin dans la troisième partie, nous avons abordé quelques notions sur les vulnérabilités associées au système d'information et les contres mesures.

Chapitre II :
Etude théorique sur les systèmes de détection d'intrusion

I. Introduction

L'interconnexion des réseaux, c'est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques (récepteur, concentrateur, pont, routeur, modem), ils servent aussi à interconnecter les ordinateurs d'un parc informatique.

Un Système de Détection d'Intrusion est une sonde placée judicieusement sur un réseau ou un système, et qui va repérer les activités douteuses ou anormales sur cette cible et alerter les responsables sécurité. De cette façon, on peut obtenir une connaissance des tentatives réussies (ou non) d'attaque ou d'intrusion sur le système. On différencie plusieurs types d'IDS, à savoir les NIDS (ou Network Intrusion Detection System), qui se basent sur des analyses réseau, les HIDS (ou Host Intrusion Detection System), qui surveillent l'activité d'un hôte, et enfin les IDS hybrides, qui combinent HIDS et NIDS.

II. Contexte

Les entreprises évoluent dans un monde compétitif et concurrentiel. Les ressources humaines restent importantes mais il ne faut non plus négliger les informations qu'elles produisent dans le système d'information de toute entreprise. Cependant, les données, élément majeur du système d'information, se doivent d'être protégées. Leur protection se résume en trois éléments que sont : la confidentialité, l'intégrité, la disponibilité.

Dans le contexte actuel avec l'explosion de l'internet, on assiste au développement des codes malveillants d'où la nécessité de mettre en place des mesures de sécurité pour protéger tout système d'information. Alors la mise en place d'un système pour détecter et prévenir les attaques sur les systèmes informatiques devient une priorité.

III. Problématique

Cependant dans la pratique les entreprises se heurtent rapidement à de nombreuses difficultés, et celles-ci croissent de manière proportionnelle à la taille et à la complexité des systèmes d'information de l'entreprise : temps de réaction trop long, multiplication des types de systèmes et des vulnérabilités associées, manque d'expertise technique, problème de régression, coûts de déploiement, gestion des matériels nomades.

IV. Solution

Donc la meilleure façon de protéger un réseau ou un système informatique est de détecter les attaques et de se défendre avant même qu'elles ne puissent causer des dommages. Ainsi beaucoup font appel à cet effet aux systèmes de détection d'intrusion ou aux systèmes de prévention d'intrusion les plus polyvalents.

V. Système de détection d'intrusion

1. Définition d'un IDS

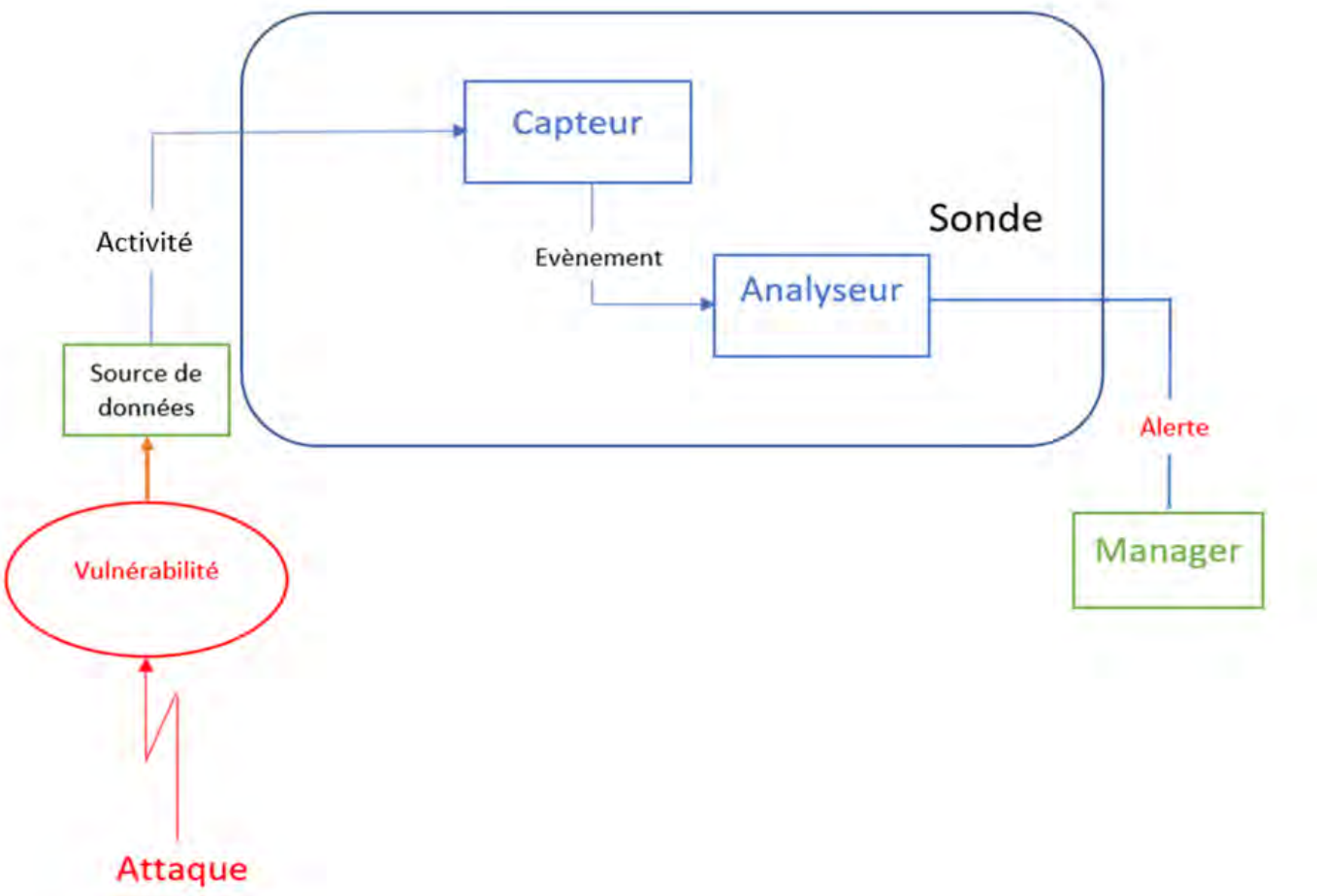
Le premier modèle de détection d'intrusion est développé en 1984 par Dorothy Denning et Peter Neuman, qui s'appuie sur des règles d'approche comportementale. Ce système appelé IDES (Intrusion Detection Expert System), en 1988 Il est développé à un IDS (système de détection d'intrusion). Ce dernier est un ensemble de composants logiciels et/ou matériels destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte), son rôle est de surveiller les données qui transitent sur ce système. Il permet ainsi d'avoir une action de détection et/ou d'intervention sur les risques d'intrusion. Afin de détecter les attaques que peut subir un système ou un réseau informatique.

Deux notions sont utilisées lorsque nous parlons d'IDS :

- Faux positif : Qui consiste à une alerte provenant d'un système de détection d'intrusion mais qui ne correspond pas à une attaque réelle.
- Faux négatif : Qui consiste à une attaque ou à une intrusion réelle mais qui n'est pas alertée.

2. L'architecture d'un IDS

Le schéma suivant décrit les trois composants qui composent un système de détection d'intrusion.
Dans ce schéma nous voyons les interactions entre ces trois éléments.



Architecture d'un IDS

Capteur : Les capteurs sont placés sur le réseau et ont généralement deux cartes réseaux : l'une est en mode furtif c'est-à-dire ne possède aucune adresse IP, l'autre est reliée à l'appareil de sécurité. Les capteurs observent donc l'activité par le biais d'une source de données et fournit à l'analyseur une séquence d'évènement qui renseignent l'évolution de l'état du système. On distingue trois types de capteurs : les capteurs systèmes, les capteurs réseaux et les capteurs applicatifs.

Analyseur : L'analyseur analyse la séquence fournit par le capteur et détermine s'il y'a des éléments caractéristiques d'une activité malveillante

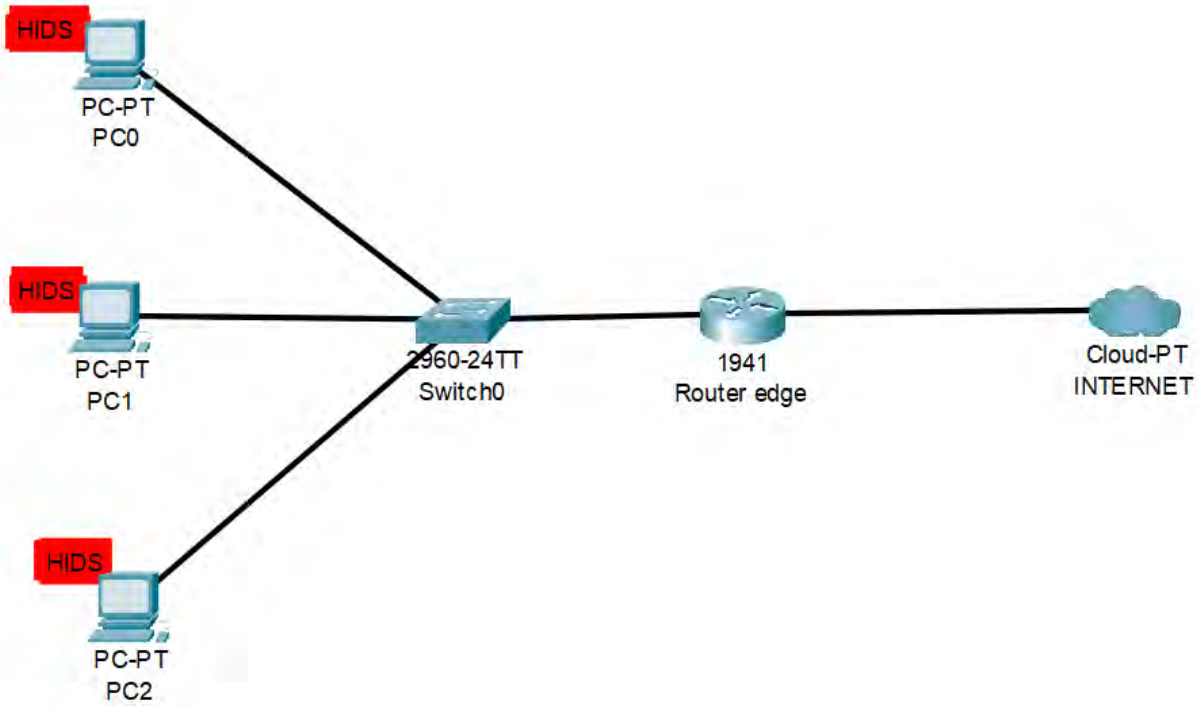
Manager : Le manager collecte les alertes produites par le capteur les met en forme et les présente à l'opérateur. Eventuellement le manager peut être chargé de la réaction à adopter.

3. Les types d'IDS

Les types d'attaque mis en œuvre par les attaquants étant divers, il existe différents types d'IDS :

3.1. Les systèmes de détection d'intrusion basée sur l'hôte (HIDS)

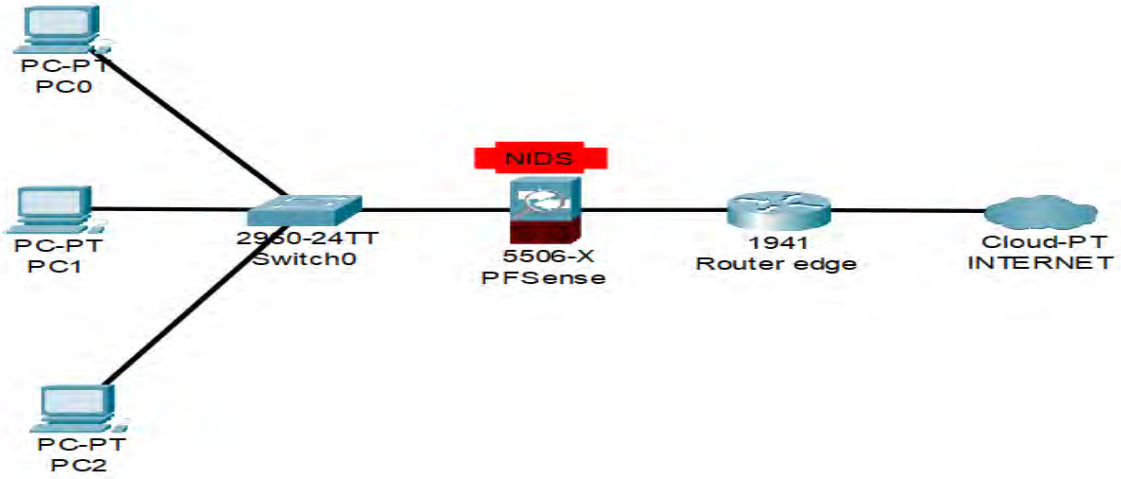
L'HIDS surveille le trafic sur une seule machine. Il analyse des données telles que les journaux système et vérifie l'intégrité des fichiers. Pour que le HIDS soit efficace il faut que le système soit sain. En effet si le système a été préalablement compromis le HIDS ne sera pas efficace.



Exemple d'un HIDS dans un réseau

3.2. Les systèmes de détection d'intrusion basée sur le réseau (NIDS)

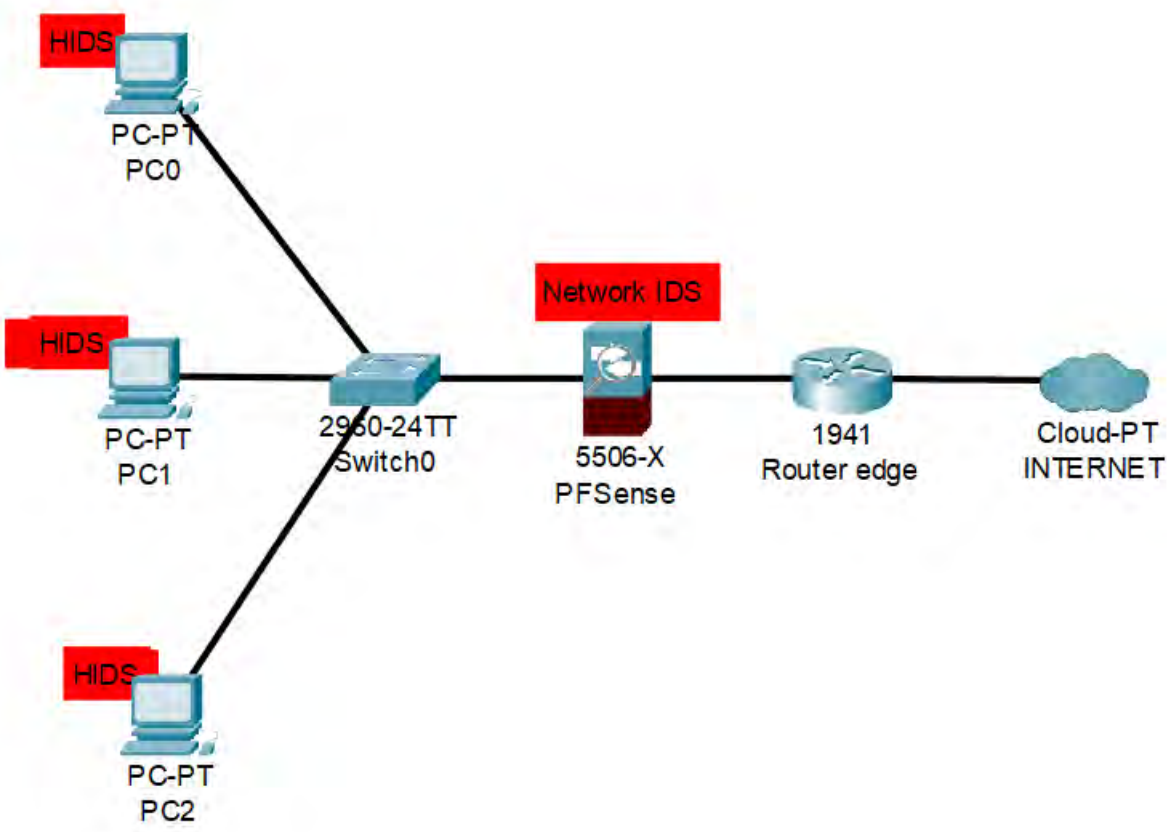
Les NIDS sont des IDS dédiés aux réseaux. Ils comportent généralement une sonde qui écoutent sur le segment réseau à surveiller en temps réel. Donc, le NIDS analyse et génère des alertes si les paquets sembles dangereux et s'il détecte une intrusion.



Exemple d'un NIDS dans un réseau

3.3. Le système de détection d'intrusion hybride

IDS hybride rassemble les caractéristiques de HIDS et NIDS. En effet, l'IDS hybride permet de surveiller et d'analyser le réseau et les hôtes du réseau. Les sondes agissent comme des NIDS ou des HIDS selon leur emplacement, ils réunissent toutes les alertes et les remontent au niveau d'une machine ou elles sont centralisées.



Exemple d'un IDS hybride dans un réseau

	Avantages	Inconvénients
HIDS	-Faux positifs moins courant -Observe les attaques sur les hôtes -Détecte des attaques impossibles à détecter par les NIDS car sur le réseau le trafic est souvent crypté	-Détecte moins les scans -Plus vulnérable aux attaques DoS/DDoS -Consomme plus de CPU -Problème d'interopérabilité -taux élevé de faux négatifs
NIDS	-Capteur difficilement détectable -Détecte plus facilement un scan -Filtrage du trafic	-Probabilité de faux positifs élevés -Coût -Point névralgique du réseau
IDS hybride	-Réaction sur les analyseurs -Meilleure corrélation -Moins de faux négatifs	-Probabilité de faux positifs élevés

Tableau comparatif des différents IDS

4. Mode de fonctionnement d’un IDS

On distingue deux aspects dans le fonctionnement d’un IDS : le mode de détection d’une anomalie et la réponse apportée après la détection.

Le mode de détection : Nous notons deux types de détection :

- La détection d’anomalies : Elle consiste à détecter des anomalies par rapport au trafic habituel. L’IDS découvre d’abord le fonctionnement normal des éléments surveillés de ce fait ils sont en mesure de signaler les divergences par rapport au fonctionnement de référence.

- La reconnaissance des signatures : Cette méthode consiste à rechercher les empreintes d’attaques connues sur l’élément que l’IDS surveille. De ce fait, des mises à jour fréquentes sont nécessaires.

La réponse apportée : Il existe deux types de réponse :

-La réponse active : Elle a pour but de détecter puis de stopper une attaque. Donc le firewall bloque le trafic malveillant en fermant le port ou en interdisant l’adresse IP de l’attaquant.

- La réponse passive : Elle a pour but de seulement détecter une attaque puis enregistrer les intrusions dans un fichier log.

5. Les limites d’un IDS

Bien qu’ils aient des avantages les IDS ont aussi des limites :

Consommation des ressources : Les système de détection d’intrusion sont trop consomment beaucoup de ressources. Notons aussi que les fichiers logs peuvent avoir de grandes tailles.

Vulnérabilité aux attaques DoS : Le hacker peut tenter une attaque par déni de service au niveau du système de détection d’intrusion ou au niveau du système d’exploitation de la machine supportant l’IDS.

Surcharge : Les IDS peuvent être surchargés dans le cas où le trafic est important, en effet un tel trafic sera difficile à analyser.

V. Conclusion

Dans ce chapitre, nous avons dans une première partie poser la problématique à laquelle se confrontent les entreprises, proposer de mettre en place un IDS comme solution de la problématique posée.

Nous avons étudié ce qu’est un IDS en le définissant et en étudiant son architecture.

Nous avons également théoriquement vu comment fonctionne un IDS et ses limites.

Chapitre III :

Mise en place d'un Système de Détection d'Intrusion

I. Introduction

Dans ce chapitre nous allons implémenter l'IDS Snort sous pfSense. En effet nous allons dans un premier temps mettre en place pfSense pour ensuite mettre installer et configurer notre IDS Snort.

Enfin nous ferons quelques tests pour voir comment notre IDS va réagir face à ces menaces.

1. Présentation de pfSense

pfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD.

Il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou de petite entreprise.

1.1. Les services proposés par pfSense

pfSense offre une multitude de services parmi ceux-là nous pouvons citer :
- La gestion des interfaces réseau
-Le filtrage du trafic
-La traduction d'adresse réseau (NAT)
- La gestion des accès internet
-Les services VPN (SSL, IPSec, etc.)
-Serveur DHCP
-Serveur DNS
-Solution proxy

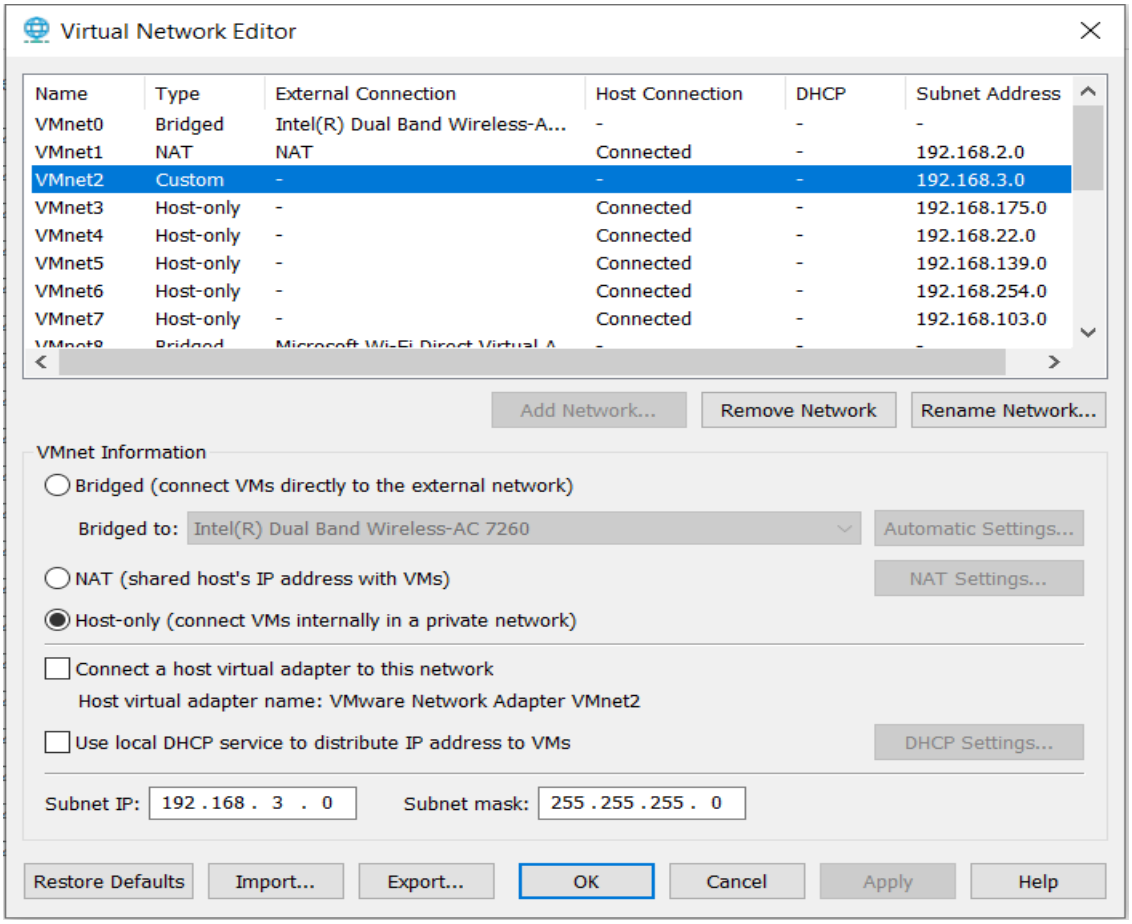
1.2. Justification du choix de pfSense

-Multitudes de services qu'il offre,
-pfSense est un pare-feu open source donc gratuit
- La configuration minimum recommandée est facile à satisfaire (CPU 1Ghz, ram 1Go, disque dure 1Go)
-Large documentation

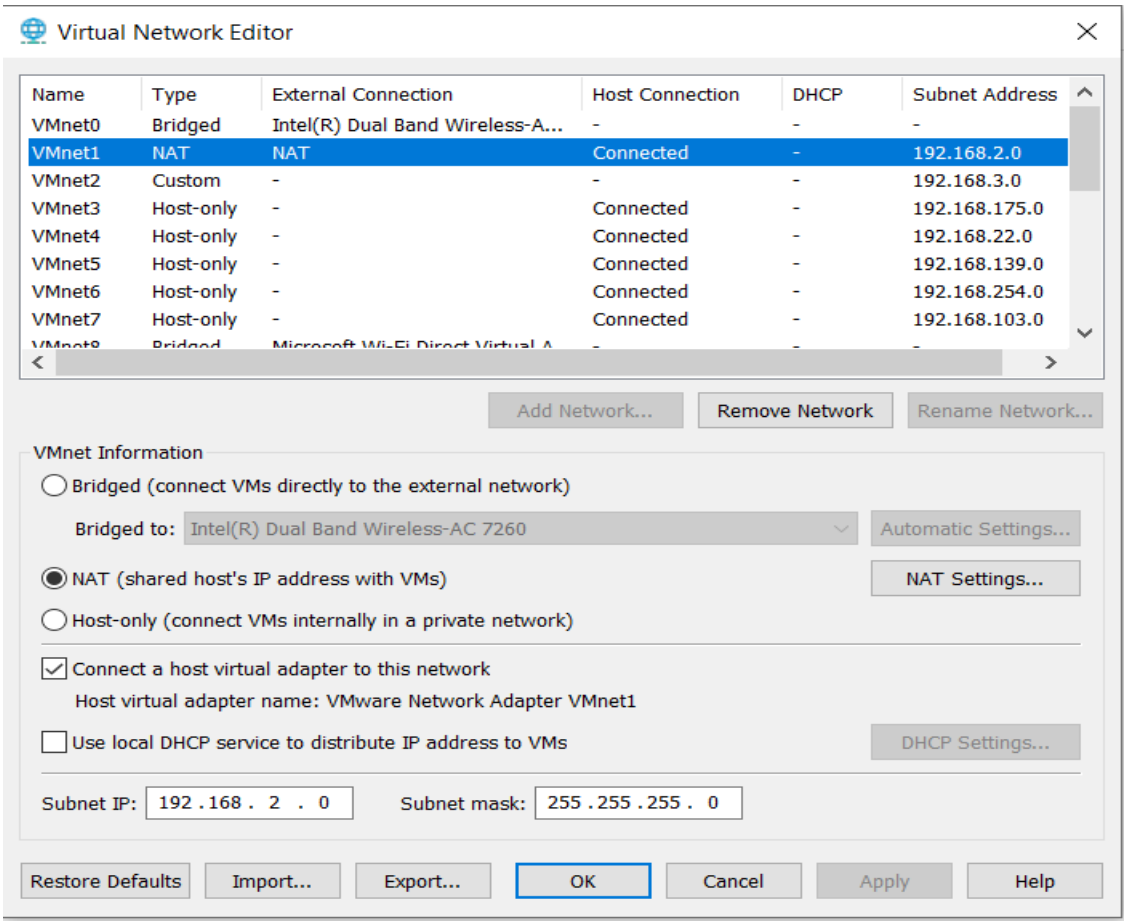
2. Installation de pfSense

Architecture :

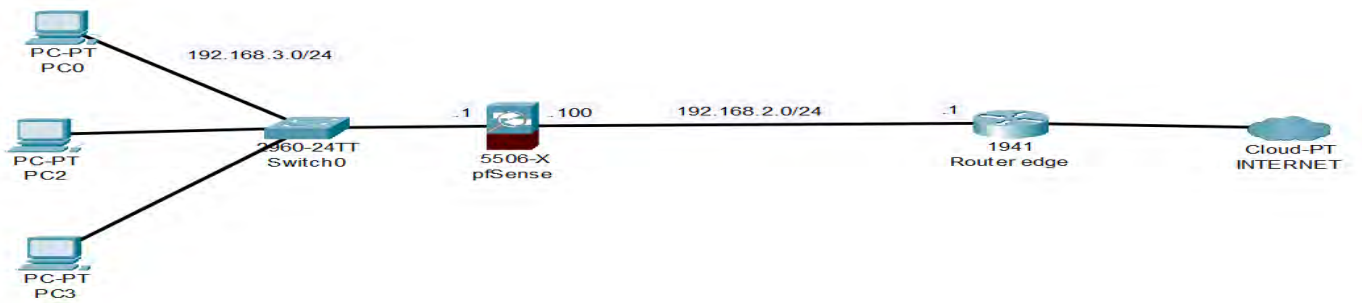
Pour la mise en place de l'architecture nous avons utilisé VMware Workstation.
Ainsi pour les machines du LAN nous avons utilisé la carte graphique VMnet2. Donc les machines se trouvant dans le LAN auront les adresses 192.168.3.0/24.



Pour les machines se trouvant au niveau du WAN, nous les avons assignées la carte graphique VMnet1.
Donc les machines se trouvant au niveau du WAN auront les adresses 192.168.2.0/24.
La carte graphique VMnet1 est configurée en mode NAT (Network Address Translation).



Pour notre pfSense nous avons deux cartes graphiques :
- La VMnet2 liée au LAN.
- La VMnet1 liée au WAN.
De ce fait donc, les machines se situant sur le LAN pourraient accéder à INTERNET en passant par le pare-feu pfSense. En effet le pare-feu pourra joindre les machines du LAN et celles du WAN.



Architecture du réseau

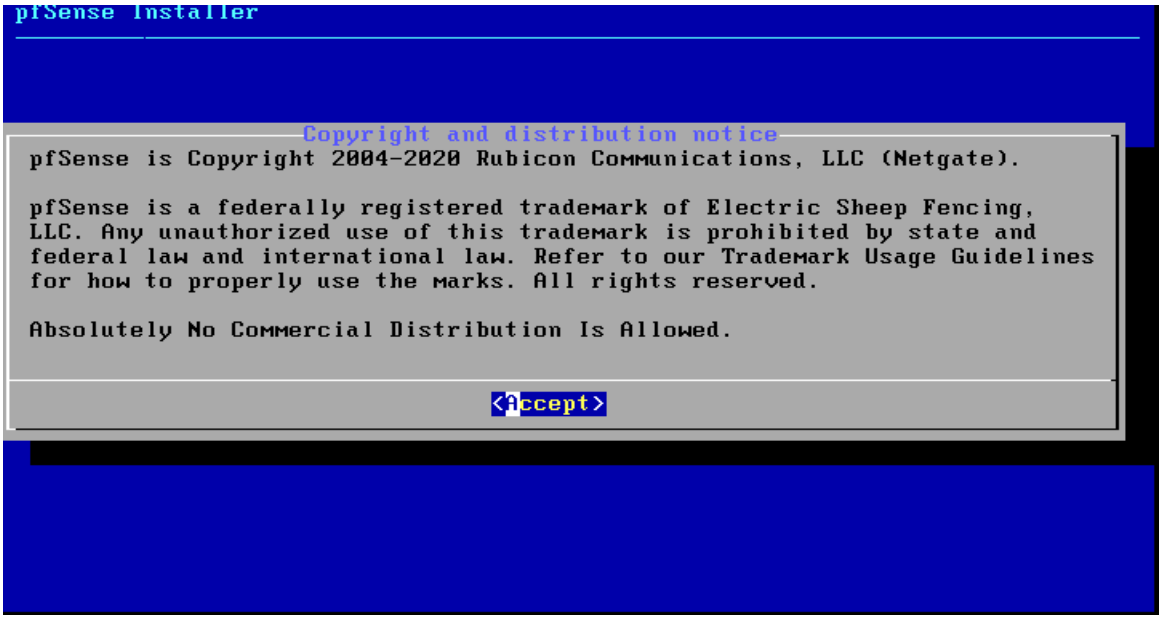
La configuration minimum pour installer pfSense est :

CPU: 1GHz

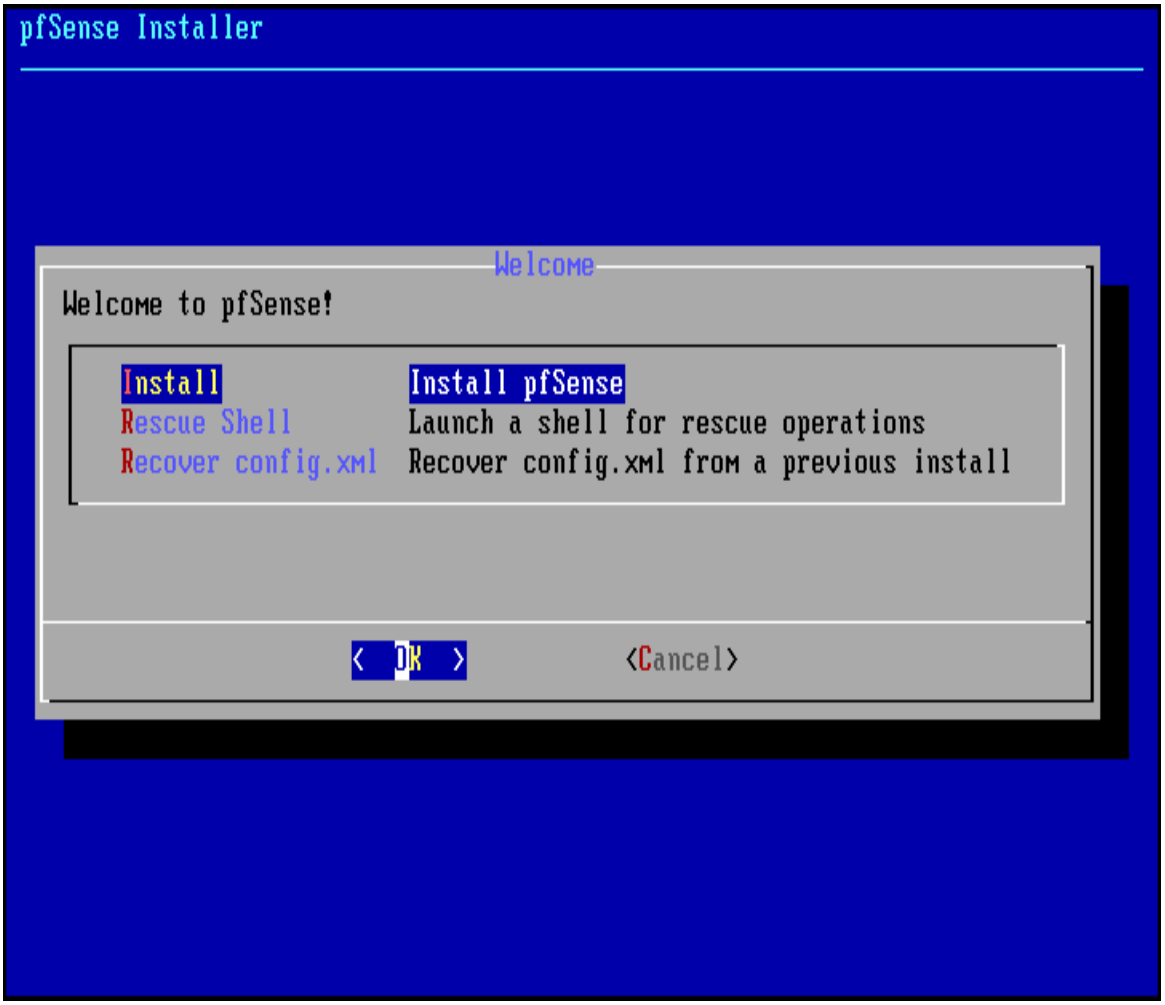
RAM: 1Go

Disque dur: 1Go

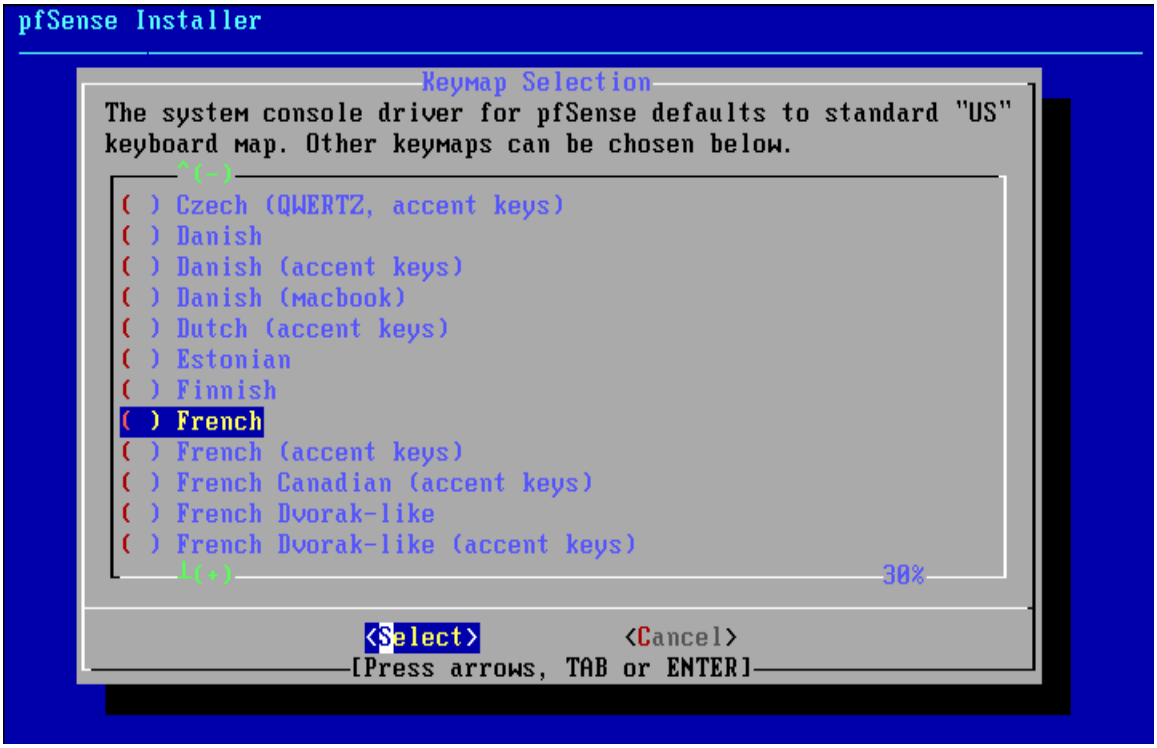
Ici nous un avis de droit d'auteur et de distribution, appuyer sur **entrée** pour continuer.



Nous voulons installer pfSense, c'est le choix par défaut appuyer sur entrée pour poursuivre l'installation.



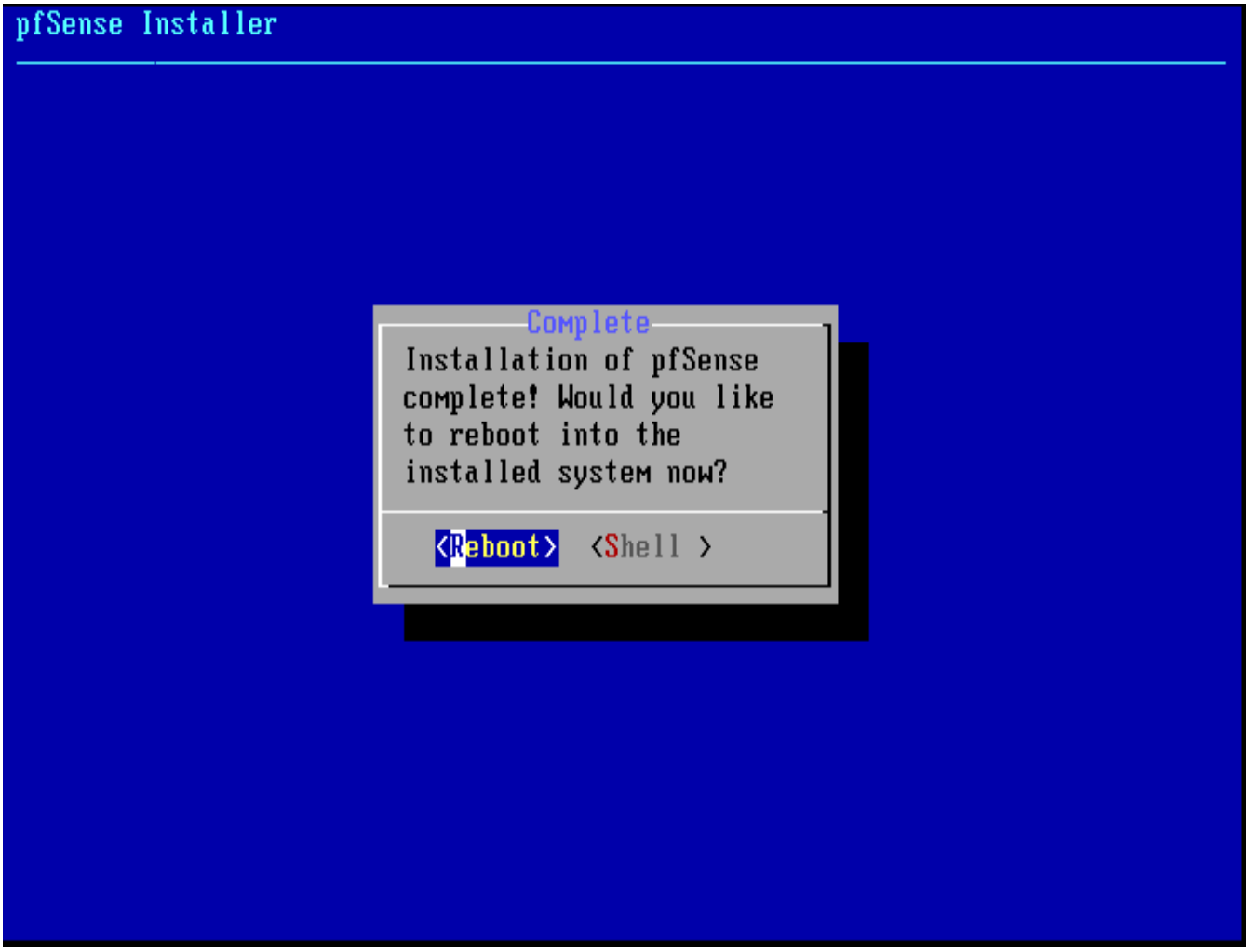
Ensuite pfSense nous demande de choisir la disposition de notre clavier, nous avons un azerty donc nous choisissons **french** puis appuyer sur **entrée**.



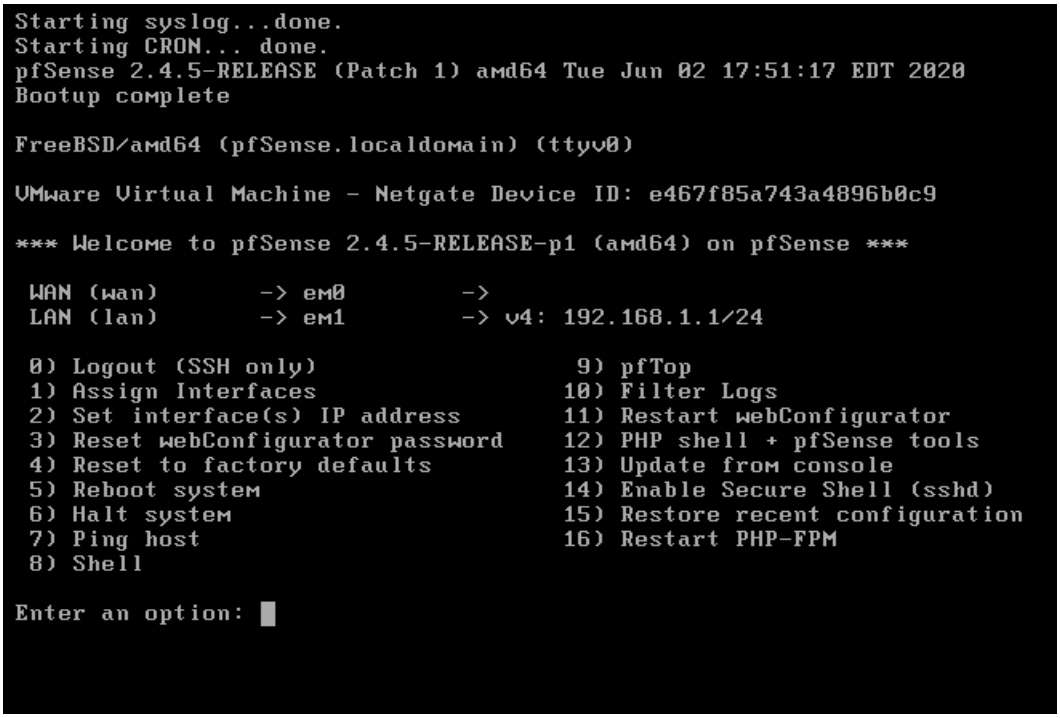
Ensuite ici pfSense nous demande comment nous souhaitons partitionner notre disque dur. Nous choisissons **Guided Disk Setup** puis appuyons sur **entrée**.

L'installation est presque terminée reste plus qu'à redémarrer notre pfSense.
Pour cela choisir **No**.

Ici choisir **Reboot** pour lancer le redémarrage de pfSense.

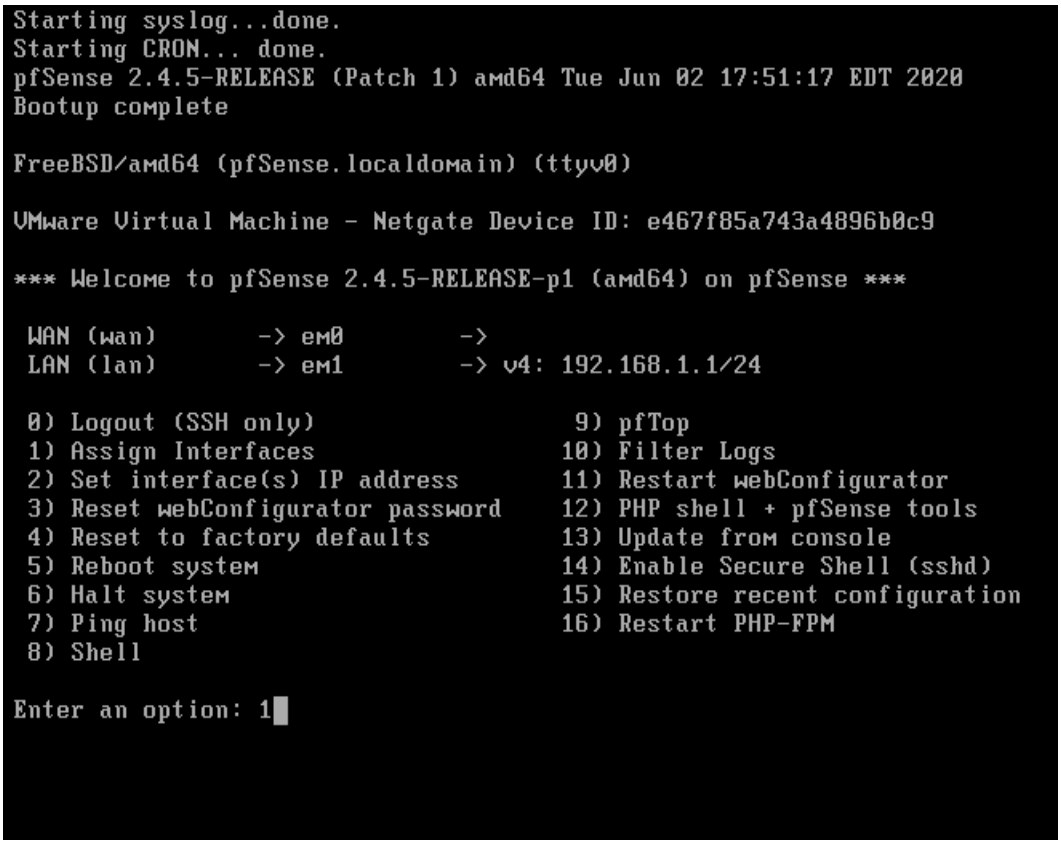


L'installation est terminée nous arrivons sur l'écran d'accueil de pfSense. Nous avons différentes options allant de 0 à 16 selon les besoins.
La prochaine étape consistera à la configuration des adresses sur les interfaces.



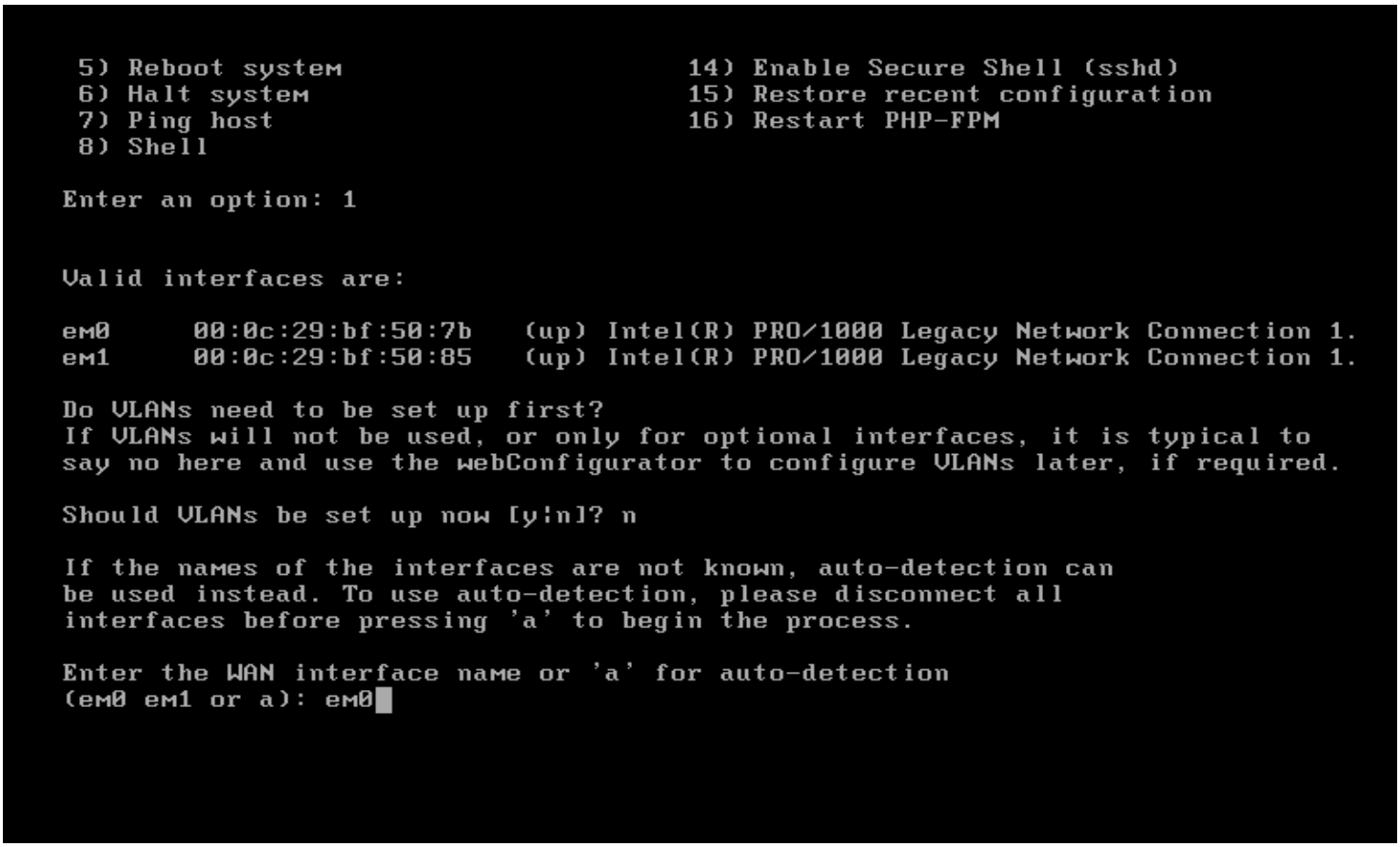
3. Configuration des adresses IP sous pfSense

Choisissons l'option **1** pour la configuration des adresses sur les interfaces.



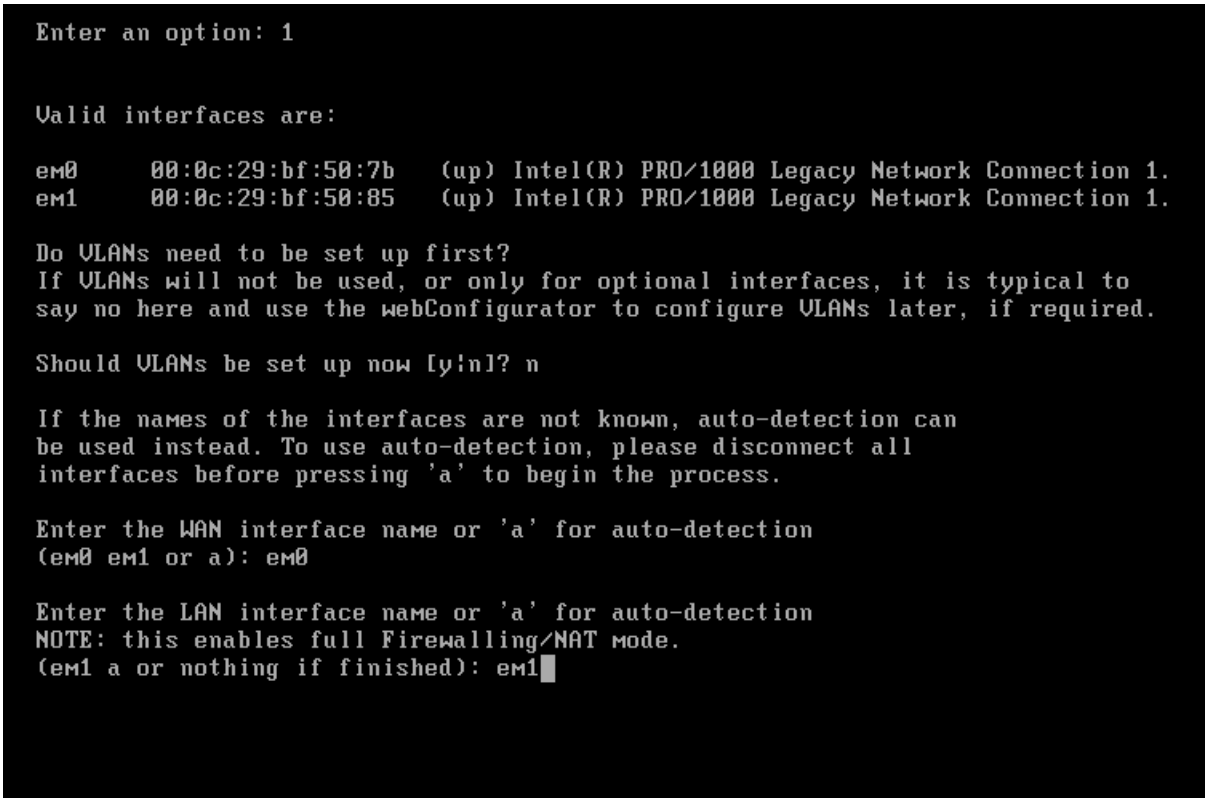
pfSense nous demande si nous souhaitons créer des VLANs, c'est selon l'architecture que nous souhaitons mettre en place dans notre cas nous choisissons **n**.

Ici pfSense nous demande de choisir le nom de l'interface WAN donc interface qui sera relié à INTERNET nous choisissons le nom par défaut **EM0.**



pfSense nous demande ensuite de choisir le nom de l'interface LAN donc interface qui sera relié à notre réseau interne nous choisissons le nom par défaut **EM1.**

Donc pfSense doit avoir au moins deux cartes réseaux.



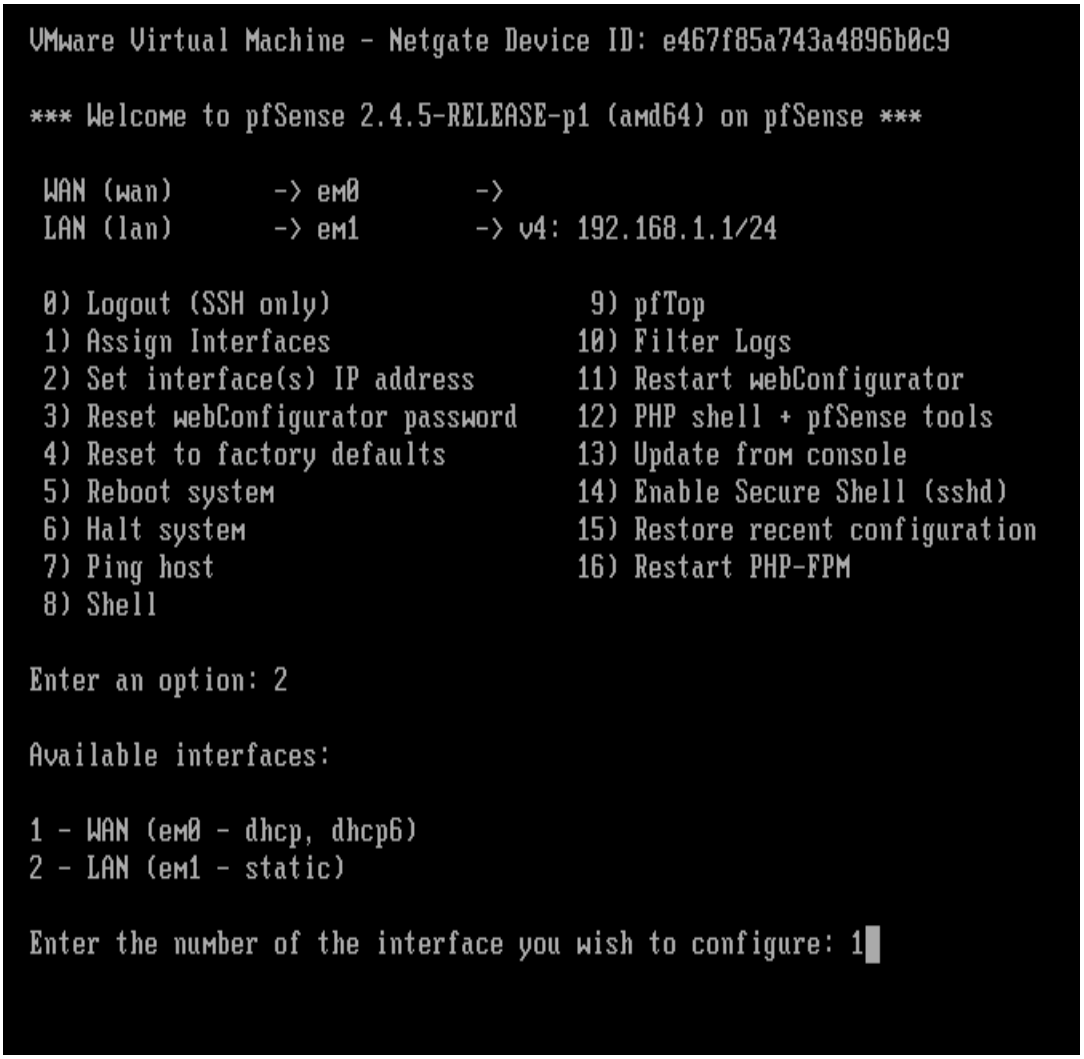
Choisir **y** pour confirmer la configuration.

```
em1     00:0c:29:bf:50:85   (up) Intel(R) PRO/1000 Legacy Network Connection 1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y|n]? y
```

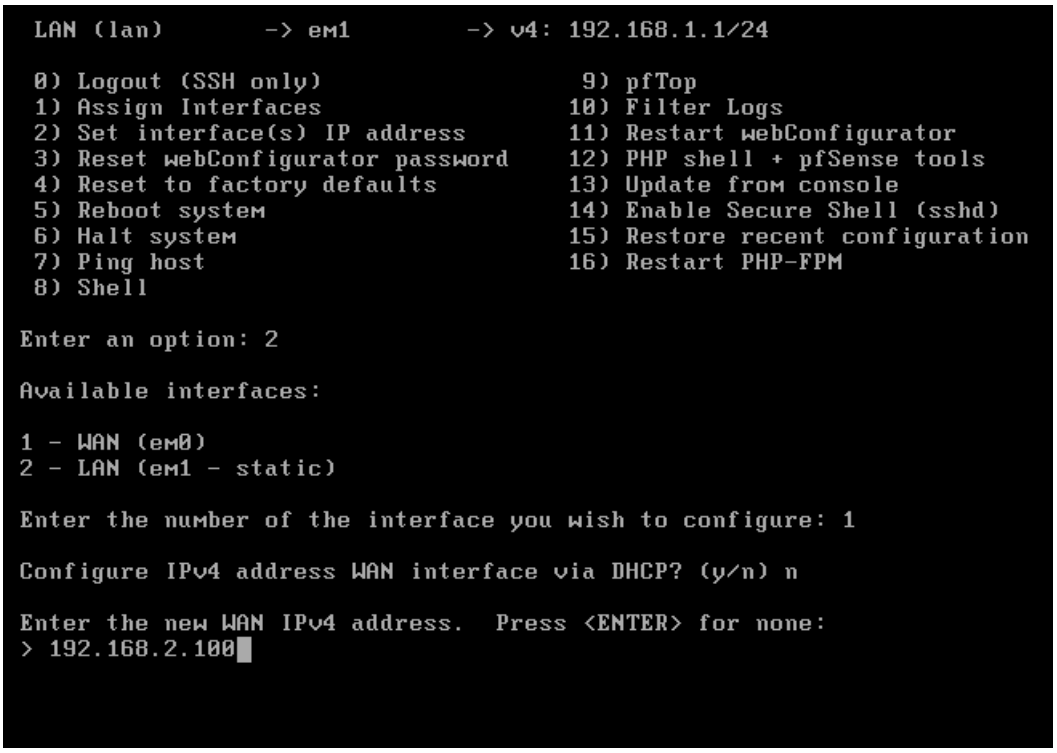
Après avoir donné des noms à nos deux interfaces, nous allons aussi leurs attribuer des adresses IP. Pour cela choisir l'option **2**.

```
WAN  -> em0
LAN  -> em1

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: e467f85a743a4896b0c9

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        ->
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2
```

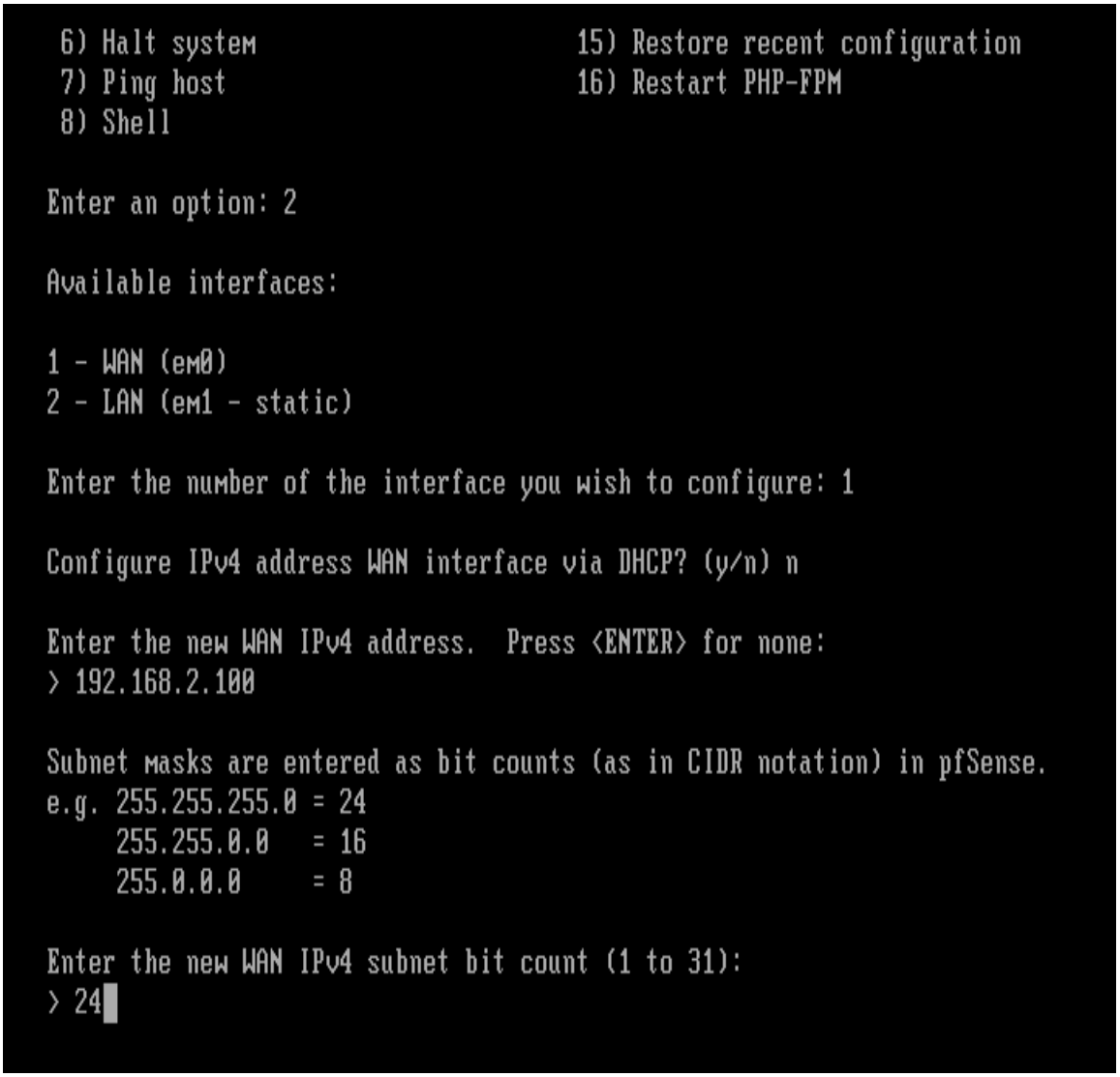
Nous allons d'abord configurer l'adresse de l'interface WAN. Donc choisissons l'option **1**.



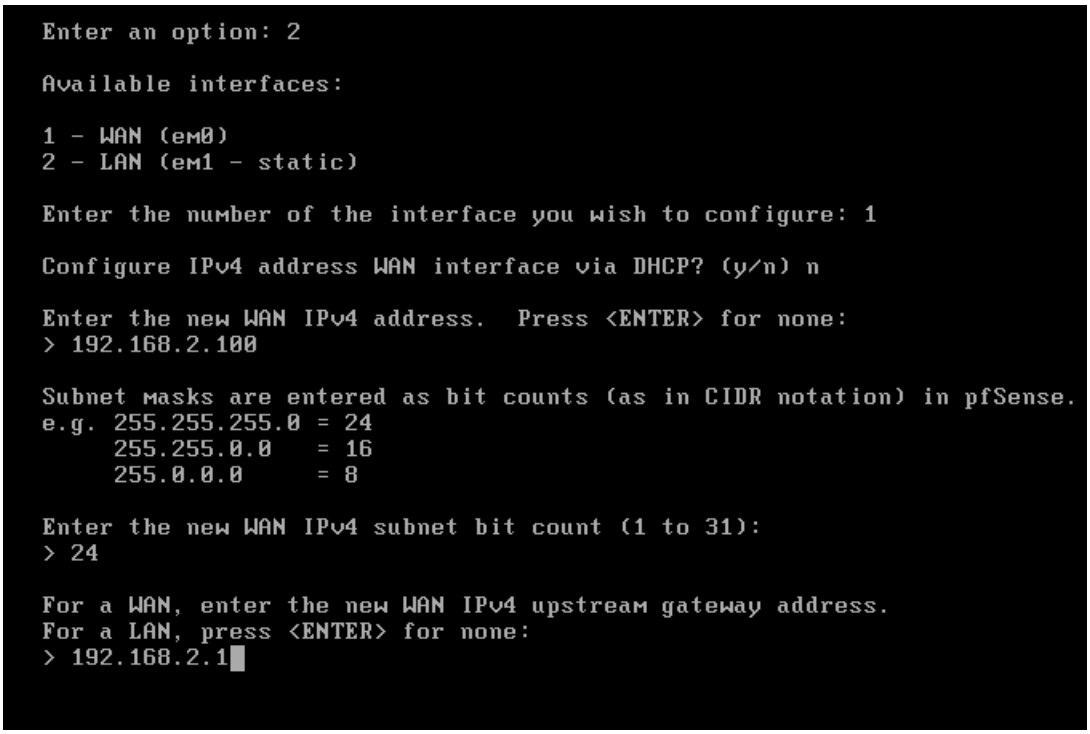
pfSense nous demande de donner l'adresse IP de l'interface WAN, nous choisissons **192.168.2.100**.



pfSense nous demande le masque du sous-réseau, nous choisissons **24**.



pfSense nous demande la passerelle par laquelle nous passerons pour accéder à INTERNET : **192.168.2.1**



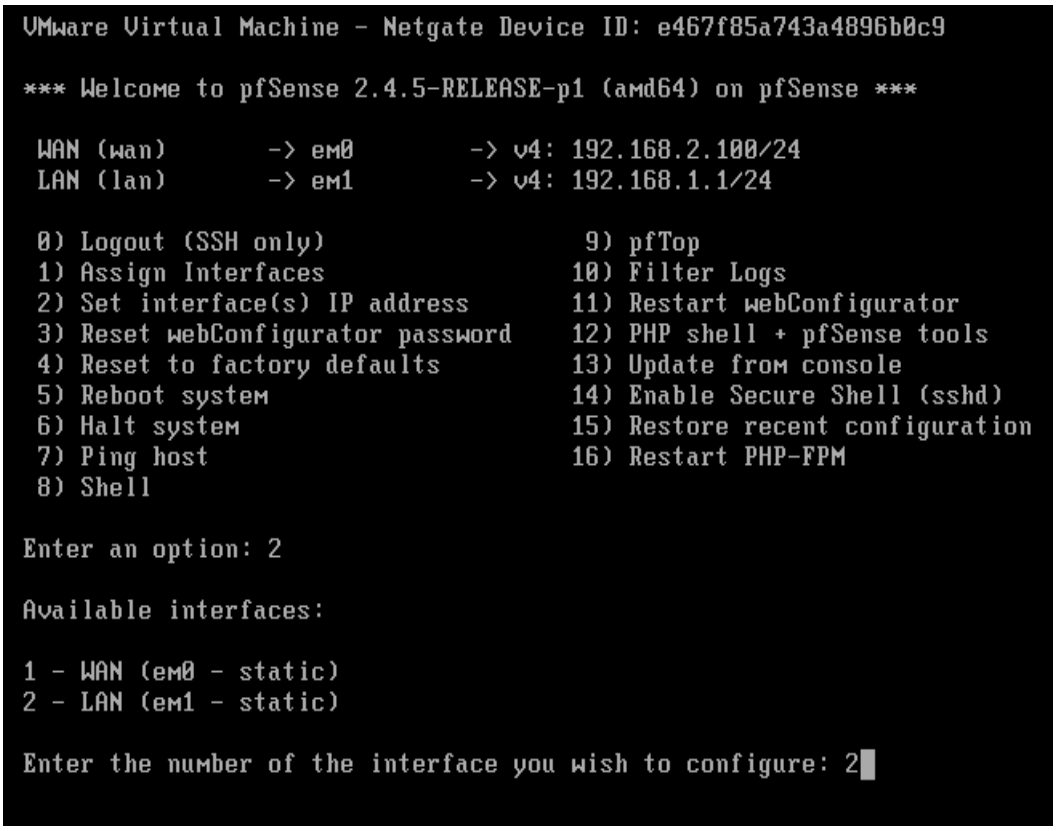
Nous ne voulons pas configurer DHCP6 donc nous choisissons **n.**

```
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.2.100

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.2.1

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
```

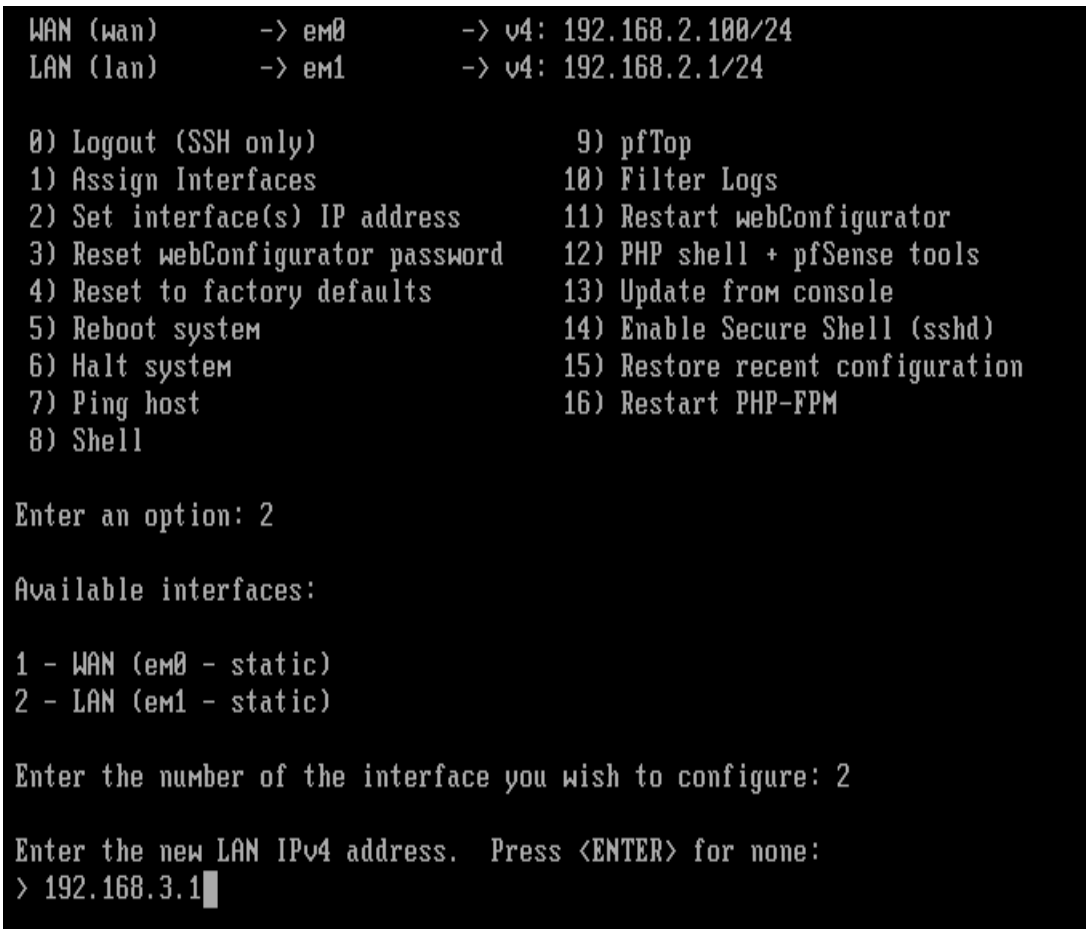
pfSense nous demande si nous voulons accéder l'interface de pfSense depuis le WAN en utilisant le protocole http, pour des raisons de sécurité nous choisissons **n**.

```
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.2.100

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.2.1

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

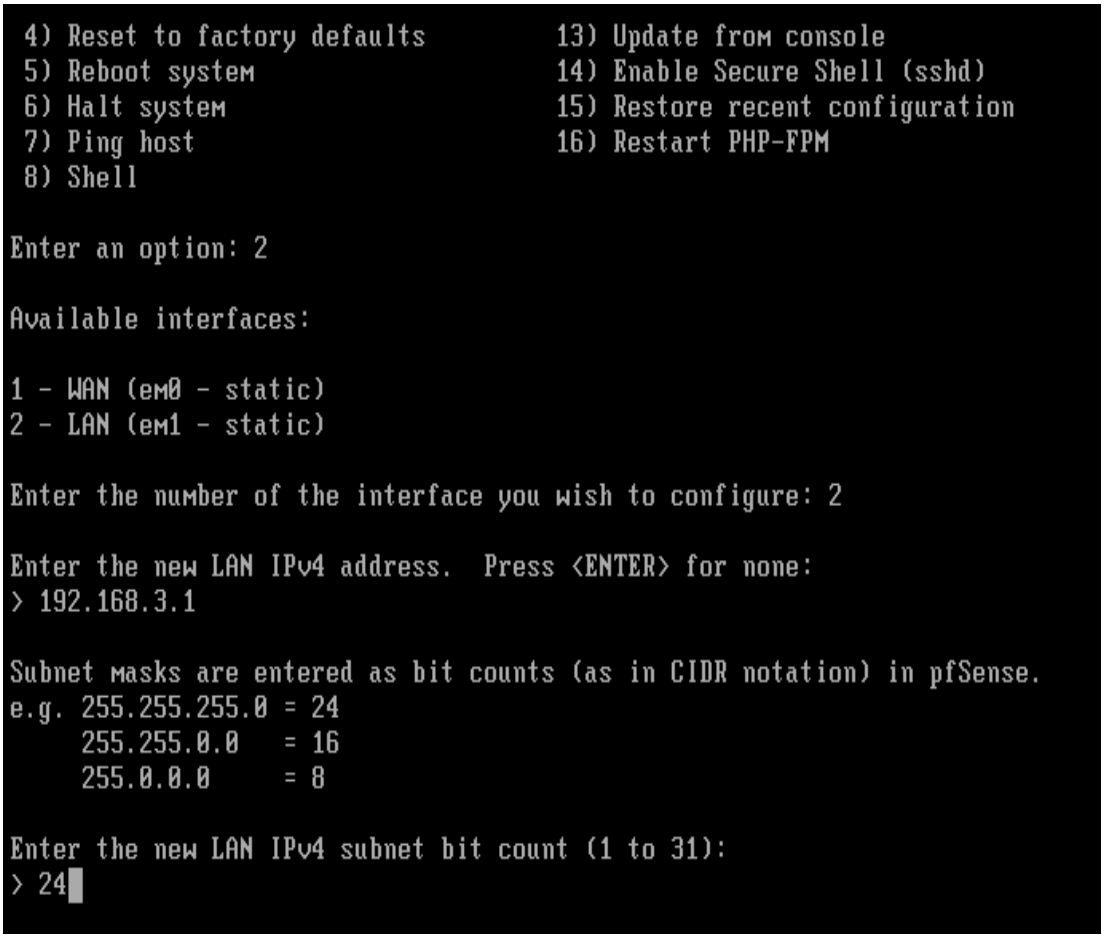
La configuration de l'interface WAN terminée nous passons à l'interface LAN pour cela choisir d'abord **2** pour assigner des adresses puis **2** pour choisir l'interface LAN.



pfSense nous demande d'attribuer une adresse IP sur l'interface LAN : **192.168.3.1**

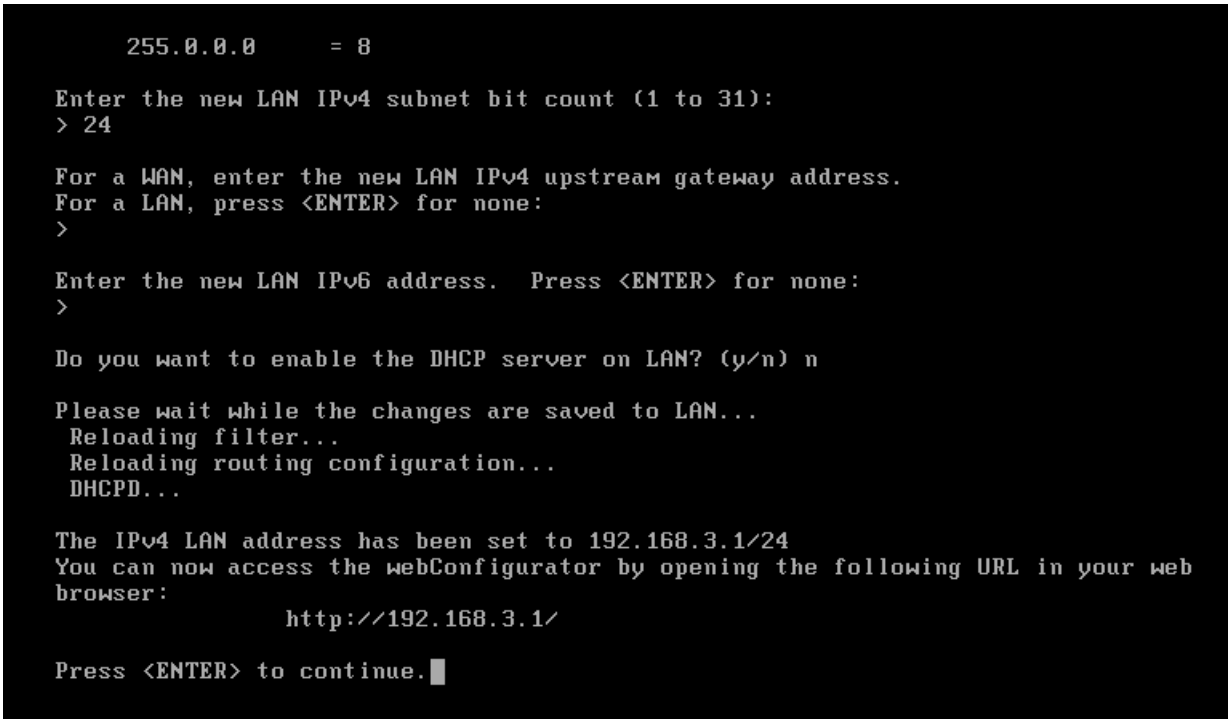


Ici pour le masque du sous-réseau choisir **24**.



Nous ne souhaitons pas octroyer d'adresse des adresses IP dynamiquement donc nous choisissons **n**.

Remarquons que pfSense ne nous a pas demandé la passerelle au niveau du LAN, normal notre pfSense jouera le rôle de passerelle ainsi toutes les connexions entrantes et sortantes du LAN passeront forcément par le pfSense. En d'autres termes si pfSense est éteint, nos machines locales (du LAN) n'auront pas accès à INTERNET. A cette étape les machines du LAN ont accès à l'interface de pfSense.



Pour voir si notre configuration est bonne nous pouvons faire un Ping sur le 8.8.8.8 pour voir si nous avons accès à INTERNET.

```
 1) Assign Interfaces               10) Filter Logs
 2) Set interface(s) IP address     11) Restart webConfigurator
 3) Reset webConfigurator password  12) PHP shell + pfSense tools
 4) Reset to factory defaults       13) Update from console
 5) Reboot system                   14) Enable Secure Shell (sshd)
 6) Halt system                     15) Restore recent configuration
 7) Ping host                       16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=103.071 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=241.732 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=202.567 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 103.071/182.457/241.732/58.367 ms

Press ENTER to continue.
```

Nous pouvons aussi faire un Ping sur une machine du LAN.

```
 1) Assign Interfaces               10) Filter Logs
 2) Set interface(s) IP address     11) Restart webConfigurator
 3) Reset webConfigurator password  12) PHP shell + pfSense tools
 4) Reset to factory defaults       13) Update from console
 5) Reboot system                   14) Enable Secure Shell (sshd)
 6) Halt system                     15) Restore recent configuration
 7) Ping host                       16) Restart PHP-FPM
 8) Shell

Enter an option: 7


Enter a host name or IP address: 192.168.3.10

PING 192.168.3.10 (192.168.3.10): 56 data bytes
64 bytes from 192.168.3.10: icmp_seq=0 ttl=128 time=0.457 ms
64 bytes from 192.168.3.10: icmp_seq=1 ttl=128 time=0.930 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=128 time=1.052 ms

--- 192.168.3.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.457/0.813/1.052/0.257 ms

Press ENTER to continue.
```

Voilà notre pfSense est configuré. Nous avons un récapitulatif sur la version du pfSense, l'adresse par laquelle nous accéderons à l'interface du pfSense, le nom des interfaces et les adresses qui leur sont associées et les différentes options allant de 0 à 16 pour administrer pfSense.

```
The IPv4 LAN address has been set to 192.168.3.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.3.1/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: e467f85a743a4896b0c9

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 192.168.2.100/24
 LAN (lan)       -> em1        -> v4: 192.168.3.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

4. Installation et configuration de Snort

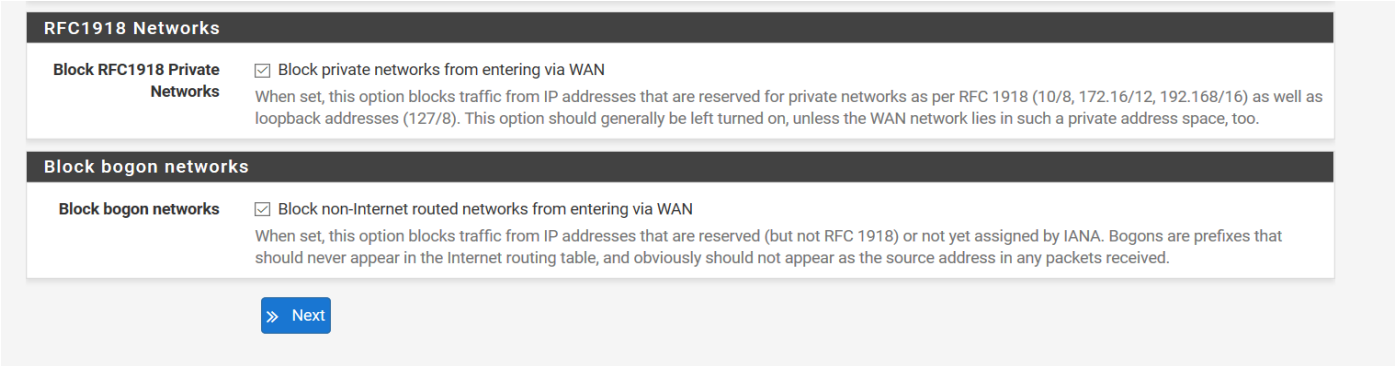
Une fois sur une machine du LAN, lançons un navigateur et saisissons l'adresse par laquelle nous accédons à l'interface de pfSense dans notre cas c'est **http://192.168.3.1** le nom d'utilisateur par défaut est **admin** le mot de passe **pfsense**.

Automatiquement après pfSense nous montre les réglages que nous avions fait auparavant. Ici nous voyons l'adresse au niveau du WAN, le masque et la passerelle.

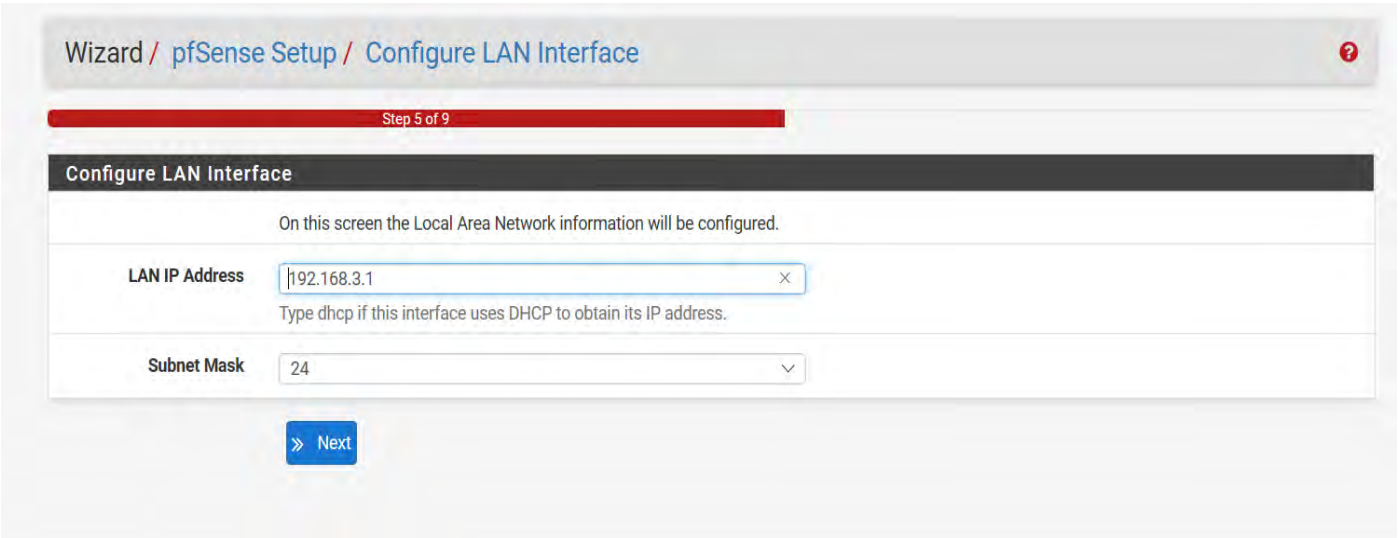
Block RFC1918 Private Networks : Un réseau privé est un réseau qui utilise les plages d'adressage IP définies par la RFC 1918 « Address Allocation for Private Internets ». Ces adresses ne sont pas routées sur Internet. Un réseau privé peut être numéroté librement avec les plages d'adresses privées prévues à cet effet. Par opposition aux adresses publiques d'Internet, ces adresses ne sont pas uniques, plusieurs réseaux pouvant utiliser les mêmes adresses.

Nous cochons donc cette case pour bloquer toutes les adresses IP définies par la RFC 1918.

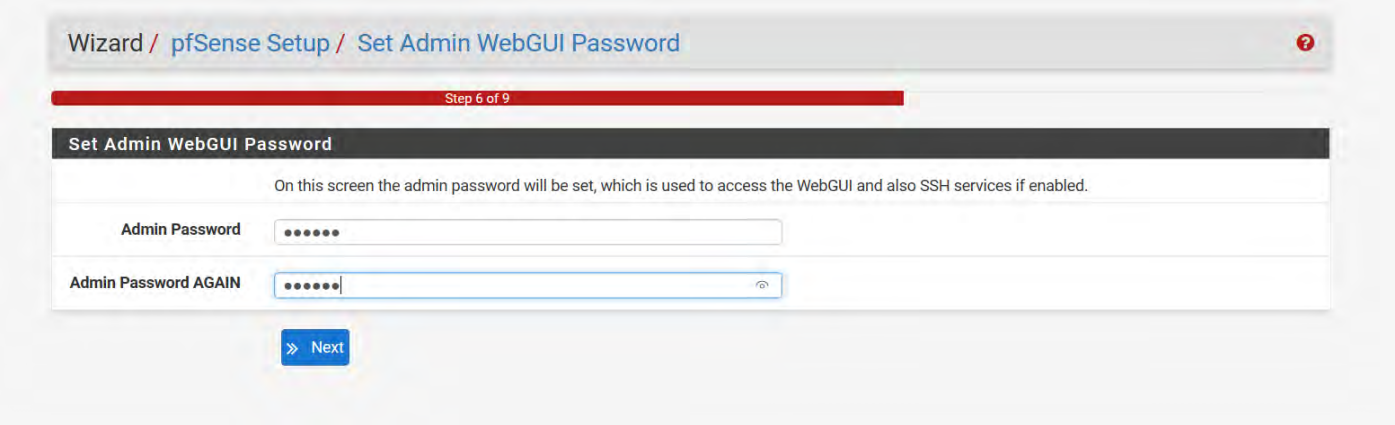
Block bogon networks : Nous cochons cette case pour bloquer toutes les fausses adresses venant du WAN.



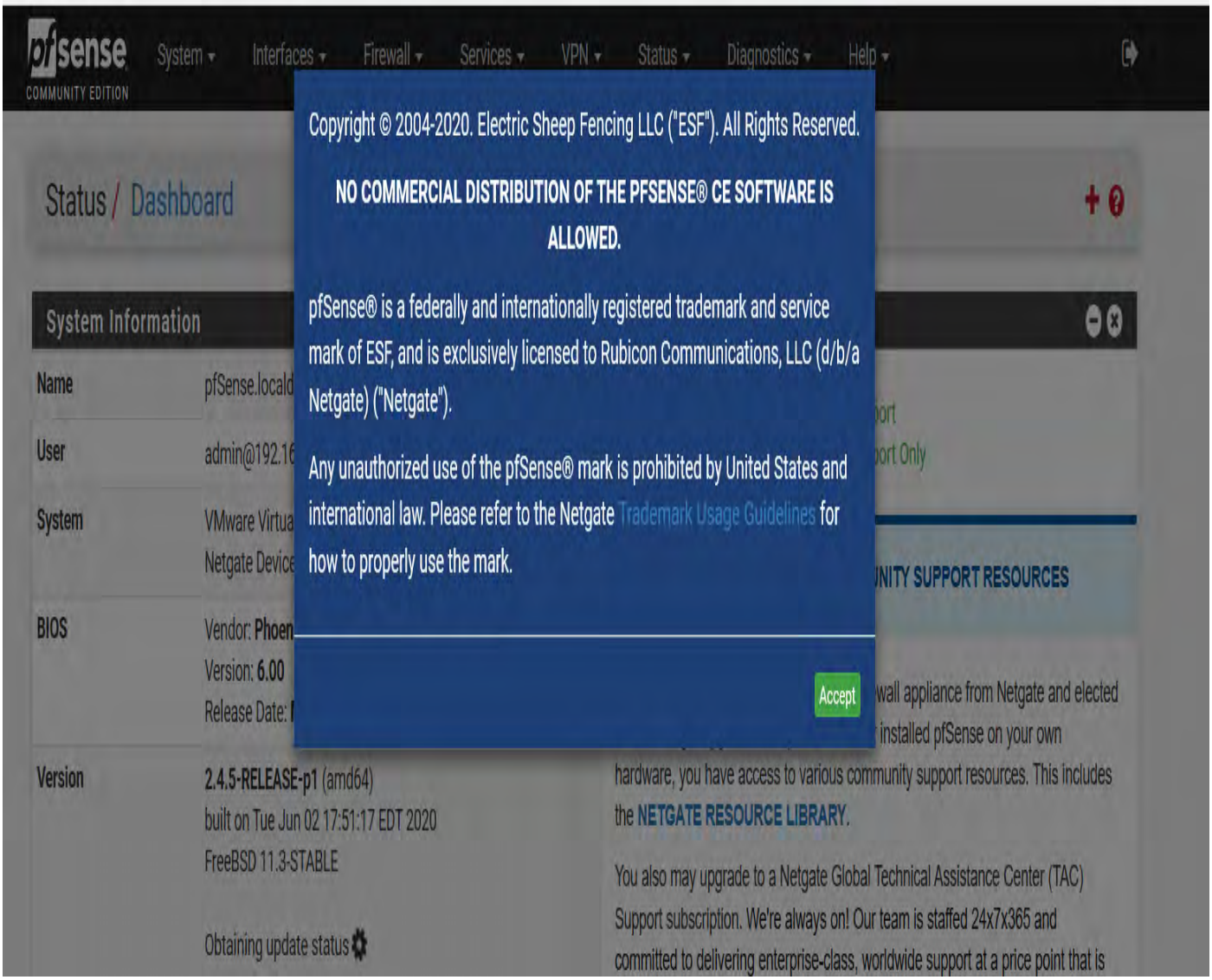
Ici nous voyons l'adresse IP de l'interface LAN configurée au préalable.



Nous mettons un autre mot de passe afin de mieux sécuriser notre pfSense.



Ici nous avons les termes du droit d'auteur. Nous cliquons sur **Accept** pour finir.
La configuration de notre pfSense étant faite la prochaine étape consiste à l'installation du package de notre IDS Snort.



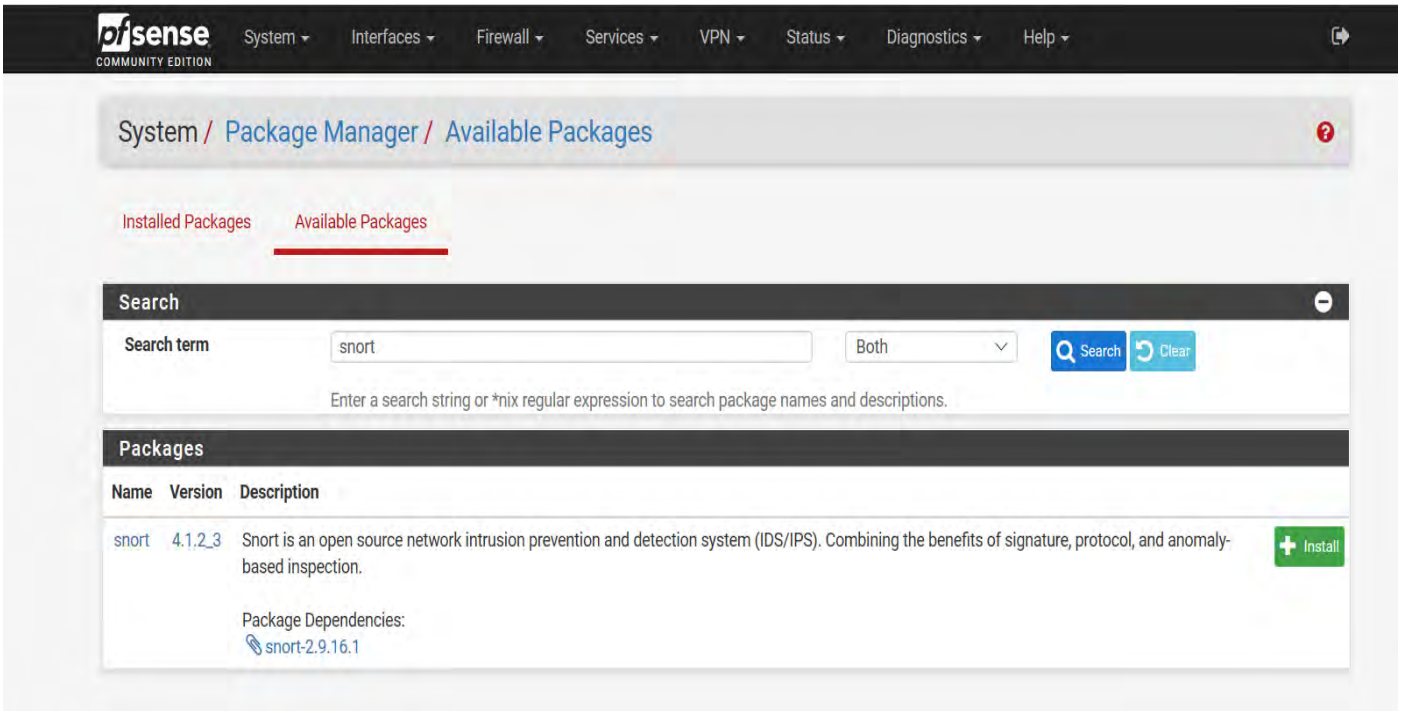
A la page d'accueil de pfSense nous avons des informations comme le nom de domaine, l'utilisateur connecté, la version du pfSense le processeur du serveur où est installé le pfSense ….

System Information	
Name	pfSense.localdomain
User	admin@192.168.3.10 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **8ab0c52174997ab7fe0c**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Wed Jul 22 2020**
Version	**2.4.5-RELEASE-p1** (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MDS Mitigation	Inactive

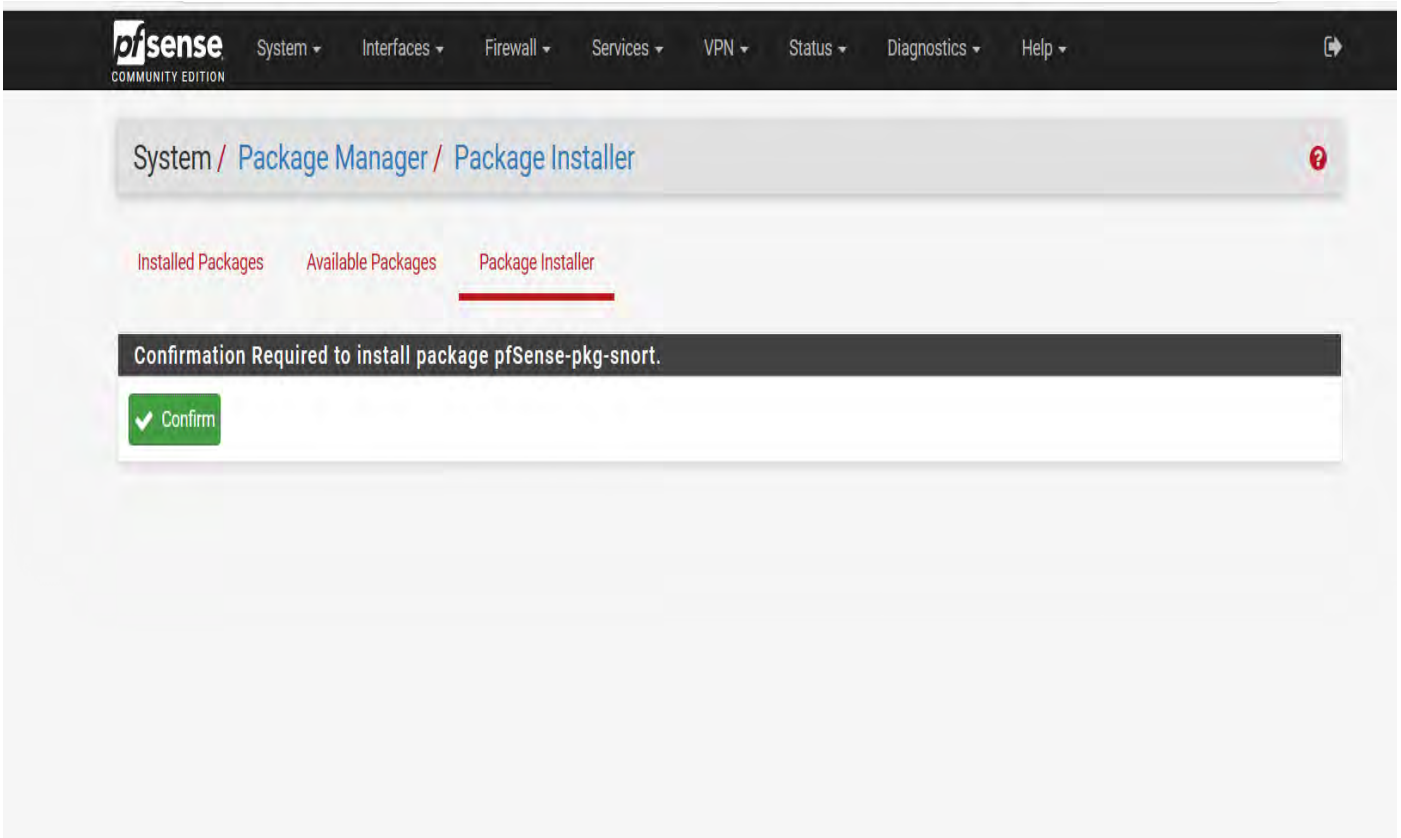
Nous avons aussi d'autres informations très utiles sur les performances du serveur comme l'utilisation du CPU, l'utilisation de la mémoire ram et du stockage.

Uptime	00 Hour 09 Minutes 13 Seconds
Current date/time	Thu May 20 12:15:40 UTC 2021
DNS server(s)	• 127.0.0.1
Last config change	Wed Mar 10 15:40:44 UTC 2021
State table size	0% (26/19000) Show states
MBUF Usage	0% (768/1000000)
Load average	0.51, 0.58, 0.40
CPU usage	2%
Memory usage	73% of 199 MiB
SWAP usage	6% of 1023 MiB
Disk usage: /	6% of 18GiB - ufs
/var/run	3% of 3.4MiB - ufs in RAM

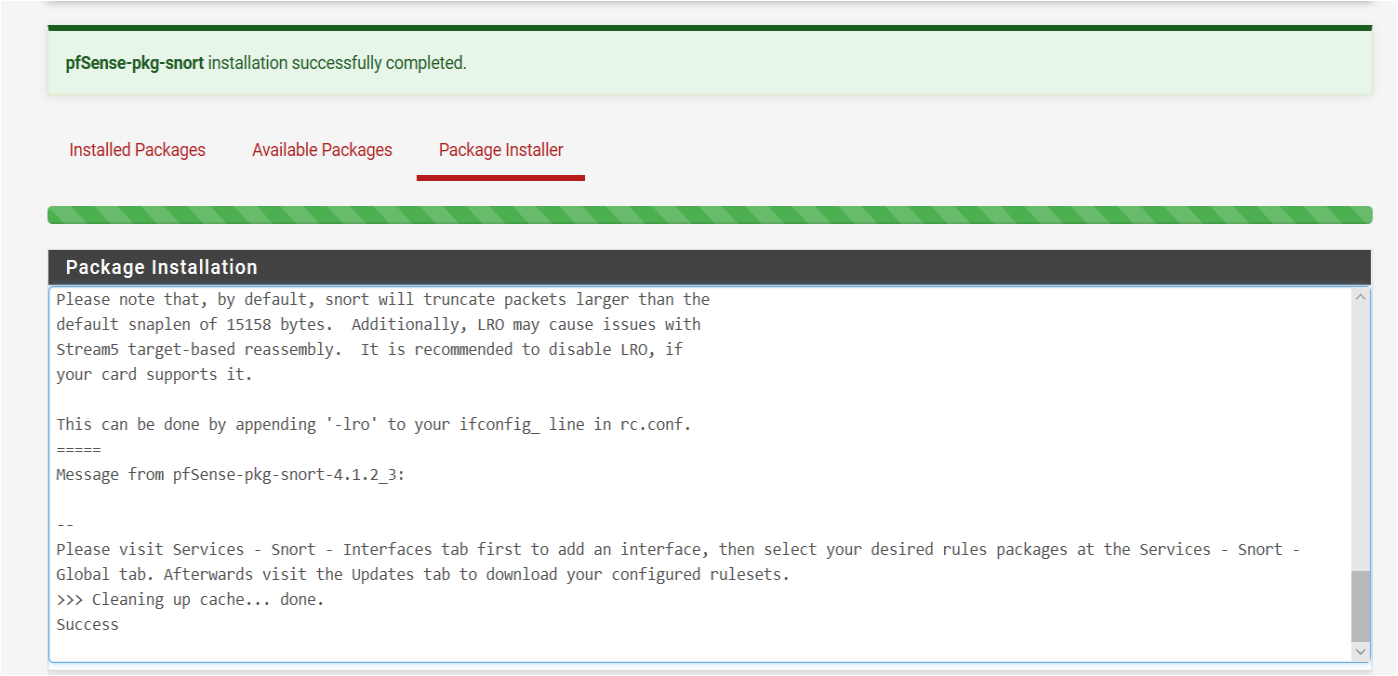
Pour installer Snort, il se rendre sur **Sytem/Install packages/Avalaible packages** puis rechercher **Snort**.



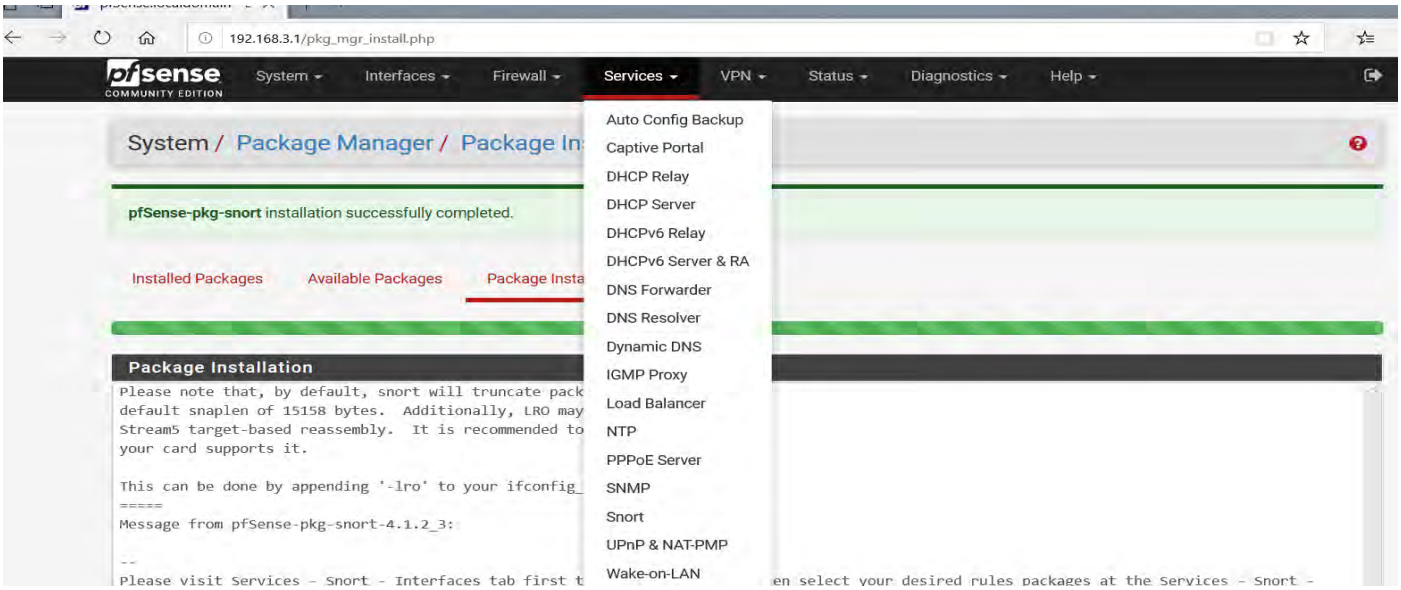
Ici nous confirmons l'installation de Snort.



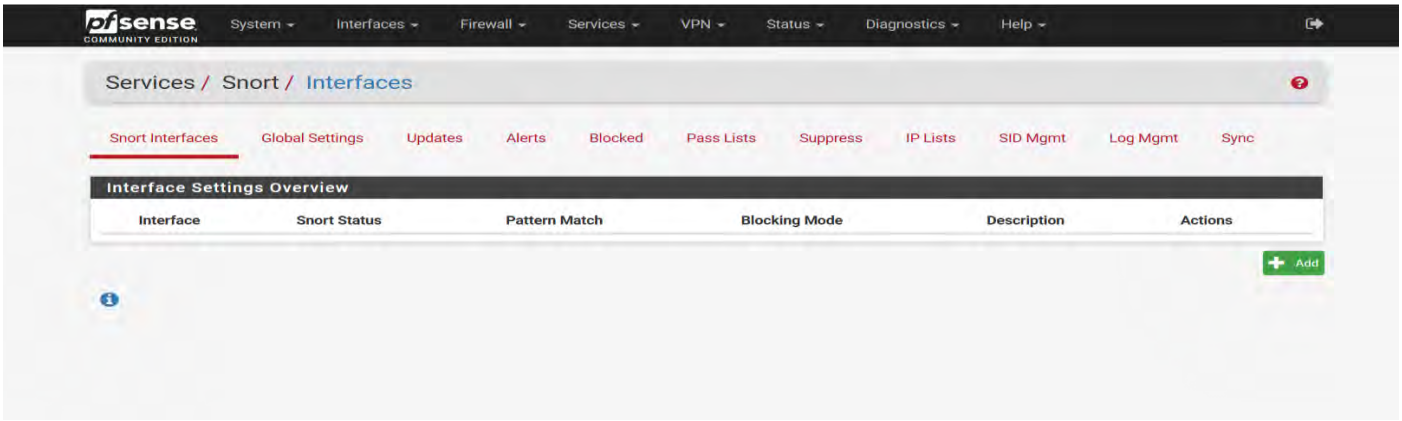
L’installation s’est terminée avec succès.



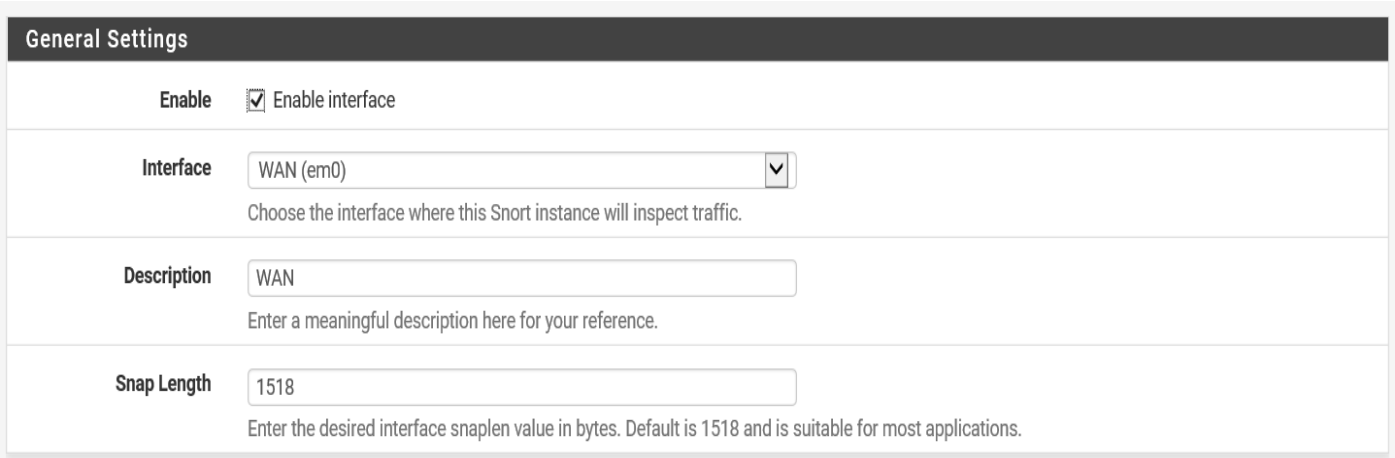
Maintenant au niveau de **Services** nous retrouvons notre **Snort**. Cliquons dessus pour configurer Snort.



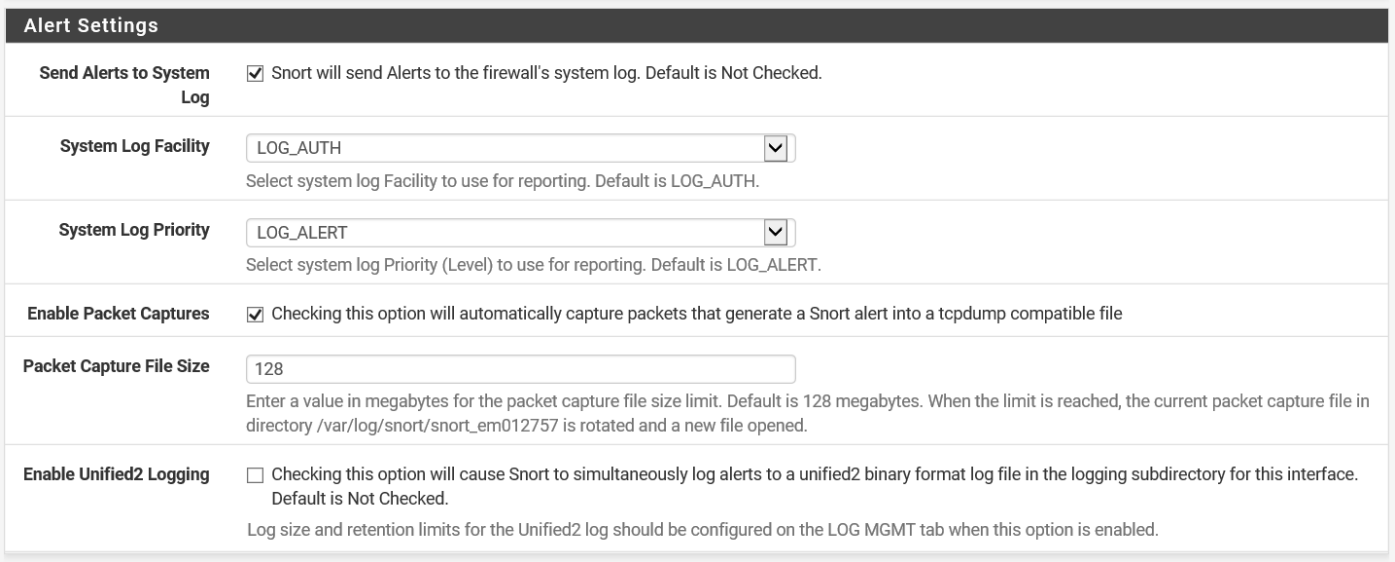
Nous cliquons sur **add** pour ajouter une nouvelle interface WAN. De ce fait nous allons surveiller les connexions entrantes depuis le WAN.



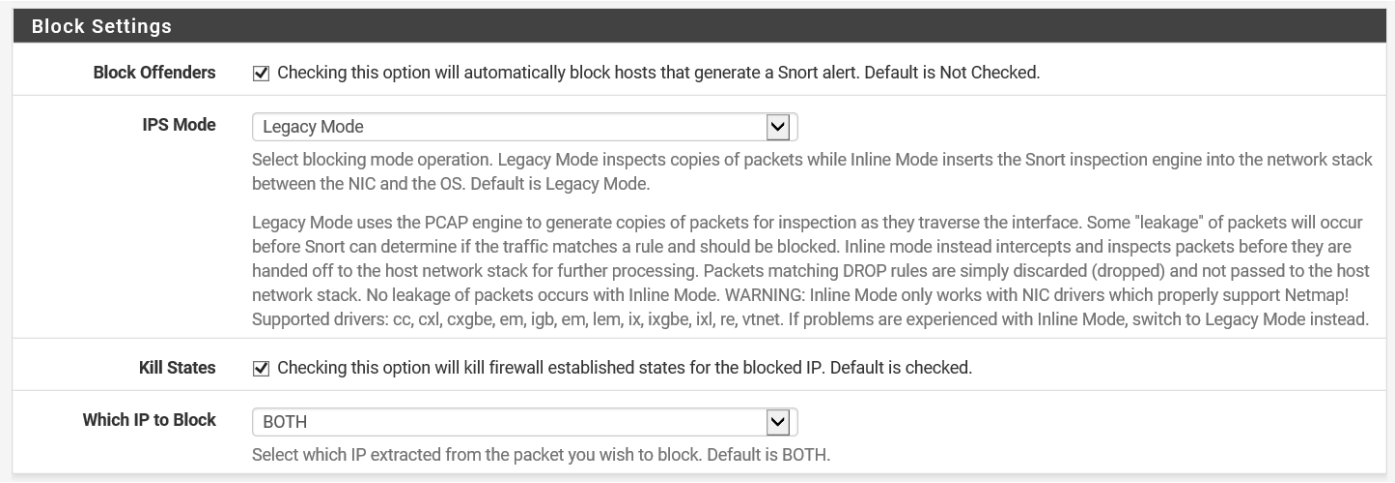
Nous activons l'interface.



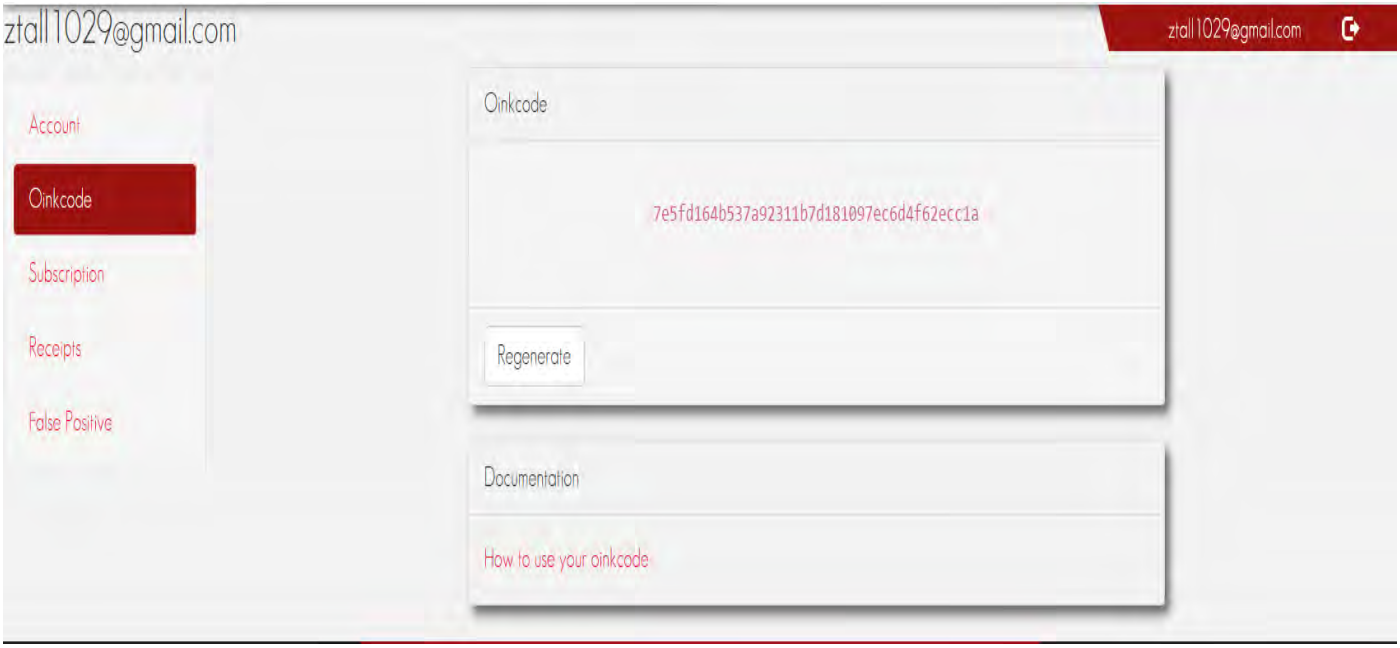
Nous cochons également l'option **Send Alerts to System Log**.



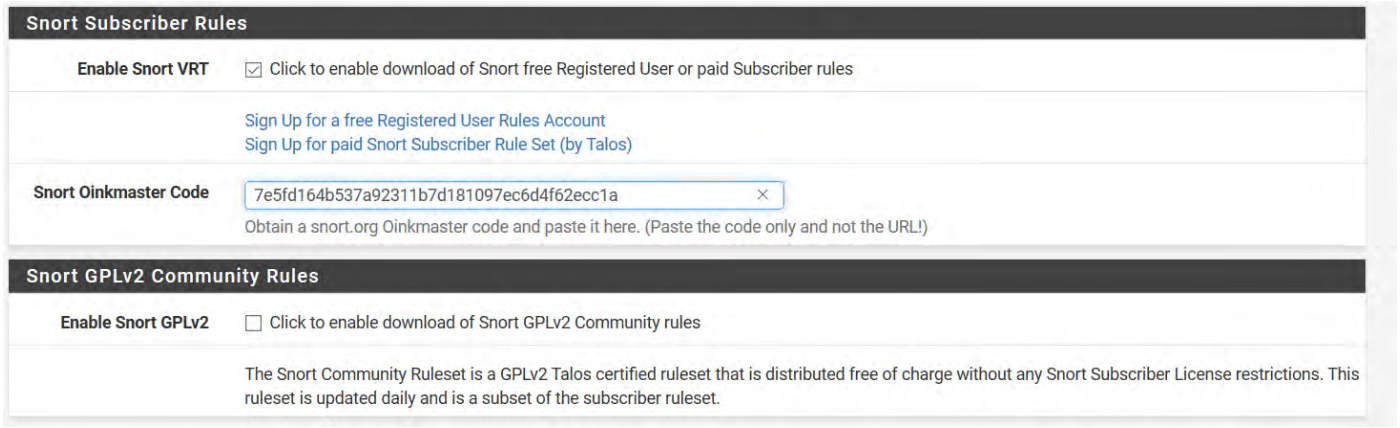
Nous cochons également l'option **Block Offenders** pour que Snort bloque tous les hôtes qui font que Snort génère des alertes.



Après s'être enregistré cliquons sur notre profil puis sur Oinkcode générer un code.

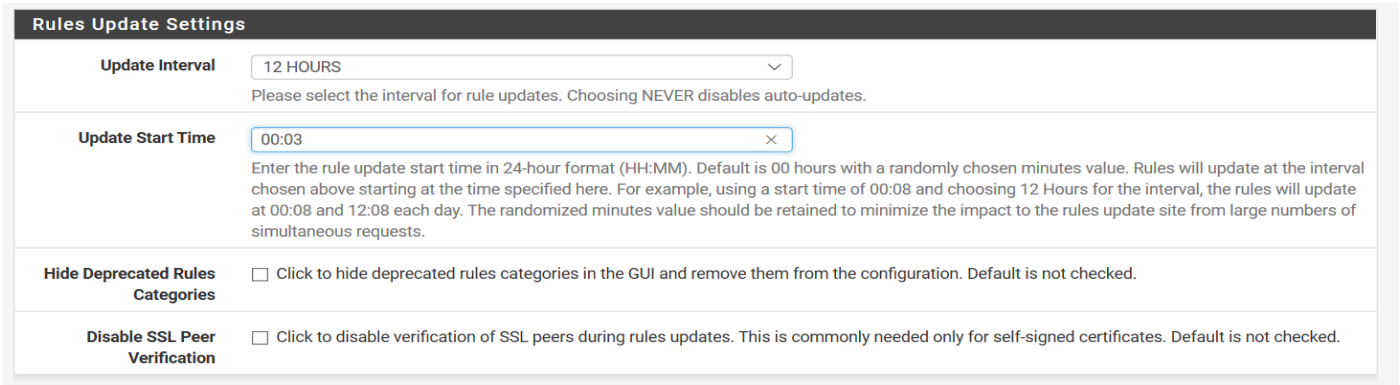


Snort VRT est un ensemble standard de règles qui nécessite soit un code pour utiliser de ces règles. Pour cela il faut s'enregistrer en cliquant sur **sign up for a free Registered User Rules Account**.

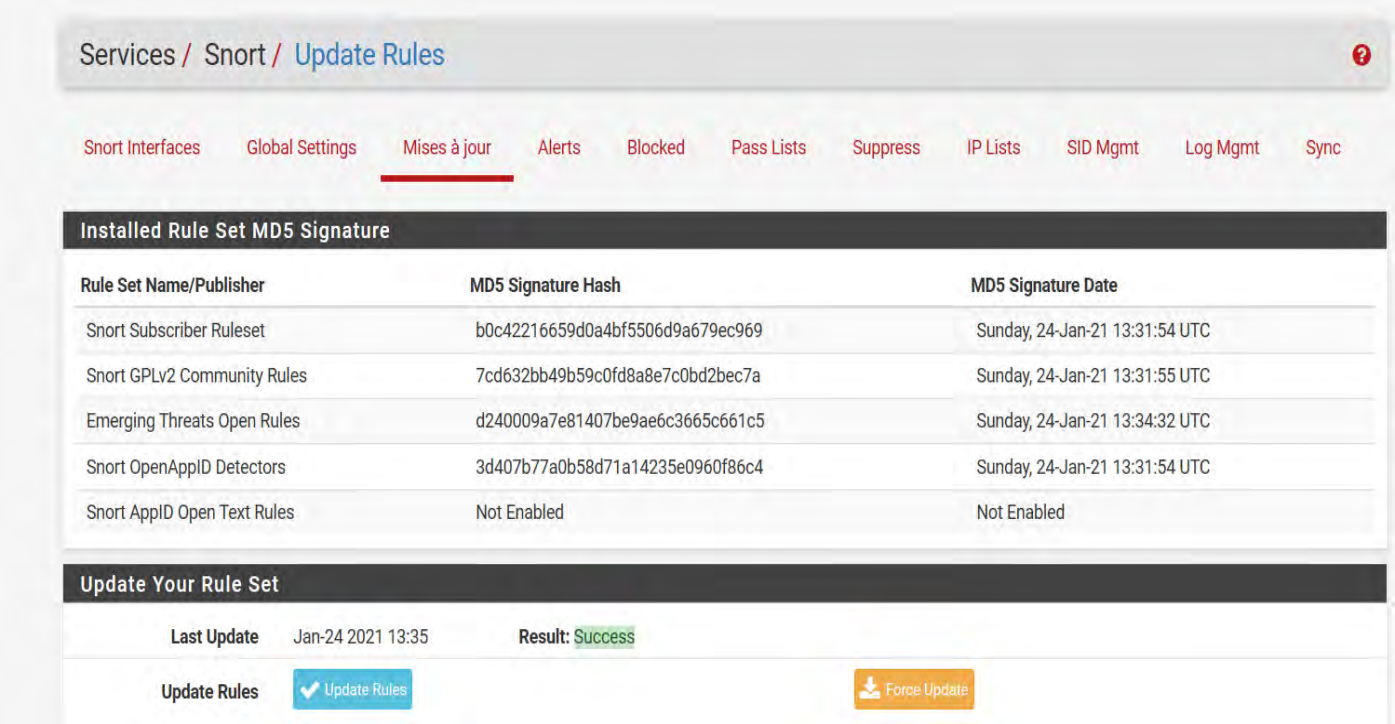


Choisissions la durée d'intervalle des mises à jour automatiques. Dans notre cas **12 heures**.

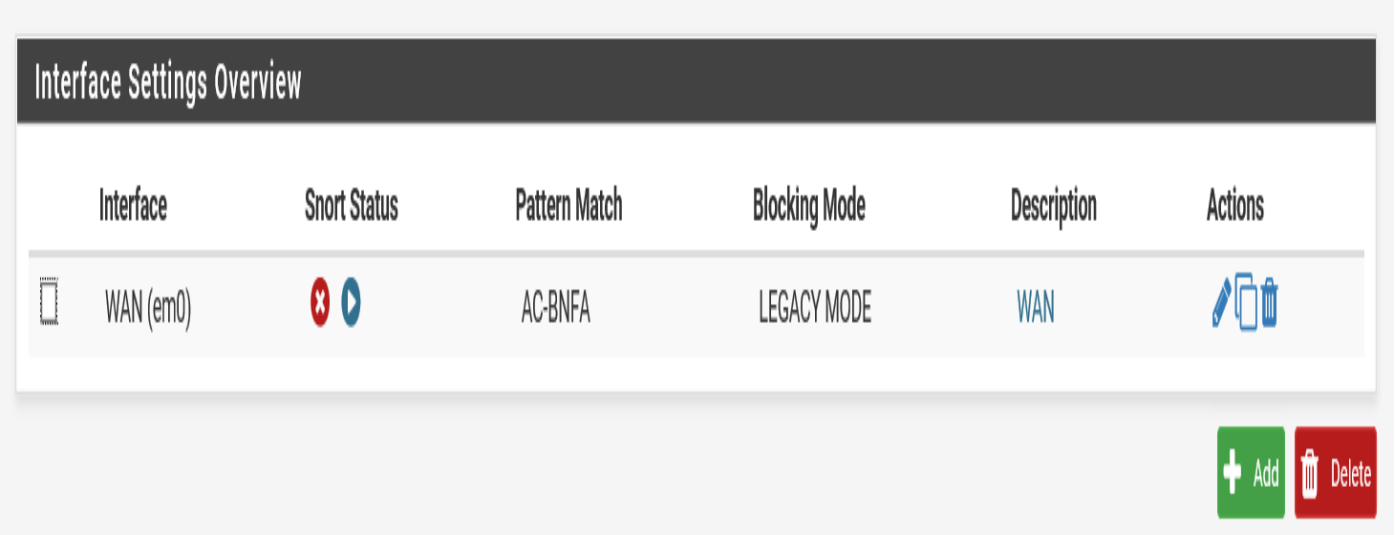
Et la mise à jour commencera à **00:03**.

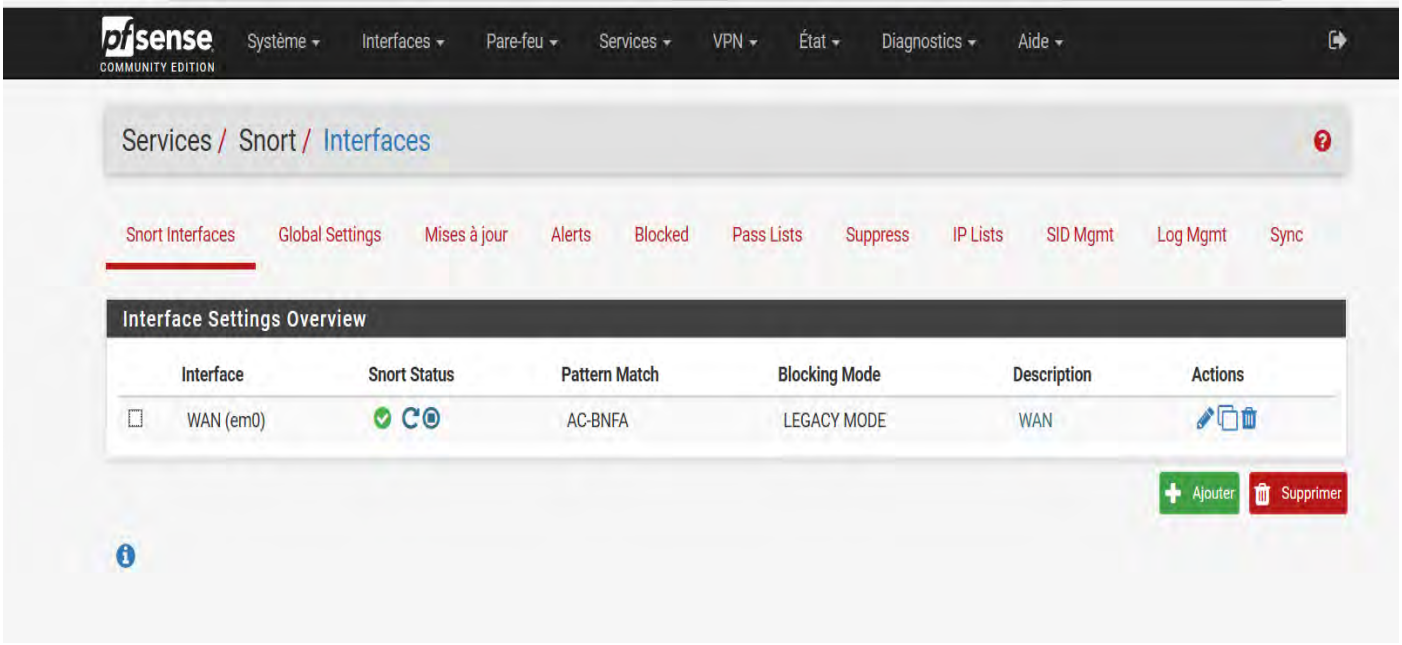


Une fois les règles définies appuyons sur **Updat Rules** pour qu'elles soient effectives.



A cette étape nous pouvons activer la surveillance sur notre interface LAN.

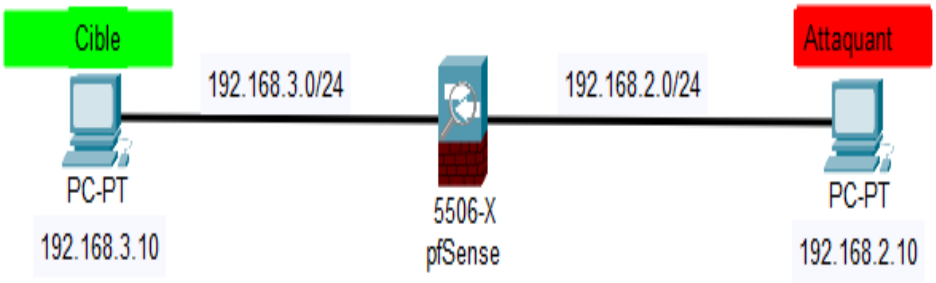




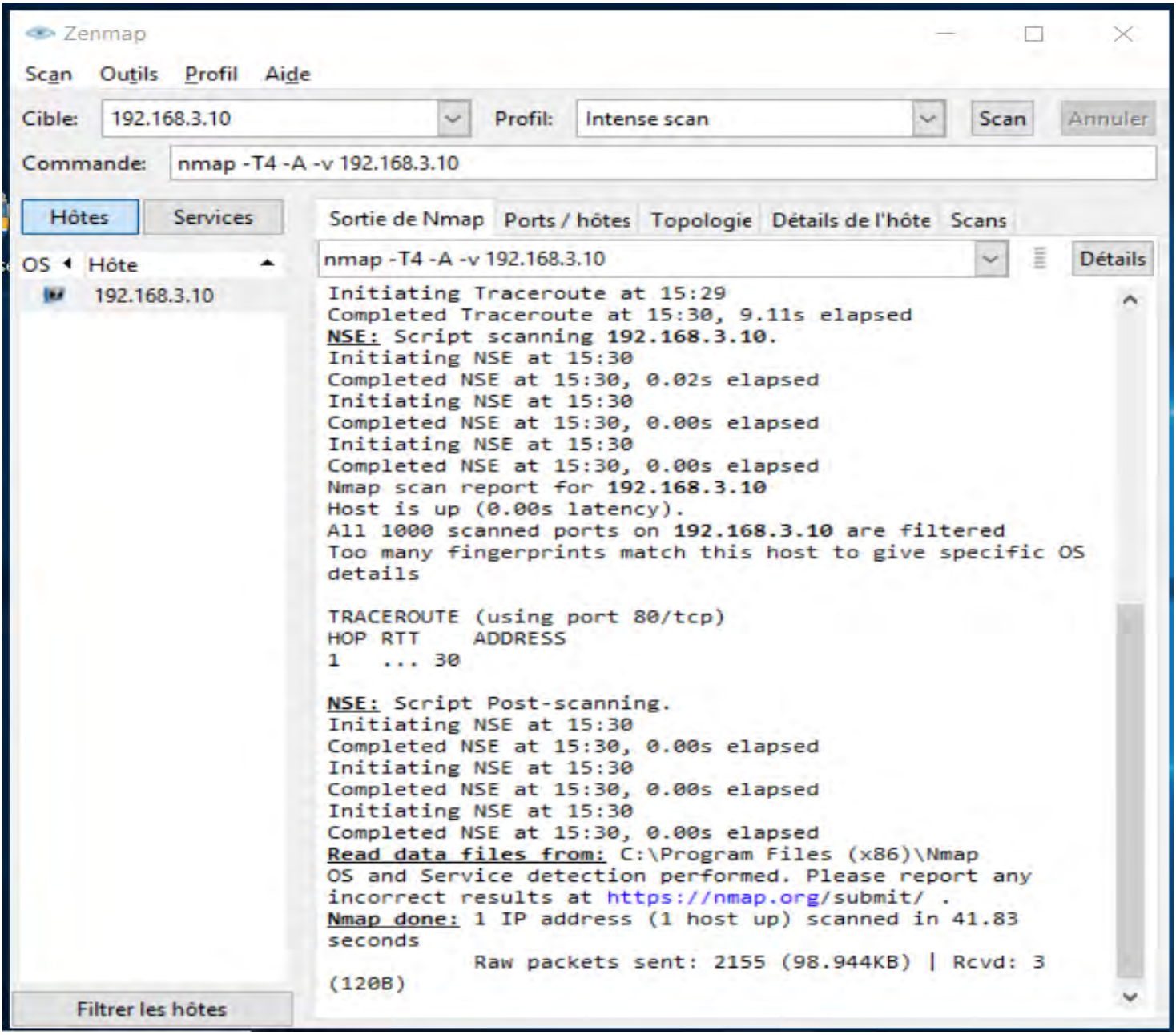
5. Test de la solution

5.1. Zenmap

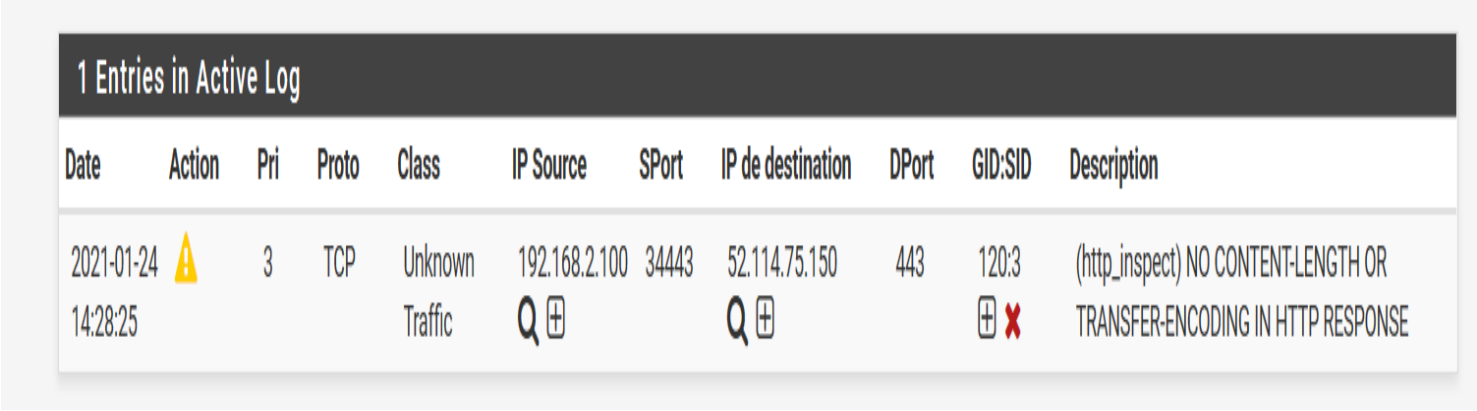
5.1.1. Maquette de test sur une machine se trouvant dans notre LAN.



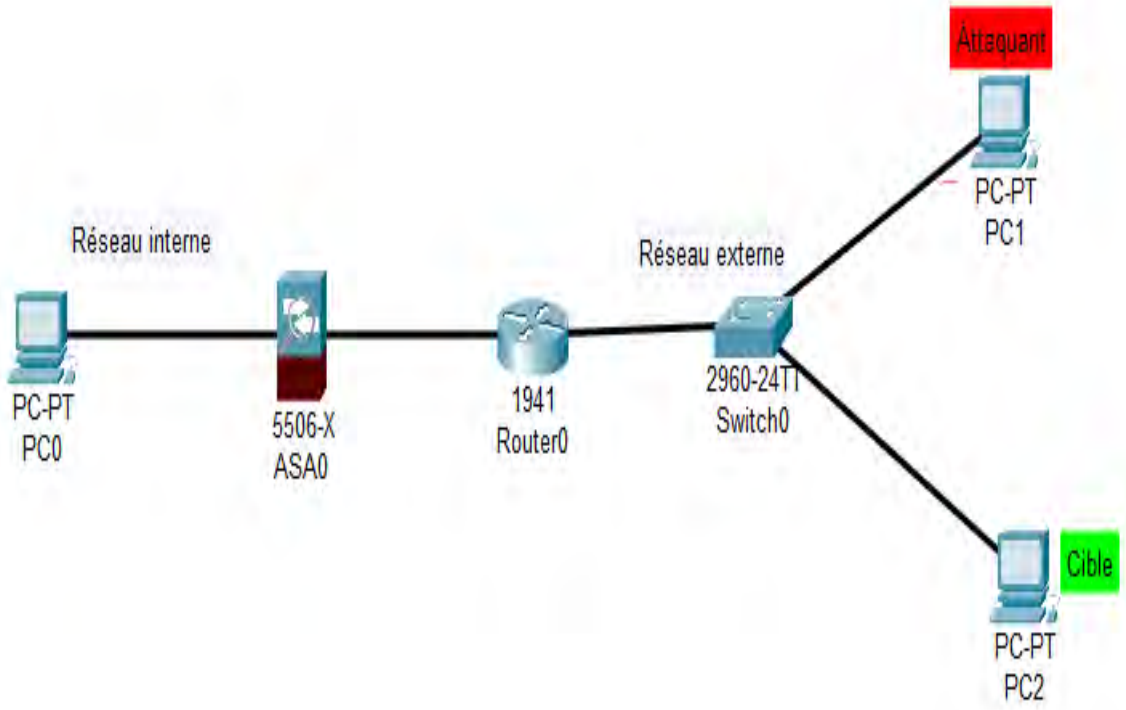
Résultat du scan : Nous n'avons aucune information que ce soit sur les ports ou sur le système d'exploitation.



Au niveau de Snort nous voyons une alerte qui s'est créée.



5.1.2. Maquette de test sur une machine se trouvant au niveau du WAN



Résultat du scan : Nous avons des informations sur les ports ouverts et le type d'OS utilisé.

```
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:FC:06:8B (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: DESKTOP-TO3TC6V, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:fc:06:8b (VMware)
| Names:
|   DESKTOP-TO3TC6V<20>  Flags: <unique><active>
|   DESKTOP-TO3TC6V<00>  Flags: <unique><active>
|_  WORKGROUP<00>        Flags: <group><active>
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-25T12:02:25
|_  start_date: N/A
```

II. Conclusion

Dans ce chapitre nous avons présenté, installé et configuré le pare-feu pfSense, nous avons aussi montré les services et les fonctionnalités qu'il offre. Nous avons aussi installé et configuré l'IDS Snort et enfin nous avons fait des tests avec l'outil Zenmap.

Les systèmes de détection et de prévention d'intrusion complètent les taches des autres équipements de sécurité comme les antivirus, les VPN …

Conclusion générale

De nos jours, la sécurité des réseaux informatiques demeure un sujet très complexe pour les acteurs du monde informatique, car les enjeux qui tournent autour de ce sujet sont très importants et les variables difficiles à maitriser.

Ce document présente quelques notions en sécurité informatiques en générale dont les systèmes de détection et de prévention d'intrusion. Pour montrer comment les IDS et IPS fonctionnent, nous avons pris comme exemple Snort sous le pare-feu pfsense qui est un très bon outil pour la détection et la prévention d'intrusion. Il effectue en temps réel des analyses du trafic et journalise les paquets IP suspicieux transitant sur le réseau.

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 informatique ne permet de garantir une sécurité fiable à 100%.

Webographie

https://www.frameip.com/firewall (Décembre 2020)

https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information (Janvier 2021)

https://www.reddit.com/r/PFSENSE/comments/fw6b0l/does_pfsense_have_waf_capabilities_to_filter_on/https://blog.varonis.fr/ (Janvier 2021)

https://doc.sambaedu.org/installer_reseau_test/co/presentation_pfsense.htmlhttps://www.certilience.fr/ (Janvier 2021)

https://www.securiteinfo.com (Février 2021)

https://www.rene-reyt.fr/documents/informatique/petit-resume-de-securite-informatique/securite-informatique-les-techniques-dattaque/ (Février 2021)

Jabou Chaouki Détection d'anomalies sur le réseau 2009 (Février 2021)

https://fr.wikipedia.org/wiki/PfSense (Février 2021)

docs.netgate.com/pfsense/en/latest/index.html (Mars 2021)

https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/#:~:text=Local%20Area%20Network%20(LAN)%20ou,Network%20(GAN)%20ou%20r%C3%A9seau%20global (Avril 2021)

https://fr.wikipedia.org/wiki/Encapsulation_(r%C3%A9seau)#:~:text=L'encapsulation%2C%20en%20informatique%20et,protocole%20dans%20un%20autre%20protocole. (Avril 2021)

https://fr.wikipedia.org/wiki/Routage (Avril 2021)

https://fr.wikipedia.org/wiki/Routage_dynamique#:~:text=Le%20routage%20dynamique%20ou%20routage,de%20communication%20dans%20un%20syst%C3%A8me. (Mai 2021)

https://fr.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol (Mai 2021)

https://fr.wikipedia.org/wiki/File_Transfer_Protocol#:~:text=File%20Transfer%20Protocol%20(protocole%20de,des%20fichiers%20sur%20cet%20ordinateur. (Mai 2021)

https://fr.wikipedia.org/wiki/HyperText_Transfer_Protocol_Secure (Mai 2021)

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/le-https-cest-quoi/ (Mai 2021)

https://fr.wikipedia.org/wiki/Routing_Information_Protocol#:~:text=Routing%20Information%20Protocol%20(RIP%2C%20protocole,de%20communiquer%20aux%20routeurs%20voisins. (Mai 2021)

https://web.maths.unsw.edu.au/~lafaye/CCM/internet/telnet.htm (Mai 2021)

https://fr.wikipedia.org/wiki/Telnet (Mai 2021)

https://www.frameip.com/dns/ (Mai 2021)

https://fr.wikipedia.org/wiki/Domain_Name_System (Mai 2021)

https://cisco.goffinet.org/ccna/services-infrastructure/protocole-resolution-noms-dns/#:~:text=Le%20protocole%20et%20le%20syst%C3%A8me,principalement%20le%20port%20UDP%2053. (Mai 2021)

https://www.ionos.fr/digitalguide/serveur/know-how/udp-user-datagram-protocol/ (Mai 2021)

https://fr.wikipedia.org/wiki/User_Datagram_Protocol (Mai 2021)

https://fr.wikipedia.org/wiki/Secure_Shell (Mai 2021)

https://www.ionos.fr/digitalguide/serveur/outils/protocole-ssh/ (Mai 2021)

https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-linternet-protocol-definition-dip/#:~:text=appel%C3%A9s%20datagrammes%20IP).-,Le%20protocole%20IP%20%3A%20d%C3%A9finition%20et%20historique,donn%C3%A9es%20dans%20les%20r%C3%A9seaux%20num%C3%A9riques. (Mai 2021)

https://www.websecurity.digicert.com/fr/ca/security-topics/what-is-ssl-tls-https (Mai 2021)

https://www.ionos.fr/assistance/email/microsoftr-outlook/quest-ce-que-pop3/ (Mai 2021)

https://fr.wikipedia.org/wiki/Internet_Message_Access_Protocol (Mai 2021)

https://blog.netwrix.fr/2019/07/24/tout-ce-quil-faut-savoir-sur-les-equipements-reseau/ (Mai 2021)

https://fr.wikipedia.org/wiki/Serveur_informatique (Mai 2021)

https://fr.wikipedia.org/wiki/Exploit_(informatique) (Mai 2021)

Table des matières

Les mots clés

Snort
Réseau
Scan
Intrusion
Détection
Attaque
IPS : Système de Prévention d'Intrusion (Intrusion Prevention System)
IDS : Système de Détection d'Intrusion (Intrusion Detection System)
DMZ : Zone démilitarisée (Demilitarized Zone)
HIPS : Système de Prévention d'Intrusion Hôte (Host-based Intrusion Detection System)
NIDS : Système de Détection d'Intrusion Réseaux (Network-based Intrusion Detection System)
INTERNET : Réseau Interconnecté (Interconnected Network)
WAN : Réseau étendu (Wide Area Network)
LAN : Réseau Local (Local Area Network)
IP : Protocole d'Internet (Internet Protocol)
TCP : Protocole de Contrôle de Transmission (Transmission Control Protocol)
DoS : Déni de Service (Denial of Services)
DDoS : Déni de Service Distribué (Distributed Denial of Services)
VPN : Réseau Privé Virtuel (Virtual Private Network)

Résumé

Le principal objectif de cette étude est porté sur la mise en place d'un système de détection d'intrusion pour sécuriser un réseau local en utilisant un IDS réseau qui est Snort.

Dans le premier chapitre, nous avons d'abord commencé par contextualiser le milieu dans lequel évoluent les entreprises, ensuite nous avons décrit une problématique de sécurité à laquelle sont confrontées les entreprises et enfin avons proposé une solution.

Dans le deuxième chapitre, nous avons fait une étude théorique en énonçant d'abord l'historique de l'avènement des réseaux informatiques, nous avons aussi étudié les objectifs de la sécurité informatique, nous avons vu quelques notions de base sur la sécurité des systèmes d'information, ensuite nous avons vu la notion de politique de sécurité, nous avons aussi vu quelques attaques sur les systèmes d'information notamment les attaques sur les réseaux, les attaques sur les hôtes et les attaques sur les applications et les contres mesures à adopter pour se défendre et enfin nous avons étudié les système de détection d'intrusion ainsi que leurs types, leur fonctionnement et leur architecture.

Dans le dernier chapitre, nous avons eu une approche pratique en présentant et en installant d'abord le pare-feu pfSense, puis nous avons présenté le système de détection d'intrusion open source Snort, ensuite nous avons installé et configuré Snort et enfin nous avons fait un test de scan sur une machine se trouvant sur notre réseau donc sécurisé et sur une autre machine ne se trouvant pas sur notre réseau donc non sécurisé et avons affiché les résultats des scans.

Summary

The main objective of this study is to set up an intrusion detection system to secure a local network using a network IDS which is Snort.

In the first chapter, we first started by contextualizing the environment in which companies operate, then we described a security problem facing companies and finally proposed a solution.

In the second chapter, we made a theoretical study by first stating the history of the advent of computer networks, we also studied the objectives of computer security, we saw some basics on the security of systems information, then we saw the concept of security policy, we also saw some attacks on information systems including attacks on networks, attacks on hosts and attacks on applications and countermeasures to adopt to defend themselves and finally we studied intrusion detection systems as well as their types, their operation and their architecture.

In the last chapter we took a hands-on approach by introducing and installing the pfSense firewall first, then we introduced the open source intrusion detection system Snort, then we installed and configured Snort and finally we We did a scan test on a machine located on our network therefore secure and on another machine not located on our network therefore not secure and displayed the results of the scans.